RAPORT ZAGROŻEŃ MOBILNYCH Q1 2014

Raport Zagrożeń Mobilnych oparty jest na informacjach z aplikacji mobilnych, zebranych w okresie od 1 stycznia do 31 marca 2014 roku. Zgromadzone próbki i dane są skanowane przez wiele wewnętrznych systemów analitycznych oraz poddane są pogłębionym badaniom przez zespół Threat Reasearch Analysts w F-Secure

Poprzednie Raporty Zagrożeń znajdziesz na F-Secure Labs/Threat Reports

ZNALEZIONE W ŚWIECIE

W pierwszym kwartale 2014 nasze Laboratoria wykryły bądź otrzymały setki tysięcy próbek aplikacji mobilnych ze stron takich jak Google Play Store, niezależnych sklepów z aplikacjami oraz wprost od użytkowników. Aby określić zagrożenia, analizujemy każdą pozyskaną aplikację pod kontem szkodliwego kodu. Jeśli znajdziemy jakiś, aplikacje gromadzone są w **rodziny** określone na podstawie podobieństwa zachowania programu oraz w sposobie jego napisania. Unikalne próbki w rodzinie nazywamy **wariantami**.

NOWE RODZINY I WARIANTY

W 1 kwartale 2014 roku znaleźliśmy 275 rodzin nowych zagrożeń (lub nowych wariantów znanych już rodzin) działających na platformie Android. Odkryliśmy również 1 nową rodzinę zagrożeń na iOS i Symbiana.

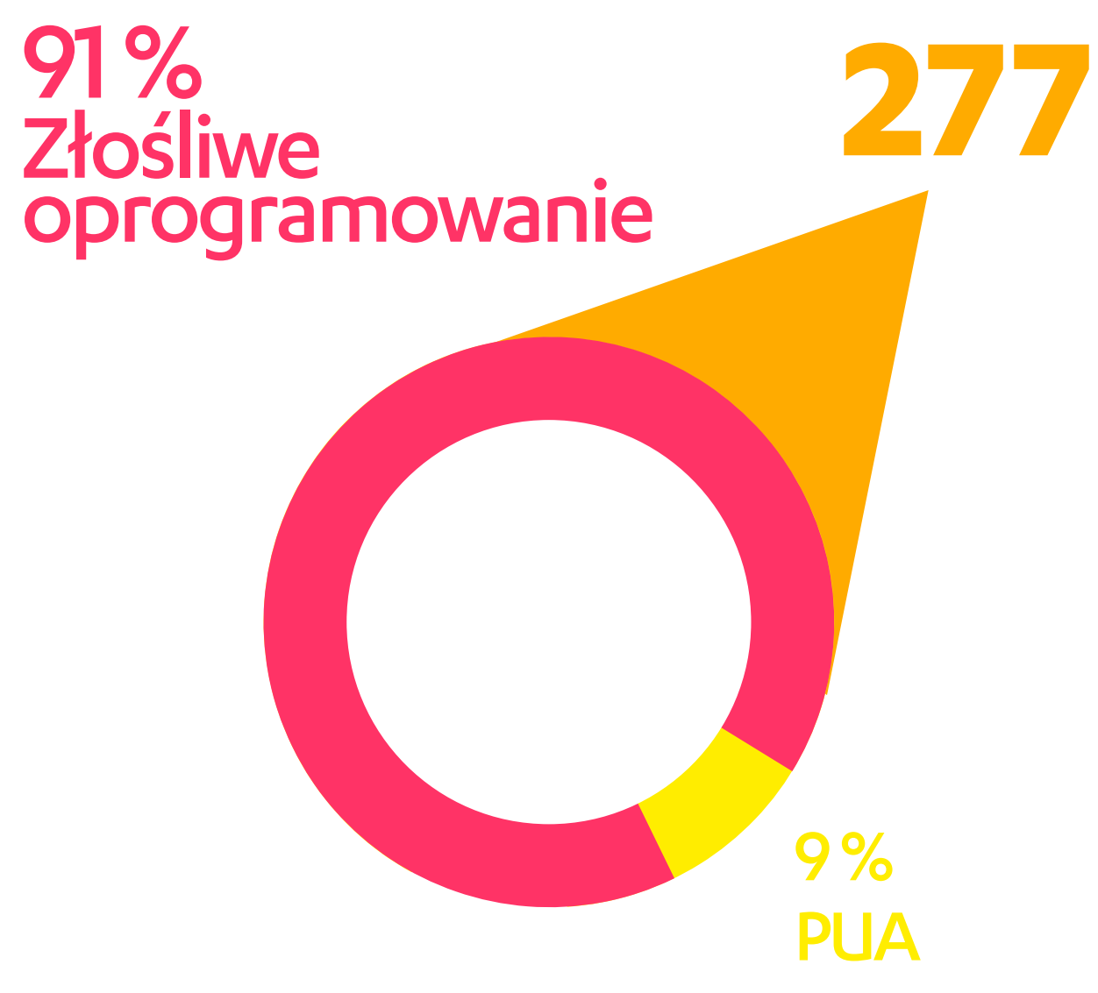
275 **Android**

1 iPhone

1 Symbian

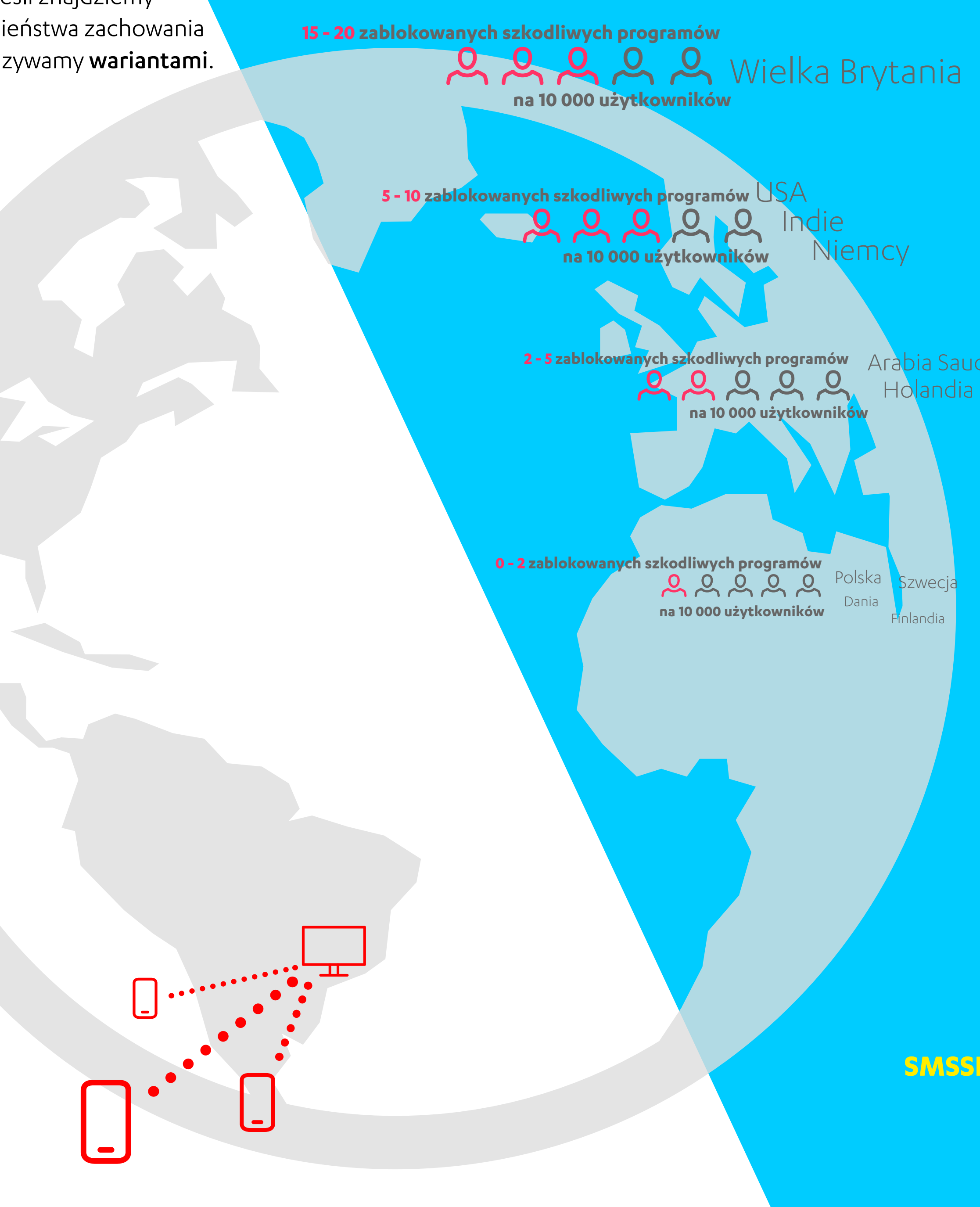
KATEGORIE

91% tych nowych rodzin jako złośliwe oprogramowanie, ponieważ sprawiały poważne zagrożenie dla bezpieczeństwa urządzeń bądź informacji użytkownika. Pozostałe zostały sklasyfikowane jako Potentially Unwanted App (PUA - Potencjalnie Niechciane Aplikacje), które mogą przypadkowo spowodować zagrożenie dla prywatności lub urządzenia użytkownika.



WIDZIANE PRZEZ UŻYTKOWNIKÓW

W porównaniu z zagrożeniami na komputery PC, liczba zagrożeń mobilnych jest bardzo niewielka. Mimo to w 1 kwartale 2014 r. androidowi użytkownicy produktu F-Secure Mobile Security wysyłali do naszego chmurowego systemu telemetrycznego stały strumień raportów o wykrytym i zablokowanym złośliwym oprogramowaniu.

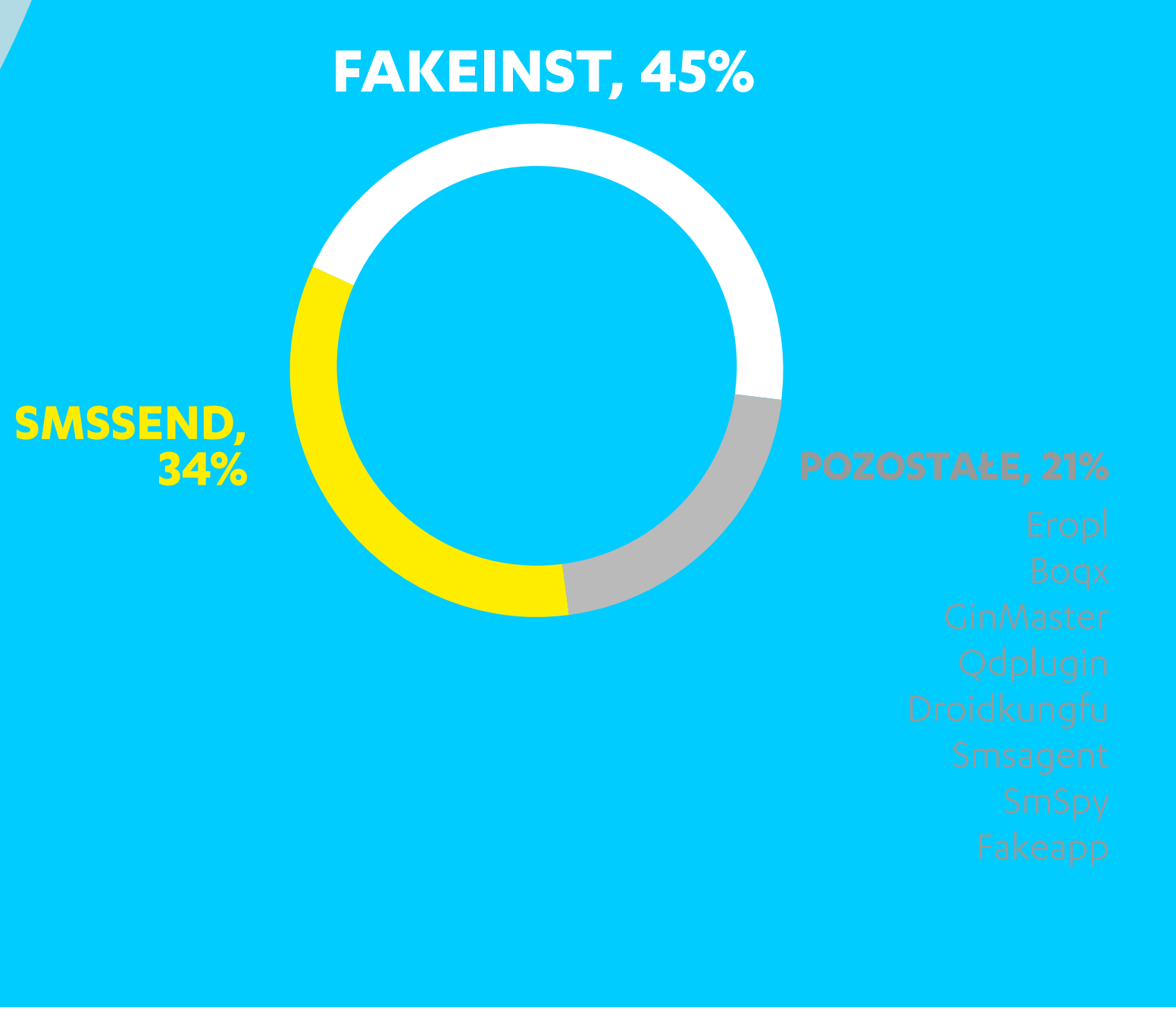


GORĄCE LOKALIZACJE

W pierwszym kwartale 2014 roku najwięcej aktywności związanych ze szkodliwym oprogramowaniem zostało wykrytych i zablokowanych na urządzeniach z Androidem użytkowników z Wielkiej Brytanii. W USA, Indiach, Niemczech, Arabii Saudyjskiej i Holandii także zaobserwowano znaczną ilość szkodliwego oprogramowania. Pozostałe kraje pozostały wykluczone ze względu na znikomą wartość danych statystycznych.

TOP 10 ZAGROŻEŃ NA ANDROIDA

Mimo, że istnieją setki rodzin złośliwych programów, większość użytkowników ma do czynienia tylko z garstką najpopularniejszych zagrożeń. W 1 kwartale 2014 zagrożenia z TOP 10 stanowiły aż 76% wszystkich wykryć na Androidzie. W tej dziesiątce 45% stanowiła rodzina FakeInst, za nią zaś był SMSSend i pozostałe 8 innych rodzin.



JAK DZIAŁAJĄ

Trojany są obecnie najpowszechniejszym typem zagrożeń mobilnych. Większość trojanów, które zauważyliśmy w 1 kwartale 2014 r. podejmują co najmniej jedną z poniżysz aktywności:

Wysyłanie SMSów
Ukryte wysyłanie wiadomości na numery premium lub do serwisów bazujących na subskrypcjach SMS

Pobieranie plików i aplikacji
Pobieranie i instalacja niechcianych plików lub programów na urządzeniu

Śledzenie lokalizacji
Ukryte śledzenie lokalizacji GPS

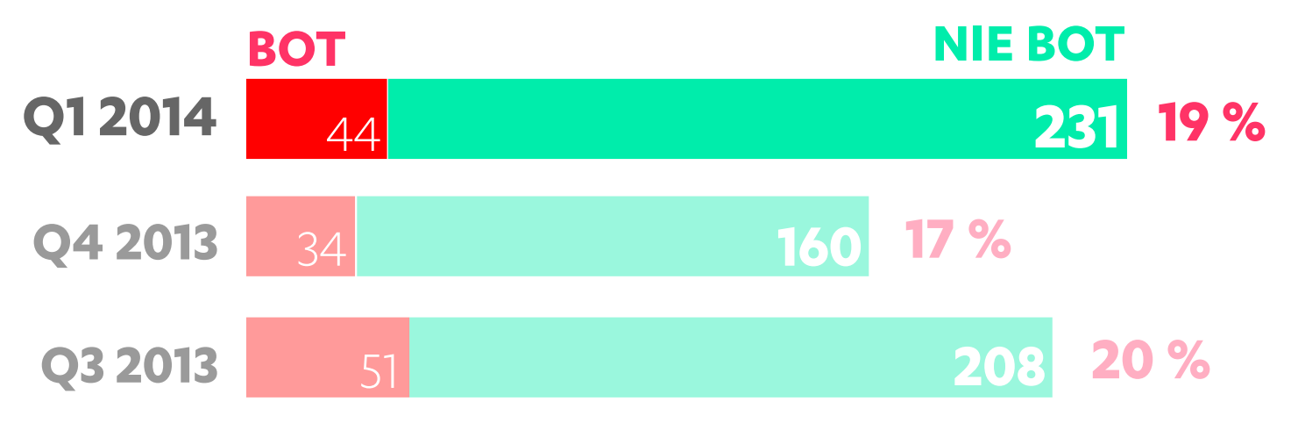
Skanowanie przez fałszywa aplikację
Udaje mobilne rozwiązanie antywirusowe, ale nie ma żadnych funkcjonalności

Klikanie w linki
Łączenie się ze stronami www w celu zwiększenia liczby odsłon danej witryny

Oszustwa bankowe
Ukryte monitorowanie i przekierowywanie SMSów związanych z operacjami bankowości internetowej

Kradzież danych
Kradzież osobistych danych, takich jak pliki, kontakty, zdjęcia i innych prywatnych szczegółów

Obciążanie opłatami
Obciążanie „opłatami” za używanie/aktualizację/instalację legalnej i zazwyczaj darmowej aplikacji



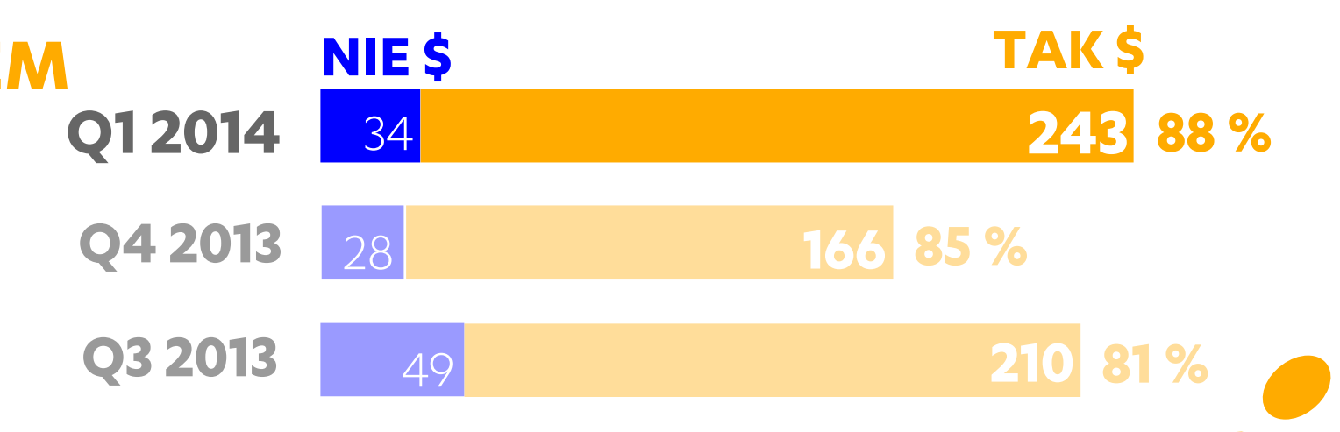
POWIĄZANE Z BOTNETAMI

19% nowych rodzin i wariantów łączy się przez internet z przenośnym serwerem Command & Control (C&C). Urządzenia, które łączą się w ten sposób z nieautoryzowanym serwerem znane są jako boty, grupa takich urządzeń to botnet.

Aplikacje te mogą otrzymywać instrukcje z atakującego serwera C&C, które wymuszają na nich takie działania jak instalowanie programów, gromadzenie informacji bądź wysyłanie SMSów.

MOTYWOWANE ZYSKIEM

88% nowych rodzin i wariantów powiązane były w pewien sposób z zarabianiem pieniędzy od użytkownika, który przypadkowo zainstalował aplikację, np. wysyłając SMS premium lub pobierając opłatę za darmowy program.



PODSUMOWANIE KRAJOBRAZU ZAGROŻEŃ

Rozwój złośliwego oprogramowania w 1 kwartale 2014 roku nadal związany jest niemal wyłącznie z platformą Android i potwierdza trend, który obserwowaliśmy w ciągu ostatnich dwóch lat. Spośród wszystkich próbek aplikacji, jakie zebraliśmy w tym okresie, niemal 14% stanowiły złośliwe aplikacje na Androida (pozostałe zostały określone jako PUA - Potentially Unwanted Application, czyli Potencjalnie Niechciana Aplikacja, bądź czyste).

Znaczna większość złośliwych próbek na Androida, które zebraliśmy, były trojanami. Mimo, że większość z nich technicznie nie kwalifikowało się do rodzin szczególnie skupiających się na **wysyłaniu SMSów** (np. SMSSender), niemal 83% zauważonych przez nas trojanów wysyłało reklamowe wiadomości, co czyniło z tego zdecydowanie najczęstszą niepożądaną aktywność. Jednym z najciekawszych rozwiązań związanych z tym problemem było zaprezentowanie niezwłocznych powiadomień o wysyłaniu SMSów na numery premium w Adroidzie 4.2 (Jelly Bean). Użytkownik mógł wybrać, czy blokować, czy zezwalać na tego typu połączenia, co z pewnością ukróciło ten proceder.

Trojany powiązane z pobieraniem oprogramowania, kradzieżą danych i oszustwami bankowymi były drugim co do częstotliwości występowania grupą zagrożeń i razem stanowił niemal 10% wszystkich szkodliwych próbek. Nowy, zauważony przez nas w ostatnim czasie sposób zachowania trojanów polega na obciążaniu płatnościami za darmowe aplikacje. Mechanizm polega na przepakowaniu aplikacji (zazwyczaj dostępnej za darmo) i ponownej dystrybucji z dodanym żądaniem zapłaty **(Trojan:Android/FakeFlash.C).**

Poza trojanami, druga najpowszechniejszą grupą zagrożeń był **backdoory**, które stanowiły 5% próbek szkodliwych aplikacji w ostatnim kwartale. Pozostałe typy malware'u to **exploity, robaki** i pozostałe, które wspólnie miały udział na poziomie poniżej 5%. Niska liczba nie-trojanów opracowana została przez tych, którzy chcieli sprawdzić możliwości techniczne platformy. Jedynym nowym exploitem w tym kwartale był Pileup, wykryty przez badaczy uniwersyteckich [5] nadawał nowe uprawnienia szkodliwemu oprogramowaniu podczas upgradeowania systemu, podczas gdy nowo odkryty toolkit Dendroid [6], którego klasyfikujemy jako backdoora, został opracowany przez twórców szkodliwego oprogramowania, którzy chcieli zautomatyzować tworzenie tworze nie trojanów ze zdalnym dostępem (Remote Access Trojans - RATs), które mogłyby omijać zabezpieczenie Google Play Store. Jeśli ten toolkit zostanie powszechniej wykorzystany przez ludzi rozpowszechniających złośliwe oprogramowanie, bezpieczeństwo rynku aplikacji mobilnych może być bardziej zagrożone niż dotychczas.

Jednym ze sposobów oceny bezpieczeństwa rynku aplikacji mobilnych, który zastosowaliśmy, jest porównanie liczby złośliwego oprogramowania z danego sklepu ze wszystkimi aplikacjami z tego źródła. Według tego kryterium, najwyższy współczynnik malware'u mają serwisy skierowane przede wszystkim do mieszkańców Chin: Mumayi (7%), Wandoujia (5%), Anzhi i Baidu (oba po 3%). Dla porównania - zaledwie 0.1% próbek z Google Play Store rozpoznaliśmy jako szkodliwe oprogramowanie.

NAJCIEKAWSZE BADANIA W TYM KWARTALE

NA ANDROIDA

99% nowych zagrożeń, które powstały w 1 kwartale 2014, dotyczy platformy Android, nie dziwi zatem fakt, że najciekawsze rozwiązania techniczne w szkodliwym oprogramowaniu są związane właśnie z nią. Oto kilka wartych uwagi pomysłów cyberprzestepców dotyczących malware'u na Androida:

TROJANY Z WINDOWSA PRZENOSZĄ SIĘ NA ANDROIDA [1]

Trojan bankowy o nazwie **Droidpak**, który skierowany jest na Windowsa na komputery PC, próbuje również zainstalować trojana bankowego na urządzenia z systemem Android w momencie podłączenia poprzez łącze USB z zainfekowanym komputerem. Zależnie od wariantu wykrywamy trojan nazwany **Trojan-Spy:Android/Smforw.H** albo **Trojan:Android/Gepew.A** lub **.B**).

PIERWSZ TROJAN TOR [2]

Trojan:Android/Torsm.A jest pierwszym trojanem na tę platformę, który wykorzystuje open-sourcowego klienta Orbot w popularnej sieci anonimizującej TOR, by komunikować się z serwerem C&C. Utrudnia to (jeśli wręcz nie uniemożliwia) namierzanie i wyłączanie serwera C&C.

PIERWSZY TROJAN DO WYDOBYWANIA KRYPTOWALUTY [3]

Trojan:Android/CoinMiner.A jest rozpowszechniany w przepakowanej aplikacji. Podczas gdy jest instalowany, automatycznie przejmuje urządzenie do wydobywania kryptowaluty (w tym przypadku Litecoin) na rzecz autora programu. Poza opłatami za transfer danych, ciągłe używanie urządzania mogło również wpływać na długość życia baterii.

PIERWSZY BOOTKIT [4]

Trojan:Android/Oldboot.A jest uznawany za pierwszego bootkita na Androida lub malware, który wpływa na najwcześniejsze etapy bootowania urządzenia, co sprawia, że jest niezwykle trudny do wykrycia lub usunięcia. Program został zaprojektowany tak, aby rozpowszechniać się w aktualizacjach firmware'u. Najwięcej infekcji zanotowano w Chinach.

PILEUP EXPLOIT [5]

Badacze zauważyli podatności w Androidzie, które mogą zezwolić zainstalowanemu szkodliwemu oprogramowaniu na zwiększenie jego upoważnień podczas aktualizowania systemu. Nazwali tę lukę **Pileup** (skrót od "privilage escalation through updating").

IPHONE I SYMBIAN

Mimo, że większość twórców złośliwego oprogramowania skoncentrowała się na produkcji aplikacji na Androida, kilku z nich spróbowało swych sił w programach na na iPhony i na platformę Symbian. Poniższe dwa zagrożenia były jednymi w pierwszym kwartale 2014 nowymi zagrożeniami malware'ami niezwiązanymi z platformą Android.

TROJAN:IPHONE/ADTHIEF.A

Badacze po raz pierwszy zaraportowali odnalezienie podejrzanej biblioteki używanej popularnym frameworku używanym do tworzenia aplikacji. Kiedy została zainstalowana na iPhonie pozbawionym firmowych ograniczeń (Jailbreak), złośliwy program przechwytuje moduły reklamowe w różnych aplikacjach,aby wyświetlać własną reklamę. iPhone'y bez modyfikacji firmware'u nie są podatne na tego trojana.

TROJAN:SYMBOS/SMSJEG.B

Trojan ten jest nietypowy, ponieważ pojawił się na platformie Symbian, podczas gdy zdecydowana większość złośliwego kodu tworzona jest z myślą o systemach z bardziej perspektywiczną przyszłością. Gdy jest zainstalowany, wysyła w tle wiadomości SMS.

ZŁAMANIE ZABEZPIECZE SKLEPÓW Z APLIKACJAMI

Twórcy szkodliwego oprogramowania poszukują dróg do obejścia zabezpieczeń używanych przez sklepy z aplikacjami. Zabezpieczenia te dają pewność, że oferowane są tylko zatwierdzone aplikacje. Czasami cyberprzestępcom udaje się dostać to serwisów z aplikacjami (zazwyczaj jednak tylko na chwilę).

Google Play Store to obecnie największy i z pewnością najbardziej kontrolowany oficjalny sklep z aplikacjami dostępnymi na całym świecie. Tak więc, gdy złośliwe oprogramowanie trafi do niego, może ono dotrzeć do dużej liczby użytkowników, co oczywiście czyni z niego łakomy kąsek dla osób rozpowszechniających malware.

W 1 kwartale 2014 roku złośliwe oprogramowanie było przez krótki czas obecne w Play Store. Obecnie jednak zostało ono usunięte.

Trojan:Android/FakeFlash.C

Trojan-Spy:Android/Wabek.A

DENDROID TOOLKIT [6]

Backdoor:Android/Dendroid.A jest zestawem narzędzi do tworzenia Remote Access Trojans (RAT), które pozwala atakującym tworzyć trojany, które mogą mieć zdalny dostęp do funkcji audio i wideo zainfekowanego urządzenia. Tworzy także trojana, który potrafi obejść zabezpieczenia Google Play Store.

ŹRÓDŁA

1. Securelist; Roman Unuchek; *The first Tor Trojan for Android*; opublikowano 25 lutego 2014; https://www.securelist.com/en/blog/8184/The_first_Tor_Trojan_for_Android
2. Symantec; Flora Liu; *Windows Malware Attempts to Infect Android Devices*; opublikowano 23 Stycznia 2014; http://www.symantec.com/connect/blogs/windows-malware-attempts-infect-android-devices
3. Trend Micro blog; Veo Zhang; *Mobile Malware Mines Dogecoins and Litecoins for Bitcoin Payout;* opublikowano 25 Marca 2014; http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-malware-mines-dogecoins-and-litecoins-for-bitcoin-payout/
4. ZDNet; Lian Tung; *Modded firmware may harbour world's first Android bootkit*; opublikowano 28 Stycznia 2014; http://www.zdnet.com/modded-firmware-may-harbour-worlds-first-android-bootkit-7000025665/
5. Malwarebytes Unpacked; Joshua Cannell; *Research Paper Shows Upgrading Android Could Upgrade Malware;* opublikowano 20 Marca 2014; http://blog.malwarebytes.org/mobile-2/2014/03/research-paper-shows-upgrading-android-could-upgrade-malware/
6. Ars Technica; Dan Goodin; *Malware designed to take over cameras and record audio enters Google Play;* opublikowano 8 Marca2014; http://arstechnica.com/security/2014/03/malware-designed-to-take-over-cameras-and-record-audio-enters-google-play/

CO MOŻESZ ZROBIĆ

Zablokuj swoje urządzenie
Pomimo obaw o ataki online, najprostszą metodą, aby szkodliwe oprogramowanie znalazło się na urządzeniu jest manualne zainstalowanie go przez niepowołaną osobę. Najpierw zadbaj o fizyczną ochronę urządzenia. Blokowanie chroni przed osobami, które mogą zmieniać jego ustawienia i instalować aplikacje (takie jak narzędzie monitorujące lub oprogramowanie szpiegujące).

Używaj ochrony przed kradzieżą
Ochrona przeciwkradzieżowa umożliwia Ci zdalne usunięcie danych na Twoim urządzeniu, włączając w to nośniki wymienne, jeśli uważasz, że urządzenie jest nie do odzyskania.Niektóre rozwiązania antykradzieżowe zawierają także narzędzie do namierzania lokalizacji albo włączania alarmu w momencie, kiedy próbujesz je odnaleźć.

Ustaw blokadę wiadomości
Jeśli Twoje urządzenie nie jest wyposażone w Androida w wersji 4.2 (Jellybean), pomyśl o zablokowaniu połączeń i SMSów na numery premium u Twojego operatora. Jest to szczególnie wygodne dla rodziców, którzy chcą, aby urządzenia ich dzieci nie generowały niespodziewanych kosztów.

Pobieraj aplikacje tylko z zaufanych źródeł
W ustawieniach domyślnych urządzenia z Androidem mają zablokowaną instalację aplikacji z innych źródeł niż Play Store. Możesz sprawdzić, czy tak jest w przypadku Twojego urządzenia, w jego ustawieniach (Ustawienia>Aplikacje>Nieznane źródła). Jeśli ta opcja jest zaznaczona, aplikacje spoza Play Store mogą być zainstalowane. Odznacz tę opcję.

Analizuj uprawnienia aplikacji
Czy instalujesz aplikację z Play Store czy tez innych źródeł, sprawdź, o jakie upoważnienia prosi aplikacja. Czy wymaga połączenia z internetem by przechowywać pliki na zewnętrznym dysku, czy po to, by wysyłać SMSy? Sprawdź stronę producenta oprogramowania, żeby sprawdzić, jakich uprawnień wymaga. Możesz też zapoznać się recenzjami aplikacji, aby sprawdzić opinie innych użytkowników.

Skanuj pobrane aplikacje
Jeśli pobierasz aplikację z innego źródła niż Play Store, użyj wiarygodnego programu antywirusowego dla urządzeń mobilnych, żeby ją przeskanować przed jej instalacją. Możesz potraktować to jako sprawdzenie ukrytych funkcji aplikacji - jej niewymienionych, ale dozwolonych działań. Jeśli ocena antywirusa jest dla Ciebie akceptowalna, możesz zainstalować aplikację.

Produkty F-SECURE, które Ci pomogą:

MOBILE SECURITY
Mobilna ochrona bankowości internetowej i przeglądania, kontrola rodzicielska, skanowanie aplikacji i dużo więcej. Teraz wyposażone w **Application Privacy** - moduł, który sprawdza aplikacje pod kątem Twojej prywatności i uprawnień, których żądają.

KEY
Zabezpiecz swoje dane logowania silnym mechanizmem szyfrującym. Jedno hasło nadrzędne pozwala Ci dostać się do aplikacji i zarządzać z jej poziomu hasłami do Twojej poczty czy banku. Synchronizuj swoje hasła na różnych urządzeniach w bezpiecznej chmurze F-Secure.

APP PERMISSIONS
Poznaj wszystkie uprawnienia, których żądają aplikacje zainstalowane na Twoich urządzeniach przenośnych. Dowiedz się, które programy mogą naruszać Twoją prywatność, które mogą narażać Cię na dodatkowe koszty, a które mogą wpływać na czas pracy baterii.

FREEDOME
Łącz się bezpiecznie z internetem za pomocą Virtual Private Network (VPN) - szyfrowanego połączenia, które chroni Cię przed namierzaniem Twojego ruchu sieciowego, złośliwymi stronami internetowymi i szkodliwym oprogramowaniem.

F-Secure.