Autor: Filip Peterek PET0342

LokiBot

Trojský kůň LokiBot byl poprvé detekován v roce 2015, objevuje se však dodnes. LokiBot byl využit pro velké množství útoků na více platforem. Během své pětileté historie tento malware posloužil jako keylogger, ransomware, server umožňující ovládat infikované zařízení pomocí příkazů poslaných přes HTTP, a jako nástroj umožňující krádež souborů obsahujících důležitá či privátní data, jako jsou hesla uložená v prohlížečích, apod.

LokiBot se ve svých počátcích šířil zejména na operačním systému Android. Nejprve infikoval knihovny systému Android a byl použit ke krádeži přihlašovacích údajů. Později se začal šířit pomocí .pdf souborů. Velkou škodu tento trojský kůň dokázal napáchat, když začal napadat populární, zejména bankovní, aplikace. LokiBot uměl na zařízení nainstalovat SOCKS5 proxy a přesměrovávat odchozí packety. Dále uměl rozesílat SMS zprávy a zobrazovat falešné notifikace. Po kliknutí na takovou notifikaci zobrazil LokiBot falešný overlay používaný pro phishing. Pokud se uživatel pokusil LokiBota smazat, nebo mu odebrat práva, malware spustil svou ransomware rutinu, vypsal zprávu, že zašifroval všechna uživatelská data, a požadoval zaplacení určitého výpalného pomocí Bitcoinu. Malware díky chybě v kódu uživatelská data nezašifroval, bylo jej možné odstranit po nabootování do safe modu. I přesto se ale tvůrcům LokiBota podařilo tímto způsobem ukrást přes 1.5 milionu dolarů.

V roce 2018 byl LokiBot, nepřekvapivě, detekován také na operačním systému Microsoft Windows. Původně se šířil jako spustitelný soubor využívající framework .NET, spárovaný s vysoce obfuskovaným zdrojovým kódem trojského koně napsaného v jazyce C#. Soubor se zdrojovým kódem také obsahoval velkou spoustu nesmyslného, ale validního, kódu, který neměl nic společného s malwarem. Spustitelný soubor fungoval pouze jako instalátor, software, který sám o sobě není považován za nebezpečný. Instalátory jsou využívány velkým množstvím softwaru v operačním systému Windows a antiviry je většinou nedetekují jako nebezpečné soubory, jinak by si uživatel pomalu nemohl ani instalovat software. Instalátor kód v jazyce C# zkompiloval, a výsledný binární soubor uložil do skryté složky. Spojení instalátoru a obfuskovaného kódu zpočátku umožnilo LokiBotu vyhnout se detekci antiviry. LokiBot byl ve Windows využíván ke krádeži dat a posílání již výše zmíněných příkazů pomocí protokolu HTTP. LokiBot využil toho, že běžný uživatel pravděpodobně nemá na svém stroji spuštěný HTTP server, zvláště na operačním systému Windows, ale také toho, že port 80 většinou není blokován firewally, a na infikovaném stroji spustil HTTP server, který poté útočník mohl využít k převzetí kontroly nad strojem.

Antiviry se samozřejmě postupně naučily LokiBota detekovat. Tvůrci malwaru samozřejmě nezaháleli, a brzy vynalezli způsob, jak předejít detekcí antiviry. Zdrojový kód trojského koně skryli pomocí techniky zvané ‘Steganografie.’ Steganografie je technika, která slouží ke kódování zpráv nebo kódu do na první pohled neškodných souborů, např. obrázků, jiných textových souborů, Word dokumentů, apod. Tyto soubory byly validní, zobrazitelné a renderovatelné, uživatel na první pohled nemohl poznat, že je s nimi něco špatně. Zdrojový kód byl později také kódován pomocí kódování base64, což dále ztížilo detekci nebezpečného kódu. Instalátor soubor dekódoval, čímž získal původní program v jazyce C# a dále již postupoval jako obvykle. Následně začali tvůrci LokiBota místo C# využívat také jazyka Visual Basic, který jim, díky tomu, že také funguje na platformě .NET, poskytoval naprosto stejné možnosti jako jazyk C#, nevyžadoval ale kompilaci a instalaci. Místo instalace binárního souboru, který by mohl vzbuzovat pozornost, byl radši kód interpretován při každém spuštění.

V únoru roku 2020 využil LokiBot popularity hry Fortnite. Malware se maskoval jako Epic Launcher, využívaný například hrou Fortnite. Při instalaci falešného launcheru byl počítač uživatele automaticky infikován také LokiBotem. Tvůrci LokiBota zde využili zejména vysoké popularity hry Fortnite mezi dětmi. Menší děti často neví, kde hledat oficiální Epic Launcher, často ještě neumějí používat počítač, nebo také nemají své vlastní uživatelské účty v operačním systému. LokiBot tak mohl využít dětské naivity a neznalosti k přístupu k datům rodičů, datům často zneužitelných, jako jsou například bankovní údaje.

LokiBot často ke svému šíření využíval sociální inženýrství. Jako obrana proti takovýmto útokům slouží vzdělávání uživatelů, aby neotvírali přílohy nevyžádaných emailů, neznáme soubory stažené z internetu, aby si ověřovali že skutečně stahují správný soubor ze správných stránek, aby neposkytovali absurdní pravomoce aplikacím a programům (např. kalkulačka pravděpodobně nepotřebuje přístup k fotoaparátu nebo geolokaci), apod. Dále pomáhá udržovat antivirový software aktualizovaný. Užitečnou ochranou může být ale také porovnávání kontrolního součtu staženého souboru s kontrolním součtem uvedeným na oficiálních stránkách distributora, nebo využívání rolling release distribuce bezpečného operačního systému a pravidelné updatování kernelu.

Zdroje

[1] https://www.zdnet.com/article/new-lokibot-trojan-malware-campaign-comes-disguised-as-a-popular-game-launcher/

[2] https://www.zdnet.com/article/lokibot-information-stealer-now-hides-malware-in-image-files/

[3] https://us-cert.cisa.gov/ncas/alerts/aa20-266a

[4] https://www.bleepingcomputer.com/news/security/lokibot-android-banking-trojan-turns-into-ransomware-when-you-try-to-remove-it/