Egy malware kalandjai az NMHH-nál

Incidenskezelés az üzemeltetés nézőpontjából

EIVOK 60

Barczi Tamás

Hatósági IT

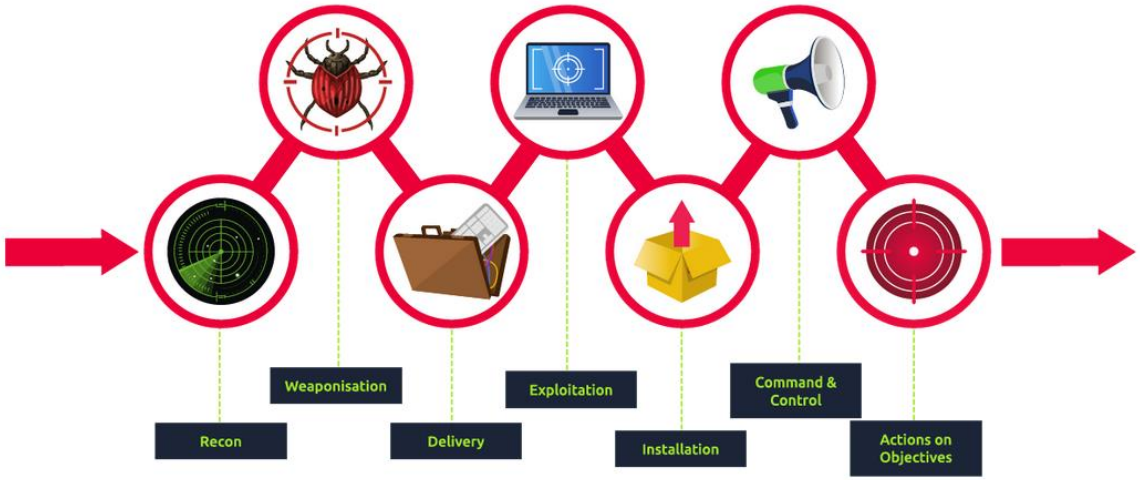
- IT nélkül a hatósági munkavégzés elképzelhetetlen
  - Minden kolléga életében központi helyet foglalunk el

Esemény előtt vagy után? Esetleg közben?

- Hogy néz ki az üzemeltetés szintjéről?
- Hogyan lesz gyors, hatékony és fájdalommentes?
- Növekvő fenyegetettség – szinte bárki lehet támadás célpontja

A malware útja

- Recon
- Weaponisation
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objectives



Recon

- OSINT
- Publikusan elérhető adatok, leak DB-k, darkweb

Mit teszünk mi?

- Támadási felület csökkentése
- Leak DB-ben szereplő adatok használatával belsős takarítás

Weaponization

- Exploitok alapján létrehozzák a megfelelő payloadot, például…

Mit teszünk mi?

- Hash ellenőrzések
- Threat db-k
- RBL-ek
- CSIRT

Delivery

- Phishing mailek
- USB driveok
- Watering hole attack

Mit teszünk mi?

- Proxyk, tűzfalak, sandboxok, és logelemzők hada
- A felhasználók biztonsági tudatosságra oktatása

Exploitation

- Miután sikeresen megtörtént a célbajuttatás, a sérülékenységek kihasználásával laterális hálózati mozgás és magasabb jogosultságok megszerzése a cél

Mit teszünk mi?

- Gyanús írás/olvasás arány, szokatlan kapcsolatok, scannelés, sessionök száma, teljesítmény anomáliák figyelése
- Rendszerek, szignatúrák és szabályok folyamatos frissítése

Installation

- Állandó backdoor létrehozása a későbbi hozzáféréshez
- Web shell, Meterpeter, Windows servicek létrehozása és módosítása, run keyek hozzáadása a registryben vagy a startup folderben

Mit teszünk mi?

- Vírusírtók, endpoint protectionök, és központosított monitoring

Command & Control

- C2 channel működtetése, IRC, DNS tunneling, Telegram RAT,

Mit teszünk mi?

- Proxyk, kifelé irányuló tartalmak bontása és szűrése

Actions on Objectives

- A hat fázis után a „munka” gyümölcse:
  Belépési adatok, belső felderíés, adatok gyűjtése és kijuttatása, backupok és shadow copyk törlése, adatok felülírása, titkosítása, olvashatatlanná tétele

- Mit teszünk mi?
- Belső monitorozás, gyanús írás/olvasás arány, szokatlan kapcsolatok, scannelés, sessionök száma, hibás loginok mennyisége és…

Esemény után – kétségbeesés helyett

- Ha már nyakoncsíptük a támadót:
- Sandbox elemzések szeparált környezetben (főleg, de nem kizárólag NKI), Autopsy, egyéb forensics eszközök és játszós környezetek
- Tanulságok levonása
- Dokumentációk frissítése
- Új folyamatok kialakítása

NMHH mint lakossági szolgáltató

- KiberPajzs projekt
- Digipedia.hu
  - Gyerekvédelem, online pénzügyek, netes veszélyek, adatvédelem

Nemzeti Média- és Hírközlési Hatóság

Köszönöm megtisztelő figyelmüket!