RAPORT NA TEMAT ZAGROŻEŃ

SWITCH ON FREEDOM

F-Secure.

www.f-secure.pl

SPIS TREŚCI

SPIS TREŚCI 2

PRZEGLĄD 3

PRZEDMOWA 4

GODNE UWAGI 5

KALENDARZ INCYDENTÓW 6

PODSUMOWANIE KRAJOBRAZU ZAGROŻEŃ 8

10 NAJCZĘSTSZYCH DETEKCJI 9,11

ZŁOŚLIWE OPROGRAMOWANIE MOBILNE 12

ZŁOŚLIWE OPROGRAMOWANIE DO MACA 14

ŹRÓDŁA 15

RAPORT NA TEMAT ZAGROŻEŃ W SKRÓCIE

KALENDARZ INCYDENTÓW

Strona 6

2014

STYCZEŃ

LUTY
- Wydano aktualizacje iOS naprawiające poważny błąd w obsłudze SSL
- Aktywne ataki na nową usterkę dnia zerowego w IE

MARZEC

KWIECIEŃ
- Rozszerzenie Coremax przejmuje kontrolę nad przeglądarkami
- Oficjalne zakończenie wsparcia dla Windows XP

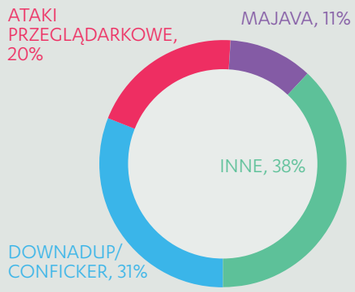
MAJ
- „Policyjne" oprogramowanie wymuszające okup trafia do Androida

CZERWIEC
- FBI namierza osobę stojącą za botnetem Gameover Zeus
- Hakerzy z grupy „Oleg Pliss" aresztowani w Moskwie

ZŁOŚLIWE OPROGRAMOWANIE DO KOMPUTERÓW PC 10 NAJCZĘSTSZYCH DETEKCJI

Strony 9, 11

Krajobraz zagrożeń dla systemu Windows jest pełen istniejących rodzin złośliwego oprogramowania. Niektóre z nich pozostają w obiegu od lat, utrzymywane przy życiu przez niezałatane luki w zabezpieczeniach.



10 NAJCZĘSTSZYCH DETEKCJI

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

2 ATAKI PRZEGLĄDARKOWE
Zbiór złośliwych programów, technik lub exploitów używanych w celu przekierowania przeglądarki do złośliwych witryn, w których system może być narażony na dalsze ataki.

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

a na dalszych miejscach...

SALITY | RAMNIT | AUTORUN | WORMLINK | BROWSER EXPLOIT | EXPIRO | ZEROACCESS

ZŁOŚLIWE OPROGRAMOWANIE DO MACA

Strona 14

Podczas gdy krajobraz zagrożeń Windows jest zdominowany przez stare i istniejące złośliwe programy, na dotychczas cichej scenie Maca pojawiają się nowi pretendenci. Złośliwe oprogramowanie staje się coraz bardziej wyrafinowane pod względem możliwości oraz metod dystrybucji.

25 NOWYCH WARIANTÓW odkrytych od stycznia do czerwca 2014 r.

13 wariantów spośród tych należy do **5 NOWYCH** rodzin

MASK
Element cyberszpiegowskiej operacji określanej mianem „The Mask". Atakuje instytucje rządowe i firmy energetyczne.

CLIENTSNOW
Używany w atakach ukierunkowanych na społeczności tybetańskie i ujgurskie.

LAOSHU
Trojan zdalnego dostępu, który rozprzestrzenia się za pośrednictwem fałszywych wiadomości e-mail o przesyłce kurierskiej.

COINTHIEF
Trojański program szpiegowski przeznaczony do kradzieży kryptowalut. Udawał złamaną wersję aplikacji do systemu OS X, ale później zaczął rozprzestrzeniać się za pośrednictwem „strojanizowanych" aplikacji do obsługi kryptowalut.

COINSTEALER
Program do kradzieży bitmonet, który udaje aplikację umożliwiającą dostęp do bazy transakcji z serwisu Mt. Gox.

ZŁOŚLIWE OPROGRAMOWANIE MOBILNE

Strona 12

Android nadal pozostaje ulubionym celem większości zagrożeń mobilnych. Istnieją jednak również ataki wymierzone w iOS, choć jest ich znacznie mniej.

ANDROID + iOS

294 NOWE RODZINY lub WARIANTY

1 nowa RODZINA

SSLCREDTHIEF
Podpisany plik biblioteczny monitoruje wychodzące połączenia SSL, aby kraść nazwy i hasła Apple ID.

3 CZOŁOWE RODZINY ANDROID

SMSSEND
Duża rodzina złośliwych programów, które wysyłają wiadomości SMS na numery typu premium (o podwyższonej taryfie).

FAKEINST
Pozoruje instalator aplikacji, a w rzeczywistości wysyła wiadomości SMS na numery typu premium.

EROPL
Po cichu gromadzi dane z urządzenia i przekazuje je do zdalnego serwera.

$ $ $ WYMUSZANIE OKUPU

ANDROID

KOLER: pierwszy program wymuszający okup (prawie)
Mobilna wersja „policyjnego" oprogramowania Reveton do wymuszania okupu. Informuje, że szyfruje pliki w urządzeniu, ale w rzeczywistości tylko wyłącza przycisk Wstecz, aby utrzymać na ekranie żądanie okupu.

ANDROID

SLOCKER: pierwszy program do wymuszania okupu z szyfrowaniem i obsługą sieci Tor Szyfruje obrazy, dokumenty i pliki wideo w urządzeniu; wyłącza przycisk Wstecz, aby zakłócić kontrolę użytkownika nad urządzeniem. Komunikuje się z serwerem dowodzenia za pośrednictwem sieci Tor albo wiadomości SMS.

iOS

Oleg Pliss uderza w Australii
W maju „Oleg Pliss" zablokował konta kilku użytkowników w Australii, podobno używając funkcji „Znajdź mój iPhone", i domagał się okupu. Apple zaprzeczyło spekulacjom o luce w usłudze iCloud.

PRZEDMOWA

Serwisy internetowe co chwila publikują alarmujące informacje na temat ataków wirusów komputerowych czy wycieków poufnych danych. Od momentu, kiedy pojawiły się pierwsze szkodliwe programy komputerowe, mające raczej charakter złośliwego żartu, minęło dużo czasu – teraz wirusy to skuteczne narzędzia w rękach osób, które chcą za ich pomocą osiągnąć konkretny zysk, najczęściej wyrażany w twardej walucie.

Z miesiąca na miesiąc powstają ich nowe, coraz bardziej zaawansowane wersje, a ich liczba rośnie w błyskawicznym tempie. Co więcej, problem złośliwego oprogramowania przestał dotyczyć wyłącznie komputerów PC z Windowsem. Wraz ze wzrostem liczby smartfonów i tabletów na rynku, cyberprzestępcy zaczęli się interesować użytkownikami platformy Android i iOS. Ich celem są prywatne pliki użytkowników, dane do logowania do sklepów internetowych czy serwisów bankowości online, a także numery kart kredytowych. Mogą też zablokować komputer, żądając sowitego okupu za możliwość ponownego z niego korzystania.

Sieć jest pełna zagrożeń, dlatego nasi Abonenci mogą skorzystać z pakietu Ochrona Internetu, dostępnego na komputery, smartfony i tablety. Dzięki współpracy z zaufanym partnerem, firmą F-Secure, która ma ponad 25 lat doświadczenia w walce z wirusami komputerowymi, zapewniamy naszym Klientom ochronę przed utratą poufnych danych, takich jak zdjęcia, filmy czy ważne dokumenty przechowywane na dysku. Umożliwiamy im korzystanie bez obaw z serwisów aukcyjnych, bankowości online i sklepów internetowych.

KONIEC GRY?

Sean Sullivan
Doradca ds. bezpieczeństwa
F-Secure Labs

Zakłócenie pracy botnetu GameOver ZeuS (GOZ) przez organa ścigania[1] pod wieloma względami było wielkim sukcesem — ale co dalej? Botnet został osłabiony, ale nie całkowicie zniszczony. Jego twórca nie został aresztowany, nadal pozostaje na wolności i buduje nowy botnet.

Dlaczego podjęto działania przeciwko GOZ?

CryptoLocker[2], zaawansowany trojan do wyłudzania okupu instalowany przez GOZ, był bez wątpienia ważnym argumentem za akcją przeciwko botnetowi. CryptoLocker, który szyfruje wszystkie dokumenty i pliki danych na dysku ofiary, był zbyt niebezpieczny. Nie było innego remedium, niż zapłacenie okupu za klucz odszyfrowujący, więc jedynym sposobem powstrzymania ataku była prewencja. Ponieważ CryptoLocker był dostarczany przez GOZ, postanowiono uderzyć w botnet.

Eskalacja

CryptoLocker to doskonały przykład na to, że osłabienie (ale nie całkowite zniszczenie) botnetu w rodzaju GameOver ZeuS jest bardzo niebezpieczne. Zadajmy sobie pytanie:

„Skoro CryptoLocker odnosił takie sukcesy, dlaczego Slavik (botmaster GOZ) nie zainstalował go w całym botnecie?"

> „Co się stanie, jeśli następną taktyką obronną będzie zostać jadowitym? ”

Oczywista odpowiedź: ponieważ wtedy nie miałby już botnetu. Wszystkie dwa miliony botów nie mogłyby aktywować CryptoLockera bez jednoczesnego zniszczenia infrastruktury GOZ.

Ale jeśli infrastrukturę i tak utracono ze względu na wyłączenie botnetu? Co przeszkodzi przyszłej wersji GOZ zainicjować „samozniszczenie" (na przykład zrzucić „bombę szyfrującą"), jeśli bot nie zdoła skomunikować się z serwerem dowodzenia przez określony czas? Nic.

Ewolucja

Historia złośliwego oprogramowania to historia ewolucji. Motorem tej ewolucji jest dynamika drapieżnik-ofiara. Za każdym razem, kiedy łowca odkrywa zwierzynę, potrzebna jest nowa taktyka pozwalająca uniknąć wykrycia. Co się stanie, jeśli następną taktyką obronną będzie zostać jadowitym?

Łowcy powinni mieć się na baczności.

ŹRÓDŁA
1. United States Department of Justice; *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator*; 2 Czerwca 2014; http://www.justice.gov/opa/pr/2014/June/14-crm-584.html
2. F-Secure; *Trojan:W32/Cryptolocker;* http://www.f-secure.com/v-descs/trojan_w32_cryptolocker.shtml

KALENDARZ INCYDENTÓW

Kalendarz incydentów przedstawia interesujące wydarzenia w dziedzinie cyfrowego bezpieczeństwa, które miały miejsce w pierwszej połowie 2014 r. Informowały o nich różne portale technologiczne, publikacje badaczy bezpieczeństwa, witryny organów ścigania, popularne gazety oraz blog F-Secure. Źródła są wymienione na stronie 15.

CYFROWA WOLNOŚĆ

GCHQ podobno szpieguje czaty wideo Yahoo

Lut: obrazy 1,8 mln „przypadkowych" użytkowników przechwycone i zapisane

Turcja blokuje Twittera, YouTube

Mar: Dostęp użytkowników tureckich do mediów społecznościowych ograniczony po interwencji rządu

Tajlandia tymczasowo blokuje Facebooka

Maj: Ministerstwo Informatyki twierdzi, że dostęp zablokowano na żądanie junty; wojsko wini „usterkę"

NSA podobno nagrywa wszystkie rozmowy telefoniczne na Bahamach

Maj: Monitorowanie uzasadnione działaniami antynarkotykowymi

NSA podobno umieszcza „tylne drzwi" w routerach

Maj: Eksportowane produkty są przechwytywane, modyfikowane pod kątem tajnych podsłuchów

Irak blokuje media społecznościowe

Cze: Działanie miało na celu „zakłócenie komunikacji między powstańcami ISIS"

Tajska junta blokuje witryny, cenzoruje raporty

Cze: Informacje o setkach zablokowanych witryn, zakaz krytycznych raportów w mediach

Dostęp do Youtube, wittera przywrócony w Turcji

Cze: Odblokowano Youtube po cofnięciu sankcji wobec Twittera w poprzednim miesiącu

ATAKI

Atak na Yahoo! prowadzi do resetowania haseł

Sty: Hasła skradzione z „zewnętrznej" bazy danych wykorzystano do dostępu do poczty

Włamania do domowych i biurowych routerów bezprzewodowych

Mar: Badacze zabezpieczeń raportują, że w ponad 300 000 urządzeń zmieniono ustawienia DNS

Flexcoin okradziony, kończy działalność

Mar: Napastnik wykorzystał usterkę w kodzie transferowym, aby ukraść 896 monet (wartych około 600 000 dol.)

Atak Windigo infekuje linuksowe serwery

Mar: Badacze raportują ponad 25 000 serwerów używanych do wysyłania spamu, przekierowywania użytkowników

Usterka Heartbleed wykorzystana do przejęcia sesji VPN

Kwi: NYT Times informuje, że napastnicy wykorzystali tę usterkę, aby dostać się do sieci atakowanej firmy

AU-CERT raportuje rosnącą liczbę cyberataków

Maj: Raport stwierdza, że 56 proc. ankietowanych firm doświadczyło cyberatakucyber attacks

TrueCrypt ostrzega, że ich oprogramowanie jest „szkodliwe"

Maj: Twórcy narzędzia do szyfrowania dysków ostrzegają, że nie jest ono bezpieczne, odradzają użytkowanie

Duży atak DDoS wymierzony w Hong Kong

Cze: Atak o natężeniu 300Gb/s+ na system zliczania głosów po obywatelskim referendum

BEZPIECZEŃSTWO

Giganci technologiczni publikują dane o żądaniach FISA

Lut: Google, Facebook i inni publikują zestawienia żądań rządu USA

Konferencja TrustyCon zorganizowana w ramach protestu

Lut: Bojkotujący konferencję RSA biorą udział w konkurencyjnej imprezie poświęconej „technologii godnej zaufania"

Windows XP oficjalnie wycofany z użytku

Kwi: Microsoft zaleca, aby użytkownicy przeszli na nowszą wersję systemu po zakończeniu wsparcia dla Windows XP

Ebay wymusza zmianę haseł wskutek ataku

Maj: Włamanie do bazy danych prowadzi do prewencyjnego resetowania haseł

Uruchomiony serwis MyBulletins, ułatwia zarządzanie aktualizacjami

Maj: Usługa ma na celu uprościć identyfikowanie stosownych aktualizacji zabezpieczeń

Google przedstawia formularz „prawa do bycia zapomnianym"

Maj: Europejski sąd nakazuje wyszukiwarce. aby na żądanie usuwała „nieistotne" łącza w UE

Usługa Google Apps dodaje szyfrowanie

Maj: Kompleksowe szyfrowanie poczty oferowane użytkownikom korporacyjnym

Rozpoczęła się kampania Reset the Net

Cze: Koalicja grup zamierza zachęcać do korzystania z narzędzi utrudniających monitorowanie

ŚCIGANIE

Autor oprogramowania Spyeye przyznaje się do winy w USA

Sty: Obywatel Rosji stworzył i rozpowszechniał program używany do oszustw bankowych

Zarzutów w sprawie piracki aplikacji do Androida

Mar: Dwie osoby skazane w USA za dystrybuowanie fałszywych aplikacji mobilnych

Zarzuty dla 9 osób w sprawie złośliwego oprogramowania Zeus

Kwi: 9 oskarżonych o zainfekowanie tysięcy firm w USA

Australia aresztuje 2 podejrzanych o ataki „Anon"

Maj: AFP oskarża 2 osoby o modyfikację witryn rządowych i ataki DoS

USA oskarża 5 chińskich hakerów o szpiegostwo

Maj: Departament Sprawiedliwości twierdzi, że członkowie PLA hakują amerykańskie firmy od 8 lat

Niemal 100 aresztowań w sprawie trojana Blackshades

Maj: Zatrzymania w USA, EU i innych krajach za sprzedaż trojana do szpiegowania użytkowników

Hakerzy z grupy „Oleg Pliss" aresztowani w Moskwie

Cze: Rosyjskie MSW twierdzi, że aresztowało 2 osoby za wyłudzanie okupu od użytkowników iOS

FBI poluje na administratora botnetu Gameover Zeus

Cze: Po wyłączeniu serwerów dowodzenia botnetu wniesiono akt oskarżenia przeciwko obywatelowi rosyjskiemu

BOTNET GAMEOVER ZEUS

- Mar: Zaczyna wykradać portfele Bitcoin i ich hasła szyfrowania
- Mar: Wstawia elementy wyłudzające informacje do witryn pośrednictwa pracy
- Cze: FBI i partnerzy rozpoczynają „Operację Tovar", apelują do użytkowników o usunięcie złośliwego oprogramowania z komputerów
- Cze: Kończy się dwutygodniowe „okno" na oczyszczenie komputerów; botnet jeszcze się nie zregenerował

BOTNET GAMEOVER ZEUS

ZŁOŚLIWE OPROGRAMOWANIE

Planowane nowe, lepsze oprogramowanie do wymuszania okupu

Sty: Badacze bezpieczeństwa informują o powstawaniu nowego zestawu „zrób to sam" do PowerLockera

GameOver Zeus zaczyna kraść bitmonety

Sty: Złośliwe oprogramowanie teraz wykrada portfele Bitcoin i ich hasła szyfrujące

Robak TheMoon rozprzestrzenia się w routerach

Lut: Routery Linksys infekowane poprzez lukę we wbudowanym oprogramowaniu rozpowszechniają kopie robaka

Rozszerzenie Coremax przejmuje kontrolę nad przeglądarkami

Kwi: Rozszerzenie przeglądarki przejmuje kontrolę nad reklamami i przekierowuje użytkowników do niechcianej witryny

Zgłoszono oszukańczą aplikację Virus Shield w Play Store

Kwi: Niedziałająca aplikacja usunięta, nabywcy otrzymali zwrot pieniędzy

„Policyjne" oprogramowanie atakuje Androida

Maj: Złośliwy program Koler próbuje zablokować zainfekowane urządzenie i wyświetla żądanie okupu

Rootkit BlackEnergy do Windows 8

Cze: Do usługi VirusTotal przekazano próbkę o celowo ograniczonej funkcjonalności

Havex poluje na systemy ICS/SCADA

Cze: Złośliwy program używany do ukierunkowanych ataków szuka systemów automatyki przemysłowej

LUKI W ZABEZPIECZENIACH

Wydano aktualizacje iOS naprawiające poważny błąd w obsłudze SSL

Lut: Luka w zabezpieczeniach SLL mogła pozwolić napastnikom na przechwytywanie ruchu między użytkownikami

Aktywne ataki na nową usterkę dnia zerowego w IE

Lut: Usterka CVE-2014-1776 w przeglądarkach IE 10 i 9 umożliwia instalację złośliwego oprogramowania

Ataki dnia zerowego na Flash Player

Lut: Adobe wydaje nadzwyczajną poprawkę usterki używanej do cichego instalowania złośliwych programów

Usterka dnia zerowego używana w ukierunkowanych atakach na Word

Mar: Dokumenty-przynęty RTF wykorzystują usterkę do zdalnego wykonywania kodu

Usterka Heartbleed na czołówkach gazet

Kwi: Miliony witryn, telefonów narażone na atak z powodu usterki w OpenSSL

Aktualizacja Java SE naprawia 37 usterek, w tym kilka krytycznych

Kwi: Poprawka rozwiązuje liczne problemy, w tym 4 uznawane za „najbardziej krytyczne"

Win XP uwzględnione w nadprogramowej poprawce

Maj: Microsoft robi wyjątek i wydaje poprawkę IE8 dla wycofanego z użytku systemu operacyjnego

Giganci technologiczni finansują ważne projekty

Maj: Fundacja Core Infrastructure Initiative będzie finansować m.in. OpenSSL, OpenSSH

PODSUMOWANIE KRAJOBRAZU
ZAGROŻEŃ

Trendy ogólne

Najbardziej zauważalnym trendem w pierwszej połowie 2014 r. była rosnąca ilość oprogramowania do wymuszania okupu, zarówno na platformach stacjonarnych, jak i mobilnych. Choć czerwcowa akcja przeciwko botnetowi **Zeus**[1] ograniczyła zagrożenie ze strony **Cryptolockera** (przynajmniej na jakiś czas), oprogramowanie wymuszające okup nadal się rozwijało; w minionym półroczu istniejące zagrożenia, takie jak **Cryptolocker**, zmieniły metody dystrybucji, szyfrowania i płatności, aby zapobiec działaniom podjętym przez organa ścigania.

Oprogramowanie do wymuszania okupu przeskoczyło na platformy mobilne, a pierwszą próbą zdobycia przyczółka w Androidzie był **Koler**[2]. Ten złośliwy program groził zaszyfrowaniem plików, choć w rzeczywistości tego nie robił, ale oprogramowanie **Slocker**, które pojawiło się wkrótce później, już tak[3]. Jak to zwykle bywa w przypadku zagrożeń dla Androida, oba te programy do wymuszania okupu udają legalne aplikacje, aby nakłonić użytkownika do ich zainstalowania.

Tymczasem próby wymuszania okupu na urządzeniach iOS przybrały inną formę. Funkcja blokady aktywacji wprowadzona w iOS 7 służy do zdalnego blokowania urządzenia iOS za pomocą hasła Apple ID. Przestępcy nadużywają jej, oferując użytkownikom nazwę i hasło Apple ID, które rzekomo umożliwiają dostęp do „bezpłatnej" treści. Jeśli użytkownik złapie przynętę i użyje tych poświadczeń do autoryzowania swojego urządzenia iOS, przestępcy zmieniają hasło, blokując urządzenie i zasadniczo przejmując nad nim kontrolę do czasu uzyskania okupu. Najbardziej godnym uwagi przypadkiem wymuszania okupu na platformie iOS był incydent z **„Olegiem Plissem"**, do którego doszło w maju w Australii i który zakończył się zatrzymaniem dwóch osób w Moskwie[4].

Jednocześnie badacze bezpieczeństwa poinformowali[5], że na podziemnych forach toczą się dyskusje dotyczące opracowania pakietu „zrób to sam" do tworzenia oprogramowania wymuszającego okup. Choć jeszcze do tego nie doszło, to zważywszy na to, że większość innych form złośliwego oprogramowania zaczyna od kodu pisanego na zamówienie, a kończy na seryjnej produkcji metodą „zbuduj to kliknięciem", wydaje się prawdopodobne, że prędzej czy później powstanie **pakiet do tworzenia oprogramowania wymuszającego okup**.

Wydarzenia te zbiegły się w czasie z coraz liczniejszymi raportami o ukierunkowanych atakach na firmy i instytucje rządowe, w których napastnicy gromadzą dane i przetrzymują je dla okupu, jak w głośnym incydencie z Nokią w roli głównej[6]. Sukcesy tych programów i ataków tylko podkreślają znaczenie ochrony danych dla użytkowników domowych, korporacyjnych i rządowych.

Tymczasem **Windows XP** zostało ostatecznie wycofane z użytku 8 kwietnia 2014 r. (niezależnie od nadprogramowej poprawki, która wyszła wkrótce po oficjalnym zakończeniu wsparcia). Pomimo zachęt do przejścia na Windows 8 (albo dowolny inny system, który jest aktywnie wspierany) szacuje się, że od 10 do 30 proc. osobistych komputerów na świecie nadal używa systemu operacyjnego, który pozostaje ulubionym celem napastników, a obecnie nie jest już łatany. Choć niektórzy użytkownicy (zwłaszcza rządowi i korporacyjni) dysponują przedłużonym wsparciem XP, dla innych bezpieczeństwo będzie w coraz większym stopniu kwestią „samoobsługi".

W pierwszej połowie 2014 r. pojawiły się również liczne raporty o budzącym wątpliwości monitoringu, cenzurze lub przetwarzaniu danych przez instytucje rządowe w wielu krajach. Duże firmy technologiczne podejmują różne działania, aby zwiększyć bezpieczeństwo swoich produktów, a także wywierają nacisk na swoje rządy, domagając się zwiększenia przejrzystości. Więcej informacji można znaleźć w naszym kalendarzu incydentów w pierwszej połowie 2014 r.

Złośliwe oprogramowanie do komputerów PC

Jak pokazuje statystyka 10 najczęstszych detekcji, w pierwszej połowie 2014 r. najczęstszymi zagrożeniami zgłaszanymi do naszych systemów telemetrycznych przez użytkowników produktów F-Secure były głównie te same rodziny złośliwego oprogramowania, które zaobserwowano w drugiej połowie roku, choć w innej kolejności. **Downadup** (w mediach nazywany również Confickerem) to najczęściej zgłaszane zagrożenie w tym półroczu, zwłaszcza na Bliskim Wschodzie, w Ameryce Południowej i w Azji. Ten sześcioletni robak nadal dobrze prosperuje, a zakończenie wsparcia dla Windows XP raczej nie poprawi sytuacji.

W minionym półroczu oprócz Downadupa najbardziej widocznymi zagrożeniami w Europie i Ameryce Północnej były **Majava** i **ataki przeglądarkowe. Sality i Ramnit**, rodziny oprogramowania infekującego pliki, również pojawiły się już kilka lat temu, ale nadal nękają użytkowników we wszystkich regionach poza Ameryką Północną i Europą.

Debiutantami w pierwszej dziesiątce są rodziny Wormlink, BrowserExploit i Expiro. Co ciekawe, godną uwagi zmianą w pierwszej połowie bieżącego roku jest to, że wykrycia konkretnych, znanych exploitów (np. CVE-2013-2471) zniknęły z naszej listy 10 najczęstszych detekcji.

10 NAJCZĘSTSZYCH DETEKCJI

Złośliwe oprogramowanie do Maca

Rok 2014 zaczął się od wykrycia niemal 20 nowych, unikatowych wariantów tylko w ciągu pierwszych dwóch miesięcy, choć później tempo zmniejszyło się i do końca pierwszego półrocza ostatecznie znaleziono 25 nowych zagrożeń dla Maca. Spośród tych nowych unikatowych wariantów 13 należy do 5 nowych rodzin, takich jak programy **Mask** i **Clientsnow** używane do ataków ukierunkowanych. Pozostałe 3 nowe rodziny — **Coinstealer**, **Cointhief** i **LaoShu** — atakują zwykłych użytkowników Maca. Więcej informacji o nowych rodzinach złośliwego oprogramowania do Maca znajduje się na stronie 14.

Zagrożenia mobilne

W pierwszym kwartale 2014 r. pojawiło się kilka godnych uwagi nowości w dziedzinie złośliwego oprogramowania mobilnego (opisanego szczegółowo w naszym raporcie o zagrożeniach mobilnych za 1 kwartał 2014 r.). W drugim kwartale 2014 r. większość zagrożeń, które użytkownicy aplikacji Mobile Security for Android zgłosili do naszych systemów telemetrycznych, nadal była wymierzona w platformę Android. Jednym z głównych typów złośliwego oprogramowania mobilnego pozostają też trojany, które zwykle wykorzystują metody socjotechniczne, aby uzyskać dostęp do urządzenia i przechowywanych w nim danych. Trzy najczęściej zgłaszane zagrożenia to rodziny **SMSSend**, **FakeInst** i **Eropl**. Ponadto w okresie tym w urządzeniach z Androidem nieoczekiwanie zaobserwowano dwa robaki SMS-Worm, dziś należące już do rzadkości. Więcej informacji o złośliwym oprogramowaniu do Androida można znaleźć na stronie 12.

Złośliwe oprogramowanie do systemu iOS

Złośliwe aplikacje działające na platformie iOS są bardzo nieliczne, ale istnieją. Inaczej niż w Androidzie, złośliwe oprogramowanie do systemu iOS było dotychczas skuteczne tylko przeciwko urządzeniem po jailbreaku, przez co narzędzia do jailbreaków tworzone przez grupy hakerskie (zwykle wykorzystujące nieudokumentowane usterki w platformie) były przedmiotem zainteresowania badaczy bezpieczeństwa. W czerwcu wydano narzędzie Pangu do systemu iOS 7.1.1, które rzekomo miało używać wykradzionych exploitów oraz instalować „szemrany" sklep z pirackimi aplikacjami. Oba problemy rozwiązano w późniejszej aktualizacji[8].

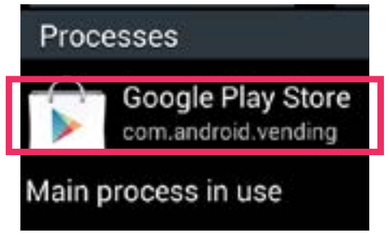
Wcześniej w pierwszym półroczu użytkownicy serwisu reddit informowali o podejrzanym pliku bibliotecznym, który później nazwano **Unflod Baby Panda**. Kiedy ten złośliwy program zostanie zainstalowany w urządzeniu iOS po jailbreaku, monitoruje wychodzące połączenia SSL, aby wykradać nazwy i hasła Apple ID[9]. Więcej informacji o złośliwym oprogramowaniu do Maca znajduje się na stronie 14.

Niezmienniki

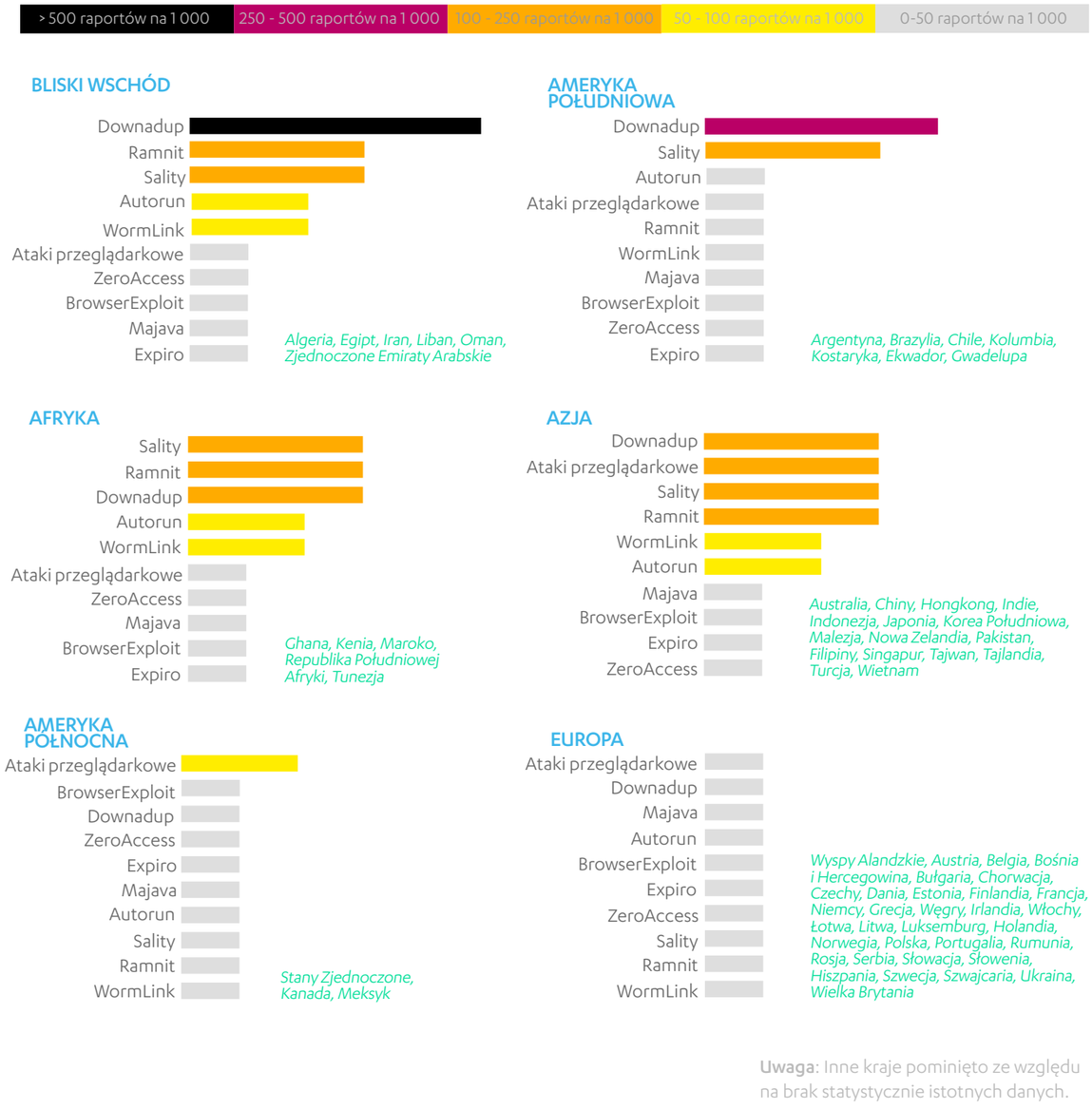
Pomimo różnych innowacji i postępów, które zaobserwowaliśmy w minionym kwartale, wiele ustaleń dotyczących bezpieczeństwa urządzeń mobilnych nie zmieniło się od czasu opublikowania naszego raportu o zagrożeniach za drugą połowę 2013 r. Kiedy w pierwszej połowie 2014 r. ponownie przyjrzeliśmy się bezpieczeństwu sklepów z aplikacjami (porównując liczbę złośliwych próbek z łączną liczbą próbek otrzymanych ze sklepu), nie dostrzegliśmy większych zmian w stosunku do wyników udokumentowanych w poprzednim raporcie. Pomimo informacji o czterech złośliwych aplikacjach wycofanych z Google Play Store w pierwszym półroczu, zważywszy na ogromną liczbę dostępnych aplikacji, niską (jak dotychczas) częstość występowania złośliwych programów oraz szybką reakcje na zgłaszane zagrożenia, Play Store pozostaje najbezpieczniejszym internetowym sklepem z aplikacjami mobilnym.

Nazwy pakietów używane przez złośliwe aplikacje do Androida również nie uległy większym zmianom. Większość pakietów nosi albo nazwę fałszywą, lecz naturalnie brzmiącą (np. com.software.app), albo składającą się z przypadkowych znaków (np. fkjsgmjl.ceinnykas). Nonsensowne nazwy są szczególnie częste w rodzinie Fakeinst.

Choć sprawdzanie nazwy oprogramowania pozostaje standardowym środkiem ostrożności w przypadku zagrożeń dla komputerów stacjonarnych, trudno stosować tę radę w Androidzie, ponieważ nazwa pakietu jest rzadko pokazywana użytkownikom i widoczna tylko w przypadku działających procesów w menu Ustawienia > Aplikacje > Pracują > Procesy. Prawdopodobnie szybko się to nie zmieni, więc zachowywanie czujności podczas pobierania aplikacji obecnie jest najskuteczniejszym sposobem na uniknięcie trojanów.



10 NAJCZĘSTSZYCH DETEKCJI
WG. REGIONU NA 1 000 UŻYTKOWNIKÓW



Uwaga: Inne kraje pominięto ze względu na brak statystycznie istotnych danych.

ŹRÓDŁA

1. Federal Bureau of Investigations; *GameOver Zeus Botnet Disrupted*; 2 czerwca 2014; http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted/gameover-zeus-botnet-disrupted
2. F-Secure Weblog; *"Police Ransomware" Expands To Android Ecosystem*; 16 Czerwca 2014; http://www.f-secure.com/weblog/archives/00002704.html
3. F-Secure Weblog; *SLocker Android Ransomware Communicates Via Tor And SMS*; 16 Czerwca 2014; http://www.f-secure.com/weblog/archives/00002716.html
4. Info Security; *'Oleg Pliss' Apple Hackers Could Be Behind Bars*; 10 Czerwca 2014; http://www.infosecurity-magazine.com/news/oleg-pliss-apple-hackers-could-be/
5. Arstechnica; Dan Goodin; *Researchers warn of new, meaner ransomware with unbreakable crypto*; 7 Stycznia 2014; http://arstechnica.com/security/2014/01/researchers-warn-of-new-meaner-ransomware-with-unbreakable-crypto/
6. BBC; *Nokia 'paid blackmail hackers millions'*; 18 Czerwca 2014; http://www.bbc.com/news/technology-27909096
7. Tech Republic; Tony Bradley; *Windows XP use declining, but millions still willingly at risk*; 16 Kwietnia 2014; http://www.techrepublic.com/article/windows-xp-use-declining-but-millions-still-willingly-at-risk/
8. International Business Times; *Pangu 1.1.0 Apple iOS 7.1.1 Jailbreak Update Adds Mac OS X Support And Removes 25PP Option*; 30 Czerwca 2014; http://www.ibtimes.com/pangu-110-apple-ios-711-jailbreak-update-adds-mac-os-x-support-removes-25pp-option-1615366
9. SektionEins; *iOS Malware Campaign "Unflod Baby Panda"*; 18 Kwietnia 2014; https://sektioneins.de/en/blog/14-04-18-iOS-malware-campaign-unflod-baby-panda.html

2 KWARTAŁ 2014 ZŁOŚLIWE OPROGRAMOWANIE MOBILNE

NOWE RODZINY lub WARIANTY

294 Android

1 iPhone

Trojan:iPhoneOS/SSLCredThief
Podpisany plik biblioteczny monitoruje wychodzące połączenia SSL, aby kraść nazwy i hasła Apple ID.

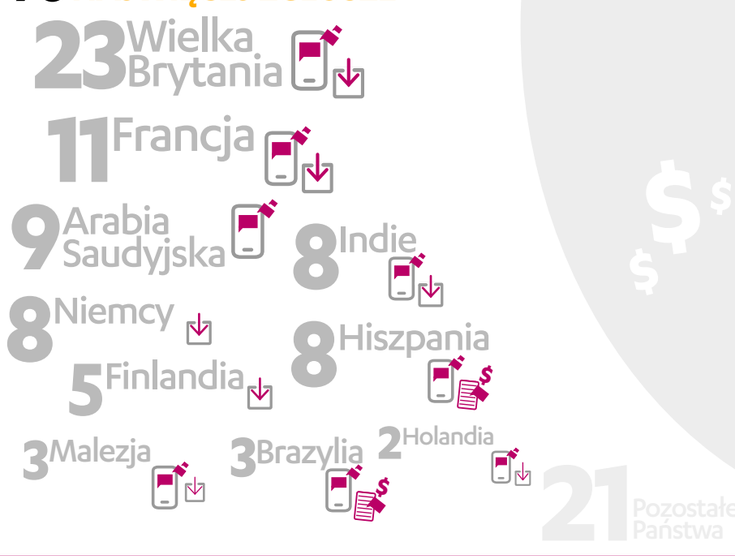
3 CZOŁOWE RODZINY ANDROID

Trojan:Android/SMSSend
Duża rodzina złośliwych programów, które wysyłają wiadomości SMS na numery typu premium.

Trojan:Android/FakeInst
Pozoruje instalator aplikacji, a w rzeczywistości wysyła wiadomości SMS na numery typu premium.

Trojan:Android/Eropl
Po cichu gromadzi dane z urządzenia i przekazuje je do zdalnego serwera.

% KRAJE, Z KTÓRYCH POCHODZI NAJWIĘCEJ ZGŁOSZE



WYMUSZENIE OKUPU

Pierwszy program do wymuszania wymuszający okup (prawie)

Trojan:Android/Koler to mobilna wersja „policyjnego" oprogramowania Reveton do wymuszania okupu. Po raz pierwszy odkryta w maju, aplikacja oferuje dostęp do treści dla dorosłych, ale po instalacji domaga się „kary" za „naruszenie bezpieczeństwa" (lub coś podobnego). Choć informuje, że szyfruje pliki w urządzeniu, w rzeczywistości tylko wyłącza przycisk Wstecz, aby utrzymać na ekranie żądanie okupu.

Pierwszy program do wymuszania okupu z szyfrowaniem i obsługą sieci Tor

Inaczej niż Koler, odkryty w czerwcu Trojan:Android/Slocker szyfruje obrazy, dokumenty i pliki wideo w urządzeniu. Podobnie jak Koler wyłącza przycisk Wstecz, aby zakłócić kontrolę użytkownika nad urządzeniem. Warianty Slockera mogą komunikować się z serwerem dowodzenia za pośrednictwem sieci Tor albo wiadomości SMS.

Oleg Pliss uderza w Australii

W maju „Oleg Pliss" zablokował konta kilku użytkowników w Australii, podobno używając funkcji „Znajdź mój iPhone", i domagał się okupu. Apple zaprzeczyło spekulacjom o luce w usłudze iCloud (niektóre raporty sugerowały, że przyczyną było wyłudzenie informacji). W czerwcu w Moskwie aresztowano dwie osoby w związku z tym atakiem.

WIADOMOŚCI

Oprogramowanie szpiegowskie prosto z fabryki

Firma specjalizująca się w bezpieczeństwie informuje, że odkryła smartfon dostarczany prosto z fabryki ze szpiegowskim kodem (**Trojan:Android/SmsSend.AC**) wbudowanym w oprogramowanie urządzenia, który zapewniałby kontrolującej go osobie pełen dostęp do danych zapisanych w telefonie.

Prepaid card-stealer

Trojan:Android/Cardbuyer podobno potrafi obchodzić procesy weryfikacji używane przez platformy gier lub płatności internetowych i przechwytuje wiadomości SMS, aby po cichu kupować przedpłacone karty na rachunek ofiary.

iDroidBot w sprzedaży

W kwietniu na rosyjskich podziemnych forach pojawiły się reklamy programu iDroidbot, który atakuje urządzenia z systemami iOS 7.1 oraz Android i potrafi m.in. wykradać zapisane informacje o kartach kredytowych oraz środki z portfeli QIWI.

Kradzieże Apple ID

Użytkownicy serwisu reddit poinformowali o podejrzanym pliku bibliotecznym, który po instalacji podłącza się do wszystkich działających procesów i monitoruje wychodzące połączenia SSL, aby kraść nazwy i hasła Apple ID. Złośliwy program później nazwano Unflod Baby Panda.

Worm: Android/ Samsapo. A

Это твои фото?

Russian: Czy to twoje zdjęcie?

Łącze w wiadomości SMS pobiera aplikację, która m.in. rejestruje telefon w usłudze typu premium, wykrada dane i wysyła samą siebie do wszystkich kontaktów.

"Dear [NAME], Look the Self-time, http://goo.gl/******

Łącze w wiadomości SMS pobiera aplikację „SelfTimer", która wysyła wiadomość tekstową do 20 kontaktów i prosi użytkowników o pobranie dodatkowego pliku.

Worm: Android/ Selfmite

W Play Store

Virus Shield

W kwietniu witryna Android Police poinformowała, że Virus Shield, oprogramowanie zabezpieczające, które trafiło na szczyt rankingu płatnych aplikacji w Google Play Store (ponad 10 000 pobrań i ocena 4,7 gwiazdki) w rzeczywistości było oszustwem. Google następnie wycofał je ze sprzedaży i zaoferował nabywcom aplikacji zwrot pieniędzy oraz kredyt na zakupy w sklepie.

★★★★ 3.99

BankMirage

Złośliwy klon legalnej aplikacji izraelskiego banku Mizrahi, który wykrada identyfikatory użytkowników z formularza logowania wewnątrz aplikacji. Badacze spekulują, że zaprojektowano go w celu zgromadzenia danych do późniejszego ataku, ponieważ aplikacja jawnie ignoruje hasła. Złośliwe oprogramowanie były dostępne w Play Store tylko przez kilka dni, po czym zostało odkryte przez firmę zajmującą się bezpieczeństwem i szybko usunięte.

BEZPŁATNE

Songs i Prized

Te dwie bezpłatne aplikacje działają podobnie, jak programy do wydobywania kryptowalut dostępne w niezależnych sklepach z aplikacjami. Po cichu zajmują się generowaniem cyfrowej waluty, kiedy urządzenie jest ładowane, i zapobiegają jego przejściu w stan uśpienia. Obie aplikacje zostały usunięte z Play Store wkrótce po wykryciu.

BEZPŁATNE

ŹRÓDŁA

1. Malware don't need Coffee; Kafeine; *Police Locker land on Android Devices*; 4 Maja 2014; http://malware.dontneedcoffee.com/2014/05/police-locker-available-for-your.html
2. McAfee Blog; Christiaan Beek; *iDroid Bot for Sale Taps Into Mobile Wallet*; 10 Kwietnia 2014; https://blogs.mcafee.com/mcafee-labs/idroid-bot-for-sale-taps-into-mobile-wallets
3. Apple Insider; *Hackers use 'Find My iPhone' to lockout, ransom Mac and iOS device owners in Australia*; 26 Maja 2014; http://appleinsider.com/articles/14/05/27/hackers-break-into-lock-macs-and-ios-devices-for-ransom-in-australia
4. GData Security Blog; *Android smartphone shipped with spyware*; 16 Czerwca 2014; https://blog.gdatasoftware.com/blog/article/android-smartphone-shipped-with-spyware.html
5. Palo Alto Networks Research Center; Claud Xiao, Zhi Xu; *Cardbuyer: New Smart Android Trojan Defeats Multi-factor Verification and Steals Prepaid Game Cards*; 24 Kwietnia 2014; http://researchcenter.paloaltonetworks.com/2014/04/cardbuyer-new-smart-android-trojan/
6. SektionEins; *iOS Malware Campaign "Unflod Baby Panda"*; 18 Kwietnia 2014; https://sektioneins.de/en/blog/14-04-18-iOS-malware-campaign-unflod-baby-panda.html
7. WeliveSecurity; Robert Lipovsky; *Android malware worm catches unwary users*; 30 Kwietnia 2014; http://www.welivesecurity.com/2014/04/30/android-sms-malware-catches-unwary-users/
8. Naked Security; Paul Ducklin; *Anatomy of an Android SMS virus - watch out for text messages, even from your friends!*; 29 Czerwca 2014; http://nakedsecurity.sophos.com/2014/06/29/anatomy-of-an-android-sms-virus-watch-out-for-text-messages-even-from-your-friends/
9. Android Police; Michael Crider; The #1 New Paid App In The Play Store Costs $4, Has Over 10,000 Downloads, A 4.7-Star Rating... And It's A Total Scam [Updated]; 10 Kwietnia 2014; http://www.androidpolice.com/2014/04/06/the-1-new-paid-app-in-the-play-store-costs-4-has-over-10000-downloads-a-4-7-star-rating-and-its-a-total-scam/
10. Lookout Blog; Meghan Kelly; *Cloned banking app stealing usernames sneaks into Google Play*; 24 Czerwca 2014; https://blog.lookout.com/blog/2014/06/24/bankmirage/
11. ZDNet; Liam Tung; *Google yanks two battery-sucking Bitcoin mining Android apps from Play store*; 28 Marca 2014; http://www.zdnet.com/google-yanks-two-battery-sucking-bitcoin-mining-android-apps-from-play-store-7000027828/

1 POŁOWA 2014 ZŁOŚLIWE OPROGRAMOWANIE DO MACA

25
NOWYCH WARIANTÓW
złośliwego oprogramowania do Maca odkryto
OD STYCZNIA DO CZERWCA 2014

60% Tylne drzwi
24% Trojan
16% Inne

19 nowych, unikalnych **WARIANTÓW**
odkryto tylko w pierwszych dwóch miesiącach

Tempo to zmniejszyło się z biegiem półrocza, ponieważ złośliwe oprogramowanie do Maca zwykle pojawia się falami.

13 WARIANTOW spośród 25 należy do

5 NOWYCH RODZIN

2 używanych w atakach ukierunkowanych

3 atakujących zwykłych użytkowników Maca

MASK
Rodzina **Mask** jest elementem głośnej cyberszpiegowskiej operacji znanej jako „The Mask". Atakuje instytucje rządowe i firmy energetyczne.

CLIENTSNOW
Rodzina **Clientsnow** ma powiązania z GhostNet. Jest jedną z wielu rodzin złośliwego oprogramowania do Maca używanych w atakach ukierunkowanych na społeczności tybetańskie i ujgurskie.

LAOSHU
Rodzina **LaoShu** (co po chińsku oznacza szczura lub mysz) to malware typu remote access trojan (RAT), który rozprzestrzenia się przez fałszywe powiadomienia mailowe.

COINTHIEF
Rodzina **CoinThief** to trojańskie programy szpiegowskie przeznaczony do kradzieży kryptowalut. Od drugiego kwartału 2013 r. rozprzestrzeniała się niepostrzeżenie przez BitTorrent, udając złamane wersje popularnych aplikacji do systemu OS X. Jednak na początku 2014 r. zmieniła taktykę i zaczęła rozprzestrzeniać się za pośrednictwem „strojanizowanych" aplikacji do obsługi kryptowalut, które są dostępne w repozytoriach online, takich jak Github, oraz popularnych serwisach z oprogramowaniem, takich jak *downloads.com*.

Zmiana taktyki okazała się skuteczna, ponieważ osoby szukające aplikacji związanych z kryptowalutami zazwyczaj są już w posiadaniu pewnej ilości kryptowaluty[1], a większość z nich nie spodziewa się, że trafi na strojanizowaną aplikację w legalnej witrynie. Doprowadziło to do zainfekowania wielu komputerów, a w końcu do odkrycia tej rodziny[2].

COINSTEALER
Rodzina **Coinstealer** to programy do kradzieży bitmonet, które udają aplikację back office[3] umożliwiającą dostęp do zastrzeżonej bazy transakcji z serwisu Mt. Gox. Były one rozpowszechniane ze złamanego konta na Reddicie i z osobistego blogu dyrektora generalnego Mt. Gox[4] po tym, jak giełda wymiany bitmonet zawiesiła działalność bez wyjaśnienia[5]. Prawdopodobnie była próbą wykorzystania stanu psychicznego klientów Mt. Gox, którzy wówczas usilnie poszukiwali dodatkowych informacji.

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

ZASOBY

1. Twitter; Broderick Aquilino; 12 Lutego 2014; https://twitter.com/BrodAquilino/status/433529401699864576
2. Threatpost; Michael Mimoso; *Mac Trojan Steals Bitcoin Wallet Credentials*; 10 Lutego 2014; http://threatpost.com/mac-trojan-steals-bitcoin-wallet-credentials/104152
3. Wikipedia; *Front and back office application*; 24 Marca 2014; http://en.wikipedia.org/wiki/Front_and_back_office_application
4. Forbes; Andy Greenberg; *Hackers Hit Mt. Gox Exchange's CEO, Claim To Publish Evidence Of Fraud*; 9 Marca 2014; http://www.forbes.com/sites/andygreenberg/2014/03/09/hackers-hit-mt-gox-exchanges-ceo-claim-to-publish-evidence-of-fraud/
5. Forbes; Andy Greenberg; *Bitcoin's Price Plummets As Mt. Gox Goes Dark, With Massive Hack Rumored*; 25 Lutego 2014; http://www.forbes.com/sites/andygreenberg/2014/02/25/bitcoins-price-plummets-as-mt-gox-goes-dark-with-massive-hack-rumored/

ŹRÓDŁA

KALENDARZ INCYDENTÓW

CYFROWA WOLNOŚĆ

1. The Guardian; Spencer Ackerman, James Ball; *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ*; 28 Lutego 2014; http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo
2. Arstechnica; Sean Gallagher; *Turkey now trying to block YouTube as social media crackdown continues*; 28 Marca 2014; http://arstechnica.com/tech-policy/2014/03/turkey-now-trying-to-block-youtube-as-social-media-crackdown-continues/
3. Reuters; *Thai ministry sparks alarm with brief block of Facebook*; 28 Maja 2014; http://in.reuters.com/article/2014/05/28/thailand-politics-facebook-idINKBN0E80U520140528
4. Arstechnica; Sean Gallagher; *NSA loves The Bahamas so much it records all its cellphone calls*; 21 Maja 2014; http://arstechnica.com/tech-policy/2014/05/nsa-loves-the-bahamas-so-much-it-records-all-its-cellphone-calls/
5. Guardian; Glenn Greenwald; *How the NSA tampers with US-made internet routers*; 12 Maja 2014; http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden
6. BBC; Joe Miller; *Iraq blocks Facebook and Twitter in bid to restrict Isis*; 16 Czerwca 2014; http://www.bbc.com/news/technology-27869112
7. CNET; Micheal Tan; *After Thailand's coup, a stifling of online dissent (Q&A)*; 12 Czerwca 2014; http://www.cnet.com/news/behind-thailands-high-tech-coup-stifling-online-dissent-q-a/
8. BBC; *YouTube access restored in Turkey*; 4 Czerwca 2014; http://www.bbc.com/news/technology-27691892

ATAKI

9. Forbes; James Lyne; *Yahoo Hacked And How To Protect Your Passwords*; 31 Stycznia 2014; http://www.forbes.com/sites/jameslyne/2014/01/31/yahoo-hacked-and-how-to-protect-your-passwords/
10. Arstechnica; Dan Goodin; *Hackers hijack 300,000-plus wireless routers, make malicious changes*; 4 Marca 2014; http://arstechnica.com/security/2014/03/hackers-hijack-300000-plus-wireless-routers-make-malicious-changes/
11. Reuters; *Bitcoin bank Flexcoin shuts down after theft*; 4 Marca 2014; http://www.reuters.com/article/2014/03/04/us-bitcoin-flexcoin-idUSBREA2329B20140304
12. TechRadar; Stu Robarts; *Windigo malware attack infects 25,000 servers*; 19 Marca 2014; http://www.techradar.com/news/computing/windigo-malware-attack-infects-25-000-servers-1235128
13. NYTimes; Nicole Perlroth; Heartbleed exploited to hack VPN device; 18 Kwietnia 2014; http://bits.blogs.nytimes.com/2014/04/18/heartbleed-internet-security-flaw-used-in-attack/?_php=true&_type=blogs&_r=0
14. The Australian; Cyber attacks on the rise; 29 Maja 2014; http://www.theaustralian.com.au/news/latest-news/cyber-attacks-on-the-rise/story-fn3dxiwe-1226936311311?nk=9a4d4fc48406e6e6a41b8e14de5fa4d6
15. KrebsonSecurity; Brian Krebs; *True Goodbye: 'Using TrueCrypt Is Not Secure'*; 29 Maja 2014; http://krebsonsecurity.com/2014/05/true-goodbye-using-truecrypt-is-not-secure/
16. The Register; Darren Pauli; *Massive DDoS attack hits Hong Kong*; 23 Stycznia 2014; http://www.theregister.co.uk/2014/06/23/most_sophisticated_ddos_strikes_hk_democracy_poll/

BEZPIECZEŃSTWO

17. F-Secure Weblog; Sean Sullivan; *FISA Transparency*; 4 Lutego 2014; http://www.f-secure.com/weblog/archives/00002666.html
18. F-Secure Weblog; Sean Sullivan; *TrustyCon Video*; 28 Lutego 2014; http://www.f-secure.com/weblog/archives/00002679.html
19. ZDNet; Larry Seltzer; *Windows XP dies at 12 1/2 after long illness*; 8 Kwietnia 2014; http://www.zdnet.com/windows-xp-dies-at-12-12-after-long-illness-7000028134/
20. BBC; Leo Kelion; *eBay makes users change their passwords after hack*; 21 Maja 2014; http://www.bbc.com/news/technology-27503290
21. PCWorld; Mark Hachman; *Microsoft simplifies security updates with MyBulletins*; 28 Maja 2014; http://www.pcworld.com/article/2207346/microsoft-simplifies-security-updates-with-mybulletins.html
22. PC Mag; Stephanie Mlot; *Google launches 'right to be forgotten' form*; 30 Maja 2014; http://www.pcmag.com/article2/0,2817,2458736,00.asp
23. Forbes; Ben Kepes; *No More Scroogled, No More NSA, Google Apps Gets Encryption*; 21 Maja 2014; http://www.forbes.com/sites/benkepes/2014/05/21/no-more-scroogled-no-more-nsa-google-apps-gets-encryption/
24. The Guardian; Dominic Rushe; *Edward Snowden calls for greater online privacy in Reset the Net campaign*; 5 Czerwca 2014; http://www.theguardian.com/world/2014/jun/05/edward-snowden-privacy-reset-the-net

ŚCIGANIE

25. United States Department of Justice; *Cyber Criminal Pleads Guilty to Developing and Distributing Notorious Spyeye Malware*; 28 Stycznia 2014; http://www.justice.gov/opa/pr/2014/January/14-crm-091.html
26. United States Department of Justice; *Leader and Co-Conspirator of Android Mobile Device App Piracy Group Plead Guilty*; 24 Marca 2014; http://www.justice.gov/opa/pr/2014/March/14-crm-303.html
27. United States Department of Justice; *Nine Charged in Conspiracy to Steal Millions of Dollars Using "Zeus" Malware*; 11 Kwietnia 2014; http://www.justice.gov/opa/pr/2014/April/14-crm-375.html
28. The Register; Simon Sharwood; *'Anons' cuffed by Australian Federal Police*; 22 Maja 2014; http://www.theregister.co.uk/2014/05/22/anons_cuffed_by_australian_federal_police/
29. The Register; Iain Thomson; *US authorities name five Chinese military hackers wanted for espionage*; 19 Maja 2014; http://www.theregister.co.uk/2014/05/19/us_authorities_name_five_chinese_military_hackers_wanted_for_espionage/
30. SC Magazine UK; Doug Drinkwater; *100 hackers arrested over Blackshades Trojan*; 19 Maja 2014; http://www.scmagazineuk.com/100-hackers-arrested-over-blackshades-trojan/article/347488/
31. Info Security; *'Oleg Pliss' Apple Hackers Could Be Behind Bars*; 10 Czerwca 2014; http://www.infosecurity-magazine.com/news/oleg-pliss-apple-hackers-could-be/
32. United States Department of Justice; *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator*; 2 Czerwca 2014; http://www.justice.gov/opa/pr/2014/June/14-crm-584.html

ZŁOŚLIWE OPROGRAMOWANIE

33. Malware Must Die; *Threat Intelligence - New Locker: Prison Locker (aka: Power Locker ..or whatever those bad actor call it)*; 3 Stycznia 2014; http://blog.malwaremustdie.org/2014/01/threat-intelligence-new-locker-prison.html
34. F-Secure Weblog; Sean Sullivan; *Gameover ZeuS Jumps on the Bitcoin Bandwagon*; 14 Marca 2014; http://www.f-secure.com/weblog/archives/00002685.html
35. InfoSec Handlers Diary Blog; Johannes Ullrich; *Linksys Worm "TheMoon" Summary: What we know so far*; 13 Lutego 2014; https://isc.sans.edu/diary/Linksys+Worm+%22TheMoon%22+Summary%3A+What+we+know+so+far/17633
36. F-Secure Weblog; *Coremex Innovates Search Engine Hijacking*; 1 Kwietnia 2014; http://www.f-secure.com/weblog/archives/00002689.html
37. Android Police; Michael Crider; *The #1 New Paid App In The Play Store Costs $4, Has Over 10,000 Downloads, A 4.7-Star Rating... And It's A Total Scam [Updated]*; 10 Kwietnia 2014; http://www.androidpolice.com/2014/04/06/the-1-new-paid-app-in-the-play-store-costs-4-has-over-10000-downloads-a-4-7-star-rating-and-its-a-total-scam/
38. F-Secure Weblog; *"Police Ransomware" Expands To Android Ecosystem*; 15 Maja 2014; http://www.f-secure.com/weblog/archives/00002704.html
39. F-Secure Weblog; Broderick Aquilino; *BlackEnergy Rootkit, Sort Of*; 13 Czerwca 2014; http://www.f-secure.com/weblog/archives/00002715.html
40. F-Secure Weblog; Daavid Hentunen; *Havex hunts ICS/SCADA systems*; 23 Czerwca 2014; http://www.f-secure.com/weblog/archives/00002718.html

LUKI W ZABEZPIECZENIACH

41. ZDNet; Violet Blue; *Major Apple security flaw: Patch issued, users open to MITM attacks*; 22 Lutego 2014; http://www.zdnet.com/major-apple-security-flaw-patch-issued-users-open-to-mitm-attacks-7000026624/
42. KrebsonSecurity; Brian Krebs; *Microsoft Warns of Attacks on IE Zero-Day*; 27 Kwietnia 2014; http://krebsonsecurity.com/2014/04/microsoft-warns-of-attacks-on-ie-zero-day/
43. PCWorld; Ian Paul; *Adobe releases emergency Flash patch for Windows and OS X systems*; 8 Lutego 2014; http://www.pcworld.com/article/2027624/adobe-releases-emergency-patch-for-windows-and-os-x-systems.html
44. Arstechnica; Dan Goodin; Zero-day vulnerability in Microsoft Word under active attack; 25 Marca 2014; http://arstechnica.com/security/2014/03/zero-day-vulnerability-in-microsoft-word-under-active-attack/
45. CNet; Richard Nieva; *Heartbleed bug: What you need to know (FAQ)*; 11 Kwietnia 2014; http://www.cnet.com/news/heartbleed-bug-what-you-need-to-know-faq/
46. KrebsonSecurity; Brian Krebs; *Critical Java Update Plugs 37 Security Holes*; 16 Kwietnia 2014; http://krebsonsecurity.com/2014/04/critical-java-update-plugs-37-security-holes/
47. Bit-tech; Gareth Halfacree; *Windows XP gets first post-EOL security patch*; 2 Maja 2014; http://www.bit-tech.net/news/bits/2014/05/02/winxp-eol-patch/1
48. SCMagazine; Marcos Colon; *Tech giants to fund vital projects*; 29 Maja 2014; http://www.scmagazine.com/core-infrastructure-initiative-to-fund-openssl-audit/article/349068/

OCHRONA INTERNETU

to profesjonalny pakiet antywirusowy, dzięki któremu:

- Bez obaw korzystasz z **bankowości elektronicznej**
- **Twoje zdjęcia**, pliki i inne dokumenty są bezpieczne
- Nikt nie wykradnie haseł do Twojej **poczty czy portali społecznościowych**
- **Dzieci surfują po internecie** bezpiecznie, a Ty masz nad tym pełną kontrolę
- Zabezpieczysz **komputer i urządzenia mobilne** bo teraz dajemy Ci pełną ochronę

Więcej informacji na stronie www.ochronainternetu.play.pl

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

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

PC ADVISOR ONLINE
www.pcadvisor.co.uk

PLAY

Usługa świadczona przez Play i F-Secure od 2011 r.

SWITCH ON FREEDOM

© F-Secure Corporation 2014. Wszystkie prawa zastrzeżone.

F-Secure