Raport consolidat eveniment cibernetic

DarkGate

DarkGate are două scopuri atât ca botnet cât și ca RAT(Remote Access Trojan), permițându-i să execute diverse acțiuni rău intenționate.
Acesta rămâne persistent în sistem prin crearea de fișiere și modificări ale registrului și comunică pe porturile **80/2351**.
Una dintre trăsăturile unice ale DarkGate este că folosește **Autoit**, care este un limbaj de scripting conceput pentru automatizarea GUI Windows și sarcinile generale de scripting.

Informații suplimentare

TIP	***Botnet/RAT***
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
Metode de infectare	• **Downloads from sites** Se folosește de adresele URL, redirecționând utilizatorii către un sistem de distribuție a traficului (TDS) pentru a descărca încărcătura malware utilă. O tactică alternativă implică exploatare a unui browser fake de actualizare. Dacă utilizator final interacționează cu butonul de actualizare a browserului contrafăcut, are loc un proces similar ca cel descris, utilizând un TDS pentru distribuirea încărcăturii malware • **Malvertising** Distribuția prin reclame online. Aceste apar pe site-uri web legitime și conduc utilizatorii către site-uri rău intenționate sau inițiază descărcări de programe malware la interacțiune. • **Executarea Psexec** DarkgGate este configurat pentru a crea un profil de utilizator, pe care îl folosește pentru deplasarea laterală în cadrul rețelei compromise. Acesta folosește Psexec pentru a executa procese de la distanță, facilitând răspândirea acestora în sistemele în rețea.

File hash	• a448c4abbb2f1844a8fa0c929cd84c2f6f57a4af0442a6a4b5307af89c35cef6 • e2a8a53e117f1dda2c09e5b83a13c99b848873a75b14d20823318840e84de243 • 5b608a6729343cf8b6752d5bb201f906920fcb472f5949e04173b907f65ceff1 • 6e068b9dcd8df03fd6456faeb4293c036b91a130a18f86a945c8964a576c1c70 • 394ee7c88a0925698ce1a2e0268ca49404591eb5cdd961d657d785993212cd86 • 22933b3ae7d125f312b6d1fe6356092cdcd1def6dca3ad128de65ba7986266ae • f8fcf37ab1e391d1809c4b5baf00d669c4263682d99230432c5199bde5914a60 • a3fc0ef279b5717d0b0dcbe25f8e543efee252cc116336a744968279ce9d3c29 • 1776dcbc4a3f430dd5ace833aac80b0954a050e5a7dec164b53b62fbe72feab3 • 00985db874d9177de4a18999f7a420260b3a4665ba2b5b32aa39433ef79819df • 0f1545a7176c45b0e7f9198cac8972167e5846e8b84cd40926f7edf338eeace2 • 10bfaeb0c00425c4749140d5c7d9f3d88537cf2f621ba7af5322b15cf205b896 • 2b24c4c883a562d0326846ee1c92840144d1d755cdb721b24a35038ea92aa0e4
IOCs	**URLS:** • hxxp[:]//185.39.18.170/A/S • hxxp[:]//5.188.87.58:2351/hzuhmgws • hxxp[:]//5.188.87.58:2351/msihzuhmgws • hxxp[:]//148.113.1.180:8080/TMDT.hta • hxxp[:]//fredlomberfile.com:2351/lpfdokkq **IP:** • 185.39.18.170 • 5.188.87.58 • 5.188.87.58 • 148.113.1.180 • 149.248.0.82 • 179.60.149.3 • 185.143.223.64 • 185.8.106.231 • 45.89.65.198 • 5.34.178.21 • 80.66.88.145 • 89.248.193.66

Detectare	• Analizați setările la internet. Înainte de a se conecta la C2, botnet-ul încercă să modifice setările la internet • Monitorizează activitatea rețelei în căutarea unor conexiuni externe neobișnuite, în special către servere C&C utilizate de botnet. DarkGate folosește **HTTP POST** pentru a comunica cu serverul C2. • Verifică lista proceselor și porturile deschise pentru porturi suspecte ca **80/2351** create de **msiexec.exe** • Identificați prezența DLL-uri suspecte: (de ex**: libcef.dll, sqlite3.dll**) • Analizați linia de comandă pentru detectare argumentului **--cpu-priority.**
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. Pentru aceasta utilizați firewall-uri sau soluții de filtrare a traficului. • **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. • **Educați-vă utilizatorii** - Angajații și clienții tăi sunt prima linie de apărare. Pentru a juca acest rol crucial, ei trebuie să aibă o educație de conștientizare a securității, care să-i învețe despre toate tipurile de atacuri de tip phishing. • **Monitorizarea instalării aplicațiilor** - DarkGate folosește instrumente de monitorizare și management de la distanță (RMM) pentru acces la desktop. Monitorizați utilizarea și instalarea unor astfel de instrumente și a altor aplicații. • **Reevaluarea securității rețelei** - Evaluați în mod regulat securitatea rețelei și revizuiți politicile de securitate pentru a vă asigura protecția continuă împotriva amenințărilor.