IstroSec

Data Sheet

Analýza malvéru

Väčšina kybernetických útokov využíva v nejakej miere škodlivé programy, tzv. malvér. Veľmi časté sú ransomvérové útoky, ale aj útoky, pri ktorých si útočníci vytvoria zadné dvierka do siete svojej obete, cez ktoré získajú vzdialený prístup, prípadne infikujú svoju obeť nejakou formou špehovacieho malvéru. Taktiež aj phishingové útoky sa v nemalej miere spoliehajú na doručenie infikovanej prílohy alebo podvrhnú obetiam webovú stránku, na ktorej môže byť umiestnený malvér.

> *V prípade cielených alebo pokročilých kybernetických útokov, sa v rámci reakcie nestačí spoliehať len na bežnú kontrolu antivírusom a škodlivý kód je potrebné podrobnejšie analyzovať.*

Kedy je potrebná podrobnejšia analýza malvéru?

- predpoklad pokročilého alebo cieleného útoku
- relatívne nová alebo neznáma vzorka malvéru, ktorá nie je detegovaná štandardnými antivírmi
- pre posúdenie rizík a možných dopadov útoku je potrebné identifikovať kompletnú funkcionalitu, schopnosti a konfiguráciu danej vzorky
- identifikácia podobných útokov a kampaní, príprava na ďalšie kroky útočníka
- threat intelligence a defensive intelligence špecializovaný na mieru konkrétnemu klientovi
- identifikácia a odstránenie perzistencie a všetkých artefaktov vytvorených malvérom bez potreby reinštalácie celého operačného systému; najmä v prípadoch, keď štandardné antivíry nájdu len malú časť artefaktov alebo vôbec žiadne

Služby v rámci analýzy malvéru

- statická a behaviorálna analýza - identifikácia typu malvéru, jeho základných charakteristík a správania
- príprava identifikátorov kompromitácie - IOCs, ktoré môžu byť použité počas riešenia incidentu, forenznej analýzy, monitoringu alebo threat huntingu
- identifikácia, či malvér cieli na konkrétnu obeť alebo je súčasťou štandardných hromadných kampaní
- extrakcia konfigurácie (pokiaľ je to možné)
- analýza funkcionality a schopností malvéru
- priradenie konkrétnej vzorky k skupine útočníkov alebo ku kampani (pokiaľ je to možné) - tzv. atribúcia
- pokročilá analýza malvéru a reverzné inžinierstvo - kompletná analýza funkcionality aj obfuskácie a ochrany pred analýzou a detekciou, výskum podobných a/alebo súvisiacich prípadov
- malware intelligence
- vytváranie špecializovaných očkovacích programov, ktoré zabránia infekcii ďalších zariadení malvérom použitým počas kybernetického útoku
- vytváranie špecializovaných programov na odstránenie artefaktov vytvorených malvérom počas útoku

IstroSec

Data Sheet

Prečo práve my?

Skúsenosti a znalosti

Naši certifikovaní experti majú dlhoročné skúsenosti s analýzou malvéru. Analyzovali stovky vzoriek, vrátane malvéru z pokročilých cielených útokov typu APT na vládne ciele aj globálne súkromné spoločnosti. Poznajú taktiky, techniky a postupy útočníkov a majú znalosti potrebné na to, aby Vám v rámci reakcie na incidenty umožnili robiť rozhodnutia na základe analýzy vzoriek malvéru použitých v rámci útoku.

Expertíza v analýze malvéru

Popri analýze malvéru sa naši experti venujú aj vlastnému výskumu v oblasti malvéru, trendov, prevencie a threat intelligence. Taktiež vytvorili viaceré komunitné open source nástroje a svoje výsledky publikovali v mnohých prácach, prípadových štúdiách aj na konferenciách v Európe aj v USA, vrátane DEFCON a BlackHat. Štyria naši experti boli súčasťou víťazného tímu LockedShields 2016.

Certifikovaní profesionáli

Experti **Istro**Sec sú držiteľmi medzinárodne uznávaných certifikátov v mnohých oblastiach. Držíme certifikáty, ako napríklad Certified Information Systems Security Professional (CISSP), Certified Information system Auditor (CISA), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA) a ďalšie.

Prípadové štúdie

Typ organizácie: Vládne inštitúcie

Poskytnutá služba: Analýza malvéru

Riešenie: Pokročilá analýza malvéru, výskum súvisiacich hrozieb a príprava identifikátorov kompromitácie.

Naši analytici počas svojho výskumu zaznamenali vzorku malvéru tváriacu sa ako dokument pochádzajúci od istej štátnej inštitúcie. Po vykonaní podrobnej analýzy odhalili, že dokument bol súčasťou phishingovej kampane, ktorá infikovala svoje obete komerčným nástrojom Cobalt Strike. Tento nástroj je často používaný penetračnými testermi aj pokročilými útočníkmi s cieľom ovládnuť napadnuté počítače. Na základe extrahovanej konfigurácie naši analytici odhalili server využívaný útočníkmi na komunikáciu s napadnutými zariadeniami. Zároveň s využitím našich metód pre malware intelligence analytici odhalili aj ďalšie servery, ktoré útočníci použili v podobných útokoch proti vládnym inštitúciám, prípadne ich mali pripravené pre nasledujúce útoky. Poskytnutím identifikátorov kompromitácie vládnej jednotke CSIRT v danej krajine tak bolo možné odhaliť ostatné obete útočníkov a zabrániť ďalším útokom využívajúcim pripravenú operačnú infraštruktúru útočníka.

Typ organizácie: Veľká komerčná vývojárska firma

Poskytnutá služba: Analýza malvéru (+forenzná analýza a riešenie incidentov)

Riešenie: Pokročilá analýza malvéru, malware intelligence, odstránenie artefaktov vytvorených malvérom počas útoku

Klientske zariadenia začali vykazovať nezvyčajne vysoké zaťaženie CPU. Spôsobovali ho spustené procesy, ktoré sa podobali na niektoré služby systému Windows, avšak neboli legitímne. Antivírový program niektoré z nich identifikoval ako malvér na ťažbu kryptomien, no ich odstránenie nebolo úspešné a veľmi rýchlo sa odstránené súbory vytvárali znova. Analýza malvéru odhalila niekoľko metód perzistencie, ktoré daný malvér využíval. Následný malware intelligence výskum odhalil ďalšie škodlivé artefakty, ktoré boli použité pri tomto útoku, avšak medzičasom už boli vymazané. Vďaka týmto artefaktom bolo možné napokon zrekonštruovať celý útok vrátane identifikácie prieniku - exploitácie zraniteľnosti webovej aplikácie, niekoľkých backdoorov a všetkých perzistencií, ktoré tak mohli byť odstránené. V spojení s údajmi z threat intelligence boli nájdené podobné útoky a vytvorená predstava o rozsiahlosti tejto celosvetovej kampane a ziskoch útočníkov.

IstroSec | Černyševského 10 | 851 01 Bratislava | Slovensko | +421 917 699 002 | info@istrosec.com | www.istrosec.com