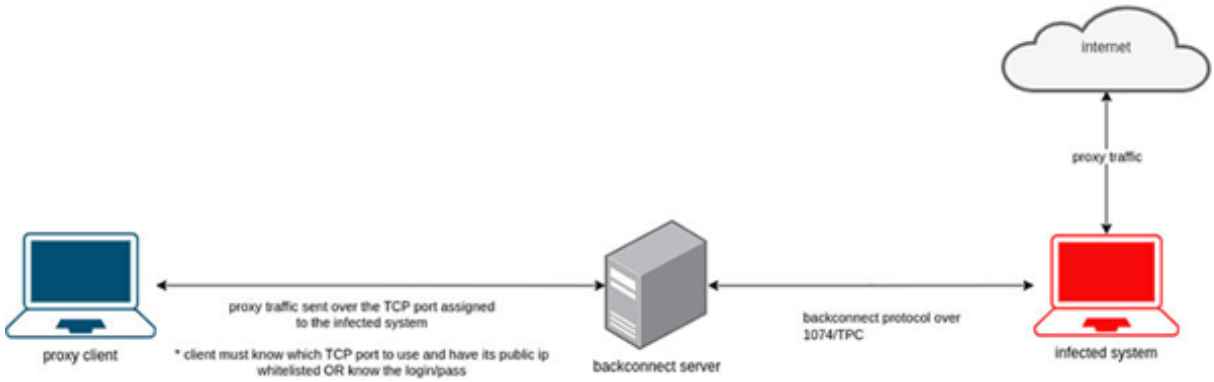
Raport consolidat eveniment cibernetic

Socks5Systemz.Botnet

Socks5Systemz.Botnet este un malware ce o dată instalat pe dispozitive preia controlul asupra lor, reconfigurându-le ca instrumente **proxy server** pentru redirecționarea traficului pe internet și facilitând atât activități rău intenționate, cât și activități anonime.

Odată instalat pe dispozitiv acesta creează două tipuri de conexiune. Primul tip de conexiune este conexiunea **HTTP/80**. Această conexiune este utilizată în principal pentru comunicarea dintre bot și server. Al doilea tip de conexiune este fluxurile de conexiune client **TCP/1074** și comenzile serverului proxy. Această conexiune este responsabilă pentru gestionarea fluxurilor de clienți și executarea comenzilor serverului proxy.



Modul de operare Socks5Systemz.Botnet

Informații suplimentare

TIP	***Botnet***
Instrumente pentru analiză	1. **Pentru scanarea rețelei** – Wireshark, TCPDUMP, Angry IP Scanner 2. **Pentru scanarea de viruși și malware** – Software antivirus existente 3. **Analiză și detectare procese** - Lordpe, Sysmon , Procces Hacker

Metode de infectare	• Socks5Systemz este livrat în mod obișnuit prin încărcătoare, cum ar fi **PrivateLoader și CrackedCantil**. Acestea încarcă malware-ul pe sistemele compromise și îi permit să înceapă procesul de infectare. • Unele atacuri care implică Socks5Systemz sunt, de asemenea, efectuate prin **e-mailuri de phishing**. • La fel infractorii pot folosi diverse tactici de inginerie socială pentru a păcăli victimele să descarce și să execute malware-ul pe dispozitivele lor.
Mod de operare	• Odată instalate, încărcătoarele aruncă și execută un fișier numit "**previewer.exe**", care în cele din urmă determină executarea botnet-ului. • Botnetul, un DLL pe 300 KB pe 32 de biți, utilizează un sistem **DGA** pentru a se conecta cu serverul său C2 și pentru a primi comenzi pentru mașinile de compromis. • Odată conectat la infrastructura **threat atters**, dispozitivul infectat este utilizat ca server proxy și vândut altor actori de amenințare.
IOC	**IP Address** • 185.141.63[.]172 • 193.242.211[.]141 • 109.230.199[.]181 • 109.236.88[.]134 • 217.23.5[.]14 • 88.80.148[.]8 • 88.80.148[.]219 • 185.141.63[.]4 • 185.141.63[.]2 • 195.154.188[.]211 • 91.92.111[.]132 • 91.121.30[.]185 **URL** • datasheet[.]fun • bddns[.]cc • send-monitoring[.]bit

Recomandări generice	1. **Monitorizați traficul de rețea**: Implementați sisteme de detectare a intruziunilor și monitorizați continuu traficul de rețea pentru conexiuni multiple și neobișnuite la Rare Endpoint, New External TCP Port. 2. **Detectarea Anomaliei Comportamentale:** Implementați sisteme avansate de detectare a anomaliilor comportamentale pentru a identifica abaterile de la comportamentul normal al utilizatorului și al sistemului. Aceste sisteme ar trebui să fie capabile să marcheze activități cum ar fi executarea frecventă și neobișnuită a comenzilor, Solicitări DNS Multiple. 3. **Monitorizarea și filtrarea porturilor:** Implementați mecanisme de monitorizare și filtrare a porturilor, care vizează în mod specific portul 80/1074, pentru a detecta și a bloca încercările de comunicare neautorizate cu serverele de backconnect. 4. **Scanarea și curățarea dispozitivelor:** Utilizați un antivirus actualizat și soluții anti-malware pentru a scana toate dispozitivele în căutarea amenințărilor. Eliminați sau izolați fișierele și programele malware identificate. 5. **Educați-vă utilizatorii:** Este important să se asigure conștientizarea și educarea utilizatorilor. Pentru aceasta ei trebuie să conștientize riscurile și să nu acceseze link-uti sau fișiere pe care le primesc prin Internet, fără a se asigura că sunt de încredere. Să evite descărcarea software-ului piratat și rularea executabilelor din surse neîncrezătoare. 6. **Reevaluarea securității rețelei:** Evaluați în mod regulat securitatea rețelei și revizuiți politicile de securitate pentru a vă asigura protecția continuă împotriva amenințărilor.

Resurse externe

	https://any.run/malware-trends/socks5systemz