Malware objeveno v Androidu

Jane K., 19. května 2020

Rumunská firma Bitdefender, která se zabývá zabezpečením počítačových systémů proti útokům zvenčí a která se považuje za jednu z nejlepších ve svém oboru oznámila, že objevila záškodnický program, neboli malware, který se zaměřuje na okrádání majitelů Androidů. Program se nazývá Mandrake a důvod, proč nebyl až doposud odhalen je ten, že se zaměřuje na jednotlivé uživatele.

Hackeři se soustředili hlavně na uživatele v členských zemích Evropské unie, ve Spojených státech, v Kanadě a v Australii. Vynechali chudší země, jako je třeba Afrika, některé arabské státy a jiné, ne příliš majetné země. Zjevně věděli, kde najít peníze.

Ten způsob, jak se na jednotlivé telefony dostali, byl s pomocí dalších programů, neboli apps, které se nacházejí v Google Play, jako jsou: OfficeScanner, Abfix, Currency XE Converter, Snap Tune Vid., CoinCast, Horoskope a Car News. V těchto programech ukryli svůj vlastní, který takto dostali na jednotlivé telefony. Hackeři pracovali důkladně, dokonce udržovali internetové stránky na jednotlivé programy, kde odpovídali na dotazy uživatelů a dokonce pro ně opravovali některé nedostatky původního programu. Také na stránkách sociálních medií měli hojnou účast.

Celý proces nainstalování jejich malware na telefon byl následující: Napřed si uživatel nainstaloval patřičný program z Google Play a s ním dostal i jejich virus. Ten se nazýval „dropper“ a byl využit pouze na to, aby stáhl na telefon instalační program, kterému říkali „loader.“ Aby to nebylo uživateli telefonu nápadné, tak to bylo vydáváno za obnovenou verzi původního programu. Loader, neboli instalační program potom stáhl hlavní program, který se jmenoval Core a tento umožnil hackerům převzít plnou kontrolu celé jednotky.

Pak mohli číst majitelovy sms zprávy a posílat přes telefon své vlastní. Mohli získat veškeré finanční přístupové informace majitele telefonu, nainstalovat nebo odinstalovat co chtěli, měli přístup ke jeho kryptoměně, pokud jakou měl, na Amazon a PayPal. Mohli rovněž provozovat fíšing útoky za účelem nakupování a financí, nebo si stáhnout seznam kontaktů majitele telefonu.

Když prohledali všecko, co na telefonu bylo a nenašli nic, co by se jim hodilo, pak spustili program, který se jmenoval „seppuku,“ což je japonské slovo pro druh sebevraždy. Tento pokyn vrátil telefon na původní nastavení, tak, jak přišel když byl původně zakoupen. A spolu s tímto bylo i jejich malware vymazáno, takže po nich nezůstala ani stopa.

Firma Bitdefender říká, že byly celkem dvě vlny této činnosti: ta první v letech 2016 až 2017 a druhá mezi 2018 a 2020. Počet obětí tohoto zločinu je odhadován na desetitisíce.

Je pravděpodobné, že své oběti okrádali tak, aby proti nim nebyly žádné důkazy a pokud možno aby to ani ti okradení nepoznali. Jak jinak by docílili, že to nikdo z majitelů telefonů nic takového nikde nehlásil? I když to zároveň nasvědčuje tomu, jak malou kontrolu svých vlastních financí lidé mívají. Rychlý pohled na zůstatek na účtu jim často postačí a nekontrolují jednotlivé položky.

Tak na příklad, jedna moje známá měla platit několika tisícový nedoplatek za plyn. Zdálo se jí to hodně peněz a tak šla na plynárnu domluvit, aby jí tento obnos strhávali po částech. Ale tam se dověděla, že peníze jí už byly strženy pár dnů před tím – nikdy si toho nevšimla!

Takové lidi hackeři milují a čím víc nedáváme pozor, tím víc na to můžeme doplatit.

ZDROJ:

https://sputniknews.com/world/202005181079342276-cybersecurity-firm-detects-android-malware-that-has-been-spying-and-stealing-from-users-since-2016/