RAPORT NA TEMAT ZAGROŻEŃ

PIERWSZA 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 każdego dnia. Przestępcy, którzy wykorzystują wirusy i złośliwe oprogramowanie do celów zarobkowych, nieustannie pracują nad nowymi sposobami ataku. Sytuacja wymaga ciągłej czujnośc, aby nasi klienci zawsze byli zawsze chronieni.

F-Secure Labs

W laboratoriach F-Secure w Helsinkach w Finlandii i w Kuala Lumpur w Malezji eksperci od bezpieczeństwa nieustannie pracują, aby zapewnić naszym klientom ochronę przed zagrożeniam i 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

W 2008 matematyk Satoshi Nakamoto (pseudonim) nadesłał artykuł techniczny na konferencję poświęconą kryptografii. Opisał w nim sieć typu peer-to-peer, w której uczestniczące systemy wykonują skomplikowane obliczenia matematyczne na tak zwanym „łańcuchu bloków". System miał na celu stworzenie zupełnie nowej waluty — kryptowaluty – opartej na matematyce. Artykuł był zatytułowany „Bitcoin: A Peer-to-Peer Electronic Cash System".

„Bitmonety" nie są związane z żadną istniejącą walutą, więc ich wartość zależy wyłącznie od tego, jak oceniają ją ludzie. Ponieważ zaś można wykorzystać je do przeprowadzania natychmiastowych globalnych transakcji, ich wartość jest zupełnie realna. Przekazywanie bitmonet przypomina wysyłanie wiadomości e-mail. Jeśli mam czyjś adres, mogę przesłać mu pieniądze — natychmiast i dokądkolwiek, z pominięciem kantorów, banków i urzędów podatkowych. W rzeczywistości kryptowaluty sprawiają, że banki przestają być potrzebne do przekazywania pieniędzy. Właśnie dlatego pomysł ten bardzo im się nie podoba.

Piękno algorytmu Bitcoin polega na rozwiązaniu dwóch głównych problemów kryptowalut poprzez ich połączenie — jak zatwierdzać transakcje i jak wprowadzać do systemu nowe jednostki waluty bez powodowania inflacji. Ponieważ w systemie nie ma banku centralnego, trzeba znaleźć jakiś sposób na zatwierdzanie transakcji, gdyż w przeciwnym razie ktoś mógłby produkować fałszywe pieniądze. W systemie Bitcoin zajmują się tym inni członkowie sieci peer-to-peer. Przynajmniej sześciu członków sieci musi zatwierdzić transakcję, zanim zostanie ona zrealizowana. Dlaczego jednak ktoś miałby zatwierdzać transakcje innych użytkowników? Ponieważ jest za to nagradzany: algorytm wydaje nowe bitmonety jako rekompensatę dla tych, którzy obsługują transakcje. Określa się to mianem „wydobywania" bitmonet.

Kiedy system Bitcoin był młody, wydobywanie było łatwe i można było bez problemu wygenerować dziesiątki bitmonet na komputerze domowym. Jednak w miarę, jak ich wartość rosła, wydobywanie stało się trudniejsze, ponieważ zwiększyła się liczba zainteresowanych tym osób. Choć kurs wymiany dolara na bitmonetę waha się, pozostaje faktem, że na początku 2013 r. jedna bitmoneta była warta 8 dolarów, a jesienią już 130 dolarów. Bitmonety mają zatem rzeczywistą wartość.

Dziś do wydobywania bitmonet i innych konkurencyjnych kryptowalut (takich jak Litecoin) wykorzystuje się duże sieci komputerowe. Podstawowa zasada jest prosta: kto ma szybkie komputery, może zarobić pieniądze. Niestety, komputery te nie muszą należeć do niego. Bywa więc, że zainfekowany komputer jakieś starszej pani z (dajmy na to) Filadelfii pracuje przez całą dobę ze stuprocentowym obciążeniem, wydobywając bitmonety na rzecz rosyjskiego cybergangu.
Jak opisano w niniejszym raporcie, drugi największy botnet na świecie już się tym zajmuje. Oceniamy, że jego operatorzy zarabiają ponad 50 000 dolarów dziennie poprzez generowanie bitmonet na zainfekowanych komputerach. Jeśli takie działania są podejmowane już dziś, łatwo domyśleć się, że botnety do wydobywania bitmonet będą bardzo popularne wśród cyberprzestępców w przyszłości.

MIKKO HYPPÖNEN
GŁÓWNY DYREKTOR DS. ZADAŃ, F-SECURE LABS
http://twitter.com/mikko

„PODSTAWOWA ZASADA WYDOBYWANIA KRYPTOWALUT JEST PROSTA: KTO MA SZYBKIE KOMPUTERY, MOŻE ZAROBIĆ PIENIĄDZE"

PODSUMOWANIE

Instalowanie poprawek zabezpieczeń można porównać do montowania zamków w oknach i drzwiach po usłyszeniu, że w mieście grasują włamywacze. Problem w tym, że włamywaczy jest wielu, a my mamy dużo okien i drzwi do zabezpieczenia i nie wiemy, które z nich jest narażone na atak. Łatamy jedną dziurę za drugą, a włamywacze wciąż próbują dostać się do środka. Brzmi to jak fabuła thrillera, ale alegoria nie jest naciągana, jeśli zważymy, jak istotne miejsce w naszym życiu zajmują dziś urządzenia komputerowe. Przestępcy ciągle szukają słabych punktów – dziur w murze, które można wykorzystać.

Ataki wymierzone w znane luki w zabezpieczeniach bardzo się rozpowszechniły, a najczęściej mamy do czynienia z takimi, które biorą na celownik Javę. W poprzednim półroczu exploity związane z Javą stanowiły mniej więcej jedną trzecią wykryć, jakie nasze klienckie programy zabezpieczające zgłosiły chmurowym systemom telemetrycznym; w tym półroczu była to już niemal połowa zgłoszonych wykryć. Exploity związane z Javą wykorzystywały głównie luki CVE-2013-1493 i CVE-2011-3544, podczas gdy atak wymierzony w lukę CVE-2011-3402 (usterka w obsłudze czcionek TrueType w systemie Windows) stanowił 10 proc. dziesięciu najczęstszych wykryć zgłoszonych w skali globalnej (4-procentowy wzrost w porównaniu z drugą połową 2012 r.). Przyjrzymy się również pakietom exploitów, które ułatwiają większość tych ataków, zwracając szczególną uwagę na Blackhole, SweetOrange i Cool.

Więcej informacji na stronie 36

Więcej informacji na stronie 34

Celem ataku opartego na exploicie jest zainstalowanie złośliwego oprogramowania – programów do wymuszania okupu, botów, trojanów bankowych albo backdoorów. W marcu i kwietniu tego roku w obiegu było oprogramowanie **wymuszające okup**, znane jako „Anti Child Porn Spam Protection". W tym samym okresie dość aktywny był również botnet ZeroAccess, choć statystyki zdają się wskazywać, że liczba infekcji trojanem ZeroAccess radykalnie spada. Prawdopodobnie jest to zasługą naszych detekcji Majava. Skutecznie zapobiegły one atakom, które w przeciwnym razie zakończyłyby się instalacją trojana ZeroAccess.

Więcej informacji na stronie 26

Niedawna zwyżka kursu wymiany bitcoinów skłoniła nas do oszacowania potencjalnych miesięcznych zysków, jakie botnet **ZeroAccess** czerpie z generowania tej waluty. Wyszła nam ogromna kwota.

Więcej informacji na stronie 30

Jedną z metod używanych w atakach typu **APT (Advanced Persistent Threat, zaawansowane uporczywe zagrożenia)** jest preparowanie dokumentów „przynęt" i wysyłanie ich do konkretnej osoby z pewnej organizacji lub branży. Analiza dokumentów APT wskazuje, że najczęściej poruszają one tematykę polityczną, korporacyjną lub wojskową.

Więcej informacji na stronie 23

Jeśli chodzi o **zagrożenia mobilne**, Android pozostaje najpopularniejszym celem. Niemal całe złośliwe oprogramowanie mobilne, które zaobserwowaliśmy w tym półroczu, operuje na tej platformie. Interesujące technicznie zagrożenia, które opisujemy w tym raporcie, to **Stels**, pierwszy złośliwy program do Androida dystrybuowany za pośrednictwem spamu, oraz bot, który używa Twittera do aktualizowana adresów swoich serwerów dowodzenia (command and control, C&C).

Więcej informacji na stronie18

Więcej informacji na stronie 14

Jeśli chodzi o komputery Mac, w pierwszej połowie 2013 r. napotkaliśmy interesujący złośliwy program o nazwie **Kumar in the Mac (KitM)**. Jest to pierwszy złośliwy program do Maca podpisany prawidłowym identyfikatorem dewelopera. Cóż za arogancja.

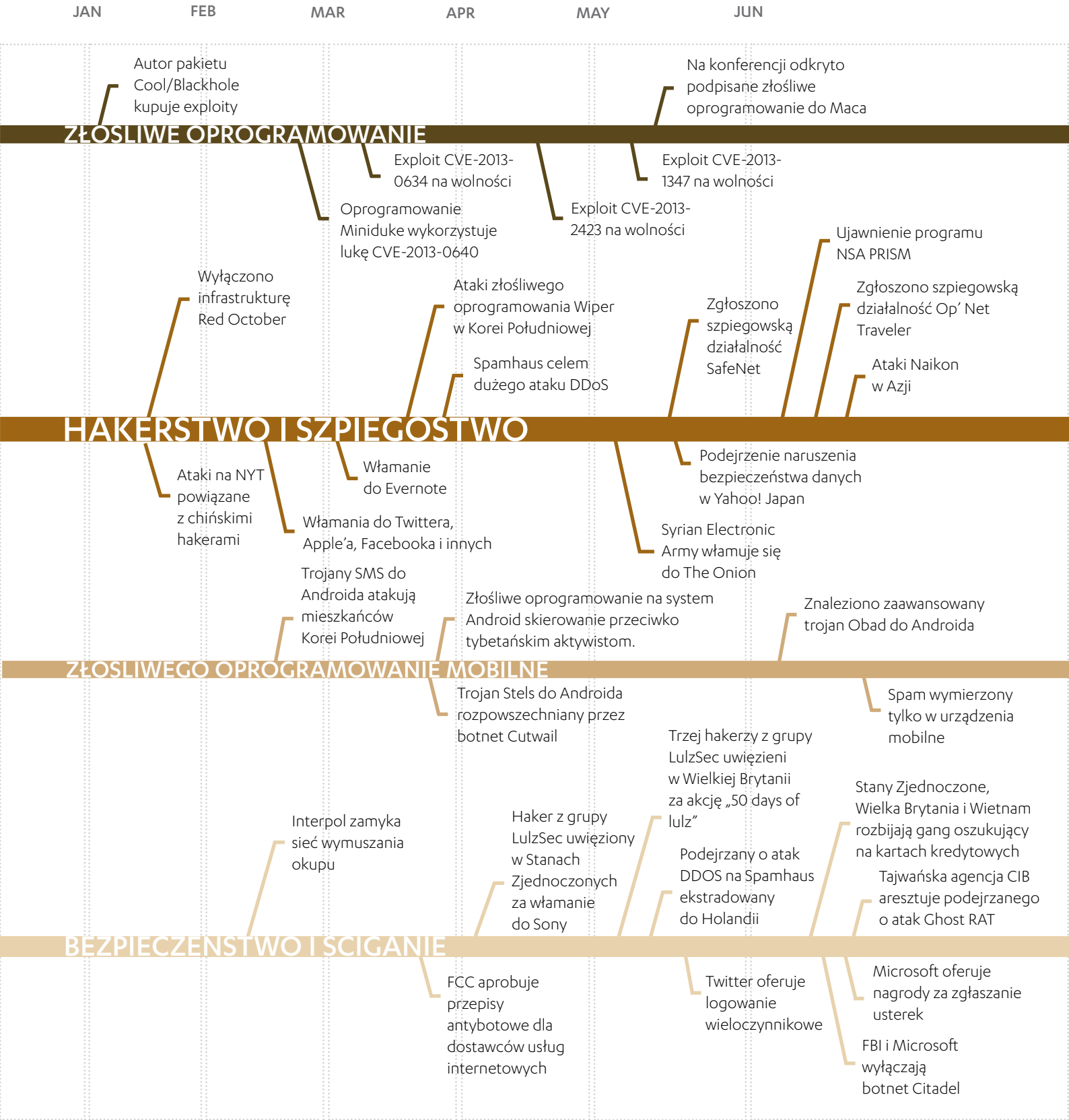
Więcej informacji na stronie 40

SPIS TREŚCI

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

WSPÓŁAUTORZY
BRODERICK AQUILINO
KARMINA AQUINO
CHRISTINE BEJERASCO
EDILBERTO CAJUCOM
SU GIM GOH
ALIA HILYATI
TIMO HIRVONEN
MIKKO HYPPONEN
SARAH JAMALUDIN
KAMIL LEONIAK
CHIN YICK LOW
JARNO NIEMELA
ZIMRY ONG
MIKKO SUOMINEN
SEAN SULLIVAN
ANTTI TIKKANEN

KALENDARZ INCYDENTÓW



Źródła: zob. strony 47-48

PRZEGLĄD

W pierwszej połowie 2013 r. obserwowaliśmy głównie dalszy rozwój znanych zagrożeń, o których pisaliśmy w poprzednich raportach. W tym półroczu szczególnie godne uwagi były: rosnąca liczba ataków opartych na exploitach, zwłaszcza wymierzonych w platformę Java; wydobywanie bitmonet i jego konsekwencje; rosnące wyrafinowanie zagrożeń mobilnych; wykrycie pierwszego podpisanego złośliwego programu do Maca; oraz profilowanie witryn wyłudzających informacje. Pomijając kwestie techniczne, w okresie tym było głośno o cyberszpiegostwie, hakerstwie i naruszeniach prywatności, ponieważ duże witryny informacyjne i firmy technologiczne raportowały liczne próby infiltracji, a ujawnienie programu gromadzenia danych realizowanego przez Agencję Bezpieczeństwa Narodowego Stanów Zjednoczonych (NSA) zrodziło obawy o prywatność w sieci.

Jak wynika ze statystyk zebranych przez nasze chmurowe systemy telemetryczne, które monitorują detekcje u klientów chronionych przez nasze produkty, większość spośród 10 najczęstszych detekcji w ciągu minionych sześciu miesięcy (zob. strona 9) była związana z exploitami. Jeśli chodzi o rozkład geograficzny, najwięcej ataków opartych na exploitach miało miejsce w Stanach Zjednoczonych i Francji. Niemal 60 proc. spośród 10 najczęstszych detekcji stanowiły ataki używające exploitów, a 80 proc. spośród nich było wymierzone w platformę Java. Statystyki te dowodzą, że napastnicy w coraz większym stopniu skupiają się na łamaniu zabezpieczeń Javy w celu uzyskania dostępu do komputerów użytkowników. Ponieważ Java jest niezwykle popularną aplikacją, można ją znaleźć w niemal każdej organizacji zajmującej się tworzeniem oprogramowania, a jeszcze lepszą ilustracją wszechobecności platformy i jej roli jako punktu wejścia dla napastników jest duży lutowy atak wykorzystujący lukę w zabezpieczeniach Javy, którego ofiarą padło wiele firm technologicznych, w tym Twitter i Facebook[1].

Więcej informacji na stronie 11

Niemal połowa ataków opartych na exploitach, które zgłosili nasi klienci, została zablokowana przez heurystyczne detekcje Majava, które zapobiegły infiltracji systemów i instalacji złośliwego oprogramowania. Co ciekawe, skuteczność mechanizmu Majava miała kuriozalny wpływ na statystyki detekcji ZeroAccess raportowane przez naszych klientów, które w porównaniu ze statystykami dla tego samego złośliwego oprogramowania z drugiej połowy 2012 r. uległy znacznemu obniżeniu. Jednak bardzo aktywny rozwój rodziny ZeroAccess, który obserwowaliśmy w ciągu minionych sześciu miesięcy, pozwala przypuszczać, że gdyby ataki oparte na exploitach były udane, większość zainstalowanego przez nie złośliwego oprogramowania byłaby związana z botnetem ZeroAccess. Zgłoszone detekcje ZeroAccess miały miejsce głównie w Stanach Zjednoczonych, Francji, Szwecji i Włoszech.

Większość zaobserwowanych ataków opartych na exploitach przeprowadzono za pomocą niewielkiej liczby pakietów. Za 70 proc. ataków odpowiadało pięć pakietów: **BlackHole, SweetOrange, Crimeboss, Styx i Cool.** W ciągu ostatnich kilku miesięcy obserwowaliśmy wzmożoną aktywność na polu tworzenia pakietów exploitów — każdego miesiąca powstawał (lub był gruntownie modernizowany) przynajmniej jeden pakiet. Pięć czołowych pakietów również aktywnie się rozwija, a ich autorzy nieustannie dodają nowe exploity wymierzone w niedawno ogłoszone luki w zabezpieczeniach.

Więcej informacji na stronie 34

Również starsze usterki, dla których wydano już poprawki, nadal przysparzają problemów użytkownikom. Niemal pięć lat po epidemii robaka **Downadup/Conficker** znaleźliśmy jego ślady w Brazylii. Choć nasza detekcja exploitów wymierzonych w lukę CVE-2011-3402 powstała w 2011 r., po upływie dwóch lat liczba klientów zgłaszających ten typ ataku wcale nie spadła. W rzeczywistości wzrosła z 6 proc. wszystkich zgłoszonych detekcji w drugiej połowie 2012 r. do 10 proc. w bieżącym okresie (głównie we Francji, Niemczech i Szwecji). Ciągłe wykrywanie zagrożeń, które zostały odkryte i zneutralizowane lata temu, stawia pod znakiem zapytania skuteczność procedur aktualizacji oprogramowania, które często pozostawiają użytkowników na łasce ataków wymierzonych w stare, dobrze znane luki w zabezpieczeniach.

Więcej informacji na stronie 36

Downadup/Conficker
Robak, który rozprzestrzenia się, wykorzystując luki w zabezpieczeniach usług sieciowych w różnych wersjach Windows

CVE-2011-3402
Luka w zabezpieczeniach parsera czcionek TrueType w systemie Windows, o której po raz pierwszy zrobiło się głośno, kiedy została wykorzystana przez złośliwe oprogramowanie Duqu w listopadzie 2011 r.

Inną działalnością, która ma się dobrze pomimo korzystania ze znanych trików, jest wyłudzanie informacji. Dzięki pakietom, które upraszczają budowanie witryn wyłudzających informacje, naciągacze mają jeszcze łatwiejsze zadanie. Zwykle używają spamu, aby zwabić ofiary do automatycznie tworzonych witryn, a następnie kradną ich dane osobowe albo pieniądze. Kiedy profilowaliśmy znane witryny wyłudzające informacje, odkryliśmy, że najpopularniejszy typ tych portali naśladuje usługi płatnicze, banki i serwisy z grami, a 73 proc. z nich to fałszywe witryny PayPal.

Więcej informacji na stronie 44

Oprogramowanie wymuszające okup nadal pozostaje w obiegu, a w marcu i kwietniu tego roku zaobserwowaliśmy przypadki ataków wymierzonych specjalnie w klientów korporacyjnych w krajach takich jak Hiszpania i Włochy. Niemal wszystkie przypadki, na jakie natrafiliśmy w tym półroczu, należały do dwóch szerokich kategorii: szyfrowania danych oraz rzekomych komunikatów policyjnych, przy czym częstszy był ten drugi typ.

Więcej informacji na stronie 26

Jak Mikko wspomniał w przedmowie, wydobywanie walut **Bitcoin** i Litecoin jest jedną z bardziej zyskownych opcji dla cybreprzestępców. Interesujący charakter mają związki między oprogramowaniem ZeroAccess a bitmonetami. Choć to złośliwe oprogramowanie początkowo zawierało moduł do wydobywania bitmonet, usunięto go z próbek, które znaleźliśmy we wrześniu ubiegłego roku. W kwietniu tego roku moduł został przywrócony, akurat wtedy, gdy pieniężna wartość bitmonet przekroczyła 200 dolarów[2]. Jednak pod koniec kwietnia znów zrezygnowano z funkcji generowania bitmonet. Sprawa jest dość tajemnicza, choć niektórzy spekulują, że powodem jest wysoki koszt utrzymywania prywatnej puli serwerów oraz duża moc obliczeniowa potrzebna do wydobywania bitoment, co utrudnia ukrywanie złośliwego oprogramowania na zainfekowanych komputerach. Spróbowaliśmy oszacować* potencjalne miesięczne zyski z wydobywania bitmonet i doszliśmy do wniosku, że jest to kwota rzędu 1,8 mln dolarów.

Więcej informacji na stronie 30

* na podstawie ostrożnego założenia, że 5 proc. ofiar ma systemy o mocy obliczeniowej wystarczającej do wydobywania bitoment

Na froncie Maca interesujące były lutowe ataki, ponieważ próbowały dosięgnąć użytkowników tej platformy, zwłaszcza pracowników firmy Apple, za pośrednictwem przechwyconej witryny dewelopera aplikacji mobilnych[1]. Choć ataki na użytkowników Maca nie są niczym nowym, dotychczas były wymierzone głównie w działaczy politycznych – co potwierdza przypadek znalezienia **podpisanego oprogramowania szpiegowskiego** na Macu aktywisty, który brał udział w majowej konferencji Oslo Freedom Forum. Może nie jest więc przypadkiem, że spośród 33 nowych rodzin lub wariantów złośliwego oprogramowania do Maca, które zaobserwowaliśmy w pierwszej połowie 2013 r., 57,6 proc. stanowiły backdoory.

Więcej informacji na stronie 40

Biorąc pod uwagę zasięg i skalę lutowych ataków oraz spekulacje na temat ich zamierzonego celu, można uznać je za **„zaawansowane uporczywe zagrożenia" (APT)**. Jednakże w atakach APT częściej wykorzystuje się dokumenty-przynęty, specjalnie spreparowane tak, aby zainteresowały użytkowników docelowej organizacji. Ze względu na naturę tych plików większość potencjalnych ofiar nie chce dzielić się nimi z nikim z zewnątrz. Analiza dokumentów, które zdołaliśmy pozyskać, pozwala wyciągnąć ogólne wnioski na temat ich zawartości. Na przykład najczęściej odnoszą się do tematów politycznych (65 proc.), korporacyjnych (14 proc.) i wojskowych (14 proc.), a najczęściej używane języki to angielski, chiński i arabski. Analiza ta umożliwiła nam naszkicowanie przybliżonego profilu osoby, którą dokumenty te starają się zwabić.

Advanced Persistent Threat
Potajemna, wyrafinowana i ukierunkowana infiltracja wybranej organizacji, często z myślą o długofalowym celu.

Więcej informacji na stronie 23

Na scenie **zagrożeń mobilnych** najczęściej atakowanym systemem pozostaje Google Android, który odpowiada za 96 proc. nowych rodzin lub wariantów złośliwego oprogramowania, jakie odkryliśmy w pierwszej połowie 2013 r. Ponadto w tym półroczu sklep Google Play Store prześcignął Apple App Store i stał się największym serwisem z aplikacjami, przekraczając w lipcu próg miliona aplikacji. Pomimo wątpliwości co do bezpieczeństwa Play Store pozostaje on zdecydowanie najbezpieczniejszym sklepem z aplikacjami do Androida, ponieważ większość nowego złośliwego oprogramowania do Androida odkryliśmy w witrynach innych niż Play Store. Jeśli chodzi o funkcjonalność, większość zaobserwowanych przez nas zagrożeń mobilnych należało do kategorii trojanów bankowych albo złośliwych reklam. Trojany bankowe, które zwykle wykradają mobilne kody autoryzacji transakcji (Mobile Transaction Authentication Number, mTAN), występują coraz częściej, ponieważ coraz więcej banków przechodzi na tę metodę weryfikowania transakcji online. W ciągu ostatnich kilku miesięcy odnotowaliśmy też wzrost liczby złośliwych reklam — reklam prowadzących do witryn, które rozpowszechniają złośliwe oprogramowanie mobilne — zarówno w samych aplikacjach, jak i w witrynach odwiedzanych podczas mobilnych sesji przeglądania sieci. Wreszcie spośród wszystkich zagrożeń mobilnych, które zaobserwowaliśmy w tym półroczu, szczególnie godny uwagi jest Stels — pierwszy (choć zapewne nie ostatni) złośliwy program do Androida który jest rozpowszechniany przez botnet Cutwail w spamie naśladującym wiadomości od amerykańskiego urzędu podatkowego (Internal Revenue Service, IRS).

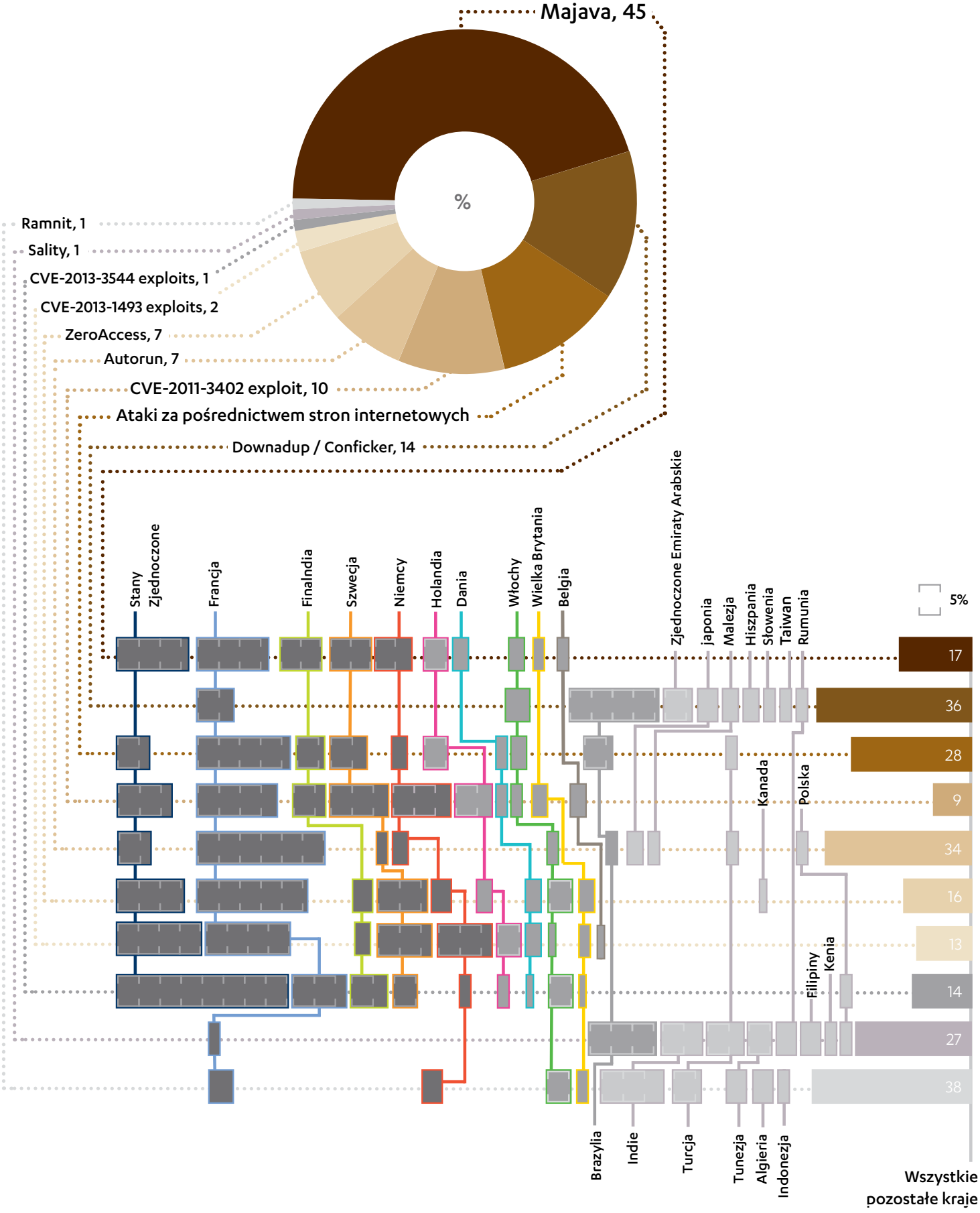
Więcej informacji na stronie 18

Więcej informacji na stronie 14

ŹRÓDŁA

1. Weblog F-Secure; Sean Sullivan; Timeline: Hacks Related to Apple; opublikowano 20 lutego 2013 r.: http://www.f-secure.com/weblog/archives/00002507.html
2. Kurs wymiany Bitcoin; http://bitcoincharts.com/charts/mtgoxUSD
3. Weblog F-Secure; Sean Sullivan; Mac Spyware Found at Oslo Freedom Forum; opublikowano 16 maja 2013 r.; http://www.f-secure.com/weblog/archives/00002554.html

10 NAJCZĘSTSZYCH DETEKCJI I 10 NAJCZĘŚCIEJ ATAKOWANYCH PRZEZ NIE KRAJÓW W PIERWSZEJ POŁOWIE 2013 ROKU, PROCENTOWO



GODNE UWAGI

WODOPOJE

Jeśli chodzi o bezpieczeństwo informacji, najbardziej godnym uwagi wydarzeniem z początku 2013 r. było bez wątpienia włamanie do kilku internetowych gigantów (Twitter, Facebook, Apple, Microsoft) oraz wielu innych firm z Doliny Krzemowej poprzez „wodopój" w deweloperskim pakiecie SDK do iPhone'a [6,7].

Był to istotny incydent, z którego jednak przeciętny użytkownik nie dowiedział się wiele na temat ataków u wodopoju, prawdopodobnie dlatego, że zaatakowane firmy nie dzielą się ważnymi szczegółami.

Co się zatem wydarzyło?

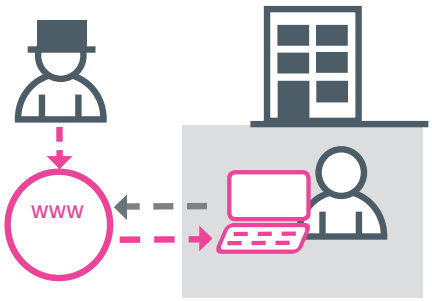
Historia zaczęła się 1 lutego od posta na blogu Boba Lorda, dyrektora ds. bezpieczeństwa informacji w Twitterze, pod tytułem: *Keeping our users secure* [2].

„...napastnicy mogli uzyskać dostęp do ograniczonych informacji — nazw, adresów e-mail, tokenów sesji oraz zaszyfrowanych wersji haseł — o około 250 tysiącach użytkowników."

Lord podał, że hasła i tokeny są resetowane — normalna procedura w przypadku włamania. Ale na końcu posta poradził, żeby „użytkownicy wyłączyli obsługę Javy w swoich przeglądarkach", i stwierdził, że atak nie jest dziełem „amatorów".

Definicja: atak u wodopoju [1]

Napastnik chce zaatakować konkretną grupę (organizację, branżę lub region). Atak składa się z trzech faz:



1. ***Odgadnąć, jakich witryn internetowych często używa dana grupa.***
2. ***Zainfekować jedną lub wiele takich witryn złośliwym oprogramowaniem.***
3. ***Ostatecznie niektórzy członkowie danej grupy zostaną zainfekowani***

Wykorzystanie witryn, którym grupa ufa, sprawia, że strategia ta jest skuteczna nawet w przypadku grup odpornych na ukierunkowane wyłudzanie informacji i inne formy phishingu.

Post Lorda sugerował, że przyczyną włamania była luka w zabezpieczeniach Javy w przeglądarce. Wiedząc, że wśród pracowników Twittera jest wielu użytkowników Maca, poprosiliśmy firmę Apple o próbki użyte do ataku i usłyszeliśmy, że „Twitter nie udostępnił żadnych próbek".

A potem...

Ciąg dalszy nastąpił 15 lutego, kiedy Facebook opublikował na blogu wpis zatytułowany: *Protecting People On Facebook* [3].

"...dział bezpieczeństwa Facebooka odkrył, że nasze systemy były celem wyrafinowanego ataku. Atak nastąpił, kiedy kilku pracowników odwiedziło witrynę dewelopera aplikacji mobilnych, która została przejęta przez napastników."

Atak przeprowadzono za pomocą exploita dnia zerowego za pośrednictwem witryny dewelopera aplikacji mobilnych — jak się później okazało, winny był pakiet iPhone Dev SDK. Dyrektor ds. bezpieczeństwa Facebook, Joe Sullivan, stwierdził w wywiadzie udzielonym Ars Technica, że atak dotknął również kilka innych firm.

W dniu, w którym pojawił się post na blogu Facebooka, Apple udostępniło kod backdoora (bez kontekstu) na liście mailingowej badaczy antywirusowych. Nam jednak kontekst wydał się jasny, więc zaczęliśmy szukać potwierdzenia, że backdoor miał związek z włamaniem do Facebooka.

19 lutego Reuters podał [4], że samo Apple padło ofiarą ataku, a 22 lutego na blogu Microsoftu pojawił się post zatytułowany: Recent Cyberattacks [5].

Przestępcy — ale nie oprogramowanie przestępcze

Kluczowa lekcja z tych wszystkich włamań jest taka: grupa przestępców zdołała włamać się do licznych internetowych firm za pośrednictwem wodopoju. Atak był ukierunkowany i wymagał ludzkiej pracy — nie użyto zautomatyzowanego oprogramowania przestępczego.

Nic dziwnego. W przypadku tak cennych celów, jak Twitter, Facebook, Apple i Microsoft napastnicy najwyraźniej byli skłonni poświęcić swój czas.

Czego się nauczyliśmy?

W tym momencie, kiedy dowiemy się o włamaniu do witryny, powinniśmy zadać sobie pytanie — czy było to zwykłe naruszenie bezpieczeństwa danych? Czy może witryna byłaby dobrym wodopojem? Nie wydaje się jednak, żeby interesowało to szerokie masy użytkowników.

Tak przynajmniej wynika z niedawnych doniesień o włamaniu na forum społeczności NASDAQ[8] – choć z drugiej strony... rzecz miała miejsce latem. Może w historii tej kryje się coś więcej.

Czas niemal na pewno pokaże.

ŹRÓDŁA

1. Wikipedia; *Watering Hole;* ostatnio zmodyfikowano 17 września 2013 r.; http://en.wikipedia.org/wiki/Watering_Hole
2. Twitter, Bob Lord; *Keeping our users secure*; opublikowano 1 lutego 2013 r.; https://blog.twitter.com/2013/keeping-our-users-secure
3. Facebook; *Protecting People On Facebook; opublikowano 15 lutego 2013 r.;* https://www.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766
4. Reuters; Jim Finkle i Joseph Menn; *Exclusive: Apple, Macs hit by hackers who targeted Facebook*; opublikowano 19 lutego 2013 r.; http://www.reuters.com/article/2013/02/19/us-apple-hackers-idUSBRE91I10920130219
5. Microsoft; *Recent Cyberattacks*; opublikowano 22 lutego 2013 r.; http://blogs.technet.com/b/msrc/archive/2013/02/22/recent-cyberattacks.aspx
6. NYTimes; Nicole Perlroth; Apple Computers Hit by Sophisticated Cyberattack; opublikowano 19 lutego 2013 r.; bits.blogs.nytimes.com/2013/02/19/apple-computers-hit-by-sophisticated-cyberattack/
7. F-Secure Weblog; Sean Sullivan; *Timeline: Hacks Related to Apple;* opublikowano 20 lutego 2013 r.; http://www.f-secure.com/weblog/archives/00002507.html
8. F-Secure Weblog; Sean Sullivan; *NASDAQ's Community Forum*; opublikowano 23 sierpnia 2013 r.; http://www.f-secure.com/weblog/archives/00002595.html

STUDIA PRZYPADKÓW

STELS

Stels to trojan na Androida, który pełni wiele funkcji — może zmienić zainfekowane urządzenie w bota, który stanie się częścią większego botnetu, albo działać jako trojan bankowy, który wykrada kody mTAN. Stels zadebiutował w listopadzie 2012 r., a od tego czasu w sieci odkryto kilka różnych wariantów trojana.

Firma F-Secure zidentyfikowała ponad 1300 unikatowych próbek Stelsa, które można podzielić na trzy główne warianty. Próbki każdego wariantu zaobserwowano po raz pierwszy 15 listopada, 28 listopada i 9 grudnia. Warianty zidentyfikowano na podstawie nazwy pakietu użytej w pierwotnym kodzie źródłowym: ru.beta, ru.stels2 i ru.stels4. Wewnętrzne numery wersji znalezione w kodzie i plikach konfiguracyjnych potwierdzają, że wariant ru.beta rzeczywiście jest pierwszą wersją, a ru.stels2 drugą. Nowsze wersje Stelsa prawdopodobnie nie zastępują starych, ponieważ wszystkie trzy warianty napotkano jednocześnie.

TABELA 1. POLECENIA TYLNYCH DRZWI W PIERWSZEJ WERSJI STELSA

POLECENIE	FUNKCJA
botId	Zmienia identyfikator bota
catchSms	Określa, jakie przychodzące wiadomości SMS będą przechwytywane (na podstawie źródłowego numeru telefonu i treści wiadomości)
deleteSms	Określa, jakie przychodzące wiadomości SMS będą usuwane (na podstawie źródłowego numeru telefonu i treści wiadomości)
httpRequest	Wykonuje żądanie HTTP
makeCall	Nawiązuje połączenie telefoniczne
notification	Pokazuje powiadomienie na pasku stanu
openUrl	Otwiera adres URL w przeglądarce internetowej
removeAllCatch-Filters	Zaprzestaje przechwytywania przychodzących wiadomości SMS
removeAllSmsFil-ters	Zaprzestaje usuwania przychodzących wiadomości SMS
sendContactList	Pobiera listę kontaktów z książki telefonic-znej i wysyła ją do serwera dowodzenia
sendPackageList	Pobiera z telefonu listę zainstalowanych aplikacji i wysyła ją do serwera dowodzenia
sendSMS	Wysyła wiadomość SMS
sendSMSLog	Pobiera wiadomości SMS z folderów skrzynki odbiorczej i wiadomości wysłanych, a następnie wysyła je do serwera dowodzenia
server	Zmienia adres serwera dowodzenia
subPref	Zmienia sufiks dodawany do wiadomości SMS wysyłanych przez trojana
twitter	Aktualizuje nazwę konta na Twitterze używanego do dystrybuowania informacji o nowych serwerach dowodzenia
update	Pobiera i instaluje aplikację
uninstall	Odinstalowuje aplikację
wait	Czeka przez określony czas przed ponownym kontaktem z serwerem w celu odebrania nowych poleceń

Główne funkcje

Trzy warianty Stelsa wykonują te same podstawowe funkcje po otrzymaniu poleceń od serwera dowodzenia (C&C). Polecenia są przekazywane przez połączenie HTTP i dostarczane w postaci zaszyfrowanych plików JavaScript Object Notification (JSON), które później są deszyfrowane i analizowane przez trojana. Różne polecenia zapewniają posiadaczowi bota różne metody czerpania zysków, na przykład poprzez wysyłanie wiadomości SMS na numery premium oraz wykradanie informacji o urządzeniu. Funkcja przechwytywania przychodzących wiadomości SMS pozwala na wykradanie kodów mTAN, które banki wysyłają swoim klientom, a zatem na ominięcie dwuczynnikowego uwierzytelniania używanego do zatwierdzania transakcji online. Pełną listę poleceń dostępnych w pierwszej wersji Stelsa podano w tabeli 1.

Z wyjątkiem „sendSmsLog", te same polecenia pojawiają się w drugiej wersji Stelsa, ale w wersji trzeciej zaszły pewne zmiany, co pokazano w tabeli 2. Choć instrukcje takie jak „subPref" i „botId" nie zawsze są obecne, wszystkie warianty Stelsa obsługują polecenia związane z głównymi funkcjami, na przykład tymi, które umożliwiają przechwytywanie i wysyłanie wiadomości SMS.

W tabeli 3 zamieszczono listę serwerów C&C, z którymi komunikują się wykryte próbki Stelsa. Każdy serwer komunikuje się tylko z jedną wersją Stelsa, przy czym większość nawiązuje kontakt z wersją 2. Prawdopodobnie za różnymi wersjami i odmianami Stelsa kryją się różni twórcy, a przynajmniej wiele botnetów należących do różnych osób.

Oprócz komunikowania się z serwerem C&C niektóre warianty wersji 2 używają wiadomości e-mail do utrzymywania kontaktu z właścicielem botnetu. Raz na tydzień warianty te wysyłają do napastnika wiadomość z następującymi informacjami:

- adres URL serwera C&C,
- nazwa zapasowego konta na Twitterze,
- numer International Mobile Equipment Identity (IMEI),
- numer International Mobile Subscriber Identity (IMSI),

TABELA 2: POLECENIA TYLNYCH DRZWI W TRZECIEJ WERSJI STELSA

COMMAND	FUNCTIONALITY
call	Nawiązuje połączenie telefoniczne
clearDeleteFilters	Zaprzestaje usuwania przychodzących wiadomości SMS
clearListenFilters	Zaprzestaje przechwytywania przychodzących wiadomości SMS
deleteSMS	Określa, jakie przychodzące wiadomości SMS będą usuwane (na podstawie źródłowego numeru telefonu i treści wiadomości)
httpRequest	Wykonuje żądanie HTTP
install	Pobiera i instaluje aplikację
listenSMS	Określa, jakie przychodzące wiadomości SMS będą przechwytywane (na podstawie źródłowego numeru telefonu i treści wiadomości)
message	Pokazuje okno komunikatu w celu otwarcia adresu URL
notify	Pokazuje powiadomienie na pasku stanu
openUrl	Otwiera adres URL w przeglądarce internetowej
run	Uruchamia zainstalowaną aplikację
sendContactList	Pobiera listę kontaktów z książki telefonicznej i wysyła ją do serwera dowodzenia
sendDeviceInfo	Wysyła informacje o urządzeniu do serwera dowodzenia (numer telefonu, wersja systemu operacyjnego, model i producent telefonu, operator, czy uzyskano uprawnienia superużytkownika)
sendPackageList	Pobiera z telefonu listę zainstalowanych aplikacji i wysyła ją do serwera dowodzenia
sendSMS	Wysyła wiadomość SMS
uninstall	Odinstalowuje aplikację

TABELA 3: ADRESY SERWERÓW DOWODZENIA DLA RÓŻNYCH WERSJI STELSA

WERSJA 1
kitherbin[kropka]com

WERSJA 2
33files[kropka]info
a1paybill[kropka]net
androidfan[kropka]name
bot[kropka]mobiportal[kropka]net
bot[kropka]moblife[kropka]org
istorhol[kropka]ru
marhc-nikolay[kropka]info
mobiportal [kropka]net
play-google[kropka]mobi
ponelnet[kropka]info
serviseru[kropka]ru
skladchik[kropka]in
ynfdbdybdd1[kropka]freeiz [kropka] com

WERSJA 3
droidad[kropka]net
steamads[kropka]info

- numer telefonu,
- model urządzenia,
- producent urządzenia,
- wersja systemu operacyjnego.

Wiadomość jest wysyłana za pośrednictwem strony http://[...]anonymouse.org/[...]/cgi-bin/anon-email.cgi na adres app[kropka]stels2@gmail[kropka]com.

Media społecznościowe jako wsparcie serwerów dowodzenia

Problem ze scentralizowanymi botnetami polega na tym, że jeśli właściciel utraci kontrolę nad serwerem dowodzenia, nie może również sterować botami. Twórca (lub twórcy) Stelsa rozwiązali ten problem, konfigurując kilka kont na Twitterze, z których boty mogą pobrać nowy adres serwera dowodzenia, jeśli stary jest już niedostępny.

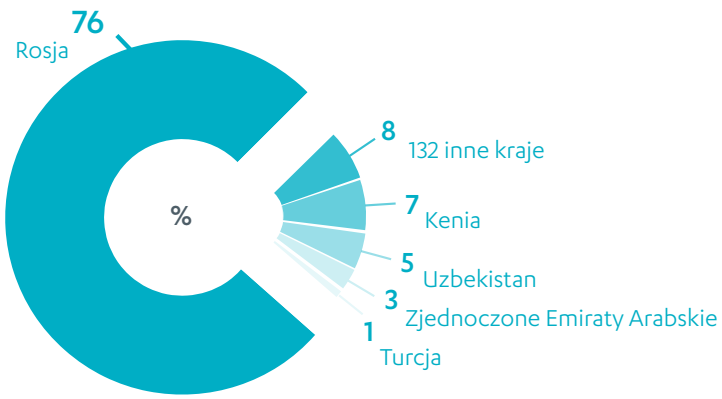
W pierwszej implementacji trojan Stels analizuje stronę na Twitterze, szukając zaszyfrowanych wiadomości, które mogą zawierać nowy adres serwera dowodzenia. Późniejsza implementacja wyszukuje zaszyfrowane wiadomości w opisie konta. Jako wsparcie serwerów dowodzenia wykorzystywano konta użytkowników Twittera „Vaberg1" i „app36005565". Nie wydaje się jednak, żeby konta te były używane wcześniej.

Rysunek 1: Konto w serwsie Twitter przeznaczone do rozpowszechniania instrukcji obsługi trojana Stels

W trzeciej wersji Stelsa Twitter zastąpiono rosyjskim serwerem mikroblogerskim, Juick. Stels analizuje źródło RSS konta założonego przez autora, przeszukując stronę internetową, http://rss[kropka]juick[kropka]com/ACCOUNTNAME/blog for the strings <description><![CDATA[które identyfikują początek wiadomości. Następnie trojan deszyfruje wiadomości i ustawia odszyfrowany łańcuch jako nowy adres serwera dowodzenia.

W maju 2013 r. właściciel botnetu stracił kontrolę nad jedną ze swoich domen C&C, droidad.net. Był zmuszony wykorzystać zapasowy kanał komunikacji w postaci konta Juick o nazwie „droidad". Na rysunku 2 widać, jak 24 maja z tego konta wysłano zaszyfrowaną wiadomość, w której znajdował się nowy adres serwera dowodzenia dla trzeciej wersji Stelsa. Po odszyfrowaniu wiadomości okazało się, że nowa domena to steamads[kropka]info.

GEOGRAFICZNA DYSTRYBUCJA DETEKCJI STELSA, PROCENTOWO*



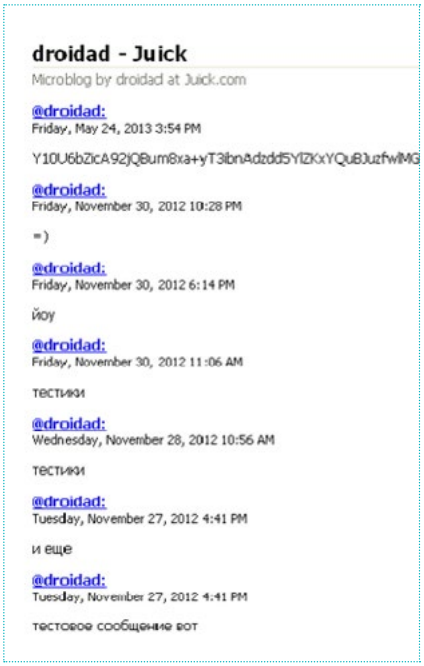
*Na podstawie danych telemetrycznych F-Secure za pierwszą połowę 2013 r.

Dystrybucja

Złośliwe oprogramowanie na Androida dotychczas rozprzestrzeniało się głównie za pośrednictwem niezależnych sklepów z aplikacjami, a Stels nie różni się pod tym względem. Jest dystrybuowany poprzez spaces.ru, popularny rosyjski serwis społecznościowy dla użytkowników urządzeń mobilnych, gdzie dołączono go do legalnych aplikacji, aby zwabić ofiary. Aplikacje-przynęty używane przez twórcę (lub twórców) Stelsa to przede wszystkim gry. Interesującym odkryciem w pierwszym kwartale roku było znalezienie Stelsa w spamie pozorującym wiadomości od amerykańskiego urzędu skarbowego (IRS) i rozsyłanym przez botnet Cutwail (http://www.secureworks.com/cyberthreat-intelligence/threats/stels-android-trojan-malwareanalysis/). Użytkownik, który kliknął łącze w urządzeniu z Androidem, był kierowany do strony, która prosiła go o zaktualizowanie aplikacji Flash Player. „Aktualizacja" instalowana przez użytkownika była w rzeczywistości trojanem Stels. Oprócz używania nazwy Flash Player, Stels może również korzystać z fałszywej aktualizacji o nazwie „Google Updater". Na rysunku 3 pokazano, jak wygląda infekcja Stelsem na liście zainstalowanych aplikacji.

Podsumowanie

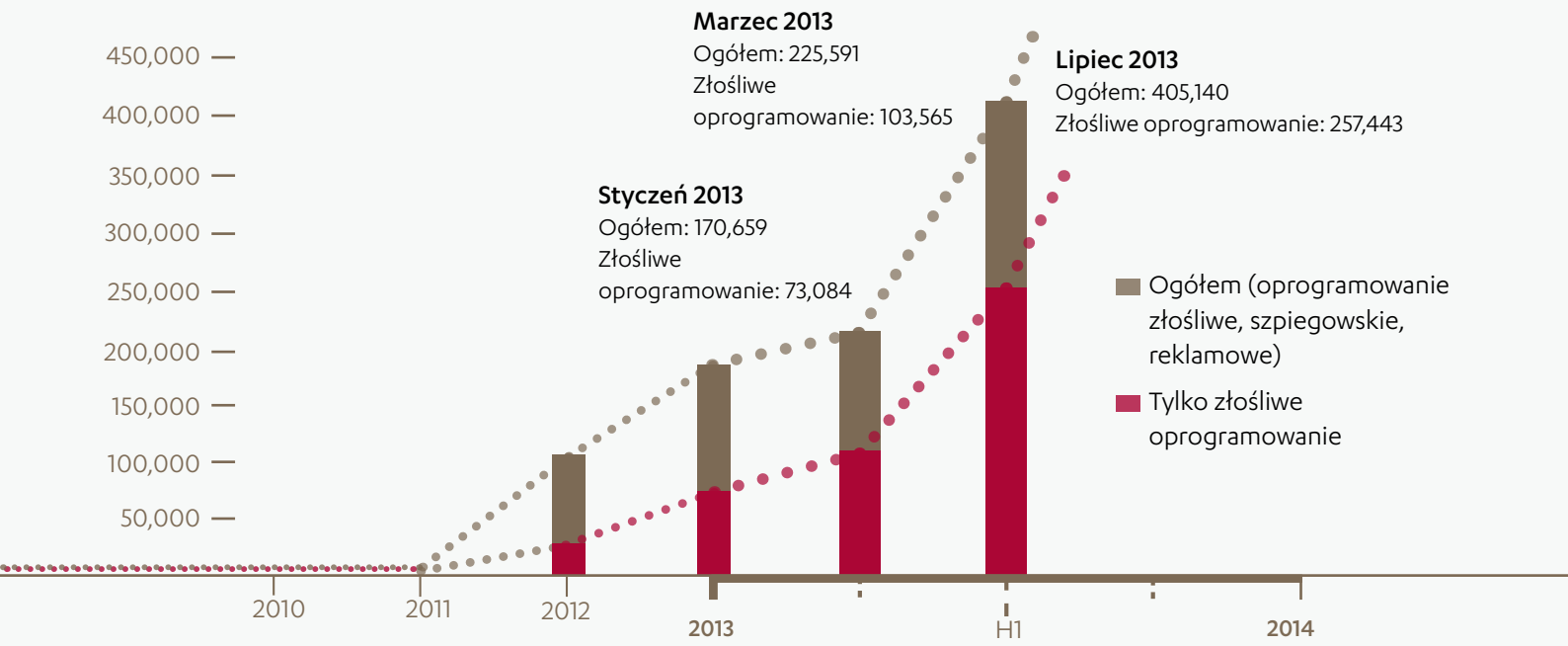
Stels to elastyczny bot, który oferuje właścicielowi botnetu różne opcje zarobkowe, w tym wiadomości SMS, połączenia telefoniczne, instalację oprogramowania, a nawet możliwość przechwytywania kodów mTAN. Trojana zaprojektowano tak, aby mógł funkcjonować przez długi czas, ponieważ autor dołączył zapasową metodę zmieniania serwerów dowodzenia, gdyby stare stały się niedostępne. Mieliśmy już do czynienia ze złośliwymi programami, które używały spamu jako metody dystrybucji i wykorzystywały media społecznościowe jako część infrastruktury dowodzenia, ale były to programy przeznaczone dla systemu Windows. Fakt, że Stels używa tych samych metod, świadczy o tym, że złośliwe oprogramowanie na Androida zbliża się do poziomu wysoko rozwiniętych zagrożeń w systemie Windows.



Rysunek 2: Botmaster Stelsa wysyła lokalizację nowego serwera dowodzenia za pośrednictwem konta w serwisie Juick

Rysunek 3: Trojan Stels podszywający się pod program Google Updater

ŁĄCZNA LICZBA PAKIETÓW APLIKACJI ANDROIDA (APK), OD 2010 R. DO POŁOWY 2013 R.



ŁĄCZNA LICZBA RODZIN LUB WARIANTÓW NA PLATFORMĘ

Nowo znalezione rodziny lub warianty, 1. połowa 2013 r.

Wszystkie znalezione rodziny lub warianty, od 2000 r. do połowy 2013 r.

PLATFORMA

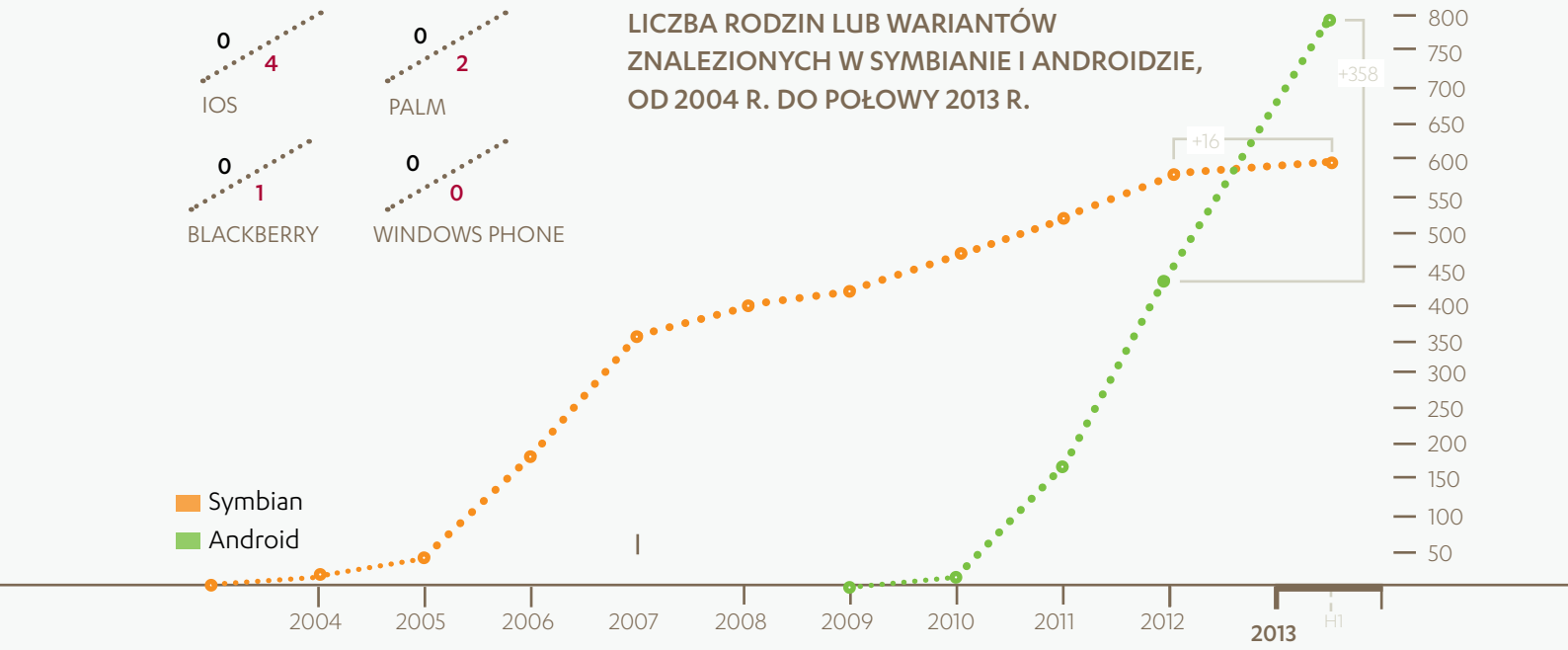
ANDROID	SYMBIAN
358 / 793	16 / 598
POCKETPC: 0 / 41	J2ME: 0 / 20
IOS: 0 / 4	PALM: 0 / 2
BLACKBERRY: 0 / 1	WINDOWS PHONE: 0 / 0

ZŁOŚLIWE OPROGRAMOWANIE MOBILNE

Od końca 2011 r. obserwujemy szybki wzrost łącznej liczby plików lub programów wymierzonych w urządzenia mobilne, dystrybuowanych na wszystkich platformach. Dotyczy to szczególnie aplikacji do Androida (powyżej). Liczba detekcji pakietów APK od marca wskazuje, że rośnie tempo tworzenia nowych pakietów dla tej platformy.

Choć samo zliczenie napotkanych przez nas programów daje imponujące liczby, większość z zaobserwowanych plików to po prostu repliki kilku unikatowych rodzin (programów zgrupowanych na podstawie podobnego kodu lub działania i wykrywanych poprzez te wspólne cechy). Dlatego bardziej miarodajne jest podsumowanie unikatowych rodzin albo nowych wariantów znanych rodzin znalezionych na danej platformie w ciągu roku (po lewej stronie i poniżej). Liczby te pozwalają nam m.in. ustalić, na czym skupiają się twórcy złośliwego oprogramowania.

LICZBA RODZIN LUB WARIANTÓW ZNALEZIONYCH W SYMBIANIE I ANDROIDZIE, OD 2004 R. DO POŁOWY 2013 R.



ANDROID

Platforma Android nadal cieszy się szczególną atencją twórców złośliwego oprogramowania. Daje się zauważyć rosnące zainteresowanie sposobami na atakowanie użytkowników z pominięciem sklepu Google Play Store. W tym artykule przyjrzymy się trendom w rozwoju złośliwego oprogramowania dla tej platformy w drugim kwartale 2013 r.

Android wciąż dominuje

Android zachowuje dominującą pozycję na rynku systemów operacyjnych do smartfonów. International Data Corporation (IDC) raportuje, że platforma reprezentowała 79,3 proc. wszystkich dostaw smartfonów w drugim kwartale bieżącego roku[1]. Drugą najpopularniejszą platformą jest naturalnie iOS, który reprezentował 13,2 proc. wszystkich nowych telefonów dostarczonych na rynek w tym okresie. Większą niespodzianką jest to, że w zeszłym kwartale platforma Windows Phone po raz pierwszy prześcignęła BlackBerry (3,7 proc. do 2,9 proc.) i została trzecim najpopularniejszym systemem operacyjnym do smartfonów. Wszystkie pozostałe platformy w tym kwartale nie zdobyły nawet jednego procenta rynku.

Przy takich liczbach nie dziwi, że twórcy złośliwego oprogramowania skupiają się na Androidzie. 96 proc. nowych rodzin lub wariantów, które zaobserwowaliśmy w pierwszej połowie 2013 r., operuje na tej platformie. W drugim kwartale roku 99 proc. nowych zagrożeń wykryliśmy w Androidzie, a na stronach 20-21 profilujemy 6 najbardziej interesujących złośliwych programów, które napotkaliśmy w tym okresie.

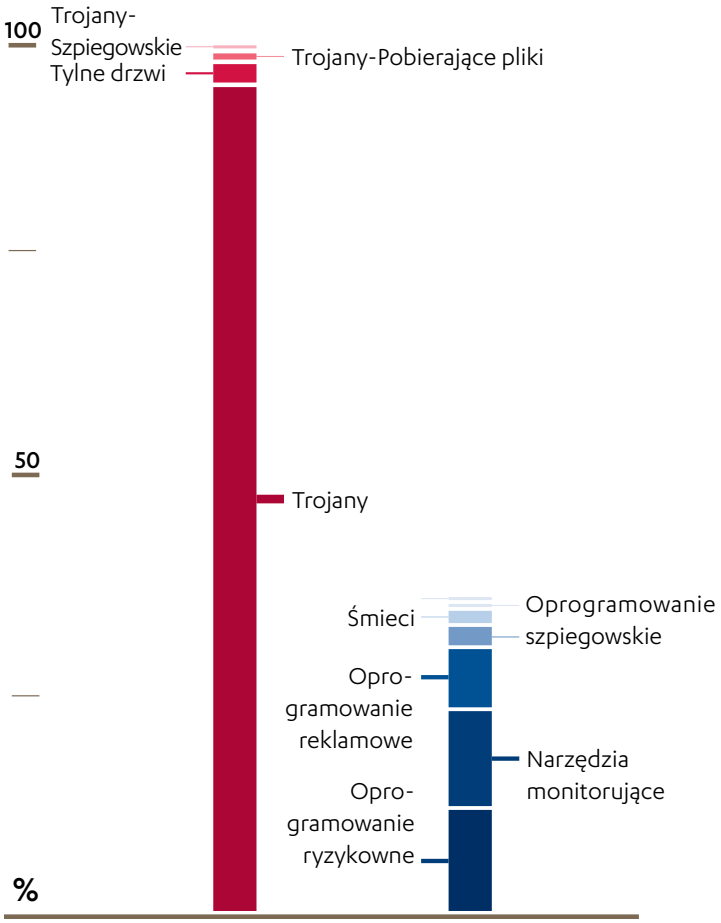
Google Play Store

Choć Apple App Store pozostaje najmocniejszym rynkiem, jeśli chodzi o zyski twórców aplikacji[2], w lipcu 2013 r. stracił tytuł największego sklepu z aplikacjami, kiedy Google poinformowało, że Play Store zaaprobował milionową aplikację, przewyższając liczbę 900 000 aplikacji, które wówczas oferowało Apple. Liczba ta nie obejmuje licznych aplikacji, które są dostępne w różnych niezależnych witrynach. Niestety, choć sama liczba aplikacji i sklepów zapewnia użytkownikom Androida szeroki wybór, drugą stroną medalu jest to, że napastnicy mają wiele możliwości „trojanizowania" legalnych aplikacji, a także wiele sposobów rozpowszechniania złośliwego oprogramowania.

W 2012 r. w Play Store wprowadzono środki bezpieczeństwa, które m.in. mają identyfikować złośliwe aplikacje udostępniane w sklepie. Choć wydają się skuteczne, nie eliminują całkowicie ryzyka — na przykład nie usuwają aplikacji, które sklasyfikowalibyśmy jako oprogramowanie reklamowe lub ryzykowne, i nie blokują reklam (ani w Play Store[3], ani w samych aplikacjach), które użytkownicy mogliby uznać za niepożądane, podejrzane albo zwyczajnie złośliwe.

Styk reklam, prywatności i bezpieczeństwa pozostaje szarym obszarem w Androidzie ze względu na otwarty ekosystem platformy, używanie reklam do czerpania zysków z głównie bezpłatnych aplikacji oraz brak skutecznego systemu

NOWE RODZINY LUB WARIANTY W PIERWSZEJ POŁOWIE 2013 R., WEDŁUG TYPU

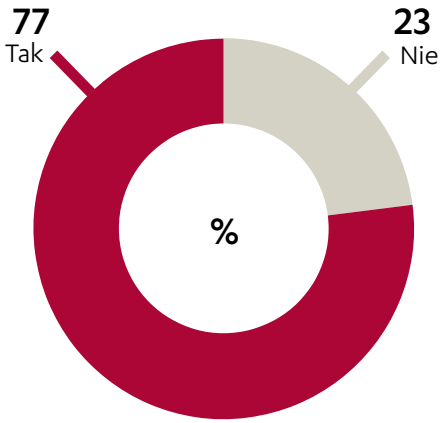


sprawdzania reputacji modułów reklamowych używanych w większości programów. Jednak pomimo okazjonalnych kłopotów Play Store jest nadal uważany za najbezpieczniejsze źródło aplikacji do Androida.

Poza Play Store

Uważamy, że coraz skuteczniejsze zabezpieczenia w Play Store doprowadziły do wzrostu liczby złośliwych programów rozpowszechnianych za pośrednictwem innych wektorów ataku. W drugim kwartale 2013 r. odkryliśmy 205 nowych rodzin lub wariantów znanych zagrożeń dla Androida, z czego większość pochodziła z źródeł innych niż Play Store. Poza oficjalnym sklepem z aplikacjami szczególnie interesujące są takie trendy, jak złośliwe reklamy, ataki typu drive-by download oraz mobilne trojany bankowe.

CZY NOWA RODZINA LUB WARIANT ZŁOŚLIWEGO OPROGRAMOWANIA JEST MOTYWOWANY ZAROBKOWO?



„Malvertising": reklamowanie złośliwego oprogramowania

Reklamy są coraz częściej używane do rozpowszechniania złośliwego oprogramowania, prawdopodobnie ze względu na łatwość implementacji i szeroki zasięg. Dotychczasowe metody dystrybucji zwykle polegały na umieszczeniu złośliwych łączy lub kodu w przejętej witrynie albo, jeszcze prościej, na wykorzystaniu sieci reklamowych do promowania łączy do złośliwych produktów. W tym drugim przypadku same reklamy mogą być wyświetlane w dobrej wierze.

Strategią reklamową, która wykorzystuje dobrą reputację Play Store, a jednocześnie omija zabezpieczenia serwisu, jest użycie fałszywych reklam. Ta technika inżynierii społecznej polega na zamieszczeniu reklamy, która wydaje się dotyczyć produktu dostępnego w Play Store, ale po kliknięciu otwiera w przeglądarce witrynę innego sklepu.

Zaobserwowaliśmy też reklamy wyświetlane podczas sesji surfowania na urządzeniach mobilnych i promujące fałszywe „mobilne programy antywirusowe"[4] — zasadniczo odpowiednik podobnych metod dystrybuowania rzekomych antywirusów dla komputerów PC. Innej techniki używa Trojan:Android/Badnews.A, w którym reklamy wyświetlane wewnątrz aplikacji promują coś, co okazało się oszukańczą subskrypcją płatnej usługi SMS.

Mobilne ataki typu drive-by download

Zaobserwowaliśmy również próby instalacji złośliwego oprogramowania podczas przeglądania zainfekowanych witryn na urządzeniach z Androidem[5]. W przeciwieństwie do ataków typu drive-by download znanych z komputerów PC, ataki te wciąż są względnie widoczne dla użytkownika, ponieważ powodują automatyczne wyświetlenie prośby o zgodę na zainstalowanie aplikacji (co daje okazję do usunięcia niepożądanego programu).

Ten wektor ataku również wymaga albo przejęcia legalnej witryny, albo przekierowania użytkownika do złośliwej witryny (obie te metody są dobrze znane każdemu dystrybutorowi złośliwego oprogramowania, który terminował na komputerach PC). Można oczekiwać, że w przyszłości złośliwe oprogramowanie będzie nadal rozpowszechniane w ten sposób.

Mobilne trojany bankowe

Bardziej bezpośrednim zagrożeniem dla użytkowników są mobilne trojany bankowe — zwykle złośliwe oprogramowanie, które próbuje wykradać kody autoryzacji transakcji mobilnych (mTAN). Programy tego typu zaczęły się mnożyć, od kiedy banki udostępniły klientom opcję uwierzytelniania dwuczynnikowego podczas zakupów w internecie. W tym kwartale odkryliśmy trojana Trojan:Android/Pincer.A, który może być powiązany ze zgłoszonymi w lipcu fałszywymi aplikacjami bankowymi wymierzonymi w użytkowników Commonwealth Bank[6], a także z programem Trojan:Android/FakeKRBank.A, który atakował użytkowników w Korei.

Wreszcie w drugim kwartale 2013 r. zaobserwowaliśmy, że na podziemnych rynkach sprzedaje się więcej pakietów narzędziowych, które automatyzują proces tworzenia mobilnych trojanów bankowych. Dlatego spodziewamy się, że niebawem tego rodzaju zagrożenia staną się bardziej powszechne i być może będą dalej ewoluować.

SOURCES

1. International Data Corporation; *Apple Cedes Market Share in Smartphone Operating System Market as Android Surges and Windows Phone Gains, According to IDC*; opublikowano 7 sierpnia 2013 r.; http://www.idc.com/getdoc.jsp?containerId=prUS24257413
2. Forbes; Chuck Jones; *Apple Still Dominates Tablet And App Store Usage But Android Is Gaining Ground*; opublikowano 31 maja 2013 r.; http://www.forbes.com/sites/chuckjones/2013/05/31/apple-still-dominates-tablet-and-app-store-usage-but-android-is-gaining-ground/
3. Weblog F-Secure; Sean Sullivan; *Google Play: Potentially Unwanted*; opublikowano 11 marca 2013 r.; http://www.f-secure.com/weblog/archives/00002521.html
4. Weblog F-Secure; Sean Sullivan; *Fake Antivirus Scan Scam Via Google Play App Ads*; opublikowano 13 czerwca 2013 r.; http://www.f-secure.com/weblog/archives/00002567.html
5. Kanał FSLabs na Youtube; *Drive-by Android Malware*; opublikowano 3 maja 2013 r.; http://www.youtube.com/watch?v=aYFX8V7EXbA
6. The Age; Liam Tung; *Fake CommBank Android security app targets mobile customers*; opublikowano 16 czerwca 2013 r.; http://www.theage.com.au/it-pro/security-it/fake-commbank-android-security-app-targets-mobile-customers-20130716-hv0w0.html

GODNE UWAGI ZAGROŻENIA DLA UŻYTKOWNIKÓW ANDROIDA, 2. KWARTAŁ 2013 R.

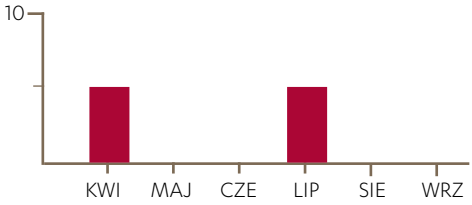
Poniżej opisano sześć złośliwych programów na Androida, które są reprezentatywne dla zagrożeń mobilnych odkrytych w drugiej połowie 2013 r.

Liczba znanych unikatowych próbek ma dawać ogólne pojęcie o wielkości danej rodziny złośliwego oprogramowania. Ponadto **liczba detekcji Protection Network**, jeśli jest dostępna, pokazuje, ile razy urządzenie chronione przez F-Secure Mobile Security zgłosiło próbę instalacji złośliwego oprogramowania do naszych chmurowych systemów telemetrycznych w drugim i trzecim kwartale 2013 r. Porównanie niskiego współczynnika blokowanych infekcji mobilnych do znacznie większego współczynnika blokowanych zagrożeń dla komputerów PC może świadczyć zarówno o względnej rzadkości infekcji mobilnych, jak i o skuteczności mobilnych rozwiązań antywirusowych.

TROJAN:ANDROID/BADNEWS.A

Liczba znanych unikatowych próbek: 113
Data odkrycia najstarszej znanej próbki: 2013-03-03

Liczba detekcji Protection Network

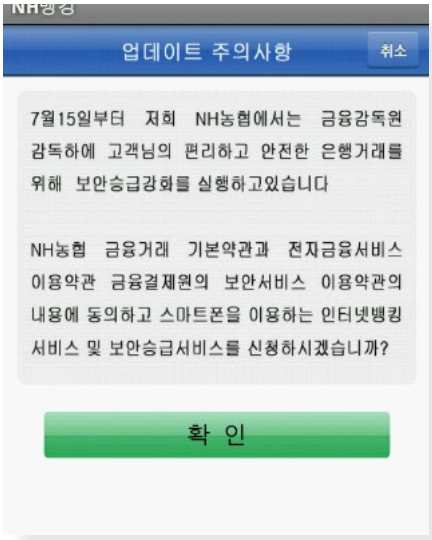


Dystrybucja
Warianty trojana Badnews znaleziono w następujących internetowych sklepach z aplikacjami: Google Play, Opera, Baidu, Anzhi i Liqucn

Podsumowanie
Warianty Badnews to trojany, które zarabiają na wiadomościach SMS wysyłanych na numery premium. Po instalacji aplikacja wyświetla reklamę płatnej usługi SMS.

TROJAN-DROPPER:ANDROID/FAKEKRBANK.A, TROJAN:ANDROID/FAKEKRBANK.A

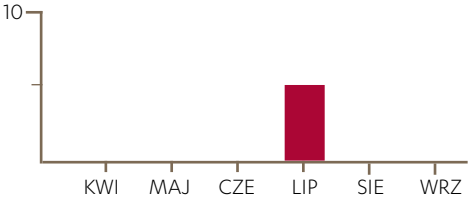
Liczba znanych unikatowych próbek: 64
Data odkrycia najstarszej znanej próbki: 2013-05-20



Dystrybucja
Nieznana

Podsumowanie
Po instalacji Fakekrbank przechwytuje wiadomości SMS i przekazuje je metodą URL POST do zdalnego serwera wraz z nazwą i numerem urządzenia.

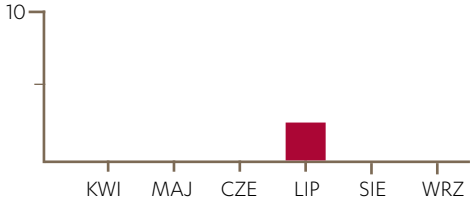
LICZBA DETEKCJI PROTECTION NETWORK



TROJAN:ANDROID/VMVOL.A

Liczba znanych unikatowych próbek: 43
Data odkrycia najstarszej znanej próbki: 2013-03-28

Liczba detekcji Protection Network

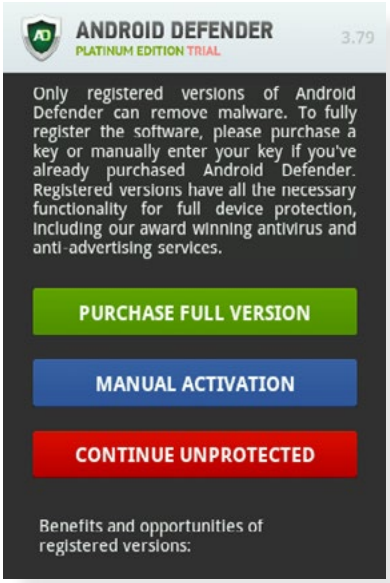


Dystrybucja
Niepotwierdzona w Google Play, rejestry wskazują, że trojan został usunięty.

Podsumowanie
Po instalacji VMVol.A wysyła numer telefonu i numer IMEI (International Mobile Equipment Identity) urządzenia do zdalnego serwera. Przekazuje też kopię wysłanych wiadomości, w tym treść wiadomości oraz numer odbiorcy.

TROJAN:ANDROID/FAKEDEFENDER.A

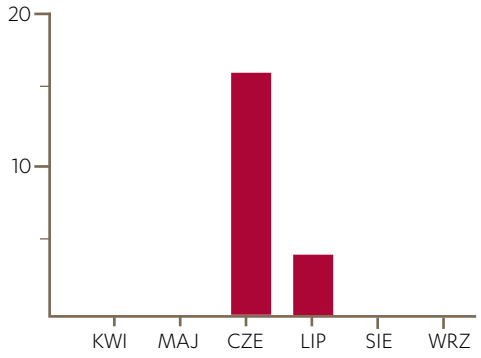
Liczba znanych unikatowych próbek: 14
Data odkrycia najstarszej znanej próbki: 2013-03-24



Dystrybucja
Reklamy firm trzecich wyświetlane na urządzeniach mobilnych.

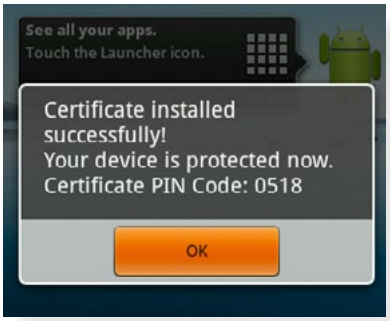
Podsumowanie
Podobnie jak fałszywe programy antywirusowe do komputerów PC, Fakedefender podszywa się pod program antyszpiegowski do urządzeń mobilnych. Program nie zapewnia reklamowanych funkcji skanowania ani usuwania złośliwego oprogramowania.

Liczba detekcji Protection Network



TROJAN:ANDROID/PINCER.A

Liczba znanych unikatowych próbek: 11
Data odkrycia najstarszej znanej próbki: 2013-03-19



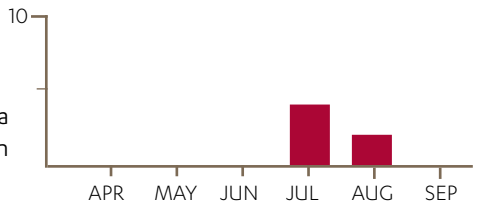
Dystrybucja
Ta aplikacja jest rozpowszechniana przez witryny wyłudzające informacje (zwykle imitujące stronę banku) albo złośliwe łącza w wiadomościach SMS. Może też być dystrybuowana jako część złośliwego oprogramowania do komputerów PC.

Podsumowanie
Po instalacji Pincer przesyła wiadomości SMS do zdalnego serwera dowodzenia (C&C). Może również wykradać bankowe kody mTAN oraz wykonywać instrukcje przekazywane zdalnie przez serwer dowodzenia.

TROJAN:ANDROID/OBAD.A

Liczba znanych unikatowych próbek: 6
Data odkrycia najstarszej znanej próbki: 2013-05-16

Liczba detekcji Protection Network



Dystrybucja
Warianty trojana Obad są reklamowane w złośliwych witrynach podczas przeglądania stron internetowych na urządzeniu z Androidem. Instalacja w urządzeniu klienckim prawdopodobnie odbywa się metodą drive-by download.

Podsumowanie
Po instalacji w urządzeniu warianty trojana Obad zyskują przywileje administracyjne i wykorzystują exploit, aby złamać warstwę zabezpieczeń systemu operacyjnego Android. Obad gromadzi i przesyła do zdalnego serwera dowodzenia następujące dane: adres Media Access Control (MAC), numer IMEI, nazwę operatora, bieżący czas i informację o tym, czy uzyskano przywileje superużytkownika. Serwer dowodzenia może też wydawać polecenia zainstalowanej aplikacji, m.in. wysłać wiadomość SMS, sprawić, aby urządzenie działało jako proxy albo zdalna powłoka, otworzyć adres URL w mobilnej przeglądarce, pobrać i zainstalować dodatkowe komponenty, pozyskać listę kontaktów oraz szczegółowe informacje o określonej zainstalowanej aplikacji i wysłać plik przez Bluetooth.

ZALECENIA: Ochrona przed złośliwym oprogramowaniem mobilnym

Zabezpieczanie urządzenia

Dziś większość osób korzysta z kont e-mail (osobistych lub służbowych) oraz innych krytycznych usług na urządzeniach mobilnych. Jest to wygodne, ale oznacza, że w przypadku kradzieży można stracić znacznie więcej, niż tylko samo fizyczne urządzenie.

Ponadto, pomimo obaw o ataki z internetu, o infekcję najłatwiej wtedy, gdy ktoś uzyska dostęp do urządzenia i ręcznie zainstaluje złośliwe oprogramowanie. Innymi słowy, przede wszystkim należy zadbać o fizyczne bezpieczeństwo urządzenia.

1. Zablokuj urządzenie

Zablokowanie urządzenia uniemożliwia innym majstrowanie przy jego ustawieniach albo zainstalowanie aplikacji (takiej jak narzędzie monitorujące albo aplikacja szpiegowska) bez Twojej wiedzy. Aby blokada była skuteczna, zadbaj o to, aby hasło, kod lub wzorzec były unikatowe, najlepiej łatwe do zapamiętania, a trudne do odgadnięcia.

2. Skonfiguruj ochronę antykradzieżową

Ochrona antykradzieżowa zwykle umożliwia zdalne usunięcie danych z telefonu, łącznie z zawartością kart pamięci, jeśli dojdziesz do wniosku, że już nie odzyskasz urządzenia.

Niektóre rozwiązania antykradzieżowe pokazują również lokalizację urządzenia albo wydają dźwięk alarmowy, co przydaje się, kiedy próbujesz odszukać urządzenie.

Blokowanie niepożądanych usług

Złośliwe oprogramowanie może zarabiać na potajemnym wysyłaniu wiadomości SMS na numery premium, subskrybowanie płatnych usług albo zmuszanie urządzenia do dzwonienia na numery premium. Zablokowanie połączeń telefonicznych albo wysyłania wiadomości na numery premium pozwala zminimalizować straty finansowe, nawet jeśli urządzenie zostanie zainfekowane. Zapobiega to również oszustwom, które nie mają związku ze złośliwym oprogramowaniem, kiedy ktoś bez wiedzy użytkownika rejestruje go w płatnej usłudze i przekazuje rozliczenia do jego operatora komórkowego, licząc na to, że zostaną one po cichu dodane do rachunku.

3. Skonfiguruj blokowanie wiadomości

Większość operatorów pozwala użytkownikom skorzystać z usługi, która blokuje nawiązywanie połączeń lub wysyłanie wiadomości SMS klasy premium. Jest to szczególnie przydatne dla rodziców, którzy nie chcą, aby dzieci naraziły ich na niepotrzebne koszty. Aby skonfigurować tę usługę, skontaktuj się ze swoim operatorem. Niektóre usługi zapewniają też numer PIN albo inną metodę, która pozwala na selektywne usunięcie blokady, jeśli użytkownik sobie tego zażyczy.

SOURCES

1. Weblog F-Secure; Sullivan, Sean; *Post-PC Attack Site: Only Interested in Smartphones/Tablets*; opublikowano 19 czerwca 2013 r.; http://www.f-secure.com/weblog/archives/00002569.html

Podczas pobierania aplikacji

Jeśli zadbałeś już o fizyczne bezpieczeństwo urządzenia, pamiętaj również o następujących środkach ostrożności, kiedy będziesz pobierać aplikacje.

4. Pobieraj aplikacje tylko z Play Store

Domyślnie urządzenia z Androidem blokują instalowanie aplikacji ze źródeł innych niż Play Store. Aby sprawdzić, czy Twoje urządzenie zezwala tylko na aplikacje z Play Store, zajrzyj do menu ***Ustawienia > Aplikacje > Nieznane***. Jeśli pole wyboru jest zaznaczone, można instalować aplikacje z innych źródeł. Usuń zaznaczenie z tego pola.

5. Sprawdź zezwolenia, o które prosi aplikacja

Bez względu na to, czy pobierasz programy z Play Store, czy z innych źródeł, przeczytaj listę uprawnień, o które prosi aplikacja (te, które mogą budzić wątpliwości ze względu na kwestie bezpieczeństwa lub prywatności, wymieniono poniżej po prawej stronie).

- **Usługi, za które płacisz**
  - **Nawiązywanie połączeń telefonicznych**
  - **Wysyłanie wiadomości SMS lub MMS**
- **Twoja lokalizacja**
- **Twoje informacje osobiste**

Jeśli żądane uprawnienia wydają się nadmierne lub niezwiązane z przeznaczeniem aplikacji — na przykład prosta gra prosi o możliwość wysyłania wiadomości SMS — możesz dokładniej sprawdzić dewelopera; renomowani twórcy aplikacji zwykle wyjaśniają, do czego potrzebne są uprawnienia. Jeżeli uznasz ich racje, będziesz mógł pobrać aplikację.

Przy okazji, aplikacje takie jak PocketPermissions, LBE Privacy lub PermissionDog dobrze wyjaśniają przeznaczenie mało zrozumiałych uprawnień. Niektóre z nich oferują też możliwość ograniczenia uprawnień zainstalowanych aplikacji, choć takie funkcje są przeznaczone dla zaawansowanych użytkowników.

6. Skanuj aplikacje mobilnym antywirusem

Po pobraniu aplikacji do urządzenia przeskanuj ją za pomocą renomowanego mobilnego programu antywirusowego. W ten sposób możesz skontrolować „ciche" działania aplikacji — dozwolone akcje, które są implikowane przez listę uprawnień aplikacji (na przykład wysyłanie informacji o urządzeniu do zdalnego serwera), ale mogą budzić wątpliwości użytkownika. Jeśli werdykt programu antywirusowego Cię usatysfakcjonuje, możesz zainstalować aplikację..

W sieci

W miarę, jak strony internetowe ewoluowały, aby uwzględnić potrzeby użytkowników mobilnych, złośliwe witryny szły w ich ślady[1].

7. Używaj ochrony przeglądania

Aby nie natknąć się na złośliwą witrynę, kiedy surfujesz po sieci na urządzeniu mobilnym, używaj funkcji ochrony przeglądania (dostępnej w większości rozwiązań antywirusowych) do blokowania szkodliwych stron.

ATAKI APT

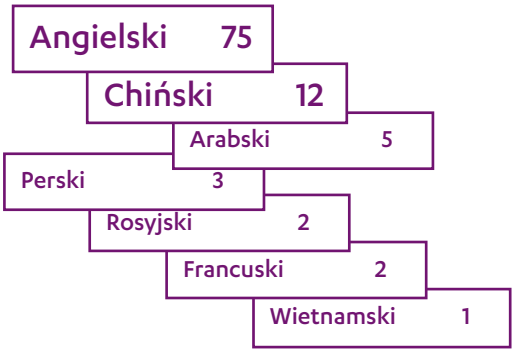
Ataki APT (Advanced Persistent Threat, zaawansowane uporczywe zagrożenia) polegają na dostarczeniu (zwykle jakąś metodą socjotechniczną) specjalnie przygotowanego dokumentu do użytkownika albo użytkowników w docelowej organizacji lub branży. W 2012 i 2013 r. dużo mówiło się o poszczególnych kampaniach APT i ważnych indywidualnych przypadkach. Choć te przypadki są interesujące, pomyśleliśmy, że warto byłoby nakreślić ogólny obraz ofiar ataków APT.

Aby uzyskać wgląd w ogólną sytuację, losowo wybraliśmy i przeanalizowaliśmy 100 dokumentów APT z naszej kolekcji próbek. Przykładowe dokumenty sklasyfikowaliśmy według języka, tematu, a w razie możliwości również ukierunkowania państwowego — to znaczy kraju, z myślą o którym stworzono dany dokument. Choć treść dokumentu APT nie identyfikuje bezpośrednio napastnika, zebrane informacje dają dobre pojęcie o potencjalnych ofiarach, bo jeśli atak ma się udać, dokument musi być wystarczająco dobrą przynętą.

Dokumenty w językach innych niż angielski przetłumaczono komputerowo, więc ich treść nie była w pełni zrozumiała, ale okazało się to wystarczające do celów klasyfikacji. Wyodrębniliśmy też tekst z pierwszych stron wszystkich przykładowych dokumentów i przedstawiliśmy go w postaci chmury słów (zob. strona 24), aby pokazać wyrazy najczęściej używane w dokumentach APT.

Na podstawie statystyk wygenerowanych podczas analiz stwierdziliśmy, że angielski jest najczęstszym językiem dokumentów PT, co ma sens zarówno z perspektywy napastnika, jak i ofiary, ponieważ jest to język międzynarodowego biznesu i polityki, więc napastnik nie musi produkować dokumentów-przynęt w języku ofiary, potencjalnie innym niż angielski.

JĘZYKI UŻYWANE W DOKUMENTACH APT

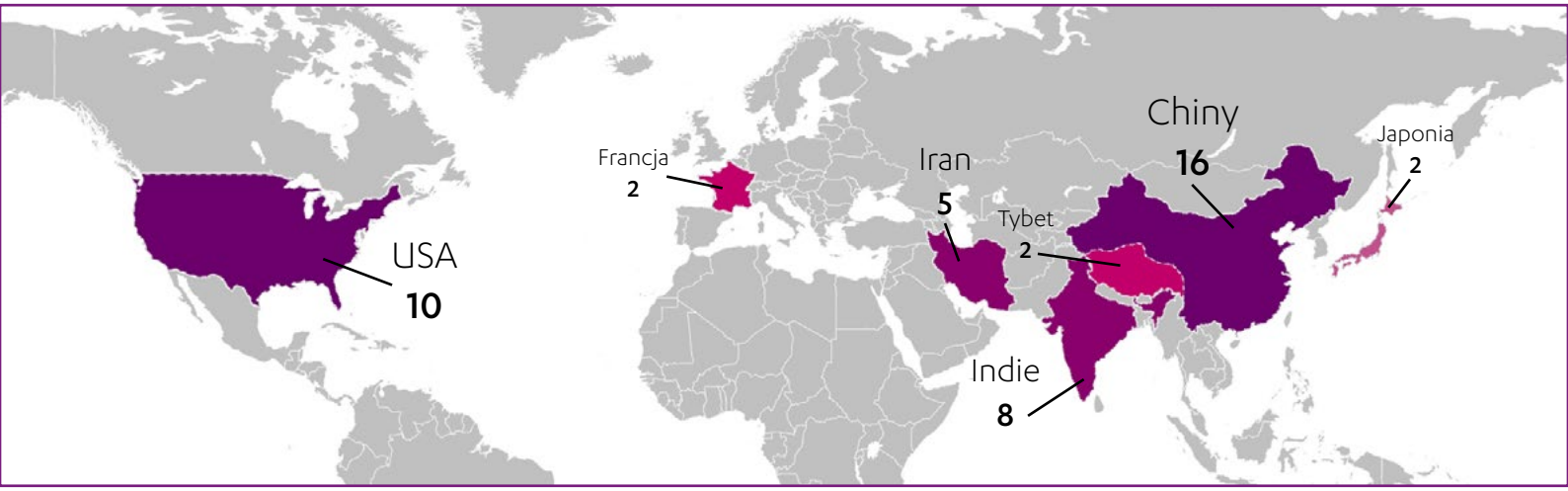


Ataki polityczne

Jak pokazuje chmura słów oraz statystyki naszych badań, dokumenty APT najczęściej mają treść polityczną, zwykle w postaci raportu z jakiegoś politycznie interesującego wydarzenia albo bardziej długofalowej analizy. Ogólnie rzecz biorąc, dokumenty-przynęty zawierają typ treści, który byłby interesujący dla urzędnika ambasady, pracownika rządowego albo innej osoby aktywnej lub świadomej politycznie.

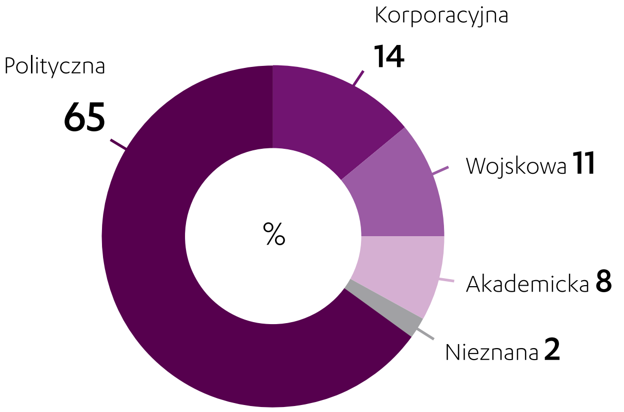
Dokumenty polityczne zwykle dotyczą Chin lub Indii; często pojawiają się również tematy związane ze Stanami Zjednoczonymi. Wydaje się, że wiele spośród nich omawia relacje między Stanami Zjednoczonymi a Chinami albo Indiami i Chinami. Można z tego wywnioskować, że najczęstszym celem motywowanego politycznie ataku APT jest ktoś, kto pochodzi ze Stanów Zjednoczonych lub Indii (lub jest z nimi jakoś powiązany) i interesuje się Chinami..

PAŃSTWOWE UKIERUNKOWANIE DOKUMENTÓW APT *



** Na mapie przedstawiono tylko państwa, które były celem więcej niż jednego dokumentu APT w zbiorze próbek*

TREŚĆ DOKUMENTÓW APT



CHMURA NAJCZĘSTSZYCH SŁÓW W DOKUMENTACH APT

POLITYCZNE

KORPORACYJNE

WOJSKOWE

Źródło: Tagul.com

Ataki korporacyjne

Użytkowników korporacyjnych zwykle wabi się dokumentami, które wyglądają jak protokoły lub raporty z konferencji. Ma to sens, ponieważ protokoły z konferencji zwykle są rozpowszechniane pocztą e-mail w ramach standardowych praktyk biznesowych, więc łatwo je pozyskać, zmodyfikować i przekazać dalej jako wydania „poprawione". Drugim najczęstszym typem korporacyjnego dokumentu APT są raporty, które również można względnie łatwo pozyskać i puścić w obieg jako wiarygodny materiał biznesowy.

Jak widać w korporacyjnej chmurze słów, największym zainteresowaniem szpiegów cieszy się branża lotniczo-kosmiczna i energetyczna. Podobnie jak dokumenty polityczne, korporacyjne dokumenty APT często zawierają odniesienia do Chin lub innych krajów azjatyckich, co sugerowałoby, że napastnicy są zainteresowani celami, które operują w branży lotniczo-kosmicznej lub energetycznej i w jakiś sposób są powiązane z państwami azjatyckimi.

Ataki wojskowe

Podobnie jak w przypadku innych kategorii ofiar, znaczną część dokumentów APT kierowanych do wojska stanowią raporty na tematy, które mogą być interesujące dla personelu wojskowego. Co ciekawe, oprócz tematów czysto militarnych wiele dokumentów porusza kwestie osobistych finansów żołnierzy, na przykład zawiera informacje o podatkach albo o emeryturach wojskowych. W takich przypadkach napastnicy próbowali atakować ofiary za pomocą dokumentów budzących zainteresowanie z przyczyn osobistych, a nie zawodowych, czego nie zaobserwowaliśmy w żadnej innej kategorii.

Ataki akademickie

Liczba dokumentów APT w naszym zbiorze próbek, które brały na cel personel akademicki, była zbyt mała, aby wyciągać istotniejsze wnioski. Na podstawie nielicznych próbek można stwierdzić, że napastnicy próbują zwabić ofiary albo materiałami związanymi z konkretną dziedziną akademicką, albo tematami administracyjnymi, takimi jak CV, notatki lub formularze.

Podsumowanie

Aby opracować ten raport, użyliśmy dokumentów APT uzyskanych z publicznych źródeł , co oznacza, że próbka najprawdopodobniej nie jest reprezentatywna, ponieważ wiele zaatakowanych firm zapewne uważa materiały APT za tak wrażliwe, że albo nie udostępniają ich wcale, albo tylko z klauzulą poufności, co nie pozwala wykorzystać ich w publicznym badaniach.

Pomimo to w oparciu o materiał, którym możemy się podzielić, da się skonstruować podstawowy profil ofiar ataków APT: są to przede wszystkim osoby, które pracują z materiałami politycznymi, zwłaszcza te, które są powiązane z Chinami oraz innymi dużymi graczami z regionu Południowo-Wschodniej Azji. Choć korporacje, wojsko i instytucje akademickie przyciągają mniej uwagi, każdy, kto dysponuje interesującymi informacjami, może stać się celem ataku APT.

TEMATY POJAWIAJĄCE SIĘ W WIĘCEJ NIŻ JEDNYM DOKUMENCIE APT

Raport **40**
List **7**
Konferencja **6**
Usługi finansowe **4**
Lotnictwo i kosmonautyka **4**
Aktywizm **3**
Seks-skandal **3**
Curriculum Vitae **3**
Reklama samochodu dyplomatycznego **2**
Bankowość **2**
Lista kontaktów **2**

WYMUSZANIE OKUPU

Oprogramowanie typu ransmoware to typ złośliwego oprogramowania, który wyłudza pieniądze od użytkowników zainfekowanych komputerów. Zwykle przejmuje kontrolę nad danymi lub komputerem i domaga się opłaty za odzyskanie dostępu. Ostatnio pisaliśmy o problemach z oprogramowaniem wymuszającym okup w naszym raporcie na temat zagrożeń w pierwszej połowie 2012 r. Od tego czasu, również w pierwszej połowie 2013 r., zagrożenie to pozostawało bardzo aktywne.

Dwa typy oprogramowania wymuszającego okup

Warto porównać dwa typy oprogramowania wymuszającego okup, które obecnie infekuje komputery użytkowników. Ich jedyną wspólną cechą jest wyłudzanie pieniędzy od ofiar przez przetrzymywanie czegoś cennego — danych albo samego komputera. Jak się wkrótce przekonamy, pod innymi względami bardzo się różnią.

Pierwszy typ to oprogramowanie szyfrujące. Po zainfekowaniu komputera szyfruje ono dane i domaga się pieniędzy za klucz kryptograficzny niezbędny do przywrócenia plików. Drugi typ to oprogramowanie policyjne. Po udanej infekcji wyświetla ono ekran z żądaniem okupu za odblokowanie komputera. Jest to po prostu okno dialogowe, które wypełnia cały ekran. Użytkownik nie może zamknąć tego okna i przerwać działania złośliwego programu.

Szyfrujące oprogramowanie do wymuszania okupu

Infekcja oprogramowaniem szyfrującym przebiega w nietypowy sposób. Większość złośliwych programów dostaje się do komputera metodą drive-by download (cichej instalacji bez wiedzy użytkownika), wykorzystując słabe punkty podatnej aplikacji, takiej jak Java. Celem często są komputery osobiste, zwłaszcza tych użytkowników, którzy mają złe nawyki, jeśli chodzi o przeglądanie witryn internetowych.

Natomiast oprogramowanie szyfrujące często atakuje korporacyjne serwery Windows, w których szyfruje wszystkie pliki danych, po czym domaga się opłaty za ich odszyfrowanie. Serwery te nie powinny być używane do przeglądania sieci i czytania wiadomości e-mail. W wielu przypadkach okazywało się, że w serwerze działała usługa pulpitu zdalnego (RDP), a konta użytkowników były chronione słabymi hasłami. Napastnicy odgadywali hasło i logowali się do systemu za pośrednictwem usługi RDP.

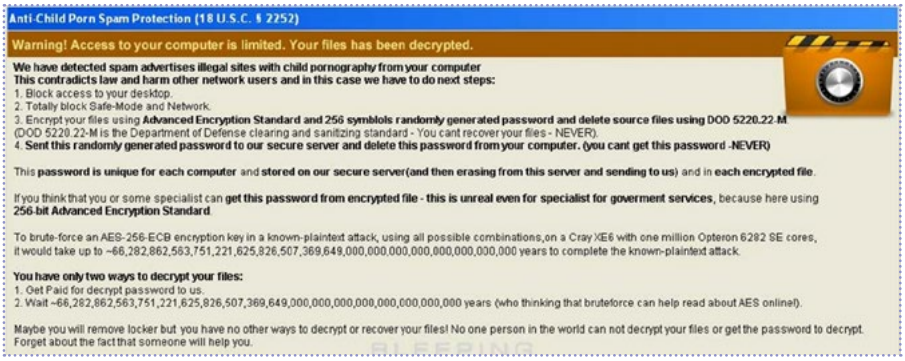
Rozkład geograficzny

Ponieważ infekcja nie jest w pełni zautomatyzowana, a napastnicy ręcznie włamują się do serwerów, liczba infekcji oprogramowaniem szyfrującym jest mała w porównaniu z oprogramowaniem policyjnym. W pierwszej połowie 2013 r. w F-Secure Labs obserwowaliśmy „fale" ataków, które były wymierzone w serwery w jednym kraju, a następnie przechodziły do innego kraju.

Oprogramowanie „Anti Child Porn Spam Protection" atakowało klientów korporacyjnych, m.in. w Hiszpanii i Włoszech, w marcu i kwietniu. Aktywne były też inne podobne programy wymuszające okup.

Działanie

Działanie oprogramowania szyfrującego jest zwykle bardzo proste. Kiedy napastnik uzyska dostęp do korporacyjnego serwera, ręcznie uruchamia złośliwy program. Program wylicza pliki na serwerze, szyfrując wszystkie pliki danych, ale pomijając pliki systemowe, aby uniknąć sytuacji, w której uruchomienie systemu byłoby niemożliwe. Do szyfrowania używa się mocnych algorytmów kryptograficznych, a po zakończeniu operacji klucz jest bezpiecznie usuwany. Program szyfruje również wszystkie pliki w udziałach sieciowych; jeśli serwer ma dostęp do kopii zapasowych, one także zostają zaszyfrowane.



Rysunek 1: Zrzut ekranowy programu „Anti-Child Porn Spam Protection"

Mechanizm płatności

Do odszyfrowania plików potrzebny jest klucz kryptograficzny. Ofiary otrzymują informacje, jak dostarczyć napastnikowi okup w zamian za klucz. W wielu przypadkach płatności dokonuje się online za pośrednictwem takich systemów płatniczych, jak Moneypak, Paysafecard lub Ukash. Kwota może wynosić 500 lub więcej dolarów.

SZYFRUJĄCE oprogramowanie		POLICYJNE oprogramowanie
Szyfruje dane użytkownika i domaga się „okupu” w zamian za klucz deszyfrujący	infekcja	Wyświetla „ekran blokady”, rzekomo w imieniu lokalnych organów ścigania. Domaga się zapłacenia „kary” w zamian za odblokowanie komputera.
Korporacyjne serwery Windows, w których działa usługa pulpitu zdalnego (RDP)	cel	Komputery przeciętnych użytkowników
Odgadywanie hasła w celu włamania się do systemu oraz logowanie się z wykorzystaniem usługi RDP	metoda infekcji	Przekierowywanie użytkowników do serwerów z pakietami exploitów; komputery użytkowników są infekowane automatycznie
Ręczny. Śledzenie dowodów wpłaty i dostarczanie klucza pocztą e-mail	mechanizm płatności	Zautomatyzowany. Automatycznie wysyłanie kodu PIN do serwerów dowodzenia
Wylicza wszystkie pliki w serwerze i szyfruje pliki danych, pomijając pliki systemowe. Klucz szyfrujący jest bezpiecznie usuwany po zakończeniu operacji	sposób działania	Ma w rejestrze punkt startowy, który automatycznie uruchamia złośliwe oprogramowanie po restarcie systemu, zwykle w „trybie awaryjnym”. Ekran blokady pojawia się natychmiast

W typowej sytuacji napastnik prosi ofiarę o przesłanie zaszyfrowanego pliku, który następnie zwraca w postaci odszyfrowanej. Ofiara musi też przesłać przez e-mail dowód wpłaty. Ponieważ napastnik musi śledzić ofiary i klucze potrzebne do odszyfrowania ich plików (każdej przypisuje się inny klucz), ręczna praca związana z tą korespondencją ogranicza liczbę ofiar, które można zaatakować jednocześnie. Jednoczesne zaatakowanie miliona ofiar jest niemożliwe. Może to wyjaśniać „fale” ataków — napastnicy biorą na cel ograniczony zbiór serwerów w jednym kraju, a następnie biorą się za następny.

Policyjne oprogramowanie do wymuszania okupu

Oprogramowanie policyjne bierze nazwę od „ekranu blokady”, który pojawia się na zainfekowanym komputerze. Ekran blokady wyświetla komunikat rzekomo pochodzący od lokalnych organów ścigania, sugerując udział komputera w nielegalnej działalności, takiej jak naruszenie praw autorskich albo dystrybucja pornografii dziecięcej. Za większość infekcji odpowiada zaledwie kilka rodzin oprogramowania policyjnego; w minionym półroczu szczególnie godne uwagi były Reveton i Urausy. Obie rodziny infekują użytkowników za pomocą pakietów exploitów podczas przeglądania sieci. Użytkownicy są przekierowywani do serwera internetowego, który automatycznie zaraża komputer za pośrednictwem luki w zabezpieczeniach.

Stwierdzono przypadki, w których złośliwe reklamy pojawiały się w popularnych witrynach, takich jak MSN Italy, i przekierowywały użytkowników do serwerów z policyjnym oprogramowaniem do wymuszania okupu. Jednak najpopularniejszą metodą nadal wydają się złośliwe reklamy w witrynach dla dorosłych.

Rysunek 2: Zlokalizowane policyjne oprogramowanie do wymuszania okupu

Rozkład geograficzny

Oprogramowanie policyjne wykorzystuje zlokalizowane komunikaty, aby przekonać użytkowników zainfekowanych komputerów. Zarówno Reveton, jak i Urausy operują w kilku krajach, takich jak Wielka Brytania, Niemcy, Francja, Arabia Saudyjska i Włochy (zob. rysunek 2).

W przeciwieństwie do oprogramowania szyfrującego, ekran blokady oprogramowania policyjnego zawiera logo państwowych organów ścigania i jest często przetłumaczony na lokalny język. Obecnie lista lokalizacji obsługiwanych przez Urausy obejmuje następujące kraje:
Argentyna, Australia, Austria, Belgia, Boliwia, Kanada, Chorwacja, Cypr, Czechy, Dania, Ekwador, Finlandia, Francja, Niemcy, Grecja, Węgry, Irlandia, Włochy, Jordania, Łotwa, Liban, Luksemburg, Malta, Meksyk, Maroko, Holandia, Nowa Zelandia, Norwegia, Palestyna, Polska, Portugalia, Rumunia, Arabia Saudyjska, Słowacja, Słowenia, Hiszpania, Szwecja, Szwajcaria, Turcja, Zjednoczone Emiraty Arabskie, Wielka Brytania, Stany Zjednoczone i Urugwaj

Koszty lokalizacji sprawiają, że poszczególne rodziny oprogramowania wymuszającego okup zapożyczają od siebie zawartość ekranu blokady, przez co trudno jest stwierdzić, która rodzina odpowiada za infekcję, na podstawie wyświetlanego ekranu.

Działanie

Podobnie jak w przypadku oprogramowania szyfrującego, działanie oprogramowania policyjnego jest dość proste. Po infekcji program odczekuje kilka minut, zanim wyświetli ekran blokady. To opóźnienie sprawia, że ofierze jest trudniej stwierdzić, która z odwiedzonych witryn odpowiada za infekcję.

Złośliwe oprogramowanie ma punkt startowy w rejestrze, co gwarantuje, że zostanie uruchomione ponownie po restarcie komputera, zwykle w „trybie awaryjnym". Ekran blokady pojawia się natychmiast po restarcie, przez co usunięcie złośliwego programu jest trudne.

Jak chronić się przed oprogramowaniem wymuszającym okup?

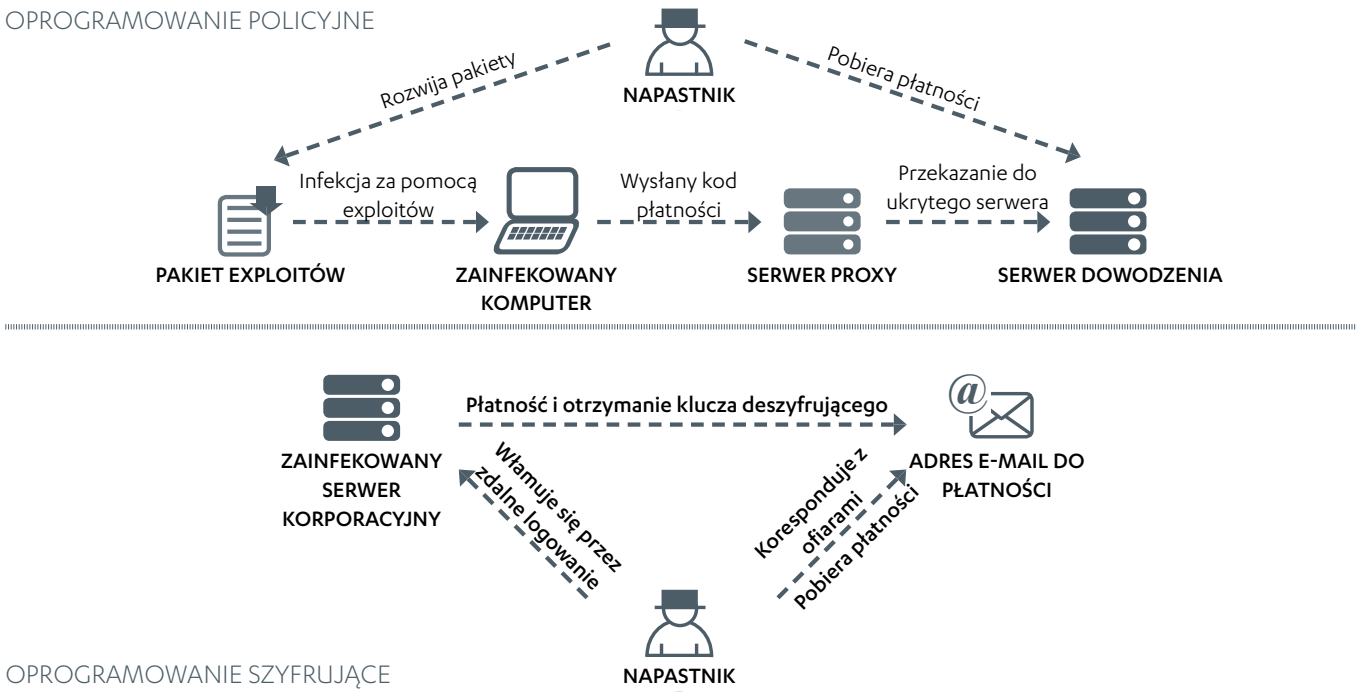
- Włącz ochronę przeglądania i funkcję DeepGuard w swoim produkcie F-Secure, aby omijać z daleka złośliwe witryny
- Aktualizuj oprogramowanie, aby zabezpieczyć się przed pakietami exploitów
- Odinstaluj Javę, jeśli jej nie potrzebujesz, albo zachowaj ją we wtórnej przeglądarce, której nie używasz do codziennego przeglądania sieci
- Jeśli padniesz ofiarą oprogramowania policyjnego, zmień wszystkie hasła, które miałeś zapisane w komputerze
- Regularnie rób kopie zapasowe, aby zabezpieczyć się przed oprogramowaniem szyfrującym. Upewnij się, że kopie nie są dostępne z poziomu samego serwera

Oprogramowanie Reveton ma również drugi moduł, pozwalający napastnikowi zarabiać na ofiarach, które odmawiają zapłacenia okupu. Moduł ten automatycznie wykrada nazwy użytkownika i hasła zapisane w przeglądarce internetowej, klientach FTP i innych programach. Napastnik może wykorzystać te dane albo odsprzedać je komuś innemu.

Mechanizm płatności

W przeciwieństwie do oprogramowania szyfrującego, niemal każdy program policyjny wykorzystuje w pełni zautomatyzowane metody płatności. Na ekranie blokady użytkownik może wprowadzić kod PIN do systemu płatności online, takiego jak Moneypak, Paysafecard lub Ukash. Kod ten jest automatycznie wysyłany do serwera dowodzenia w celu weryfikacji. Infrastruktura dowodzenia składa się z kilku serwerów proxy, których zadaniem jest zatarcie śladów napastnika. Ze względu na wysoki stopień automatyzacji przestępcy, którzy używają tego typu oprogramowania wymuszającego okup, mogą brać na cel tysiące ofiar i bez najmniejszych problemów obsługiwać płatności.

SCHEMAT DZIAŁANIA OPROGRAMOWANIA SZYFRUJĄCEGO I POLICYJNEGO



Oprogramowanie wymuszające okup i bitmonety w Azji

Większość wykrytych przez nas przypadków wymuszania okupu miała miejsce w Europie, na Bliskim Wschodzie i w Stanach Zjednoczonych.

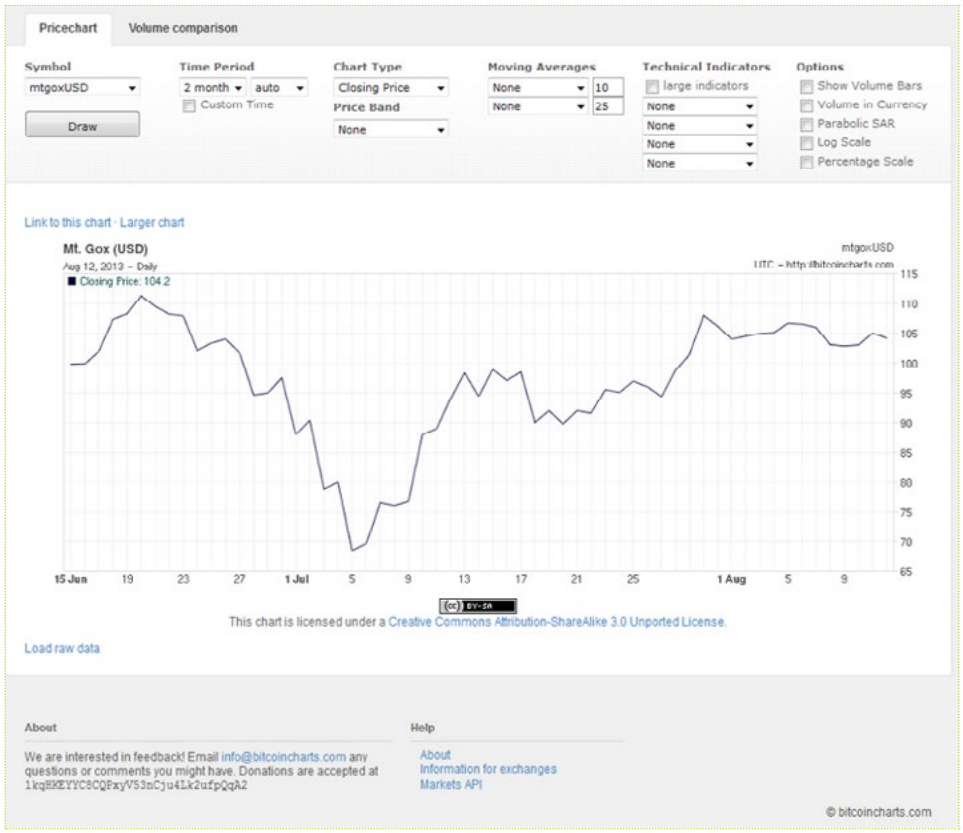
Jednak w regionie azjatyckim nie zaobserwowaliśmy zbyt wielu prób użycia oprogramowania wymuszającego okup do wyłudzania pieniędzy od ofiar, prawdopodobnie dlatego, że nie ma tu wygodnych i anonimowych systemów płatności, takich jak Ukash, Moneypak i Paysafecard. W Europie systemy te pozwalają ofierze łatwo kupić przedpłaconą kartę w sklepie i wykorzystać do zapłacenia okupu (nie informując władz o wymuszeniu, zwłaszcza w przypadku oprogramowania policyjnego). Odbiorcę po drugiej stronie również można łatwo przeszkolić bez podawania zbyt wielu informacji osobistych, a dzięki automatyzacji może on przyjmować okupy od setek, a nawet tysięcy ofiar.

W Azji większość krajów nie ma takiego systemu elektronicznych płatności (być może ze względu na dużą ilość oszustw w tej części świata), a ofiary dotychczas musiały używać bankowości internetowej do elektronicznego transferu funduszy. Skoro jednak bitmonety cieszą się w Azji coraz większą popularnością z powodu swojej pseudo-anonimowej natury, czy w przyszłości napastnicy spróbują podbić tę część świata za pomocą oprogramowania, które będzie przyjmować okup w wirtualnej walucie?

Chiny są obecnie drugim największym oraz najszybciej rosnącym rynkiem bitmonet na świecie i ustępują tylko Stanom Zjednoczonym. Wirtualne waluty są tu znane dzięki monecie Q wprowadzonej w połowie lat dwutysięcznych przez portal Tencent (wszystko zaczęło się od zakupów awatarów w sieci) i gry internetowe. Ponieważ w Chinach ścisła kontrola finansowa utrudnia wydawanie pieniędzy w zagranicznych sklepach, bitmonety mogą okazać się idealną wirtualną walutą dla Chińczyków, ponieważ można przekształcić ją w waluty, które są akceptowane przez takie witryny jak Paypal i Amazon.

Ponieważ system Bitcoin jest całkowicie zdecentralizowany, rządowi byłoby bardzo trudno wtrącać się w jakiekolwiek kwestie związane z użyciem bitmonet, których nie da się prześledzić, zablokować ani wyeliminować z obiegu. Dla cyberprzestępców byłby to idealny sposób na bezpieczne przekazywanie i pranie pieniędzy zgromadzonych za pomocą oprogramowania wymuszającego okup.

Komputery PC to nie jedyna platforma, która w przyszłości będzie atakowana przez oprogramowanie wymuszające okup. Rosnąca liczba użytkowników Androida, zwłaszcza w Azji, skłania twórców złośliwego oprogramowania do rozszerzenia działalności również na platformy mobilne, przez co szkodliwe programy do Androida stają się coraz bardziej zaawansowane. Najistotniejsza jest rosnąca liczba fałszywych antywirusów oraz programów wymuszających okup, które trafiają na platformę mobilną. Po instalacji w urządzeniu fałszywe antywirusy wyświetlają komunikat o rzekomym wykryciu zagrożenia. Ma on skłonić użytkownika do zapłacenia za oprogramowanie, które usunie „infekcję", co przynajmniej duchowo przypomina metody programów wymuszających okup.



Rosnąca wartość bitmonet w stosunku do amerykańskiego dolara

Ponieważ Azja jest jednym z największych rynków smartfonów i bezpłatnych aplikacji pobieranych z niezależnych sklepów, prawdopodobnie w przyszłości będzie tu działać więcej twórców złośliwego oprogramowania, próbujących znaleźć kreatywne sposoby na infekowanie urządzeń mobilnych fałszywymi antywirusami albo oprogramowaniem wymuszającym okup.

WYDOBYWANIE KRYPTOWALUT

Operacje wydobywania kryptowalut trwają od wielu lat. Dwie czołowe waluty, Bitcoin i Litecoin, stały się świętym Graalem organizacji cyberprzestępczych, które potrzebują strumienia trudnych do wyśledzenia przychodów. Jako waluta zdecentralizowana, bitmonety są dokładnie tym, na co zawsze czekali.

Rozwój złośliwego oprogramowania do wydobywania bitmonet, 2008–2012

W 2008 matematyk Satoshi Nakamoto (pseudonim) nadesłał pracę na konferencję poświęconą kryptografii. W artykule technicznym pod tytułem „Bitcoin: A Peer-to-Peer Electronic Cash System" opisał sieć typu peer-to-peer, w której uczestniczące systemy wykonują skomplikowane obliczenia matematyczne na tak zwanym „łańcuchu bloków". System miał na celu stworzenie zupełnie nowej waluty — kryptowaluty – opartej na matematyce.

Bitmonety nie są związane z żadną istniejącą walutą, więc ich wartość zależy wyłącznie od tego, jak oceniają ją ludzie. Niektórzy sprzedawcy przyjmują bitmonety jako środek płatniczy. Przekazywanie bitmonet przypomina wysyłanie wiadomości e-mail. Wszystko, czego potrzeba do natychmiastowego przelania pieniędzy, z pominięciem kantorów, banków i urzędów podatkowych, jest adres powiązany z czyimś plikiem portfela. Kryptowaluty mogłyby sprawić, że banki przestaną być potrzebne do przekazywania pieniędzy. Właśnie dlatego pomysł ten bardzo im się nie podoba.

W 2010 r., kiedy z bitmonet zaczęli korzystać pierwsi entuzjaści, ich wartość wynosiła zaledwie kilka dolarów. Przy takim kursie wielu wątpiło, czy będą one dobrą inwestycją. Kiedy jednak temat został nagłośniony przez media, wartość bitmonet wystrzeliła w górę. To bez wątpienia przykuło uwagę przestępców.

Pierwsze złośliwe programy, które wykorzystywały procesor zainfekowanego komputera do obliczeń związanych z bitmonetami, odkryto w 2011 r. Obliczenia, zwane „wydobywaniem" (mining), nagradzały twórców złośliwego oprogramowania monetami. Taktyka ta nie przyniosła jednak takich dochodów, jakich początkowo spodziewali się autorzy. W drugim kwartale 2011 r. liczba tych złośliwych programów spadła. Ich twórcy doszli do wniosku, że bardziej opłaci się po prostu sprzedawać dostęp do zainfekowanych komputerów, niż samemu wydobywać monety

W krótkim czasie autorzy złośliwego oprogramowania zdołali zaadaptować kod w taki sposób, aby efektywniej wydobywać monety. W czwartym kwartale 2011 r. niektóre rodziny złośliwego oprogramowania, takie jak Trojan.Badminer opisany przez firmę Symantec[1], zaczęły używać programów wydobywczych, które specjalizują się w obliczeniach przyspieszanych za pomocą procesora graficznego (GPU). Korzystanie z GPU jest 50 razy bardziej zyskowne, niż używanie najlepszego procesora głównego (CPU), więc cyberprzestępcy szybko przestawili się na tę metodę.

Rysunek 1: Niestandardowe narzędzie wydobywcze na sprzedaż

Do często używanych programów wydobywczych należą bfgminer/cgminer, cudaminer i Ufasoft's Coin. Są to programy o otwartym kodzie źródłowym, a autorzy złośliwego oprogramowania starają się trzymać ich publicznych kompilacji, aby uniknąć ukierunkowanych detekcji sygnaturowych.

Niektóre cybergangi używają niestandardowych narzędzi wydobywczych, często pisanych przez niezależnych deweloperów, którzy wolą pozostawać w „szarej strefie". Przykładami takich narzędzi są Silent Miner, Chrome Miner i Insidious Miner. Silent Miner nadal ma działającą witrynę internetową, gdzie można go kupić za zwykłe pieniądze za pośrednictwem PayPala albo za bitmonety poprzez serwis Mt. Gox.

Rozwój złośliwego oprogramowania do wydobywania bitmonet, pierwsza połowa 2013 r.

W 2013 r. zaczęły pojawiać się różne złośliwe programy do wydobywania bitmonet, o czym donosili producenci antywirusów. Oto wydarzenia szczególnie godne uwagi:

- **Kwiecień 2013** - Wśród użytkowników Skype'a szerzyła się wiadomość ze złośliwym łączem. Łącze prowadziło do złośliwego pliku wykonywalnego, który pobierał dodatkowe komponenty z serwera dowodzenia. Jednym ze zidentyfikowanych komponentów było narzędzie do

wydobywania bitmonet, które działało po cichu w tle.

- **Maj 2013** - Złośliwe oprogramowanie wydobywcze używało pliku automatycznej konfiguracji serwera proxy (Proxy Auto-Configuration, PAC), aby przekierowywać zainfekowane ofiary do fałszywej witryny Mt. Gox. Przeglądarka internetowa ofiary kontaktowała się z należącym do przestępców serwerem proxy w sposób zdefiniowany w pliku PAC. Próba przejścia do oryginalnej witryny Mt. Gox kończyła się przekierowaniem do fałszywej witryny działającej na serwerze przestępców[2].
- **Czerwiec 2013** - Cyberprzestępcy rozpowszechniali ukierunkowany spam, który prowadził do fałszywej witryny Mt. Gox. Adres URL tej witryny zawierał podobną nazwę domenową drugiego poziomu, „mtgox", ale inne domeny pierwszego poziomu — „.org", „.net". „.co.uk" oraz „.de". Trik ten był łatwiejszy do wykrycia, niż złośliwy plik PAC[3].
- **Koniec czerwca 2013** - Badacze z firmy Webroot odkryli na podziemnym rynku najnowsze narzędzie do tworzenia programów wydobywczych. Program generowany przez to narzędzie rzekomo miał być utajniony i niewidoczny. Na podstawie analizy próbki stwierdziliśmy, że przestępcy użyli programu wydobywczego firmy Ufasoft, który jest dostępny bezpłatnie w oficjalnej witrynie[4].

Oszacowanie zysków botnetu ZeroAccess

Największa dotychczas operacja wydobywcza była dziełem botów z rodziny ZeroAccess. To złośliwe oprogramowanie składa się z zaawansowanego rootkita, który ukrywa jego obecność, oraz tak zwanych „wtyczek". Podczas gdy wolniejsze komputery przydają się do oszukiwania na kliknięciach, szybsze czasem otrzymują dodatkową wtyczkę do wydobywania bitmonet.

Aby obliczyć, jakie zyski może przynieść operacja wydobywcza, poczyńmy kilka założeń:

- Według sondażu przeprowadzonego przez Valve Corporation w maju 2013 r.[5] gracze najczęściej używają kart graficznych NVIDIA 400/500/600 oraz AMD 5000/6000, które pozwalają obliczać około 225 megahaszy/s na typowym komputerze gracza.
- Podejrzewa się, że ZeroAccess infekuje około 100 000 komputerów dziennie. Każdego miesiąca botnet składa się z 3-5 mln aktywnych instalacji; w danym przedziale czasu w działalności wydobywczej może brać udział około 2 mln komputerów (połowa botnetu).
- Jeśli 5 proc. spośród nich (prawdopodobnie więcej) to komputery graczy, proste obliczenie daje nam 22 500 000 megahaszy/s:
  $(2x10^6)\ (0.05)\ (225\ \text{Megahaszy/s}) = 22.5x10^6\ \text{Megahaszy/s}$
- Przy obecnych cenach (100 USD = 1 BTC)[7] i trudności wydobywania równej 19 339 258 napastnicy mogą zarabiać następującą kwotę:

TABELA 1: SZACUNKOWY ZYSK Z DZIAŁALNOŚCI WYDOBYWCZEJ ZEROACCESS

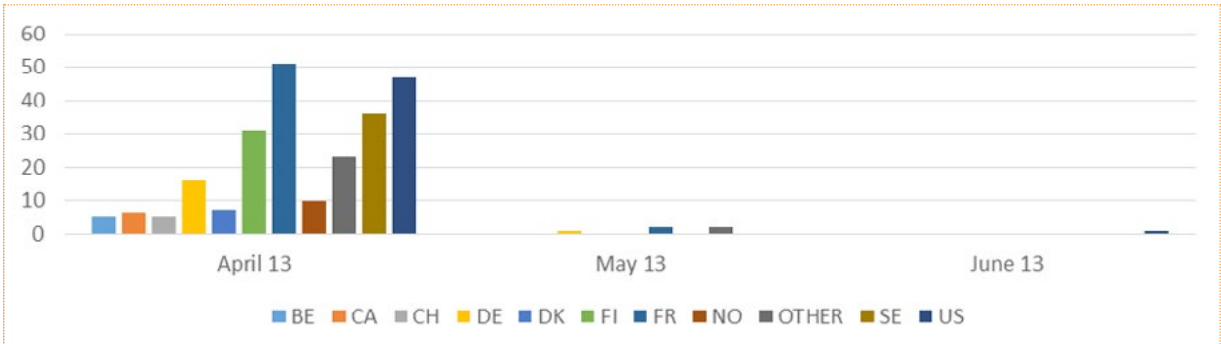
	USD ($)	BTC (฿)
Dzienny zysk	58,913	585
Tygodniowy zysk	412,295	4,095
Miesięczny zysk	1,790,976	17,787

Przy miesięcznym zysku wynoszącym 1,7 mln dol. z 5 proc. ofiar, działalność wydobywcza napędzana przez ZeroAccess bez wątpienia jest lukratywną opcją dla cyberprzestępców.

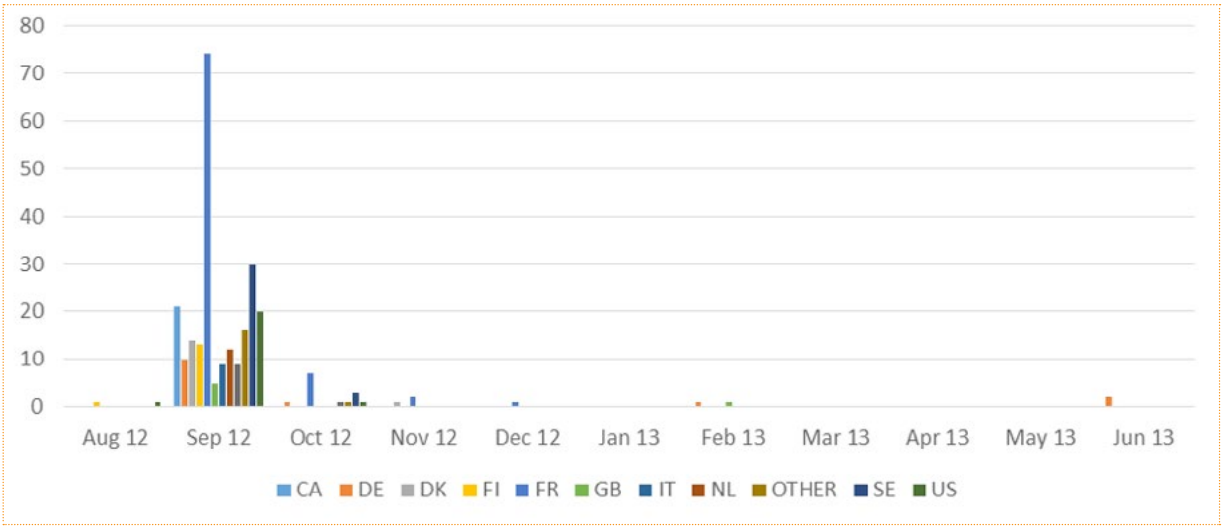
Aktualizacje wtyczki ZeroAccess do wydobywania bitmonet

Operator botnetu ZeroAccess od pewnego czasu często aktualizuje wtyczkę odpowiedzialną za wydobywanie bitmonet. Co ciekawe, choć wtyczka Bitcoin jest nadal aktywnie aktualizowana i dostarczana do zainfekowanych komputerów, z jej pliku binarnego zniknął kod wydobywczy.
Na podstawie próbek zgromadzonych przez nasze systemy zaplecza ustaliliśmy historię aktualizacji binarnego pliku wtyczki Bitcoin. Data wydania pliku pochodzi z czasowego znacznika kompilacji. Aktualizacja jest zwykle wydawana co miesiąc, ale w kilku przypadkach operator botnetu wydłużył ten okres do dwóch miesięcy. Botnet używa prywatnego serwera

KRAJE ZAATAKOWANE PRZEZ WTYCZKĘ BITCOIN WYDANĄ W KWIETNIU 2013 R.



KRAJE ZAATAKOWANE PRZEZ WTYCZKĘ BITCOIN WYDANĄ W SIERPNIU 2012 R.



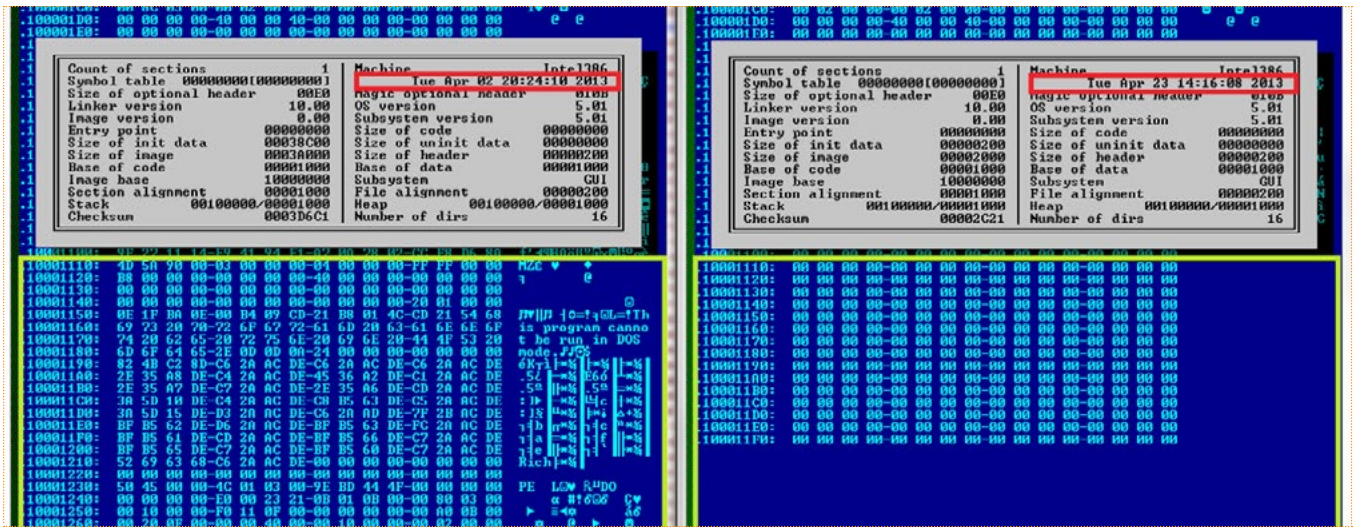
puli do rozpowszechniania bloku kryptograficznego, który mają rozwiązać węzły robocze — zainfekowane komputery z wtyczką wydobywczą. Serwer puli używany przez wtyczkę Bitcoin, którą wydano w sierpniu 2012 r., został zidentyfikowany jako „google-updaete[kropka]com". Od września 2012 r. do kwietnia 2013 r. operator botnetu wypuszczał binarny plik wtyczki, który nie zawiera kodu wydobywczego.

TABELA 2: DATY WYDANIA WTYCZKI BITCOIN

Data kompilacji pliku binarnego	Zawiera kod do wydobywania bitmonet?	
	TAK	NIE
Sierpień 2012	x	
Wrzesień 2012		x
Listopad 2012		x
Grudzień 2012		x
Luty 2013		x
Marzec 2013		x
Kwiecień 2013	x	

2 kwietnia 2013 r. operator botnetu wydał nową wtyczkę Bitcoin, w której ponownie pojawił się kod do wydobywania bitmonet używający innego prywatnego serwera puli, „ooyohrmebh9qfof[kropka] com". Ten plik binarny, zawierający kod wydobywczy, nie przetrwał długo. Zrzut ekranowy na rysunku 3 pokazuje porównanie między starszą i nowszą wersją wtyczki Bitcoin, które pochodzą z jednego miesiąca. Plik po prawej stronie to najnowsza wtyczka, zbudowana 23 kwietnia 2013 r. Żółty prostokąt pokazuje, że osadzony, spakowany narzędziem UPX plik binarny Utasoft Coin zniknął z pliku wtyczki. Innymi słowy, od 23 kwietnia do dziś (dnia, w którym napisano ten artykuł) ZeroAccess nie zawiera kodu do wydobywania bitmonet.

Brak kodu wydobywczego nie oznacza jednak, że operator przestał czerpać zyski ze swojego botnetu. Nadal funkcjonuje kod do oszukiwania na kliknięciach, który znajduje się w tym samym binarnym pliku wtyczki. Nie wiadomo, dlaczego operator botnetu zrezygnował z funkcji wydobywania bitmonet pomimo korzystnego kursu wymiany. Można jednak snuć pewne przypuszczenia:



Rysunek 2: Porównanie starszej i nowszej wersji wtyczki Bitcoin

- skonfigurowanie i utrzymanie własnego serwera puli prywatnej jest zbyt kosztowne,
- wydobywanie bitmonet na zainfekowanej maszynie jest zbyt natarczywe i głośne,
- niełatwo jest wygenerować bitmonetę bez użycia dedykowanego komputera, zwłaszcza kiedy operator botnetu domyślnie wyłącza akcelerację GPU.

Podsumowanie

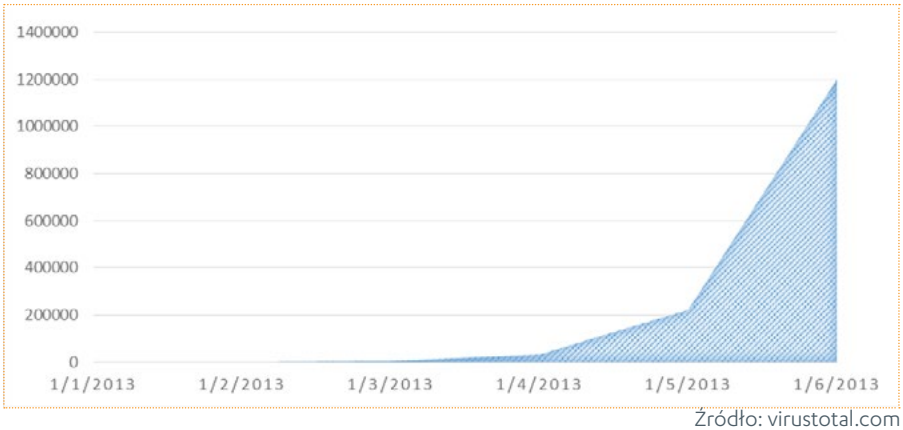
Trudno ocenić światowy zasięg infekcji, ponieważ napastnicy używają powszechnie dostępnych narzędzi wydobywczych, które mogły, ale nie musiały zostać zainstalowane bez zgody użytkownika. Zdołaliśmy jednak policzyć próbki związane z wydobywaniem bitmonet dla każdego miesiąca pierwszej połowy 2013 r.

Jak można się było spodziewać, wykres odzwierciedla (z niewielkim opóźnieniem) kurs wymiany BTC podawany przez kantor Mt. Gox.

Od czasu wprowadzenia bitmonet w 2009 r. istniały dwa typy złośliwego oprogramowania do czerpania zysków z wirtualnej waluty. Pierwszy to warianty, które wykradają ofiarom pliki portfela Bitcoin. Drugi to warianty, które wykonują legalne programy wydobywcze na zainfekowanych komputerach, umożliwiając bicie monet bez płacenia za sprzęt ani elektryczność. Najwyraźniej cyberprzestępcy zrezygnowali z pierwszego typu ataku z powodu dodatkowej funkcji zabezpieczającej w kliencie Bitcoin. Funkcja ta szyfruje plik „wallet.dat", przez co jest on bezwartościowy dla napastników, którzy nie zdołali przechwycić hasła przez rejestrowanie naciśnięć klawiszy.

Przy obecnych trendach nie będzie niczym dziwnym, jeśli w przyszłości pojawi się więcej złośliwego oprogramowania drugiego typu. Trudno jednak ocenić potencjalne przychody, ponieważ programy te rozprzestrzeniają się w inny sposób i często używają „wydobywania p2pool", w którym każdy zainfekowany komputer wydobywa monety „solo" na wskazany adres portfela. Typowe wektory infekcji takim oprogramowaniem to Skype i inne komunikatory, poczta e-mail, drive-by-download oraz exploity.

ROZWÓJ ZŁOŚLIWEGO OPROGRAMOWANIA DO WYDOBYWANIA BITMONET



Źródło: virustotal.com

Źródło: mtgox.com

PAKIETY EXPLOITÓW

W ciągu kilku ostatnich lat pakiety exploitów stały się popularnym, wygodnym narzędziem, za pomocą którego napastnicy i dystrybutorzy złośliwego oprogramowania efektywnie wynajdują nowe ofiary. W pierwszej połowie 2013 r. obserwowaliśmy szybki rozwój pakietów exploitów oraz nasilającą się konkurencję między nimi. Pojawili się nowi pretendenci, a starsze, ugruntowane pakiety rozbudowano o nowe cele ataku i nowe sposoby unikania wykrycia.

Pięć czołowych pakietów exploitów

Według danych telemetrycznych F-Secure za 70 proc. wszystkich detekcji związanych z pakietami exploitów w pierwszej połowie 2013 r. odpowiadało pięć pakietów: Blackhole, SweetOrange, Crimeboss, Styx i Cool. 28 innych pakietów odpowiada za pozostałe 30 proc. wykryć.

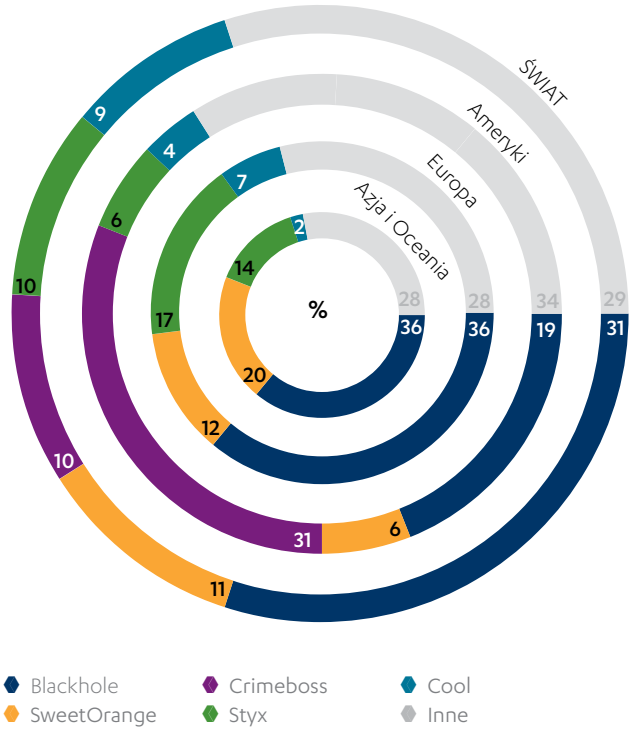
Wśród pięciu czołowych pakietów sam Blackhole odpowiadał za 31 proc. wszystkich detekcji zgłoszonych do naszego chmurowego systemu w tym okresie. Działanie tego pakietu opisaliśmy po raz pierwszy w naszym raporcie na temat zagrożeń w pierwszej połowie 2012 r. Rok później zmieniło się niewiele, jeśli nie liczyć dodania exploitów wymierzonych w nowo opisane luki, takie jak CVE-2013-2423 oraz CVE-2013-0422 (zob. „Wykorzystywanie luk w zabezpieczeniach" na stronie 36), oraz modyfikacji wzorców URL witryn rozpowszechniających exploity.

Jeśli chodzi o pozostałe pakiety z pierwszej piątki, SweetOrange jest najbliższym konkurentem Blackhole i odpowiada za 11 proc. wszystkich światowych detekcji związanych z pakietami exploitów. Geograficzny rozkład klientów, którzy zgłosili te detekcje (wykres po prawej stronie), wskazuje, że choć większość pakietów operuje w każdym regionie (zwłaszcza Blackhole, praktycznie wszechobecny), to Crimeboss skupia się niemal wyłącznie na Amerykach, gdzie odpowiadał za 31 proc. wszystkich detekcji związanych z pakietami exploitów.

Nowi gracze

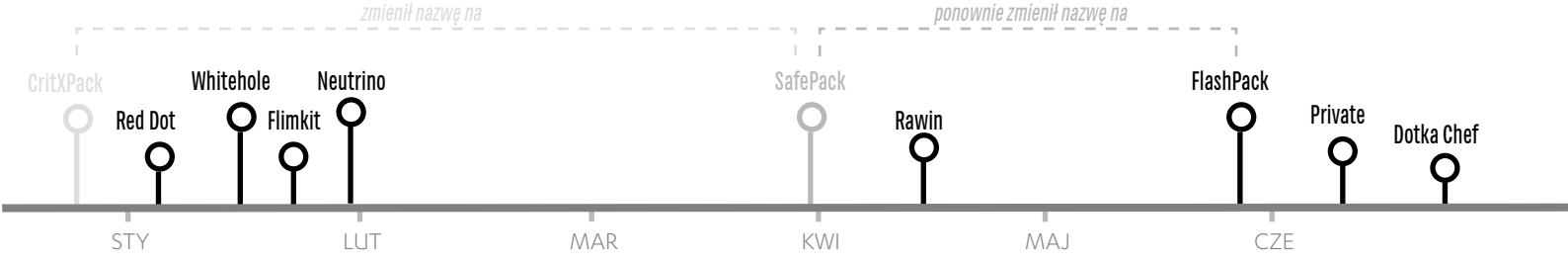
IW ciągu sześciu miesięcy zaobserwowaliśmy siedem nowych pakietów exploitów (zob. oś czasu na dole), a starszy pakiet CritXPack, znany też jako SafePack i FlashPack, pojawiał się pod nowymi nazwami. Choć pakiety te odniosły umiarkowany sukces w porównaniu z Blackhole, a nawet SweetOrange, rosnąca liczba aktywnych pakietów exploitów zapewnia jeszcze więcej opcji dystrybutorom złośliwego oprogramowania. W nowej grupie szczególnie godny uwagi jest pakiet Whitehole, który skupia się na lukach w deweloperskiej platformie Javy.

GEOGRAFICZNA DYSTRYBUCJA 5 CZOŁOWYCH PAKIETÓW EXPLOITÓW W 1. POŁOWIE 2013 R., PROCENTOWO



W drugiej połowie 2013 r. 31 proc. naszych klientów z całego świata zgłosiło wykrycie ataku Blackhole, co oznacza, że jest to najbardziej rozpowszechniony pakiet exploitów.

NOWE PAKIETY EXPLOITÓW NAPOTKANE W 1. POŁOWIE 2013 R. WG DATY PIERWSZEGO WYKRYCIA



W 1. połowie 2013 r. zaobserwowaliśmy serię nowych pakietów exploitów

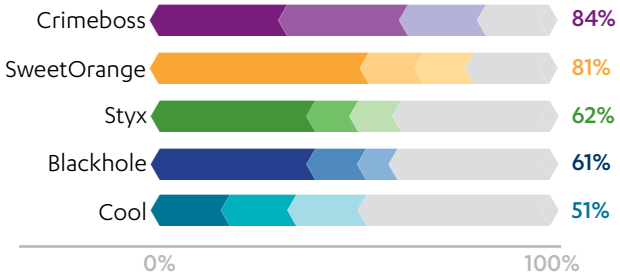
Ataki na niedawno nagłośnione luki w zabezpieczeniach

Jak już wspomniano, twórcy pakietów exploitów zwykle szybko dodają do swoich produktów exploity wymierzone w nowo ogłoszone luki. Tak było również w pierwszej połowie 2013 r. Przykładem może być luka CVE-2013-2423 w zabezpieczeniach Javy; wymierzony w nią moduł Metasploit został opublikowany 20 kwietnia, a dzień później odkryliśmy, że pakiet CrimeBoss już zaczął atakować tę lukę.

Ponadto nowy pakiet exploitów, Private, jako pierwszy zaczął wykorzystywać lukę CVE-2013-1347 w 8. wersji Internet Explorera. Ta szczególna luka znalazła się w centrum uwagi z powodu włamania do witryny Departamentu Pracy Stanów Zjednoczonych na początku maja 2013 r.; zaledwie kilka dni później Microsoft wydał odpowiednią poprawkę. Miesiąc później, 11 czerwca, pakiet Private Pack zaczął już wykorzystywać tę lukę.

W lipcu 2013 r. przynajmniej pięć luk, które zostały ogłoszone publicznie w minionym półroczu, trafiło do różnych pakietów exploitów. Cztery spośród pięciu luk — CVE-2013-0422, CVE-2013-0431, CVE-2013-1493 i CVE-2013-2423 — były związane z deweloperską platformą Javy. Exploity te są identyfikowane przez różne detekcje w naszych produktach zabezpieczających, w tym przez specyficzne detekcje Exploit:Java/CVE-2013-2423.A i Exploit:Java/CVE-2013-2423.B, a także przez zaawansowaną detekcję ogólną, Exploit:Java/Majava.C.

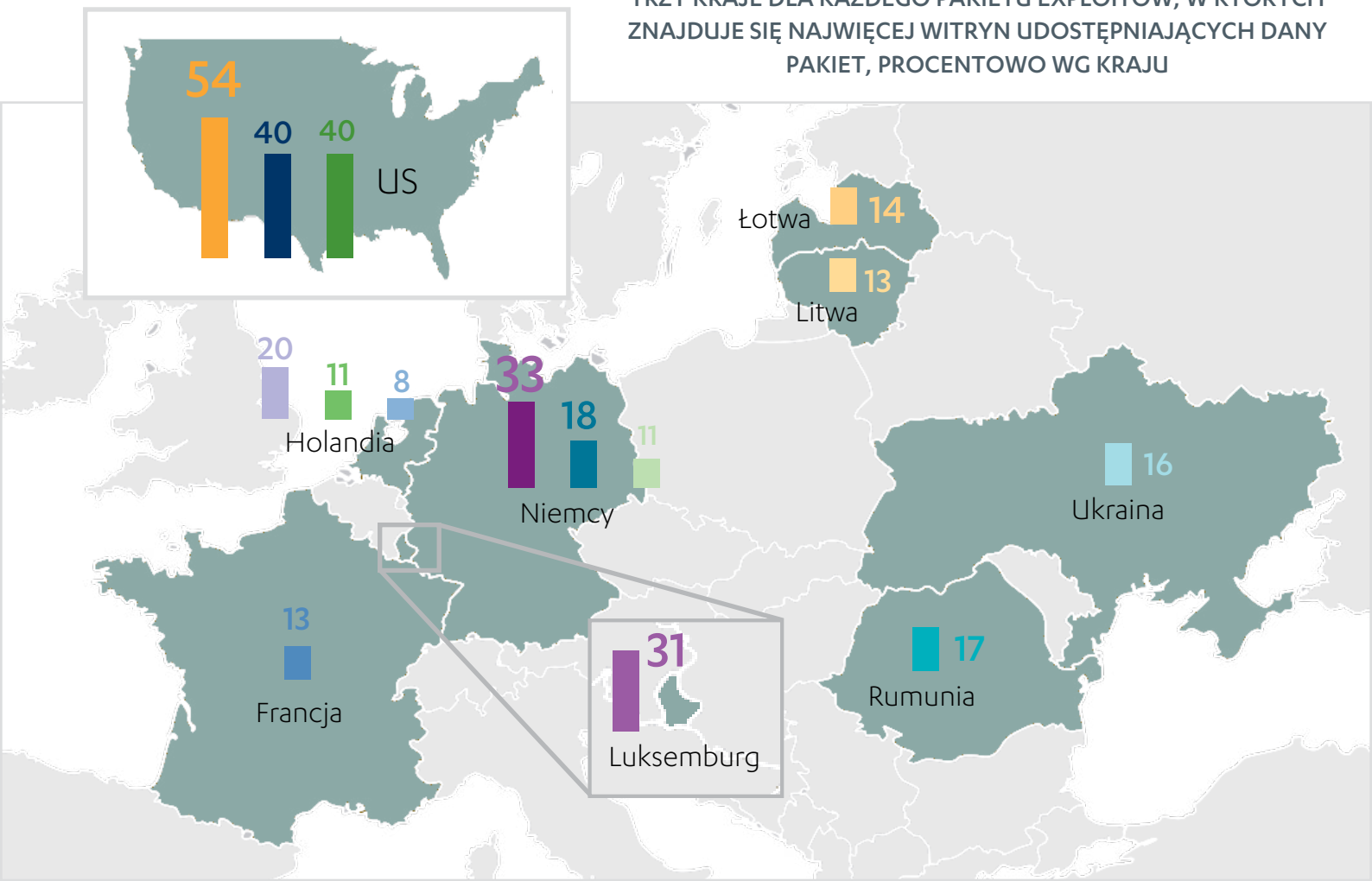
TRZY KRAJE DLA KAŻDEGO PAKIETU EXPLOITÓW, W KTÓRYCH ZNAJDUJE SIĘ NAJWIĘCEJ WITRYN UDOSTĘPNIAJĄCYCH DANY PAKIET, PROCENT ŁĄCZNEJ LICZBY WITRYN



Nowe triki

Ponieważ wiele pakietów exploitów skupia się na atakowaniu Javy, nic dziwnego, że w ciągu minionych sześciu miesięcy firma Oracle wydawała aktualizacje, które zamykały luki w zabezpieczeniach i ogólnie zwiększały stopień bezpieczeństwa produktu. Szczególnie godna uwagi była wersja Java 7 Update 11, która nie tylko załatała lukę CVE-2013-0422, ale również zwiększyła domyślny poziom zabezpieczeń Javy z „średniego" na „wysoki". Zmiana to oznacza, że przed uruchomieniem apletu pojawia się okno ostrzegawcze, w którym użytkownik musi kliknąć przycisk „Uruchom". W odpowiedzi napastnicy zmienili metody i omijają tę funkcję, wczytując serializowane aplety albo pliki Java Network Launch Protocol (jnlp).

TRZY KRAJE DLA KAŻDEGO PAKIETU EXPLOITÓW, W KTÓRYCH ZNAJDUJE SIĘ NAJWIĘCEJ WITRYN UDOSTĘPNIAJĄCYCH DANY PAKIET, PROCENTOWO WG KRAJU



Kolejny trik, który wprowadzono w pierwszej połowie 2013 r., polega na tym, że kilka pakietów exploitów, m.in. Neutrino, Sakura i Redkit, zaczęło szyfrować swój kod binarny algorytmem XOR lub AES, aby uniknąć wykrycia.

Hosting witryn z exploitami

Użytkownicy zwykle napotykają pakiety exploitów podczas przeglądania sieci, kiedy odwiedzają zainfekowaną stronę albo zostają przekierowani do złośliwej witryny. Większość witryn rozpowszechniających pakiety exploitów znajduje się w Stanach Zjednoczonych i Europie. Znaczna część wszystkich witryn z exploitami działa w trzech krajach — Stanach Zjednoczonych, Niemczech i Holandii.

Niektóre pakiety exploitów preferują hosting w określonych krajach. 84 proc. wszystkich witryn z pakietem Crimeboss znajduje się zaledwie trzech krajach — Niemczech, Luksemburgu i Holandii. Tymczasem w Stanach Zjednoczonych działa 54 proc. witryn, które rozpowszechniają pakiet SweetOrange, a także 40 proc. witryn z pakietami Blackhole i Styx. Śledzenie adresów IP związanych z pakietami pozwoliło zidentyfikować numery systemów autonomicznych (ASN) zaangażowanych w hosting witryn z exploitami. Na przykład 14 proc. adresów IP pakietu Blackhole, 12 proc. adresów pakietu Styx i 7 proc. adresów pakietu Cool prowadzi do systemu AS16276 zarządzanego przez OVH Systems.

Ochrona przed pakietami exploitów

Jeśli chodzi o ochronę przed pakietami exploitów, zwykle doradza się szybkie aktualizowanie narażonych systemów, kiedy tylko producent wyda odpowiednie poprawki. Jednak w przypadku zagrożeń dnia zerowego najskuteczniejsze jest ograniczenie „powierzchni ataku" każdego systemu podłączonego do internetu. Wymaga to wielowarstwowej „głębokiej obrony" i obejmuje takie elementy, jak zabezpieczenia przeglądarki, skanowanie ruchu WWW, filtrowanie poczty e-mail oraz dobrze zaimplementowane systemy wykrywania i zapobiegania włamaniom. Rady dotyczące ochrony systemu przed pakietami exploitów podano w ramce „Rekomendacje" na stronie 39.

WYKORZYSTYWANIE LUK W ZABEZPIECZENIACH

W pierwszej połowie 2013 r., podobnie jak w 2012 r., wykorzystywanie luk w zabezpieczeniach pozostawało popularnym sposobem na uzyskanie dostępu do komputera ofiary, czy to w celu zainstalowania złośliwego oprogramowania, czy też podjęcia jakichś innych niegodziwych działań. W tym artykule przyjrzymy się kilku interesującym trendom, które zaobserwowaliśmy w ciągu pierwszych sześciu miesięcy 2013 r.

Nacisk na zagrożenia dnia zerowego

Przez większą część 2012 r. obserwowaliśmy głównie ataki wymierzone w luki, które były publicznie znane od pewnego czasu, często od lat. Na przykład jedną z najczęściej atakowanych luk była usterka CVE-2010-0288 w programach Adobe Reader i Acrobat, którą odkryto dwa lata wcześniej.

W 2013 r. zauważyliśmy jednak rosnący nacisk na wykorzystywanie luk dnia zerowego, które nie zostały jeszcze załatane przez producenta narażonej aplikacji. W tym okresie nasze dane telemetryczne wskazywały, że aż 95 proc. zgłaszanych detekcji, które identyfikowały ataki na konkretne luki w zabezpieczeniach, było wymierzonych w zaledwie pięć luk, przy czym spośród tych pięciu najczęściej atakowanych luk trzy zostały ogłoszone publicznie w ciągu minionych sześciu miesięcy. Nie przypadkiem każda z tych pięciu luk jest znanym celem różnych pakietów exploitów (zob. artykuł „Pakiety exploitów" na stronie 34).

CVE-2011-3402 — najczęściej atakowana luka w zabezpieczeniach

W pierwszej połowie 2013 r. zdecydowanie najczęściej atakowano lukę CVE-2011-3402 (usterkę w obsłudze czcionek TrueType w systemie Windows). O luce tej po raz pierwszy zrobiło się głośno, kiedy została wykorzystana przez złośliwe oprogramowanie Duqu w ukierunkowanej kampanii na początku 2012 r.; pod koniec 2012 r. dodano ją do różnych pakietów exploitów. Od tego czasu liczba ataków na tę jedną lukę niebotycznie wzrosła, a w minionym półroczu odpowiadała ona za 69 proc. wszystkich zgłoszonych detekcji związanych z exploitami.

Java — drugi najczęściej atakowany program

Spośród pięciu najczęściej atakowanych luk cztery znajdują się w deweloperskiej platformie Javy, albo w środowisku uruchomieniowym (JRE), albo w dodatku do przeglądarki. Nie ma w tym nic dziwnego, ponieważ obok systemu operacyjnego Windows (również popularnego celu exploitów) Java jest prawdopodobnie drugim najbardziej rozpowszechnionym programem w środowisku IT przeciętnej organizacji.

Jednak w pierwszej połowie 2013 r. problemy z bezpieczeństwem Javy przyciągnęły niepożądaną uwagę po serii skutecznych ataków na duże firmy technologiczne i medialne, takie jak Facebook, Twitter, Apple i NBC, spośród których część potwierdziła, że za włamania do ich systemów odpowiadał exploit dnia zerowego wymierzony w Javę.

Aby zwalczyć narastające problemy z bezpieczeństwem, w minionym półroczu firma Oracle wydała kilka poprawek, a także zwiększyła domyślny poziom zabezpieczeń Javy na „wysoki". Samo Oracle zaleca, aby instalować te poprawki najszybciej, jak to możliwe, ponieważ wiele usterek usuwanych przez aktualizacje ma krytyczną naturę. Ponadto różne firmy specjalizujące się w bezpieczeństwie (a także Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych) radzą użytkownikom i organizacjom usunąć niepotrzebne instalacje środowiska uruchomieniowego Javy w celu zabezpieczenia się przez intruzami — a przynajmniej usunąć lub wyłączyć dodatek Javy do przeglądarki, który stanowi pierwszy punkt wejścia do programu.

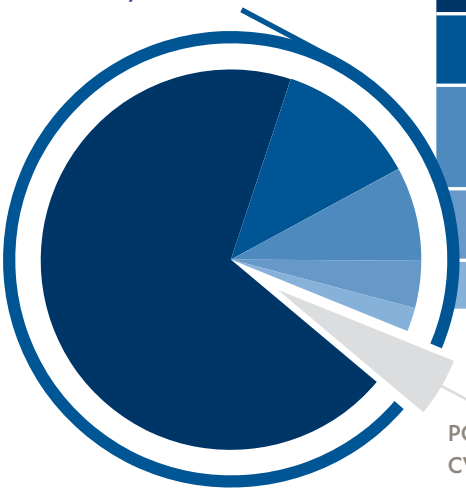
Niestety, usunięcie środowiska uruchomieniowego albo dodatku nie jest sensowną opcją dla firm, które używają Javy do ważnych celów biznesowych. W organizacjach, które stoją przed takim dylematem, alternatywą bywa uszczelnienie zabezpieczeń systemów albo sieci — skuteczniejsze, ale bardziej skomplikowane rozwiązanie, niż proste odinstalowanie programu. Strategie łagodzenia problemu w takich firmach prawdopodobnie będą obejmować modyfikowanie ustawień bezpieczeństwa Javy, skonfigurowanie przeglądarek pod kątem minimalizacji wykonywania niepożądanych apletów (albo zainstalowanie dodatków firm trzecich, które się tym zajmą) oraz monitorowanie ruchu sieciowego.

Geograficzny rozkład ataków na luki w zabezpieczeniach

Prawdopodobnie nie będzie niespodzianką, że krajem, w którym zgłoszono najwięcej ataków na luki w zabezpieczeniach, są Stany Zjednoczone. Według naszych danych telemetrycznych w ciągu sześciu minionych miesięcy około 78 na 1000 użytkowników ze Stanów Zjednoczonych odnotowało detekcję, która identyfikowała exploit konkretnej luki.

DETEKCJE EXPLOITÓW W 1. POŁOWIE 2013 R., PODSUMOWANIE

5 luk CVE odpowiada za **95%** wszystich ataków



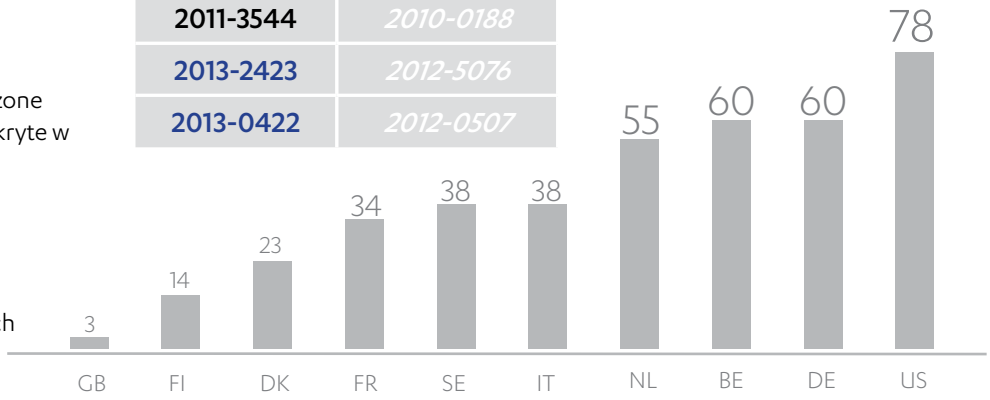
CVE	Narażony program	Uwagi
2011-3402	Windows OS	Atakowana przez wiele pakietów exploitów, zwłaszcza Cool
2013-1493	Java	Wpływa tylko na Javę w przeglądarkach internetowych
2011-3544	Java	Atakowana przez wiele pakietów exploitów, zwłaszcza Blackhole
2013-2423	Java	Atakowana przez wiele pakietów exploitów
2013-0422	Java	Wpływa tylko na JRE 7

Pięć najczęściej wykorzystywanych luk
95 proc. wszystkich ataków na luki w zabezpieczeniach zgłoszonych przez naszych klientów w pierwszej połowie 2013 r. było wymierzonych w 5 luk, z czego 4 w Javie.

H1 2013	2012
2011-3402	2011-3402
2013-1493	*2010-0188*
2011-3544	*2010-0188*
2013-2423	*2012-5076*
2013-0422	*2012-0507*

Stare przemija
3 spośród 5 najczęściej atakowanych luk (oznaczone na niebiesko) zostały odkryte w ostatnich 6 miesiącach

10 najczęściej atakowanych krajów
Według współczynnika powszechności exploitów*, w pierwszej połowie 2013 r. najwięcej ataków na luki w zabezpieczeniach napotkali użytkownicy w Stanach Zjednoczonych, Niemczech i Belgi



*Współczynnik powszechności exploitów na 1000 użytkowników oblicza się, dzieląc łączną liczbę detekcji exploitów przez liczbę klientów w danym kraju, a następnie mnożąc wynik przez 1000

Wiele ataków na luki w zabezpieczeniach występowało również w Niemczech, gdzie około 60 na 1000 użytkowników zgłosiło wykrycie w tym samym okresie. Spośród 10 najczęściej atakowanych krajów wszystkie, oprócz Stanów Zjednoczonych, znajdują się w Europie.

Rosnący rynek na exploity

Od lat często przeoczanym aspektem bezpieczeństwa jest sposób postępowania w przypadku odkrycia luki w zabezpieczeniach, zwłaszcza luki dnia zerowego w popularnej aplikacji. Badacze bezpieczeństwa i producenci aplikacji spierają się, czy najlepszym rozwiązaniem problemu jest utajnienie odkrycia (odpłatne lub nie), czy też jego publiczne ujawnienie w celu zmuszenia deweloperów do poprawienia usterki.

Jest to szczególnie istotne w kontekście coraz aktywniejszego i szybko rosnącego rynku „handlu exploitami”[1], który zasadniczo czerpie zyski z badań nad lukami w zabezpieczeniach poprzez sprzedaż wyników najwyżej licytującemu. Oprócz samego producenta aplikacji inni gracze (kontrahenci rządowi, inni badacze oraz twórcy złośliwego oprogramowania) stają się potencjalnymi nabywcami informacji, którą kiedyś udostępniano bezpłatnie lub za symboliczną kwotę.

Choć sprzedaż exploitów jest legalna, zwykle miała sekretną naturę. Jednak w miarę, jak wykorzystywanie luk w zabezpieczeniach upowszechnia się zarówno w atakach ukierunkowanych, jak i w dystrybucji złośliwego oprogramowania, działalność ta staje się bardziej widoczna, choć nie do końca otwarta. Na początku 2013 r. donoszono[2], że autor pakietu Blackhole/Cool zamieścił na rosyjskim forum cyberprzestępczym ofertę kupna exploitów. Jak wynika z tłumaczenia przytoczonego w doniesieniu, „ekskluzywny program” oferowany przez autora pakietu obejmował też zapłatę za „ulepszenia istniejących publicznych exploitów oraz każde dobre rozwiązanie, które zwiększy współczynnik udanych ataków”.

Rządy podobno również kupują exploity, rzekomo w celu wykorzystania ich do ofensywnych cyberataków[3], pomimo rosnących obaw, że działalność ta w ostatecznym rozrachunku zagrozi bezpieczeństwu i wolnościom cywilnym ich własnych obywateli[4]. Choć żaden rząd nie przyznał otwarcie, że jest aktywnie zaangażowany w kupowanie exploitów, większość raportów sugeruje, że parają się tym agencje amerykańskie i chińskie.

Zwalczanie handlu exploitami

W pierwszej połowie 2013 r. Microsoft uruchomił program „nagród za zgłaszanie usterek”, aby zachęcić badaczy do odpowiedzialnego ujawniania luk w zabezpieczeniach swoich produktów. Firma dołączyła w ten sposób do nielicznych podmiotów (m.in. Facebooka i powiązanej z HP organizacji Zero Day Initiative), które próbują ograniczyć rynek „exploitów na sprzedaż”, oferując zapłatę za informacje o lukach w zabezpieczeniach. Inicjatywy te mają jednak silną konkurencję; raporty sugerują, że niektóre rządy są skłonne płacić sześciocyfrowe sumy zarówno za krytyczne informacje, jak i umowę o zachowaniu odkrycia w tajemnicy, co zasadniczo gwarantuje nabywcy tajny punkt dostępu do interesującego go programu.

Zaangażowanie rządów w handel exploitami przełożyło się również na wstępne rozmowy o wprowadzeniu przepisów, które regulowałyby rynek[5], przynajmniej w Unii Europejskiej. Dopóki jednak nie wejdą one w życie, rynek handlu exploitami prawdopodobnie będzie rósł. Trudno wyrokować, jakie to będzie miało konsekwencje dla cyberbezpieczeństwa, ale organizacje powinny z pewnością przykładać większą uwagę do obrony swoich sieci i systemów przed atakami na luki w zabezpieczeniach.

ŹRÓDŁA

1. Forbes; Bruce Schneier; *The Vulnerabilities Market and the Future of Security*; ; opublikowano 30 maja 2012 r.;
2. http://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/
3. Krebs on Security; Brian Krebs; *Crimeware Author Funds Exploit Buying Spree*; opublikowano 7 stycznia 2013 r.;
4. https://krebsonsecurity.com/2013/01/crimeware-author-funds-exploit-buying-spree/
5. NY Times; Nicole Perlroth i David E. Sanger; *Nations Buying as Hackers Sell Flaws in Computer Code*; opublikowano 13 lipca 2013 r.; http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html
6. Reuters; Joseph Menn; *Special Report: U.S. cyberwar strategy stokes fear of blowback;* opublikowano 10 maja 2013 r.; http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510
7. Slate; Ryan Gallagher; *Cyberwar's Gray Market: Should the secretive hacker zero-day exploit market be regulated?*; opublikowano 16 stycznia 2013 r.; http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html

REKOMENDACJE: Ochrona przed exploitami

1 Instaluj aktualizacje zabezpieczeń

Stosuj poprawki zabezpieczeń, kiedy tylko zostaną udostępnione przez producentów aplikacji. Bardzo utrudni to pakietom exploitów przeprowadzenie udanego ataku na komputer.

Oprócz wprowadzenia konsekwentnego cyklu poprawek (zwłaszcza jeśli dostarczanie ich do użytkowników jest problematyczne) firmy mogą bronić się przed exploitami za pomocą systemu wykrywania i zapobiegania włamaniom (IDS/IPS) wyposażonego w aktualne sygnatury.

15 NAJCZĘŚCIEJ ATAKOWANYCH LUK W ZABEZPIECZENIACH W 1. POŁOWIE 2013 ROKU (WG NUMERU CVE)

CVE	NARAŻONY PROGRAM	OPUBLIKOWANO
2013-2423	Java	16 Kwietnia 2013
2013-1493	Java	4 Marca 2013
2013-1331	Microsoft Office	11 Czerwca 2013 (MS13-051)
2013-0809	Java	4 Marca 2013
2013-0422	Java	13 Stycznia 2013
2012-5076	Java	16 Października 2012
2012-4681	Java	30 Sierpnia 2012
2012-1723	Java	12 Czerwca 2012
2012-0507	Java	17 Maja 2012
2011-3544	Java	18 Października 2011
2011-3402	System Windows	8 Maja 2012 (MS12-034)
2010-0188	Adobe Reader i Acrobat	23 Lutego 2010
2010-0840	Java	30 Marca 2010
2010-1885	System Windows	10 Czerwca 2010 (MS10-042)
2007-5659	Adobe Reader i Acrobat	6 Maja 2008

!! EXPLOITY DNIA ZEROWEGO

Nawet po pełnej aktualizacji programów i zablokowaniu przeglądarek internetowych firmy obawiające się ataków opartych na exploitach powinny wziąć pod uwagę to, że napastnicy mogą wykorzystać nieujawnioną lukę w zabezpieczeniach. W takich przypadkach ostatnią linią obrony jest dobrze zaimplementowana konfiguracja IDS/IPS albo równoważny system, który potrafi identyfikować podejrzaną aktywność na komputerach w chronionej sieci. Choć ogólne rady są tu mniej przydatne, taki system ochrony powinien być unikatową kombinacją monitorowania sieci, zapory oraz białych i czarnych list, dostosowaną do zwykłych potrzeb i środowiska pracy użytkowników.

2 Zminimalizuj „powierzchnię ataku"

Aktualizowanie zabezpieczeń i wykrywanie włamań jest skuteczne przeciwko znanym atakom na już załatane luki. Jednak w przypadku ataków dnia zerowego, na które jeszcze nie znaleziono sposobu, najefektywniejszą ochroną jest minimalizacja „powierzchni ataku" (różnych wektorów, które umożliwiają uruchomienie złośliwego kodu) w każdym systemie podłączonym do internetu.

Dla większości użytkowników „ograniczenie powierzchni ataku" oznacza po prostu uszczelnienie zabezpieczeń przeglądarki internetowej. Dotyczy to zwłaszcza sytuacji, w których odinstalowanie dodatku Javy do przeglądarki (obecnie preferowanego wektora ataku dla wielu pakietów exploitów), nie wchodzi w grę. W takich przypadkach użytkownik może zwiększyć stopień bezpieczeństwa przeglądarki poprzez:

(i) Aktualizowanie Javy

W wydaniu Java 7 Update 11 domyślny poziom zabezpieczeń Javy zwiększono na „wysoki". Konfiguracja ta oznacza, że użytkownicy muszą jawnie zatwierdzić wykonywanie apletu (czy to niepodpisanego, czy podpisanego samodzielnie).

(ii) Wyłączenie dodatku Javy w przeglądarce

Jeśli aktualizacja Javy nie wchodzi w grę, użytkownik może skupić się na zarządzaniu dodatkiem do przeglądarki, wyłączając go i włączając tylko wtedy, kiedy jest potrzebny. Można to zrobić jednym kliknięciem w panelu sterowania Javy (opcja dostępna w wydaniu Java 7 Update 10) albo za pośrednictwem ustawień przeglądarki. Instrukcje wyłączania Javy w różnych przeglądarkach internetowych można znaleźć pod adresem: http://www.java.com/en/download/help/disable_browser.xml

(iii) Używanie dwóch przeglądarek

Zamiast majstrować przy ustawień zabezpieczeń, użytkownik może wybrać strategię dwóch przeglądarek, w której jedna przeglądarka z włączonym dodatkiem Javy jest przeznaczona wyłącznie do korzystania z witryny lub aplikacji, która tego wymaga. Inne strony przegląda się za pomocą oddzielnej przeglądarki bez dodatku.

(iv) Włączenie opcji „Click to Play"

W większości przeglądarek obsługujących Javę dodatkowym zabezpieczeniem może być funkcja blokowania dodatków. W Firefoksie i Operze nosi ona nazwę „Click to Play", podczas gdy Chrome ma opcję „Blokuj wszystko" na stronie Ustawienia treści. Funkcja ta zapobiega automatycznemu wykonywaniu dodatków (nie tylko Javy) i wymaga, aby użytkownik kliknął dodatek, zanim zostanie on uruchomiony.

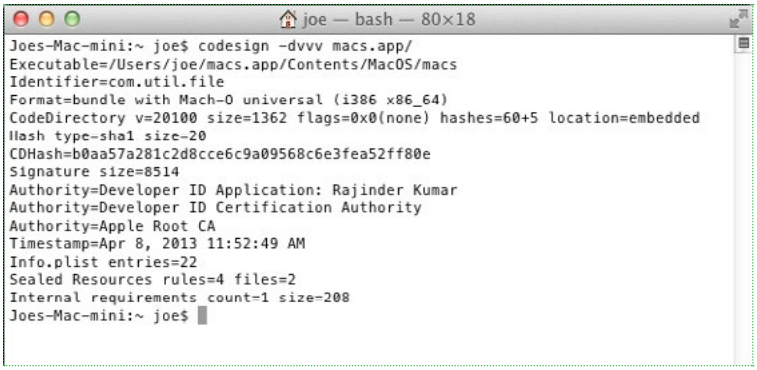
(v) Używanie aplikacji firm trzecich

Inną możliwością jest użycie programów firm trzecich, które blokują automatyczne uruchamianie dodatków podczas wczytywania strony, chyba że użytkownik postanowi inaczej. Najpopularniejszym programem tego typu jest NoScript, który blokuje wiele typów aktywnej treści w przeglądarkach wywodzących się z Mozilli, choć istnieje również kilka innych aplikacji, które działają w podobny sposób.

KUMAR IN THE MAC (KitM)

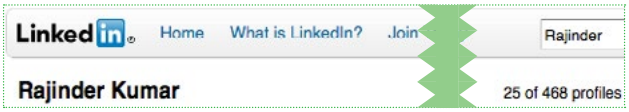
W pierwszej połowie 2013 r. zaobserwowaliśmy pierwsze złośliwe oprogramowanie do Maca podpisane ważny identyfikatorem dewelopera Apple. Gdyby ktoś nie znał się na podpisywaniu kodu, wyjaśnijmy, że identyfikator dewelopera Apple jest jak podpis w firmie cyfrowej. Zupełnie tak samo jak ręczny podpis, który wiąże dokument z autorem, cyfrowy podpis wiąże kod z deweloperem.

W zeszłym roku Apple wprowadziło do systemu OS X zabezpieczenie o nazwie Gatekeeper. Gatekeeper domyślnie pozwala na wykonywanie tylko tych aplikacji, które pochodzącą od zidentyfikowanych deweloperów. Pomaga to zapobiec przypadkowemu uruchomieniu złośliwego oprogramowania, które zwykle nie jest podpisane. Twórcy złośliwego oprogramowania nie chcieliby przecież, aby dało się ich powiązać ze szkodliwym aplikacjami, prawda?



Rysunek 1: Cyfrowy certyfikat KitM

Jak na ironię, właśnie tak postąpił pewien programista. Aby obejść zabezpieczenia wprowadzone przez Apple, złośliwe oprogramowanie zostało podpisane identyfikatorem niejakiego Rajindera Kumara (zob. rysunek 1), stąd nazwa KitM („Kumar in the Mac"). KitM to nasze oznaczenie próbek podpisanych tym identyfikatorem dewelopera Apple.



Rysunek 2: Wyniki wyszukiwania Rajindera Kumara w LinkedIn

Nie wiadomo, czy za złośliwym oprogramowaniem rzeczywiście stoi Rajinder Kumar. Wyszukiwanie jego nazwiska w LinkedIn zwróciło przynajmniej 468 wyników (zob. rysunek 2), więc może to równie dobrze być indyjski odpowiednik „Jana Kowalskiego". Napastnicy mogli posłużyć się przypadkowym nazwiskiem, aby uzyskać identyfikator dewelopera Apple[1].

Tak czy owak, Apple szybko unieważniło ten identyfikator, aby zapobiec przyszłym infekcjom.

Złośliwe oprogramowanie zostało odkryte przez niezależnego badacza, Jacoba Appelbauma. Znalazł on dwa warianty oprogramowania szpiegowskiego w Macu angolskiego aktywisty podczas warsztatów na konferencji Oslo Freedom Forum.

Pierwszym wariantem był pakiet aplikacyjny z plikiem o nazwie „FileBackup". Po jego odkryciu zaczęliśmy przeglądać nasze systemy backupu pod kątem próbek o tej samej nazwie i znaleźliśmy jedną z dnia 21 kwietnia 2012 r.[2, 3]. Próbka miała nie tylko taką samą nazwę, ale również struktury wewnętrzne, w tym klasy, metody itd., co pozwoliło nam stwierdzić, że rzeczywiście był to wcześniejszy wariant. Próbka zawierała również ścieżki kompilacji, które wskazywały, że złośliwe oprogramowanie jest w rzeczywistości przerobioną wersją narzędzia open source o nazwie FileBackup przeznaczonego do tworzenia kopii zapasowych w sieci (zob. rysunek 3).

Narzędzie to używa pliku konfiguracyjnego o nazwie „FileBackup.ini", aby ustalić, które pliki skopiować (na podstawie rozszerzeń) i gdzie wysłać kopię (na podstawie docelowego adresu URL). Naturalnie spróbowaliśmy zlokalizować odpowiedni plik konfiguracyjny złośliwego oprogramowania. Trafiliśmy na plik udostępniony nam przez partnera w tym

```
/Users/MacAdmin/Downloads/FileBackup-1/main.m /Users/MacAdmin/Downloads/FileBac
kup-1/build/FileBackup.build/Release/FileBackup.build/Objects-normal/i386/main.
o _main /Users/MacAdmin/Downloads/FileBackup-1/FileBackupAppDelegate.m /Users/M
acAdmin/Downloads/FileBackup-1/build/FileBackup.build/Release/FileBackup.build/
Objects-normal/i386/FileBackupAppDelegate.o -[FileBackupAppDelegate application
```

Rysunek 3: Pobrany projekt o nazwie „FileBackup-1"

```
<URL>liveapple.eu/vmacdata/upload.php</URL>
<EXTENSION>txt;doc;docx;eml;emlx;fdf;fdr;pdf;jpg;jpeg;xls;xlsx;fdx;idx;knt;kwd;
log;lst;lwp;mbox;msg;mw;pages;wpr;tiff;ppt;pptx</EXTENSION>
```

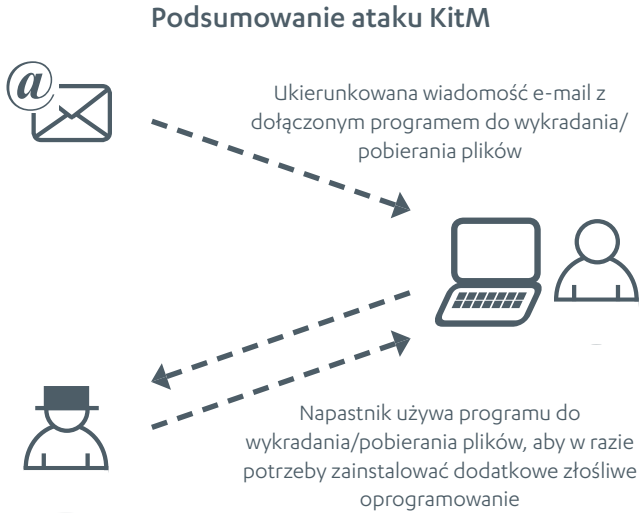
Rysunek 4: Docelowy adres URL i rozszerzenia określone w pliku konfiguracyjnym

samym czasie, w którym otrzymaliśmy wspomnianą wcześniej próbkę[4]. Okazało się, że plik konfiguracyjny określał domenę (zob. rysunek 4) podobną do tych w nowszych wariantach, które opisujemy poniżej w tabeli 1. Potwierdzało to, że próbka nie jest nieszkodliwym narzędziem, ale rzeczywiście jest używana w złośliwy sposób, a ponadto dowodziło, że ataki APT zaczęły się znacznie wcześniej, niż ktokolwiek przypuszczał.

Inny wariant odkryty przez Appelbaum to coś, z czym jeszcze się nie spotkaliśmy. Wariant ten robi zrzuty ekranowe, zamiast gromadzić pliki. Analiza próbki pokazała, że dużo kodu pochodzi z wersji wykradającej pliki, a część nawet nie jest używana. Z tego wywnioskowaliśmy, że wariant do zrzutów ekranowych jest deweloperską odnogą wersji wykradającej pliki.

Od tego czasu zgłoszono kolejne przypadki infekcji, co doprowadziło do odkrycia innych wcześniejszych wariantów[5]. Niektóre warianty wykradające pliki mają funkcję pobierania. Zazwyczaj używany był tylko kod do kradzieży plików, ale w jednym przypadku program pobrał aplikację towarzyszącą, która okazała się identyczna z narzędziem do robienia zrzutów ekranowych odkrytym przez Appelbauma. Uważamy zatem, że najprawdopodobniej stało się tak również w przypadku angolskiego aktywisty.

Figure 6: Project for Elance



Rysunek 5: Podsumowanie ataku KitM

Atak można podsumować następująco (zob. rysunek 5): ofiara otrzymuje ukierunkowaną wiadomość e-mail z załącznikiem w postaci narzędzia wykradającego pliki. Zauważmy, że niektóre warianty tego narzędzia potrafią pobierać pliki. Załącznik, który jest aplikacją, udaje dokument, obraz albo inny typ mediów. Jeśli ofiara nabierze się na trik socjotechniczny i zainfekuje swój komputer, napastnicy mogą zainstalować w nim dodatkowe złośliwe oprogramowanie, w zależności od celu ataku. Dotychczas wykorzystywano tylko narzędzie do robienia zrzutów ekranowych, ale nie będzie niczym dziwnym, jeśli w

TABELA 1: PODSUMOWANIE ROZWOJU PRÓBEK

OKRES ATAKU	NIEZNANY (OTRZYMANA W KWIETNIU 2012 R.)	GRUDZIEŃ 2012	1. POŁOWA 2013	MAJ 2013
Podpisana przez Rajindera Kumara (KitM)	Nie	Tak	Tak	Tak
Klasyfikacja rodziny złośliwego oprogramowania	Hackback	Hackback	Hackback	Brak klasyfykacji
Nazwa pliku / prefiks AppDelegate	FileBackup	FileBackup	FileBackup	macs / macps
Funkcje	Gromadzi pliki	Gromadzi pliki	Gromadzi / pobiera pliki	Robi zrzuty ekranowe
Używa pliku “FileBackup.ini”	Tak	Nie	Nie	Nie
Używa pliku “login.scpt”	Tak	Nie	Nie	Nie
Zawiera plik “login.scpt”	Tak	Tak	Tak	Nie
Domena docelowego adresu URL	liveapple[kropka]eu	liveapple [kropka]eu	liveapple[kropka]eu; securitytable[kropka] org	securitytable [kropka]org
Domena adresu URL wtórnego modułu	Nie dotyczy	Nie dotyczy	liveapple[kropka]eu; torqspot[kropka]org	Nie dotyczy
Starsza domena znaleziona w próbce	researcherzone[kropka] net (używana awaryjnie)	Brak	Brak	docsforum[kropka]info

przyszłości pojawi się wariant rejestrujący naciśnięcia klawiszy albo instalujący backdoory. Ataki APT często mają takie komponenty.

Badacze bezpieczeństwa powiązali odkryte przypadki z większą operacją szpiegowską znaną jako Operation Hangover[6]. Wiadomo, że brali w niej udział niezależni deweloperzy[7]. Co ciekawe, ścieżkę z nazwą „Elance" (zob. rysunek 6) znaleziono w nieużywanym pliku (login.scpt — zob. tabela 1) w niektórych wariantach wykradających pliki . „Elance" może odnosić się do internetowego serwisu do rekrutacji wolnych strzelców[8].

Rozwój głównych próbek podsumowaliśmy w tabeli 1. Jak widać, przez większość operacji napastnicy używali domeny „liveapple[kropka]eu" jako centrum dowodzenia, co trwało do pierwszych miesięcy 2013 r. (lutego). Jednak w próbce z kwietnia 2012 r. znaleziono starszą domenę „researcherzone[kropka]net". Może to wskazywać, że istnieją dotąd nieodkryte, wcześniejsze próbki, które używają tej domeny jako centrum dowodzenia.
W późniejszych miesiącach pierwszej połowy 2013 r. (kwiecień) domeny zmieniono na „securitytable[kropka]org" (docelowy adres URL dla wykradanych plików) oraz „torqspot[kropka]org" (adres URL używany przez wtórny modułu). Wiemy, że wtórnym modułem hostowanym w domenie „torqspot[kropka]org" było narzędzie do robienia zrzutów ekranowych odkryte przez Appelbauma. Nikt jednak nie znalazł jeszcze próbki, która byłaby wtórnym modułem hostowanym w domenie „liveapple[kropka]eu", kiedy była ona aktywna. Autorzy dodali funkcję pobierania na długo przed wariantem „securitytable[kropka]org"/"torqspot[kropka]org", co niemal gwarantuje, że taka próbka istnieje. Prawdopodobnie nie służy ona do wykradania plików, być może jest wcześniejszym wariantem narzędzia do robienia zrzutów ekranowych albo innym typem złośliwego programu, takim jak backdoor albo rejestrator klawiszy, który używa „liveapple[kropka]eu" jako docelowej domeny.

Wreszcie starsza domena „docsforum[kropka]info" znaleziona w narzędziu do robienia zrzutów ekranowych może wskazywać, że istnieją nieodkryte próbki wtórnego modułu, które używają tej domeny jako centrum dowodzenia.

Tak czy owak, użytkownicy mogą być niemal pewni, że ich program antywirusowy wykryje, a najprawdopodobniej również zablokuje infekcje tymi potencjalnymi wariantami przejściowymi. Wiadomo bowiem, że napastnicy zawsze używali oprogramowania wykradającego pliki, które należy do dobrze znanej (przynajmniej obecnie) rodziny o nazwie Hackback. Jeśli chodzi o zaginione moduły wtórne, wiemy, że napastnicy podpisywali swój kod, zanim zaczęli używać modułów wtórnych, co oznacza, że te zaginione warianty również będą podpisane. U użytkowników produktów F-Secure te warianty zostaną zidentyfikowane jako Kumar in the Mac (KitM).

ŹRÓDŁA

1. Twitter; Sean Sullivan; opublikowano 16 maja 2013 r.; https://twitter.com/5ean5ullivan/status/334987332556054528
2. Twitter; Sean Sullivan; opublikowano 16 maja 2013 r.; https://twitter.com/5ean5ullivan/status/335055459859980290
3. Próbka; skrót SHA1: 93decbdc89e52d5c5bde5d443f131f001e2b49d7
4. Próbka; skrót SHA1: 55374f3a281bd81e70ae1be8857085906cc87204
5. Weblog F-Secure; Sean Sullivan; *Mac Spyware Bait: Lebenslauf für Praktitkum;* opublikowano 23 maja 2013; http://www.f-secure.com/weblog/archives/00002559.html
6. Weblog F-Secure; Sean Sullivan; *Big Hangover;opublikowano 21 maja 2013 r.;* http://www.f-secure.com/weblog/archives/00002557.html
7. Dark Reading; Kelly Jackson Higgins; *'Hangover' Persists, More Mac Malware Found;* opublikowano 18 lipca 2013 r.; http://www.darkreading.com/attacks-breaches/hangover-persists-more-mac-malware-found/240158537
8. Elance; http://www.elance.com/

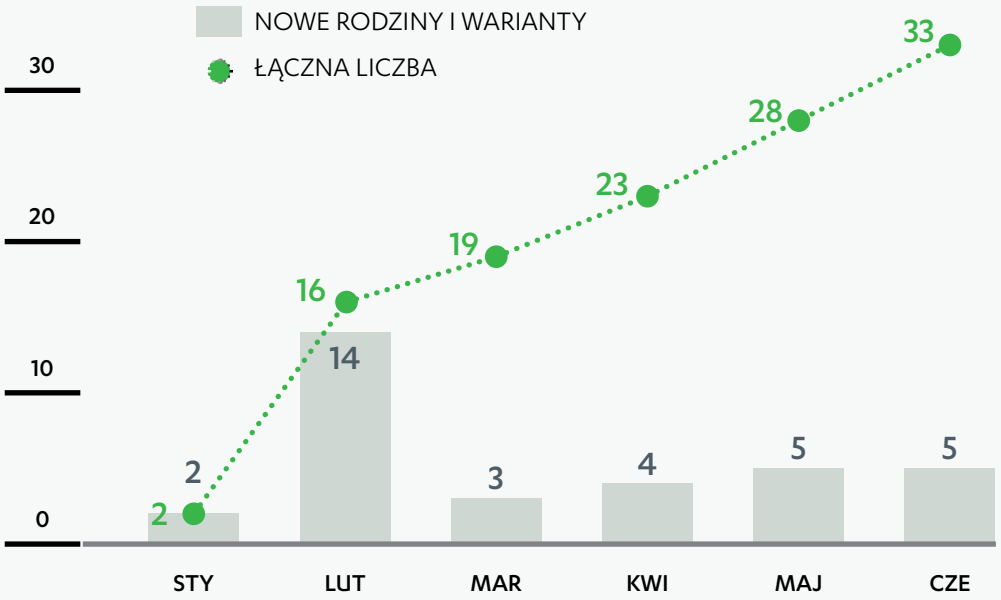
ZŁOŚLIWE OPROGRAMOWANIE DO MACA

PIERWSZA POŁOWA 2013 R.

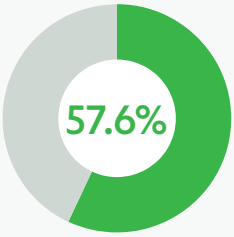
OGÓŁEM (STY-CZE 2013) =

33

rodziny i warianty złośliwego oprogramowania do Maca

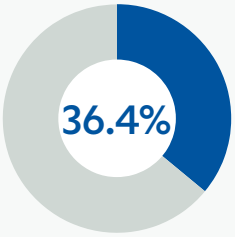


BACKDOORY



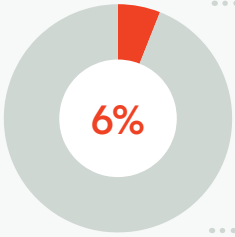
19/33

TROJANY



12/33

INNE



2/33

1/2 ROOTKIT
1/2 WIRUS

STY

2/2 TYLNE DRZWI

LUT

10/14 TYLNE DRZWI
4/14 TROJAN-SZPIEG

MAR

1/3 ROOTKIT
1/3 TYLNE DRZWI
1/3 TROJAN-SZPIEG

KWI

3/4 TYLNE DRZWI
1/4 WIRUS

MAJ

1/5 TYLNE DRZWI
4/5 TROJAN-SZPIEG

CZE

2/5 TYLNE DRZWI
1/5 TROJAN
1/5 TROJAN-POBIERAJĄCY PLIKI
1/5 TROJAN-SZPIEG

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

WYŁUDZANIE INFORMACJI

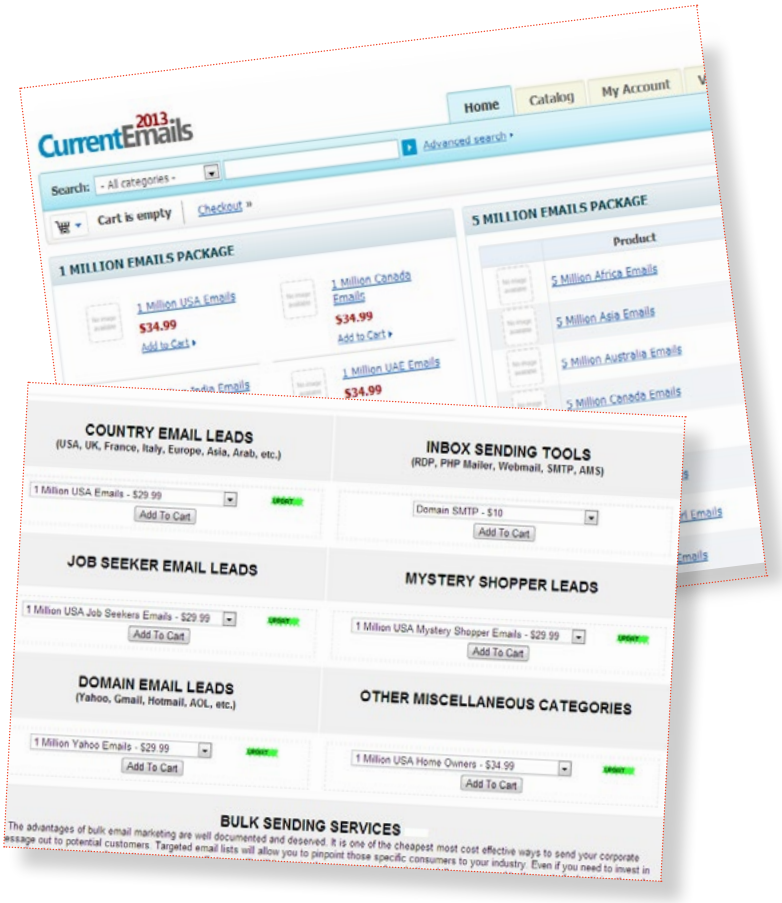
Kiedy mówimy o phishingu – wyłudzaniu informacji, zwykle myślimy o naszych kontach bankowych oraz danych, które umożliwiają dostęp do nich. Ale w erze jednorazowych haseł i uwierzytelniania wieloczynnikowego prosta strona phishingowa rzadko ma szansę na obejście takich wyrafinowanych zabezpieczeń. Dlatego pojawiły się bardziej zaawansowane trojany, które służą do włamywania się na dostępne w sieci konta bankowe.

Nie oznacza to, że phishing odszedł do historii; naciągacze po prostu stali się mniej wybredni, jeśli chodzi o łupy. Dziś każdy, kto spędza czas w sieci, ma coś, co można ukraść i spróbować sprzedać. Od kiedy każda informacja w sieci jest do wzięcia, obowiązuje zasada: *jeśli coś ma nazwę użytkownika i hasło, to może być i zapewne jest celem wyłudzeń.*

Są to zarówno konta Google, Yahoo, AOL lub Live używane do poczty e-mail i przechowywania plików w sieci, jak i konta na Facebooku i Twitterze, które pomagają utrzymać kontakt z różnymi osobami. Zagrożone są nawet witryny randkowe; Match.com i SeniorPeopleMeet to tylko niektóre serwisy, których użytkownicy są celem ataków. A witryny i portale z grami? Battle.net, Steam, Runescape, Habbo, czy komuś to coś mówi?

Pozyskiwanie celów

Najbardziej widocznym miejscem, w którym użytkownicy mogą trafić na phishingowe adresy URL, są niepożądane wiadomości e-mail. Odbiorców spamu można kupić masowo na podziemnych rynkach, a nawet w różnych witrynach, które oferują adresy e-mail na sprzedaż (zob. rysunek 1). Po pozyskaniu adresów zaczyna się spamowanie. Pomimo niskiego współczynnika kliknięć związanego ze spamem sama liczba wiadomości rozsyłanych na cały świat przekłada się na wystarczający ruch, że metoda ta pozostaje podstawą biznesowego modelu naciągaczy.



Rysunek 1: Witryny sprzedające adresy e-mail

Rysunek 2: Strona wyłudzająca informacje bezpośrednio (po lewej) i pośrednio (po prawej) (bottom)

Kiedy użytkownik kliknie łącze w wiadomości e-mail, trafia do witryny phishingowej, która zwykle jest przygotowana z myślą o konkretnym celu.

Typy witryn wyłudzających informacje

Sprofilowaliśmy 71 proc. wszystkich phishingowych adresów URL, które zgromadziliśmy w pierwszym półroczu, i odkryliśmy, że dzielą się one na dwa typy: *wyłudzenia bezpośrednie i pośrednie.*

Wyłudzenia bezpośrednie polegają po prostu na wyświetleniu fałszywej strony, która naśladuje rzeczywistą witrynę i służy do wykradania poświadczeń logowania, a czasem również innych informacji (zob. rysunek 2, lewy górny róg). Ten typ wyłudzeń jest znany od dawna i niewiele się zmienił, pominąwszy coraz bardziej profesjonalny wygląd i działanie witryn phishingowych. Jeśli jednak chodzi o ogólne rozpowszechnienie, wyłudzenia bezpośrednie nadal przebijają pośrednie w stosunku 99 do 1.

Wyłudzenia pośrednie są względnie nowe i polegają na wyświetleniu fałszywej strony, która naśladuje wtórną witrynę-przynętę, służącą do wykradania poświadczeń do innej witryny, która jest rzeczywistym celem. Witryna-przynęta może być na przykład serwisem do wypełniania deklaracji podatkowych połączonym z różnymi bankami, a naśladująca ją witryna phishingowa może oferować nową „funkcję", która wymaga, aby użytkownicy tych banków wprowadzili swoje nazwy i hasła w celu „zweryfikowania konta" (zob. rysunek 2, dół). Wyłudzenia pośrednie biorą na cel głównie, choć nie wyłącznie, witryny związane z nieruchomościami, podatkami i logistyką.

Rozkład witryn wyłudzających informacje

Jeśli chodzi o informacje, która jest najcenniejszym łupem dla oszustów, zdecydowanym liderem są poświadczenia PayPal — ta internetowa usługa płatnicza jest celem 73 proc. sprofilowanych przez nas witryn phishingowych, podczas gdy wszystkie inne organizacje składają się na pozostałe 27 proc. Łatwo zrozumieć, dlaczego te informacje są tak pożądane — to w praktyce darmowe pieniądze. Ponieważ zaś usługa jest bardzo rozpowszechniona, można znaleźć ofiary we wszystkich częściach świata.

Naciągacze, dzisiaj mniej wybredni, z konieczności zajmują się szeroką gamą kategorii (typów atakowanych celów), choć 10 najpopularniejszych kategorii, co nie dziwi, jest w jakiś sposób powiązane z handlem internetowym. Witryny phishingowe rozwijają też działalność, biorąc na cel marki z różnych

POJEDYNCZE DOMENY BIORĄCE NA CEL KLIENTÓW WIELU ORGANIZACJI

regionów i krajów (nawet jeśli te marki są również obecne na rynkach międzynarodowych). Geograficzny rozkład witryn pishingowych i ich kategorii podano na następnej stronie.

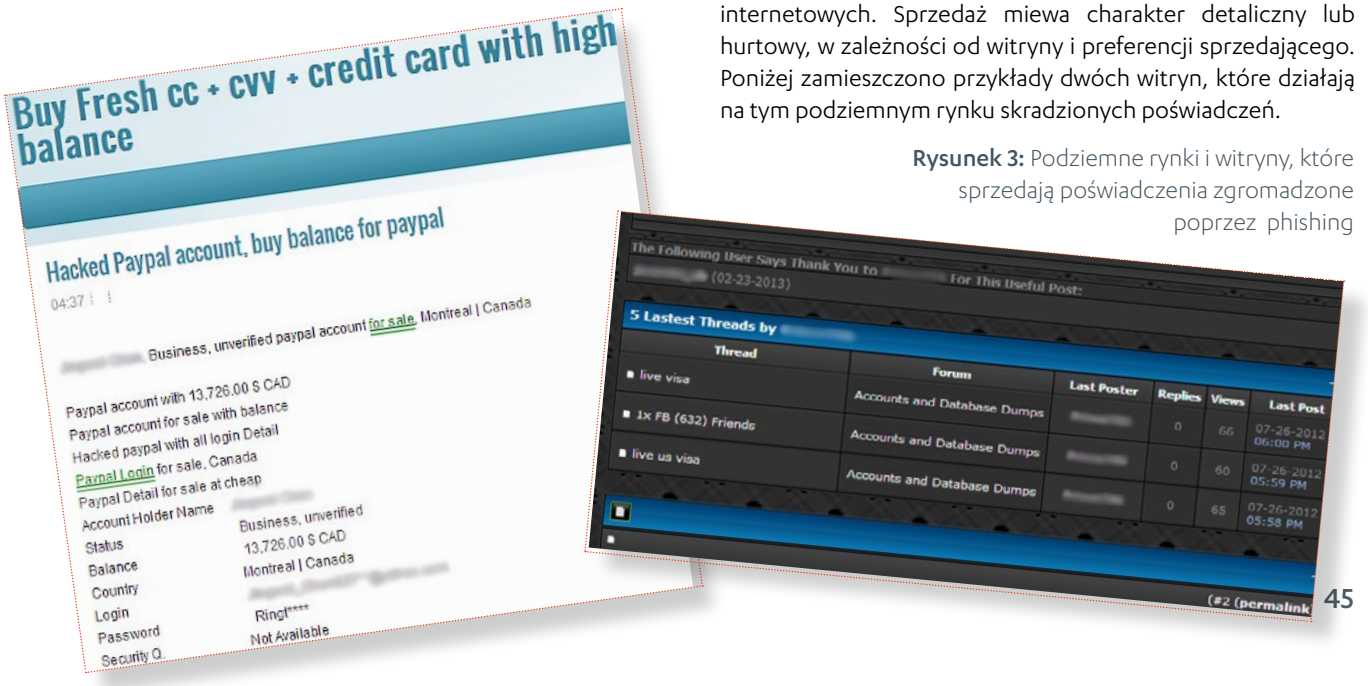
Phishing zautomatyzowany i rozproszony

Od czasu rozpowszechnienia się pakietów phishingowych (zestawów narzędzi, które automatyzują proces tworzenia witryn phishingowych), budowanie stron wyłudzających informacje stało się łatwiejsze i każdy jest potencjalną ofiarą. Pakiety te pozwalają złoczyńcom generować różne strony dla różnych celów. Choć w artykule tym nie będziemy szczegółowo omawiać poszczególnych pakietów phishingowych, warto wspomnieć o podobnym formacie wielu łączy, które prowadzą do automatycznie generowanych stron, co z kolei wskazuje, że do wyłudzania informacji wykorzystywane są pakiety phishingowe.

Innym godnym uwagi trendem jest phishing rozproszony, wymierzony w wiele instytucji finansowych oraz innych celów i prowadzony z jednej domeny. Technika ta pozwala zwodzić potencjalne ofiary znacznie niższym kosztem, ponieważ nie wymaga tworzenia wielu domen do atakowania wielu celów. Powyżej przedstawiono przykład phishingu rozproszonego.

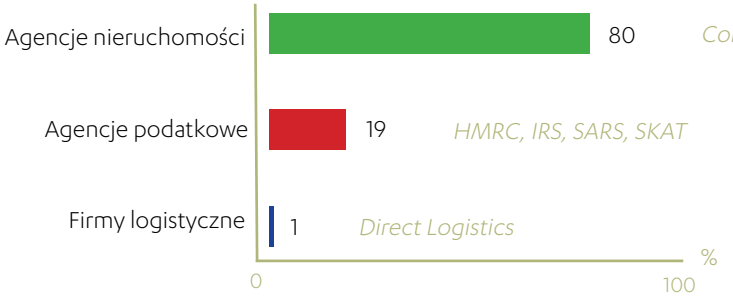
Sprzedawanie plonów

Kiedy wyłudzacze zdobędą informacje o ofiarach, mogą sprzedać je na podziemnych rynkach lub w witrynach internetowych. Sprzedaż miewa charakter detaliczny lub hurtowy, w zależności od witryny i preferencji sprzedającego. Poniżej zamieszczono przykłady dwóch witryn, które działają na tym podziemnym rynku skradzionych poświadczeń.

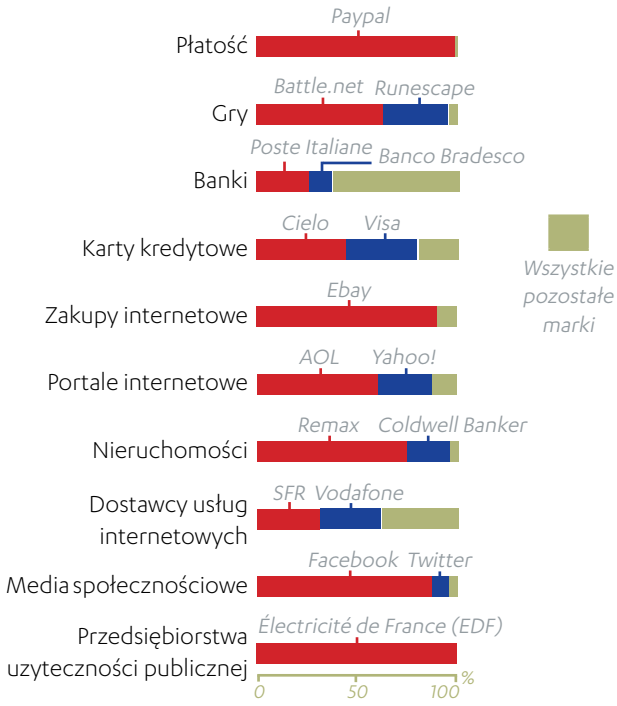


Rysunek 3: Podziemne rynki i witryny, które sprzedają poświadczenia zgromadzone poprzez phishing

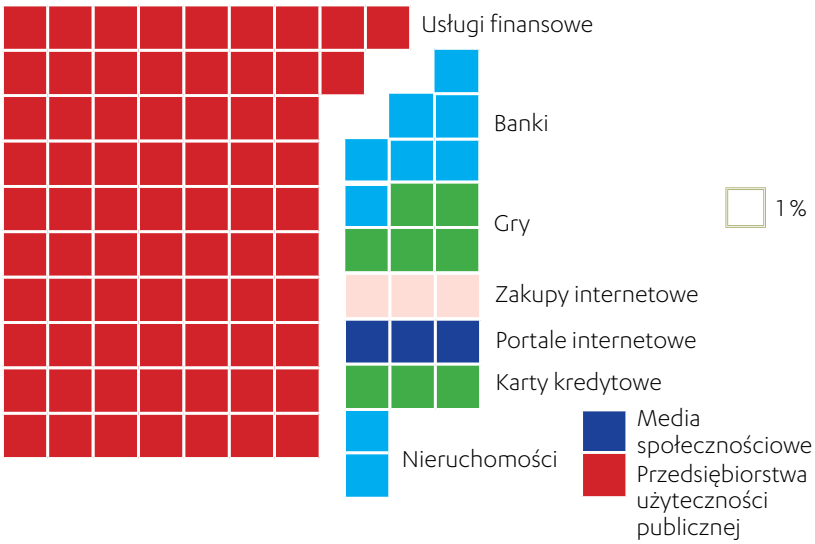
KATEGORIE I MARKI, KTÓRE SĄ CELEM WYŁUDZEŃ POŚREDNICH, PROCENTOWO



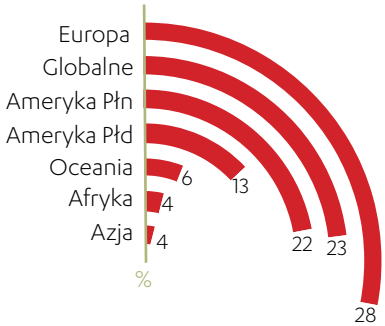
10 MAREK NAJCZĘŚCIEJ BĘDĄCYCH CELEM PHISHINGU, PROCENTOWO



10 KATEGORII WITRYN NAJCZĘŚCIEJ BĘDĄCYCH CELEM PHISHINGU, PROCENTOWO



ATAKOWANE MARKI WG REGIONU, PROCENTOWO



LICZBA ATAKOWANYCH MAREK WG KATEGORII

ŹRÓDŁA

KALENDARZ INCYDENTÓW W 1. POŁOWIE 2013 R. (STRONA 6)

ROZWÓJ ZŁOŚLIWEGO OPROGRAMOWANIA

[1] Krebs on Security; Krebs, Brian; *Crimeware Author Funds Exploit Buying Spree*; opublikowano 7 stycznia 2013 r.; http://krebsonsecurity.com/2013/01/crimeware-author-funds-exploit-buying-spree/

[2] Securelist; GReAT; *The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor*; opublikowano 27 lutego 2013 r.; http://www.securelist.com/en/blog/208194129/The_MiniDuke_Mystery_PDF_0_day_Government_Spy_Assembler_0x29A_Micro_Backdoor

[3] Weblog F-Secure; Aquino, Karmina; *Flash Exploit Targets Uyghur Website*; opublikowano 13 marca 2013 r.; http://www.f-secure.com/weblog/archives/00002524.html

[4] Weblog F-Secure; Aquino, Karmina; *CVE-2013-2423 Java Vulnerability Exploit ITW;* opublikowano 23 kwietnia 2013 r.; http://www.f-secure.com/weblog/archives/00002544.html

[5] Microsoft; Microsoft Security Tech Center; *Microsoft Security Advisory (2847140)*; opublikowano 14 maja 2013 r.; http://technet.microsoft.com/en-us/security/advisory/2847140

[6] The Register; Thomson, Iain; *Mac malware found with valid developer ID at freedom conference*; opublikowano 17 maja 2013 r.; http://www.theregister.co.uk/2013/05/17/mac_malware_steals_screenshots/

HAKERSTWO I SZPIEGOSTWO

[1] Arstechnica; Goodin, Dan; *Red October espionage platform unplugged hours after its discovery*; opublikowano 19 stycznia 2013 r.; http://arstechnica.com/security/2013/01/red-october-espionage-platform-unplugged-hours-after-its-discovery/

[2] New York Times; Perlroth, Nicole; *Hackers in China Attacked The Times for Last 4 Months*; opublikowano 30 stycznia 2013 r.; http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

[3] Weblog F-Secure; Sullivan, Sean; *Timeline: Hacks Related to Apple*; opublikowano 20 lutego 2013 r.; http://www.f-secure.com/weblog/archives/00002507.html

[4] Weblog F-Secure; Sullivan, Sean; *Evernote Hacked: 50 Million E-mail Addresses Exposed*; opublikowano 4 marca 2013 r.; http://www.f-secure.com/weblog/archives/00002516.html

[5] Guardian UK; Branigan, Tania; *South Korea on alert for cyber-attacks after major network goes down*; opublikowano 20 marca 2013 r.; http://www.guardian.co.uk/world/2013/mar/20/south-korea-under-cyber-attack

[6] Arstechnica; Bright, Peter; *Spamhaus DDoS grows to Internet-threatening size*; opublikowano 28 marca 2013 r. http://arstechnica.com/security/2013/03/spamhaus-ddos-grows-to-internet-threatening-size/

[7] Onion Inc.'s Tech Blog; Onion Inc.'s Tech Team; *How the Syrian Electronic Army Hacked The Onion*; opublikowano 8 maja 2013 r.; http://theonion.github.io/blog/2013/05/08/how-the-syrian-electronic-army-hacked-the-onion/

[8] Wired UK; Shubber, Kadhim; *Millions of users' data hacked in Yahoo Japan security breach*; opublikowano 20 maja 2013 r.; http://www.wired.co.uk/news/archive/2013-05/20/yahoo-japan-hacked

[9] Trend Micro; Wilhoit, Kyle; *Hiding in Plain Sight: A New Targeted Attack Campaign*; opublikowano 17 maja 2013 r.; http://www.guardian.co.uk/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism

[10] Guardian; Hopkins, Nick; *UK gathering secret intelligence via covert NSA operation*; opublikowano 7 czerwca 2013 r.; http://www.guardian.co.uk/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism

[11] Securelist; GReAT; *"NetTraveler is Running!" - Red Star APT Attacks Compromise High-Profile Victims*; opublikowano 4 czerwca 2013 r.; http://www.securelist.com/en/blog/8105/NetTraveler_is_Running_Red_Star_APT_Attacks_Compromise_High_Profile_Victims

[12] Trend Micro; Aquino, Marhalito; *RARSTONE found in Targeted Attacks*; opublikowano 13 czerwca 2013 r.; http://www.guardian.co.uk/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism

ROZWÓJ ZŁOŚLIWEGO OPROGRAMOWANIA MOBILNEGO

[1] McAfee; Zhang, Michael; *SMS Trojan Targets South Korean Android Devices*; opublikowano 25 lutego 2013 r.; http://blogs.mcafee.com/mcafee-labs/sms-trojan-targets-south-korean-android-devices

[2] Dell SecureWorks; Stone-Goss, Brett; *Stels Android Trojan Malware Analysis*; opublikowano 22 marca 2013 r.; http://www.secureworks.com/cyber-threat-intelligence/threats/stels-android-trojan-malware-analysis/

[3] Arstechnica; Gallagher, Sean; *First targeted attack to use Android malware discovered*; opublikowano 27 marca 2013 r.; http://arstechnica.com/security/2013/03/first-targeted-attack-to-use-android-malware-discovered/

[4] The Register; McAllister, Neil; *Sneaky new Android Trojan is WORST yet discovered*; opublikowano 7 czerwca 2013 r.; http://www.theregister.co.uk/2013/06/07/android_obad_trojan/

[5] Weblog F-Secure; Sullivan, Sean; *Post-PC Attack Site: Only Interested in Smartphones/Tablets*; opublikowano 19 czerwca 2013 r.; http://www.f-secure.com/weblog/archives/00002569.html

BEZPIECZEŃSTWO I ŚCIGANIE

[1] Europol; Europol; *Police dismantle prolific ransomware cybercriminal network*; opublikowano 13 lutego 2013 r.; https://www.europol.europa.eu/content/police-dismantle-prolific-ransomware-cybercriminal-network

[2] SCMagazine; Colon, Marcus; *New anti-bot code of conduct approved by FCC*; opublikowano 28 marca 2013 r.; http://www.scmagazine.com/new-anti-bot-code-of-conduct-approved-by-fcc/article/233756/

[3] Reuters; *Accused LulzSec hacker gets year in prison over Sony breach*; opublikowano 18 kwietnia 2013 r.; http://uk.reuters.com/article/2013/04/18/usa-lulzsec-hacker-idUKL2N0D521220130418

[4] The Register; Leyden, John; *British LulzSec hackers hear jail doors slam shut for years*; opublikowano 16 maja 2013 r.; http://www.theregister.co.uk/2013/05/16/lulzsec_sentencing/

[5] ZDNet; van Blommestein, Michiel; *Spamhaus DDoS suspect extradited, faces Dutch court*; opublikowano 9 maja 2013 r.; http://www.zdnet.com/spamhaus-ddos-suspect-extradited-faces-dutch-court-7000015120/

[6] Arstechnica; Gallagher, Sean; *Twitter launches two-factor authentication, too late to save The Onion*; opublikowano 23 maja 2013 r.; http://www.zdnet.com/spamhaus-ddos-suspect-extradited-faces-dutch-court-7000015120/

[7] BBC; *FBI and Microsoft take down $500m-theft botnet Citadel*; opublikowano 6 czerwca 2013 r.; http://www.bbc.co.uk/news/technology-22795074

[8] FBI; *Leader in $200 Million International Stolen Data Ring Charged in New Jersey as Part of Worldwide Takedown*; opublikowano 5 czerwca 2013 r.; http://www.fbi.gov/newark/press-releases/2013/leader-in-200-million-international-stolen-data-ring-charged-in-new-jersey-as-part-of-worldwide-takedown

[9] ZDNet; Whittaker, Zack; *Microsoft unleashes bug bounty program — for betas, too*; opublikowano 19 czerwca 2013 r.; http://www.zdnet.com/microsoft-unleashes-bug-bounty-program-for-betas-too-7000016956/

[10] Trend Micro; Aquino, Marhalito; *Targeted Attack in Taiwan Uses Infamous Gh0st RAT*; opublikowano 23 czerwca 2013 r.; http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attack-in-taiwan-uses-infamous-gh0st-rat/

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 2012 r. firma odnotowała przychody w wysokości 157 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

F-Secure