Raport consolidat eveniment cibernetic

Phorpiex Botnet

Phorpiex (alias Trik) este un malware modular cunoscut pentru capacitatea sa de a menține o rețea botnet extinsă. Spre deosebire de alte rețele bot, Phorpiex nu se concentrează asupra atacurilor DDoS, în schimb, a fost implicat în numeroase campanii de e-mail spaming la scară largă și în distribuția altor programe malware, cum ar fi **LockBit.**
Acesta rămâne persistent în sistem prin crearea de fișiere și modificări ale registrului. Botnet-ul i comunică pe portul **40500/5555.**

Termeni și definiții

Malware modular este o amenințare avansată care atacă un sistem în câteva etape. În loc să explodeze front door, malware-ul modular adoptă o abordare mai subtilă, instalează mai întâi doa componentele esențiale care cercetează securitatea sistemului și a rețelei. După identificarea cu succes a mediului local hackerii pot să ajusteze mai ușor același malware pentru diferite ținte prin simpla adăugare sau eliminare a componentelor, chiar și după ce infectatrea sistemului a avut loc.

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	• **Infected USB drives** - La conectarea cu un dispozitv compromis (de ex USB care deja conține componenta malware). • **Phishing emails** - Acivarea link-ului sau a fișierului infectat dintr-un mesaj de tim spam-phishing. • **Dropped by malware** - Botnet-ul pate fi adăugat de către alte programe malware aflate deja pe dispozitiv. • **Downloads from sites** - Descărcări de pe site-uri care pretind că livrează software legitim • **Incorporates worm modules** - Phorpiex se poate auto-răspândi

Principalele funcționalități	• **Malware Delivery Botnet:** Phorpiex are capacitatea de a furniza programe malware suplimentare odată ce botnetul sa instalat cu success pe dispozitiv. Botnet-ul poate instala o serie de malware ca: Ransomware, Cryptomining, Spambots, Infostealers. • **Mailing Botnet**: Cealaltă utilizare principală a rețelei bot Phorpiex este ca un mail. Se știe că Phorpiex trimite o varietate de e-mailuri spam, inclusiv: Extortion and sextortion, Malware delivery, Phishing. • **Cryptocurrency mining malware:** Phorpiex folosește un miner XMRIG pentru a monetiza gazdele cu Monero. În plus față de mineritul Monero, el se încarcă și în portofelele Bitcoin. La fel are mineri suplimentari de Etherium, care caută resurse ale dispozitivului pe care poate să le folosească pentru minerit.
• **IOC**	**IP Address** • 154.65.129.46 • 200.93.73.250 • 213.230.69.229 • 46.100.181.186 • 217.12.85.22 • 151.239.29.44 • 63.251.126.10 • 72.5.161.12 • 72.26.218.86 **SHA256** • 7ba150c8808edf187a1ccf8d0532d0732fff2bbe28f76d6e2f02f8196669dd06 • 0b4996c03b059d1a10349f715b6b21ad9926912faae834581f0c96b24ff1b33f • 9f3f80167c5d39efb9e81507efec6d9bdc5e31323f9d6d89630374c7fe490f33 • ef1563a962d2d86ceb1dd09056f87fcab4c32e3ca6481c51950d3b6db49d1087 • 5bf79a111467a85abe57f1f3e92f2279b277cccae53ed28c584267717ba372f8 **MD5** • be9388b42333b3d4e163b0ace699897b • 1382c0a4a9e0a9a2c942458652a4a0e4 • 5381689d4c9a0ce9d0f67dd8485188d2 • 55bb483e2022b3ff766a80262c1078d5 • 1318fbc69b729539376cb6c9ac3cee4c • 839e3c02d9070878a7b230dc25e0ec50 • e2e3268f813a0c5128ff8347cbaa58c8 • 8d8e6c7952a9dc7c0c73911c4dbc5518

Detectare PhorpiexBotnet	1. Monitorizați activitățile rețelei în căutarea unor conexiuni externe neobișnuite, în special către servere C&C utilizate de botnet. 2. Verifică lista proceselor și porturile deschise pentru procese/porturi suspecte ca **40500/5555** utilizate de PhorpiexBotnet pentru C&C. 3. Identificați prezența DLL-uri: **sbiedll.dll, sbiedllx.dll, dir_watch.dll, wpespy.dll, wine_get_unix_file_name**. 4. Caută un model al unui nume executabil al procesului de sistem care nu este legitim și rulează dintr-un dosar care este creat printr-un algoritm aleatoriu 13-15 numere lungi. 5. Efectuează o analiză avansată a memoriei sistemelor suspecte pentru a depista cod injectat sau alte semne de infecție activă.
Eliminarea PhorpiexBotnet	**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 DriveMgr.exeI, WINSYSDRV.exe). • Verificați și curățați cheile de registru suspecte(de ex: winsvcs.exe, lsass.exe). **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. • Implementați măsuri de securitate suplimentare, cum ar fi controlul aplicațiilor. **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, evitarea deschiderii atașamentelor necunoscute și instalarea soft-urilor numai din suse sigure. • Conștientizarea de a se asigura că dispozitivele portabile sunt sigure înainte de a fi folosite.