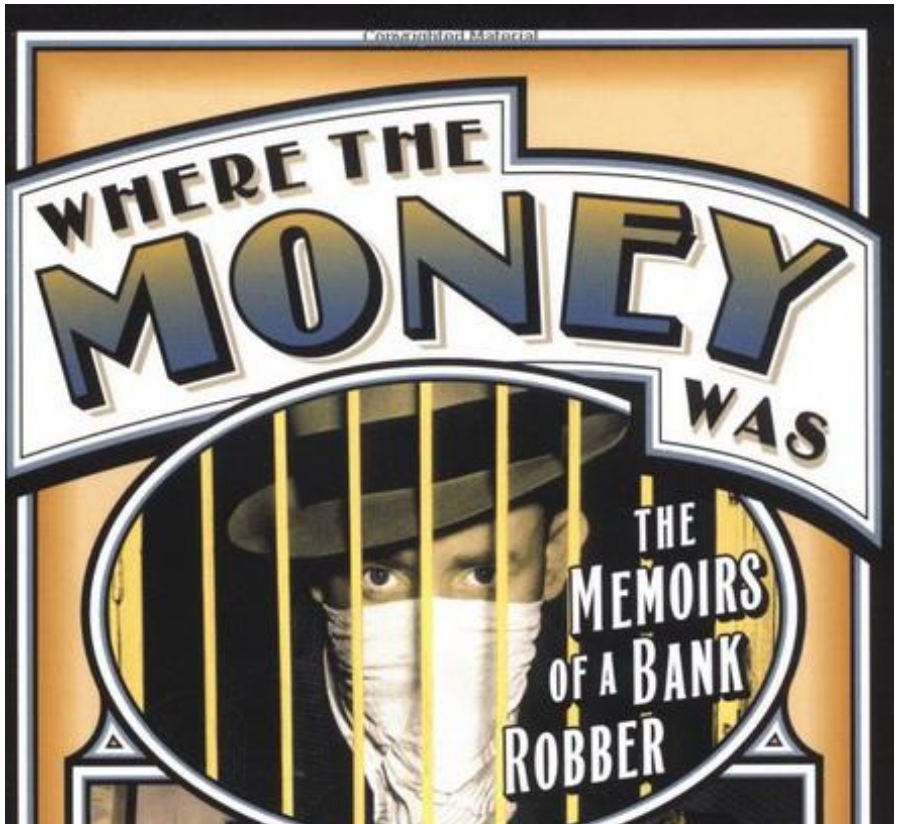
A támadók gondolkodásmódjának változása egy banki malware evolúciójának tükrében



RÓLAM

Sándor Fehér

- **CEO** of White Hat IT Security
- **IT security manager**
- **Visiting lecturer** @ Óbuda University Budapest
- **15+ years** of ITS experience
- **OSCP, OSCE** certified
- **CISM** certified
- Father of one
- Enthusiastic mountain biker
- IT Sec community builder

MIÉRT EZ A TÉMA?

Egyre nagyobb bajt okoznak a pénz motivált támadók.

VÉDEKEZŐ OLDAL

Incident Response Team

- Az ő feladatuk, hogy ~~ha~~ **amikor** incidens van, akkor reagáljanak
- Jellemzően külső erőforrásból

Blue Team

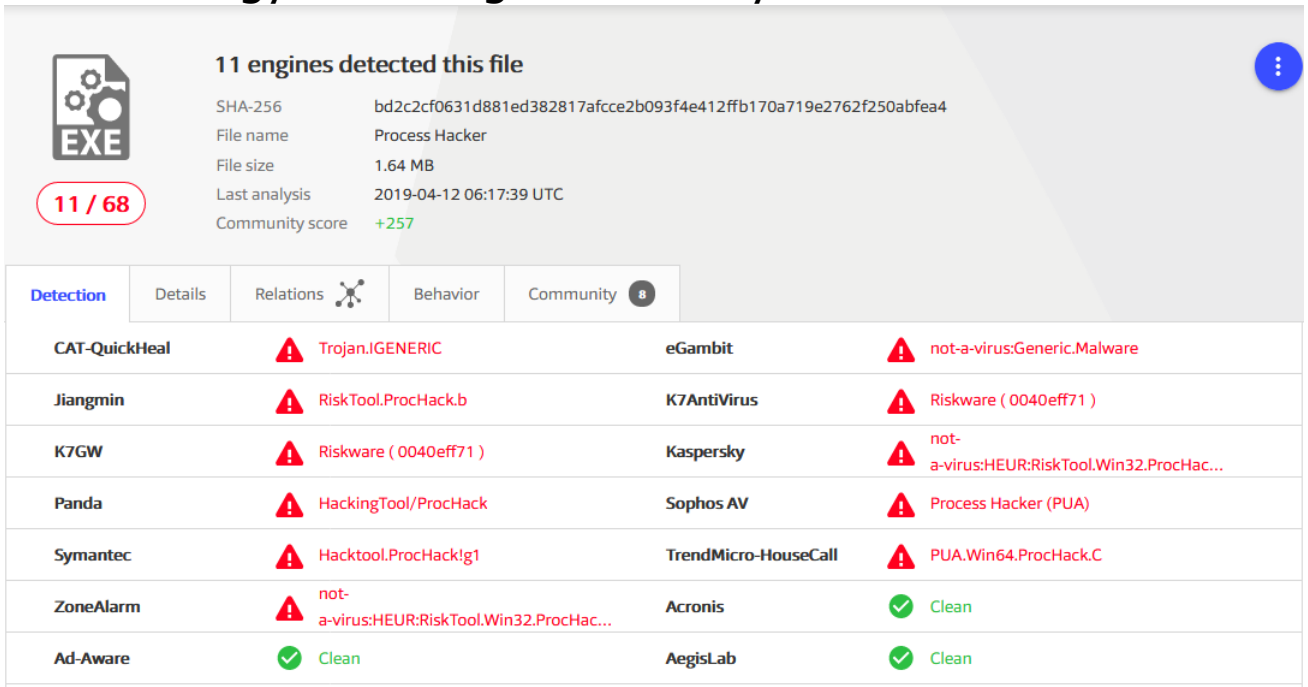
- Az ő feladatuk a vállalaton belüli IT rendszer biztonságának szavatolása
- Jellemzően belső erőforrás

MÚLT

- Egy **malware** általában egy funkcióval bírt
- **Kategóriák**: adware, spyware, RAT, trojan, PUA, rootkit, keylogger, virus, worm, stb.
- **Kill chain**: bejuttatás, perzisztencia, kívánt cél elérése
- **Eszköztár**: keylogger, 1-day exploitok, RAT (remote access tool), célspecifikus kód (pl. banki trójaiak – Zeus, Kronos)
- **Miért**: mert csak a netbankolásból lehetett pénzt szerezni
- Kivétel – **APT**
  - nem számít az anyagi vagy emberi erőforrás
  - cél az információszerzés
  - nekik volt a kezükben 0-day, 1-day, rootkit, satellite connections…

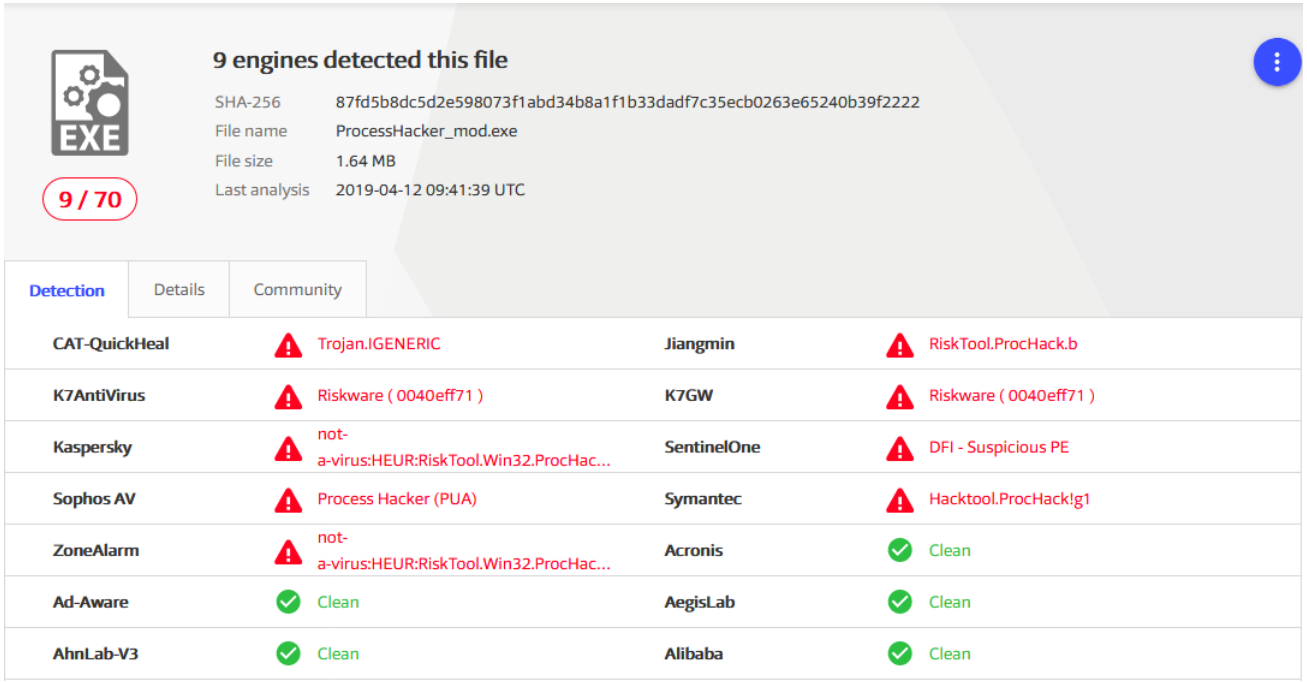
IR KIHÍVÁSOK RÉGEN

- Detekció szignatúra alapon elérte az elégséges szintet
- Detekció esetén: replikált példányok keresése, C2 csatorna szűrése, perzisztencia kiiktatása, majd eltávolítás
- Persze szignatúra és szignatúra között is van különbség
  - gyakran „csak” hash adatbázis volt egy antivírus
  - relatív egyszerű megkerülni az ilyen szintű szűrést



IR KIHÍVÁSOK RÉGEN

- Detekció szignatúra alapon elérte az elégséges szintet
- Detekció esetén: replikált példányok keresése, C2 csatorna szűrése, perzisztencia kiiktatása, majd eltávolítás
- Persze szignatúra és szignatúra között is van különbség
  - gyakran „csak” hash adatbázis volt egy antivírus
  - relatív egyszerű megkerülni az ilyen szintű szűrést



JELEN

- Nagyobb a probléma!
- **Miért**: sokkal több „értékes” van a gépünkön (desktop, mobile, cloud):
  - banki azonosítók,
  - accountok bankkártya-adatokkal vagy anélkül
  - kriptovaluta
  - GPU idő
  - hozzáférés a géphez, hálózathoz, VPN stb.
  - szenzitív vagy értékes adat – ransomable
- Sokkal több pénz → sokkal több erőforrás → sokkal fejlettebb technológia

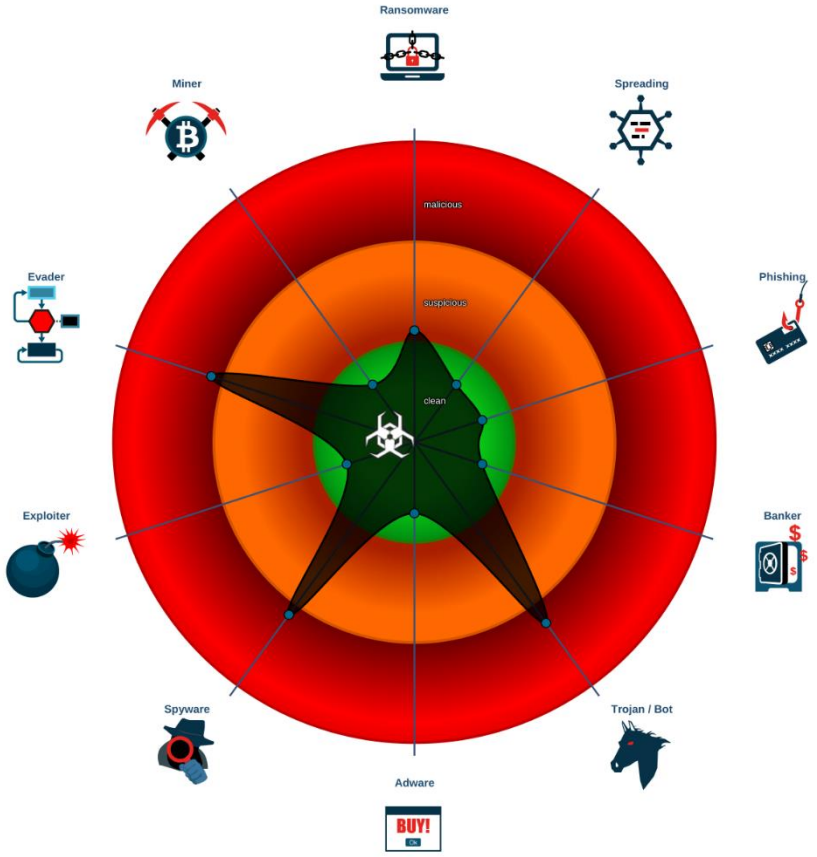
JELEN

Hány weboldal / account / applikáció fér hozzá bankkártya adatokhoz?

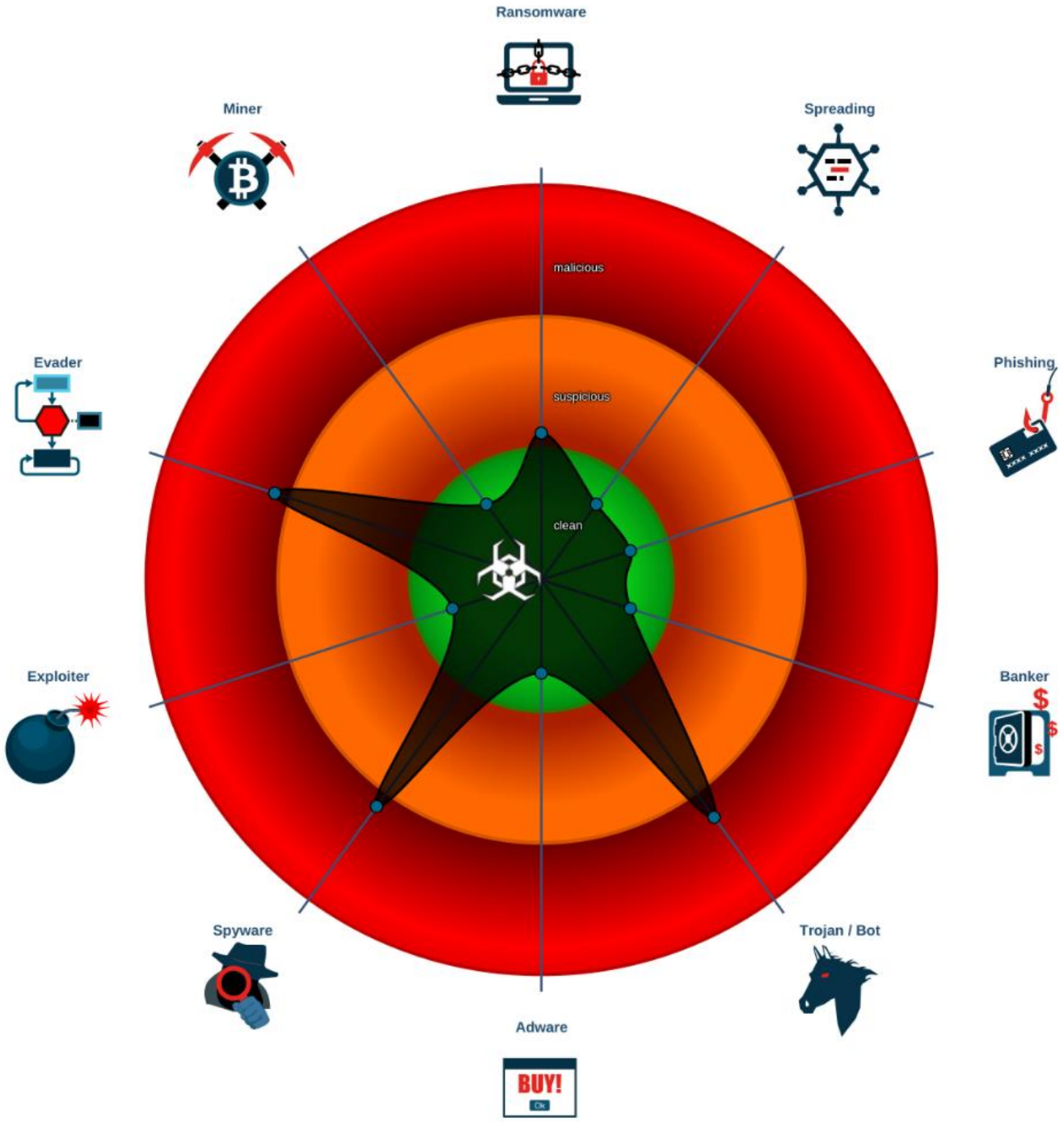
- online bankolás
- online fizetési platform
  - PayPal, Simple, P2P fizetési platformok
- online fizetés
  - számtalan webshop és app
- kriptovaluta
  - tőzsde, fizetés, tranzakciók
- játék / applikációk
  - Steam, Origin, Play Store, App Store, Microsoft Store, PlayStation Store

JELEN

- 0-day kivételével minden rendelkezésre áll (az meg csak azért nem, mert nincs szükség rá)
- **moduláris** malware, **fejlett C2** infrastruktúra
- **kategóriák** átalakultak, és direkt besorolás helyett eloszlásssal sorolnak be egy támadó kódot: ransomware, spreading, phishing, banker, trojan, adware, spyware, exploiter, evader, miner kevert klasszifikáció
- **kill chain**: terjesztés, bejuttatás, perzisztencia, belső recon, lateral movement, több cél
- minden állomásra van vehető "szolgáltatás": spam service, phishing kit, exploit kit, Malware-as-a-Service, C2 panel - akár Tor hálózaton



JELEN


Ransomware
Miner
Spreading
malicious
suspicious
clean
Evader
Phishing
Exploiter
Banker
Spyware
Trojan / Bot
Adware
BUY!
Ok

TRICKBOT

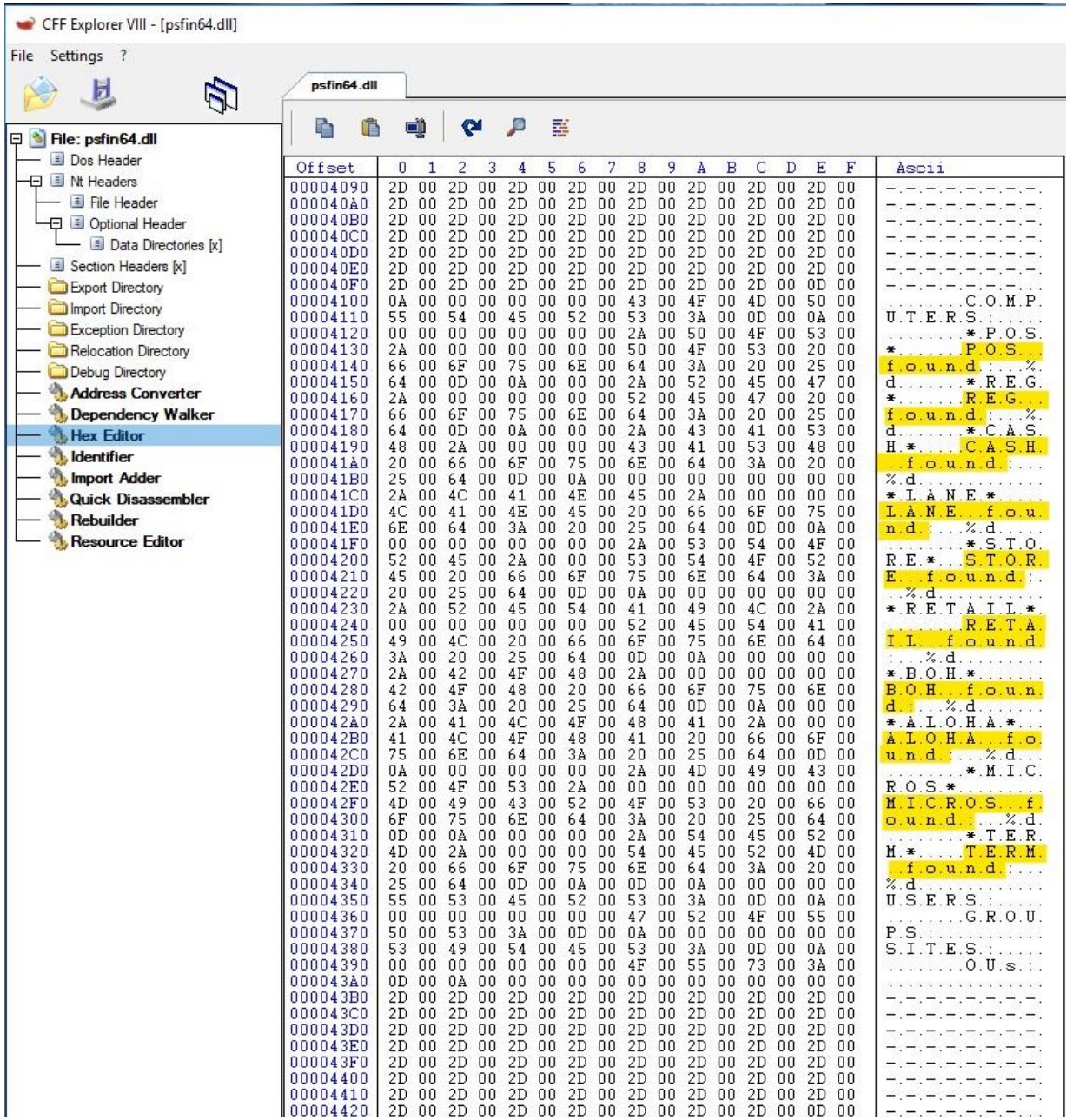
- 2016-ban indult ezen a néven "egyszerű" banki trójaiként
- Mára túl van a 400. verzión, és legalább 15 különböző modulja van
- Pénzszerzés
  - banki honlapokról azonosítók lopása
  - egyéb (minden) account ellopása
  - kriptovaluta bányászás
  - ransomware, ha a target high-value
- Automatizált fertőzés és framework, operátorokkal kiegészítve

TRICKBOT MODULOK

Felderítés

- appinfoDll64.dll: felhasználók és ütemezett feladatok
- mailsearcher64.dll: e-mail kliensek
- networkDll64.dll: hálózati beállításokkal kapcsolatos információ
- psfin64.dll: **Point Of Sale felderítés**
- systeminfo64.dll: rendszerinformációk

TRICKBOT MODULOK

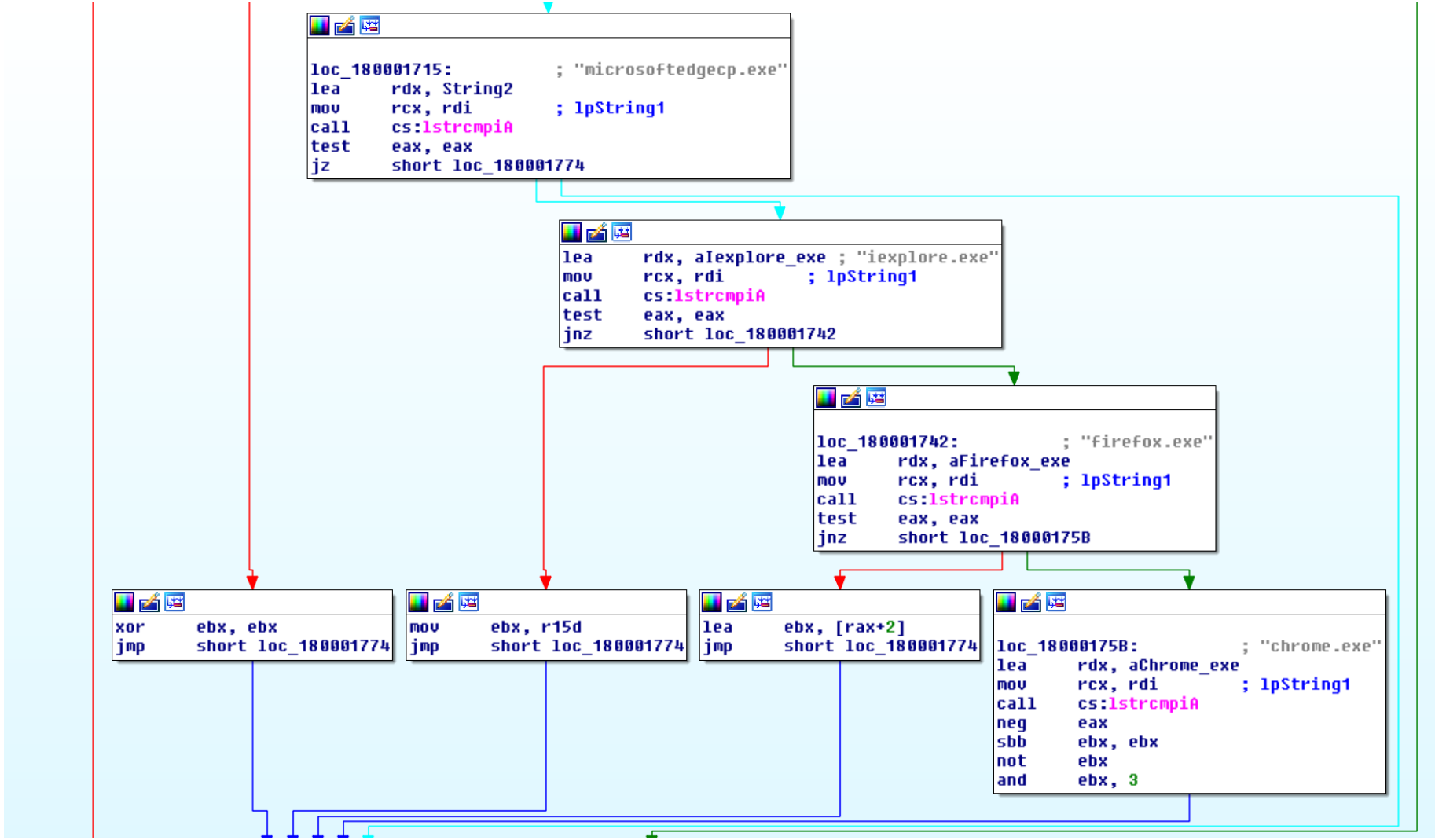


TRICKBOT MODULOK

Adatgyűjtés

- injectDll64.dll: böngészőkbe épülve bankkártya-adatok lopása
- pwgrab64.dll: böngészőkben és egyéb szoftverek által tárolt jelszavak (**putty, VNC**, stb.)
- NewBCtestnDll64.dll: BackConnect SOCKS5 proxy

TRICKBOT MODULOK



TRICKBOT MODULOK

Terjedés hálózaton belül

- shareDll64.dll: C$ és ADMIN$ megosztásokon keresztül, távoli telepítés
- tabDll64.dll: ReflectiveDLLInjection implementáció
- wormDll64.dll: lateral movement modul, többek közt EternalBlue-val felszerelve

IR KIHÍVÁSOK MOST

- Pusztán szignatúra alapú detekció nem elégséges
- Nem elég a DMZ-t védeni és monitorozni, belső forgalmat is kell
- Napi szintű kampányok új mintákkal, új verziókkal
- Memória rezidens malware komponensek
- Alternatív fallback csatornák
- Aktív támadói jelenlét: az IR tevékenység azonosítása
- Moduláris malware - külön komponensek jogosultságemeléshez, lateral movementhez, rejtőzködéshez, kód injectionhöz, credential harvestinghez, speciális környezethez (point of sale), kriptovaluta-lopáshoz, stb.
- Malware fejlesztő csapatok "összefogása" - Emotet moduláris downloader, Trickbot moduláris trójai, Ryuk célzott ransomware
- Skálázódás és hybrid C2 infrastruktúra

TANULSÁGOK

- Pénz motivált támadók sokat fejlődtek
- Malware-eknek:
  - moduláris felépítésük lett
  - fejlesztési életciklus is jelentősen rövidült,
  - igazodnak a célponthoz,
  - reagálnak a támadókra.

Egyre magasabb technológiai színvonal szükséges a támadó elávolítással foglalkozó szakemberek részéről!

KÖSZÖNÖM
A FIGYELMET!

KÉRDÉSEK?

https://www.linkedin.com/in/fehersandor/

@Wh173Hat

white hat
IT SECURITY