Raport consolidat eveniment cibernetic

Torpig.Mebroot.Botnet

Torpig.Mebroot.Botnet (alias **Anserin** sau **Sinowa**l) este un tip de botnet răspândit în scopul colectării de date personale și corporative sensibile cum ar fi contul bancar și informațiile despre cardul de credit.

Acesta vizează computerele care utilizează Microsoft Windows, recrutând o rețea de zombi pentru botnet. Torpig.Mebroot.Botnet ocolește software-ul antivirus prin utilizarea tehnologiei **rootkit** și scanează sistemul infectat pentru acreditări, conturi și parole, precum și potențial permițând atacatorilor acces complet la computer. De asemenea, se presupune că este capabil să modifice datele de pe computer și poate efectua atacuri **man-in-the-browser**.

Informații suplimentare

TIP	***Botnet***
Descriere tehnică	**Torpig.Mebroot.Botne**t folosește tehnici avansate pentru a infecta și persista pe sistem, incluzând: - Modificări la nivel de **Master Boot Record (MBR).** - Canale de comunicație criptate cu serverele C2 (Command & Control). - Porturi frecvent utilizate pentru comunicații: - **80 (HTTP)**: Pentru conexiuni web standard. - **443 (HTTPS):** Pentru comunicații criptate. - **8080, 8443:** Alternative pentru HTTP/HTTPS. - Porturi randomizate: Determinate din serverele DNS
Detectarea pe dispozitive individuale	**1. Identificarea proceselor suspecte:** - Listează procesele care deschid conexiuni externe: netstat -bano | findstr ":80" - Verifică procesele ascunse folosind Sysinternals Process Explorer. **2. Scanarea și analiza registrului Windows:** - Chei suspecte care pot fi asociate cu Torpig: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run **3. Verificarea fișierelor infectate:** - Scanează fișierele de sistem: sfc /scannow

Detectarea în rețea locală	**Captură și analiză de traffic local** 1. Instrumente recomandate: - Wireshark: Pentru analiza pachetelor. 2. Pași de analiză: - Configurează un port mirroring pe switch pentru a intercepta traficul din segmentul rețelei. - Utilizează Wireshark pentru a căuta traficul către domenii necunoscute sau IP-uri suspecte. - Filtru în Wireshark pentru Torpig: http.request or tcp.port == 80 or tcp.port == 443 - Analizează cererile DNS pentru domenii generate automat (DGA): dns.qry.name matches "(.*)\.(com|net|ru)" **Logare și corelare** 1. Inspectează logurile de rețea WireShark -Aplică un filtru pentru traficul de interes: ip.dst - Caută cereri repetate către IP-uri neobișnuite. 2. Monitorizare DNS WireShark: - Aplică următorul filtru pentru a afișa doar cererile DNS: dns - Acest filtru afișează toate pachetele DNS, incluzând cererile și răspunsurile. -Dacă vrei să filtrezi doar cererile DNS dns.flags.response == 0 - Caută nume de domenii generate aleatoriu (DGA): dns.qry.name matches "^[a-z0-9]{10,}\.(com|net|ru)$"
Eliminarea în medii avansate	**1. Utilizează un mediu live pentru curățare:** - Boot de pe un mediu USB sau CD cu instrumente de curățare (Ex. Malware Bytes - Rulează comenzi pentru repararea MBR: bootrec /fixmbr bootrec /fixboot **2. Dezinstalează și curăță rootkit-uri:** - Folosește GMER sau Malwarebytes Anti-Rootkit pentru detectarea și eliminarea rootkit-urilor. **3. Patch-uri și actualizări:** - Asigură-te că toate actualizările sistemului de operare sunt aplicate pentru a preveni reinfectarea.

Măsuri preventive avansate	**1. Segmentarea rețelei:** - Separă dispozitivele critice în VLAN-uri pentru a limita răspândirea botnet-ului. **2. Hardening pentru stații și servere:** - Dezactivează porturile neutilizate. - Restricționează accesul administrativ la stațiile de lucru. **3. Monitorizare activități anormale** -Configurează alarme pentru detectarea traficului neobișnuit, accesului la porturi sensibile sau autentificărilor eșuate frecvente.

Resurse externe

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