RAPORT ZAGROŻEŃ

DRUGA POŁOWA 2013

Chronimy to, co dla Ciebie ważne| www.f-secure.com

F-Secure

Ochrona przez całą dobę

Pracę Response Labs wspierają automatyczne systemy, które śledzą zagrożenia w czasie rzeczywistym, gromadząc i analizując setki tysięcy próbek danych każdego dnia. Przestępcy, którzy wykorzystują wirusy i złośliwe oprogramowanie do celów zarobkowych, nieustannie pracują nad nowymi sposobami ataku. Sytuacja wymaga ciągłej czujności, aby nasi klienci zawsze byli chronieni.

F-Secure Labs

AW laboratoriach F-Secure w Helsinkach w Finlandii i w Kuala Lumpur w Malezji eksperci od bezpieczeństwa nieustannie pracują, aby zapewnić naszym klientom ochronę przed zagrożeniami czyhającymi w sieci.

W każdym momencie personel F-Secure Response Labs monitoruje światową sytuację w zakresie bezpieczeństwa, aby szybko i efektywnie radzić sobie z nagłymi epidemiami wirusów i złośliwego oprogramowania.

.

PRZEDMOWA

MIKKO HYPPÖNEN
DYREKTOR DS. BADAŃ,
F-SECURE LABS
HTTP://TWITTER.COM/MIKKO

Nasi przeciwnicy wciąż się zmieniają. Kiedyś zwalczaliśmy internetowych hakerów. Potem internetowych przestępców. Dziś coraz większe obawy budzi postępowanie rządów.
Ale czy inwigilacja rządowy jest rzeczywistym problemem w świecie, w którym każdy zdaje się beztrosko dzielić całym swoim życiem? Ludzie piszą na Twitterze, co jedzą na śniadanie, udostępniają swoją lokalizację na Forsquare, chwalą się randkami na Facebooku i publikują zdjęcia rodziny i przyjaciół na Instagramie. Dla niektórych nie jest to problem — przynajmniej na razie. Zresztą wszystkie te serwisy zachęcają do takich zachowań, ponieważ właśnie na nich zarabiają.

Udostępnienie zdjęć z zakrapianej imprezy nie ma wielkiego znaczenia, jeśli nie jesteś kimś szczególnie ważnym. Jeśli jednak po dziesięciu latach zostaniesz publiczną figurą, nauczycielem lub politykiem, sprawa będzie wyglądać inaczej, a wtedy może być za późno, żeby cokolwiek zmienić. W rzeczy samej, interesujące będą wybory prezydenckie w okolicach 2040 roku, kiedy zdjęcia i posty kandydatów z okresu młodzieńczego buntu zostaną wyciągnięte na światło dzienne ze starych serwisów społecznościowych i zarchiwizowanych forów dyskusyjnych.
Ale w inwigilacji rządowej nie chodzi o gromadzenie informacji, które udostępniamy publicznie i dobrowolnie. Chodzi o gromadzenie informacji, o których nawet nie wiemy, że je udostępniamy, takich jak słowa wpisywane w wyszukiwarkach, prywatne wiadomości e-mail i SMS albo lokalizacja naszego telefonu w danym momencie. Tego rodzaju inwigilacja jest możliwa dopiero od kilku lat za sprawą internetu i telefonów komórkowych. Właśnie dlatego się ją prowadzi: bo można. Ale sama techniczna możliwość inwigilacji wcale jej nie usprawiedliwia.

> “W INWIGILACJI RZĄDOWEJ NIE CHODZI O GROMADZENIE INFORMACJI, KTÓRE UDOSTĘPNIAMY PUBLICZNIE I DOBROWOLNIE.
>
> CHODZI O GROMADZENIE INFORMACJI, O KTÓRYCH NAWET NIE WIEMY, ŻE JE UDOSTĘPNIAMY”

STRESZCZENIE

W 2013 roku na całym świecie — a w szczególności w branży bezpieczeństwa komputerowego — było głośno o rzekomej inwigilacji obcych rządów i o działaniach hakerskich podejmowanych przez amerykańską Agencję Bezpieczeństwa Narodowego (NSA), które ujawnił Edward Snowden. Zalew tych rewelacji wzbudził obawy (delikatnie mówiąc) i skłonił niektórych do bliższego zbadania mechaniki przeglądania internetu przez większość dzisiejszych użytkowników w celu ustalenia, co naraża ich na inwigilację i gromadzenie danych. W naszym artykule poświęconym prywatności opisujemy, jak aktywność lub osobiste informacje użytkownika mogą zostać przechwycone i zgromadzone bez jego wiedzy, nawet podczas odwiedzania legalnych, „czystych" witryn.

Ogólny niepokój wywołany tymi wiadomościami sprawił m.in., że zainteresowano się działaniami, które podejmują firmy w celu ochrony prywatności swoich klientów. Producentów z branży bezpieczeństwa komputerowego pytano o stanowisko w sprawie złośliwego oprogramowania używanego przez rządy. Poszanowanie prywatności jest jedną z kluczowych wartości F-Secure, co znajduje odzwierciedlenie w sposobie, w jaki projektujemy nasze produkty. Ponadto zawsze wykrywaliśmy i będziemy wykrywać każdy złośliwy program, bez względu na jego źródło, w tym oprogramowanie tworzone przez agencje rządowe. Dotyczy to na przykład „tylnych drzwi" R2D2, które zaczęliśmy wykrywać w 2011 r.[1], a które podobno były używane przez niemiecki rząd.

Oprócz złośliwych programów rządowych zajmujących się gromadzeniem danych lub monitorowaniem, nie brak też oportunistycznych zagrożeń motywowanych chęcią zysku. Dobrym przykładem z drugiej połowy 2013 r. jest ukierunkowany atak na laptop zawodowego pokerzysty. W laptopie tym zainstalowano trojan zdalnego dostępu (Remote Access Trojan, RAT), który umożliwiał oglądanie ręki gracza podczas internetowych turniejów. Takie ataki na graczy popularnie zwanych „rekinami karcianymi" określa się mianem sharkingu (od ang. shark – rekin).

Jeśli chodzi o ataki w większej skali, przyjrzymy się bliżej botnetowi Mevade, który pojawia się na naszej liście 10 najczęstszych detekcji w minionym półroczu. Opiszemy najczęściej spotykanie warianty botnetu oraz używane przez niego serwery dowodzenia (C&C), a także sposób, w jaki korzysta on z sieci TOR i udostępnia pliki w sieci peer-to-peer (P2P) Kad.

Godnym uwagi wydarzeniem w drugiej połowie 2013 r. było aresztowanie osoby podejrzewanej o stworzenie i dystrybuowanie pakietów exploitów Blackhole i Cool. W miarę, jak liczba raportowanych detekcji tych pakietów zmniejsza się, przyglądamy się, jak inni rywale próbują wypełnić lukę, szczególnie pakiet Angler z exploitami wymierzonymi w Javę, Flasha i Silverlighta.

Jeśli chodzi o front zagrożeń mobilnych, spośród 10 krajów najczęściej raportujących złośliwe oprogramowanie do Androida na szczycie listy znalazły się Arabia Saudyjska i Indie. Wskazujemy pewne trendy w rodzajach aplikacji, które są przepakowywane lub „trojanizowane", i podkreślamy charakterystyczne cechy takich zmodyfikowanych pakietów. Badamy niezależne sklepy z aplikacjami, aby ustalić, jakie jest prawdopodobieństwo, że użytkownicy napotkają w nich złośliwe oprogramowanie, i analizujemy, w jaki sposób zagrożenia przedostają się do urządzeń z Androidem.

Profilujemy najpopularniejsze wektory ataku używane do dostarczania złośliwego oprogramowania do urządzeń użytkowników i odkrywamy, że najczęściej używane są kanały przeglądarkowe, z silnym naciskiem na exploity wymierzone w deweloperską platformę Javy. Jest to zresztą zbieżne z czołowym typem zagrożenia wśród 10 najczęstszych detekcji w omawianym okresie — atakami za pośrednictwem witryn internetowych.

Wreszcie w drugiej połowie 2013 r. zaobserwowaliśmy niewielki, ale stały wzrost liczby nowych zagrożeń na platformie Mac, choć nadal pozostaje ona bardzo mała w porównaniu z systemem Windows, a nawet z Androidem.

ŹRÓDŁO

1. F-Secure Weblog; Mikko Hypponen; *Possible Governmental Backdoor Found ("Case R2D2");* published 8 October 2011; http://www.f-secure.com/weblog/archives/00002249.html

SPIS TREŚCI

NINIEJSZY RAPORT NA TEMAT ZAGROŻEŃ OMAWIA TRENDY I NOWE WYDARZENIA ZAOBSERWOWANE W KRAJOBRAZIE ZŁOŚLIWEGO OPROGRAMOWANIA PRZEZ ANALITYKÓW F-SECURE LABS W DRUGIEJ POŁOWIE 2013 R. DOŁĄCZONO TEŻ STUDIA PRZYPADKÓW POŚWIĘCONE GODNYM UWAGI, SZEROKO ROZPOWSZECHNIONYM ZAGROŻENIOM Z TEGO OKRESU.

CWSPÓŁAUTORZY
BRODERICK AQUILINO
KARMINA AQUINO
CHRISTINE BEJERASCO
EDILBERTO CAJUCOM
SU GIM GOH
ALIA HILYATI
MIKKO HYYKOSKI
TIMO HIRVONEN
MIKKO HYPPONEN
SARAH JAMALUDIN
CHOON HONG LIM
ZIMRY ONG
MIKKO SUOMINEN
SEAN SULLIVAN
MARKO THURE
JUHA YLIPEKKALA

KALENDARZ INCYDENTÓW W DRUGIEJ POŁOWIE 2013 R.

NSA

HAKERSTWO I SZPIEGOSTWO

Wrzesień
Procesy sądowe prowadzą do publikacji sądowego nakazu
Tajny nakaz sądowy autoryzował „nowatorskie wykorzystanie" istniejącej technologii do gromadzenia danych przez NSA

Październik
NSA gromadzi listy kontaktów z usług e-mail i komunikatorów internetowych
Kontakty z usług e-mail i IM są przechwytywane podczas tranzytu przez międzynarodowe łącza danych

Październik
Raporty o podsłuchach NSA budzą oburzenie w wielu krajach
Francja, Niemcy i inne kraje protestują przed nadmierną inwigilacją ich obywateli

Listopad
NSA przechwytuje ruch między centrami danych
Program o nazwie MUSCULAR przechwytywał niezaszyfrowany ruch między centrami danych technologicznego giganta

Wrzesień
GCHQ rzekomo włamuje się do belgijskiej firmy telekomunikacyjnej
Raport o włamaniu w niemieckim Spieglu prowadzi do śledztwa w sprawie incydentu w Brukseli

Październik
Kod źródłowy i hasła wykradzione podczas włamania do witryny Adobe
Skradziono kod źródłowy wielu produktów Adobe, a także dane logowania użytkowników witryny Adobe

Październik
Włamanie do witryny vBulletin ujawnia dane klientów
Włamanie do witryny producenta oprogramowania do obsługi forów dyskusyjnych ujawnia dane klientów, w tym hasła

Listopad
Zaobserwowano masowe przekierowania ruchu internetowego
Ruch przechodził przez Białoruś i Islandię, badacze nie wiedzą, jak i dlaczego

BEZPIECZEŃSTWO I ŚCIGANIE

Lipiec
FBI oskarża 5 osób o „największe cyberataki w USA w ciągu ostatnich 7 lat"
Pięć osób oskarżono o masowe kradzieże numerów kart kredytowych od amerykańskich detalistów i banków

Sierpień
Rosja skazuje właściciela Chrono-Pay za wynajęcie botnetu
Sędzia skazuje Pavla Vrublevsky'ego na 2,5 roku kolonii karnej za cyberatak na rywala

Październik
Witryna narkotykowa Silk Road zamknięta, operator aresztowany
FBI oskarża obywatela Stanów Zjednoczonych o handel narkotykami i pranie pieniędzy

Październik
Twórca pakietów exploitów Black-Hole i Cool aresztowany
Rosja aresztuje „Pauncha", twórcę i operatora dwóch najbardziej rozpowszechnionych pakietów exploitów

Sierpień
Microsoft poprawia usterki ujawnione na konferencji CanSecWest

Wrzesień
Debiutuje iOS7 z nowymi zabezpieczeniami

Listopad
Microsoft wydaje poprawkę luki dnia zerowego CVE-2013-3906

Wrzesień
Komitet Praw Obywatelskich UE debatuje nad amerykańską inwigilacją
Komitet rozpoczyna badanie kwestii związanych z amerykańską inwigilacją obywateli UE

Wrzesień
RSA wycofuje algorytm szyfrowania „związany z NSA"
RSA Security ostrzega klientów, aby przestali używać szyfrowania, które prawdopodobnie zostało złamane przez NSA

Październik
EU uchwala poprawkę przepisów o ochronie danych
Prawodawcy zwiększają zakres ochrony prywatności w sieci; nowe prawo oczekuje na zatwierdzenie przez 28 krajów członkowskich

Listopad
Microsoft zwiększa nagrodę za wskazanie usterek do 100 000 dol
Firma liczy na to, że większa nagroda zachęci więcej osób do nadsyłania raportów o usterkach

ZŁOŚLIWE OPROGRAMOWANIE

Lipiec
„Tylne drzwi" Janicab ukrywają się przy użyciu znaku RLO
Złośliwa aplikacja używa znaku Right-to-Left Override (RLO), aby udawać, że jest plikiem Worda, a nie programem

Sierpień
Wymuszające okup oprogramowanie Browlock pojawia się w nowych krajach
Złośliwe oprogramowanie podszywające się pod komunikat policyjny rozszerza się ze Stanów Zjednoczonych, Wielkiej Brytanii i Kanady na Niemcy, Włochy i Francję

Wrzesień
Botnet Mevade używa sieci TOR do dystrybucji oprogramowania reklamowego, złośliwych aplikacji
Polecenia C&C dla szeroko rozpowszechnionego botnetu prowadzą do nagłego wzrostu ruchu w sieci anonimizującej

Październik
Ukierunkowane ataki wykorzystują lukę CVE-2013-3893
Ukierunkowane ataki wymierzone w usterkę w Internet Explorerze; wydano też moduł Metasploit wykorzystujący tę lukę

Lipiec
Zgłoszono lukę w zabezpieczeniach podobną do „Masterkey"
Chińscy badacze informują o luce, która umożliwia dodanie złośliwego kodu do nagłówka pliku

Lipiec
Mobilny trojan używa Google Cloud Messaging (GCM)
Mechanizm GCM jest używany przez trojan Tramp do odbierania zdalnych poleceń

Lipiec
Reklamy fałszywego mobilnego antywirusa
Reklamy fałszywego mobilnego antywirusa pojawiają się w aplikacjach i w mobilnych przeglądarkach

Sierpień
W dokumentacji FinFisher pojawia się informacja o obsłudze Windows Phone
Mobilne oprogramowanie szpiegowskie działa na wielu platformach, w tym Windows Phone

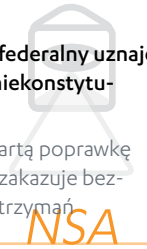
W kalendarzu incydentów za drugą połowę 2013 r. wymienione są interesujące zdarzenia związane z bezpieczeństwem informacji, które zostały opisane w różnych portalach technologicznych, publikacjach lub witrynach badawczych, ważnych gazetach lub na internetowym blogu F-Secure. Źródło każdej pozycji kalendarza jest wymienione na stronie 36.

Listopad
NSA podobno zainfekowała 50 000 systemów na świecie
Podłożone oprogramowanie ma na celu „gromadzenie danych wywiadowczych" z zainfekowanych systemów

Grudzień
NSA rzekomo śledzi miliony rozmów telefonicznych
Dane używane do śledzenia wspólników podróżujących ze znanymi celami w ramach programu „Co-Traveller"

Grudzień
NSA podobno „jeździ na grzbiecie" ciasteczek Google'a
NSA i GCHQ mają używać śledzących plików cookie w witrynach Google'a do lokalizowania celów

Grudzień
Amerykański sędzia federalny uznaje program PRISM za „niekonstytucyjny"
Program narusza czwartą poprawkę do konstytucji, która zakazuje bezzasadnych rewizji i zatrzymań



Listopad
Dane z włamania do Cupid Media znalezione na serwerze
Dane ze styczniowego włamania do witryny randkowej znaleziono na tym samym serwerze, co dane wykradzione z Adober

Listopad
Giełdy wymiany Bitcoina stają się celem cyberprzestępców
Szybujący kurs bitmonet prowadzi do ukierunkowanych ataków na internetowe portfele Bitcoin

Grudzień
Znaleziono serwer z danymi wykradzionymi przez botnet
Botnet Pony gromadził z zainfekowanych systemów dane logowania do popularnych witryn

Grudzień
Target informuje o naruszeniu bezpieczeństwa danych klientów
Napastnicy podobno zainfekowali systemy kasowe, aby gromadzić dane klientów

Listopad
FBI aresztuje dwóch braci pod zarzutem cyberwłamań
Dwaj bracia ze Stanów Zjednoczonych zostali oskarżeni o kradzież milionów z rachunków bankowych i maklerskich

Listopad
Wielka Brytania skazuje hakera Stratfor na 10 lat
Jeremy Hammond trafia do więzienia za kradzież informacji o kartach kredytowych z prywatnej agencji wywiadu.

Listopad
ICANN zamyka serwis „Dynamic Dolphin
Organ nadzorczy branży rejestracji domen odbiera licencję rejestratorowi, który sprzyjał spamerom

Grudzień
13 osób przyznaje się do udziału w ataku DoS na Paypal
Atak przeprowadzono w proteście przeciwko decyzji Paypala o zerwaniu związków z WikiLeaks

Grudzień
Adobe poprawia usterki Flasha i Shockwave'a

Grudzień
Microsoft poprawia lukę dnia zerowego CVE-2013-3906 i inne

Listopad
Giganci technologiczni wzmacniają zabezpieczenia przed podsłuchami NSA
Yahoo!, Google, Facebook i inni uszczelniają swoje systemy, aby zablokować potencjalne ingerencje NSA

Listopad
Facebook ostrzega użytkowników, którzy padli ofiarą włamania do Adobe
Serwis społecznościowy prosi użytkowników, którzy używają tych samych danych logowania do obu witryn, aby zmienili hasła

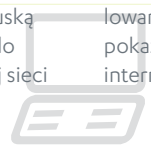
Listopad
UE wnosi o więcej praw dla swoich obywateli, których dane są przetwarzane w Stanach Zjednoczonych
UE domaga się prawa do zadośćuczynienia na zasadach prawa Stanów Zjednoczonych dla obywateli UE, którzy podlegali amerykańskiej inwigilacji

Grudzień
Microsoft, FBI i inni zakłócają działanie botnetu ZeroAccess
Przerwano kontakt między zainfekowanymi systemami w Stanach Zjednoczonych a adresami IP serwerów dowodzenia

Listopad
W Stanach Zjednoczonych i Wielkiej Brytanii ogłoszono alarm dotyczący CryptoLockera
Organy CERT w Stanach Zjednoczonych i Wielkiej Brytanii ostrzegają obywateli w związku z rosnącą liczbą raportów o tym oprogramowaniu wymuszającym okup

Listopad
Luka CVE-2013-3906 wykorzystywana w ukierunkowanych atakach
Specjalnie spreparowane pliki Worda wykorzystują tę lukę do ataków na Bliskim Wschodzie i w Azji Południowej

Grudzień
Znaleziono fałszywe „zaufane" certyfikaty dla domen Google'a
Fałszywe certyfikaty SSL podobno były używane przez francuską agencję bezpieczeństwa do szpiegowania w prywatnej sieci



Grudzień
Poinformowano o trojanie wymierzonym w pokerzystów
Złośliwe oprogramowanie instalowane po cichu na komputerze pokazuje karty gracza podczas internetowych meczów

Sierpień
Na konferencji BlackHat zaprezentowano lukę „Masterkey" w systemie Android
Usterka umożliwia edytowanie kodu aplikacji bez wpływu na podpis kryptograficzny

Sierpień
Exploit Masterkey znaleziony w wielu aplikacjach
W Chinach znaleziono aplikacje z exploitem wymierzonym w niedawno opublikowaną lukę „Masterkey"

Wrzesień
Poinformowano o obejściu czytnika linii papilarnych w iOS
Grupa hakerów opublikowała prosty sposób na obejście czytnika linii papilarnych w iPhonie 5S

Październik
Google wycofuje aplikacje z agresywną biblioteką reklamową
Aplikacje z biblioteką reklamową o kryptonimie „Ad Vulna" mają zostać wycofane ze sklepu, jeśli autorzy nie zaktualizują biblioteki

PRZEGLĄD

ZMIANY W KRAJOBRAZIE ZAGROŻEŃ

W miarę, jak coraz bardziej uzależniamy się od internetu i jego usług, nieuchronnie wzrasta zagrożenie naszej „połączonej społeczności". Według statystyk za drugą połowę 2013 r. (opartych na anonimizowanych danych, które są wysyłane do naszych chmurowych systemów telemetrycznych przez programy klienckie działające w komputerach stacjonarnych i urządzeniach mobilnych), liczba **ataków przeglądarkowych** — które zwykle wykorzystują specjalne techniki albo złośliwe oprogramowanie, aby przekierować przeglądarkę do złośliwej witryny — zwiększyła się dwukrotnie w tym sześciomiesięcznym okresie w porównaniu z pierwszą połową roku. Ataki przeglądarkowe były w rzeczywistości najczęściej raportowanym typem ataku, o czym świadczy nasza lista 10 najczęstszych detekcji w drugiej połowie 2013 r. (następna strona). Kiedy podzieliliśmy te zagrożenia według krajów, które raportują odpowiednie detekcje, stwierdziliśmy, że ataki przeglądarkowe są raportowane najczęściej w Szwecji, Francji, Finlandii i Niemczech.

Choć w atakach przeglądarkowych często używa się **exploitów**, ten konkretny typ zagrożenia klasyfikujemy oddzielnie ze względu na jego istotną pozycję wśród najbardziej rozpowszechnionych zagrożeń. Trzy czołowe detekcje związane z exploitami, które zaobserwowaliśmy w drugiej połowie 2013 r., to Majava oraz ataki wymierzone w luki CVE-2013-2471 i CVE-2013-1493. Nie przypadkiem wszystkie trzy mają związek z usterkami w deweloperskiej platformie Javy, która zyskała taką popularność wśród firm i deweloperów, że stała się głównym celem ataków. Ilustruje to nowa pozycja na naszej liście najczęstszych detekcji — wykrycia exploitów, które są wymierzone w lukę CVE-2013-2471 w niektórych aplikacjach Java Web Start oraz wersjach apletów Javy działających w piaskownicy.

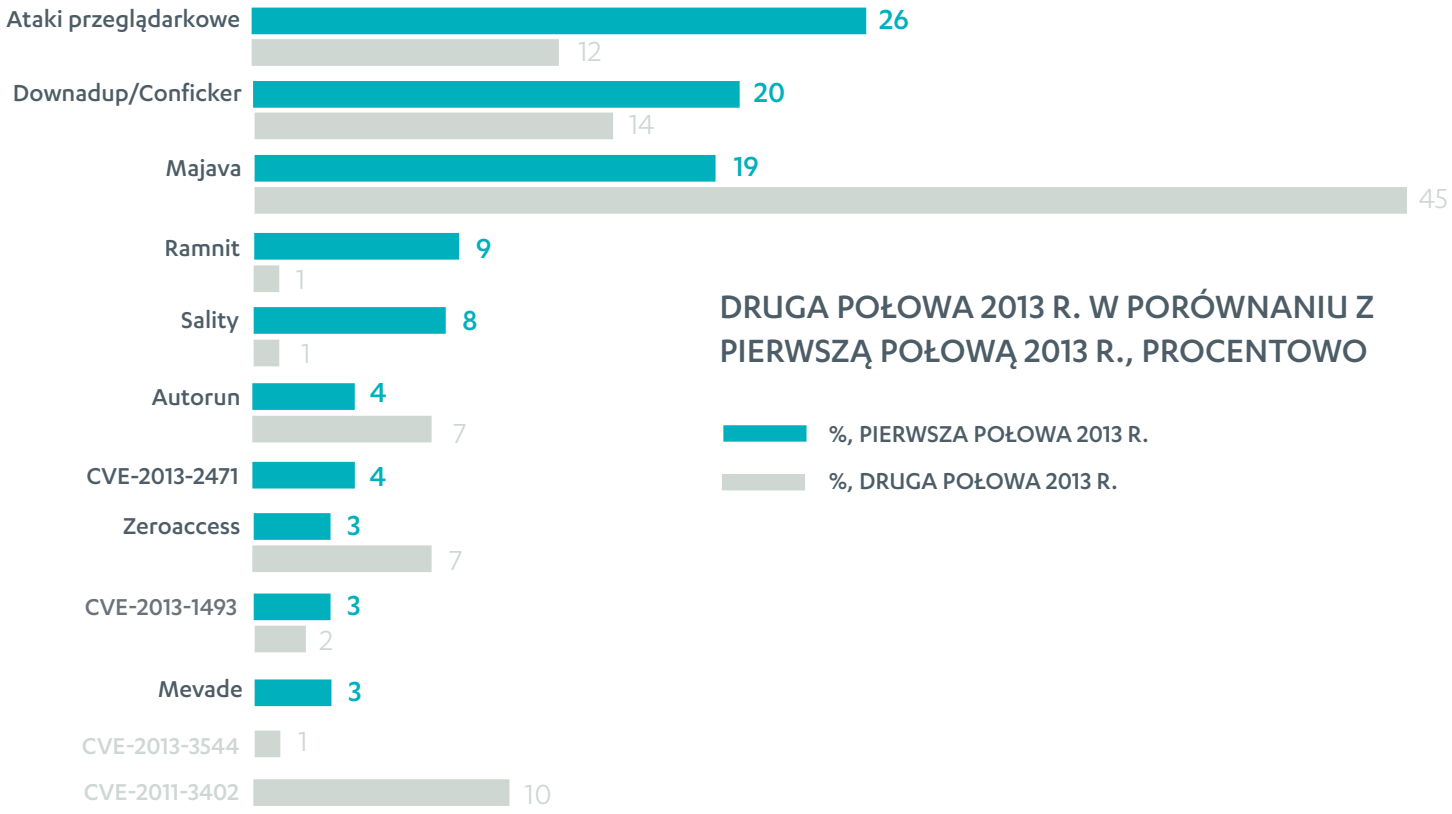
Jeśli połączymy procentowe udziały tych trzech zagrożeń (odpowiednio 19, 4 i 3 proc.), okaże się, że exploity związane z Javą stanowią drugi najczęściej raportowany typ zagrożenia w drugiej połowie 2013 r., przy czym większość raportów pochodzi ze Stanów Zjednoczonych, Francji, Niemiec i Finlandii. Jednak w rzeczywistości liczba exploitów związanych z Javą zmniejszyła się w porównaniu z pierwszą połową 2013 r. Może to mieć związek z październikowym zatrzymaniem „Pauncha"[1], domniemanego twórcy pakietów exploitów BlackHole i Cool, które odpowiadały za znaczną część ataków na Javę. Od tego czasu liczba raportowanych detekcji BlackHole i Cool znacznie spadła. Niestety, w ten sposób po prostu powstała pustka, którą usiłują zapełnić nowi pretendenci, na przykład twórca szybko zyskującego na popularności **pakietu exploitów Angler**.

Znanym, nadal aktywnym zagrożeniem jest robak, który identyfikujemy jako **Downadup** (w mediach zwany również Confickerem). Choć ma on już swoje lata (po raz pierwszy znaleziono go w 2008 r.), to nadal uparcie utrzymuje się w pierwszej dziesiątce detekcji. Pozostaje bardzo aktywny w Brazylii, niewiele mniej w Zjednoczonych Emiratach Arabskich, a niedaleko za tymi krajami plasują się Włochy.

Ciągłą aktywność robaka Downadup można przypisać „czynnikom środowiskowym": znaczna część sieci lub systemów nadal działa pod kontrolą starych, niepołatanych systemów operacyjnych Windows, co daje robakowi rezerwuar „habitatów", w których może gnieździć się i kontynuować infekcje; pewną rolę może odgrywać też niedostępność wykwalifikowanych, skrupulatnych specjalistów, którzy potrafiliby całkowicie usunąć to oprogramowanie z zainfekowanej sieci, bo jeśli ta procedura nie zostanie wykonana prawidłowo, może dojść do ponownej infekcji. Niestety, komputery i sieci działające pod kontrolą starszych wersji systemów operacyjnych i oprogramowania biznesowego wciąż nie należą do rzadkości, nawet w najbardziej rozwiniętych krajach. Ten stan rzeczy jest jeszcze powszechniejszy w takich regionach, jak **Azja**, w których ogólnie rzecz biorąc obserwujemy znacznie więcej starszych zagrożeń, niedziałających już przeciwko nowszym albo regularniej aktualizowanym systemom.

10 NAJCZĘSTSZYCH DETEKCJI

DRUGA POŁOWA 2013 R.



DRUGA POŁOWA 2013 R. W PORÓWNANIU Z PIERWSZĄ POŁOWĄ 2013 R., PROCENTOWO

%, PIERWSZA POŁOWA 2013 R.

%, DRUGA POŁOWA 2013 R.

KRAJE ODPOWIEDZIALNE ZA 10 NAJCZĘSTSZYCH DETEKCJI W DRUGIEJ POŁOWIE 2013 R., PROCENTOWO

%

	Francja	USA	Szwecja	Brazylia	Finlandia	Niemcy	Holandia	Włochy	Wielka Brytania	Polska	Dania	Malezja	Tunezja	Indie	Turcja	Wietnam	Belgia	Egipt	Pakistan	Rumunia	Japonia	Taiwan	Bułgaria	Kanada	Kolombia	Indonezja	Meksyk	Słowenia	Norwegia	Zjednoczone Emiraty Arabskie	Pozostałe
Ataki przeglądarkowe	12	7	18		9	9	6	4	3		4						3														25
Downadup/Conficker	6			18				7				6									3	2	4		3			4		16	32
Majava	12	20	9		10	9	7	3	5	3	3																				17
Ramnit				3								4	6	12	7	19		6	4	3						4					33
Sality				13						3		9	3	13	12	8		4	2	2											30
Autorun	12			7						4		10	3	8	5						4	3					4				41
CVE-2013-2471	9	10	13		15	11	7	3	4	5	5																				17
Zeroaccess	22	23	6		4	4	3	3	7		3												3								22
CVE-2013-1493	10	17	13		9	14	7		4		4						3														27
Mevade	32	3	6	5	5	4	6	4	3	5																		4			16

Inne długowieczne zagrożenia, które nadal pozostają aktywne, to **Ramnit** (robak z funkcją infekowania plików, który odkryto w 2010 r.) oraz **Sality** (polimorficzny wirus infekujący pliki zaobserwowany po raz pierwszy w 2003 r.). W przeciwieństwie do robaka Downadup, te dwa zagrożenia z czasem ewoluowały, ponieważ inni autorzy złośliwego oprogramowania modyfikowali je i wypuszczali ich warianty do własnych niegodziwych celów, więc ich ciągła obecność w naszych statystykach jest spowodowana głównie aktywnymi działaniami napastników. W drugiej połowie 2013 r. zarówno Ramnit, jak i Sality, które wcześniej odpowiadały za 1 proc. dziesięciu najczęściej raportowanych detekcji, zwiększyły swoje udziały do odpowiednio 9 i 8 proc. Zagrożenia te były najbardziej aktywne w Wietnamie, Indiach, Turcji i Brazylii.

Odwrotny trend obserwujemy w przypadku botnetu **ZeroAccess**, który w pierwszej połowie 2013 r. odpowiadał za 4 proc. dziesięciu najczęściej raportowanych detekcji, a w drugiej już tylko za 3 proc. Oznacza to ogromny spadek w porównaniu z drugą połową 2012 r., kiedy to ZeroAccess reprezentował aż 27 proc. detekcji zgłoszonych do naszych systemów. Upadek tego botnetu można przypisać działaniom, podjętym przez dział przestępstw cyfrowych Microsoftu we współpracy z FBI i partnerami branżowymi, które zablokowały cały ruch sieciowy między systemami komputerowymi w Stanach Zjednoczonych a 18 znanymi serwerami dowodzenia (C&C) ZeroAccess — choć dalsze badania wskazują, że akcja ta odniosła mniejszy skutek, niż początkowo sądzono[2]. Tak czy inaczej, dalsze obserwacje aktywności botnetu[3] sugerują, że nie jest on już aktywnie rozwijany przez operatorów i dlatego skurczył się do obecnych rozmiarów. Nieliczne wykrycia ZeroAccess mają miejsce głównie we Francji, Stanach Zjednoczonych i Wielkiej Brytanii.

Innym debiutantem na liście dziesięciu najczęstszych detekcji jest **Mevade**. Choć samo zagrożenie nie jest nowe (odkryto je pod koniec 2012 r.), to po raz pierwszy trafiło na naszą listę. Reprezentowało 3 proc. zgłoszonych detekcji i było najbardziej aktywne we Francji, Szwecji i Holandii. Botnet Mevade jest znany z tego, że jako pierwszy intensywnie wykorzystuje anonimizującą sieć Tor, aby ukrywać swój ruch. Oznacza to, że taktyki takie jak sinkholing, czyli przekierowywanie ruchu pod adres IP kontrolowany przez administratora systemu lub badacza bezpieczeństwa w celu śledzenia i zwalczania botnetów, są nieskuteczne. Ponadto utrudnia to, a wręcz uniemożliwia wyłączenie botnetu.

Najczęstszym **wektorem infekcji**, przez który złośliwe oprogramowanie trafia do użytkowników, pozostaje internet. Obejmuje to takie kanały, jak wymuszone pobieranie złośliwego oprogramowania do komputera użytkownika przez pakiet exploitów, złośliwe reklamy (malvertising), a także skażone pakiety oprogramowania pochodzące z serwisów udostępniania plików oraz, oczywiście, ze złośliwych witryn. Ponadto, jeśli chodzi o **prywatność w sieci**, szeroko rozpowszechnione użycie plików cookie, skryptów i innych technik śledzenia użytkowników oznacza, że nawet zablokowanie złośliwego programu może nie wystarczyć, aby zapobiec utracie danych osobistych.

Co do platform mobilnych, nieustająca dominacja systemu operacyjnego **Android** sprawia, że jest on niemal wyłącznym celem zagrożeń mobilnych, które zaobserwowaliśmy w omawianym okresie. Choć względnie niska liczba luk w zabezpieczeniach Androida sprawia, że sam system operacyjny jest trudnym celem ataku, autorzy złośliwego oprogramowania obchodzą te środki bezpieczeństwa dzięki względnej łatwości dostarczania swoich „produktów" oraz skłaniania użytkowników, aby zainstalowali je w swoich urządzeniach z przywilejami, które pozwalają używać urządzenia (i danych użytkownika) z korzyścią dla napastnika. Wśród dziesięciu najczęstszych detekcji złośliwego oprogramowania do Androida, które zostały zgłoszone do naszych systemów w drugiej połowie 2013 r., ponad 75 proc. pochodziło z Arabii Saudyjskiej i Indii. W okresie tym najczęściej raportowanymi rodzinami złośliwego oprogramowania do Androida były GinMaster, Fakeinst i SmsSend, które albo gromadzą dane z urządzenia, albo wysyłają wiadomości SMS klasy premium.

Wreszcie jeśli chodzi o zagrożenia dla platformy Mac, obserwowaliśmy niewielki, ale stały wzrost. W drugiej połowie 2013 r. pojawiło się 18 nowych zagrożeń, co jednak jest bardzo małą liczbą w porównaniu z systemem Windows, a nawet Androidem. 83 proc. spośród tych debiutantów to „tylne drzwi", a resztę

ŹRÓDŁA

1. Krebs on Security; Brian Krebs; *Meet Paunch: The Accused Author of the BlackHole Exploit Kit*; published 6 December 2013; http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/
2. Arstechnica; Sean Gallagher; *Microsoft disrupts botnet that generated $2.7M per month for operators;* published 7 December 2013; http://arstechnica.com/security/2013/12/microsoft-disrupts-botnet-that-generated-2-7m-per-month-for-operators/
3. Naked Security by Sophos; James Wyke; *Have we seen the end of the ZeroAccess botnet?* published 7 January, 2014; http://nakedsecurity.sophos.com/2014/01/07/have-we-seen-the-end-of-the-zeroaccess-botnet/

GODNE UWAGI

TROJANY RZĄDOWE

BĘDZIEMY JE WYKRYWAĆ

Pod koniec października 2013 r. F-Secure i wiele innych firm produkujących oprogramowanie antywirusowe otrzymało list od duńskiej organizacji na rzecz praw cyfrowych, Bits of Freedom, która wspólnie z koalicją podobnych stowarzyszeń oraz zainteresowanych przedstawicieli świata akademickiego wystąpiła o formalne przedstawienie polityki firmy w zakresie wykrywania programów tworzonych i dystrybuowanych przez rządy, organy ścigania oraz inne jednostki państwowe. Poniżej znajduje się fragment wniosku o informacje oraz pełny tekst odpowiedzi przesłanej przez dyrektora generalnego F-Secure, Christiana Fredriksona 1 listopada 2013 r.

"Kilka rządów planuje przyznać lub przyznało organom ścigania prawo do zdalnego włamywania się do komputerów, zarówno w kraju, jak i za granicą, w celu inwigilowania użytkowników w ramach prowadzonych dochodzeń. Aby złamać zabezpieczenia osobistych komputerów użytkowników, organy ścigania muszą wykorzystać luki w zabezpieczeniach i zainstalować złośliwe oprogramowanie, które będzie gromadzić dane z docelowych komputerów.

Jako producent oprogramowania antywirusowego odgrywacie ważną rolę w zapewnianiu bezpieczeństwa użytkownikom internetu, którzy podejmują działania wymagające poufności, takie jak korzystanie z bankowości elektronicznej. Nie może być zatem żadnych wątpliwości, że wasze oprogramowanie gwarantuje stopień bezpieczeństwa niezbędny do utrzymania ich zaufania.

Konsumenci i firmy, których systemy chronicie, powinni mieć pewność, że złośliwe programy i wirusy będą wykrywane i usuwane, bez względu na ich źródło. Dlatego chcielibyśmy prosić was o przedstawienie waszej polityki w tym zakresie. Mówiąc ściślej, docenilibyśmy odpowiedzi na następujące pytania:

1. Czy kiedykolwiek wykryliście oprogramowanie używane przez dowolny rząd (lub jednostkę państwową) do celów inwigilacji?

2. Czy kiedyś zostaliście poproszeni przez przedstawicieli rządu, aby obecność konkretnego oprogramowania nie była wykrywana, a jeśli już, to żeby użytkownicy waszego oprogramowania nie byli o tym powiadamiani? Jeśli tak, czy moglibyście podać informacje o podstawie prawnej takiego wniosku, rodzaju oprogramowania, które mielibyście pomijać, oraz okresie czasu, przez który mielibyście zezwalać na jego używanie?

3. Czy kiedykolwiek spełniliście taką prośbę? Jeśli tak, czy moglibyście podać te same informacje, co w punkcie powyżej, oraz wyjaśnić, co skłoniło was do zaakceptowania rządowego wniosku?

4. Czy moglibyście zadeklarować, jak zareagowalibyście na taki wniosek w przyszłości?"

ODPOWIEDŹ F-SECURE

W firmie F-Secure Corporation bardzo cieszymy się, że Bits of Freedom (i inne organizacje stojące za tym wnioskiem o informacje) zwiększają świadomość tego bardzo ważnego zagadnienia. Co więcej, odpowiadamy na te pytania z dumą, ponieważ mamy bardzo zdecydowane poglądy na te kwestie.

Oto nasze odpowiedzi:

1. **Tak, wykrywaliśmy złośliwe oprogramowanie rządowe używane przez organy ścigania (takie jak trojan R2D2 używany przez niemiecki rząd).**
2. **Nie**
3. **Nie**
4. **Gdybyśmy zostali poproszeni przez przedstawicieli rządu o niewykrywanie konkretnego złośliwego oprogramowania, odpowiedzielibyśmy odmownie. Źródło złośliwego oprogramowania nie ma wpływu na naszą decyzję o jego wykrywaniu. Jeśli oprogramowanie jest złośliwe, będziemy chronić przed nim naszych klientów. Nasz proces decyzyjny sprowadza się do prostego pytania: czy nasi klienci chcieliby, żeby dany program działał w ich systemie? W przypadku trojanów rządowych odpowiedź oczywiście brzmi „nie".**

Chcielibyśmy również podkreślić, że nasza polityka w tym zakresie nie zmieniła się, od kiedy ogłosiliśmy ją w 2001 r. Można ją przeczytać pod adresem http://www.f-secure.com/en/web/labs_global/policies.

ŹRÓDŁO:

1. 1. F-Secure Weblog; Mikko Hypponen; F-Secure Corporation's Answer to Bits of Freedom; opublikowano 6 listopada 2013 r.; http://www.f-secure.com/weblog/archives/00002636.html

KONIEC JEST BLISKI?

8 kwietnia tego roku system operacyjny Microsoft Windows XP osiągnie koniec swojego przedłużonego okresu wsparcia. Co potem? Brak publicznych aktualizacji systemu. Brak publicznych aktualizacji zabezpieczeń. Użytkownicy będą pozostawieni samym sobie. Ale XP to nadal bardzo popularny — a przynajmniej rozpowszechniony — system operacyjny (szczegóły można znaleźć w innych sekcjach niniejszego raportu).
W raporcie tym omawiamy dwie statystyki detekcji, które odzwierciedlają dwa bardzo poważne zagrożenia dla użytkowników Windows: ataki przeglądarkowe i ataki wymierzone w Javę. A system XP jest szczególnie kłopotliwy, bo kiedy zostanie przejęty przez napastnika, dużo trudniej go naprawić, niż nowsze wersje Windows. W przypadku XP rzeczywiście lepiej zapobiegać, niż leczyć.

Prognoza: media głównego nurtu nagłośnią „ostateczny termin" 8 kwietnia jako potencjalną apokalipsę typu „Y2K" (problemu roku 2000). A kiedy 9 kwietnia nic się nie stanie? Dziennikarze znowu będą pytać, o co było tyle hałasu. Tymczasem w prasie technicznej... reporterzy będą cierpliwie czekać na pierwszą krytyczną lukę ery post-XP. Kiedy (nie jeśli) jakiś exploit dnia zerowego na rynek, wtedy pojawią się obawy i poważne pytania. Czy systemowi XP można zaufać?

Ale nie wszystko jest stracone. Łatanie XP nie jest pierwszą linią obrony, a przynajmniej nie powinno.

Niektóre firmy będą używać Windows XP przez cały 2014 r., albo ze względu na zobowiązania kontraktowe, albo dlatego, że robią to ich klienci, więc XP będzie potrzebny, aby ich wspierać. W takich sytuacjach menedżerowie IT będą mieli naprawdę pełne ręce roboty. Zaleca się odizolować systemy XP albo przenieść je do innych sieci niż te, w których znajduje się krytyczna własność intelektualna. Firmy już teraz powinny podejmować podobne kroki w stosunku do użytkowników, którzy wykorzystują urządzenia osobiste do celów służbowych („Bring Your Own Device", BYOD). XP to po prostu kolejny zasób, którym trzeba zarządzać.

Ci, którzy będą nadal używać XP w domu, pozostaną w miarę bezpieczni jeszcze przez jakiś czas, ale będą musieli koniecznie przeanalizować swoje nawyki, jeśli chodzi o korzystanie z komputera i internetu (zwłaszcza o przeglądanie stron internetowych):

1. Należy zainstalować ostatnią aktualizację Windows XP.
2. Należy zainstalować alternatywną przeglądarkę lub przeglądarki (są bezpłatne!) — nie polegać wyłącznie na Internet Explorerze. Nie należy też używać Internet Explorera jako przeglądarki domyślnej.
3. Jeśli w komputerze zainstalowano pakiet Microsoft Office, należy upewnić się, że jest w pełni zaktualizowany. Starsze wersje Office domyślnie uruchamiają na przykład kod Flasha osadzony w dokumentach. W przypadku używania starszej wersji Office należy ustawić bardziej restrykcyjne opcje zabezpieczeń. Nie należy otwierać dokumentów z niezaufanych źródeł.
4. Należy przejrzeć oprogramowanie firm trzecich i odinstalować wszystko, co nie jest potrzebne. Ci, którzy zamierzają zostać przy XP, powinni zrobić „wiosenne porządki" i pozbyć się starego oprogramowania, ponieważ „stare" często znaczy „narażone na atak".
5. Jeśli chodzi o oprogramowanie firm trzecich, należy rozważyć wyłączenie lub odinstalowanie dodatków do przeglądarki. Warto ustawić przeglądarkę tak, aby „zawsze pytała", co robić z takimi dokumentami, jak pliki PDF
    a. Czy na domowym laptopie potrzebna jest Java? Prawdopodobnie nie.
    b. W zaawansowanych ustawieniach przeglądarki znajdują się opcje „kliknij, aby uruchomić". Są one warte dodatkowego wysiłku.
6. Należy zaopatrzyć się w aktualny produkt zabezpieczający z antywirusem i zaporą sieciową.
7. Komputer XP należy podłączyć do domowego routera NAT, który będzie pełnił funkcję sprzętowej zapory (w praktyce oznacza to, że nie należy podłączać laptopa do darmowych hotspotów Wi-Fi, lecz trzymać go w domu w zaufanej sieci).
8. 8. Wreszcie... warto zastanowić się nad zmianą systemu operacyjnego. Jeśli ktoś nie lubi Windows 8, zawsze pozostaje Windows 7. Instalację OEM można nadal nabyć w wielu sklepach internetowych.

SHARKING

GRACZE NA CELOWNIKU

W F-Secure Labs otrzymujemy mnóstwo próbek. Większość trafia do nas przez internet, ale od czasu do czasu ktoś osobiście odwiedza jedno z naszych laboratoriów i przynosi swój komputer do analizy śledczej.

W zeszłym roku na początku września pod naszą centralą w Helsinkach zaparkowało Audi R8, z którego wysiadł dwudziestokilkulatek. Był to Jens Kyllönen — zawodowy pokerzysta, który gra zarówno na tradycyjnych turniejach, jak i w internecie. Jens jest graczem dużego kalibru, który w zeszłym roku wygrał kwoty sięgające 2,5 mln euro. Dlaczego gwiazda pokera wpadła do nas z wizytą? Oto jego historia.

W zeszłym roku Jens uczestniczył w turnieju pokerowym, który odbywał się w 5-gwiazdkowym hotelu w Barcelonie. Spędził dzień na turnieju, a kiedy podczas przerwy poszedł do pokoju, nie znalazł w nim swojego laptopa. Kiedy po zaalarmowaniu obsługi hotelowej wrócił do pokoju, laptop był na miejscu, ale nie uruchamiał się prawidłowo. Jens obawiał się, że coś może być nie tak.

Podejrzewając, że ktoś mógł włamać się do jego komputera, Jens poprosił nas o jego przeanalizowanie, więc wykonaliśmy pełne obrazy śledcze i przystąpiliśmy do pracy. Niebawem okazało się, że przeczucie go nie myliło — laptop rzeczywiście był zainfekowanym trojanem zdalnego dostępu (Remote Access Trojan, RAT), a znaczniki czasowe plików zgadzały się z godzinami, w których laptop zaginął. Napastnik najwyraźniej zainstalował trojana z pamięci USB i skonfigurował go tak, aby uruchamiał się automatycznie po każdym restarcie systemu. RAT pozwala napastnikowi zdalnie oglądać wszystko, co jest wyświetlane na ekranie laptopa — w tym karty ofiary podczas internetowych meczów pokerowych (zob. ilustracja po prawej stronie). To złośliwe oprogramowanie używa obfuskacji, ale nie jest szczególnie skomplikowane. Ponieważ napisano je w Javie, może działać na dowolnej platformie (MacOS, Windows, Linux). Jest to bardzo ogólny sposób ataku, który działa w przypadku wszystkich internetowych witryn pokerowych, jakie znamy.

Po przeanalizowaniu laptopa Jensa zaczęliśmy szukać innych ofiar. Okazało się, że inny profesjonalny gracz, Henri Jaakkola, który podczas turnieju dzielił pokój z Jensem, również miał w laptopie tego samego trojana.

Nie po raz pierwszy zaatakowano profesjonalnych pokerzystów za pomocą trojanów; poprzednio badaliśmy kilka przypadków, w których wykorzystano złośliwe oprogramowanie do kradzieży setek tysięcy euro. Godne uwagi jest jednak to, że do ataku nie doszło w sieci — napastnik zadał sobie trud, aby dostać się do systemów ofiar w rzeczywistym świecie. Ukierunkowane ataki na profesjonalnych pokerzystów (popularnie zwanych „rekinami karcianymi") są już na tyle powszechne, że otrzymały własną nazwę: sharking.

JAK TO DZIAŁA

The normal view of the online poker game, as seen by the attacker (cards at the front of the screen).

RAT pokazuje karty użytkownika zainfekowanej maszyny (w tym przypadku dwie damy). Zapewnia to napastnikowi strategiczną przewagę w grze.

Przypomina to whaling, czyli ukierunkowane ataki na wyższe kadry kierownicze.

Jaki więc płynie morał z tej historii? Jeśli masz laptopa, którego używasz do obracania dużymi kwotami pieniędzy, dbaj o jego bezpieczeństwo. Radę tę powinni wziąć do serca nie tylko zawodowi pokerzyści, którzy grywają w internecie, ale również dyrektorzy dużych firm, którzy przelewają duże sumy między różnymi krajami świata.

UWAGA: NINIEJSZY ARTYKUŁ ZACZERPNIĘTO Z WPISU NA BLOGU F-SECURE, KTÓRY NOSIŁ TEN SAM TYTUŁ I ZOSTAŁ OPUBLIKOWANY 10 GRUDNIA 2013 R.

STUDIA PRZYPADKÓW

AZJA POD LUPĄ

Azja rozwija się w szybkim tempie, czemu towarzyszy proporcjonalny wzrost detekcji złośliwego oprogramowania, które są zgłaszane do naszych chmurowych systemów telemetrycznych z tego regionu. W niniejszym raporcie omawiamy niektóre trendy wyłaniające się ze statystyk, które zebraliśmy w drugiej połowie 2013 r. z Japonii, Malezji, Tajwanu, Hongkongu, Filipin i Indii.

DOWNADUP CIĄGLE GROŹNY

Godny uwagi jest robak, który identyfikujemy jako Downadup (zwany też w mediach Confickerem). Nadal plasuje on się wysoko wśród detekcji zgłaszanych z regionu azjatyckiego, zwłaszcza w Malezji, gdzie zajmuje pierwsze miejsce na liście. Duża liczba infekcji Confickerem jest również raportowana na Filipinach i Tajwanie. Ciągła obecność tego złośliwego oprogramowania w naszych statystykach dotyczących Azji jest dość zaskakująca, ponieważ ma już ono ponad pięć lat. Microsoft ostrzegł użytkowników o luce wykorzystywanej przez Confickera w październiku 2008 r. i wkrótce potem opublikował nadprogramową poprawkę zabezpieczeń, aby wyeliminować ten wektor ataku. To, że robak nadal operuje w regionie, sugeruje, że przynajmniej w Azji nadal jest wiele systemów Windows XP, które działają bez tych poprawek.

INFEKCJE MAILCABEM

Na Tajwanie numerem jeden wśród wykrywanych infekcji jest wiekowy makrowirus, który identyfikujemy jako X97M.Mailcab. Po raz pierwszy zaobserwowany pod koniec 2012 r., Mailcab rozprzestrzenia się w zainfekowanych skoroszytach programu Microsoft Excel, które są dystrybuowane w postaci załączników do wiadomości e-mail. Po otwarciu złośliwy plik obniża poziom zabezpieczeń pakietu Office, a następnie wysyła swoje kopie do kontaktów z programu pocztowego Outlook (cecha charakterystyczna dla robaków).

Utrzymująca się obecność Mailcaba jest dość zaskakująca, ponieważ makrowirusy i robaki (takie jak Conficker), niegdyś bardziej rozpowszechnione, w ostatnich latach stały się znacznie mniej groźne, bo twórcy oprogramowania wprowadzili środki bezpieczeństwa, które uniemożliwiają im infekowanie plików i rozprzestrzenianie się w tak gwałtowny sposób, jak kiedyś. Pojawienie się Mailcaba w naszych statystykach świadczy o tym, że w Azji wciąż pozostają w użyciu starsze wersje programów biznesowych.

ZAGROŻENIA MOBILNE

Tymczasem w Indiach, od kiedy dostępne są tańsze smartfony z Androidem i szerokopasmowa łączność bezprzewodowa, poczesne miejsce w statystykach zajmują detekcje złośliwego oprogramowania mobilnego. Choć znaczna większość detekcji dotyczy potencjalnie niepożądanych aplikacji (PUA), które są względnie nieszkodliwe, najczęściej raportowanym złośliwym programem w tym kraju jest Trojan:Android/GinMaster. Trojan ten jest rozpowszechniany w strojanizowanej aplikacji, a po instalacji wykorzystuje exploit, aby zainstalować w urządzeniu dodatkowe programy i wykradać informacje. Podobnie jak większość aplikacji do Androida, które identyfikujemy jako złośliwe oprogramowanie, jest on rozpowszechniany głównie poprzez niezależne sklepy z aplikacjami.

Ogólniej rzecz biorąc, z Indii nadal zgłaszana jest szeroka gama zagrożeń, które niegdyś były bardziej powszechne, ale obecnie w większości krajów zniknęły niemal całkowicie. Mówiąc ściślej, warianty rodzin Sality, Ramnit i Autorun (odpowiednio polimorficzny wirus infekujący pliki, robak z funkcjami infekowania plików oraz robak) zajmują poczesne miejsce w indyjskich statystykach. Zagrożenia te zostały wyeliminowane lata temu przez twórców odpowiednich programów, a ich dalsza obecność w Indiach świadczy o znacznej liczbie komputerów, w który działa starsze, niezaktualizowane oprogramowanie.

JAVA

Jeśli chodzi o Japonię, w drugiej połowie 2013 r. zaobserwowaliśmy spadek liczby exploitów wymierzonych w Javę, które były bardzo rozpowszechnione w pierwszym półroczu, zwłaszcza tych identyfikowanych jako rodzina Majava. Większość przedsiębiorstw używa Javy do uruchamiania samodzielnie napisanych aplikacji i do obsługi starszych systemów. Do niedawna hakerzy intensywnie atakowali niezaktualizowane środowiska Javy, czemu sprzyjał klimat, w którym firma Oracle co chwila ogłaszała nowo odkrytą lukę w zabezpieczeniach. Niedawny spadek liczby detekcji związanych z Javą każe nam jednak przypuszczać, że wiele środowisk wykorzystujących Javę albo jej wtyczki zostało już zaktualizowanych.

WINDOWS XP

Wreszcie jeśli chodzi o komputery stacjonarne Windows XP pozostaje preferowanym systemem do użytku osobistego i biznesowego, obecnie reprezentując około 30 proc. wszystkich użytkowników komputerów PC[1]. Większość z nich znajduje się w Azji, gdzie piractwo nadal szaleje. Warto też nadmienić, że według Bloomberg BusinessWeek[2] nawet 90 proc. bankomatów może nadal działać pod kontrolą Windows XP.

Microsoft niedawno zapowiedział, że 8 kwietnia 2014 r. zakończy świadczenie pomocy technicznej dla użytkowników Windows XP. Oznacza to, że nie będzie już nowych aktualizacji zabezpieczeń, poprawek niezwiązanych z bezpieczeństwem, opcji pomocy technicznej ani aktualizacji materiałów technicznych dostępnych w internecie. Użytkowników wzywa się do przejścia na najnowszą wersję Windows, 8.1, a przynajmniej na Windows 7. Oba te systemy obecnie mają mniej znanych luk w zabezpieczeniach i lepszy model bezpieczeństwa niż XP.

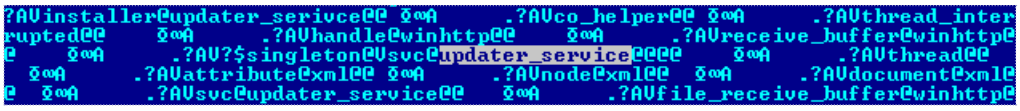
ŹRÓDŁA

1. Net Applications; Desktop Operating System Market Share (January, 2014); http://www.netmarketshare.com/operating-system-market-share.aspx
2. Bloomberg BusinessWeek; Nick Summers; ATMs Face Deadline to Upgrade From Windows XP; opublikowano 16 stycznia 2014 r.; http://www.businessweek.com/articles/2014-01-16/atms-face-deadline-to-upgrade-from-windows-xp

WIĘCEJ INFORMACJI O MEVADE

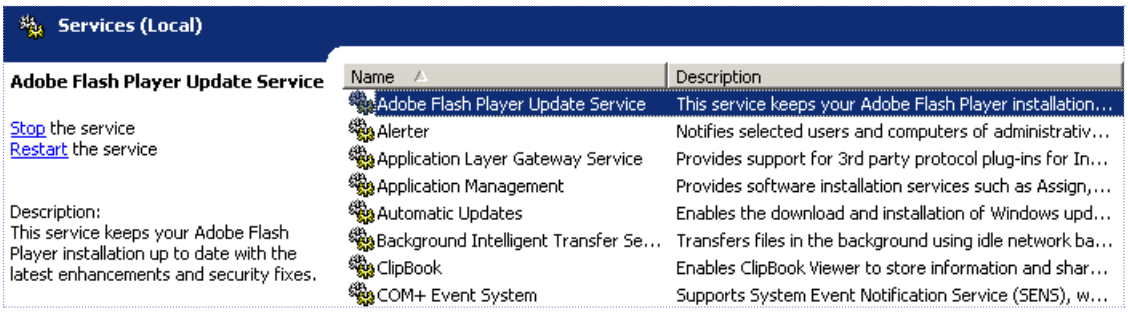
Mevade, jedna z najbardziej rozpowszechnionych rodzin złośliwego oprogramowania w drugiej połowie 2013 r., reprezentowała około 3 proc. naszych detekcji w tym okresie. Nie jest to jednak debiutant na scenie złośliwego oprogramowania. Wariant formalnie ochrzczony nazwą rodziny został po raz pierwszy zaobserwowany przez nasze systemy już w grudniu 2012 r., a badacze z firmy Fox-IT powiązali z jeszcze starszymi odmianami sięgającymi 2009 r. na podstawie pokrewnych nazw detekcji. Przypisali mu też odpowiedzialność za nagły wzrost liczby użytkowników sieci Tor pod koniec sierpnia 2013 r.[1]

Od tego czasu z rodziny Mevade wyłoniło się kilka wariantów, każdy z innymi funkcjami. Nasze statystyki detekcji pokazują, że najbardziej rozpowszechnionym wariantem był program do pobierania plików, który stanowił około 97 proc. wszystkich



Rysunek 1. Nazwa modułu w komponencie do pobierania plików

detekcji Mevade. Łańcuchy tekstu w próbce tego wariantu (rysunek 1) sugerują, że jest to tylko aktualizator, który pełni również rolę instalatora, a nie samodzielny wariant trojana. Zgadza się to z naszymi statystykami, ponieważ po zablokowaniu instalatora inne komponenty nie powinny mieć możliwości zainfekowania systemu. Łańcuchy tekstu pasują też do przykrywki trojana, który podszywa się pod usługę aktualizacji programu Adobe Flash Player (**rysunek 2**).



Rysunek 2. Mevade podszywający się pod usługę aktualizacji Flash Playera

Komponent aktualizacyjny regularnie kontaktuje się z serwerem dowodzenia (C&C) w oczekiwaniu na instrukcje instalacji. Komunikat ma następujący format:

- http://{SERVER}/updater/{UUID}/{VERSION}

{UUID} to unikatowy identyfikator zainfekowanego komputera, który stanowi połączenie GUID (HKLM\Software\Microsoft\Cryptography) oraz numeru seryjnego woluminu, a {SERWER} jest wybierany z listy nazw domenowych zakodowanych na stałe w programie (**tabela 1**).

Tabela 1. Nazwy domenowe zakodowane w komponencie do pobierania plików

svcupd[dot]net	updsvc[dot]com
srvupd[dot]com	updsvc[dot]net
srvupd[dot]net	updsrv[dot]net

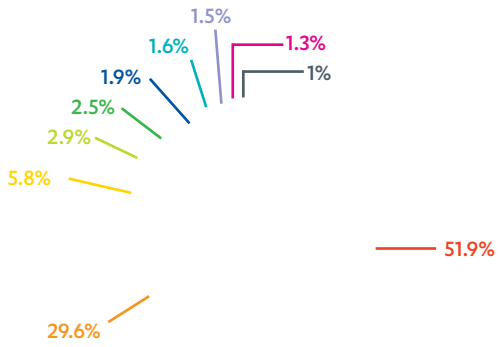
Jeśli jest to tylko komponent aktualizacyjny, to co z właściwym złośliwym kodem? Kiedy przeprowadzaliśmy tę analizę, żadna z domen nie przekładała się na adres hosta. W produktach F-Secure jest jednak funkcja, która pokazuje historię pliku w systemie. Na jej podstawie stwierdzilismy, że komponent instalował inne próbki Mevade, konkretnie te warianty, które używają sieci Tor.

Potwierdzają to nasze statystyki detekcji. Jeśli pominiemy komponent aktualizacyjny Mevade, na pierwszych trzech miejscach znajdują się warianty używające sieci Tor. Łącznie reprezentowały one ponad 80 proc. pozostałych wariantów (rysunek 3). Dwie najczęściej wykrywane próbki zostały skompilowane 1 września 2013 r., a trzecia 23 sierpnia 2013 r.

Jak już wspomniano, warianty te instalują w systemie klienta sieci Tor. Dla niewtajemniczonych: Tor to wirtualna podsieć internetu, której członkowie są anonimowi dla siebie nawzajem. Zwykle jest używana jako sieć tranzytowa przez tych, którzy chcą zachować anonimowość, kiedy odwiedzają inne serwery w internecie.

Jej innym, mniej popularnym zastosowaniem jest hosting ukrytych serwerów w samej wirtualnej sieci. „Ukryty" znaczy tutaj, że serwery są nieosiągalne z internetu bez użycia klienta Tor. Oznacza to zarazem, że serwery są fizycznie nie do wyśledzenia, a więc stanowią idealne miejsce dla przestępców zarządzających nielegalnymi usługami, którzy mogą ukryć je przed organami ścigania bez odłączania się od sieci. Właśnie tutaj działają serwery dowodzenia Mevade, stąd potrzeba zainstalowania klienta Tor.

PRZYKŁADOWA DYSTRYBUCJA MEVADE



SKRÓTY PRÓBEK INNYCH NIŻ KOMPONENT DO POBIERANIA PLIKÓW

60e3e4227497ad83885e859903cb98d769ed9b9c
12df7f18c8b07e2fa955e58427c5a52ac3b785e6
edc7a434f18424d73c1403a15ee417fbd59eea95
86adb7af4d1a582dfdd021c9521d0c2d50d5354f
014ace48897e81052b9552a5a7ab04d00a8e5227
85bd27ba64a150536fc42445df9efae775c52c8c
669c1e6857c541160906e8fb89a5f708b7fa2c50
c79cef4ae59b5a304bfa0b05b8bf2d1a8f0b81b8
127cb991ca9908e71e231ab0be9318c1cde818bd
9c9c3a26f7876b9a7e633ea5c72ee57c52e82f5a

Rysunek 3: Dystrybucja próbek Mevade innych niż komponent do pobierania plików

MEVADE'S SETUP

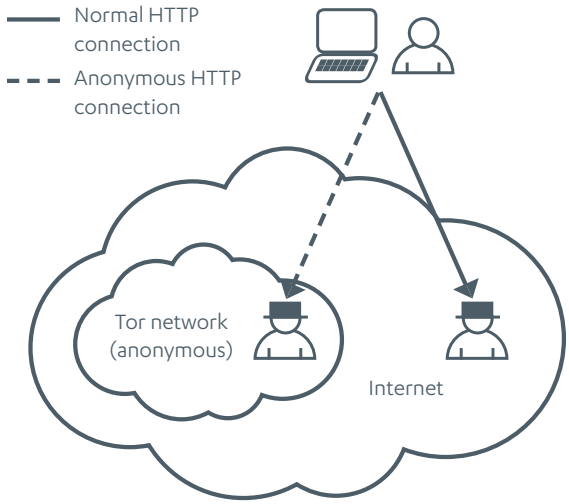


Figure 4: Struktura dowodzenia Mevade

Badacze bezpieczeństwa we współpracy z rejestratorami nazw domenowych często zmieniają rekordy nazw związanych z botnetami i przekierowują je do serwerów, które są kontrolowane przez badaczy. Ten proces, określany mianem sinkholingu, wykorzystuje się do studiowania, mierzenia i zakłócania botnetów. Jednak serwery w sieci Tor używają nazw domenowych, które w rzeczywistości są pseudonazwami wywodzącymi się z tajnych kluczy, znanych tylko operatorom serwera. Nie mają one żadnego związku z nazwami domenowymi w internecie. Bez tajnych kluczy posługiwanie się tymi pseudonazwami jest niemożliwe. Z tej przyczyny, a także ze względu na anonimową naturę sieci Tor, botnet jest teoretycznie odporny na sinkholing i próby zablokowania.

Oprócz wariantów, które używają serwerów w sieci Tor, znaleźliśmy również kilka odmian (skompilowanych po 14 września 2013 r.), które kontaktują się ze zwykłymi serwerami HTTP[2,3]. Na rysunku 4 podsumowano strukturę dowodzenia Mevade, a w **tabeli 2** i **tabeli 3** wymienione są nazwy domenowe zaszyte w kodzie złośliwego oprogramowania.

Tabela 2. Pseudonazwy domenowe serwerów dowodzenia Mevade w sieci Tor

pomyeasfnmtn544p[dot]onion	wsytsa2omakx655w[dot]onion
ijqqxydixp4qbzce[dot]onion	lqqth7gagyod22sc[dot]onion
7fyipi6vxyhpeouy[dot]onion	lorpzyxqxscsmscx[dot]onion
onhiimfoqy4acjv4[dot]onion	mdyxc4g64gi6fk7b[dot]onion
6tlpoektcb3gudt3[dot]onion	ye63peqbnm6vctar[dot]onion
qxc7mc24mj7m4e2o[dot]onion	7sc6xyn3rrxtknu6[dot]onion
lqqciuwa5yzxewc3[dot]onion	l77ukkijtdca2tsy[dot]onion

Tabela 3. Zwykłe nazwy domenowe alternatywnych serwerów dowodzenia Mevade

angelikajongedijk[dot]no-ip[dot]biz
stuartneilseidman[dot]dyndns[dot]pro

Jedną z funkcji Mevade, która odróżnia tego trojana od większości innych złośliwych programów, jest możliwość udostępniania plików w sieci Kad. Nie po raz pierwszy złośliwe oprogramowanie używa tej sieci. Wiadomo, że osławione oprogramowanie TDL wysyła i pobiera polecenia przez sieć Kad[4], aby utrudnić zablokowanie botnetu. Jednakże Mevade dotychczas nie wykazał się podobnymi zdolnościami. Wydaje się, że obecnie trojan komunikuje się ze swoimi serwerami dowodzenia tylko przez HTTP. Dotyczy to zarówno serwerów zlokalizowanych w sieci Tor, jak i poza nią. Podsumowanie komunikacji Mevade z serwerami znajduje się w **tabeli 4**.

Tabela 4. Podsumowanie komunikacji z serwerami dowodzenia

LOKALIZACJA	OPIS
http://{SERVER}/data	Stąd złośliwe oprogramowanie pobiera listę peerów w sieci Kad
http://{SERVER}/cache	Tutaj złośliwe oprogramowanie zgłasza dane statystyczne
http://{SERVER}/policy	Stąd złośliwe oprogramowanie otrzymuje polecenia

Dni, w których złośliwe oprogramowanie było pisane przez hobbystów, dawno minęły. Dziś powstaje ono w bardzo konkretnych celach. Jednak trudno ocenić przeznaczenie Mevade przez samo przyglądanie się próbkom. Żaden z serwerów dowodzenia w sieci Tor nie był dostępny online w czasie tej analizy; żaden ze zwykłych serwerów HTTP nie zwracał prawidłowej odpowiedzi. Z poleceń obsługiwanych przez trojana (**tabela 5**) wynika, że operatorzy botnetu mogą zrobić praktycznie wszystko w zainfekowanym systemie.

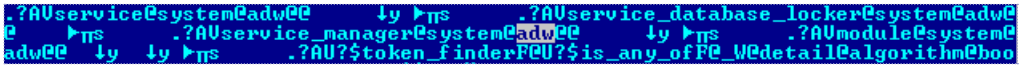
Table 5:Obsługiwane polecenia

update	execute
mirrors	share
update-config	

Możemy tylko spekulować na podstawie łańcuchów tekstu znalezionych w próbkach. Autorzy programu nadali jednemu z modułów (**rysunek 5**) nazwę „adw". Brzmi to jak „adware", co może sugerować, że stworzono go z myślą o zarabianiu na instalacji oprogramowania reklamowego firm trzecich. A może taki był pierwotny cel, ale z czasem zaczęto czerpać zyski w modelu opłaty za instalację.

Serwery dowodzenia są nietypowo ciche jak na botnet tej wielkości. Wydaje się, że w czasie analizy operatorzy czekali na właściwych nabywców. Oczywiście nie można wykluczyć, że serwery zostały już poddane sinkholingowi albo zablokowane, ale, jak wspomniano wcześniej, jest to mało prawdopodobne, ponieważ byłoby to bardzo trudne, a wręcz niemożliwe, przynajmniej w przypadku serwerów w sieci Tor.

Bardziej prawdopodobne jest to, że operatorzy botnetu wykorzystują lub wynajmują moc obliczeniową zainfekowanych systemów do wydobywania bitmonet. Badacze odkryli, że niektóre domeny historycznie związane z tymi, których używa Mevade, obecnie wykorzystuje się do działań związanych z generowaniem wirtualnej waluty[5]. Wydobywanie bitmonet stały się jedną z preferowanych technik monetyzacji złośliwego oprogramowania, od kiedy kurs waluty Bitcoin wystrzelił w górę w 2013 r.[6] Jest to również bardziej dyskretny sposób na czerpanie zysków z botnetu, który zmniejsza prawdopodobieństwo, że użytkownicy zauważą i usuną złośliwe oprogramowanie.



Rysunek 5. Nazwa modułu w głównym komponencie

ŹRÓDŁA

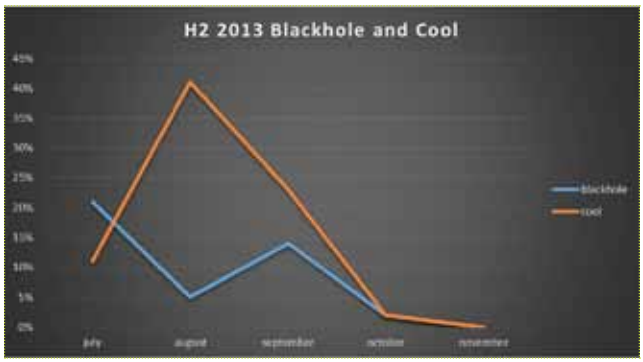
1. Fox-IT; ydklijnsma; Large botnet cause of recent Tor network overload; opublikowano 5 września 2013 r.; http://blog.fox-it.com/2013/09/05/large-botnet-cause-of-recent-tor-network-overload/
2. Próbka; skrót sha1: e17eeb872c12ce441ff29fc3ab21d74b008c70f5
3. Próbka; skrót sha1: 8a5f79e405844ebbb41b417d8a2e0c9759d6a6dd
4. About.com, Mary Landesman; TDSS aka TDL: A Botnet Framework; http://antivirus.about.com/od/virusdescriptions/p/Tdss-Aka-Tdl-A-Botnet-Framework.htm
5. AnubisNetworks Blog, João Gouveia i Martijn Grooten; UnknownDGA17:The Mevade connection; opublikowano 7 listopada 2013 r.; http://www.anubisnetworks.com/unknowndga17-the-mevade-connection/
6. Bloomberg, Olga Kharif; Bitcoin Tops $1,000 as Virtual Money Gains Popularity; opublikowano 28 listopada 2013 r.; http://www.bloomberg.com/news/2013-11-27/bitcoin-surges-to-1-000-as-virtual-money-gains-wider-acceptance.html

PAKIETY EXPLOITÓW

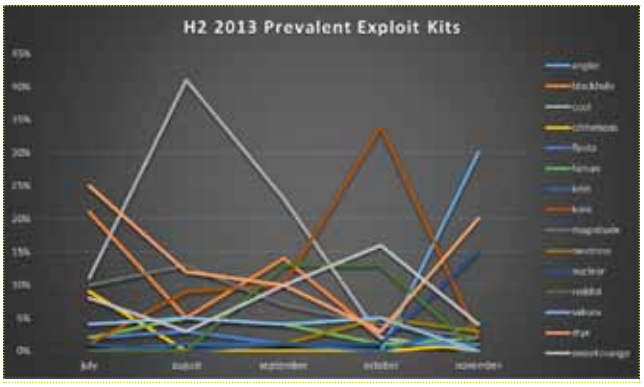
NOWY PRETENDENT

W drugiej połowie 2013 r. mieliśmy do czynienia z największym dotychczas wydarzeniem w świecie pakietów exploitów — zatrzymano niejakiego Pauncha, którego podejrzewa się o stworzenie i dystrybucję pakietu Blackhole[1]. Skutki tego zdarzenia były widoczne w naszych danych telemetrycznych. Paunch został zatrzymany w październiku, a w tym samym miesiącu zaobserwowaliśmy spadek infekcji wykorzystujących pakiety Cool i Blackhole (zob. rysunek 1). Jednocześnie na fali wznoszącej znalazły się trzy inne pakiety — Angler, Styx i Nuclear (zob. rysunek 2). Być może ich twórcy starają się wykorzystać aresztowanie Pauncha.

Gang Reveton, który używał pakietu exploitów Cool, szybko zareagował i przerzucił się na nowy pakiet. Według badacza bezpieczeństwa znanego jako Kafeine, Reveton sięgnął po pakiet Whithole już kilka godzin po tym, jak poinformowano o zatrzymaniu Pauncha. Dzień później Kafeine zauważył, że gang Reveton zaczął używać Anglera. Wygląda na to, że znaleziono zamiennik pakietu Cool.



Rysunek 1: Spadek liczby infekcji przy użyciu pakietów Blackhole i Cool



Rysunek 2: Rosnąca liczba infekcji przy użyciu pakietów Angler, Styx i Nuclear

Pakiet exploitów Angler pojawił się po raz pierwszy w naszych danych telemetrycznych w ostatnim tygodniu września. Zwykle jest dystrybuowany za pośrednictwem złośliwych reklam.

STRONA DOCELOWA I WZORZEC URL

Adresy URL Anglera do tej pory miały dość prosty format, przez co łatwo je zidentyfikować. Oto kilka przykładów:

- http://ku[...]va.da[...]in.ca/se2v9pa2gx
- http://tn[...]ig.pi[...]et.com/s6u9qe8qtk
- http://ha[...]an.na[...]lq.com/m2b3hvvg2n
- http://je[...]ne.ma[...]ne.com/1gi0tjg36m
- http://ve[...]at.xa[...]ls.com/gwxywna71f

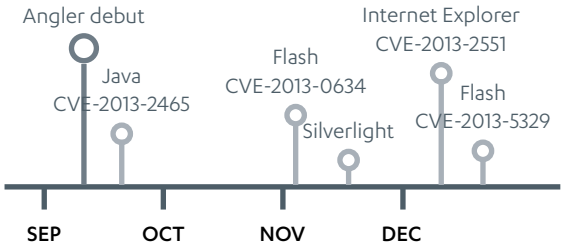
Strona docelowa również ma godne uwagi cechy. Początkowo tytuł strony docelowej brzmiał „Gmail". Następnie zmieniono go na „Microsoft apple.com". W grudniu zmieniono go ponownie na „Micrsoft apple.com" (z brakującą literą „o") (zob. **rysunek 3**)..

Rysunek 3: Tytuł strony docelowej zmieniony na "Micrsoft apple.com"

Inną szczególną cechą strony docelowej jest użycie właściwości obiektu okna jako znaczników dla wtyczek podatnych na atak. Wszystkie właściwości mają wspólny prefiks, który autorzy od czasu do czasu aktualizują. Na przykład w połowie listopada prefiks brzmiał „sterling", a właściwości window.sterlingj, window.sterlingf i window.sterlings wskazywały obecność podatnych wersji Javy, Flasha i Silverlighta. Pod koniec grudnia prefiks zmieniono na „zitumba".

F-Secure wykrywa stronę docelową jako **Exploit:JS/AnglerEK.A**.

EXPLOITY



Rysunek 4: Luki w zabezpieczeniach wykorzystywane przez Anglera

Internet Explorer

W grudniu 2013 r. do Anglera dodano exploit wymierzony w lukę CVE-2013-2551. Luka ta została zademonstrowana przez VUPEN-a podczas konkursu Pwn2Own na konferencji CanSecWest 2013, która odbyła się w marcu 2013 r. Microsoft załatał lukę w maju 2013 r.

F-Secure wykrywa exploit CVE-2013-2551 w Anglerze jako **Exploit:JS/AnglerEK.A**.

Java

Kiedy Angler pojawił się po raz pierwszy we wrześniu 2013 r., zawierał tylko jeden exploit, który był wymierzony w lukę CVE-2013-2465 w zabezpieczeniach Javy. Luka ta została załatana w poprawce Java 7 update 25, którą wydano w czerwcu 2013 r.

W grudniu 2013 r. Angler nadal atakował tę samą lukę w zabezpieczeniach Javy. Pojawił się jednak pewien interesujący szczegół, jeśli chodzi o dostarczanie exploitu — archiwum JAR skompresowano za pomocą programu gzip i Pack200, metody kompresji specjalnie zoptymalizowanej pod kątem archiwów JAR. Angler to pierwszy (i obecnie jedyny) pakiet exploitów, który używa metody Pack200.

F-Secure wykrywa exploity Javy w Anglerze jako **Exploit:Java/CVE-2013-2465.A** and **Exploit:Java/Majava.J**.

Flash

Pierwszy exploit Flasha dodano do Anglera w listopadzie 2013 r. Był on wymierzony w lukę CVE-2013-0634, którą załatano w lutym 2013 r.

Exploit Flasha używa szyfrowania i obfuskacji. Zewnętrzna warstwa exploitu odszyfrowuje osadzony kod Flasha za pomocą jednobajtowego klucza XOR i wczytuje go. Większość nazw metod, klas i zmiennych w wewnętrznym kodzie Flasha poddano obfuskacji, uzyskując takie nazwy, jak _e_-----, _e_--_ oraz _e_--_- (zob. **rysunek 5)**. Ponadto najważniejsze łańcuchy zostały zaszyfrowane algorytmem AES128. Łańcuchy są deszyfrowane „w locie" za pomocą klucza przechowywanego w programie. Na przykład wyrażenie regularne, które uaktywnia lukę w zabezpieczeniach, jest zapisane w postaci zaszyfrowanej algorytmem AES128.

W grudniu 2013 r. do Anglera dodano obsługę luki CVE-2013-5329 w zabezpieczeniach Flasha, która została załatana w listopadzie 2013 r. Angler był pierwszym pakietem exploitów, który atakował tę lukę. Jednocześnie plik Flasha nadal zawierał exploit luki CVE-2013-0634.

Algorytm szyfrowania zewnętrznej warstwy zmieniono z jednobajtowego XOR na RC4. Zamiast po prostu przechowywać

Rysunek 5: Nazwy metod, klas i zmiennych poddane obfuskacji

klucz szyfrowania w pliku Flasha i stamtąd go wczytywać, składa się go bajt po bajcie w kodzie ActionScript w czasie wykonania. Autorzy exploita zwrócili też szczególną uwagę na wczytywanie osadzonego obiektu Flasha — używają metody flash.system.WorkerDomain.createWorker zamiast dobrze znanej i bardziej popularnej metody flash.display.Loader.loadBytes method. Co więcej, wszystkie łańcuchy związane z wczytywaniem obiektu Flasha (tzn. nazwy klas i metod) są chronione szyfrem AES128 i deszyfrowane na bieżąco. Po RC4 nie ma już dalszych warstw obfuskacji ani szyfrowania, a odszyfrowany kod Flasha zawiera takie łańcuchy, jak „attack", „Shellcode" i „DoExploit".

F-Secure wykrywa exploity Flasha w Anglerze jako **Exploit:SWF/Salama.H**.

Silverlight

W listopadzie do Anglera dodano exploit wymierzony w Silverlighta, co oznacza, że jest to pierwszy w historii pakiet exploitów, który atakuje Silverlighta. Exploit wykorzystuje dwie różne luki w zabezpieczeniach: CVE-2013-3896 i CVE-2013-0074. Luka CVE-2013-3896 pozwala napastnikowi uzyskać informacje o pamięci procesu i wykorzystać je do obejścia zabezpieczeń ASLR i DEP. Microsoft załatał ją w październiku 2013 r. Druka luka, CVE-2013-0074, umożliwia wykonywanie kodu w kontekście zabezpieczeń bieżącego użytkownika i została usunięta przez Microsoft w marcu 2013 r.

Choć Flash i Java mają znacznie większy udział w rynku, są przynajmniej dwa prawdopodobne powody, dla których autorzy Anglera dodali exploit Silverlighta. Po pierwsze, było to łatwe — działający exploit z pełnym kodem źródłowym został opublikowany w witrynie Packet Storm w październiku 2013 r. Po drugie, Silverlight jest wymagany przez przynajmniej jedną bardzo popularną witrynę: Netflix. Ma ona ponad 40 milionów abonentów, którzy używają Silverlighta do strumieniowej transmisji wideo.
F-Secure wykrywa exploit Silverlighta jako **Exploit:MSIL/CVE-2013-0074.E.**

ŹRÓDŁO

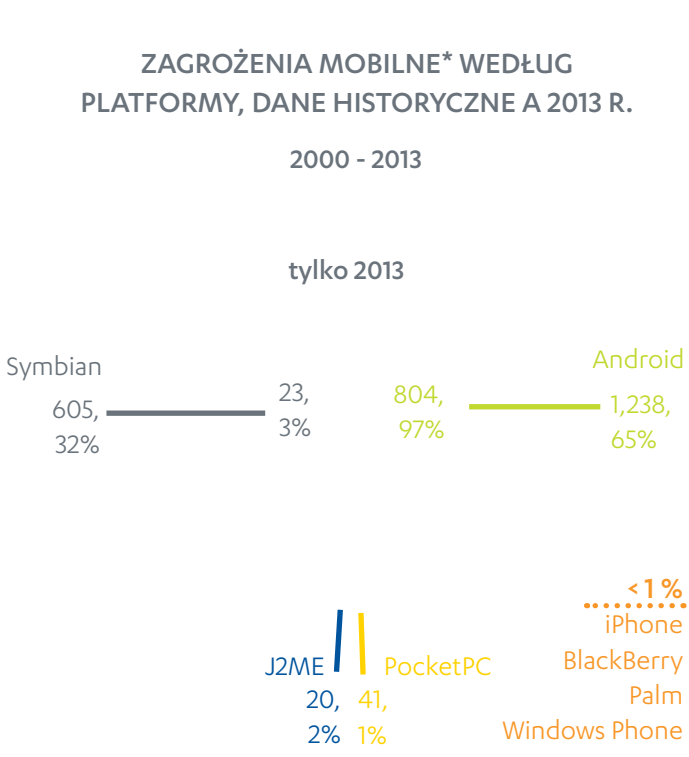
1. Krebs on Security; Brian Krebs; *Meet Paunch: The Accused Author of the BlackHole Exploit Kit*; published 6 December 2013; http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/

WSZYSTKO O ANDROIDZIE

Nikogo już nie zdziwi, że Android pozostaje najczęściej atakowanym mobilnym systemem operacyjnym. Platforma ta była celem dla 804 nowych rodzin lub wariantów złośliwego oprogramowania, co stanowi 97 proc. nowych zagrożeń, jakie zaobserwowaliśmy do końca 2013 r. Pozostałe 23 nowe zagrożenia (3 proc. w skali roku) były wymierzone w Symbiana. W minionym roku nie pojawiło się żadne nowe zagrożenie na innej platformie. Ze względu na tak dużą dysproporcję, kiedy w niniejszym raporcie na temat zagrożeń omawiamy zagrożenia mobilne w drugiej połowie roku, to skupiamy się tylko na zagrożeniach dla użytkowników Androida.

LZ danych zgłoszonych do chmurowych systemów F-Secure przez użytkowników naszego mobilnego produktu zabezpieczającego w drugiej połowie 2013 r. wynika, że w dziesięciu najczęściej atakowanych krajach łączna liczba detekcji złośliwych programów do Androida nieznacznie przekroczyła 140 000 — jest to wciąż kropla w morzu w porównaniu z komputerami stacjonarnymi. Pomimo względnie niewielkiej liczby detekcji, warto odnotować zmiany w krajobrazie zagrożeń mobilnych, ponieważ pokazują one, jak autorzy złośliwego oprogramowania cyzelują swoją taktykę, aby zyskać więcej ofiar i usprawnić metody generowania zysków.

Spośród 10 krajów, z których zgłaszano wykrycia złośliwego oprogramowania do Androida w drugiej połowie 2013 r., aż 75 proc. raportów pochodziło z Arabii Saudyjskiej i Indii; dla porównania, pięć europejskich krajów na liście reprezentowało niewiele ponad 15 proc. zgłoszonych detekcji. Dalsza analiza daje nam szkicową mapę najczęstszych zagrożeń, z którym mają do czynienia użytkownicy naszego produktu zabezpieczającego w poszczególnych regionach lub państwach (zob. następna strona). Godnym uwagi wzorem jest szeroka dystrybucja trojanów GinMaster, które należą do pierwszej trójki rodzin złośliwego oprogramowania w Europie, Azji i obu Amerykach. Niemal równie rozpowszechniona jest duża rodzina Fakeinst, niemal równomiernie obecna w całej Europie, a także rodzina SmsSend.



* Liczba nowych rodzin albo nowych wariantów istniejących rodzin dla wszystkich platform mobilnych.

ULEPSZONE ZABEZPIECZENIA

Choć autorzy złośliwego oprogramowania są niemal całkowicie skupieni na Androidzie — a może właśnie dlatego — nie można powiedzieć, że Google nie podejmuje aktywnych starań o zwiększenie stopnia bezpieczeństwa platformy. Każda nowa wersja wydawana przez giganta technologicznego zawiera pewne zmiany, które ograniczają skutki działania złośliwego oprogramowania. Na przykład w Androidzie 4.3 (Jellybean) wprowadzono prośbę o potwierdzenie, która jest wyświetlana, kiedy aplikacja Wiadomości wysyła dużą liczbę SMS-ów w krótkim czasie. Chroni ona przed aplikacjami, które po cichu wysyłają setki SMS-ów (choć podobno bywa irytująca dla użytkowników, którzy regularnie wysyłają wiadomości grupowe). We wrześniowym wydaniu Androida 4.4 (Kit Kat) również pojawił się wiele poprawek bezpieczeństwa, choć usunięcie ukrytej funkcji AppOps może być interpretowane jako krok wstecz przez tych, którzy chcą mieć większą kontrolę nad przywilejami zainstalowanych aplikacji.

Choć ulepszenia dodawane do kolejnych wersji stopniowo zwiększają stopień bezpieczeństwa samej platformy, z konkretnymi urządzeniami bywa różnie, ponieważ pofragmentowana natura ekosystemu Androida praktycznie uniemożliwia zapewnienie jednolitej ochrony wszystkim użytkownikom. Dla większości użytkowników oznacza to, że bezpieczeństwo urządzeń spoczywa głównie w ich rękach — w przenośni i dosłownie.

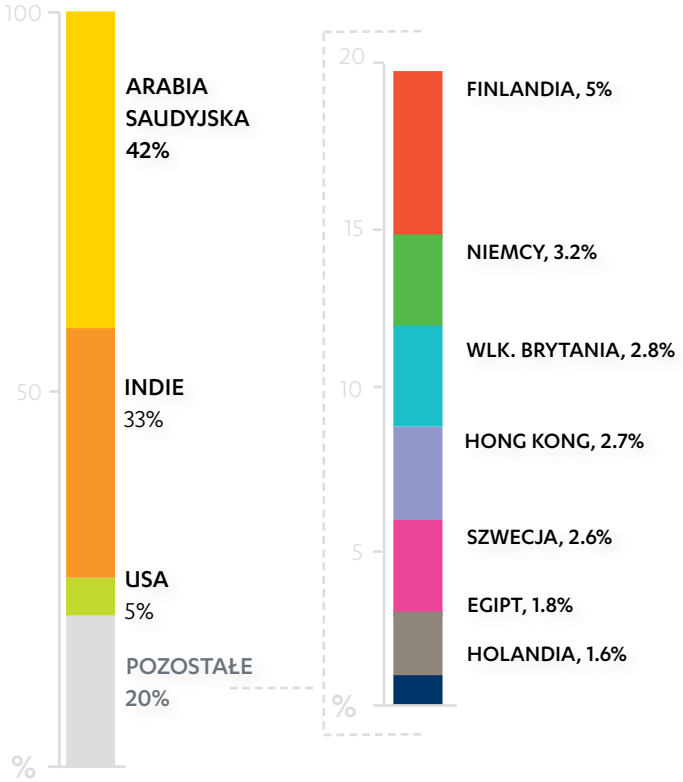
WYKORZYSTYWANIE UŻYTKOWNIKÓW

W przeciwieństwie do złośliwego oprogramowania wymierzonego w komputery stacjonarne, do dziś tylko nieliczne szkodliwe programy do Androida atakują luki w zabezpieczeniach systemu operacyjnego, takie jak luka Masterkey, która została publicznie ogłoszona na początku 2013 r. (więcej informacji o lukach w zabezpieczeniach Androida znajduje się na stronie 28). Choć później w niezależnych sklepach z aplikacjami odkryto nieliczne programy wykorzystujące tę lukę, to dotychczas były one wyjątkami od reguły. Może to po prostu wynikać z faktu, że Android jest względnie szczelny — w 2013 r. ujawniono publicznie zaledwie 7 luk w zabezpieczeniach Androida[1], podczas gdy w przypadku platformy iOS było to 90 luk ujawnionych w tym samym okresie[2]. Bardziej cyniczna hipoteza zakłada jednak, że autorom złośliwego oprogramowania nie chce się szukać skomplikowanych sposobów ataku, skoro mogą po prostu skłonić użytkownika, aby przyznał im dostęp do urządzenia.

ŹRÓDŁA

1. CVE Details; *Google > Android > Vulnerability Statistics;* http://www.cvedetails.com/product/19997/Google-Android.html
2. CVE Details; *Apple > Iphone Os > Vulnerability Statistics;* http://www.cvedetails.com/product/15556/Apple-Iphone-Os.html

10 KRAJÓW NAJCZĘŚCIEJ ZGŁASZAJĄCYCH DETEKCJE ZŁOŚLIWEGO OPROGRAMOWANIA DO ANDROIDA W DRUGIEJ POŁOWIE 2013 R.,

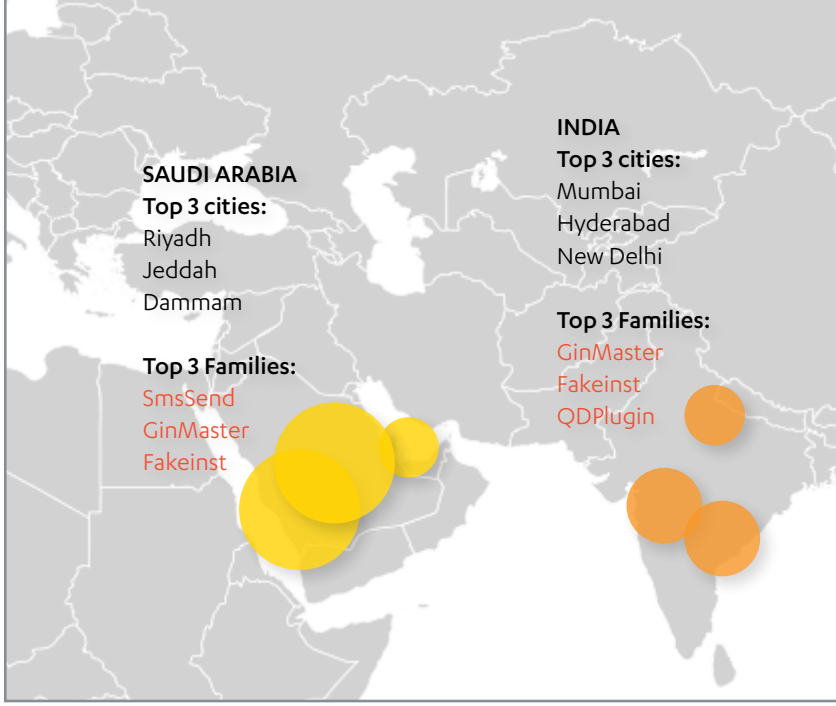


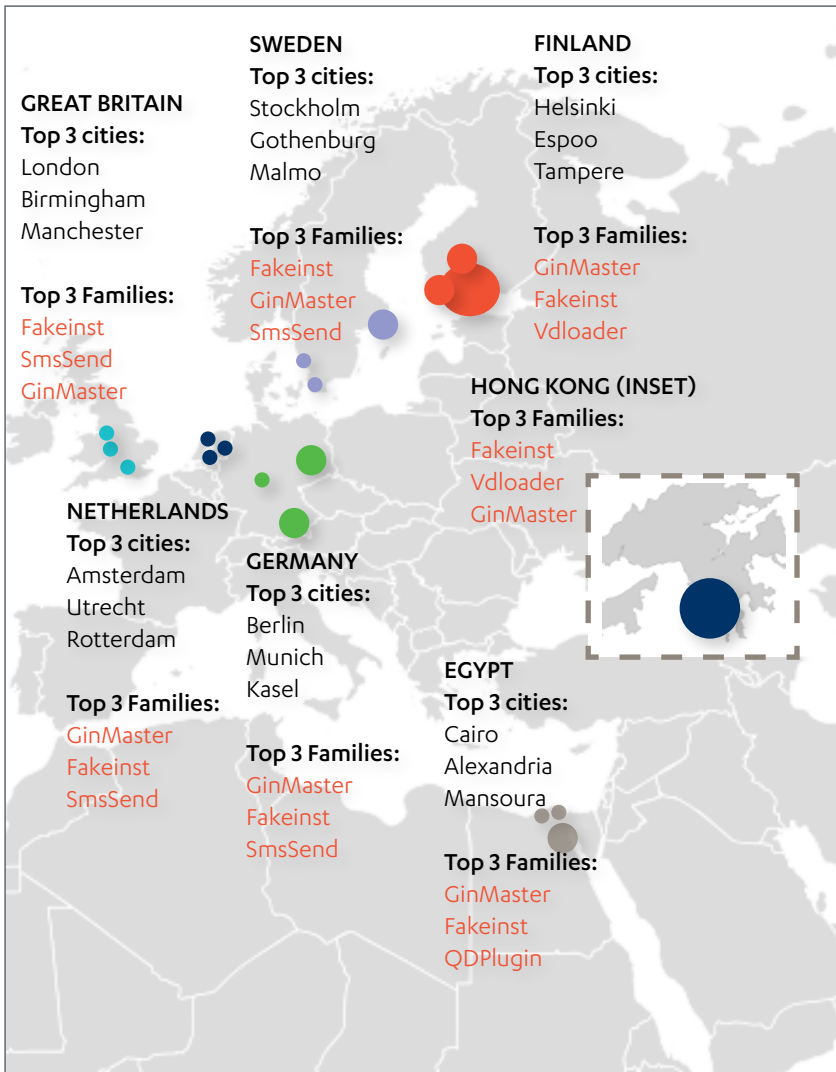
W drugiej połowie 2013 r. dziesięć najczęściej atakowanych krajów zgłosiło do naszych systemów chmurowych niewiele ponad 140 000 detekcji złośliwych programów do Androida, przy czym większość detekcji raportowano z Arabii Saudyjskiej i Indii. Pozostałe 25 proc. wykryć było rozproszonych po Europie, a innymi godnymi uwagi krajami były tylko Hongkong i Egipt.

NAJCZĘŚCIEJ WYKRYWANE RODZINY ZŁOŚLIWEGO OPROGRAMOWANIA I 3 NAJCZĘŚCIEJ ATAKOWANE STA W 10 NAJCZĘŚCIEJ ATAKOWANYCH KRAJACH W RUGIEJ POŁOWIE 2013 R., WEDŁUG LICZBY DETEKCJI

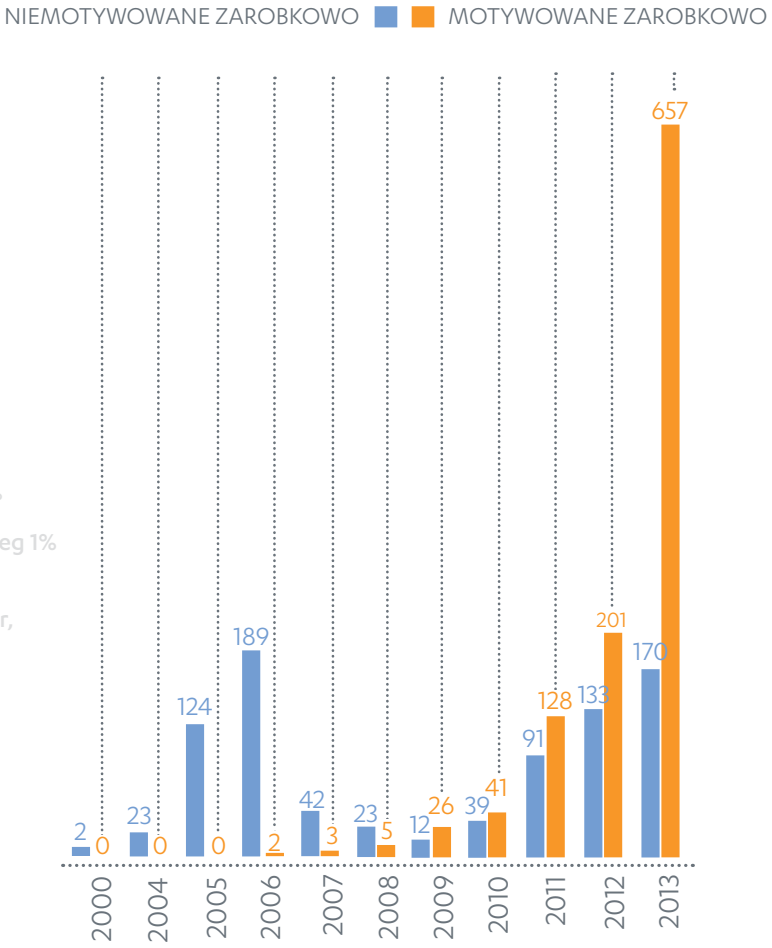
Mapy po prawej stronie przedstawiają 3 najczęściej atakowane miasta w każdym z 3 najczęściej atakowanych krajów (powyżej), w oparciu o liczbę detekcji znanych rodzin złośliwego oprogramowania na Androida, które zostały zgłoszone do naszych systemów chmurowych.

Porównujemy również 3 rodziny złośliwego oprogramowania na Androida najczęściej wykrywane w każdym z państw z pierwszej dziesiątki — z wyjątkiem specjalnego regionu administracyjnego Hongkongu, który do celów ilustracyjnych jest tu traktowany jak jedno miasto.

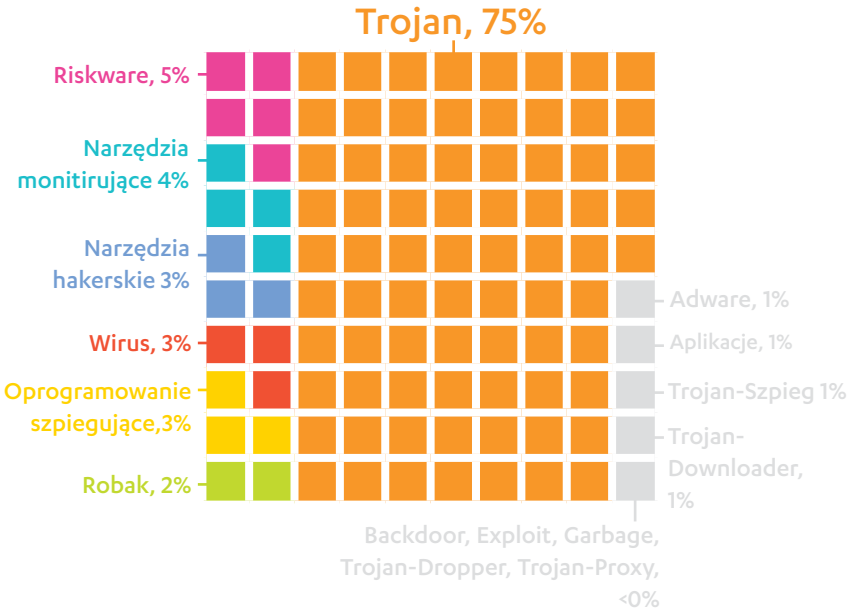




ZAGROŻENIA MOBILNE* MOTYWOWANE ZAROBKOWO 2000 - 2013 R.



ZAGROŻENIA MOBILNE* WEDŁUG TYPU, 2000 - 2013



* Na podstawie liczby unikatowych próbek dla wszystkich platform

ANDROID

PRZYZWOLENIE NA ZŁOŚLIWOŚĆ

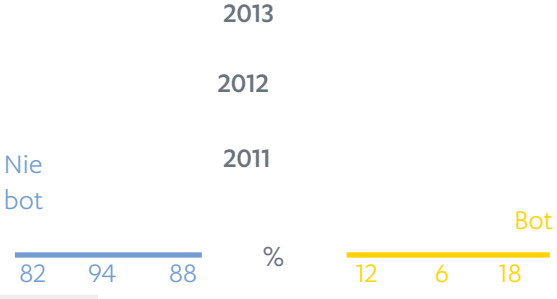
Zdecydowana większość złośliwych aplikacji do Androida wykorzystuje mechanikę interakcji użytkownika z jego urządzeniem. Najczęściej spotykany typ złośliwego oprogramowania — trojany (zob. wyżej) — zawiera złośliwe procedury wstawione do pakietów legalnych programów (najczęściej popularnych gier i aplikacji kasynowych), które są następnie redystrybuowane w różnych sklepach z aplikacjami, często pod nową nazwą, która przypomina pierwotną aplikację. Przepakowana aplikacja zwykle prosi o więcej uprawnień, niż oryginalny, niestrojanizowany program, co jest „słabym punktem", który umożliwia trojanowi wykonywanie złośliwych procedur, czy chodzi o wysyłanie wiadomości SMS, czy o łączenie się z botnetem podobnie zainfekowanych urządzeń (prawy dolny róg). Przepakowywanie aplikacji zasadniczo jest nowym wcieleniem inżynierii społecznej, ponieważ trojany wykorzystują niepowstrzymane pragnienie zainstalowania i używania popularnej aplikacji, aby zyskać przywileje niezbędne do wykonywania złośliwych procedur.

W niektórych przypadkach przepakowana aplikacja przynosi straty nie tylko użytkownikowi urządzenia — który płaci za wiadomości SMS wysyłane przez złośliwe oprogramowanie albo za aplikację, która powinna być darmowa — ale również twórcy pierwotnej aplikacji, jeśli był to płatny program, który teraz jest rozpowszechniany za darmo albo z zyskiem dla tego, kto ją przepakował. Większość zagrożeń mobilnych, które zaobserwowaliśmy w 2013 r., było motywowanych zarobkowo (na górze). Więcej informacji o trendach w złośliwych aplikacjach w tym okresie znajduje się na stronie 25.

REKLAMY ZŁOŚLIWEGO OPROGRAMOWANIA MOBILNEGO

Najczęściej używanym kanałem dystrybucji złośliwego oprogramowania mobilnego są nadal niezależne sklepy z aplikacjami, ale w kilku ostatnich latach zdarzało się, że w przeglądarkach mobilnych pojawiały się reklamy złośliwych programów o mniej więcej następującej treści: „Ostrzeżenie! Twoje urządzenie jest zainfekowane. Pobierz naszą aplikację, aby zdezynfekować swoje urządzenie". Jest to zasadniczo metoda dystrybucji fałszywego oprogramowania antywirusowego przeniesiona z platform stacjonarnych na mobilne. Więcej informacji o kanałach dystrybucji złośliwego oprogramowania znajduje się w studium przypadku „Profilowanie wektorów infekcji" na stronie 33.

MOBILNE BOTY DO ANDROIDA†, 2011 - 2013 R.



† Na podstawie liczby detekcji (rodziny i warianty) programów z funkcjami bota w odpowiednich latach.

TRENDY W APLIKACJACH I SKLEPACH Z APLIKACJAMI

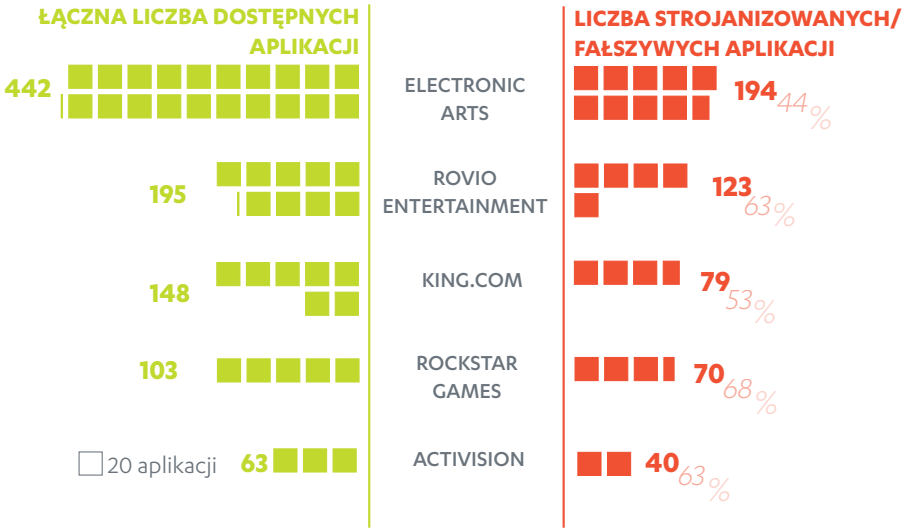
W DRUGIEJ POŁOWIE 2013 R. ZNALEŹLIŚMY LUB OTRZYMALIŚMY I SKLASYFIKOWALIŚMY 182 015 APLIKACJI MOBILNYCH. PONIŻEJ ZNAJDUJE SIĘ KILKA OBSERWACJI OPARTYCH NA ZGROMADZONYCH PRÓBKACH.

PRZEPAKOWANE LUB SFAŁSZOWANE APLIKACJE

Autorzy złośliwego oprogramowania, którzy chcą zmaksymalizować liczbę ofiar instalujących ich „produkty", często wykorzystują zainteresowanie popularnymi aplikacjami, zwłaszcza grami. Częstą taktyką jest przepakowywanie lub trojanizowanie legalnych, popularnych aplikacji w celu dołączenia złośliwego kodu. Twórcy złośliwego oprogramowania mogą też stworzyć fałszywą aplikację o wyglądzie legalnego programu (ta sama nazwa, ikona), ale bez jego funkcjonalności.

WPrzepakowane czy sfałszowane, aplikacje spreparowane przez napastnika mogą zawierać dowolny rodzaj złośliwego kodu. Na przykład częstym dodatkiem jest prosta, ograniczona funkcja cichego wysyłania SMS-ów, wymuszająca na użytkowniku zapłacenie za aplikację, która w rzeczywistości powinna być darmowa. Rzadziej fałszywa aplikacja jest pełnym trojanem z dodatkowymi funkcjami, które narażają na niebezpieczeństwo dane lub urządzenie użytkownika, a także grożą zawyżonym rachunkiem. Do szarego obszaru należą aplikacje, które zostały przepakowane, ale nie po to, aby dodać złośliwy kod. W takich przypadkach do aplikacji mógł zostać wstawiony moduł reklamowy przynoszący zyski temu, kto przepakował aplikację (a nie deweloperowi oryginalnego programu). Inny scenariusz to złamane programy, w których dodatkowy kod umożliwia korzystanie z aplikacji bez płacenia za nią, i w tym przypadku ze szkodą dla pierwotnego autora.

DEWELOPERZY I WYDAWCY, KTÓRYCH APLIKACJE TROJANIZOWANO LUB FAŁSZOWANO W DRUGIEJ POŁOWIE 2013 R.



8 APLIKACJI Z PLAY STORE, KTÓRE SĄ NAJCZĘŚCIEJ PRZEPAKOWYWANE

% próbek danej aplikacji znalezionych w drugiej połowie 2013 r., które są przepakowanymi wersjami dystrybuowanymi za pośrednictwem niezależnych sklepów

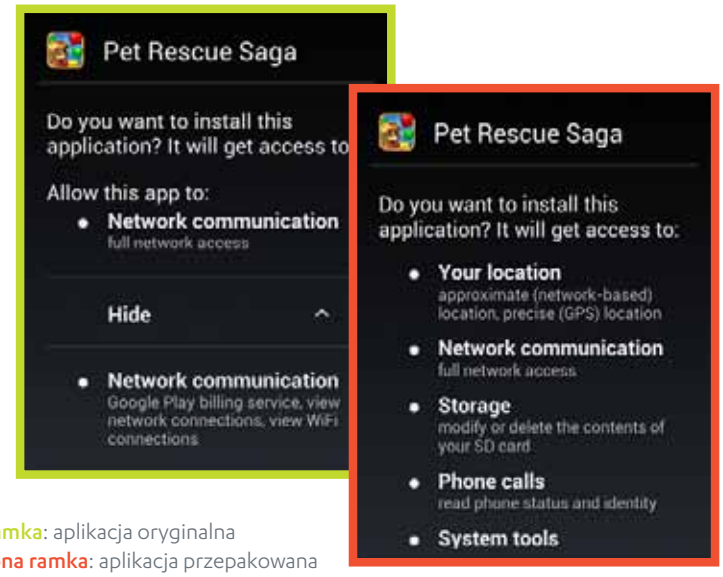
CZĘSTO TROJANIZOWANE APLIKACJE

Niektórzy twórcy lub wydawcy oprogramowania (powyżej) wydają się szczególnie cierpieć na przepakowywaniu lub fałszowaniu produktów, ponieważ znaczna część ich programów ma strojanizowane lub fałszywe wersje dostępne w niezależnych sklepach.

W połowie grudnia 2013 r. przyjrzeliśmy się 20 najpopularniejszym aplikacjom w Google Play Store i zbadaliśmy wskaźnik ich trojanizacji. W tym przypadku za strojanizowaną wersję uznawaliśmy taką, która używa nazwy pierwotnego pakietu i aplikacji, ale prosi o więcej uprawnień, niż oryginał. Okazało się, że spośród 20 najpopularniejszych aplikacji w Play Store 8 ma wiele strojanizowanych wersji, które są dostępne w niezależnych sklepach (po lewej stronie).

Co interesujące, obie aplikacje, które miały najwyższy odsetek strojanizowanych wersji ze zmienionymi uprawnieniami, były programami kasynowymi. Spośród wszystkich próbek aplikacji „Doubledown Casino - Free Slots", które znaleźliśmy w drugiej połowie 2013 r., 33 proc. stanowiły wersje przepakowane i redystrybuowane za pośrednictwem niezależnych sklepów z aplikacjami, podobnie jak 23 proc. próbek aplikacji „Slotmania - Free Slots" zaobserwowanych w tym samym okresie. Ponieważ aplikacje hazardowe to jeden z nielicznych typów programów (pominąwszy aplikacje bankowe), które wiążą się z transakcjami pieniężnymi, duże rozpowszechnienie ich strojanizowanych wersji szczególnie nie dziwi. Sześć pozostałych aplikacji, które miały wiele strojanizowanych wersji, to popularne gry.

UPRAWNIENIA, O KTÓRE PROSI APLIKACJA PRZEPAKOWANA I ORYGINALNA



Żółta ramka: aplikacja oryginalna
Czerwona ramka: aplikacja przepakowana

10 UPRAWNIEŃ, O KTÓRE NAJCZĘŚCIEJ PROSZĄ PRZEPAKOWANE APLIKACJE, PROCENTOWO

APLIKACJE PROSZĄCE O JEDNO UPRAWNIENIE %	ŻĄDANE UPRAWNIENIE	APLIKACJE PROSZĄCE O WIELE UPRAWNIEŃ %
	android.permission.	
1	INTERNET	98
	READ_PHONE_STATE	96
	WRITE_EXTERNAL_STORAGE	90
98	SEND_SMS	84
	RECEIVE_SMS	77
	ACCESS_NETWORK_STATE	72
	READ_SMS	67
	WAKE_LOCK	57
	RECEIVE_BOOT_COMPLETED	52
1	OTHERS	<50
	com.android.launcher.permission.	
	INSTALL_SHORTCUT	67

ANDROID

ŻĄDANE PRZYWILEJE

Co do dodatkowych przywilejów, o które proszą strojanizowane wersje, najczęściej mają one związek z dołączonym modułem reklamowym, ale niektóre umożliwiają również wykonywanie złośliwego kodu. Te dodatkowe uprawnienia to coś, co ostrożni użytkownicy mogą wykorzystać do identyfikowania aplikacji, których nie chcieliby instalować. Na przykład powyżej pokazano dodatkowe uprawnienia, o które prosi strojanizowana wersja popularnej gry Pet Rescue Saga. Kiedy ktoś instaluje tę aplikację i widzi, że domaga się ona dostępu do „Połączeń telefonicznych", powinien zadać sobie pytanie: „Po co grze takie uprawnienie"?

Przyglądając się bardziej ogólnie łącznym statystykom uprawnień, o które prosi złośliwe oprogramowanie, spośród 182 015 złośliwych aplikacji znalezionych przez nas w drugiej połowie 2013 r. 99 proc. domagało się wielu uprawnień. Powyżej wymieniono dziesięć najczęściej żądanych przywilejów. Łatwo się domyślić, dlaczego pierwsza czwórka wygląda w ten sposób. Uprawnienie (INTERNET) jest niezbędne, ponieważ stanowi jeden z fundamentalnych elementów złośliwego oprogramowania. Dostęp do zewnętrznej pamięci masowej (WRITE_EXTERNAL_STORAGE) przydaje się do zapisywania pobranych danych, co jest operacją typową dla złośliwych programów. W przypadku urządzeń mobilnych nie dziwi też uprawnienie (SEND_SMS), które umożliwia wysyłanie SMS-ów.

Spośród wszystkich złośliwych programów, które zaobserwowaliśmy w tym okresie, zaledwie 1 proc. prosiło o tylko jedno uprawnienie. W tym podzbiorze najczęściej żądano dość oczywistego uprawnienia SEND_SMS.

NAZWY PAKIETÓW

23 proc. zbadanych przez nas złośliwych programów podszywa się pod legalne aplikacje, używając nazw pakietów, które wyglądają na autentyczne, jak pokazano w chmurze tekstowej (po prawej stronie). Inne złośliwe programy (zwłaszcza z rodziny Fakeinst) nie wysilają się i po prostu używają przypadkowych

TEKSTOWA CHMURA NAZW PAKIETÓW UŻYWANYCH PRZEZ ZŁOŚLIWE OPROGRAMOWANIE DO ANDROIDA

nazw pakietów (po prawej stronie), co zwykle oznacza, że plik jest mocno podejrzany.

Dziwić może to, że kiedy użytkownik instaluje aplikację Androida, te podejrzane nazwy pakietów nie są wyświetlane — byłoby dobrze, gdyby to niedopatrzenie zostało naprawione w przyszłych wersjach systemu operacyjnego.

ZŁOŚLIWE OPROGRAMOWANIE W SKLEPACH

Obecnie niezależne sklepy z aplikacjami do Androida wydają się rozwijać w dość dużym tempie. Widać to po łącznej liczbie próbek aplikacji (złośliwych i niezłośliwych) o znanym pochodzeniu, które otrzymaliśmy w drugiej połowie roku (reprezentowanej przez rozmiary kół na rysunku po prawej stronie). Co nie dziwi, to fakt, że z wyjątkiem ogromnego, międzynarodowego Google Play Store, cztery największe sklepy — Anzhi, Mumayi, Baidu i eoeMarket — służą użytkownikom z kontynentalnych Chin, którzy mają ograniczony dostęp do Play Store.

Ludowa mądrość głosi, że niezależne sklepy z aplikacjami są najbardziej prawdopodobnym źródłem złośliwego oprogramowania. Aby z grubsza zmierzyć, jak bardzo narażony jest użytkownik, który przegląda te sklepy, policzyliśmy złośliwe programy otrzymane w próbkach z danego sklepu i porównaliśmy je z łączną liczbą próbek z tego samego źródła. Liczyliśmy tylko unikatowe, oddzielne próbki, więc wiele próbek tego samego złośliwego programu policzyliśmy tylko raz.

Jak się okazuje, w czterech największych sklepach niespełna 10 proc. próbek miało złośliwy charakter. Spośród wszystkich zbadanych sklepów najwyższy udział złośliwego oprogramowania zaobserwowaliśmy w Android159 — sklasyfikowaliśmy w ten sposób 33 proc. pochodzących z niego próbek.

Na dole listy znalazł się Google Play z najniższym udziałem złośliwego oprogramowania w zebranych próbkach (0,1 proc.) — w tym przypadku dobrze być ostatnim! Ponadto jest największe prawdopodobieństwo, że Play Store szybko usunie szkodliwe aplikacje, więc napotkane tam złośliwe oprogramowanie zwykle nie cieszy się długim żywotem.

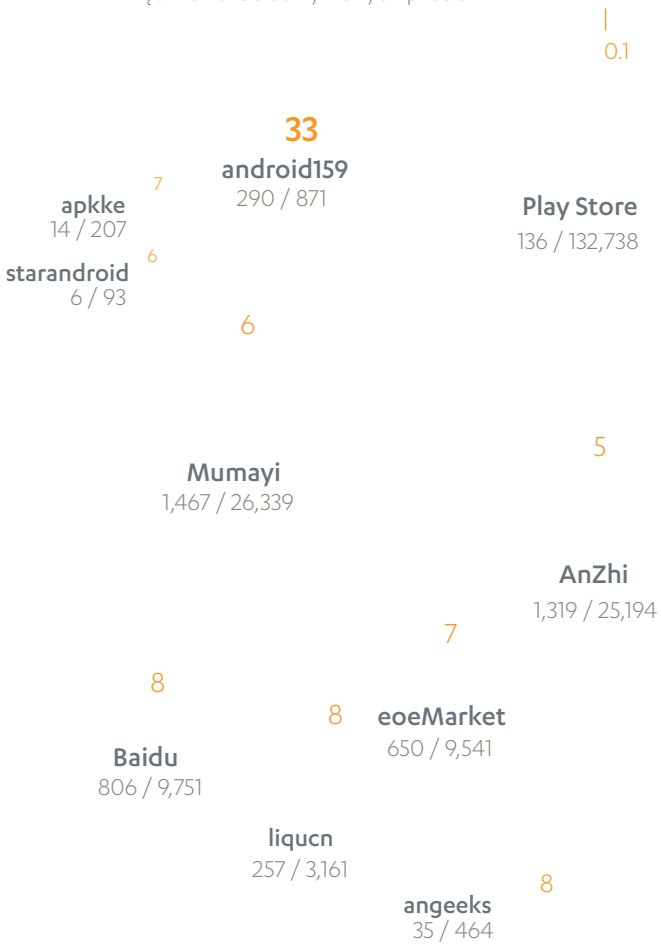
OPROGRAMOWANIE REKLAMOWE I RYZYKOWNE W GOOGLE PLAY

Wreszcie dla porównania zbadaliśmy statystyki oprogramowania reklamowego i ryzykownego, które jest dostępne w Google Play Store (na dole).

OTRZYMANE PRÓBKI ZŁOŚLIWEGO OPROGRAMOWANIA, WG SKLEPU Z APLIKACJAMI

% próbek pochodzących z danego sklepu sklasyfikowanych jako złośliwe oprogramowanie

unikatowe próbki złośliwego oprogramowania / łączna liczba otrzymanych próbek



LICZBA* PRÓBEK OPROGRAMOWANIA REKLAMOWEGO I RYZYKOWNEGO ZNALEZIONYCH W GOOGLE PLAY STORE

Oprogramowanie reklamowe

Aplikacje są klasyfikowane jako **oprogramowanie reklamowe,** jeśli zawierają funkcję wyświetlania reklam, która naraża prywatność lub bezpieczeństwo użytkownika, na przykład poprzez ujawnianie lub gromadzenie danych osobistych albo kierowanie do podejrzanych aplikacji, witryn lub treści.

Rodzina	Łączna liczba
AirPush	9,382
AdWo	369
Ropin	59
Dowgin	22
Waps	23

Rodzina	Łączna liczba
Minimob	51
SmsReg	4
PremiumSMS	1

Oprogramowanie ryzykowne

Aplikacje są klasyfikowane jako **oprogramowanie ryzykowne,** jeśli mogą narażać prywatność lub bezpieczeństwo użytkownika, kiedy są używane w niewłaściwy sposób. Uwaga: warianty z rodziny PremiumSMS można sklasyfikować jako oprogramowanie reklamowe lub ryzykowne, w zależności od ich działania.

* Liczba unikatowych, oddzielnych próbek; wiele kopii unikatowej próbki policzono tylko raz

LUKI W ZABEZPIECZENIACH ANDROIDA

POD KONIEC DRUGIEJ POŁOWY 2013 R. LICZBA ZNANYCH LUK W ZABEZPIECZENIACH ANDROIDA POZOSTAJE ZASKAKUJĄCO MAŁA, ZWAŻYWSZY NA ILOŚĆ OPROGRAMOWANIA ZNAJDUJĄCEGO SIĘ W CAŁYM EKOSYSTEMIE.

Ogólna reguła jest taka, że ataki przeciwko urządzeniom Androida nie są wymierzone bezpośrednio w lukę w zabezpieczeniach samego systemu operacyjnego. Zamiast tego napastnik wykorzystuje lukę w zabezpieczeniach zainstalowanej aplikacji, co z kolei umożliwia mu manipulowanie urządzeniem.

PRODUCENCI URZĄDZEŃ JAKO ŹRÓDŁO LUK W ZABEZPIECZENIACH

Zwykło się mówić, że luki w zabezpieczeniach, które mogą zostać wykorzystane przez napastnika, pojawiają się w urządzeniach głównie za sprawą instalowanych przez użytkownika, niezależnych aplikacji. Istnieją jednak inne, „ciche" źródła luk w zabezpieczeniach, nad którym użytkownicy nie mają żadnej kontroli. Badania[1] opublikowane w 2013 r. pokazują, że istotnym źródłem problemów są producenci urządzeń, którzy dostosowują standardowy kod Androida, aby zainstalować w urządzeniu własne funkcje lub aplikacje. Autorzy raportu posuwają się do stwierdzenia, że nawet 85 proc. aplikacji wstępnie instalowanych w urządzeniach zwiększa ryzyko, deklarując większe uprawnienia, niż to rzeczywiście konieczne. Te same badania wskazują, że od 65 do 85 proc. wszystkich w luk zabezpieczeniach wynika z takich dostosowań.
Ekosystem Androida z założenia pozwala producentom na oferowanie wielu urządzeń, z których każde działa pod kontrolą innej wersji platformy (i często ma własny harmonogram aktualizacji wersji). Doprowadziło to do innego nazwiska, które przyczynia się do obecności luk w urządzeniach z Androidem: fragmentacji platformy. Liczne konfiguracje platformy sprawiają, że producenci mają problemy z regularnym dostarczaniem poprawek zabezpieczeń do wszystkich użytkowników ich urządzeń. Choć „nieoficjalne" poprawki opracowywane metodami społecznościowymi częściowo łagodzą problem, to wymagają pewnej świadomości użytkowników oraz umiejętności technicznych.

POWIERZCHNIE ATAKU

Pomijając kwestię, czy dana aplikacja została zainstalowana przez użytkownika, czy przez producenta urządzenia, przyjrzyjmy się teraz samym aplikacjom. W każdym urządzeniu podłączonym do internetu najbardziej oczywistą aplikacją, do której można się zdalnie włamać, jest przeglądarka internetowa. Widać to szczególnie dobrze w komputerach stacjonarnych, ale urządzenia mobilne nie są wyjątkiem i pojawiło się już kilka exploitów wymierzonych zarówno w standardową przeglądarkę Androida, jak i w Firefoksa do Anroida (zob. następna strona).

Odtwarzacz Adobe Flash do Android to kolejny atrakcyjny cel dla zdalnych napastników. Długa historia problemów z bezpieczeństwem tej aplikacji (na komputerach PC) sugeruje, że jej mobilny odpowiednik również może zawierać jeszcze nieodkryte słabe punkty. Najnowsza poważna luka w zabezpieczeniach, odkryta w 2013 r. (zob. następna strona), dotyczy wielu produktów Adobe i ma charakter wieloplatformowy.

Ponieważ użytkownicy mają bardzo ograniczony wgląd w potencjalnie szkodliwe działanie aplikacji, fałszywe lub złośliwe aplikacje mogą spowodować jeszcze więcej szkód za sprawą luk w zabezpieczeniach, które można zaatakować lokalnie (zob. następna strona). Exploity polegające na eskalacji przywilejów pozwalają aplikacjom na niepożądane działania bez wiedzy użytkownika, a podatne na atak programy i usługi umożliwiają kradzież informacji.

WYKORZYSTYWANIE LUK W ZABEZPIECZENIACH

Jeśli nawet urządzenie z Androidem ma lukę w zabezpieczeniach, trzeba stworzyć specjalny kod, który będzie ją atakował. Kiedy powstawał ten tekst, witryna **Metasploit**, otwartego narzędzia używanego do testów penetracyjnych, zawierała bardzo nieliczne exploity wymierzone w platformę Android. Może to mieć wiele przyczyn, na przykład taką, że cel jest wciąż zbyt ezoteryczny albo zbyt nowy. To powiedziawszy, dość łatwo znaleźć zasoby, które pomogą zainteresowanym w stworzeniu takiego kodu, podczas gdy ci, którym nie chce się pracować, mogą po prostu kupić dzieła innych w witrynach takich jak **inj3ct0r.**

ŹRÓDŁA

1. North Carolina State University; Lei Wu, Michael Grace, Yajin Zhou, Chiachih Wu, Xuxian Jiang; *The Impact of Vendor Customizations on Android Security*; published 4 November 2013; http://www.cs.ncsu.edu/faculty/jiang/pubs/CCS13.pdf
2. CVE Details; *Vulnerability Details : CVE-2013-3363*; http://cvedetails.com/cve/2013-3363
3. CVE Details; *Vulnerability Details : CVE-2013-6632*; http://www.cvedetails.com/cve/CVE-2013-6632
4. IBM:Security Intelligence Blog; Roee Hay; *A New Vulnerability in the Android Framework: Fragment Injection*; published 10 December 2013; http://securityintelligence.com/new-vulnerability-android-framework-fragment-injection/
5. Pwn2Own 2013, PacSec 2013 Conference; Heather Goudey; *Local Japanese team exploits mobile applications to install malware on Samsung Galaxy S4*; published 13 November 2013; http://www.pwn2own.com/local-japanese-team-exploits-mobile-applications-install-malware-samsung-galaxy-s4/
6. CVE Details; *Vulnerability Details : CVE-2013-4787*; http://www.cvedetails.com/cve/CVE-2013-4787
7. Bluebox Blog; Jeff Forristal; *Uncovering Android Master Key That Makes 99% of Devices Vulnerable*; published 3 July 2013; http://bluebox.com/corporate-blog/bluebox-uncovers-android-master-key/
8. Bluebox Blog; Jeff Forristal; Commentary on the Android "Master Key" Vulnerability "Family"; published 29 July 2013; http://bluebox.com/corporate-blog/commentary-on-the-android-master-key-vulnerability-family/
9. Saurik; Jay Freeman; *Android Bug Superior to Master Key*; http://www.saurik.com/id/18
10. Saurik; Jay Freeman; *Exploit (& Fix) Android "Master Key"*; http://www.saurik.com/id/17

ANDROID W 2013 R.

TPoniższe luki w zabezpieczeniach Androida zostały publicznie ujawnione w 2013 r.

1 KONFIGURACJA, 2 LUKI (CVE-2013-4777 I CVE-2013-5933)

Dwie oddzielne luki w konkretnej konfiguracji wersji 2.3.7 Androida na telefonie Motorola Defy XT w ofercie Republic Wireless umożliwiają lokalnym użytkownikom wykonywanie poleceń powłoki z przywilejami superużytkownika albo doprowadzenie do przepełnienia bufora. W obu przypadkach exploit umożliwia napastnikowi uzyskanie nieautoryzowanego dostępu do informacji albo zmodyfikowanie konfiguracji urządzenia.

OBEJŚCIE BLOKADY URZĄDZENIA (CVE-2013-6271)

Luka w zabezpieczeniach pakietu „com.android.settings.ChooseLockGeneric" w wersjach Androida od 4.0 do 4.3, który umożliwia użytkownikowi zmodyfikowanie mechanizmu blokady urządzenia, mogłaby zostać wykorzystana przez specjalnie spreparowaną aplikację do obejścia ograniczeń

LOKALNA PODMIANA OBIEKTU FRAGMENT W INTERFEJSIE UŻYTKOWNIKA (CVE-2013-3666)

Badacze bezpieczeństwa aplikacji w IBM ogłosili, że znaleźli lukę w szkielecie interfejsu użytkownika. W swojej demonstracji koncepcji wykazali, że można użyć specjalnie spreparowanego obiektu Intent, aby podmienić obiekt Fragment w znanej klasie Activity w aplikacji ustawień systemu. Następnie za pomocą dodatkowych parametrów tego samego obiektu Intent można nakazać podmienionemu obiektowi Fragment, aby pominął pytanie o PIN. Pozwoliłoby to napastnikowi zmienić uprzywilejowane ustawienia urządzenia bez odpowiedniej autoryzacji. Atak ten działa przynajmniej na urządzeniach, które poprzedzają najnowsze wydanie Android 4.4

EXPLOIT PRZEGLĄDARKI (CVE-2013-6632)

Ta usterka dotyczy wszystkich przeglądarek Chrome w wersjach Androida starszych niż 31.0.1650.57. Została ujawniona, kiedy japoński zespół wykorzystał ją, aby zainstalować złośliwe oprogramowanie w telefonie podczas konkursu Mobile Pwn2Own na konferencji PacSec 2013. Luka pozwala zdalnemu napastnikowi wykonać dowolny kod albo spowodować uszkodzenie pamięci w procesie przeglądarki Chrome. Nie są znane żadne rzeczywiste ataki na tę lukę.

EXPLOIT FLASHA (CVE-2013-3363)

Tę lukę można wykorzystać zdalnie za pomocą specjalnie spreparowanego pliku Adobe Flash. Jest ona obecna w wielu produktach Adobe, m.in. we wszystkich wersjach odtwarzacza Adobe Flash starszych niż 11.1.111.73 w Androidzie 2.x i 3.x oraz starszych niż 11.1.115.81 w Androidzie 4.x. Nie są znane żadne rzeczywiste ataki na tę lukę.

„MASTER KEY" (CVE-2013-4787)

Ta luka, omówiona w naszym raporcie na temat zagrożeń mobilnych za czwarty kwartał 2013 r., została również odnaleziona w samym systemie operacyjnym Android i wynika ze sposobu, w jaki platforma obsługuje pakiety instalacyjne (APK). Są to zwykłe archiwa ZIP, które zawierają pewne pliki potrzebne do sprawdzenia integralności i pochodzenia archiwum. Proces instalacji oprogramowania używa dwóch oddzielnych implementacji do odczytu tych plików manifestu i zweryfikowania integralności archiwum, lecz niestety, niewielkie różnice w implementacji pozwalają napastnikowi przeszmuglować dowolne pliki i nadpisać oryginalne pliki w każdym pakiecie instalacyjnym. Dalsze prace doprowadziły do odkrycia kolejnych usterek w obsłudze archiwów ZIP w Androidzie, które umożliwiają znacznie bardziej wyrafinowane ataki. Pod koniec 2013 r. w niezależnych sklepach z aplikacjami znaleziono wiele złośliwych programów atakujących tę lukę.

PRYWATNOŚĆ W SIECI

Choć prywatność online od dawna jest ważną kwestią dla osób dbających o bezpieczeństwo, doniesienia o szpiegowskich działaniach NSA w 2013 r. wzbudziły obawy również wśród przeciętnych obywateli sieci. Internauci są bardziej świadomi ciekawskich oczu, które mogą śledzić ich poczynania w sieci, od kiedy do innych grup zainteresowanych inwigilacją użytkowników dołączyły rządy (ich własne lub obce). W tym artykule opiszemy kilka sposobów, które pozwalają gromadzić informacje o działaniach użytkownika w sieci albo jego dane osobiste.

ANALITYKA INTERNETOWA

W miarę, jak rośnie liczba użytkowników internetu, analityka internetowa — badanie ruchu w celu zwiększenia efektywności witryny — stała się nieodzownym narzędziem do studiowania zachowań użytkowników, zapewniającym wgląd w przepływ informacji między nimi a witryną. Aby przeprowadzić taką analizę, operatorzy witryn mogą po prostu zainstalować oprogramowanie open source, takie jak AWStats, aby gromadzić dane na temat odwiedzających. Są też usługi chmurowe oferowane przez różne firmy, które specjalizują się w analityce internetowej, co jest preferowaną opcją dla operatorów nastawionych komercyjnie.

Ogólnie rzecz biorąc, analityka internetowa polega na gromadzeniu i analizowaniu danych w celu stworzenia użytecznego „profilu" gościa witryny. Gromadzone informacje to na przykład typ przeglądarki, urządzenie użyte w celu uzyskania dostępu do witryny, rozdzielczość ekranu urządzenia, słowa kluczowe wpisane na pasku wyszukiwania, kliknięcia użytkownika w sklepie internetowym, czas przed przejściem na następną stronę itd. Komercyjne usługi analityczne próbują zautomatyzować pomiar i gromadzenie takich danych.

Ze względu na naturę gromadzonych danych analityka internetowa rodzi wiele pytań i wątpliwości, nie tylko wśród osób zawodowo zajmujących się bezpieczeństwem, ale również wśród internautów, którzy cenią prywatność. Mówiąc bardzo ogólnie, samego gromadzenia danych nie uważa się za naruszenie prywatności; wielu osobom nie podoba się jednak profilowanie wykonywane na podstawie zebranych informacji.

Najbardziej typowym i oczywistym komercyjnym zastosowaniem analityki internetowej jest reklama. Dystrybutorzy reklam zwykle próbują gromadzić informacje o gościach witryny, aby lepiej dobierać materiały reklamowe. Zebrane dane są używane w połączeniu ze śledzącymi plikami cookie (o których będzie mowa później), aby pomóc dystrybutorom reklam w zwiększeniu sprzedaży ich klientów (wydawców) poprzez kierowanie odpowiednich reklam do użytkowników, którzy, jak się zakłada, chcieliby je oglądać. Klienci dystrybutorów skorzystaliby na tym, że ich produkty lub usługi byłyby reklamowane mniejszym nakładem pracy (ponieważ metoda ta jest w dużej mierze zautomatyzowana) i z większą dokładnością wśród najbardziej odpowiednich użytkowników. Niektóre firmy badań marketingowych wykorzystują jawne usługi analityki internetowej, aby legalnie gromadzić ogromną ilość danych do profilowania.

Entuzjastycznymi użytkownikami analityki internetowej są też firmy zajmujące się marketingiem e-mail, które wykorzystują podobne techniki, co dystrybutorzy reklam, śledząc zachowania użytkowników w czasie czytania wiadomości.

COOKIES

Pliki cookie — plik tekstowe, które umożliwiają zapisywanie pewnych informacji z serwera na lokalnym komputerze użytkownika — to mechanizm przechowywania danych witryny, który jest najlepiej znany przeciętnemu internaucie. „Podstawowe" pliki cookie są nieodłączną częścią współczesnej sieci, ponieważ umożliwiają takie elementarne działania, jak zautomatyzowany dostęp do witryny albo „bezstanowe" żądania HTTP.

Istnieją jednak inne, bardziej zaawansowane pliki cookie, które wzbudzają więcej obaw u osób ceniących prywatność — przede wszystkim śledzące pliki cookie albo pliki cookie firm trzecich. Są one często używane do przechowywania historii przeglądania i mogą zostać zapisane na komputerze użytkownika przez kod JavaScript w witrynie albo przez nagłówek odpowiedzi HTTP. Śledzące pliki cookie mogą rejestrować historię aktywności użytkownika (odwiedzone strony, towary w koszyku sklepowym itd.). Choć są powszechnie używane w mniej lub bardziej uczciwych intencjach do dobierania wyświetlanych reklam, gromadzenie takich danych i możliwość wykorzystania ich do osobistego zidentyfikowania użytkownika niepokoi tych, którym zależy na prywatności.

Rysunek 1. Skrypt Google Analytics w popularnej witrynie plotkarskiej

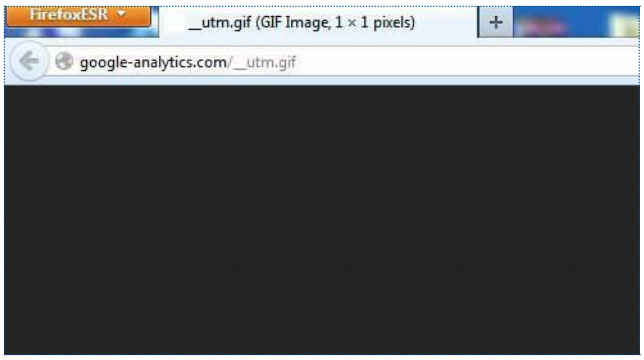
Alternatywą dla śledzących plików cookie są pliki cookie Flasha, znane też jako lokalne obiekty współdzielone (Local Shared Objects). Wprowadzono je dlatego, że wielu użytkowników blokuje pliki cookie albo usuwa je ze swoich przeglądarek. Taktyka ta nie działa w przypadku plików cookie Flasha, przez co są one popularne wśród internetowych reklamodawców. Z raportu opublikowanego w 2009 r.[4] i z kilku innych badań wynika, że pliki cookie Flasha regularnie pojawiają się w 100 najczęściej odwiedzanych witrynach. Inne badania mediów społecznościowych przeprowadzone w 2011 r. pokazują, że 31 na 100 witryn przynajmniej w jednym przypadku wykorzystywało pliki cookie HTTP i Flasha do tych samych celów[5].
Inny typ pliku cookie, znany jako Evercookie[6], został opracowany przez Samy'ego Kamkara pod kątem jak największej trwałości w przeglądarce. Jest tak agresywny, że techniki, które umożliwiają usunięcie innych typów plików cookie, nie wystarczają do zatarcia wszystkich śladów identyfikowalnych informacji. Ma wbudowany mechanizm obronny, który wykrywa każdą próbę usunięcia pliku, i odtwarza się w przypadku podjęcia takiej próby. Ze względu na agresywne działanie plików Evercookie są one również znane jako „super cookie" albo „zombie cookie"[7]. Tajne dokumenty NSA[8] sugerują też, że pliku Evercookie użyto do wyśledzenia użytkowników Tor kryjących się w anonimowej sieci.

ROLA SKRYPTÓW W GROMADZENIU DANYCH

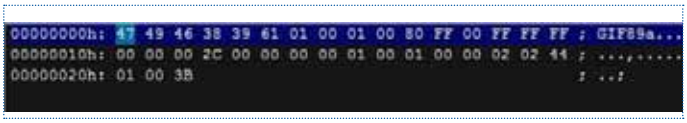
Od kiedy przeglądarki internetowe obsługują popularny język JavaScript, do gromadzenia danych powszechnie używa się również skryptów. Obiekty JavaScript działające po stronie klienta mogą dostarczać wielu informacji, takich jak rodzaj przeglądarki, ustawienia językowe przeglądarki, platforma itd. Zbiór informacji z tych i innych źródeł może posłużyć do wygenerowania „podpisu", który odróżnia jednego użytkownika od drugiego. W F-Secure Labs nasza usługa mierząca reputację sieci i witryn odnotowała „ślady" tej metody śledzenia w popularnych serwisach, zwłaszcza na blogach i w witrynach z wiadomościami, które mają ogromną liczbę dziennych odsłon.
Skrypt analityki internetowej oferowany przez Google jest jednym z narzędzi najczęściej używanych do takich celów. Usługa Google Web Analytics oferuje kod analityczny, który można łatwo skopiować i wkleić na własną stronę. Struktura tych kodów jest czysta i łatwo dostrzegalna. Na rysunku 1 pokazano przykład zaczerpnięty z popularnego celebryckiego blogu, perezhilton.com.

Oprócz skryptów większość współczesnych przeglądarek obsługuje język HTML, który umożliwia zgromadzenie jeszcze więcej informacji o urządzeniu klienckim. Na przykład funkcja geolokacji w HTML5 pozwala uzyskać szerokość i długość geograficzną użytkownika, aby wyświetlić jego pozycję na stronie internetowej. Ewentualne obiekcje użytkownika przed gromadzeniem takich informacji to już inna sprawa.

W HTML5 wprowadzono również funkcję Web Storage[2], która umożliwia zapisywanie (znacznie większej) ilości danych w systemie użytkownika, aby przyspieszyć korzystanie z sieci i zwiększyć stopień bezpieczeństwa. Poprzednio dane zapisywano



Rysunek 2: Plik obrazu o rozmiarach jednego piksela używany na



Rysunek 3: Zawartość pliku

w plikach cookie, co miało tę wadę, że informacje z tych plików mogły być wysyłane w żądaniach — ku niezadowoleniu osób ceniących prywatność — i prowadziło do praktyki usuwania plików cookie w celu zatarcia ewentualnych śladów. Na marginesie, dostawcy technologii internetowych dostrzegają ten słaby punkt współczesnego modelu sieci i tworzą produkty lub usługi, które łagodzą obawy o naruszenie prywatności. Dobrze znana wtyczka o nazwie NoScript[3] pozwala użytkownikom blokować wykonywanie kodu JavaScriptu, Flasha, Javy i innych podobnych programów na stronach internetowych. Wyłączenie kodu JavaScript ma jednak ten skutek, że choć pomaga chronić prywatność, to zakłóca funkcjonalność wielu witryn internetowych, a niektóre czyni całkowicie bezużytecznymi, więc użytkownicy muszą wybierać, czy chcą uzyskać dostęp do witryny, czy ryzykować swoją prywatność.

ROBAKI INTERNETOWE

Pominąwszy używanie (bądź nadużywanie) plików cookie i skryptów, witryny mogą gromadzić informacje o użytkowniku na inne sposoby. Tak zwane „podkładanie pluskwy" polega na umieszczeniu w witrynie specjalnego obiektu, który jest niewidoczny dla użytkowników. Pluskwy internetowe są znane pod wieloma nazwami — sygnalizator internetowy, pluskwa śledząca, tag lub tag strony[1] — ale wszystkie służą do tego samego celu.

Jedną z powszechnie stosowanych pluskiew jest ukrywanie na stronie internetowej pliku obrazu obok rzeczywistej treści przeznaczonej do wyświetlenia. Obraz jest bardzo mały (**rysunek 2**), najczęściej o szerokości i wysokości jednego piksela, a plik obrazu zwykle ma format GIF lub podobny (**rysunek 3**). Metoda ta bywa określana mianem piksela śledzącego, piksela 1x1 albo tagu pikselowego. Kiedy użytkownik odwiedza stronę zawierającą piksel śledzący, serwer może zidentyfikować go jako powracającego gościa.

ŚLEDZENIE ZA POMOCĄ CZCIONEK

Oprócz popularnych metod śledzenia badacze rozważają

stosowanie bardziej zaawansowanych technik. Jedna ze zbadanych metod śledzenia użytkowników wykorzystuje czcionki zainstalowane w komputerze użytkownika. Pomysł opiera się na tym, że różne systemy operacyjne, takie jak Windows i Mac OS, zawierają wstępnie zainstalowane, unikatowe zbiory czcionek, które można łatwo rozróżnić. Następnie badacze rozwinęli tę metodę i sklasyfikowali zbiory czcionek w poszczególnych systemach, aby identyfikować różne wersje systemu operacyjnego, architektury (32- lub 64-bitowe), a nawet pakiety oprogramowania biurowego. Wyniki badań sugerują, że metoda oparta na czcionkach pozwala odróżniać użytkowników bez bardziej aktywnego analizowania „odcisków palców"[9].

PRZYSZŁOŚĆ ŚLEDZENIA

Śledzenie odgrywa wielką rolę w reklamie i będzie ją nadal odgrywać w bliskiej przyszłości. Google, internetowy gigant, który jest również liderem branży reklamy online, bada nowe sposoby śledzenia użytkowników. Jeden z nich polega na zastąpieniu plików cookie anonimowym identyfikatorem, powiązanym z użytkownikami przeglądarki Chrome, który pełniłby podobną funkcję[10]. Z kolei Microsoft zapowiedział, że pracuje nad własną technologią śledzenia międzyplatformowego, która ma zastąpić wszędobylskie pliki cookie. Nowe rozwiązanie umożliwi śledzenie osób między komputerami stacjonarnymi, tabletami, smartfonami, konsolami do gier i innymi usługami[11]. Wydarzenia te prawdopodobnie zrodzą jeszcze więcej pytań o to, jak zagwarantować prywatność użytkownika w coraz bardziej eksponowanym środowisku.

Jakiej jednak ochrony prawnej mogą oczekiwać internauci, jeśli ich prywatność zostanie naruszona? Choć problem jest niezwykle skomplikowany, zwłaszcza w przypadku usług internetowych przeznaczonych dla publiczności międzynarodowej, warto przyjrzeć się sprawie z niedalekiej przeszłości. W grudniu 2007 r. Facebook uruchomił program o nazwie Beacon, w którym prywatne informacje użytkowników były automatycznie udostępniane publicznie bez ich zgody. Zostało to uznane za naruszenie prywatności i ostatecznie doprowadziło do pozwów przeciwko firmie. Program Beacon został następnie przerwany i założono fundusz w wysokości 9,5 mln dol. z myślą o zwiększeniu stopnia prywatności i bezpieczeństwa. Nie udzielono jednak żadnej rekompensaty użytkownikom Facebooka, na których program wpłynął negatywnie[12].

ŹRÓDŁA

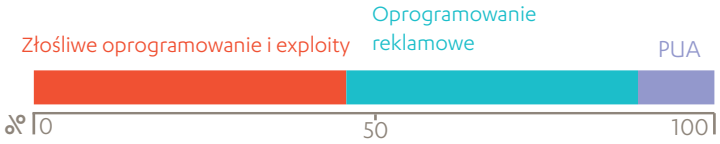
1. Wikipedia; *Web bug*; updated 26 December 2013; http://en.wikipedia.org/wiki/Web_bug
2. W3C; Ian Hickson; *Web Storage*; updated 30 July 2013; http://www.w3.org/TR/webstorage/
3. NoScript; http://noscript.net/
4. Wikipedia; *Internet Privacy*; updated 22 January 2014; http://en.wikipedia.org/wiki/Internet_privacy#cite_note-21
5. Wikipedia; *Internet Privacy*; updated 22 January 2014; http://en.wikipedia.org/wiki/Internet_privacy#cite_note-Heyman.2C_R._2011-22
6. Evercookie; Samy Kamkar; *Evercookie – Never Forget*; published 11 October 2010; http://samy.pl/evercookie/
7. Ensighten; *Super Cookies, Ever Cookies, Zombie Cookies, Oh My!*; http://www.ensighten.com/blog/super-cookies-ever-cookies-zombie-cookies-oh-my
8. Wikipedia; *Evercookie*; updated 18 December 2013; http://en.wikipedia.org/wiki/Evercookie
9. Károly Boda, Ádám Máté Földes, Gábor György Gulyás, Sándor Imre; *User Tracking on the Web via Cross-Browser Fingerprinting*; published 2011; http://pet-portal.eu/files/articles/2011/fingerprinting/cross-browser_fingerprinting.pdf
10. The New York Times; Claire Cain Miller; *Google Is Exploring an Alternative to Cookies for Ad Tracking*; published 19 September 2013; http://bits.blogs.nytimes.com/2013/09/19/google-is-exploring-an-alternative-to-cookies-for-ad-tracking/?_php=true&_type=blogs&_r=1
11. Ad Age; Tim Peterson; *Bye, Bye Cookie: Microsoft Plots Its Own Tracking Technology to Span Desktop, Mobile, Xbox*; published 9 October 2013; http://adage.com/article/digital/microsoft-cookie-replacement-span-desktop-mobile-xbox/244638
12. Wikipedia; *Lane v. Facebook, Inc.*; updated 4 October 2013; http://en.wikipedia.org/wiki/Lane_v._Facebook,_Inc.

PROFILOWANIE WEKTORÓW INFEKCJI

Przyjrzymy się teraz kanałom dystrybucji najczęściej używanym przez napastników w drugiej połowie 2013 r. i wyjaśnimy, dlaczego unikanie pornografii i Javy może być kluczem do bezpieczeństwa w sieci.

Większość użytkowników komputerów obecnie zakłada (bo powtarzano im to do znudzenia), że większość infekcji ma źródło w internecie — i oczywiście mają rację. Ale co to właściwie znaczy „większość" i jakie rodzaje witryn są za to odpowiedzialne?

100 NAJCZĘSTSZYCH DETEKCJI, PROCENTOWO WEDŁUG TYPU



Aby się dowiedzieć, stworzyliśmy listę 100 najczęstszych detekcji zgłaszanych do naszych systemów chmurowych podczas kilku tygodni drugiej połowy 2013 r., po czym sklasyfikowaliśmy każdą detekcję według zidentyfikowanego typu oprogramowania (powyżej). Następnie dla każdej detekcji zbadaliśmy znane wektory infekcji, czyli sposoby, w jaki szkodliwe programy trafiają do użytkowników, i otrzymaliśmy poniższy rozkład (na dole strony).

PRZEDE WSZYSTKIM SIEĆ WWW

Looking at the results, we see that malware unsurprisingly has the Przyglądając się wynikom, widzimy, że złośliwe oprogramowanie zajmuje pierwsze miejsce, z udziałem 47 proc. w 100 najczęstszych detekcjach. Oprogramowanie reklamowe nie zostaje daleko z tyłu i odpowiada za 42 proc. detekcji, podczas gdy potencjalnie

TYPOWE WEKTORY INFEKCJI

Poniżej znajduje się skrócona lista różnych kanałów, którymi złośliwe pliki trafiają do celu:

- Pliki i sieci

Oprogramowanie rozpowszechniane przez infekowanie plików albo w robakach rozprzestrzeniających się za pomocą sieci, nośników wymiennych itd.

- Łączenie oprogramowania

Oprogramowanie wstawione do instalatora innej (często bezpłatnej) aplikacji. Kategoria obejmuje również oprogramowanie pobierane z internetu podczas instalacji programu.

- P2P

Pliki dystrybuowane w sieciach peer-to-peer (P2P).

- Udostępnianie/dystrybucja oprogramowania

Oprogramowanie rozpowszechniane za pomocą witryn lub platform do udostępniania plików.

- Złośliwe reklamy

Reklamy używane do cichego pobierania oprogramowania albo do przekierowywania użytkownika do „jednorazowej" witryny.

- Exploity/infekcje przeglądarkowe

Złośliwe witryny wykorzystują lukę w zabezpieczeniach komputera użytkownika, aby po cichu zainstalować w nim oprogramowanie.

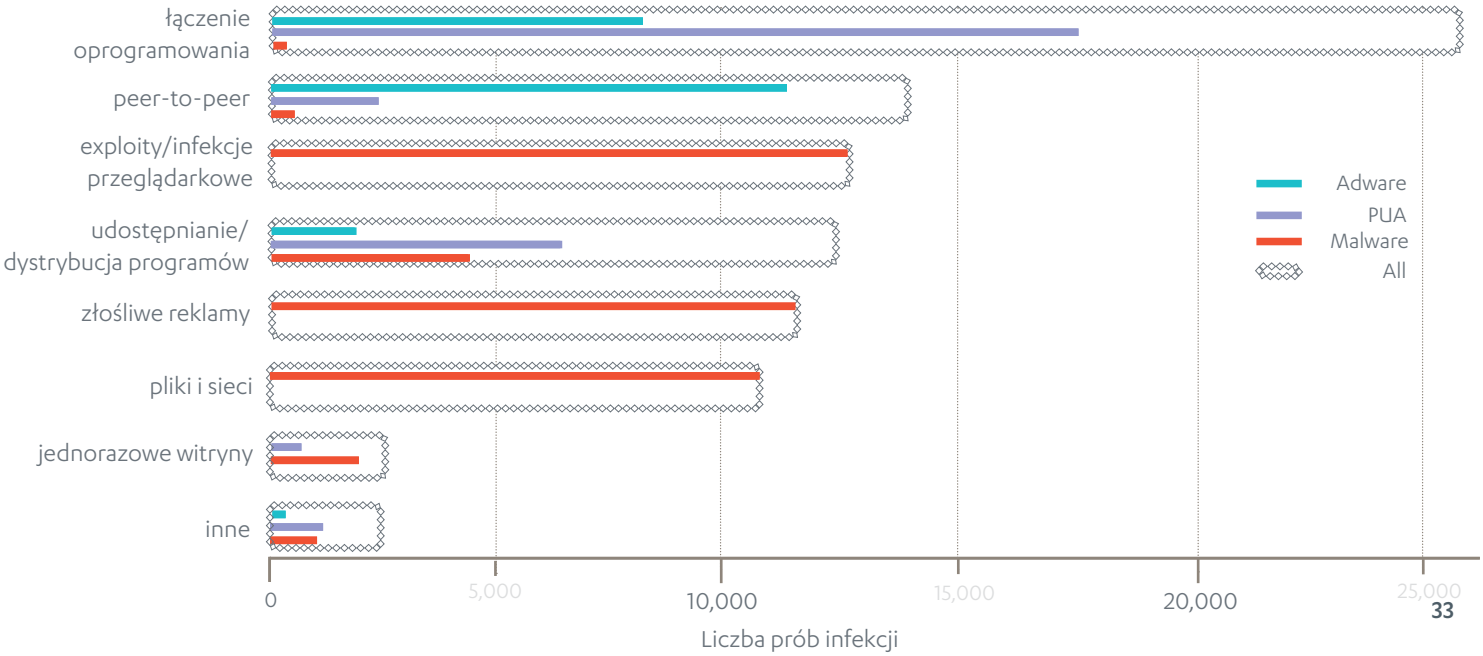
- Jednorazowe witryny

Witryny stworzone wyłącznie w celu dystrybucji złośliwego oprogramowania.

- Inne

Pliki rozpowszechniane w dowolny inny, niezdefiniowany tu sposób.

PODZIAŁ 100 NAJCZĘSTSZYCH DETEKCJI WEDŁUG WEKTORA INFEKCJI



niepożądane aplikacje (PUA) uplasowały się na ostatnim miejscu z udziałem 11 proc. Łączne dane wskazują, że zdecydowanie najczęstszym wektorem infekcji jest łączenie oprogramowania. Czy jednak rzeczywiście jest to najczęstszy sposób dostarczania złośliwego oprogramowania (które daje największe powody do obaw)? Podzieliliśmy oprogramowanie rozpowszechniane tą metodą według typu i uzyskaliśmy jaśniejszy obraz.

Okazuje się, że łączenie oprogramowania jest używane głównie do dystrybucji oprogramowania reklamowego i potencjalnie niepożądanych aplikacji. Rzeczywiście złośliwe pliki były rozpowszechniane za pomocą „metod przeglądarkowych", to znaczy poprzez exploity znajdujące się w witrynach internetowych, złośliwych reklamach, pakietach oprogramowania pobranych z serwisów do udostępniania plików, a wreszcie z witryn jednorazowych (które, w przeciwieństwie do legalnych witryn przejętych przez napastników, są tworzone do czysto złośliwych celów). Nawet jeśli nie dołączymy plików rozpowszechnianych w sieciach Peer-to-Peer (P2P), oprogramowanie rozpowszechniane za pośrednictwem sieci WWW stanowi 72 proc., czyli lwią część detekcji w naszej przykładowej setce. Zatem sieć WWW jest zdecydowanie największym źródłem złośliwych infekcji.
Potencjalnie niepożądane aplikacje wydają się opierać temu trendowi, ponieważ czołowym wektorem ich dostarczania są sieci P2P. Kiedy jednak przyjrzymy się bliżej naszym danym, okaże się, że jest to zasługą jednego, bardzo rozpowszechnionego programu Application:W32/BProtector (opisanemu bliżej w artykule poświęconym trojanowi Mevade). Gdybyśmy pominęli tę infekcję, sieć WWW byłaby źródłem 94 proc. detekcji na naszej liście.
Jak można było przewidzieć, dystrybucja oprogramowania reklamowego również opiera się na sieci WWW. 88 proc. pochodzi z pakietów oprogramowania, które można powiązać z serwisami udostępniania i dystrybucji plików oraz z witrynami jednorazowymi. Z tych liczb można wnioskować, że większość oprogramowania reklamowego pochodzi z witryn, które dodają je jako „bonus", kiedy użytkownicy pobierają inne, pożądane aplikacje.

POBIERAĆ CZY NIE?

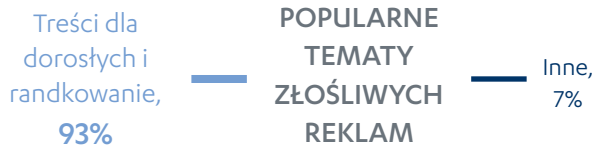
Ustaliliśmy zatem, że użytkownicy wchodzą w kontakt ze szkodliwymi programami głównie wtedy, kiedy surfują po sieci — ale w najbliższym czasie raczej nikt nie zamierza rezygnować z internetu. Jakie więc środki ostrożności może przedsięwziąć użytkownik, aby zamknąć złośliwemu oprogramowaniu drogę do swojego systemu?

W porównaniu ze złośliwym oprogramowaniem, unikanie oprogramowanie reklamowego i potencjalnie niepożądanych aplikacji jest łatwiejsze. Ich najczęstszym wektorem są pakiety oprogramowania rozpowszechniane w serwisach pobierania plików i sieciach P2P, na które dają się złapać użytkownicy szukający konkretnego narzędzia lub programu. W przeciwieństwie do bardziej agresywnych metod dystrybucji, które wymuszają instalację oprogramowania, witryny te pozwalają użytkownikowi zrezygnować z pobierania pliku, jeśli zauważy coś podejrzanego. W miarę, jak kolejni użytkownicy odkrywają, że konkretny plik jest niepożądany, ta metoda dystrybucji staje się coraz mniej efektywna.

CZY TO REKLAMA ZŁOŚLIWEGO OPROGRAMOWANIA?

Unikanie złośliwego oprogramowania w sieci wymaga jednak szczególnej ostrożności, ponieważ specjalnie projektuje się je tak, aby było trudne do zauważenia. Złośliwe reklamy to druga najczęstsza metoda dystrybucji złośliwego oprogramowania, która odpowiada za 37 proc. przeglądarkowych infekcji złośliwym oprogramowaniem, choć używa jej tylko 8 spośród 47 złośliwych programów na naszej liście.

Choć w ten sposób rozprzestrzeniają się tylko nieliczne rodziny złośliwego oprogramowania (na naszej liście były to Redirector, Salama i Browlock), potencjalne grono ofiar takiego wektora ataku jest ogromne. Dlatego sprofilowaliśmy adresy URL



używane przez powyższe rodziny, aby odkryć popularne tematy złośliwych reklam.

AJak się okazuje, większość złośliwych reklam ma związek z treściami dla dorosłych i randkowaniem. Jest to szczęśliwy zbieg okoliczności, bo choć nie dałoby się odfiltrować witryn poświęconych tematom ogólnym, takim jak stolarstwo czy dekarstwo, większość programów antywirusowych oferuje funkcję „kontroli rodzicielskiej", która odfiltrowuje konkretne typy treści, m.in. reklamy pornografii i serwisów randkowych. Korzystanie z tej funkcji pozwala uniknąć przynajmniej 93 proc. najpopularniejszych, złośliwych kampanii reklamowych.

EXPLOITY PRZEGLĄDARKOWE, INFEKCJE WITRYN I WITRYNY JEDNORAZOWE

Złośliwe oprogramowanie jest najczęściej dostarczane za pomocą exploitów przeglądarkowych, zainfekowanych witryn oraz witryn jednorazowych. W przeciwieństwie do złośliwych reklam, ten wektor nie jest ograniczony do konkretnych tematów lub typów witryn, które można by odfiltrować. Nie należy jednak tracić nadziei — choć

nie da się wyizolować niebezpiecznych tematów, to można wskazać najczęściej atakowane wtyczki do przeglądarek. Badając złośliwe oprogramowanie w naszym zbiorze próbek, ustaliliśmy, że 94 proc. exploitów było wymierzonych we wtyczkę deweloperskiej platformy Javy.

PODSUMOWANIE

W ostatecznym rozrachunku unikanie niepożądanego oprogramowania w sieci sprowadza się do trzech prostych rad, które bardzo łatwo zapamiętać:

- **Jeśli oprogramowanie wydaje się choćby odrobinę podejrzane, nie instaluj go, bez względu na to, skąd je wziąłeś.**
- **Unikaj witryn pornograficznych i randkowych — albo włącz kontrolę rodzicielską w swoim programie antywirusowym, aby odfiltrowywać te typy treści.**
- **Jeśli rzadko korzystasz z wtyczki Javy, odinstaluj ją z przeglądarki.**

Oczywiście, wskazówki te nie gwarantują stuprocentowego bezpieczeństwa — ale pozwalają się do niego zbliżyć..

ZŁOŚLIWE KOD NA MACA

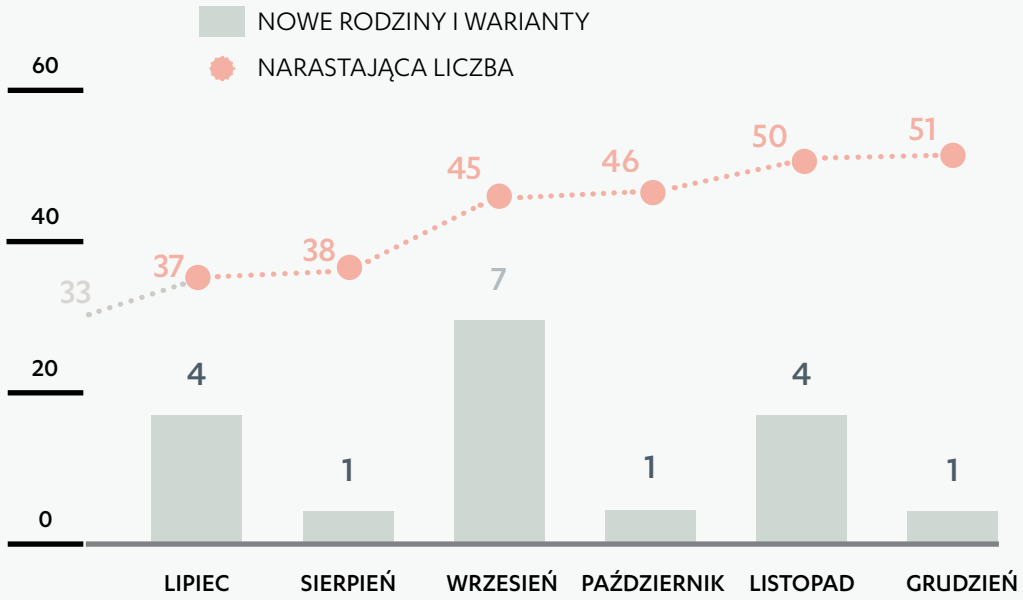
DRUGA POŁ. 2013 R.

ŁĄCZNA LICZBA (STYCZEŃ-GRUDZIEŃ 2013 r.)

51

rodzin i wariantów złośliwego oprogramowania na Maca

Sty - Cze	Lip - gru
33	18



BACKDOOR

83%

15/18

TROJAN

11%

2/18

POZOSTAŁE

6%

1/18

1/18 ROOTKIT

LIP

2/4 BACKDOOR

2/4 TROJAN

SIE

1/1 BACKDOOR

WRZ

7/7 BACKDOOR

PAŹ

1/1 BACKDOOR

LIS

3/4 BACKDOOR

1/4 OTHERS

GRU

1/1 BACKDOOR

Uwaga: pokazano liczbę wykrytych unikatowych wariantów.
Oznacza to, że przepakowane instalatory nie są liczone, a złośliwe programy złożone z wielu komponentów są liczone jako jeden.

ŹRÓDŁA

HAKERSTWO I SZPIEGOSTWO

NSA

1. Washington Post; Ellen Nakashima; *FISA court releases opinion upholding NSA phone program;* published 17 Sep, 2013
http://www.washingtonpost.com/world/national-security/fisa-court-releases-opinion-upholding-nsa-phone-program/2013/09/17/66660718-1fd3-11e3-b7d1-7153ad47b549_story.html

2. The Verge; Bryan Bishop; *NSA reportedly collecting millions of email address books and IM contact lists worldwide;* published 14 Oct 2013;
http://www.theverge.com/2013/10/14/4838966/nsa-reportedly-collecting-millions-of-email-address-books-and-im

3. AP for Yahoo! News; Deb Riechmann & Kimberly Dozier; *France joins list of allies angry over NSA spying;* published 21 Oct 2013;
http://news.yahoo.com/france-joins-list-allies-angry-over-nsa-spying-224519206.html

4. Arstechnica; Sean Gallagher; *How the NSA's MUSCULAR tapped Google's and Yahoo's private networks;* published 1 Nov 2013
http://arstechnica.com/information-technology/2013/10/how-the-nsas-muscular-tapped-googles-and-yahoos-private-networks/

5. PCWorld; Lucian Constantin; *NSA infected 50,000 networks with specialized malware;* published 25 Nov 2013
http://www.pcworld.com/article/2066840/nsa-reportedly-compromised-more-than-50000-networks-worldwide.html

6. Washington Post; Barton Gellman and Ashkan Soltani; *NSA tracking cellphone locations worldwide, Snowden documents show;* published 5 Dec 2013;
http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html

7. ZDNet; Larry Seltzer; *NSA using Google cookies, app location data to track targets;* published 11 Dec 2013;
http://www.zdnet.com/nsa-using-google-cookies-app-location-data-to-track-targets-7000024178

8. International Business Times; Eric Brown; *NSA Phone Spying Program Ruled Unconstitutional By Federal Judge;* published 16 Dec 2013:
http://www.ibtimes.com/nsa-phone-spying-program-ruled-unconstitutional-federal-judge-1510756

9. The Register; John Leyden; *Latest Snowden reveal: It was GCHQ that hacked Belgian telco giant;* published 20 Sep 2013;
http://www.theregister.co.uk/2013/09/20/gchq_belgacom_hack_link/

10. Arstechnica; Dan Goodin; *Password hack of vBulletin.com fuels fears of in-the-wild 0-day attacks;* published 18 Nov 2013;
http://arstechnica.com/security/2013/11/password-hack-of-vbulletin-com-fuels-fears-of-in-the-wild-0-day-attacks/

11. F-Secure Weblog; Sean Sullivan; Adobe Hacked; published 4 Oct 2013
http://www.f-secure.com/weblog/archives/00002617.html

12. Renesys Blog; Jim Cowie; *The New Threat: Targeted Internet Traffic Misdirection;* published 19 Nov 2013;
http://www.renesys.com/2013/11/mitm-internet-hijacking/

13. Krebs on Security; Brian Krebs; *Cupid Media Hack Exposed 42M Passwords;* published 20 Nov 13
http://krebsonsecurity.com/2013/11/cupid-media-hack-exposed-42m-passwords/

14. Arstechnica; Dan Goodin; *Bitcoin's skyrocketing value ushers in era of $1 million hacker heists;* published 27 Nov 2013;
http://arstechnica.com/security/2013/11/bitcoins-skyrocketing-value-ushers-in-era-of-1-million-hacker-heists/

15. Trustwave SpiderLabs Blog; Daniel Chechik; *Look What I Found: Moar Pony!;* published 3 Dec 2013;
http://blog.spiderlabs.com/2013/12/look-what-i-found-moar-pony.html

BEZPIECZEŃSTWO I ŚCIGANIE

1. The Wired; Kim Zetter; *Feds Identify the Young Russians Behind the Top U.S. Cyber Thefts in Last 7 Years;* published 25 Jul 2013
http://www.wired.com/threatlevel/2013/07/albert-gonzalez-conspirators/

2. Krebs on Security; Brian Krebs; *Pavel Vrublevsky Sentenced to 2.5 Years;* published 02 Aug 2013
http://krebsonsecurity.com/2013/08/pavel-vrublevsky-sentenced-to-2-5-years/

3. Forbes; Andy Greenberg; *End Of The Silk Road: FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market;* published 2 Oct 2013;
http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/

4. F-Secure Weblog; Karmina Aquino; *Blackhole, Supreme No More;* published 11 Oct 2013 http://www.f-secure.com/weblog/archives/00002622.html

5. InfoSecurity-Magazine; *Fidelity Investments Cyber-heist Suspects Arrested in California;* 16 NOV 13 http://www.infosecurity-magazine.com/view/35641/fidelity-investments-cyberheist-suspects-arrested-in-california/

6. The Register; Iain Thomson; *Stratfor email, credit-card hacker Hammond thrown in cooler for 10 YEARS;* published 15 Nov 2013; http://www.theregister.co.uk/2013/11/15/judge_throws_book_at_stratfor_hacker_with_decadelong_sentence/

7. Krebs on Security; Brian Krebs; *Spam-Friendly Registrar 'Dynamic Dolphin' Shuttered;* published 25 Nov 13 http://krebsonsecurity.com/2013/11/spam-friendly-registrar-dynamic-dolphin-shuttered/

8. The Register; John Leyden; *PayPal 13 plead guilty to launching DDoS attacks;* published 9 Dec 2013; http://www.theregister.co.uk/2013/12/09/paypal_13_guilty_pleas/

9. Krebs on Security; Brian Krebs; *Microsoft Patches Plug 23 Security Holes;* published 13 Aug 2013 http://krebsonsecurity.com/2013/08/microsoft-patches-plug-23-security-holes/

10. F-Secure Weblog; Sean Sullivan; *iOS 7 Security Prompts;* published 19 Sep 2013 http://www.f-secure.com/weblog/archives/00002610.html

11. Microsoft Security Research & Defense Blog; *CVE-2013-3906: a graphics vulnerability exploited through Word documents;* published 5 Nov 13 http://blogs.technet.com/b/srd/archive/2013/11/05/cve-2013-3906-a-graphics-vulnerability-exploited-through-word-documents.aspx

12. ZDNet; Larry Seltzer; *Adobe patches security issues in Flash and Shockwave players;* published 10 Dec 2013; http://www.zdnet.com/adobe-patches-security-issues-in-flash-and-shockwave-players-7000024150/

13. ZDNet; Larry Seltzer; *Microsoft patches 4 zero-day vulnerabilities in major Patch Tuesday event;* published 10 Dec 2013; http://www.zdnet.com/microsoft-patches-4-zero-day-vulnerabilities-in-major-patch-tuesday-event-7000024145/

14. F-Secure Weblog; Sean Sullivan; *EU Parliament Civil Liberties Committee on US Surveillance;* published 5 Sep 2013 http://www.f-secure.com/weblog/archives/00002603.html

15. The Wired; Kim Zetter; *RSA Tells Its Developer Customers: Stop Using NSA-Linked Algorithm*; published 19 Sep 2013; http://www.wired.com/threatlevel/2013/09/rsa-advisory-nsa-algorithm/

16. Los Angeles Times; Carol J. Williams; *Amid NSA spying, European lawmakers vote to tighten data protection;* published 21 Oct 2013; http://www.latimes.com/world/worldnow/la-fg-wn-europe-data-protection-nsa-spying-20131021,0,1164544.story

17. The Register; Iain Thomson; *Microsoft breaks bug-bounty virginity in $100,000 contest;* published 19 Jun 2013; http://technet.microsoft.com/en-US/security/dn425036

18. Washington Post; Craig Timberg, Barton Gellman and Ashkan Soltani; *Microsoft, suspecting NSA spying, to ramp up efforts to encrypt its Internet traffic;* published 27 Nov 2013; http://www.washingtonpost.com/business/technology/microsoft-suspecting-nsa-spying-to-ramp-up-efforts-to-encrypt-its-internet-traffic/2013/11/26/44236b48-56a9-11e3-8304-caf30787c0a9_story.html

19. Krebs on Security; Brian Krebs; *Facebook Warns Users After Adobe Breach;* published 11 Nov 2013; http://krebsonsecurity.com/2013/11/facebook-warns-users-after-adobe-breach/

20. The Guardian; Ian Traynor; *NSA surveillance: Europe threatens to freeze US data-sharing arrangements;* published 26 Nov 2013; http://www.theguardian.com/world/2013/nov/26/nsa-surveillance-europe-threatens-freeze-us-data-sharing

21. Naked Security Blog; Lee Munson; *Microsoft and partners fight back against the ZeroAccess botnet*; published 6 Dec 2013; http://nakedsecurity.sophos.com/2013/12/06/microsoft-and-partners-take-down-zeroaccess-botnet/

ZŁOŚLIWE OPROGRAMOWANIE I LUKI W ZABEZPIECZENIACH

1. F-Secure Weblog; Brod Aquilino; *Windows Version of the Janicab Malware;* published 23 July 2013 http://www.f-secure.com/weblog/archives/00002581.html

2. F-Secure Weblog; SecResponse; *Browlock Ransomware Targets New Countries;* published 14 Aug 2013 http://www.f-secure.com/weblog/archives/00002590.html

3. F-Secure Weblog; Sean Sullivan; *IE Vulnerability Update #Japan #Metasploit;* published 2 Oct 2013; http://www.f-secure.com/weblog/archives/00002615.html

4. The Register; Neil McAllister; *Malware culprit fingered in mysterious Tor traffic spike;* published 9 Sep 2013; http://www.theregister.co.uk/2013/09/09/malware_culprit_fingered_in_mysterious_tor_traffic_spike/

5. US-CERT; *CryptoLocker Ransomware Infections;* published 5 Nov 2013 http://www.us-cert.gov/ncas/alerts/TA13-309A

6. F-Secure Weblog; Sean Sullivan; *Microsoft Security Advisory (2896666) #APT;* published 6 Nov 2013 http://www.f-secure.com/weblog/archives/00002634.html

7. ZDNet; Michael Lee; *Google catches French govt spoofing its domain certificates;* published 9 Dec 2013; http://www.zdnet.com/google-catches-french-govt-spoofing-its-domain-certificates-7000024062/

8. F-Secure Weblog; SecResponse; *Sharking: High-Rollers in the Crosshairs;* published 10 Dec 2013 http://www.f-secure.com/weblog/archives/00002647.html

9. Naked Security Blog; Lee Munson; *Anatomy of another Android hole - Chinese researchers claim new code verification bypass;* published 17 July 2013; http://nakedsecurity.sophos.com/2013/12/06/microsoft-and-partners-take-down-zeroaccess-botnet/

10. F-Secure Mobile Threat Report Q3 2013; *Threat Highlights (p. 10)*; published 6 Nov 2013; http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf

11. F-Secure Mobile Threat Report Q3 2013; *Threat Highlights (p. 8);* published 6 Nov 2013; http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf

12. F-Secure Weblog; Mikko Hypponen; *FinFisher Range of Attack Tools;* published 30 Aug 2013; http://www.f-secure.com/weblog/archives/00002601.html

13. Bluebox Blog; *Black Hat Presentation on Android "Master Key";* published 16 Aug 2013; http://bluebox.com/corporate-blog/android-master-key-presentation/

14. F-Secure Mobile Threat Report Q3 2013; *Threat Highlights (p. 9);* published 6 Nov 2013; http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf

15. Forbes; *iPhone Fingerprint Scanner Hacked; Should You Care?;* Mark Rogowsky; published 22 Sep 2013; http://www.forbes.com/sites/markrogowsky/2013/09/22/iphone-fingerprint-scanner-hacked-should-you-care/

16. FireEye Blog; *Ad Vulna: A Vulnaggressive (Vulnerable & Aggressive) Adware Threatening Millions;* published 4 Oct 2013; http://www.fireeye.com/blog/technical/2013/10/ad-vulna-a-vulnaggressive-vulnerable-aggressive-adware-threatening-millions.html

Krótko o F-Secure

Krótko o F-Secure

F-Secure chroni cyfrowe życie konsumentów i przedsiębiorstw od ponad 20 lat. Nasze usługi internetowego bezpieczeństwa i chmurowego przechowywania treści są dostępne u ponad 200 operatorów z ponad 40 krajów na całym świecie oraz darzone zaufaniem w milionach domów i firm.

W 2013 r. firma odnotowała przychody w wysokości 155 mln euro i zatrudniała ponad 900 pracowników w 20 międzynarodowych biurach. F-Secure Corporation jest notowana na giełdzie NASDAQ OMX Helsinki Ltd. od 1999 r.

Chronimy to, co dla Ciebie ważne

Chronimy niezastąpione