Advanced Persistent Threat (APT)

Pojem Advanced Persistent Threat (APT) je používán k popisu sofistikovaných hackerských technik zaměřených přímo na konkrétní cíl, kterým mohou být úspěšné velké společnosti, či dokonce státy.

Co je to APT - Advanced Persistent Threat?

Jedná se o velmi pokročilé techniky útoků, které se vyznačují:

Zaměřením:
organizace, finanční instituce, státy. Inflitrace není náhodná, malware je navržen specificky pro konkrétní cíl.

Pokročilostí:
jsou zneužívána doposud neobjevená slabá místa nebo zero-day zranitelnosti. Používají se rootkity, techniky zatemnění a maskování.

Perzistencí:
hrozba přetrvává, dokud útočník není úspěšný. Používají se pokročilé a cílené techniky sociálního inženýrství a phishingu na různých kanálech.

Proč tradiční formy ochrany nefungují?

Útoky tohoto typu jsou velmi sofistikované a těžko detekovatelné tradičními bezpečnostními opatřeními původně navrhnutými pro starší a méně pokročilé hrozby.

Hlavním důvodem slabé (nebo žádné) detekce APT tradičními prvky ochrany je způsob odhalování založený na signaturách malwaru a známých vzorech jeho chování. Tyto metody detekce jsou nedostatečné a ponechávají organizace nechráněné vůči rychle se měnícím hrozbám, které využívají neznámé nebo zero-days zranitelnosti. Útočník ve svůj prospěch využívá současně více vektorů hrozeb jako například web, email, sdílení souborů, mobilní zařízení, přičemž konkrétní útok je zpravidla rozdělen do několika fází, které trvají až několik měsíců.

Tradiční bezpečnostní opatření, která při detekci APT selhávají:

- **Antivirus** – schopný detekce známých druhů malwaru. Dynamický charakter pokročilého malwaru způsobuje, že antivirové společnosti nedokáží vydávat aktualizace dostatečně rychle. Tím se stanice stávají nechráněné po dobu minimálně jednoho dne od prvního výskytu nového malwaru.
- **IPS systémy** – detekce pokročilejšího druhu malwaru pomocí různých technik, původně navržených pro síťovou analýzu. Nedokáží odhalit zapouzdřený malware na aplikační vrstvě (prohlížeč, flash plugin, PDF soubor a jiné) a většinou jsou schopné detekovat pouze známé útoky.
- **Next-Generation Firewall** – kombinuje přístup klasického firewallu s technikami analýzy paketů (DPI) a IPS. Detekce malwaru se děje na základě signatur, avšak nedokáže úspěšně detekovat hrozby typu zero-day a cílený APT malware. Automaticky negeneruje pravidla pro nový druh malwaru.

Charakteristika produktů pro detekci APT

- Nenahrazují tradiční formy ochrany, ale doplňují detekci o APT.
- Poskytují ochranu před zero-day malwarem, APT a cílenými útoky.
- Kombinují a korelují data z více možných vektorů útoku jako jsou web, email, sdílení souborů.
- Dokáží odhalit malware v různých stádiích od průniku po extrakci dat.
- Poskytují ochranu v reálném čase před APT hrozbami.
- Poskytují analýzu síťových toků na základě detekce zpětných volání malwaru na C&C server, a to napříč různými síťovými protokoly.
- Umožňují integraci nejpoužívanějších SIEM řešení (McAfee Nitro, HP ArcSight, RSA, IBM QRadar) a EndPoint protection řešení (McAfee).
- Automaticky generují pravidla pro detekci neznámého malwaru na základě analýzy jeho chování.

Nabídka našich služeb

- Analýza vhodného řešení a návrh nasazení ochrany před APT – analýza existujících bezpečnostních opatření a navržení nových.
- Implementace zvoleného řešení.
- Podpora, rozvoj řešení a odborné konzultace k jednotlivým nálezům.
- Pronájem řešení ochrany proti APT (formou služby).

Naše přínosy

- Nekončíme jen implementací a podporou, aktivně pomáháme při řešení incidentů.
- Budujeme komplexní obranu, vnímáme slabá místa zabezpečení a dokážeme navrhnout řešení na míru.
- Naši konzultanti disponují know-how z oblasti hackerských útoků a pokročilého malwaru.

Nekupujte zajíce v pytli

- Využijte možnost nezávazného vyzkoušení nové technologie ochrany před APT ve vlastním prostředí vnitřní sítě.
- Instalace je velmi jednoduchá a vyžaduje minimální nebo žádné změny v současné konfiguraci.

www.aec.cz

Příklady APT ve světě

Stuxnet – speciální červ vytvořený s cílem narušit íránské úsilí jaderného rozvoje.

Operace Aurora - zero-day zranitelnost v Internet Exploreru 6.0, která byla použita při pokusu o krádež duševního vlastnictví a získání přístupu k uživatelským účtům v Google, Adobe, Symantec a mnoha dalších význačných organizacích.

Útok na RSA - phishingový e-mail poslaný na malou skupinu zaměstnanců, přičemž dobře reflektoval bezpečnostní návyky ve firmě. E-mail obsahoval soubor aplikace Excel s přílohou, pomocí které byl instalován backdoor přes Adobe Flash zero-day zranitelnost.

Zero-day zranitelnost v Internet Exploreru (CVE-2014-1776) byla využita pro cílený útok na vojenský, letecký a energetický průmysl. Útok měl původ v Číně a skládal se z phishigových emailů, které v sobě obsahovaly odkaz na webové servery s exploit kódem.

AEC, spol. s r.o.
Purkyňova 2845/101
612 00 Brno, Czech Republic
Phone: +420 530 507 200
Fax: +420 530 507 220

AEC, spol. s r.o.
European Business Center
Dukelských hrdinů 34
170 00 Praha 7, Czech Republic
Phone: +420 267 311 402
Fax: +420 266 177 155

AEC
DATA SECURITY