Filip Peterek, PET0342

Esport
Analýza souborů

Soubor 1 - Bezpečný soubor

link: https://cuckoo.cert.ee/analysis/1954904/summary
analyzovaný soubor: putty.exe
hodnocení: 0.7

PuTTY je známá aplikace, která slouží jako grafický Windows klient pro vzdálené připojení k TTY unixových systémů (např. pomocí Telnet nebo SSH). To, že je PuTTY známý program ovšem ještě neznamená, že se nepotýkáme s kompromitovaným binárním souborem obsahujícím kromě programu PuTTY také nebezpečný kód, nebo že se prostě nějaký program za PuTTY nesnaží vydávat. Nejjednodušší způsob, jak ověřit pravost binárního souboru je pomocí checksumu (MD5, SHA256, apod.). I tak ale může být vhodné, nebo alespoň zajímavé, ověřit si binární soubor analyzátorem.

Analyzátor YARA nalezl spoustu akcí, které by mohly být potenciálně nebezpečné, v kombinaci s jiným chováním programu. Mezi tyto akce patří například kontrola, jestli je program debugován, vyhledávání konstant a hashů, komunikace pomocí TCP, komunikace s DNS, vytváření mutexů, vytváření záznamů v registerech, úprava uživatelského profilu nebo tvorba screenshotů. Ačkoliv by všechny tyto akce mohly představovat potenciální problém (např. čtení hashů a komunikace pomocí TCP socketu by mohl teoreticky mohl být pokus o ukradení privátních klíčů), v rámci kontextu aplikace PuTTY toto chování dává smysl. SSH využívá klíče vygenerované pomocí SHA256 pro ověřování totožnosti, dává tedy smysl, že PuTTY bude implementovat možnost číst, případně i vytvářet, tyto klíče. Komunikace pomocí TCP v programu, který slouží pro vzdálenou komunikaci, asi nikoho nepřekvapí, stejně jako tvorba mutexů, bez kterých se v multithreaded aplikacích neobejdeme.

Také byla detekována kontrola množství systémové paměti. Množství paměti sice může pomoct při detekci virtuálních strojů (kterým je většinou přiřazen pouhý zlomek celkové paměti fyzického stroje), také ale může sloužit k detekci méně výkonných strojů a program se může chovat šetrněji.

Dále byl detekován pokus načíst soubor s ‘nezvyklou příponou’ jako dynamickou knihovnu (dll). To sice může znít podezřele, avšak při podrobnějším prozkoumání zjistíme, že tím souborem byl ‘hhctrl.ocx’. Tento soubor je oficiální knihovna vytvořená Microsoftem, balená např. k Internet Exploreru. Vzhledem k původu souboru je tedy pochopitelné, že jej analyzační software detekuje jako potenciálně nebezpečný soubor, načtení tohoto souboru však pravděpodobně nepředstavuje bezpečnostní problém.

Soubor 2 - Nebezpečný soubor

link: https://cuckoo.cert.ee/analysis/1954820/summary
analyzovaný soubor: Adobe Photoshop - 2020 v21 1 2 (x64x86) Patched.exe
hodnocení: 10

Program Photoshop pravděpodobně není třeba představovat. Adobe Photoshop je všeobecně známý software sloužící k úpravě fotografií a tvorbě grafiky. V tomto případě je ovšem více než jasné, že se útočník snaží za Photoshop vydávat, případně pouze do binárky Photoshopu přidal nebezpečný kód a útočí na lidi, kteří nejsou ochotní obětovat 15€ měsíčně a Photoshop si chtějí socialisticky přivlastnit (upirátit).

V případě tohoto souboru YARA nedetekovala nic. Přesto však bylo nalezeno spousta potenciálních i reálných problémů a spousta akcí, které by program na úpravu grafických souborů neměl dělat. Dotaz na název stroje nemusí značit problém. Stejně tak alokace executable paměti nebo kontrola množství paměti, Photoshopu nedělá problém využít velké množství RAM a na slabějším HW by se mohl chovat šetrněji, i za cenu snížení komfortu uživatele.

Prohledávání paměti a procesů nebo tvorba spustitelných souborů na disku už je podezřelejší, přesto to nemusí znamenat problém. HTTP request na externí adresu už je podezřelý dost. HTTP requesty na localhost nebo HTTP requesty v rámci lokální sítě problém neznamenají, ovšem nezabezpečený HTTP request na externí adresu už vypadá podezřele. Dále program jako Photoshop pravděpodobně nepotřebuje kontrolovat stavy interfaců počítače a zjišťovat jejich adresy.

Ze závažnějších problémů by kontrola názvu CPU ještě mohla dát smysl, např. pro průzkum trhu při následujícím vývoji. Sbírání informací o nainstalovaných aplikacích může být využito např. pro kontrolu závislostí nebo kompatibilních programů, program hledal např. instalaci Pythonu 2.7 (ačkoliv interpretery jsou většinou baleny k programům, aby si uživatel nemusel instalovat interpretery jazyků Python, Lua apod. sám) nebo dalších Adobe produktů.

Nepopíratelným problémem je ovšem detekce messengerů, sbírání informací o nainstalovaných messengerech a účtech, pokus o přístup do Bitcoin peněženky a přidávání ransomware crypto přípony (.wallet) za enkryptované soubory. Dále jako indikátor nebezpečnosti programu slouží to, že byl detekován 60 antiviry jako škodlivý soubor. S největší pravděpodobností se tedy v tomto případě nejedná o skutečný Photoshop, ale o ransomware, který se snaží ukrást od oběti kryptoměny, ať už nevědomě nebo vědomě.

Software pro analýzu samozřejmě nemusí nutně znát kontext programu, jak bylo zmíněno výše, kontrola přítomnosti interpreteru Python nemusí nutně znamenat bezpečnostní riziko, přesto je ovšem schopný relativně přesně detekovat nebezpečný software např. pomocí akcí, nebo jejich kombinací, typických pro malware. Bezpečnost našich zařízení ale můžeme ovlivnit sami také analýzou výstupů analyzačního softwaru, nebo např. pouhou analýzou práv, o které si software zažádá (např. kalkulačka na telefonu pravděpodobně nepotřebuje přístup ke kontaktům a fotoaparátu).