RAPORT O ZAGROŻENIACH

DRUGA POŁOWA 2014r.

F-Secure

SPIS TREŚCI

RAPORT O ZAGROŻENIACH W DRUGIEJ POŁOWIE 2014 R. – PRZEGLĄD...

KALENDARZ INCYDENTÓW

Strona 8

LIPIEC	SIERPIEŃ	WRZESIEŃ	PAŹDZIERNIK	LISTOPAD	GRUDZIEŃ
	Trojan SynoLocker atakuje urządzenia NAS	Usterka POODLE w szyfrowaniu SSL UE powołuje pilotażowy zespół ds. cyberprzestępczości	Złośliwe oprogramowanie w bankomatach na całym świecie Google umożliwia zabezpieczanie kont za pomocą kluczy USB		Auragold stworzony przez NSA podobno potrafi włamać się do każdej sieci bezprzewodowej Duże włamanie do Sonyskłania FBI do wydania ostrzeżenia

MOBILNE ZAGROŻENIA

Strona 14

Android nadal jest głównym celem ataków większości złośliwego oprogramowania mobilnego.
Zagrożenia wymierzone w iOS istnieją, ale jest ich znacznie mniej.

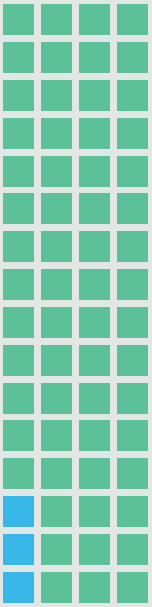
KOLER I SLOCKER

Od czasu debiutu w pierwszej połowie 2014r. Koler i Slocker, rodziny oprogramowania wymuszającego okup, szybko rosną w miarę, jak ich autorzy tworzą nowe warianty.
Jak wskazują statystyki detekcji u użytkowników naszych produktów, jest to obecnie najbardziej rozpowszechnione oprogramowanie wymuszające okup w urządzeniach z systemem Android.

TROJAN-SZPIEG: IPHONEOS/WIRELURKER

Pirackie aplikacje zawierające Wirelurkera są oferowane w niezależnych witrynach z aplikacjami do systemu OS X. Do urządzeń iOS, które podłączy się przez USB do zainfekowanych komputerów, pobierane są aplikacje. Apple zablokowało aplikacje zarażone Wirelurkerem w swoim sklepie.

NOWE RODZINY: 61 ANDROID + 3 iOS



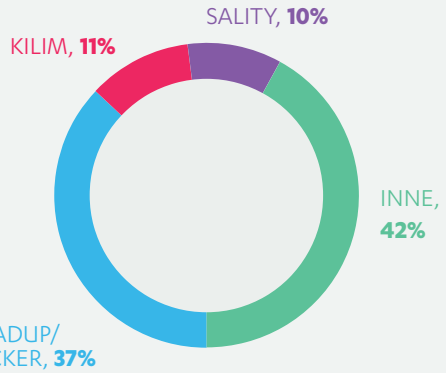
ZŁOŚLIWE OPROGRAMOWANIE DO KOMPUTERÓW PC

10 NAJCZĘSTSZYCH ZAGROŻEŃ

Strona 11

Lista najczęstszych zagrożeń dla komputerów z systemem Windows jest nadal zdominowana przez istniejące rodziny złośliwego oprogramowania. Niektóre z tych rodzin pozostają w obiegu od wielu lat i rozprzestrzeniają się poprzez infekowanie komputerów z niezałatanymi lukami w zabezpieczeniach.

PROCENTOWO



KLASYFIKACJA

1 DOWNADUP (znany też jako CONFICKER)
Ten 7-letni atakuje lukę MS08-067 w zabezpieczeniach systemu Windows. Rozprzestrzenia się przez internet oraz nośniki wymienne i udziały sieciowe.

2 KILIM
Zbiór złośliwych rozszerzeń przeglądarki internetowej, które publikują niepożądaną treść (wiadomości i/lub łącza, „lajki" itd.) na kontach użytkowników Facebooka. Mogą również zmieniać ustawienia przeglądarki.

3 SALITY
Duża rodzina wirusów, które infekują pliki EXE i ukrywają swoją obecność w zarażonym systemie. Warianty tego wirusa mogą przerywać procesy, kraść dane i wykonywać inne szkodliwe działania.

4 RAMNIT
5 AUTORUN
6 RIMECUD
7 MAJAVA
8 ANGLEREK
9 WORMLINK
10 BROWLOCK

ZŁOŚLIWE OPROGRAMOWANIE DO MACA

Strona 15

W krajobrazie zagrożeń do Maca pojawili się nowi przybysze, którzy próbują wypełnić dotychczas cichą scenę. Złośliwe oprogramowanie staje się bardziej wyrafinowane pod względem możliwości oraz metod dystrybucji.

17 NOWYCH WARIANTÓW odkrytych od LIPCA do GRUDNIA 2014 = 16 „TYLNYCH DRZWI" + 1 FAŁSZYWY ANTYWIRUS

3 NOWE RODZINY

WIRELURKER
Infekuje urządzenia iOS podłączone przez USB do zainfekowanych komputerów OS X.

VENTIR
Wykrada nazwy oraz hasła użytkowników i przekazuje je do zdalnego serwera.

XLSXMD
Używany w atakach typu Advanced Persistent Threat (APT).

PRZEDMOWA

Mikko Hypponen
Główny dyrektor ds. badań
F-Secure
@Mikko

Spędzam mnóstwo czasu, myśląc o naszych wrogach.

Mocno wierzę, że identyfikacja napastnika to jedna z najważniejszych rzeczy, które organizacja może zrobić, żeby się zabezpieczyć. To znaczy trzeba ustalić, kim jest przeciwnik.

Nie jest to tak proste, jak mogłoby się wydawać – różne organizacje są na celowniku różnych napastników. A nie ma mowy, żebyśmy się obronili, jeśli nie rozumiemy, kim są napastnicy. Różne grupy mają różne motywy; używają odmiennych technik i wybierają różne cele.

Różne ataki wymagają stosowania różnych środków obronnych. Ochrona danych i numerów kart kredytowych przed przestępcami internetowymi to coś zupełnie innego, niż ochrona sieci przed rozproszonym atakiem DoS gangu „haktywistów".

> "..identyfikacja napastnika to jedna z najważniejszych rzeczy, które organizacja może zrobić, żeby się zabezpieczyć"

Czymś zupełnie innym jest również ochrona organizacji przed atakiem szpiegowskim przypuszczonym przez wrogie państwo. Niektóre organizacje mogą być nawet celem ataku ekstremistów lub terrorystów.

Dobra wiadomość jest taka, że nie każda organizacja jest łakomym kąskiem dla wszystkich napastników.

Zła wiadomość jest taka, że nikt nie rozpozna napastników tak skutecznie, jak sama atakowana organizacja. Identyfikację napastników trudno powierzyć komuś innemu.

Wszyscy mamy ograniczone zasoby i budżety na ochronę sieci.
Zrozumienie wroga pomoże nam skoncentrować je tam, gdzie ma to największe znaczenie.

ZWOLENNICY PRYWATNOŚCI ZADAJĄCY NIEWŁAŚCIWE PYTANIA ROBIĄ WIĘCEJ SZKODY, NIŻ POŻYTKU

Sean Sullivan
Doradca
ds. bezpieczeństwa
F-Secure
@5ean5ullivan

Firma F-Secure niedawno przeprowadziła krótki sondaż badający postrzeganie bezpieczeństwa i prywatności. 1004 osoby (501 z Wielkiej Brytanii i 503 ze Stanów Zjednoczonych) odpowiedziały na następujące pytanie:

Czy masz coś do ukrycia?

Przewidywałem, że większość respondentów odpowie „nie", i 83 proc. rzeczywiście tak zrobiło. Odsetek odpowiedzi przeczących był nieco wyższy w Wielkiej Brytanii, niż w Stanach Zjednoczonych.

Czy wynik ten dowodzi, że ludziom nie zależy na prywatności? Nie! Oczywiście, że nie. Czy uczestnicy sondażu podali „niewłaściwą" odpowiedź (jak sugerowali w przeszłości niektórzy moi koledzy)? Nie. Odpowiedź jest właściwa – to pytanie było złe. Co przez to rozumiem?

Pytanie ludzi, czy mają coś do ukrycia, budzi skomplikowane i często sprzeczne emocje. Równie dobrze moglibyśmy zapytać: **„Czy jesteś nieuczciwy?"**. Pytanie jest nacechowane emocjonalnie, więc nic dziwnego, że ludzie reagują defensywnie – to zupełnie naturalne, że 83 proc. odpowiedziało przecząco. Oczekiwanie innego wyniku byłoby naiwne.

Następne pytanie w sondażu brzmiało:

Czy chciałbyś dzielić się wszystkim, co dzieje się w Twoim życiu, z każdym, wszędzie, cały czas, na zawsze?

Spodziewałem się, że większość znów odpowie „nie". Przewidywania okazały się prawidłowe – 89 proc. respondentów nie chciało być ekshibicjonistami. Ponownie odsetek odpowiedzi przeczących był nieco wyższy wśród Brytyjczyków, niż Amerykanów.

Moim zdaniem oba pytania zmierzają w jednym kierunku – czy prywatność jest ważna?

Ja myślę, że jest.

Niestety, obawiam się, że zbyt wielu zwolenników prywatności obecnie pyta ludzi, czy mają coś do ukrycia. A to nie służy sprawie.

W przyszłych sondażach planuję wypróbować pytania takie jak to:

Czy w Twojej przeszłości są rzeczy, o których wolałbyś zapomnieć?

Przewiduję, że większość zapytanych odpowie „tak".

A odpowiedź twierdząca skłoni ludzi do wysłuchania tego, co mamy im do powiedzenia.

UWAGI

1. Aby uzyskać więcej informacji o sondażu, w tym kopię danych, można skontaktować się z Seanem Sullivanem na Twitterze.

ARTYKUŁ

DLACZEGO?

David Perry
Gościnnie
http://davidperryvirus.com/

Jaka jest natura zagrożeń?

Co to oznacza dla Ciebie osobiście?

Jak te zagrożenia przejawiają się w Twoim życiu?

Jak mają się do tych, z którymi mieliśmy do czynienia w przeszłości?

Co można na to poradzić?

Utrata prywatności będzie znacznie groźniejsza, niż złośliwe oprogramowanie.

Powszechnie wiadomo, że istnieją programy napisane po to, żeby zniszczyć nasze komputery, tylko że wcale ich nie ma. Choć przez ostatnie 24 lata pracuję w branży bezpieczeństwa komputerowego i oglądam malware[1] pod mikroskopem, jeszcze nie widziałem żadnego wirusa, trojana, robaka ani żadnego innego złośliwego programu, który uszkodziłby system komputerowy. Dane, zgoda – niewielka część złośliwego oprogramowania niszczy dane i oprogramowanie, a jeszcze mniejsza wymazuje i nadpisuje pamięć ROM w BIOS-ie, ale uszkodzone monitory, dyski twarde lub systemy zhakowane tak, że nadają się tylko do kosza? Nigdy w życiu.

Jeśli wyrzuciłeś komputer dlatego, że był uszkodzony przez wirusy, to popełniłeś błąd. To się po prostu nie zdarza. Może uważasz inaczej. Może twierdzi tak Twój kuzyn, który pracuje z komputerami. Może znasz kogoś, kto zna kogoś w CIA, kto zarzeka się, że to prawda, ale nic z tych rzeczy. Owszem, w przyszłości jakiś jeszcze nieznany typ sprzętu komputerowego może zostać uszkodzony przez jeszcze nieznany typ złośliwego oprogramowania, ale pomimo licznych opowieści i filmów, które przekonują nas, że jest to na porządku dziennym, to się naprawdę nie zdarza.

Po drugie, być może chronisz swój komputer za pomocą programu antywirusowego (antivirus, AV). Może używasz też programu zwalczające złośliwe oprogramowanie (antimalware, AM). Ogólnie rzecz biorąc, nie ma funkcjonalnej różnicy między tymi narzędziami. Żaden program AV ani AM nigdy nie specjalizował się wyłącznie w wykrywaniu wirusów. O ile mi wiadomo, nawet najwcześniejsze programy AV wykrywały trojany i robaki. Większość złośliwego oprogramowania wykrywanego, blokowanego i usuwanego przez nowoczesne programy AV to nie wirusy. Wirusy, choć ciągle istnieją i wciąż są tworzone, obecnie stanowią tylko niewielką część malware'u.

Nie ma to znaczenia; wszystkie programy antywirusowe mają wykrywać całe złośliwe oprogramowanie. Nie daj się zwieść nazwie na pudełku. Wymyślają ją działy marketingu i dobierają tak, żeby znajome sformułowanie skłoniło Cię do kupienia produktu. Inne działy marketingu mogą liczyć na to, że nie rozumiejąc do końca, o co chodzi, kupisz drugi program do ochrony przed tym, przed czym jesteś już zabezpieczony. Wyjaśnienie, czego rzeczywiście potrzebujesz, nie jest zadaniem dla działów marketingu. To moje zadanie.

CO TO JEST MALWARE I CO ROBI?

Jak przed chwilą wyjaśniliśmy, malware to złośliwe i niepożądane oprogramowanie. Używają go różni ludzie do różnych celów. Może rysować obrazki albo pisać na ekranie. Może zniszczyć Twoje dane (obecnie rzadko to robi). Może ukraść Twoje hasło lub numer karty kredytowej, albo uzyskać dostęp do Twojego komputera. Może zaszyfrować Twoje dane i zażądać okupu. Może nawet zostać wykorzystane w celu uzyskania dostępu do systemów Twojego pracodawcy (albo pracodawcy Twojego krewnego lub przyjaciela).

PRZYPIS

1. Termin „malware" został wymyślony w 1990 r. przez Yisraela Radaia, niedawno zmarłego znawcy wirusów. Jest to ogólny termin na oznaczenie wirusów, trojanów, rootkitów, robaków, oprogramowania wyłudzającego okup, reklamowego, szpiegowskiego itd. Malware to zarówno złośliwe, jak i niepożądane oprogramowanie. Tak więc twierdzenie, że malware nigdy nie niszczy sprzętu komputerowego, to nie wybieg semantyczny, tylko fakty. To się nie zdarza. Czas przyzwyczaić się do tej myśli.

Obecnie często się zdarza, że złośliwe oprogramowanie wykorzystuje Twój system do ataku na ludzi, których nawet nie znasz. Z tych i tysiąca innych przyczyn warto je blokować. Istnieje jednak znacznie poważniejsze zagrożenie. Mamy na myśli ochronę prywatności.

PRYWATNOŚĆ

Możliwe, że prywatność taka, jaką rozumiemy dziś, to stosunkowo nowy wynalazek. W przeszłości ludzie wiedzieli, co inni robią za zamkniętymi drzwiami, bo tak naprawdę nie było żadnych zamkniętych drzwi. Cała wielopokoleniowa rodzina mieszkała w jednym pokoju. Mimo to od stuleci uważamy prywatność za niezbywalne prawo. Bliskie są nam idee praw i swobód obywatelskich. Oto cytat z deklaracji niepodległości Stanów Zjednoczonych:

> *Uważamy następujące prawdy za oczywiste: że wszyscy ludzie stworzeni są równymi, że Stwórca obdarzył ich pewnymi nienaruszalnymi prawami, że w skład tych praw wchodzi życie, wolność i swoboda ubiegania się o szczęście, że celem zabezpieczenia tych praw wyłonione zostały wśród ludzi rządy, których sprawiedliwa władza wywodzi się ze zgody rządzonych, że jeżeli kiedykolwiek jakakolwiek forma rządu uniemożliwiałaby osiągnięcie tych celów, to naród ma prawo taki rząd zmienić lub obalić i powołać nowy, którego podwalinami będą takie zasady i taka organizacja władzy, jakie wydadzą się narodowi najbardziej sprzyjające dla szczęścia i bezpieczeństwa.*

Zauważmy, że prywatność nie jest wymieniona wśród tych praw. Bywali tacy, którzy argumentowali przeciwko równości wobec prawa oraz naturze nienaruszalnych swobód. Jednak od pierwszych postanowień Wielkiej Karty Swobód, poprzez powstanie Stanów Zjednoczonych oraz wieki innych historycznych postępów, te założenia okazały się uniwersalne. Rozszerzono je o kilka innych praw, takich jak prawo do prywatności w domu i sumieniu. Ten ciąg historycznych zdarzeń można nazwać walką o sprawiedliwość. Jeśli ma to dla Ciebie znaczenie, pora, żebyś o tym pomyślał.

Jeśli nie ma prywatności, schronienia dla poglądów odmiennych od wyznawanych przez większość, to nie ma sprawiedliwości. Wyjaśnię to bliżej.

SCIENCE FICTION

W książce Graf Zero William Gibson przedstawił świat, w którym trzeba podjąć nadzwyczajne kroki, żeby uniknąć ciekawskich. Bohaterowie powieści proszą o pomoc niejakiego Finna, który zamyka ich w pokoju wypełnionym elektronicznymi obwodami blokującymi zewnętrzny monitoring. W filmie Wróg publiczny główny bohater mieszka w metalowej klatce, która chroni go przed elektronicznym podsłuchem. Może Cię to zdziwi, ale na świecie naprawdę są takie klatki. Noszą nazwę klatek Faradaya i są używane do różnych celów. Na przykład w F-Secure użyto klatki Faradaya do testowania złośliwego oprogramowania przenoszącego się bezprzewodowo między telefonami, żeby uniknąć zainfekowania innych telefonów w biurze.

Nie da się jednak spędzić życia w klatce. Żyjemy w przestrzeni publicznej, na ulicach, a co ważniejsze, jesteśmy podłączeni do sieci. Często nie zdajemy sobie z tego sprawy, ale każdy nasz krok jest nagrywany i analizowany. W ten sposób powstaje świat niemal powszechnego nadzoru.

Pomyśl o informacjach, które gromadzi Twój telefon. Zawiera całą Twoją pocztę, SMS-y, lokalizacje GPS, historię przeglądania, zdjęcia i numery, z którymi się łączyłeś. Nie jest to część jakiegoś złowrogiego planu, ale zwykłe środki reklamy i marketingu.

Ale co się dzieje, kiedy wszystkie ściany są przezroczyste? Odmówiono Ci kredytu na samochód lub mieszkanie? Zwolniono z pracy? Straciłeś pozycję w szkole lub w pracy? Płacisz za dużo na ubezpieczenie zdrowotne, ponieważ w Twojej rodzinie były przypadki cukrzycy lub innych chorób? Głosowałeś na kandydata, którego ktoś nie lubi? Niektórych z tych rzeczy nie ujawniasz bezpośrednio, ale łatwo je wydedukować. Ktoś może odmówić Ci tego czy tamtego i nawet nie dowiesz się, dlaczego.

STRACH

Wirusy nigdy nie budziły we mnie lęku. Nie boję się utraty danych, numeru karty kredytowej ani nawet pieniędzy. Mogę zawsze zarobić więcej pieniędzy albo zrobić więcej cyfrowych zdjęć, więc są to tylko uciążliwości, a w najgorszym razie szkody, z którymi można się pogodzić. Jeśli jednak stracę prywatność, jej odzyskanie będzie bardzo trudne i kosztowne. Zrób więc sobie przysługę i rozważ jakiś sposób na ochronę prywatności. Wszyscy eksperci zgadzają się, że powinieneś korzystać z wirtualnej sieci prywatnej (VPN), a tak się składa, że oferujemy rozwiązanie VPN, które jest łatwe w użyciu i bardzo bezpieczne. Nie rozwiąże ono wszystkich problemów, ale jest najlepszym pierwszym krokiem na drodze do lepszego jutra.

Switch on Freedom.

DRUGA POŁOWA 2014 r.
KALENDARZ INCYDENTÓW

CYFROWA WOLNOŚĆ

Sąd orzeka, że amerykańska policja potrzebuje nakazów rewizji urządzeń mobilnych

Czerwiec: Sąd Najwyższy Stanów Zjednoczonych orzeka, że policja musi uzyskać nakaz rewizji, aby zbadać urządzenia mobilne aresztowanych osób

Złośliwe oprogramowanie rzekomo śledzi aktywistów ruchu Umbrella

Październik: Okazuje się, że aplikacje rozpowszechniane wśród uczestników demonstracji w Hongkongu, gromadzą dane przechowywane w urządzeniach

ATAKI

Trojan Eskimo kradnie konta Steam użytkowników twitch.tv

Wrzesień: Bot naraża użytkowników platformy twitch.tv na infekcję złośliwym oprogramowaniem, które przejmuje ich konta w serwisie Steam

Home Depot potwierdza włamanie do sklepowych systemów kasowych

Wrzesień: Kasy używane w niektórych sklepach w Stanach Zjednoczonych i Kanadzie były zainfekowane złośliwym oprogramowaniem, które wykradało numery kart kredytowych i adresy e-mail klientów

Złośliwe oprogramowanie w bankomatach na całym świecie

Październik: W Malezji, Rosji i innych krajach zgłoszono przypadki instalowania złośliwego oprogramowania w bankomatach i późniejszego używania go do wypłacania pieniędzy z zainfekowanych maszyn

ZŁOŚLIWE OPROGRAMOWANIE

CosmicDuke łączy zagrożenia Cosmu i MiniDuke

Lipiec: Pojawia się pierwsze zagrożenia łączące loader wywodzący się z MiniDuke oraz kod oparty na Cosum, które wykrada dane z zainfekowanych systemów

SynoLocker atakuje urządzenia NAS

Sierpień: Trojan Synolocker atakuje sieciowe urządzenia pamięciowe (NAS); operator trojana później oferuje kupno kluczy do odszyfrowania danych

Pitou aktualizuje kod Srizbi w celu rozsyłania spamu

Sierpień: Nowy spambot Pitou dodaje nowe funkcje do starego kodu Srizbi i używa zainfekowanych systemów do rozsyłania spamu

Nowy wariant BlackEnergy przechodzi z kategorii oprogramowania przestępczego do APT

Wrzesień: Nowy wariant trojana BlackEnergy jest używany przez gang Quedagh do kradzieży danych od osób na Ukrainie i w Polsce

LUKI W ZABEZPIECZENIACH

Shellshock uderza w komputery z Linuksem, Uniksem

Wrzesień: Deweloperzy pospiesznie aktualizują programy narażone na atak w związku z usterką w popularnej powłoce GNUBourne Again Shell (BASH), pozwalającą zdalnym napastnikom uruchamiać kod na zainfekowanych komputerach

ŚCIGANIE

UE powołuje pilotażowy zespół ds. cyberprzestępczości

Wrzesień: UE powołuje zespół zadaniowy ds. cyberprzestępczości, w 6-miesięczny programie pilotażowym uczestniczy personel Europejskiego Centrum Cyberprzestępczości, FBI, NCA, niemieckiej policji federalnej

W Wielkiej Brytanii 3 osoby aresztowane za kradzieże z bankomatów przy użyciu złośliwego oprogramowania

Październik: Londyński Regionalny Zespół ds. Oszustw aresztuje 3 osoby za kradzieże z bankomatów, zarzuca im defraudację i pranie pieniędzy

Użytkownicy RAT aresztowani wskutek europejskiej operacji policyjnej

Listopad: 15 osób w kilku krajach UE aresztowano podczas skoordynowanej akcji za użycie BlackShades RAT

BEZPIECZEŃSTWO PRODUKTÓW

Xiaomi uszczelnia wyciek danych z telefonów do Mi-Cloud

Sierpień: Model Xiaomi RedMi 1S został zaktualizowany tak, że użytkownik musi wyrazić zgodę na komunikację chmurową, a dane wysyłane do chmury są szyfrowane

Google umożliwia zabezpieczanie kont za pomocą kluczy USB

Październik: Konta Google można teraz zabezpieczać dwuczynnikowo z wykorzystaniem fizycznego klucza USBsecurity

Microsoft wydaje awaryjną poprawkę usterki w Windows

Listopad: Wszystkie wspierane wersje Windows otrzymują poprawkę, która usuwa błąd uwierzytelniania użytkowników w komponencie Kerberos

Kalendarz incydentów przedstawia interesujące wydarzenia w dziedzinie cyfrowego bezpieczeństwa, które miały miejsce w drugiej połowie 2014 r. Informowały o nich różne portale technologiczne, publikacje badaczy bezpieczeństwa, witryny organów ścigania, popularne gazety oraz blog F-Secure. Źródła są wymienione na stronie 16.

CYFROWA WOLNOŚĆ

Brytyjski trybunał orzeka, że monitoring TEMPORA nie narusza praw człowieka

Grudzień: Investigatory Powers Tribunal (IPT) orzeka, że program monitoringu TEMPORA prowadzony przez brytyjską agencję GCHQ mieści się w ramach prawnych

Auragold stworzony przez NSA podobno potrafi włamać się do każdej sieci bezprzewodowej

Grudzień: Amerykańska agencja szpiegowska NSA rzekomo monitoruje wiadomości e-mail przesyłane między firmami telekomunikacyjnymi pod kątem dokumentów technicznych, które mogą pomóc we włamywaniu się do sieci bezprzewodowych

ATAKI

OnionDuke infekuje ruch w wyjściowym węźle TOR

Listopad: Rosyjski węzeł wyjściowy TOR wstawia złośliwe oprogramowanie do przechodzących przez niego programów Windows, aby kraść dane

Pakiet narzędziowy Regin używany do ataków APT w UE

Listopad: Z dokumentów ujawnionych przez Snowdena wynika, że pakiet Regin używany przez NSA i GCHQ szpieguje unijne agencje rządowe i belgijskiego operatora telekomunikacyjnego

Duże włamanie do Sony skłania FBI do wydania ostrzeżenia

Grudzień: Po ujawnieniu włamania do Sony FBI ostrzega amerykańskie firmy przed złośliwym oprogramowaniem, które może przejąć wszystkie dane w zainfekowanych systemach

ZŁOŚLIWE OPROGRAMOWANIE

Oprogramowanie Cryptowall 2.0 do wymuszania okupu znalezione „na wolności”

Październik: Nowy wariant trojana wymuszającego okup zawiera więcej funkcji zapobiegających analizie, zaktualizowane metody komunikacji

Linuksowy backdoor Turla może działać w systemie Solaris

Grudzień: Analiza linuksowego backdoora Turla ujawnia zbiór ustawień środowiskowych, które pozwalają mu działać w systemie Solaris

Pakiety exploitów Archie i Astrum na czarnym rynku

Grudzień: Nowe pakiety exploitów Archie i Astrum zdobywają przyczółek na podziemnym rynku przestępczych pakietów narzędziowych

LUKI W ZABEZPIECZENIACH

Usterka Poodle w szyfrowaniu ruchu internetowego

Wrzesie: Usterka wykryta w standardzie Secure Socket Layer(SSL) 3.0, nadal używanym przez starsze przeglądarki i serwery, może pozwolić pobliskiemu napastnikowi na przejęcie czyjegoś połączenia internetowego

ŚCIGANIE

3 osoby aresztowane w Chinach w związku ze złośliwym oprogramowaniem Wirelurker

Listopad: Podejrzani rzekomo stworzyli programy używane do ataku na urządzenia iOS podłączone do zainfekowanych maszyn

Inicjatywa CME wymierzona przeciwko trojanowi APT Moudoor

Grudzień: Producenci rozwiązań zabezpieczających podejmują inicjatywę Coordinated MalwareEradication (CME) mającą na celu trojana Moudoor używanego przez grupy szpiegowskie

UK teen pleads guilty to Spamhaus DDoS attacks

Grudzień: Londyński nastolatek przyznaje się do udziału w zeszłorocznych atakach DDoS na usługę antyspamową i sieć dystrybucji treści CloudFlarenetwork

BEZPIECZEŃSTWO PRODUKTÓW

Nadprogramowa poprawka luki CVE-2014-8439 w zabezpieczeniach Adobe Flash Player

Listopad: Adobe wydaje poprawkę luki CVE-2014-8439 w zabezpieczeniach programu Flash Player, która jest aktywnie atakowana przez pakiet exploitów Angler

Adobe wzmacnia poprawkę CVE-2014-8439

Listopad: Adobe wydaje kolejną poprawkę, aby zabezpieczyć Flash Player przed wykrytą wcześniej usterką CVE-2014-8439

Apple aktualizuje OS X, aby usunąć usterki w protokole NTP

Grudzień:Apple wydaje pierwszą zautomatyzowaną poprawkę do komputerów z systemem OS X, aby wyeliminować krytyczną lukę w obsłudze Network Time Protocol (NTP)

2. POŁ. 2014 PODSUMOWANIE KRAJOBRAZU ZAGROŻEŃ

NAJWAŻNIEJSZE NOWE ZAGROŻENIA

W detekcjach zgłoszonych do naszych systemów telemetrycznych przez użytkowników produktów F-Secure w drugiej połowie 2014 r. występowały pewne godne uwagi różnice w porównaniu z raportami zgromadzonymi w pierwszej połowie roku.

Podobnie jak w naszym raporcie za poprzednie półrocze, Downadup (znany też jako Conficker) zajmuje pierwsze miejsce na liście dziesięciu najczęstszych zagrożeń. Bardziej interesujące jest jednak rosnące znaczenie rodzin **Kilim, AnglerEK, Rimecud i Browlock**, które odzwierciedla zmiany i trendy w krajobrazie zagrożeń w 2014 r.

WYKORZYSTYWANIE LUK W ZABEZPIECZENIACH

Najbardziej godną uwagi tendencją w naszych raportach detekcji jest rosnąca dominacja złośliwego oprogramowania, które wykorzystuje luki w zabezpieczeniach. Oznacza to, że niezałatane systemy operacyjne i aplikacje wciąż przyczyniają się do statystyk detekcji, choć w znacznie mniejszej liczbie, niż w poprzednich latach.

Pewną szczególną postacią takiego złośliwego oprogramowania są pakiety exploitów – zestawy narzędzi podrzucane w zainfekowanych witrynach, która wykorzystują luki w zabezpieczeniach urządzeń gości witryny, żeby po cichu instalować szkodliwe oprogramowanie w ich komputerach. Pakiety exploitów Angler i Astrum (wymienione w naszych statystykach jako **AnglerEK i AstrumEK**) w 2014 r. szybko pięły się w górę naszych statystyk detekcji. Liczba detekcji pakietu AnglerEK rosła lawinowo, od kiedy zaczęliśmy wykrywać go we wrześniu 2014 r., co zapewniło mu poczesne miejsce na naszym wykresie częstości występowania zagrożeń (strona 13).

Złośliwe oprogramowanie, które atakuje luki w zabezpieczeniach platformy Java (określane łącznie mianem **Majava**) nadal jest wystarczająco skuteczne, aby pojawić się na naszej liście 10 najczęstszych zagrożeń. Możemy z tego wywnioskować, że użytkownicy nadal korzystają z niezałatanych wersji tej popularnej platformy deweloperskiej. Warianty rodziny **Wormlink**, które wykorzystują lukę w zabezpieczeniach systemu operacyjnego Windows, wskazują na inny popularny cel – niezałatane komputery Windows.

Rzut oka na podział zagrożeń według regionu (strona 12) pokazuje, że złośliwe oprogramowanie wymierzone w luki w zabezpieczeniach jest najbardziej aktywne w Ameryce Północnej i Europie. Choć generalizowanie bywa zwodnicze, wydaje się, że pozostałe regiony są bardziej narażone na „starsze" zagrożenia, które nie są już skuteczne przeciwko nowszym lub bardziej aktualnym systemom operacyjnym i programom.

Dlatego wydaje się uzasadnione twierdzenie, że częstość występowania oprogramowania atakującego luki w zabezpieczeniach jest luźno skorelowana z różnicami w zachowaniach użytkowników oraz konfiguracją komputerów w różnych regionach.

MEDIA SPOŁECZNOŚCIOWE I ROBAKI

Debiut **Kilima** – złośliwego rozszerzenia do przeglądarki, które atakuje użytkowników Facebooka – na liście dziesięciu najczęstszych zagrożeń ilustruje wykorzystanie witryn społecznościowych do rozprzestrzeniania złośliwego oprogramowania.

Choć zagrożenia wymierzone w sieci społecznościowe i (lub) używające ich do rozprzestrzeniania się nie są niczym nowym, jest to prawdopodobnie pierwszy rok, w którym rodzina zagrożeń atakująca jedną sieć społecznościową stała się tak powszechna. Obecność Kilima w Ameryce Południowej, na Bliskim Wschodzie i w Oceanii wynika bardziej z globalnego zasięgu Facebooka, niż z jakichkolwiek innych przyczyn, ale mimo to świadczy o wadze zagrożenia.

Choć znacznie mniej rozpowszechniona, rodzina robaków Rimecud również wykorzystuje sieci społecznościowe, żeby rozprzestrzeniać się między kontynentami.

Ciąg dalszy na stronie 13

10 NAJCZĘSTSZYCH ZAGROŻEŃ, DRUGA POŁOWA 2014 r.

37% CONFICKER/DOWNADUP

Robak, który atakuje lukę MS08-067 w zabezpieczeniach systemu Windows, aby rozprzestrzeniać się przez internet, nośniki wymienne i udziały sieciowe. Jest obecny na całym świecie już od 7 lat.

5 NAJBARDZIEJ ZAGROŻONYCH KRAJÓW
(na 10 000 użytkowników)

Zjednoczone Emiraty Arabskie	8,385
Malezja	6,274
Serbia	3,606
Rumunia	3,502
Brazylia	1,556

11% KILIM

Rodzina rozszerzeń do przeglądarki, które publikują niepożądaną treść (wiadomości i/lub łącza, „lajki" itd.) na kontach użytkowników Facebooka. Mogą też zmieniać ustawienia przeglądarki.

5 NAJBARDZIEJ ZAGROŻONYCH KRAJÓW
(na 10 000 użytkowników)

Wietnam	7,469
Filipiny	2,046
Tajlandia	1,776
Meksyk	1,265
Brazylia	1,388

10% SALITY

Duża rodzina wirusów, które infekują pliki EXE i ukrywają swoją obecność w zarażonym systemie. Warianty tego wirusa mogą przerywać procesy, kraść dane i wykonywać inne szkodliwe działania.

5 NAJBARDZIEJ ZAGROŻONYCH KRAJÓW
(na 10 000 użytkowników)

Pakistan	3,523
Egipt	1,856
Tunezia	1,095
Malezja	1,041
Turcja	1,020

8% RAMNIT

Rodzina wirusów, które infekują pliki EXE, DLL i HTML. Niektóre warianty mogą instalować plik, który próbuje pobrać więcej złośliwego oprogramowania ze zdalnego serwera.

5 NAJBARDZIEJ ZAGROŻONYCH KRAJÓW
(na 10 000 użytkowników)

Indonezja	6,527
Pakistan	3,976
Wietnam	2,645
Tunezja	1,486
Malezja	1,248

7% AUTORUN

Rodzina robaków, które rozprzestrzeniają się głównie za pośrednictwem zainfekowanych nośników wymiennych i dysków twardych. Mogą podejmować szkodliwe działania, takie jak kradzież danych, instalacja backdoorów („tylnych drzwi") itd.

5 NAJBARDZIEJ ZAGROŻONYCH KRAJÓW
(na 10 000 użytkowników)

Malezja	669
Turcja	315
Indie	306
Brazylia	160
Tajwan	143

7% MAJAVA

Zbiór exploitów atakujących deweloperską platformę Java. Udany atak może m.in. dać napastnikowi pełną kontrolę nad systemem.

5 NAJBARDZIEJ ZAGROŻONYCH KRAJÓW
(na 10 000 użytkowników)

Brazylia	132
Stany Zjednoczone	131
Kanada	113
Holandia	89
Włochy	54

7% RIMECUD

Rodzina robaków, które rozprzestrzeniają się głównie za pośrednictwem nośników wymiennych i komunikatorów internetowych. Mogą też instalować backdoory, które zapewniają zdalnemu napastnikowi dostęp i kontrolę nad systemem.

5 NAJBARDZIEJ ZAGROŻONYCH KRAJÓW
(na 10 000 użytkowników)

Hiszpanie	196
Francja	188
Włochy	89
Stany Zjednoczone	86
Wielka Brytania	81

6% ANGLEREK

Zbiór exploitów wymierzonych w różne luki w zabezpieczeniach. W najgorszym scenariuszu pomyślny atak może dać napastnikowi pełną kontrolę nad systemem.

5 NAJBARDZIEJ ZAGROŻONYCH KRAJÓW
(na 10 000 użytkowników)

Stany Zjednoczone	185
Szwajcaria	133
Kanada	122
Wielka Brytania	84
Holandia	62

5% WORMLINK

Specjalne spreparowane ikony skrótu używane do ataku na krytyczną lukę CVE-2010-2568 w systemie Windows w celu zyskania pełnej kontroli nad systemem.

5 NAJBARDZIEJ ZAGROŻONYCH KRAJÓW
(na 10 000 użytkowników)

Wietnam	2,945
Pakistan	1,438
Malezja	1,364
Tunezja	903
Filipiny	413

4% BROWLOCK

„Policyjne" oprogramowanie do wymuszania okupu, które przejmuje kontrolę nad systemem użytkownika, rzekomo za posiadanie nielegalnych materiałów. Następnie domaga się zapłacenia „grzywny" w celu przywrócenia normalnego dostępu.

5 NAJBARDZIEJ ZAGROŻONYCH KRAJÓW
(na 10 000 użytkowników)

Szwajcaria	138
Belgia	57
Stany Zjednoczone	55
Holandia	54
Niemcy	49

ZAGROŻENIA WEDŁUG REGIONU, DRUGA POŁOWA 2014

Większość zagrożeń zgłoszonych przez użytkowników F-Secure w drugiej połowie 2014 r. pochodziło z Europy i Azji, ale znacznie wzrosła liczba raportów z Ameryki Południowej.

7-letni robak Downadup wciąż nęka cztery regiony, lecz najczęściej występującym zagrożeniem w Ameryce Północnej jest teraz pakiet exploitów Angler. W Afryce dominuje wiekowa rodzina wirusów Sality. Najpoważniejszym zagrożeniem w Oceanii jest złośliwe oprogramowanie atakujące platformę Java.

AMERYKA PÓŁNOCNA

5 NAJCZĘSTSZYCH W REGIONIE, %

AnglerEK	**19**
CVE-2013-2460	19
AstrumEK	15
Majava	14
Rimecud	9

EUROPA

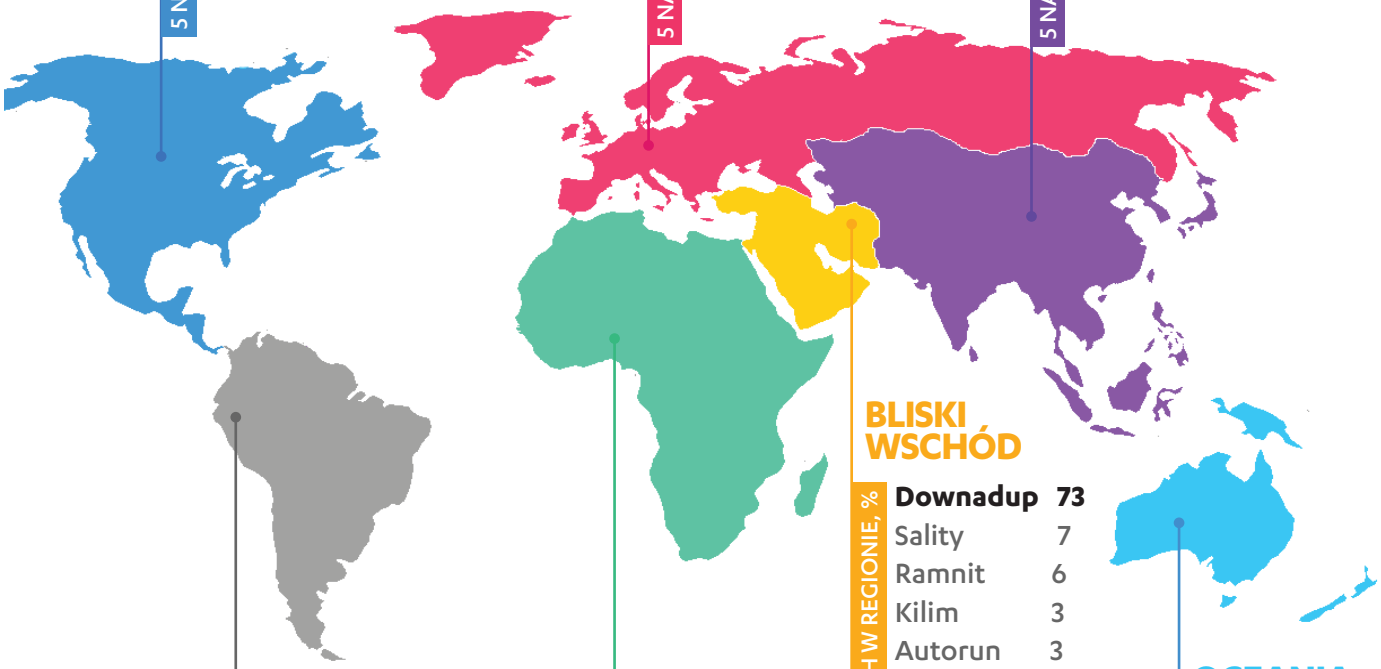
5 NAJCZĘSTSZYCH W REGIONIE, %

Downadup	**27**
Rimecud	13
AnglerEK	11
Majava	10
Autorun	8

AZJA

5 NAJCZĘSTSZYCH W REGIONIE, %

Downadup	**45**
Sality	12
Ramnit	12
Wormlink	9
Autorun	8



BLISKI WSCHÓD

5 NAJCZĘSTSZYCH W REGIONIE, %

Downadup	**73**
Sality	7
Ramnit	6
Kilim	3
Autorun	3

OCEANIA

5 NAJCZĘSTSZYCH W REGIONIE, %

Majava	**17**
Kilim	17
Autorun	16
AnglerEK	15
Rimecud	11

AMERYKA POŁUDNIOWA

5 NAJCZĘSTSZYCH W REGIONIE, %

Downadup	**33**
Kilim	28
Sality	13
Runouce	7
Majava	4

AFRYKA

5 NAJCZĘSTSZYCH W REGIONIE, %

Sality	**22**
Ramnit	20
Downadup	18
Autorun	10
Virut	9

Ciąg dalszy ze strony 10

OPROGRAMOWANIE WYMUSZAJĄCE OKUP

Wreszcie, kiedy przyglądamy się najczęstszym zagrożeniom zgłaszanym przez użytkowników naszych produktów (poniżej), rosnąca pozycja rodziny **Browlock** w statystykach detekcji odzwierciedla rozwój oprogramowania wymuszającego okup.

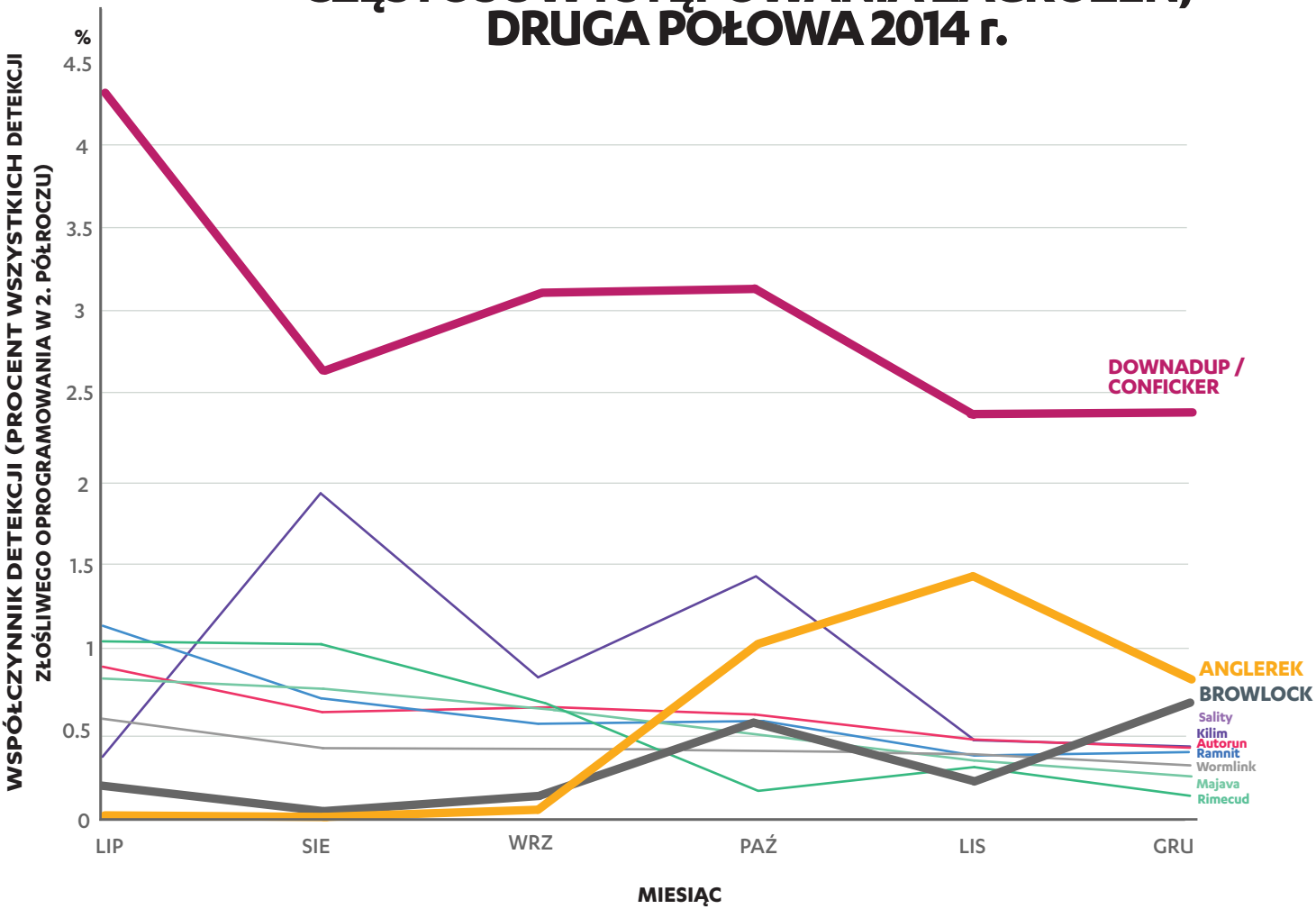
Ten konkretny typ złośliwego oprogramowania atakuje użytkowników od kilku lat i może być najbardziej problematycznym spośród obserwowanych zagrożeń. Choć szczegóły działania zależą od rodziny, bieżące odmiany oprogramowania wymuszającego okup zwykle szyfrują pliki, uniemożliwiając użytkownikom odtworzenie ich bez kluczy deszyfrowania przetrzymywanych przez napastników.

Oprócz starszych zagrożeń, takich jak **Cryptolocker i CryptoWall**, pojawiły się nowe godne uwagi rodziny, na przykład **CTB-Locker** i **SynoLocker**. Rodzina SynoLocker, która infekuje sieciowe urządzenia pamięciowe (NAS), to dowód na to, że twórcy złośliwego oprogramowania rozszerzają zasięg rażenia swoich produktów..

W systemie Anroid rośnie też liczba wariantów trojanów Koler i Slocker, obecnie największych rodzin oprogramowania wymuszającego okup od użytkowników tej platformy.

Ponieważ odszyfrowanie plików bez klucza jest niezwykle trudne, a płacenie okupu to sprawa dość drażliwa (zwłaszcza jeśli ofiarą jest firma), oprogramowanie wymuszające okup jest szczególnie kłopotliwym zagrożeniem. W przypadku infekcji zaleca się zgłosić incydent odpowiednim władzom i przywrócić pliki z czystej, niedawnej kopii zapasowej na oczyszczonym systemie.

CZĘSTOŚĆ WYSTĘPOWANIA ZAGROŻEŃ, DRUGA POŁOWA 2014 r.



ZAGROŻENIA MOBILNE, 2. POŁOWA 2014 R.

NOWE RODZINY

Oprogramowanie wymuszające okup w Androidzie

Rośnie liczba programów, które blokują dane i (lub) urządzenie użytkownika w celu wymuszenia okupu

Android **61**

iOS **3**

Próby inflitracji iOS

Napastnicy nie ustają w testowaniu zabezpieczeń iOS, szukając sposobów na włamanie się do systemu

KOLER I SLOCKER

Od czasu debiutu w pierwszej połowie 2014 r. Koler i Slocker, rodziny oprogramowania wymuszającego okup, szybko rosną w miarę, jak ich autorzy tworzą nowe warianty. Jak wskazują statystyki detekcji u użytkowników naszych produktów, jest to obecnie najbardziej rozpowszechnione oprogramowanie wymuszające okup w urządzeniach z systemem Android.

TROJAN:ANDROID/SVPENG

Ten trojan bankowy, który rozprzestrzenia się przez wiadomości SMS, wyświetla fałszywą stronę, kiedy użytkownik uruchamia aplikację bankową, i próbuje przechwycić informacje dotyczące logowania. Niektóre odmiany wymuszają też okup, blokując urządzenie i domagając się zapłacenia „grzywny" za rzekomą działalność przestępczą.

LOCKSCREEN I SCAREPACKAGE

Te dwa trojany wymuszające okup, odkryte przez badaczy bezpieczeństwa w drugiej połowie 2014 r., używają „policyjnych" powiadomień, aby skłonić użytkownika do zapłacenia „grzywny" za domniemaną działalność przestępczą. Oba zagrożenia są wykrywane przez produkty F-Secure jako warianty rodzin Koler i Slocker.

EXPLOIT:IPHONEOS/CVE-2014-4377

Specjalnie spreparowany dokument PDF otworzony w urządzeniach z niezałataną wersją iOS 7.1.x może wykorzystać lukę CVE-2014-4377 w zabezpieczeniach systemu; napastnik musiałby również wykorzystać drugą usterkę, aby zdalnie uruchomić kod.

TROJAN-SPY:IPHONEOS/WIRELURKER

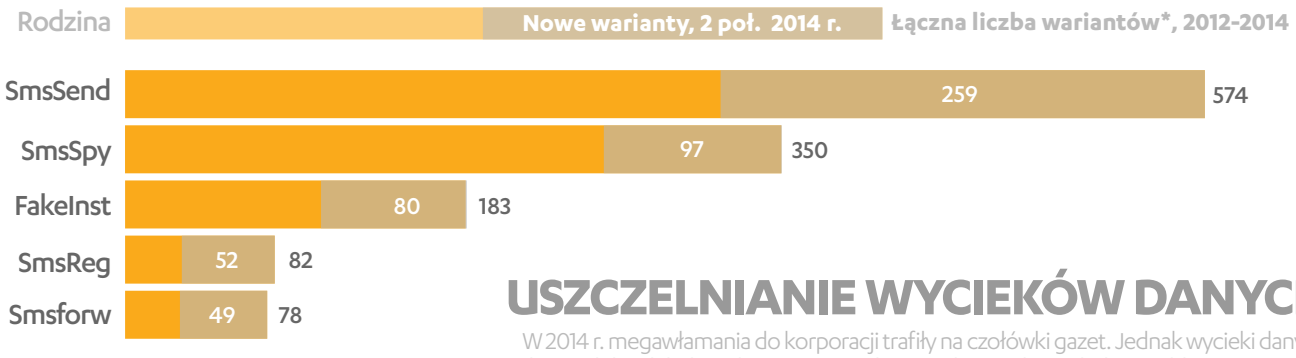
Pirackie aplikacje zawierające Wirelurkera są oferowane w niezależnych witrynach z aplikacjami do systemu OS X. Do urządzeń iOS, które podłączy się przez USB do zainfekowanych komputerów, pobierane są aplikacje. Apple zablokowało aplikacje zarażone Wirelurkerem w swoim sklepie.

BACKDOOR:IPHONEOS/XSSER

Narzędzie do zdalnej administracji przeniesione z Androida do iOS, które potrafi gromadzić dane (takie jak wiadomości SMS, przechowywane zdjęcia i kontakty) z urządzenia. Instalacja wymaga urządzenia po jailbreaku i skorzystania z pewnego niezależnego sklepu z aplikacjami.

NAJSZYBCIEJ ROSNĄCE RODZINY

Rodziny zaangażowane w wysyłanie SMSów premium rozwijały się najszybciej, gdyż ich twórcy zwiększają liczbę opracji i wariantów w ostatnim półroczu.



USZCZELNIANIE WYCIEKÓW DANYCH

W 2014 r. megawłamania do korporacji trafiły na czołówki gazet. Jednak wycieki danych z usług mobilnych były nieliczne, a wszystkie usterki zostały względnie szybko poprawione.

XIAOMI AKTUALIZUJE TELEFON

Producent smartfonów Xiaomi zaktualizował w sierpniu model Redmi Note tak, aby dostęp do usługi chmurowej nie był włączany domyślnie, lecz za zgodą użytkownika. Zabezpieczył również transmisję danych związanych z tą usługą.

SNAPCHAT ZATYKA WYCIEK

Witryna społecznościowa Snapchat zaktualizowała swoją aplikację do systemów Android i iOS, aby zapobiec „nadużyciom" wywołań API, które w grudniu doprowadziły do wycieku 4,6 mln nazw i haseł użytkowników z serwerów Snapchata.

***UWAGA:** Podano liczbę unikatowych wykrytych wariantów. Oznacza to, że przepakowane instalatory nie są liczone, a złośliwe oprogramowanie złożone z wielu komponentów liczy się tylko raz.

ZASOBY

1. Forbes; Anthony Kosner; 1 stycznia 2014 r.; https://www.forbes.com/sites/anthonykosner/2014/01/01/4-6-million-snapchat-usernames-and-phone-numbers-captured-by-api-exploit/
2. FSLabs; F-Secure Weblog; Testing the Xiaomi RedMi 1S - now with OTA update; 14 sierpnia 2014 r.; https://www.f-secure.com/weblog/archives/00002734.html
3. New York Times; Nicole Perlroth; Android Phones Hit by 'Ransomware'; 22 sierpnia 2014 r.; http://bits.blogs.nytimes.com/2014/08/22/android-phones-hit-by-ransomware/?_r=0

ZŁOŚLIWE OPROGRAMOWANIE DO MACA

2 POŁ. 2014 r.

17 NOWYCH WARIANTÓW złośliwego oprogramowania do Maca wykryto między LIPCEM a GRUDNIEM 2014 r.

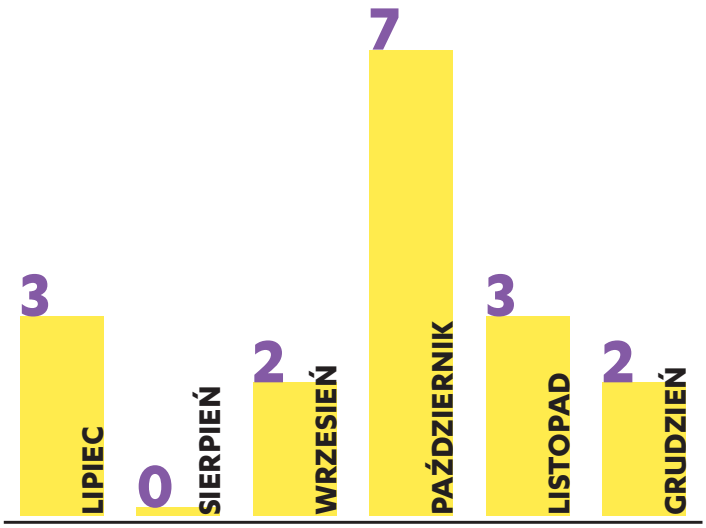
=

16 „TYLNYCH DRZWI”

+

1 FAŁSZYWY ANTYWIRUS

NOWE WARIANTY ODKRYTE W POSZCZEGÓLNYCH MIESIĄCACH



3 NOWE RODZINY

WIRELURKER

3 WARIANTY

Rodzina **WireLurker** składa się z backdoorów („tylnych drzwi”) rozpowszechnianych przez niezależny sklep z aplikacjami w Chinach. Złośliwe oprogramowanie z tej rodziny potrafi infekować urządzenia iOS podłączone do komputera OS X przez USB. Nawet urządzenie, którego nie poddano jailbreakowi, jest narażone na infekcję[1].

VENTIR

1 WARIANT

Rodzina **Ventir** składa się z backdoorów, które rejestrują nazwy i hasła użytkowników[2] oraz przekazują dane do zdalnego serwera.

XLSCMD

1 WARIANT

Rodzina **XLSCmd** składa się z backdoorów używanych do ataków typu ATP (Advance Persistent Threat, zaawansowane uporczywe zagrożenia). Ich kod jest dość podobny do odpowiedników działających w Windows, ale wersja do Maca ma dwie dodatkowe funkcje: rejestrowanie naciskanych klawiszy i robienie zrzutów ekranu[3].

***UWAGA:** Podano liczbę unikatowych wykrytych wariantów. Oznacza to, że przepakowane instalatory nie są liczone, a złośliwe oprogramowanie złożone z wielu komponentów liczy się tylko raz.

ZASOBY

1. Palo Alto Networks; Claud Xiao; WireLurker: A New Era In OS X And iOS Malware; 5 listopada 2014 r.; https://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/
2. Securelist; Mikhail Kuzin; The VentirTrojan: assemble your Mac OS spy; 16 października 2014 r.; https://securelist.com/blog/research/67267/the-ventir-trojan-assemble-your-macos-spy/
3. SC Magazine; Danielle Walker; Modular malware for OS X includes backdoor, keylogger components; 20 października 2014 r.; https://www.scmagazine.com/modular-malware-for-os-x-includes-backdoor-keylogger-components/article/378245/

ŹRÓDŁA

KALENDARZ INCYDENTÓW

CYFROWA WOLNOŚĆ

1. Adam Liptak; New York Times: Major Ruling Shields Privacy of Cellphones; Supreme Court Says Phones Can't Be Searched Without a Warrant; 25 czerwca 2014 r.; https://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html?_r=0
2. Sean Gallagher, Arstechnica; Year of the RAT: China's malware war on activists goes mobile; 3 października 2014; https://arstechnica.com/security/2014/10/year-of-the-rat-chinas-malware-war-on-activists-goes-mobile/
3. Owen Bowcott; The Guardian; UK mass surveillance laws do not breach human rights, tribunal rules; 5 grudnia 2014 r.; https://www.theguardian.com/uk-news/2014/dec/05/uk-mass-surveillance-laws-human-rights-tribunal-gchq
4. Ryan Gallagher; The Intercept; Operation Auroragold: How the NSA Hacks Cellphone Networks Worldwide; 4 grudnia 2014 r.; https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones/

ATAKI

5. FFSLabs; F-Secure Weblog; Twitch of Fate: Gamers Shamelessly Wiped Clean; 12 września 2014 r.; https://www.f-secure.com/weblog/archives/00002742.html
6. Maggie McGrath; Forbes; Home Depot Confirms Data Breach, Investigating Transactions From April Onward; 8 września 2014 r.; https://www.forbes.com/sites/maggiemcgrath/2014/09/08/home-depot-confirms-data-breach-investigating-transactions-from-april-onward/
7. Brian Krebs; Krebs on Security; Spike in Malware Attacks on Aging ATMs; 20 października 2014 r.; https://krebsonsecurity.com/2014/10/spike-in-malware-attacks-on-aging-atms/
8. FSLabs; F-Secure Weblog; OnionDuke: APT Attacks Via the Tor Network; 14 listopada 2014 r.; https://www.f-secure.com/weblog/archives/00002764.html
9. Morgan Marquis-Boire, Claudio Guarnieri i Ryan Gallagher; Secret Malware in European Union Attack Linked to U.S. and British Intelligence; 24 listopada 2014 r.; https://firstlook.org/theintercept/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/
10. Sean Sullivan; F-Secure Weblog; Who hacked Sony Pictures Entertainment and why?; 4 grudnia 2014 r.; https://www.f-secure.com/weblog/archives/00002771.html

ZŁOŚLIWE OPROGRAMOWANIE

11. Timo Hirvonen; F-Secure Weblog; CosmicDuke: Cosmu With a Twist of MiniDuke; 2 lipca 2014 r.; https://www.f-secure.com/weblog/archives/00002723.html
12. FSLabs; F-Secure Weblog; Pitou Q&A; 28 sierpnia 2014 r.; https://www.f-secure.com/weblog/archives/00002738.html
13. Arturri Lehtio; F-Secure Weblog; Ransomware Race (part 2): Personal media the next frontier?; 6 sierpnia 2014 r.; https://www.f-secure.com/weblog/archives/00002730.html
14. Sean Sullivan; BlackEnergy 3: An Intermediate Persistent Threat; 25 września 2014 r.; https://www.f-secure.com/weblog/archives/00002747.html
15. Arturri Lehtio; F-Secure Weblog; CryptoWall Updated to 2.0; 2 października 2014 r.; https://www.f-secure.com/weblog/archives/00002750.html
16. FSLabs; F-Secure Weblog; Mysterious Turla Linux Backdoor Also For Solaris?; 11 grudnia 2014 r.; https://www.f-secure.com/weblog/archives/00002775.html
17. Patricia Dacuno; Archie and Astrum: New Players in the Exploit Kit Market; 11 grudnia 2014 r.; https://www.f-secure.com/weblog/archives/00002776.html

LUKI W ZABEZPIECZENIACH

18. TTom Fox-Brewster; The Guardian; What is the Shellshock bug? Is it worse than Heartbleed? 25 września 2014 r.; https://www.theguardian.com/technology/2014/sep/25/shellshock-bug-heartbleed
19. Peter Bright; Arstechnica; SSL broken, again, in POODLE attack; 15 października 2014 r.; https://arstechnica.com/security/2014/10/ssl-broken-again-in-poodle-attack/

ŚCIGANIE

20. TTom Brewster; The Guardian; Europol launches taskforce to fight world's top cybercriminals; 1 września 2014 r.; https://www.theguardian.com/technology/2014/sep/01/europol-taskforce-cybercrime-hacking-malware
21. TTim Ring; SC Magazine; UK police arrest trio over £1.6 million cyber theft from cash machines; 24 października 2014 r.; https://www.scmagazineuk.com/uk-police-arrest-trio-over-16-million-cyber-theft-from-cash-machines/article/379115/
22. Europol; Users of Remote Access Trojans arrested in EU cybercrime operation; 20 listopada 2014 r.; https://www.europol.europa.eu/content/users-remote-access-trojans-arrested-eu-cybercrime-operation

23. John Leyden; The Register; Three WireLurker suspects arrested in China – reports; 17 listopada 2014 r.; https://www.theregister.co.uk/2014/11/17/wirelurker_suspects_china_arrests/
24. Timo Hirvonen; F-Secure Weblog; One Doesn't Simply Analyze Moudoor; 14 października 2014 r.; https://www.f-secure.com/weblog/archives/00002753.html
25. John Leyden; The Register; London teen pleads guilty to Spamhaus DDoS; 17 grudnia 2014 r.; https://www.theregister.co.uk/2014/12/17/london_teen_pleads_guilty_to_spamhaus_ddos/

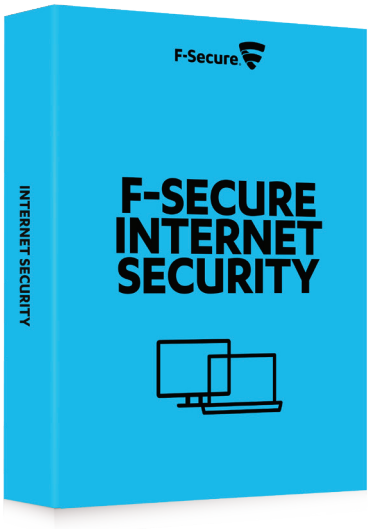
BEZPIECZEŃSTWO PRODUKTÓW

26. FSLabs; F-Secure Weblog; Testing the Xiaomi RedMi 1S - now with OTA update; 14 sierpnia 2014 r.; https://www.f-secure.com/weblog/archives/00002734.html
27. Google; Using Security Key for 2-Step Verification; 21 października 2014 r.; https://support.google.com/accounts/answer/6103523?hl=en
28. Brian Krebs; Krebs on Security; Microsoft Releases Emergency Security Update; 18 listopada 2014 r.; https://krebsonsecurity.com/2014/11/microsoft-releases-emergency-security-update/
29. Timo Hirvonen; F-Secure Weblog; Out-of-Band Flash Player Update for CVE-2014-8439; 25 listopada 2014 r.; https://www.f-secure.com/weblog/archives/00002768.html
30. Adobe; Security updates available for Adobe Flash Player; 25 listopada 2014 r.; https://helpx.adobe.com/security/products/flash-player/apsb14-26.html
31. Gregg Keizer; Computerworld; Apple deploys first-ever automatic patch to fix NTP flaw; 23 grudnia 2014 r.; https://www.computerworld.com/article/2862976/apple-deploys-first-ever-automatic-patch-to-fix-ntp-flaw.html

F-SECURE INTERNET SECURITY

Najlepsza na świecie ochrona surfowania, bankowości i zakupów w sieci

Kompletna ochrona dla tych, którzy surfują, robią zakupy, dokonują transakcji bankowych i używają mediów społecznościowych. F-Secure Internet Security zabezpiecza Twoją cyfrową treść i osobiste dane, chroniąc Cię w czasie rzeczywistym przez złośliwym oprogramowaniem, hakerami i kradzieżą tożsamości. Ochrona bankowości gwarantuje bezpieczeństwo Twoich transakcji online, a Ty i Twoje dzieci jesteście chronieni przed szkodliwymi i ordynarnymi witrynami internetowymi.



AV-TEST BEST PROTECTION AWARD
www.av-test.org

PREISTIPP LOGO FOR GOOD VALUE
www.com-magazin.de

PC ADVISOR ONLINE
www.pcadvisor.co.uk

F-SECURE FREEDOME

Zgromadziliśmy najbardziej zaawansowane zabezpieczenia — VPN, ochronę przed wirusami, szpiegostwem i wyłudzaniem danych — w jednej intuicyjnej usłudze. Freedome zaczyna Cię chronić za jednym naciśnięciem przycisku.

Usługa jest dostępna w Europie, Ameryce Północnej, Ameryce Łacińskiej, Tajlandii, Turcji i Rosji.

BĄDŹ NIEWIDOCZNY, NIE DAJ SIĘ WYŚLEDZIĆ

„Jeśli potrzebujesz bezpiecznego połączenia między urządzeniem iOS lub Android a światem online, zapewni Ci ją Freedome".

– PCWorld, 25 kwietnia 2014 r.

GET IT ON Google play

Download on the App Store

SWITCH ON FREEDOM