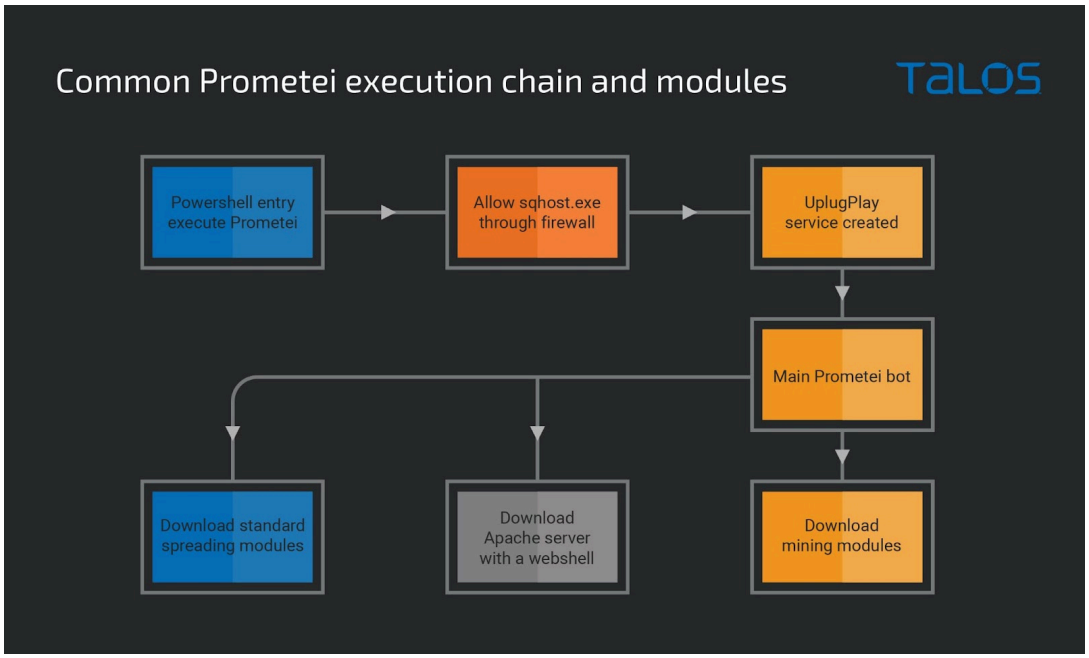
Raport consolidat eveniment cibernetic

PrometeiBotnet

Prometei Botnet este un malware care poate controla de la distanță mașinile infectate. Are capabilitățile de a se răspândi colateral în rețele, de a fura credențialele, de a executa comenzi arbitrare și de a descărca și executa componente rău intenționate. De asemenea, poate efectua minări de criptomonede și are capabilități de auto-actualizare.

PrometeiBotnet este un program malware complex, avansat și sofisticat, cu multe funcții ascunse.



Informații sumare

TIP	**Botnet**
Instrumente pentru analiză	• **Pentru scanarea rețelei** – Wireshark, TCPDUMP, Angry IP Scanner • **Pentru scanarea de viruși și malware** – Software antivirus existente • **Anliză și detectare** -NMAP, Lordpe, Sysmon , Procces Hacker
Etapele de instalare	1. Atacul începe cu încercarea de compromitere a protocolului Windows Server Message Block (SMB) prin vulnerabilități SMB, inclusiv Eternal Blue. 2. Botnet-ul are peste 15 module executabile care sunt descărcate și controlate de modulul central. Modulul central discută cu serverul de comandă și control (C2) prin HTTP. Transferă datele criptate folosind criptarea RC4, în timp ce modulul partajează cheia cu C2 folosind criptarea asimetrică. 3. Pe lângă extindere în rețea, Prometei încearcă și să recolteze parolele de administrator. Parolele găsite sunt trimise la C2 și apoi reutilizate de alte module care încearcă să confirme valabilitatea parolelor pe diferite sisteme folosind protocoale SMB și RDP. 4. Rețeaua botnet Prometei este grupată în două ramuri principale: o ramură C++ dedicată blocării operațiunilor de minerit cu recompense și una, bazată pe .NET, care se concentrează pe furtul de parole, abuzul de SMB.
IOC **Fișiere**	• **C:\windows\zsvc.exe** - este încărcat de pe serverile C2 • **C:\windows\Sqhost.exe** - este modulul bot principal. • **RdpClip.exe** -cheie componenta a malware care este utilizată pentru interacțiunea altor componente malware • **Miwalk.exe** – versiunea personalizată a Mimikatz folosită pentru recoltarea credentialelor. • **ExchDefender.exe** – crează un serviciu “Microsoft Exchange Defender” care este setat pentru a executa binarul din C:\Windows. • **SearchIndexer.exe** – este o sursă deschisă a mineritului, Monero. Vezi dacă este instalată illegal. • **Netwalker.7z** – Este o aplicație arhivă descărcată din C2. • **Nethelper2.exe and Nethelper4.exe** – crează conexiuni cu serverul SQL în rețea și încearcă să le infecteze cu modulul principal • **Windrlver.exe** – este o aplicație OpenSSH și SSLib pe care atatcatorii au creat-o astfel încât să se poată răspândi în rețea folosind SSH
	IPV4 • 23.148.145[.]237 • 69.84.240[.]57 • 103.40.123[.]34 • 103.184.128[.]180 • 103.184.128[.]244 • 194.195.213[.]62 • 211.232.48[.]65 • 103.65.236[.]53

IOC

- 177.73.237[.]55
- 221.120.144[.]101

Domain

- xinchaodbcdbh[.]org
- xinchaodbcdbh[.]com
- xinchaoabcdcf[.]org
- xinchaocecclk[.]org
- xinchaocecclk[.]net
- p1.feefreepool[.]net
- p2.feefreepool[.]net
- p3.feefreepool[.]net
- gb7ni5rgeexdcncj[.]onion

URL

- http://103.126.6.233:180/AppServ180.zip
- http://103.184.128.244/update.7z
- http://103.40.123.34/7z32.dll
- http://103.40.123.34/7z32.exe
- http://103.40.123.34/bklocal2.php
- http://103.40.123.34/bklocal4.php
- http://103.40.123.34/desktop.txt
- http://103.40.123.34/dwn.php?d=7z32.dll
- http://103.40.123.34/dwn.php?d=7z32.exe
- http://103.40.123.34/dwn.php?d=rdpcIip.exe
- http://103.40.123.34/k.php
- http://103.40.123.34/srch.7z
- http://103.40.123.34/std2.7z
- http://103.40.123.34/update.7z
- http://194.195.213.62:180/srch.7z
- http://211.232.48.65:180/update.7z
- http://23.148.145.237:180/update.7z
- http://69.84.240.57:180/AppServ180.zip
- http://mkhkjxgchtfgu7uhofxzgoawntfzrkdccymveektqgpxrpjb72oq.b32.i2p/cgi-bin/prometei.cgi
- http://mkhkjxgchtfgu7uhofxzgoawntfzrkdccymveektqgpxrpjb72oq.zero/cgi-bin/prometei.cgi
- http://p2.feefreepool.net/cgi-bin/prometei.cgi
- https://gb7ni5rgeexdcncj.onion/cgi-bin/prometei.cgi

1. Izolarea Sistemelor Afectate:

- Deconectați imediat sistemele infectate de la rețea pentru a preveni răspândirea malware-ului și pentru a întrerupe comunicarea cu serverele C2.
- Utilizați un antivirus pentru a elimina componentele rău intenționate

2. **Eliminarea Manuală a Malware-ului:**

- Identificați și ștergeți fișierele malițioase identificate în locații neobișnuite (de exemplu, %C%:\windows\Sqhost.exe).
- Verificați și curățați cheile de registru suspecte, cum ar fi **RdpClip.exe**

Eliminare PrometeiBotnet

3. Restaurarea Sistemelor:

- Reinstalați sistemul de operare pe dispozitivele afectate dacă nu se poate asigura eliminarea completă a malware-ului.
- Restaurați datele din backup-uri sigure, asigurându-vă că acestea nu sunt infectate.

4. Actualizarea și Patch-ul Sistemelor:

- Asigurați-vă că toate sistemele și aplicațiile sunt actualizate cu cele mai recente patch-uri de securitate pentru a preveni exploatarea vulnerabilităților cunoscute.
- Implementați măsuri de securitate suplimentare, cum ar fi controlul aplicațiilor și restricționarea macro-urilor în documentele Microsoft Office.

5. Educație și Conștientizare:

- Instruirea utilizatorilor în recunoașterea e-mailurilor de phishing și a altor tactici de inginerie socială.
- Promovarea practicilor de securitate, cum ar fi verificarea sursei e-mailurilor și evitarea deschiderii atașamentelor necunoscute

Resurse externe

	https://blog.talosintelligence.com/prometei-botnet-improves/