Systém skorého varovania

PUBLIC

Agenda

- Trend vývoja ochrany pre kyberzločinom
- Potreba nových informácií – Intelligence / Counterintelligence
- Analýza malware ako služba
- ESET Intelligence Service

Trendy ochrany

- IS organizácií (štátne/súkromné) sa stávajú cieľmi veľmi sofistikovaných útokov
  - Infiltrácia postupná, dlhší čas prípravy – objekty dlhší čas nečinné, kým je vykonaný útok
  - Útočí sa na najzraniteľnejší prvok = klient (klient I-bankingu, možno v budúcnosti E-government...)
- Detekcia takýchto útokov u preventívnych kontrolných systémov (firewall, IPS, AV,..) môže zlyhať
- Vzniká potreba kombinácie („mix“) s ďalšími „detektívnymi“ službami (file payload analýza, analýzy sietí,...) – tieto majú veľký význam pri odhaľovaní neznámych alebo prehliadnutých incidentov
- Nová potreba získania informácie alebo spravodajstva

Zdroj: Gartner: Market trends – Cybersecurity service providers ivade the Enterprise security services market (G00260738, 31.3.2014)

Security intelligence / counterintelligence

- Kľúčový prvok: **informácia** alebo **intelligence**
- Po nájdení novej zraniteľnosti, slabiny alebo hrozby - zverejnenie
- Ak útočník po sebe nechá stopu – informácie môžu slúžiť k ochrane v budúcnosti (alebo u iných entít)
  - napríklad informácie o
    - botnetoch a ich C&C (informácie pre organizáciu, či nie je v atakovaný daným botnetom.)
    - ďalších „zlých“ destináciách na internete, file-och, alebo iných objektoch na rôznych úrovniach
  - Môžu poskytnúť informáciu, či organizácia bola v nejakom „kontakte“ s takýmto objektom

Zdroj: Gartner: Market trends – Cybersecurity service providers ivade the Enterprise security services market (G00260738, 31.3.2014)

Východiská / predpoklady pre Security Intelligence

- ESET produkt používa vyše 110 mil. používateľov
- Denne 100 – 200 tis. detekcií potenciálnych hrozieb (malware)
- Analýza malware - zdroj informácií o:
  - Správaní / funkcionalite malware
  - Riadiacich C&C serveroch
  - Adresy serverov pre download súborov (častí malware, updatov, ...)
  - Informácie o konkrétnych web-injectoch

Analýza malware

Ako služba:

- Požiadavka zákazníka
- Úvodná analýza a odpoveď do 24 hod.
- Analýza malware
- Sprístupnenie informácií (report)
- Sledovanie stavu

ESET Intelligence Service

Momentálne ako pilot, by mohla poskytnúť organizáciám informácie:

- Či sú v súčasnosti cieľom útoku, alebo či sa chystá cielený útok
- O identifikovaných kľúčových objektoch konkrétneho botnetu
  - Príklad:
    - URL / IP adresy serverov botnetu
    - Vzorky súborov s malware, informácie o ich update-och
    - Štatistika výskytu
    - Akcie vykonané po spustení kódu

Q & A

Vďaka za pozornosť!

Peter Katrinec
IS Security Services Department

katrinec@eset.sk