Raport consolidat eveniment cibernetic

Amadey Malware

Amadey este un bot modular care îi permite să acționeze ca **loader sau info stealer.** Este conceput pentru a efectua o serie de activități rău intenționate, inclusiv recunoaștere, exfiltrare de date și încărcare de încărcări suplimentare, care variază de la troieni bancare la instrumente DDoS. Vizează toate versiunile de **Microsoft Windows.**

Acest malware folosește două straturi de algoritmi de codare pentru a evita detectarea și pentru a face analiza statică și mai dificilă. Primul strat de codare este o codificare personalizată urmată de un algoritm **Base64.** De asemenea, creează un mutex folosind **API-ul CreateMutexA()** pentru a se asigura că numai un caz a procesului său malware rulează pe gazda compromisă.

În plus față de utilizarea cheilor de registry **„Run" și „RunOnce"** vizate în mod obișnuit, Amadey modifică valoarea „pornire" din cheile **„User Shell Folders"**, permițându-i să execute automat fișierul rău intenționat la repornirea sistemului.

Termeni și definiții

Loader - În contextul securității cibernetice, un loader este un tip de software malițios utilizat pentru a descărca și executa alte tipuri de malware pe un sistem compromis. Rolul principal al unui loader este de a încărca (sau "încărca") cod malițios suplimentar, cum ar fi troieni, ransomware sau keylogger-e, fără a atrage atenția sistemului sau a utilizatorului. Acesta este adesea un component al atacurilor mai complexe, deoarece permite atacatorilor să mențină flexibilitatea în livrarea malware-ului. După ce un loader a fost instalat cu succes pe dispozitivul victimei, atacatorii pot folosi acest canal pentru a descărca și executa programe malițioase în funcție de necesități, adaptând astfel atacul în funcție de țintă.

Info Stealer - malware conceput pentru a colecta și fura informații sensibile de pe dispozitivul infectat. Aceste informații pot include: date de autentificare (nume de utilizator, parole); informații financiare (detalii despre carduri de credit, conturi bancare); cookie de sesiune și date de autentificare stocate; informații de la portofele criptografice; date personale(adrese de email, numere de telefon și alte date) stocate în browser etc.

Informații sumare

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
Infectare	• Prin email de tip spear-phishing care conțin atașamente rău intenționate. Conținutul e-mailului este creat cu atenție pentru a părea legitim, atrăgând victima să deschidă atașamentul. • Descărcări drive-by de pe surse nesigure. • Să fie propus ca sarcină utilă de către alte programe malware aflate pe dispozitiv.
IOC	**IP addresses** 183.100.39.157 179.43.155.195 190.219.153.101 79.137.205.112 193.106.175.148 104.47.53.36 201.124.98.97 187.204.8.141 60.246.82.1 193.233.20.26 193.56.146.218 31.41.244.200 **URLs** http://31.41.244.10/Dem7kTu/index.php http://185.215.113.16/Jo89Ku7d/index.php http://servicestatus.one/b2ccsaG/index.php http://31.41.244.17/ http://185.215.113.16/inc/penis.exe http://185.215.113.19/CoreOPT/index.php http://185.11.61.121/h8s9k20gnb2/index.php http://185.11.61.121/h8s9k20gnb2/Plugins/clip64.dll http://185.11.61.121/h8s9k20gnb2/Plugins/cred64.dll
	• Analizați și monitorizați traficul de rețea pentru activități suspecte, cum ar fi conexiuni frecvente către domenii cunoscute ca fiind malițioase sau către

Detectare	adrese IP suspecte. Utilizați soluții IDS/IPS pentru a detecta comunicările neobișnuite și pentru a bloca traficul către serverele C2. • Examinați logurile de la servere, endpoint-uri și soluții de securitate pentru a identifica activități neobișnuite sau suspicioase. Căutați semne de execuție a fișierelor necunoscute sau modificări neașteptate în sistemele de fișiere și registre. • Folosiți soluții de securitate actualizate pentru a efectua scanări complete ale sistemelor. Asigurați-vă că definițiile antivirus sunt la zi. Utilizați scanere dedicate pentru malware care pot identifica semnăturile specifice ale **Amadey Malware.** • Folosiți instrumente de monitorizare a sistemului pentru a urmări procesele active și pentru a detecta procesele injectate cum ar fi **rundll32.exe**. Identificați și izolați procesele suspecte care rulează din locații neobișnuite, cum ar fi directoarele temporare.
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://darktrace.com/blog/amadey-info-stealer-exploiting-n-day-vulnerabilities