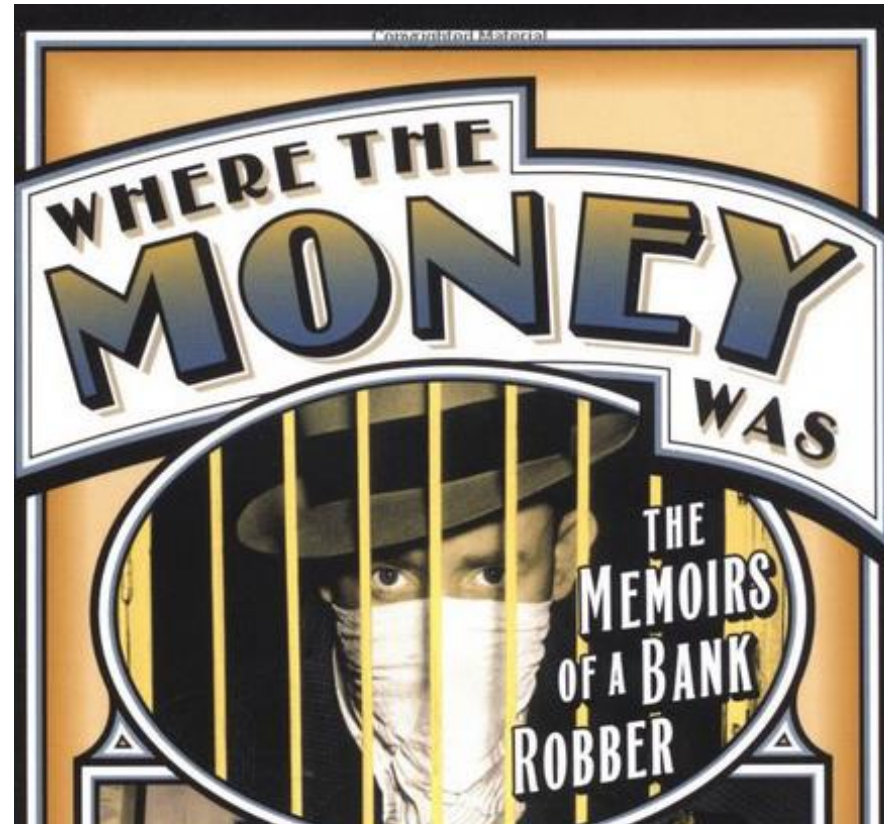




A támadók gondolkodásmódjának változása egy banki malware evolúciójának tükrében



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



11 engines detected this file

SHA-256 bd2c2cf0631d881ed382817afcce2b093f4e412ffb170a719e2762f250abfea4

File name Process Hacker

File size 1.64 MB

Last analysis 2019-04-12 06:17:39 UTC

Community score +257

11 / 68

Detection Details Relations Behavior Community 8

CAT-QuickHeal	⚠ Trojan.IGENERIC	eGambit	⚠ not-a-virus:Generic.Malware
Jiangmin	⚠ RiskTool.ProcHack.b	K7AntiVirus	⚠ Riskware (0040eff71)
K7GW	⚠ Riskware (0040eff71)	Kaspersky	⚠ not-a-virus:HEUR:RiskTool.Win32.ProcHac...
Panda	⚠ HackingTool/ProcHack	Sophos AV	⚠ Process Hacker (PUA)
Symantec	⚠ Hacktool.ProcHack!g1	TrendMicro-HouseCall	⚠ PUA.Win64.ProcHack.C
ZoneAlarm	⚠ not-a-virus:HEUR:RiskTool.Win32.ProcHac...	Acronis	✓ Clean
Ad-Aware	✓ Clean	AegisLab	✓ Clean

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



9 engines detected this file

SHA-256 87fd5b8dc5d2e598073f1abd34b8a1f1b33dadf7c35ecb0263e65240b39f2222

File name ProcessHacker_mod.exe

File size 1.64 MB

Last analysis 2019-04-12 09:41:39 UTC

9 / 70

Detection	Details	Community
CAT-QuickHeal	⚠ Trojan.IGENERIC	Jiangmin ⚠ RiskTool.ProcHack.b
K7AntiVirus	⚠ Riskware (0040eff71)	K7GW ⚠ Riskware (0040eff71)
Kaspersky	⚠ not-a-virus:HEUR:RiskTool.Win32.ProcHac...	SentinelOne ⚠ DFI - Suspicious PE
Sophos AV	⚠ Process Hacker (PUA)	Symantec ⚠ Hacktool.ProcHack!g1
ZoneAlarm	⚠ not-a-virus:HEUR:RiskTool.Win32.ProcHac...	Acronis ✓ Clean
Ad-Aware	✓ Clean	AegisLab ✓ Clean
AhnLab-V3	✓ Clean	Alibaba ✓ Clean

JELLEN



- 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

JELLEN

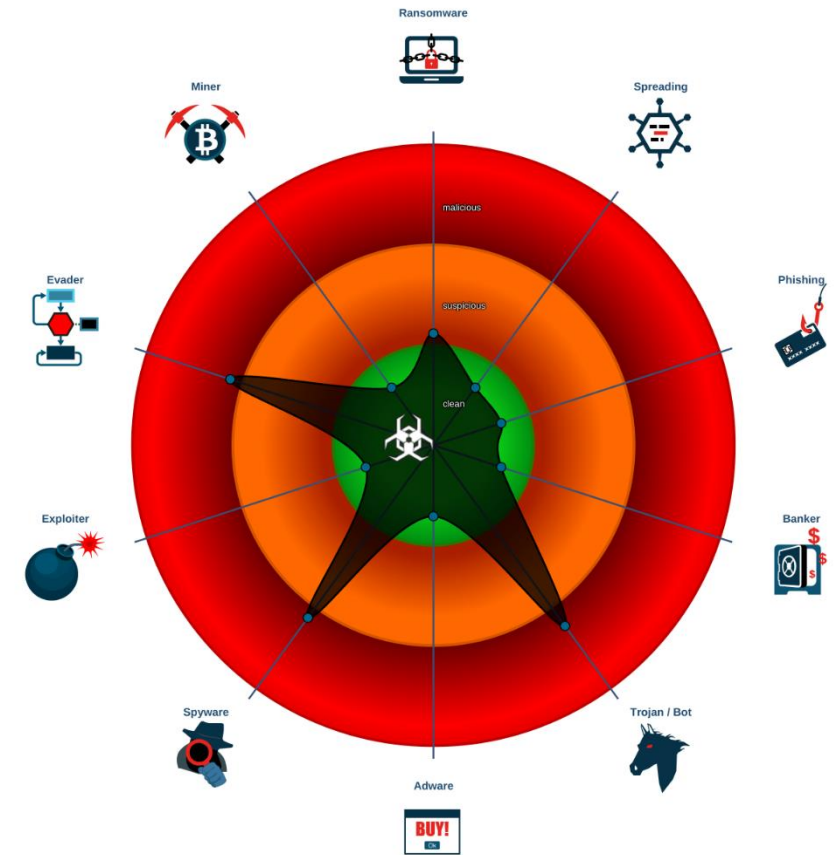
Hány weboldal / account / applikáció fér hozzá bankkártya adatokhoz?

- 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

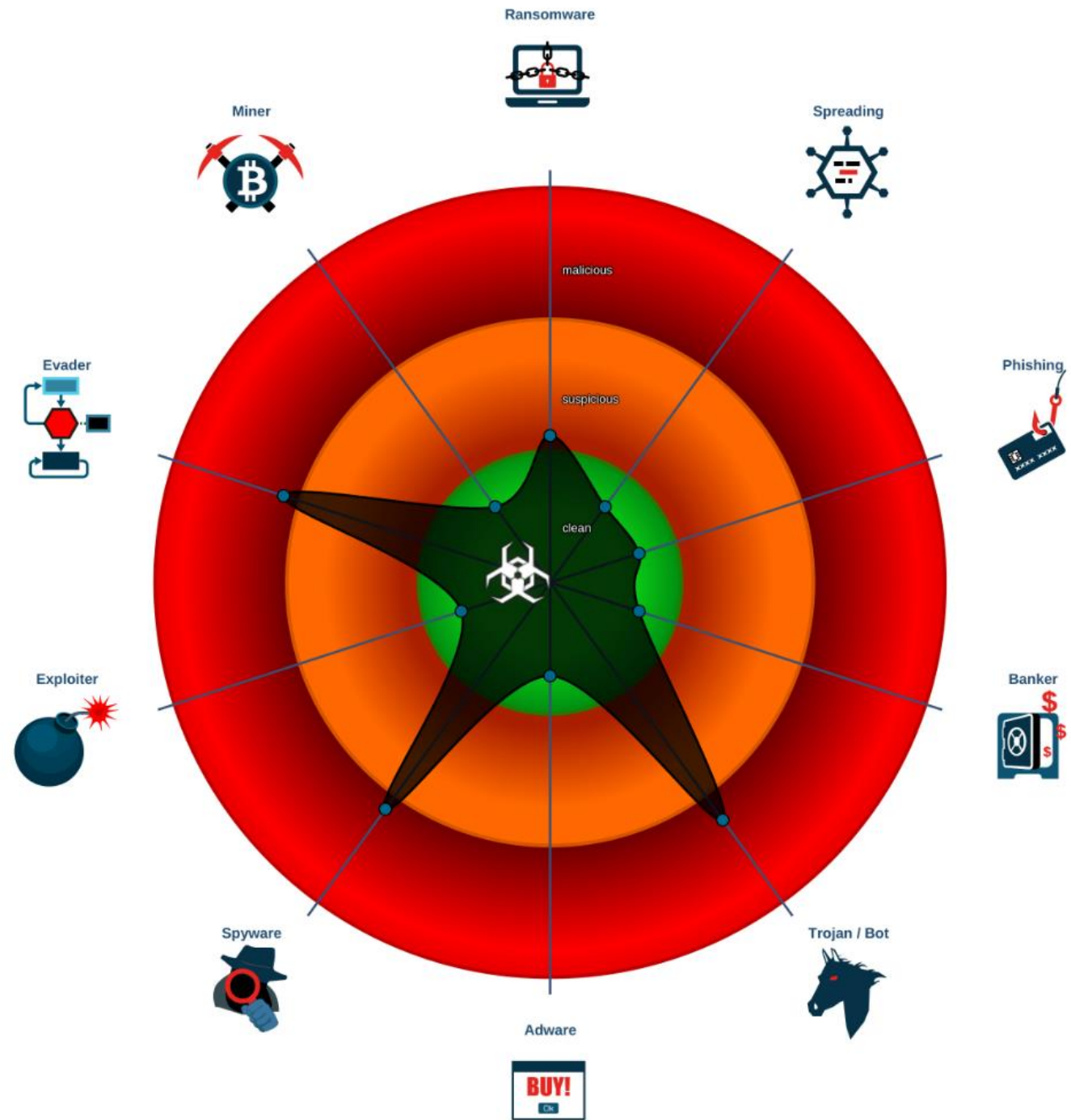


JELLEN

- 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 eloszlással 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



JELLEN



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



CFF Explorer VIII - [psfin64.dll]

File Settings ?

psfin64.dll

File: psfin64.dll

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Export Directory
- Import Directory
- Exception Directory
- Relocation Directory
- Debug Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Addr
- Quick Disassembler
- Rebuilder
- Resource Editor

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00004090	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
000040A0	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
000040B0	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
000040C0	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
000040D0	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
000040E0	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
000040F0	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
00004100	0A	00	00	00	00	00	00	43	00	4F	00	4D	00	50	00	00	C.O.M.P.
00004110	55	00	54	00	45	00	52	00	53	00	3A	00	0D	00	0A	00	U.T.E.R.S.
00004120	00	00	00	00	00	00	00	2A	00	50	00	4F	00	53	00	00	*P.O.S.
00004130	2A	00	00	00	00	00	00	50	00	4F	00	53	00	20	00	00	*.....P.O.S.
00004140	66	00	6F	00	75	00	6E	00	64	00	3A	00	20	00	25	00	f.o.u.n.d.....%
00004150	64	00	0D	00	0A	00	00	2A	00	52	00	45	00	47	00	00	d.....*R.E.G.
00004160	2A	00	00	00	00	00	00	52	00	45	00	47	00	20	00	00	*.....R.E.G.
00004170	66	00	6F	00	75	00	6E	00	64	00	3A	00	20	00	25	00	f.o.u.n.d.....%
00004180	64	00	0D	00	0A	00	00	2A	00	43	00	41	00	53	00	00	d.....*C.A.S.
00004190	48	00	2A	00	00	00	00	43	00	41	00	53	00	48	00	00	H*.....C.A.S.H.
000041A0	20	00	66	00	6F	00	75	00	6E	00	64	00	3A	00	20	00	f.o.u.n.d.....
000041B0	25	00	64	00	0D	00	0A	00	00	00	00	00	00	00	00	00	%d.....
000041C0	2A	00	4C	00	41	00	4E	00	45	00	2A	00	00	00	00	00	*I.A.N.E.*
000041D0	4C	00	41	00	4E	00	45	00	20	00	66	00	6F	00	75	00	I.A.N.E.f.o.u.
000041E0	6E	00	64	00	3A	00	20	00	25	00	64	00	0D	00	0A	00	nd.....%d.
000041F0	00	00	00	00	00	00	00	00	2A	00	53	00	54	00	4F	00	*S.T.O.
00004200	52	00	45	00	2A	00	00	00	53	00	54	00	4F	00	52	00	R.E.*.....S.T.O.R.
00004210	45	00	20	00	66	00	6F	00	75	00	6E	00	64	00	3A	00	E.f.o.u.n.d.:
00004220	20	00	25	00	64	00	0D	00	0A	00	00	00	00	00	00	00	%d.....
00004230	2A	00	52	00	45	00	54	00	41	00	49	00	4C	00	2A	00	*R.E.T.A.I.L.*
00004240	00	00	00	00	00	00	00	00	52	00	45	00	54	00	41	00	R.E.T.A.
00004250	49	00	4C	00	20	00	66	00	6F	00	75	00	6E	00	64	00	I.L.f.o.u.n.d.
00004260	3A	00	20	00	25	00	64	00	0D	00	0A	00	00	00	00	00	%d.
00004270	2A	00	42	00	4F	00	48	00	2A	00	00	00	00	00	00	00	*B.O.H.*
00004280	42	00	4F	00	48	00	20	00	66	00	6F	00	75	00	6E	00	B.O.H.f.o.un.
00004290	64	00	3A	00	20	00	25	00	64	00	0D	00	0A	00	00	00	d.....%d.
000042A0	2A	00	41	00	4C	00	4F	00	48	00	41	00	2A	00	00	00	*A.L.O.H.A.*
000042B0	41	00	4C	00	4F	00	48	00	41	00	20	00	66	00	6F	00	A.L.O.H.A.f.o.
000042C0	75	00	6E	00	64	00	3A	00	20	00	25	00	64	00	0D	00	und.....%d.
000042D0	0A	00	00	00	00	00	00	2A	00	4D	00	49	00	43	00	00	*M.I.C.
000042E0	52	00	4F	00	53	00	2A	00	00	00	00	00	00	00	00	00	R.O.S.*
000042F0	4D	00	49	00	43	00	52	00	4F	00	53	00	20	00	66	00	M.I.C.R.O.S.f.
00004300	6F	00	75	00	6E	00	64	00	3A	00	20	00	25	00	64	00	ound.....%d.
00004310	0D	00	0A	00	00	00	00	00	2A	00	54	00	45	00	52	00	*T.E.R.
00004320	4D	00	2A	00	00	00	00	00	54	00	45	00	52	00	4D	00	M*.....T.E.R.M.
00004330	20	00	66	00	6F	00	75	00	6E	00	64	00	3A	00	20	00	f.o.u.n.d.....
00004340	25	00	64	00	0D	00	0A	00	00	00	0A	00	00	00	00	00	%d.....
00004350	55	00	53	00	45	00	52	00	53	00	3A	00	0D	00	0A	00	U.S.E.R.S.
00004360	00	00	00	00	00	00	00	00	47	00	52	00	4F	00	55	00	G.R.O.U.
00004370	50	00	53	00	3A	00	0D	00	0A	00	00	00	00	00	00	00	P.S.
00004380	53	00	49	00	54	00	45	00	53	00	3A	00	0D	00	0A	00	S.I.T.E.S.
00004390	00	00	00	00	00	00	00	00	4F	00	55	00	73	00	3A	00	O.U.s.
000043A0	0D	00	0A	00	00	00	00	00	00	00	00	00	00	00	00	00	-----
000043B0	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
000043C0	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
000043D0	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
000043E0	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
000043F0	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
00004400	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
00004410	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	-----
00004420	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	2D	00	0D	00	-----

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

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 injectionhoz, credential harvestinghez, speciális környezethez (point of sale), kriptovalutalopáshoz, 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!

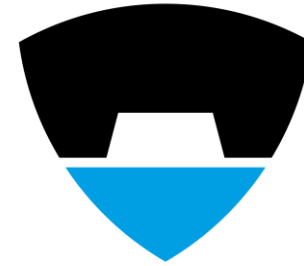
KÉRDÉSEK?



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



[@Wh173Hat](https://twitter.com/Wh173Hat)



white hat
IT SECURITY

[HTTPS://WHITEHAT.EU](https://whitehat.eu)