**Ewolucja zagrożeń IT wg Kaspersky Lab: II kwartał 2013 r.**

**Eksperci z Kaspersky Lab opublikowali raport dotyczący ewolucji zagrożeń IT obejmujący II kwartał 2013 r. Według raportu, mobilne szkodliwe oprogramowanie stanowiło najważniejszą kategorię w badanym okresie, zarówno pod względem liczby nowych odmian jak i zastosowanych technologii.**

Cyberprzestępcy nie tylko tworzą coraz więcej szkodliwego oprogramowania atakującego platformy mobilne, ale również udoskonalają możliwości i zachowanie niebezpiecznych aplikacji. Oprócz mobilnego szkodliwego oprogramowania cyberprzestępcy skoncentrowali się na realizacji kampanii, których celem było nielegalne wydobywanie i kradzież bitcoinów, ponieważ wartość tej cyfrowej waluty znacznie wzrosła w drugim kwartale 2013 r.

**II kwartał w liczbach**

Produkty firmy Kaspersky Lab wykryły i zneutralizowały łącznie 983 051 408 zagrożeń.

Zablokowano 577 159 385 infekcji urządzeń użytkowników podczas uzyskiwania przez nich dostępu do internetu.

Zablokowano 400 604 327 szkodliwych programów próbujących zainfekować maszyny użytkowników.

Do systemu wykrywania firmy Kaspersky Lab dodano 29 695 nowych modyfikacji mobilnego szkodliwego oprogramowania.

**Ewolucja mobilnego szkodliwego oprogramowania**

Do 30 czerwca 2013 r. Kaspersky Lab dodał do swojego systemu wykrywania łącznie 100 386 modyfikacji mobilnego szkodliwego oprogramowania, co stanowi znaczny wzrost w porównaniu z końcem 2012 r. (46 445 modyfikacji).

Warto zauważyć, że modyfikacje to nie jednostkowe wykrycia czy szkodliwe programy – to próbki szkodliwego kodu wykorzystywane przez cyberprzestępców do infekowania legalnych mobilnych aplikacji. Powszechną metodą stosowaną przez cyberprzestępców jest pobieranie legalnych aplikacji i modyfikowanie ich poprzez dodawanie szkodliwego kodu. Następnie cyberprzestępcy rozprzestrzeniają zmodyfikowane – tym razem niebezpieczne – aplikacje na stronach, z których mogą zostać pobrane przez użytkowników – mogą to być np. sklepy z aplikacjami. Oprogramowanie Kaspersky Lab identyfikuje próbki szkodliwego kodu wprowadzane do zmodyfikowanych aplikacji przy użyciu technologii opartych na chmurze, sztucznej inteligencji i sygnaturach antywirusowych. Wykrywając próbki szkodliwego kodu produkty Kaspersky Lab mogą zidentyfikować niebezpieczne aplikacje, zanim zostaną uruchomione na urządzeniach użytkowników.

Chociaż dominującą kategorię mobilnego szkodliwego oprogramowania stanowią tradycyjnie trojany SMS, w drugim kwartale eksperci z Kaspersky Lab zauważyli spadek ich liczby. Wynika to z faktu, że trojany tworzone dla platform mobilnych zaczęły oferować więcej możliwości i większą elastyczność.

W drugim kwartale trojany pozwalające na przejęcie kontroli nad zainfekowanymi urządzeniami odnotowały największą liczbę dodanych modyfikacji (ich udział stanowił 32,3%), na drugim miejscu znalazły się klasyczne trojany (23,2%), a na trzecim trojany SMS (27,7%). Pod względem możliwości mobilnego szkodliwego oprogramowania, cyberprzestępcy stosują obecnie techniki zaciemniania w celu uniknięcia analizy. Jednocześnie, często tworzą programy posiadające wiele szkodliwych funkcji, dzięki którym uzyskują korzyści finansowe, wykorzystując różnego typu nielegalne modele biznesowe. Nowe szkodniki mogą również kraść większą ilość danych z urządzeń użytkowników, a jednocześnie potrafią pobierać i instalować na zainfekowanych urządzeniach dodatkowe szkodliwe oprogramowanie. Zagrożenia dla Androida przeszły największą ewolucję w porównaniu z innymi platformami i zaczynają stanowić mobilny odpowiednik szkodników, których celem są komputery działające pod kontrolą systemu Windows.

**Oprogramowanie wyłudzające okup na Androidzie**

W czerwcu pojawił się pierwszy przykład stworzonej dla Androida aplikacji wyłudzającej okup (tzw. ransomware) – „Free Calls Update” (program ten był dostępny w sklepach z aplikacjami). Ransomware to rodzaj oprogramowania, którego celem jest wyłudzanie pieniędzy od ofiary poprzez blokowanie dostępu do jej urządzenia lub komputera do czasu zapłacenia przez zainfekowanego użytkownika „okupu”. Jednak nawet gdy ofiara zapłaci żądaną kwotę, dostęp do maszyny nie zostanie przywrócony. Po instalacji na urządzeniu „Free Calls Update” uruchamia się i próbuje uzyskać prawa administratora w celu zmiany ustawień sieci komórkowej i Wi-Fi na urządzeniu. Aplikacja „udaje” skanowanie w celu wykrycia szkodliwego oprogramowania i wyświetla fałszywy komunikat informujący użytkownika, że jego urządzenie zostało zainfekowane wirusem. Następnie ofiara jest nakłaniana do zakupu licencji na zestaw fałszywego mobilnego oprogramowania antywirusowego w celu usunięcia infekcji. Szkodnik wyświetla ten komunikat i jednocześnie blokuje dostęp do wszystkich funkcji telefonu, przez co stanie się on bezużyteczny.

Oprogramowanie ransomware oraz powiadomienia wysyłane przez fałszywe programy antywirusowe to częsta sztuczka stosowana w atakach z wykorzystaniem szkodliwego oprogramowania dla komputerów PC. Obecnie cyberprzestępcy wykorzystują te same metody, zarówno technicznie jak i psychologicznie, próbując wykorzystać mniej dojrzały rynek urządzeń mobilnych.

**Bitcoiny napędzają czarny rynek**

W drugim kwartale cyberprzestępcy skoncentrowali się także na tworzeniu szkodliwego oprogramowania gromadzącego bitcoiny. Bitcoiny to cyfrowa waluta tworzona w oparciu o infrastrukturę peer-to-peer (P2P) i służąca do przeprowadzania anonimowych, zdecentralizowanych transakcji finansowych. Transakcje te są przeprowadzane na serwerach, tzw. kopalniach bitcoinów, które wspomagają wymianę i przetwarzanie wirtualnych monet. Infrastruktura opiera się na sieci połączonych komputerów wykorzystywanych jako zasoby umożliwiające działanie kopalń bitcoinów. Wirtualne pieniądze mogą zostać później wymienione na inną walutę lub wykorzystane do płacenia za towary i usługi w sklepach internetowych (bitcoiny w znaczeniu cyfrowej waluty są oznaczane przy pomocy małej litery „b”, podczas gdy duża litera „B” wskazuje na infrastrukturę Bitcoin).

Wartość bitcoinów znacząco wzrosła w ostatnim roku. O ile wcześniej równowartość jednego bitcoina wynosiła mniej niż 1 cent, obecnie wzrosła do 130 dolarów amerykańskich. Mimo niestabilności tej waluty jej kurs nadal stopniowo rośnie. Popularność, anonimowość i wzrost wartości stanowią czynniki zachęcające cyberprzestępców do przeprowadzania bardziej agresywnych ataków na infrastrukturę Bitcoin. Ponadto, bitcoiny stanowią preferowaną walutę cyberprzestępców podczas prowadzenia biznesu, ponieważ zapewniają im dość dużą anonimowość. Dodatkowo, transakcje z użyciem bitcoinów nie obejmują żadnych wymogów ani procedur finansowych czy regulacyjnych, co znacznie utrudnia ich śledzenie.

W kwietniu zespół badawczy firmy Kaspersky Lab wykrył kampanię, w której cyberprzestępcy wykorzystywali Skype’a do dystrybucji szkodliwego oprogramowania służącego do ataku na infrastrukturę Bitcoin. Szkodnik ten stosował socjotechnikę, aby najpierw zainfekować ofiary, a następnie instalował na zarażonych maszynach szkodliwe oprogramowanie, które zmieniało je w „wyrobników” wydobywających bitcoiny. Bitcoiny wydobywane przez zainfekowane maszyny ofiar były następnie wysyłane na konto cyberprzestępców stojących za oszustwem.

Miesiąc później eksperci ds. bezpieczeństwa z Kaspersky Lab zidentyfikowali kolejną szkodliwą kampanię – brazylijski atak phishingowy wymierzony w infrastrukturę Bitcoin. Podobnie jak w poprzednim ataku, zastosowano socjotechnikę, aby zainfekować ofiary. Jednak tym razem zamiast Skype’a, cyberprzestępcy wykorzystywali wiadomości phishingowe, aby przekierowywać użytkowników na fałszywą wersję jednej z najpopularniejszych stron związanych z handlem bitcoinami - MtGox. MtGox obsługuje ogromną liczbę autoryzowanych transakcji, dlatego celem tej kampanii było nakłonienie użytkowników do ujawnienia swoich danych uwierzytelniających logowanie, które następnie pozwoliłyby osobom atakującym kraść bitcoiny bezpośrednio z kont użytkowników.

Pełna wersja raportu dotyczącego ewolucji zagrożeń IT w II kwartale 2013 r. jest dostępna w serwisie SecureList.pl prowadzonym przez Kaspersky Lab: <http://securelist.pl/analysis/7242,ewolucja_zagrozen_it_ii_kwartal_2013_r.html>.

Informację oraz raport można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie <http://www.kaspersky.pl/news>.