Detekcia Command and Control (C2) komunikácie

Autor: Ing. Martin Kubečka
Vedúci práce: Mgr. Martin Bečka, PhD.
Univerzita: SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
Fakulta: FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Pri mnohých kybernetických útokoch používajú škodliví aktéri Command and Control (C2) komunikáciu na udržiavanie kontroly nad kompromitovanými systémami, alebo zariadeniami. C2 komunikácia umožňuje útočníkom vykonávať vzdialené príkazy na infikovaných systémoch a prijímať z nich údaje späť, bez vedomia používateľa daného systému. Pokročilí útočníci využívajú sofistikovanejšie metódy, aby sa vyhli odhaleniu, ako napríklad používanie šifrovania, alebo maskovania ich škodlivých aktivít takými spôsobmi, aby sa daná sieťová komunikácia javila ako legitímna.

Vychádzajúc z analýzy vybraných voľne dostupných C2 frameworkov s otvoreným zdrojovým kódom a techník, ktoré poskytujú pre C2 komunikáciu, sme navrhli a vytvorili vlastnú aplikáciu na detekciu predmetnej komunikácie s názvom C2Detective. Aplikácia spracováva odchytenú sieťovú prevádzku z PCAP súborov, pričom používateľ môže taktiež využiť funkcionalitu odchytávania sieťovej prevádzky, ktorej parametre sa nastavujú prostredníctvom konfiguračného súboru. Pri návrhu popisovanej aplikácie sme kládli dôraz na zabezpečenie jednoduchej integrácie nových detekčných techník, napríklad pomocou rozšírení. Túto vlastnosť sme demonštrovali využitím lokálnej databázy C2 riadiacich serverov, ktorej údaje agreguje a spracováva nástroj C2Hunter. Tento nástroj, ktorý sme vyvíjali nezávisle od našej práce, využíva mimo iné techniku fingerprinting v spojení s dátami, ktoré poskytuje služba Shodan.

Celkovo sme implementovali jedenásť detekčných metód, ktoré v konečnom dôsledku dokážu zachytiť štrnásť potenciálnych indikátorov C2 komunikácie, a to konkrétne techniku DNS Tunneling, DGA doménové mená, známe škodlivé JA3 odtlačky, sieťové spojenia s nadmernou frekvenciou, dlhé sieťové spojenia, neobvykle veľké HTML odpovede, známe hodnoty TLS certifikátov vybraných C2 frameworkov, Tor komunikáciu a zároveň aj konkrétne sieťovú komunikáciu k výstupným uzlom Tor siete, dopytované doménové mená, ktoré sú spájané s ťažbou kryptomien, známe IP adresy a známe doménové mená C2 riadiacich serverov, ktoré prijali, alebo iniciovali sieťové spojenie, známe škodlivé URL adresy, ktoré sú spájané s C2 komunikáciou a v neposlednom rade sieťovú komunikáciu s potenciálnymi C2 riadiacimi servermi. Prostredníctvom API rozhraní vybraných služieb aplikácia C2Detective umožňuje používateľovi obohatiť detegované indikátory C2 komunikácie o informácie, ktoré sú výsledkom procesov Cyber Threat Intelligence.

Výstupom aplikácie C2Detective je správa o výsledkoch analýzy vo formáte HTML a PDF. Takéto výstupné správy poskytujú používateľovi detailný prehľad detegovaných indikátorov C2 komunikácie a ďalších relevantných informácii.