Nyomok a kibertérben:

Betekintés a malware-elemző rendszerünkbe.

Gulyás Dalma nb. hadnagy
Nemzeti Kiberbiztonsági Intézet

Biztonsági Elemző Főosztály

- Saját fejlesztésű Sandbox szolgáltatás

„Egy fertőző csatolmányt valaki megnyit!”
Innentől a kérdés: percek vagy napok múlva derül ki, hogy baj van?

Igaz történet alapján...

MAS Sandbox rendszerünkbe több szervezettől feltöltésre került egy [illegible] megegyező állomány.

Tömörített

BIZTONSÁGI ELEMZŐ SZAKTERÜLET

Summary

VERDICT: MALICIOUS

Uploaded file

Malware	Malware.Parent.RAR
Application Type	Windows Explorer
File Type	rar
ID	18792
Distinguisher UUID	12234347-4f4f-4fdf-b7f8-eccf7b1051fa
MD5	e6591ced88e32e1a4c6e5adfa1226fcc
SHA-1	7a93967c181a332f7449af89e001af72921a2679
SHA-256	8c94f47cc0f78e505a7c4f174eea1e95e230b3987f38d1e2ec5c9907a1c25068
URL	e6591ced88e32e1a4c6e5adfa1226fcc

Malware	FEC_Trojan_NSIS_Generic_6
Application Type	Windows Explorer
File Type	exe
ID	18793
Distinguisher UUID	dc02cb1f-b522-45ee-81d8-ad2759c0848d
MD5	c7bfd6636782b8cf53acea97c748de84
SHA-1	448112d35b53ca00cfd067e750a9cb49185cafc2
SHA-256	456c5507b1e3368b89a9d34492a836690644060c87a853505bf997554f93dab7
URL	139 FACTURA AGOSTO 2024.exe

Tekintettel arra, hogy több szervezet is megkapta az állományt egy e-mail csatolmányaként, elvégeztük annak manuális elemzését is.

Megállapítottuk, hogy az valóban egy TRÓJAI!

Kezdeti vektora lehet káros tevékenységeknek:

- Adatlopás
- Zsarolóvírusos támadás előkészítése
- Teljes hozzáférés szerzése számítógéphez

Milyen előnye volt a feltöltéseknek:

- Rövid időn belül elkészült egy teljes riport
- Mire Nemzeti CSIRT-en keresztül beérkeztek az első jelzések, addigra elvégeztük a feltöltött állomány manuális elemzését is
- Figyelemfelhívó tájékoztatás
- Indikátorok központi tiltása

Számos kezdődő kampányt sikerült idő előtt feltárnunk a Sandbox elindulása óta.

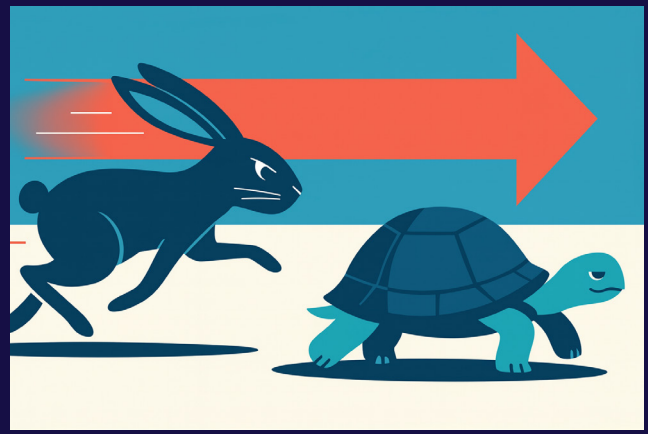
- 2024. július 1. óta ~ 2000 fájl került elemzésre a rendszerben.
- Feltöltött elemzések ~ 20% káros vagy kockázatos eredménnyel zárult.
- Az elemzett állományok ~ 25% több szervezetnél is előfordult kampányszerűen.

Miért ajánlott a rendszer használata?

- Automata kártékony állomány (malware) elemző sandbox szolgáltatás
- Statikus elemzésnél nem kerül lefuttatásra, meta adatok vizsgálata történik
- Dinamikus sandbox környezet: elszigetelt környezetben fut
- Virtuális környezetek kezelése: egyszerre több

Miért ajánlott a rendszer használata?

- A kártevők fejlődnek, egyre trükkösebbek → kézi elemzés sokszor lassú.
- **Időablak:** az incidens bekövetkezése és észlelése közötti idő kritikus.
- **Következmény:** minél később avatkozunk be, annál nagyobb a kár.
- Proaktív és preventív beavatkozás.



Szolgáltatás értékei

- Biztonság és bizalom
- Ingyenes használat
- Gyors reakció idő

Konklúzió

- Sandbox lényege a prevenció
- Tudatosság: nem jellemző üzenet, rövid határidő, hivatkozás elrejtés

Köszönöm a figyelmet!

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet

Biztonsági Elemző Főosztály

sandbox@nki.gov.hu

https://sandbox.nki.gov.hu

Gulyás Dalma nb. hadnagy