**Kaspersky Lab wykrywa nowe zagrożenia dla Androida i iOS oraz lokalizuje serwery HackingTeam**

**Kaspersky Lab informuje o zlokalizowaniu ogromnej międzynarodowej infrastruktury wykorzystywanej do kontrolowania implantów szkodliwego oprogramowania "Remote Control System" (RCS) oraz o zidentyfikowaniu niewykrytych wcześniej mobilnych trojanów działających zarówno w systemie Android, jak i iOS.**

Wykryte moduły te stanowią część "legalnego" programu spyware, RCS, znanego również jako Galileo, stworzonego przez włoską firmę HackingTeam.

Na liście ofiar zidentyfikowanych w badaniu przeprowadzonym przez Kaspersky Lab wraz z jego partnerem Citizen Lab, znajdują się aktywiści i obrońcy praw człowieka jak również dziennikarze i politycy. Infrastruktura RCS

Specjaliści z Kaspersky Lab korzystali z różnych metod w celu zlokalizowania serwerów kontroli Galileo na całym świecie. W procesie identyfikacji oparto się m.in. na specjalnych wskazówkach oraz danych o połączeniach uzyskanych z inżynierii wstecznej dostępnych próbek szkodliwego oprogramowania. Podczas analizy badacze z Kaspersky Lab zdołali zidentyfikować obecność ponad 320 serwerów kontroli RCS w ponad 40 krajach. Większość serwerów znajdowała się w Stanach Zjednoczonych, Kazachstanie, Ekwadorze, Wielkiej Brytanii i Kanadzie. W Polsce eksperci z Kaspersky Lab wykryli 7 takich serwerów.

**Mapa serwerów HackingTeam zlokalizowanych przez ekspertów z Kaspersky Lab**

Komentując wyniki najnowszych badań, **Siergiej Golowanow**, główny badacz ds. bezpieczeństwa w Kaspersky Lab, powiedział: „Obecność tych serwerów w danym państwie nie oznacza, że są wykorzystywane przez jego organy ścigania. Jednak rozmieszczenie przez użytkowników RCS serwerów w miejscach, które kontrolują, wydaje się sensownym działaniem – ryzyko problemów prawnych związanych z przekroczeniem granic lub przechwyceniem sprzętu jest wtedy minimalne”.

**Mobilne implanty RCS**

Chociaż o istnieniu trojanów mobilnych dla systemów iOS i Android stworzonych przez HackingTeam wiadomo było już od jakiegoś czasu, tak naprawdę nikt ich wcześniej nie zidentyfikował – ani nie zauważył, aby były wykorzystywane w atakach. Eksperci z Kaspersky Lab badają szkodliwe oprogramowanie RCS od kilku lat. Wcześniej tego roku zdołali zidentyfikować próbki modułów mobilnych, które odpowiadały profilom konfiguracji innego szkodliwego oprogramowania RCS z ich kolekcji. Podczas ostatniego badania otrzymano również nowe warianty próbek od ofiar za pośrednictwem opartej na chmurze sieci KSN firmy Kaspersky Lab. Ponadto, eksperci firmy współpracowali ściśle z Morganem Marquis-Boirem z Citizen Lab, który dokładnie bada zestaw szkodliwego oprogramowania HackingTeam.

**Wektory infekcji**

Osoby stojące za Galileo stworzyły specjalny szkodliwy implant dla każdego konkretnego celu. Gdy próbka jest gotowa, osoba atakująca dostarcza ją na urządzenie mobilne ofiary. Wśród znanych wektorów infekcji znajdują się ukierunkowane wiadomości phishingowe z wykorzystaniem socjotechniki – często w połączeniu ze szkodliwymi programami atakującymi przez luki (także te jeszcze niezałatane, tzw. zero-day) w systemach operacyjnych i aplikacjach oraz lokalne infekcje za pośrednictwem przewodu USB podczas synchronizacji urządzeń mobilnych.

Jednym z głównych odkryć było ustalenie, w jaki dokładnie sposób trojan mobilny Galileo infekuje iPhone’a: aby infekcja była możliwa, urządzenie musiało zostać wcześniej odblokowane metodą jailbreak. Jednak zainfekowane mogą zostać również smartfony, których nie odblokowano w ten sposób: osoba atakująca może uruchomić narzędzie do jailbreakingu takie jak ‘Evasi0n’ za pośrednictwem wcześniej zainfekowanego komputera i przeprowadzić zdalne odblokowanie, a następnie dokonać infekcji. W celu uniknięcia ryzyka zaleca się unikanie odblokowywania iPhone’a metodą jailbreak oraz regularne aktualizowanie systemu iOS na posiadanym urządzeniu do najnowszej wersji.

**Szpiegowanie szyte na miarę**

Moduły mobilne RCS zostały precyzyjnie zaprojektowane, tak aby działały w sposób dyskretny, np. poprzez zwrócenie szczególnej uwagi na żywotność baterii urządzenia mobilnego. Zostaje to osiągnięte poprzez precyzyjne dostosowanie możliwości szpiegowania do danego celu lub uruchomienie szkodliwych działań wyłącznie w ściśle określonych okolicznościach: np. nagrywanie audio może rozpocząć się tylko wtedy, gdy ofiara połączy się z określoną siecią Wi-Fi lub wymieni kartę SIM, czy też podczas ładowania urządzenia.

Mobilne trojany RCS potrafią realizować wiele różnych funkcji szpiegujących, w tym powiadamianie o lokalizacji celu, robienie zdjęć, kopiowanie zdarzeń z kalendarza, rejestrowanie nowych kart SIM, które zostały włożone do zainfekowanego urządzenia, oraz przechwytywanie rozmów telefonicznych i wiadomości, które oprócz standardowych wiadomości tekstowych SMS obejmują również wiadomości wysłane z określonych aplikacji, takich jak Viber, WhatsApp oraz Skype.

Produkty firmy Kaspersky Lab wykrywają narzędzia spyware RCS/DaVinci/Galileo jako Backdoor.Win32.Korablin, Backdoor.Win64.Korablin, Backdoor.Multi.Korablin, Rootkit.Win32.Korablin, Rootkit.Win64.Korablin, Rootkit.OSX.Morcut, Trojan.OSX.Morcut, Trojan.Multi.Korablin, Trojan.Win32.Agent, Trojan-Dropper.Win32.Korablin, Trojan-PSW.Win32.Agent, Trojan-Spy.AndroidOS.Mekir oraz Backdoor.AndroidOS.Criag.

Więcej informacji technicznych na temat nowych trojanów mobilnych oraz infrastruktury serwerów RCS pojawi się już wkrótce w serwisie SecureList.pl prowadzonym przez Kaspersky Lab.

Informację 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>.