Kaspersky Lab hlásí nový mobilní malware pro Androidy i iOS

Londýn, 24. června 2014

Trojský kůň napadající chytré telefony s Androidem i iOS a odhalení mezinárodní infrastruktury malwaru. To jsou dva zásadní body nové analytické zprávy, kterou dnes zveřejnila v Londýně společnost Kaspersky Lab.

Studie mapuje rozsáhlou mezinárodní infrastrukturu sloužící k ovládání malwarových „implantátů" dálkovým kontrolním systémem (Remote Control System, RCS). Analytici zároveň identifikovali dosud neobjevený mobilní trojan fungující jak na Androidech, tak na iOS. Tyto moduly jsou součástí takzvaného „legálního" spyware nástroje Galileo vyvinutého italskou společností HackingTeam, který ve světě využívají některé státní bezpečnostní orgány včetně policie. Na seznamu obětí dle zprávy Kaspersky Lab a partnerské laboratoře Citizen Lab figurují aktivisté, obhájci lidských práv, novináři a politici.

Infrastruktura RCS

Kaspersky Lab využila k lokalizaci řídících C&C (Command and Control) serverů Galilea po celém světě řadu bezpečnostních postupů. Při identifikaci se její analytici spoléhali zejména na specifické ukazatele a data o připojení získaná reverzním inženýrstvím existujících vzorků. Během analýzy byli experti Kaspersky Lab schopni zmapovat přítomnost více než 320 C&C serverů RCS ve více než 40 zemích. Většina z nich byla v USA, Kazachstánu, Ekvádoru, Velké Británii a v Kanadě, jeden z nich i v České republice.

„To, že jsou servery v určité zemi, neznamená, že by byly využity místními bezpečnostními orgány. Nicméně je logické, aby je uživatelé RCS spouštěli v zemi, kde potřebují operovat – minimalizují tak riziko přeshraničních právních komplikací nebo zabavení serverů," podotkl Sergej Golovanov, hlavní bezpečnostní analytik Kaspersky Lab.

„Mobilní implantáty" RCS

Ačkoliv se už v minulosti o existenci mobilních trojských koní pro iOS a Android od HackingTeamu vědělo, nikdo je dosud neidentifikoval, ani neodhalil při útoku. Kaspersky Lab zkoumá RCS malware již několik let. Letos její analytici identifikovali určité vzorky mobilních modulů, které se shodovaly s konfiguračními profily RCS malwaru v databázi společnosti. V cloudové databázi Kaspersky Security Network se také objevily nové varianty těchto vzorků. Kaspersky Lab úzce spolupracovala s Morganem Marquis-Boirem z kanadské laboratoře Citizen Lab, který podrobně zkoumá malware od firmy HackingTeam.

Metody infekce

Provozovatelé RCS Galileo vytvořili škodlivý implantát speciálně pro každý konkrétní cíl, který pak doručili do mobilního zařízení oběti. Jedním ze známých způsobů infekce je „spearphishing" skrze sociální sítě – často doplněný exploity, včetně zero-days, a lokálními infekcemi přes USB kabely při synchronizaci mobilních zařízení.

Jedním z hlavních odhalení je způsob, jak přesně mobilní trojský kůň Galileo infikuje iPhone. K tomu je zapotřebí „jailbreak" (tedy softwarová úprava iPhonu tak, aby se do něj mohly instalovat aplikace třetích stran). Nicméně zranitelné jsou i iPhony bez jailbreaku. Útočník

na nich může spustit „jaibreakový“ nástroj „Evasi0n“ pomocí předem infikovaného počítače a poté jej nakazit. Aby se tomu uživatelé vyhnuli, doporučují experti Kaspersky Lab neprovádět jailbreak na iPhonu a zároveň pravidelně aktualizovat iOS.

Špionáž na míru

Mobilní moduly RCS jsou navržené přesně tak, aby fungovaly diskrétně, například s ohledem na životnost baterie zařízení. Využívají k tomu pečlivě a na míru vytvořené špionážní technologie a speciální spouštěče. Například nahrávání audia se spustí jen tehdy, když se oběť připojí k určité Wi-Fi síti, když vymění SIM kartu nebo své zařízení nabíjí.

Obecně jsou mobilní trojské koně RCS schopny provádět řadu různých sledovacích úkolů, včetně odeslání informací o poloze cíle, fotografování, kopírování událostí v kalendáři, registrace nových SIM karet vložených do zařízení a odposlech hovorů a odezírání zpráv, včetně těch z aplikací jako jsou Viber, WhatsApp či Skype.

Více informací o zprávě Kaspersky Lab naleznete zde.

Produkty Kaspersky Lab identifikují spywarové nástroje 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, Backdoor.AndroidOS.Criag.

O společnosti Kaspersky Lab

Kaspersky Lab je největším soukromě vlastněným poskytovatelem koncových bezpečnostních řešení na světě. Společnost se řadí mezi čtyři největší prodejce bezpečnostních řešení pro koncové uživatele. Již více než 16 let patří Kaspersky Lab mezi přední inovátory v oblasti informačních technologií a poskytuje efektivní digitální bezpečnostní řešení domácím uživatelům, malým a středním firmám i velkým podnikům. Aktuálně společnost registrovaná ve Velké Británii působí v bezmála 200 zemích a oblastech a poskytuje ochranu více než 300 milionům uživatelů. Více informací o společnosti Kaspersky Lab najdete na www.kaspersky.cz.*

**Společnost zařadil na čtvrté místo žebříček „IDC Worldwide Endpoint Security Revenue by Vendor, 2012“. Žebříček vyšel ve zprávě „IDC Worldwide IT Security Products 2013-2017 Forecast and 2012 Vendor Shares – August 2013“ a řadil poskytovatele software podle zisku z prodeje koncových bezpečnostních řešení v roce 2012.*

Pro další informace prosím kontaktujte:

Michal Malysa
PR Consultant
Grayling Czech Republic
Tel.: 224 251 555
Mobil: 775 708 086
michal.malysa@grayling.com
Twitter.com/GraylingCZ