Raport consolidat eveniment cibernetic

LUMMA STEALER (SHAMEL)

Modelul Malware-as-a-Service (MaaS) continuă să ofere potențialilor atacatori o modalitate ieftină și relativ simplă de a desfășura atacuri cibernetice sofisticate și de a-și atinge scopurile nefaste. Un astfel de program de tip information stealer, denumit **"Lumma",** a fost promovat și vândut pe numeroase forumuri de pe dark web începând din 2022.

Lumma este cunoscut pentru faptul că ține sistemele de operare **Windows, de la Windows 7 la 11**, și cel puțin 10 browsere diferite, inclusiv **Google Chrome, Microsoft Edge și Mozilla Firefox.**

De asemenea, a fost observat că ține portofele de criptomonede precum **Binance și Ethereum**, precum și extensii de browser pentru portofele de criptomonede și autentificare cu doi factori (2FA) cum ar fi **Metamask și Authenticator**, respectiv. Datele din aplicații precum **AnyDesk sau KeePass** pot fi, de asemenea, exfiltrate de malware.

Lumma este livrat prin intermediul unui loader etapizat – scriptul malițios care efectuează unele verificări de bază și preia sarcina utilă de pe serverul de comandă. Cu toate acestea, acest lucru nu slăbește în niciun fel metodele de evaziune ale Lumma. Lucrul interesant despre acești loaderi este utilizarea profilului **GitHub ca server C2 intermediar**.

Funcția principală a acestor loaderi este de a se asigura că sistemul nu este o mașină virtuală sau un mediu de depanare, efectuând o revizuire de bază a sistemului și preluând sarcina utilă de pe un alt server de comandă. Acesta din urmă diferă în funcție de configurația și locația sistemului.

Informații sumare

TIP	***Lumma Stealer***
Instrumente pentru analiză	• **Pentru scanarea rețelei** – Wireshark, TCPDUMP, Angry IP Scanner ,Nmap • **Pentru scanarea de viruși și malware** – Software antivirus existente • **Analiză și detectare procese**- Lordpe, Sysmon , Procces Hacker
Metode de infectare	• **Drive-by downloads -** instalarea programului malițios atunci când utilizatorul vizitează un sait compromis sau un link dăunător • **Online scams**- când actualizări software sau antivirusuri false păcălesc utilizatorii să instaleze, fără să cunoască, Lumma Stealer • **Spam emails and messages**, când se folosesc atașamente sau link-uri pentru a instala pogramele malițioase în dispozitivele victimelor • **Bundled downloads,** când Lumma Stealer se ascunde în alte programe de de instalare a aplicaților gratis sau piratate, fără ca utilizatorul să realizeze acasta.
IoC	**MD5:** 69abcc261ae76d2b063672df06837966 **MD5:** 757661287c20b63b1c6ae4f66fc0c6d8 **MD5:** 6d07e04a6926d1dd6cc7805f866114a4 **MD5:** 8c2b02f3609019a2ea5af617a1d2556d **SHA-256:** 48cbeb1b1ca0a7b3a9f6ac56273fbaf85e78c534e26fb2bca1152ecd7542af54 **SHA-256:** 483672a00ea676236ea423c91d576542dc572be864a4162df031faf35897a532 **SHA-256:** 01a23f8f59455eb97f55086c21be934e6e5db07e64acb6e63c8d358b763dab4f **SHA-256:** 7603c6dd9edca615d6dc3599970c203555b57e2cab208d87545188b57aa2c6b1 **SHA-256:** 674d96c42621a719007e64e40ad451550da30d42fd508f6104d7cb65f19cba51
URLs	netovrema[.]pw opposesicknessopw[.]pw politefrightenpowoa[.]pw chincenterblandwka[.]pw loogsporus[.]pw/api meayyammgaterre[.]pw/api
	176.113.115.224 176.113.115.226

IP adrese	176.113.115.227 176.113.115.229 176.113.115.232 144.76.173.247 45.9.74.78 77.73.134.68 82.117.255.127 82.117.255.80 82.118.23.50
Măsuri de tratare post incident	• **Izolarea dispozitivului compromis** -Identificați dispozitivul sau sistemele suspecte 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, 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://www.kelacyber.com/wp-content/uploads/2023/05/KELA_Research_Infostealers_2023_full-report.pdf
	https://it.darktrace.com/blog/the-rise-of-the-lumma-info-stealer