Raport consolidat eveniment cibernetic

AyaBot.Botnet

AyaBot (cunoscut și sub numele **Mowfote**) este un troian care infectează mașinile Windows. Poate descărca/instala programe malware suplimentare. AyaBot comunică cu serverul prin cererea și răspunsul HTTP codificat **Base64**

Informații suplimentare

TIP	***Botnet***
Instrumente pentru analiză	Pentru scanarea rețelei – Wireshark, TCPDUMP, Angry IP Scanner Pentru scanarea de viruși și malware – Software antivirus existente Analiză și detectare procese- Lordpe, Sysmon , Procces Hacker
Registry key	**HKEY_CURRENT_USER\SOFTWARE\RegData\Data** HKEY_CURRENT_USER\Software\RegData\Data projectname = "AyaBot" HKEY_CURRENT_USER\Software\RegData\Data host = "http://{BLOCKED}amarketing.ru/content/blocks/classes/s.php" HKEY_CURRENT_USER\Software\RegData\Data referer = "bbd165072cf" HKEY_CURRENT_USER\Software\RegData\ Data id = "0" HKEY_CURRENT_USER\Software\RegData\Data timeresp = "1200000" HKEY_CURRENT_USER\Software\RegData\Data avstat = "1" HKEY_CURRENT_USER\Software\RegData\Data wormstat = "0" HKEY_CURRENT_USER\Software\RegData\ Data id = "27435"
IOC	**URL** reklamamarketing.ru/content/blocks/classes/s.php **SHA1:** 4b7ec4ee411719d8c4b1681c603042d89bd8e4e0 3fef790a16d59a55011ef4850458ca02a181370f

Detectare	• Folosiți soluții de securitate actualizate pentru a efectua scanări complete ale sistemelor. Asigurați-vă că definițiile antivirus sunt la zi. • Scanează cheile registrele pentru modificările survenite • Căutați și ștergeți aceste componente: **%User Profile%\Application Data\new.exe, %User Profile%\Application Data\regdrv.exe, %User Temp%\regdrv.exe**
Recomandări generice	• **Izolarea dispozitivului compromis** - Identificați dispozitivul sau sistemele suspecte care ar putea face parte din botnet și izolați-le de rețeaua principală. Izolarea poate fi efectuată prin: deconectarea fizică a dispozitivelor sau restricționarea accesului acestora la rețea. • **Întreruperea comunicării cu serverul de comandă și control (C&C)** - Blocați traficul de ieșire către adresele IP cunoscute asociate cu serverele de comandă și control ale botnet-ului, le găsiți în descrierea din Anexă. Pentru aceasta utilizați firewall-uri sau soluții de filtrare a traficului. • **Actualizarea software-ului și a sistemelor (patch &update)** - Asigurați-vă că toate dispozitivele și sistemele din rețea sunt actualizate la cele mai recente versiuni, inclusiv sistemele de operare, aplicațiile și software-ul de securitate. Acest lucru ajută la remedierea vulnerabilităților cunoscute și la prevenirea reinfectării. • **Scanarea și curățarea dispozitivelor compromise** - Utilizați un antivirus actualizat și soluții anti-malware pentru a scana toate dispozitivele compromise în căutarea amenințărilor. Eliminați sau izolați fișierele și programele malware identificate. • **Resetarea dispozitivelor la starea implicită** - În cazul dispozitivelor care nu pot fi curățate sau încredințate, luați în considerare resetarea acestora la setările implicite de fabrică. Asigurați-vă că după resetare toate parolele implicite sunt schimbate și actualizate. • **Analiza log-urilor** - Analizați log-urile de securitate pentru a identifica activitatea suspectă și modelele de atac. Astfel puteți afla dacă unele porturi au rămas deschise sau sunt configurate greșit, iar remedierea acestor vulnerabilități va ajuta la creșterea nivelului de securitate din rețeaua locală. • **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://blog.sonicwall.com/en-us/2013/03/delphi-based-bot-with-ddos-capabilities-march-15-2013/