AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Avalanche-andromeda malware

Autoriteti Kombëtar për Certifikim Eletronik dhe Sigurinë Kibernetike
Rruga. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Shqipëri 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Indeksi

Përmbledhje.....3

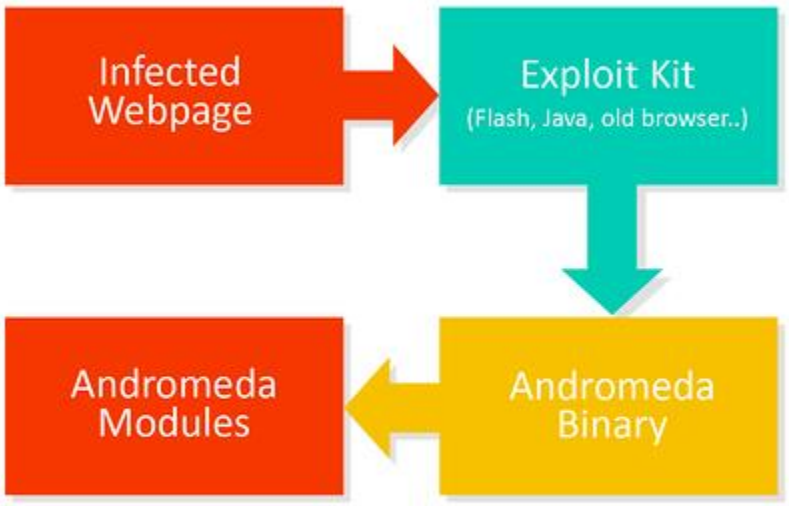
Ju rikujtojmë disa rekomandime:.....7

Referenca:.....8

Përmbledhje

Andromeda është një trojan modular i cili u pa për herë të parë në 2011. Sjellja e këtij Malware është aftësia e tij për të kontrolluar nëse po ekzekutohet apo korrigjohet në një mjedis virtual duke përdorur teknikat e makinave anti-virtuale, funksionalitetet e të cilit mund të modifikohen përmes linqeve, për shembull linqeve për keylogger, rootkit, teamviewer, spreader etj. Trojani shkarkon malware të tjerë nga serverat e tij të kontrollit, shpesh në mënyrë që të vjedhë informacionin nga kompjuterët e infektuar. Vendet më të prekura janë India (24%), Vietnami (12%) dhe Irani (7%).

Kjo familje malware u referohet varianteve që përbëhen nga backdoors që janë të lidhura me botnet-in Andromeda. Malware kryesisht synon sistemet operative windows për të krijuar një rrjet të pajisjeve të infektuar që më pas bëhen pjesë e Andromeda Botnet. Infektimi realizohet nga email me përmbajtje “phishing”, linqe të dëmshme përmes mesazheve të mediave sociale.



Malware-i është i aftë të kryejë funksionet e mëposhtme:

- I aftë për të krijuar "botnets" që mund të përdoren si nismë për sulme të mëtejshme duke shpërndarë malware të tjerë si "Ransomware" (Petya, Cerber, Troldesh), "DDoS" (Fareit, Kasidet), "Spam bot" (Cutwail & Lethic), "Backdoor" etj.
- Eshtë përdorur si pjesë e "Botnet Avalanche".
- Punon si një "backdoor" që mund të marrë komanda nga serveri i tij i kontrollit për shkarkimin dhe ekzekutimin e skedarëve, ose fshirjen nga sistemi.
- Vjedh informacione sensitive, të tilla si informacioni i sistemit operativ, adresa IP lokale, "Root volume serial number".

Ky Trojan lëshon kopjet e mëposhtme të veta në sistemin e prekur:

- %All Users Profile%\Local Settings\Temp\{random}.{random extension}
- %All Users Profile%\svchost.exe
- %All Users Profile%\{random}.exe
- %Program Data%\svchost.exe
- %User Temp%\{random}.exe

(Shënim: *%All Users Profile%* is the All Users or Common profile folder, which is C:\Documents and Settings\All Users in Windows 2000, XP, and Server 2003, and C:\ProgramData in Windows Vista and 7.. *%User Temp%* is the current user's Temp folder, which is usually C:\Documents and Settings\{user name}\Local Settings\Temp on Windows 2000, XP, and Server 2003, or C:\Users\{user name}\AppData\Local\Temp on Windows Vista and 7.)

Modifikime të Tjera të Sistemit

Ky Trojan gjithashtu krijon regjistrimin e mëposhtëm të regjistrit si pjesë e instalimit:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlS
et\
Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\Authorized
Applications\
List
%System%\svchost.exe =
"%System%\svchost.exe:*:Generic Host
Process"
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlS
et\
Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\Authorized
Applications\
List
{malware path and file name} = "{malware
path and file name}:*:Enabled:{malware
file name}"
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlS
et\
Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\Authorized
Applications\
List
%System%\msiexec.exe =
"%System%\msiexec.exe:*:Generic Host
Process"
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run
SunJavaUpdateSched = "%All Users
Profile%\svchost.exe"
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\policies\
Explorer\Run
540 = "%All Users Profile%\Local
Settings\Temp\{random}.{random
extension}"
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlS
et\
Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\Authorized
Applications\
List
{malware path and file name} = "{malware
path and file name}:*:Enabled:Marko"
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\policies\
Explorer\Run
540 = "%All Users Profile%\{random}.exe"
```

KUJDES !!!

Ju rikujtojmë disa rekomandime:

- Fshini ndryshimet e sistemit të bëra nga malware si p.sh. skedarët e krijuar / hyrjet / shërbimet e regjistrit etj.
- Monitoroni trafikun e gjeneruar nga makineritë e klientit në domain dhe adresën IP të përmendur në seksionin e instalimit.
- Shmangni shkarkimin e software-ve pirate.
- Mbroni veten nga sulmet e “Social Engineering”.
- Skanoni sistemin e infektuar me versione të përditësuara të zgjidhjes Antivirus
- Çaktivizo politikat e Autorun dhe Autoplay.
- Përdorni përdorues të privilegjuar të kufizuar (Principle of Least Privilege) në kompjuter ose lejoni hyrjen administrative në sistemet me llogari të veçanta administrative për administratorët
- Mos vizitoni faqet e internetit të pasigurta.
- Mos shkarkoni ose hapni linqe në emaile të marra nga burime jo të besueshme ose të marra papritur nga përdoruesit e besuar.
- Zbatoni një politikë të fortë fjalëkalimi dhe zbatoni ndryshime të rregullta të fjalëkalimit.
- Aktivizoni një firewall personal në vendin e punës. Çaktivizoni shërbimet e panevojshme në vendin e punës dhe serverat e agjencisë. Gjithmonë ndryshoni kredencialet e parazgjedhura të hyrjes para vendosjes në prodhim

Referenca:

https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation

https://www.cyberswachhtakendra.gov.in/alerts/andromeda.html

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/andromeda

https://blog.avast.com/andromeda-under-the-microscope

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/andromeda

https://blog.malwarebytes.com/detections/backdoor-andromeda/