TRUST IN GERMAN SICHERHEIT

G DATA Mobile Malware Raport

Threat Report H1 2014

Spis treści

W skrócie

- Z końcem roku, jak przewidują branżowi eksperci, możemy spodziewać się ponad 1,2 miliarda aktywnych urządzeń przenośnych z systemem Android. W pierwszej połowie roku na całym świecie sprzedano 563 miliony sprzętów spod znaku zielonego ludzika (489 milionów smartfonów i 74 miliony tabletów)
- W listopadzie 2014 roku prawie 70% użytkowników korzystało wciąż z przestarzałych wersji Androida. Jedynie 30,2% z nich posiadało najnowszą wersje tego mobilnego systemu operacyjnego.
- Liczba odkrywanych i opisywanych mobilnych wirusów wciąż rośnie. W drugiej połowie 2013 roku odkryto 672 940 nowe zagrożenia w porównaniu do 751 136 w pierwszej połowie roku 2014.
- W zestawieniu do analogicznego okresu w poprzednim roku (H12013/H12014) statystyki procentowe wyglądają zatrważająco. Wzrost sięgnął 43 punktów procentowych!
- Trzej muszkieterowie – szyfrowanie, oszustwa i wymuszenia. Zaobserwowaliśmy olbrzymi wzrost zainteresowania przestępców szkodnikami typu ransomware. Ten rodzaj zagrożeń jest dość łatwy do opracowania i przynosi szybkie zyski jego twórcom.
- Niezależne sklepy z aplikacjami stanowią duże ryzyko dla użytkowników, to za ich pomocą cyberprzestępcy dystrybuują aplikacje zawierające złośliwy kod.
- Nieautoryzowany firmware to często tak naprawdę backdoor. Wielu użytkowników chcąc poprawić działanie swoich urządzeń korzysta z oferty alternatywnego oprogramowania. Jego twórcy bardzo często posiłkują się ogólnie dostępnym w sieci darmowym kodem. To tylna furtka dla przestępców chcących zainfekować urządzenie.

Co nas czeka?

Tykająca bomba czyli luki w Androidzie.

Długie okresy oczekiwania na kolejne aktualizacje mobilnego systemu operacyjnego od Google zaczynają wyrastać na jeden z głównych problemów w kwestiach bezpieczeństwa urządzeń przenośnych. Kilka tygodni może zająć oczekiwanie użytkownika na aktualizacje systemu przysługującą jego konkretnemu modelowi urządzenia. W trakcie tego oczekiwania zoastają oni wystawieni na możliwe ataki. Wiele z urządzeń pozbawionych zostało możliwości zaktualizowania Androida. Niezamknięte luki w niezaktualizowanych systemach operacyjnych będą stanowiły coraz większe zagrożenie dla klientów prywatnych jak i firmowych.

Fabrycznie instalowane oprogramowanie szpiegujące.

W mijającym roku eksperci G DATA jako pierwsi na świeci odkryli i opisali przypadek fabrycznego oprogramowania szpiegującego dostarczanego wraz z firmwarem smartfonu jednego z chińskich producentów. Zgodnie z opiniami ekspertów, pojawiającymi się w dyskusjach na temat odkrycia oprogramowania spyware w telefonie Star N9500, taki przypadki jeżeli już nie są to z pewnością będą coraz częstsze. Możemy spodziewać się wykorzystywania fabrycznego oprogramowania jako nośnika dla złośliwych programów.

Zestawy do tworzenia szkodliwych programów

Zestawy do tworzenia złośliwych aplikacji na platformę Windows są powszechnie znane i dostępne w zakupie na podziemnych forach hakerskich. Zestawy do tworzenia złośliwych aplikacji mobilnych należały jeszcze niedawno do rzadkości, jednak w 2014 roku byliśmy świadkami pojawiania się takich ofert na cyberprzestępczym rynku. Eksperci z G DATA SecurityLabs oczekują w nadchodzących 12 miesiącach

większej ilości ofert umożliwiających przestępcom bez specjalistycznej wiedzy technicznej uzyskać możliwość tworzenia złośliwych aplikacji mobilnych. Będzie to miało ścisły związek z przewidywanym wzrostem ich liczby.

Infekcja – szyfrowanie – wyłudzanie

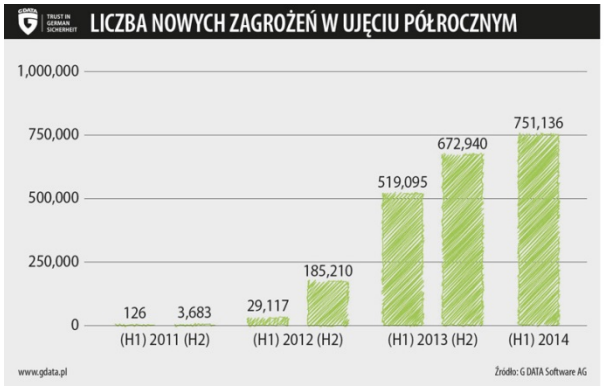
Liczba zagrożeń typu ransomware dla platformy mobilnej Android będzie wciąż rosła. Możemy spodziewać się jeszcze bardziej wyszukanych wariantów tego rodzaju zagrożeń. Najnowsza wersja Android 5.0 może ograniczyć rozpowszechnianie się ransomware ze względu na domyślne szyfrowanie danych w które została wyposażona.

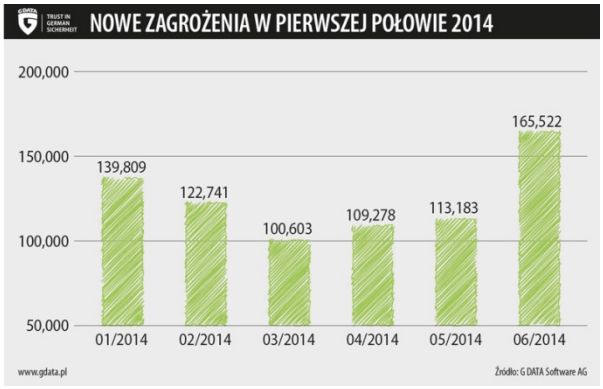
Fałszywa ochrona

FakeAV urósł do wielkiego problemu dla użytkowników mobilnych. Te tzw. aplikacje ochronne nie zabezpieczające przed żadnym zagrożeniem, a często będące zainfekowane złośliwym kodem, są coraz popularniejsze. Na początku roku dwie z takich aplikacji zrobiły furorę w androidowych marketach przynosząc ich twórcom ogromne zyski, jednocześnie w tym samym momencie nie dostarczając żadnej ochrony użytkownikom, którzy je zakupili.

Raport z rynku – codziennie pojawia się 4200 nowych próbek złośliwego oprogramowania mobilnego.

W ciągu pierwszych sześciu miesięcy tego roku eksperci bezpieczeństwa G DATA opisali 751 136 nowych próbek malware. Oznacza to wzrost rzędu 12% w porównaniu do drugiej połowy roku 2013, bezpośrednio poprzedzającego najnowsze badanie. Średnio każdego dnia do pracowników laboratorium trafiało 4200 nowych próbek.





Klasyfikacja i TOP 5

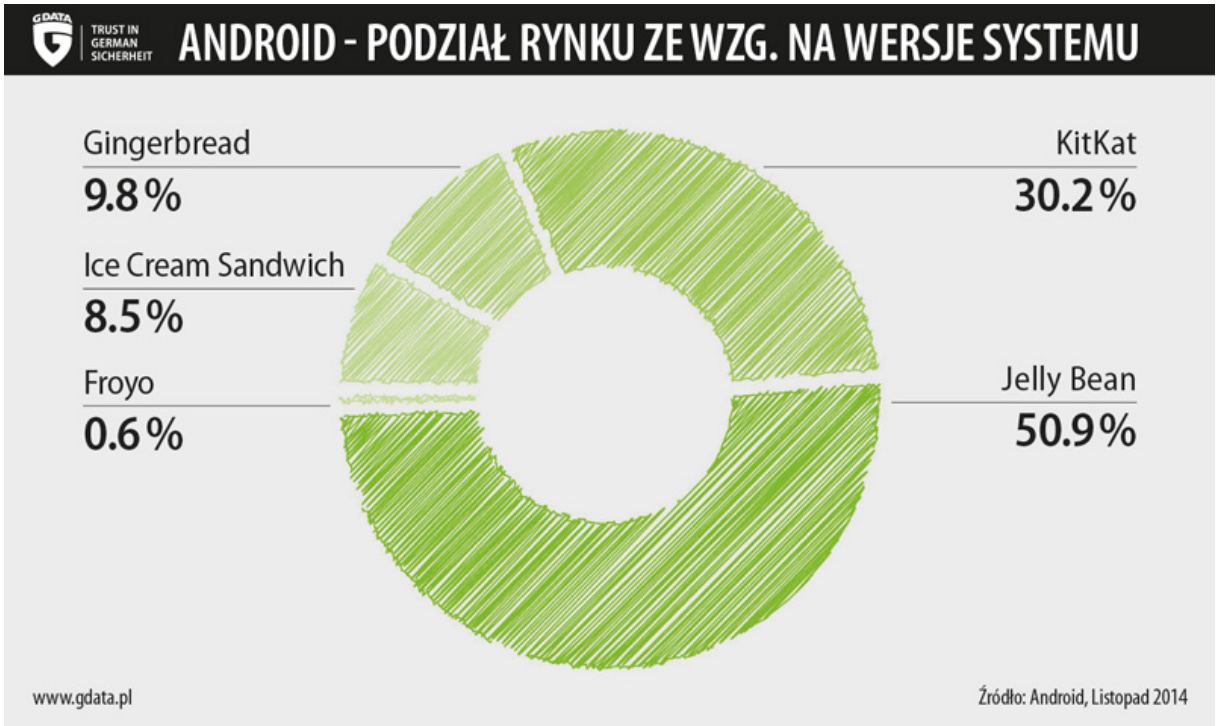
W oparciu o właściwości programów pracownicy laboratorium przypisują badane pliki do konkretnych rodzin złośliwego oprogramowania. Z przebadanych plików udało się scharakteryzować prawie 200 tysięcy szkodników. Aż cztery pozycje w TOP5 z wszystkich opisanych wariantów zajęły mobilne trojany! Duża liczba wariantów w porównaniu z poprzednim badanym półroczem spowodowana jest możliwością łatwiejszego ich tworzenia.

Malware z rodziny Backdoor.Gingermaster jest dystrybuowany z wykorzystaniem zmanipulowanych aplikacji dostępnych dla użytkowników w niezależnych androidowych marketach. Potrafi zrootować zainfekowane przez siebie urządzenie uzyskując tym samym pełną kontrolę oraz dostęp. Złośliwe oprogramowanie wykrada dane takie jak numer IMEI.

TOP5 rodzin z największą liczbą wariantów

Rodzina	Warianty
Trojan.Agent	740
Trojan.SMSSend	322
Backdoor.GingerMaster	154
Trojan.SMSForward	78
Trojan.SMSAgent	74

Wiele urządzeń mobilnych to tykające bomby z od długiego czasu nieaktualizowanym systemem operacyjnym. Długie okresy wyczekiwania na aktualizacje oprogramowania w zależności od producentów sprzętu to w chwili obecnej jeden z palących problemów bezpieczeństwa mobilnego. Starsze urządzenie dość często zostają pozbawione wsparcia, tym samym upgrade do nowszych wersji systemu z zielonym ludzikiem. Niema 70% urządzeń działa pod przestarzałym systemem. Jedynie 30,2% użytkowników korzysta z najnowszego w momencie przeprowadzania badania systemu w wersji KitKat 4.4.



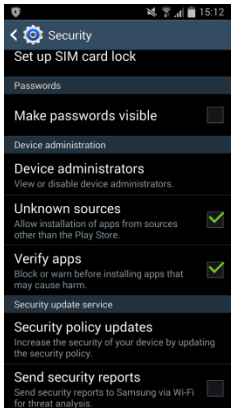
Ramsomware: rosnące ryzyko dla Androida

Ransomware (ang. ransom – okup) to specyficzny rodzaj złośliwego oprogramowania potrafiący zablokować dane użytkownika lub całe urządzenie. Szyfruje lub blokuje dostęp do danych zapisane na smartfonie lub tablecie. Szkodnik zagnieżdża się głęboko w systemie i po udanej infekcji próbuje wyświetlanymi komunikatami przekonać użytkownika, że jego urządzenie zostało zablokowane przez przedstawicieli organów państwowych (tzw. wirus policja).

By uwiarygodnić informacje o blokadzie oprogramowanie wykorzystuje moduł GPS do określenia pozycji urządzenia oraz prawdopodobnej narodowości właściciela. Użytkownik z Niemiec ujrzy fałszywy komunikat od Federalnej Policji Kryminalnej (BKA). W Polsce będą to Biuro Służby Kryminalnej lub Komenda Główna Policji.

Najczęściej padającym oskarżeniem jest posiadanie oraz przeglądanie treści pornograficznych na zaatakowanym urządzeniu. W dalszej treści komunikatu ofiara dowiaduje się o możliwości odblokowania urządzenia lub odszyfrowania danych po uiszczeniu odpowiedniej opłaty określanej jako grzywna. Płatności realizowane są z wykorzystaniem serwisów zapewniających anonimowość odbiorcom jak Paysafecard czy Ukash. Przestępcy zakładają, że większość użytkowników potraktuje oskarżenie jako powód do wstydu i będzie chciało jak najszybciej pozbyć się komunikatu i odblokować swoje urządzenie.

Jak ransomware dostaje się na urządzenie?



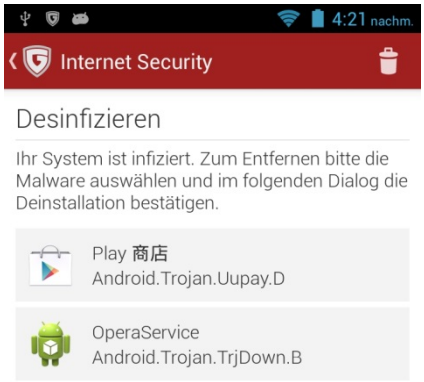
Szkodliwe pliki nie instalują się automatycznie, użytkownik sam inicjuje instalacje uruchamiając plik APK. Ściągając aplikacje mobilne z oficjalnego sklepu Google możemy być minimalnie spokojniejsi o nasze bezpieczeństwo, gdyż gigant z Redmond sprawdza wprowadzana do obiegu aplikacje pod kątem zwartości złośliwego kodu. Pozostałe sklepy tzw. third-part app stores w większości to całkowicie inny temat oraz odmienna polityka bezpieczeństwa. Oferują za darmo płatne oprogramowanie oraz aplikacje, które nie przeszyły i tak pobłażliwej selekcji Google Play. Dystrybuowane tam aplikacje mogą być zainfekowane mobilnym malwarem, a ich twórcy bazują na naiwności potencjalnych ofiar odwiedzających takie strony.

Użytkownicy odwiedzają takie sklepy, by zaoszczędzić lub całkowicie wyeliminować koszty przy instalowaniu nowych aplikacji na swoich urządzeniach. Proceder ten oczywiście nie jest do końca zgodny z obowiązującym prawem. By móc zainstalować aplikacje z nieznanego źródła użytkownicy muszą przekonfigurować funkcje systemu Android. W ustawieniach odpowiadających za bezpieczeństwo zezwalają urządzeniu na instalacje aplikacji ze źródeł innych niż sklep Google Play. Klient takiego sklepu niejako sam otwiera furtkę cyberprzestępcom do swoich danych i urządzenia przenośnego.

Spywarephone prosto z chińskiej fabryki

Wiosną tego roku specjaliści z G DATA SecurityLabs wykryli preinstalowany spyware na fabrycznie nowym smartfonie. Po raz pierwszy w historii specjaliści ds. bezpieczeństwa IT odkryli telefon z fabrycznym oprogramowaniem szpiegującym swojego właściciela. Dotychczas wielokrotnie podnoszono kwestie preinstalowanego malware'u na nowych urządzeniach. Słyszeliśmy już o złośliwym oprogramowaniu preinstalowanym na przenośnych pamięciach lub dyskach nowych komputerów, jednak to pracownicy G DATA SecurityLabs jako pierwsi na świecie wykryli trojana jako część firmware'u. Ukrywa się on pod wszystkim znaną nazwą Google Play Store i jest jedną ze standardowych aplikacji na badanym telefonie. Spyware działa w tle co skutecznie uniemożliwia jego wykrycie przez właściciela urządzenia. Również bez jego wiedzy smartfon wysyła prywatne dane zapisane w swojej pamięci na serwery znajdujące się w Chinach oraz posiada możliwość instalacji dodatkowych aplikacji.

Zmanipulowana aplikacja nie może zostać usunięta ze względu na jej pełną integracje z oprogramowaniem fabrycznym urządzenia.



Firmware zawierał trojana Android.Trojan.Uupay.D ukrywającego się pod aplikacją Google Play Store. Funkcje szpiegujące są całkowicie niewidoczne dla użytkownika i nie można ich w żaden sposób wyłączyć. Co to oznacza w praktyce? Chińscy sprawcy całego zamieszania posiadają całkowity dostęp do urządzenie oraz danych na nim zapisanych. Logi, które mogłyby zdemaskować działanie złośliwego oprogramowania są usuwane, a sam program blokuje instalacje aktualizacji odpowiedzialnych za zapewnienie bezpieczeństwa w systemie z zielonym ludzikiem.

Przegląd funkcji trojana:

- Uprawnienia
  instalacja i deinstalacja aplikacji
  odczyt/tworzenie/wysyłanie wiadomości tekstowych
  instalacja skrótów
- Działania
  wysyłanie regularnych raportów na chiński serwer C&C: IMEI, typ karty SIM, wersja systemu

Custom firmware i brak aktualizacji

Bardzo wielu producentów urządzeń przenośnych zapewnia dla swoich klientów aktualizacje Androida przez rok do dwóch od momentu premiery urządzenia. Jeżeli cyberprzestępcy znajdą lukę w systemie po zakończeniu okresu aktualizacji, użytkownik pozostaje sam na sam z grożącym mu niebezpieczeństwem. Możliwość aktualizacji do nowszej wersji Androida dają twórcy niestandardowych wersji tego mobilnego

systemu operacyjnego. Jednak decydując się na taki krok użytkownicy są zobligowani do wyłączenia dużej liczby funkcji Androida odpowiadających za ochronę.

Nieobliczalne ryzyko

Ryzyko jest ogromne gdyż nieuczciwi developerzy mogą zintegrować złośliwe oprogramowanie z customową wersją Androida. Zgodnie z badaniami naukowców z uniwersytetów w Wiedniu, Kalifornii oraz Amsterdamie niestandardowe wersje systemów operacyjnych zawierają aplikacje uzyskujące bardzo szerokie uprawnienia na urządzeniu na którym zostały zainstalowane. Z 250 przebadanych wersji systemu, aż 134 wykorzystywało kod Android Open Source Project (AOSP). Ten zabieg pozwala potencjalnym napastnikom na uzyskanie kontroli nad urządzeniem przez przejęcie uprawnień aplikacji.