Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

METODIKA K PROVĚŘOVÁNÍ INDIKÁTORŮ KOMPROMITACE

GovCERT.CZ v rámci své činnosti prevence a odhalování kybernetických bezpečnostních incidentů získává indikátory kompromitace (IoC) aktuálních bezpečnostních hrozeb. Při informaci o potenciální hrozbě můžete být kontaktování s žádostí o prověření, zda váš systém nebyl napaden a nekomunikuje se škodlivou adresou, nebo se v něm nevyskytují škodlivé soubory.

Zasílanými indikátory bývají především:

- IP adresy
- URL a domény
- hashe souborů (MD5, SHA1, SHA256)[1]

POSTUP PŘI KONTROLE

Komunikaci s IP adresami prověřte v SIEM nebo sondě za specifikované období, případně za období, které máte k dispozici. Pokud nemáte SIEM (nebo jiný centralizovaný systém) ve své sítí nasazený, zkontrolujte adresy na firewallu perimetru sítě či dostupných koncových prvcích. Komunikaci s doménami prověřte v lozích DNS a proxy. Naše doporučení zde mohou být pouze obecná, při volbě způsobu kontroly se vždy řiďte znalostí své sítě a jejích přístupových prvků.

Upozornění: IP adresy, URL ani domény nikdy nezkoušejte otevírat nebo jakkoliv kontaktovat (např. nástroji ping, traceroute, nslookup, nmap). Informujete tím útočníka, že jeho aktivita mohla být odhalena, čímž může být vyprovokován k destruktivním krokům. Nikdy také nalezené podezřelé soubory nenahrávejte k online analýze (např. na VirusTotal), útočníci mohou tyto stránky monitorovat na přítomnost vzorku.

V případě nálezu identifikujte kompromitovaný stroj ve vaší síti a prověřte na něm přítomnost malwaru dle zaslaných hashů (pokud jsou pro daný případ uvedeny). Plošné prověřování hashe v celé doméně provádějte pouze, pokud máte centralizovaný nástroj, v opačném případě nikoliv.

[1] Pokud GovCERT.cz není původcem informace, je vysoce pravděpodobné, že hashe souborů budou pouze v jednom formátu a nebude v našich možnostech zajistit i formáty jiné.

Pro usnadnění analýzy kompromitovaného systému prosím dodržujte při zajišťování dat a manipulaci se strojem dříve publikovaná doporučení GovCERT.CZ:

- Minimální požadavky pro logy, které musí být zajištěny pro spolehlivou ex-post analýzu
- Návod na zajištění dat pro forenzní analýzu

Kontrolu indikátorů provádějte bezodkladně po obdržení informace, včasné odhalení může značně snížit škody a urychlit řešení incidentu.

POSTUP PŘI KONTROLE

Pozitivní nález jakéhokoliv indikátoru bezodkladně oznamte na cert.incident@nukib.cz.
Ve zprávě přiložte:

1. Informace o stroji, na kterém byl indikátor zaznamenán:
   - adresa,
   - umístění v síti,
   - funkce,
   - operační systém.

2. Záznam nálezu (výpis z logu/SIEM) s co nejpodrobnějším detailem komunikace, zejména **čas, port** a **přenesený objem dat**.

Pokud k záznamu indikátorů došlo důsledkem vaší analytické činnosti (např. daný malware jste již dříve zachytili a v kontrolovaném prostředí ho nechali kontaktovat C&C server), oznamte i tuto skutečnost. Usnadníte nám tím případné budoucí zkoumání zaznamenaných nálezů.

V negativním případě není třeba výsledek prověřování oznamovat, pokud vás o to výslovně nepožádáme.

Veškeré vaše dotazy a konzultace můžete vždy směřovat na cert@nukib.cz.