DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Analiza *Ov3r_Stealer* și impactul său asupra securității cibernetice

Coautori:

Marius Alexe

Marius Duță

Adrian Măcău

Gabriel Niculescu

Lucian Păuc

Ștefan Cătănea-Homeghiu

București, 2024

TLP:CLEAR

Cuprins

Introducere

Prezentul document a fost elaborat de către specialiști din cadrul Directoratului Național de Securitate Cibernetică și se adresează entităților ce activează în domeniul Tehnologiei Informației, respectiv a Securității Cibernetice, care doresc să afle detalii tehnice specifice despre malware-ul *Ov3r_Stealer*, modul său de funcționare și potențialul impact al acestuia asupra sistemelor informatice, precum și tuturor utilizatorilor de dispozitive conectate la internet, pentru creșterea gradului de conștientizare asupra importanței securității cibernetice și implicit, a nivelului general de securitate cibernetică în spațiul național.

Stealer-ul: de ce este periculos și cum acționează

Un malware este un program informatic malițios sau un cod creat cu scopul de a deteriora ori perturba utilizarea normală a dispozitivelor informatice. Un astfel de program poate permite atacatorilor să acceseze în mod neautorizat un dispozitiv electronic, sistemul de operare sau datele acestuia, ori poate compromite confidențialitatea, integritatea sau disponibilitatea acestora.

Malware-ul împiedică utilizarea normală a unui dispozitiv. După ce atacatorul a obținut acces la acesta prin una sau mai multe dintre diversele tehnici, precum un e-mail de phishing, un fișier infectat, prin exploatarea unei vulnerabilități de sistem sau software, o unitate flash USB infectată sau un site web malițios, va profita de situație pentru a lansa atacuri suplimentare, spre exemplu pentru a obține credențialele, a colecta informații personale, a cripta datele, sau a vinde accesul la resursele informatice.

Malware-ul poate lua mai multe forme. Cele mai frecvent întâlnite sunt: viruși, troieni, worms, adware, spyware, ransomware, backdoors, rootkit, crypto miner, malware fără fișiere etc.[1]

Malware-urile pot fi și combinații de mai multe tipuri de programe malițioase. Spre exemplu, un malware poate ajunge la utilizator sub forma unui troian, dar odată executat poate ataca alte victime în rețea, ca un worm.

Unul dintre cele mai periculoase tipuri de malware, proiectat să sustragă informații sensibile de pe dispozitivele informatice infectate, este *stealer-ul*. Un *stealer* poate fi un troian care adună credențialele dintr-un sistem, parole salvate, informații din browser, chei de acces în portofele electronice, etc.[2] Acesta comunică în secret cu un așa-zis *centru de comandă și control (a.k.a. C2)* operat de atacatori, unde transmite toate datele culese. De obicei aceste date sunt exploatate de către atacatorii inițiali sau sunt vândute către alte persoane pe DarkWeb sau prin alte canale.[3]

Descoperirea și analiza malware-ului *Ov3r_Stealer*

Ce este Ov3r_Stealer?

Malware-ul *Ov3r_Stealer* este o formă de malware specializat în furtul de informații personale și sensibile de pe computerele infectate. Acesta poate fi clasificat drept troian, deoarece se

[1] https://www.microsoft.com/ro-ro/security/business/security-101/what-is-malware

[2] https://www.trendmicro.com/vinfo/us/security/definition/stealer

[3] https://www.threatintelligence.com/blog/stealer-malware

ascunde în spatele unor programe sau fișiere aparent legitime, dar în același timp colectează și transmite date fără consimțământul utilizatorului.

Funcționalitățile malware-ului *Ov3r_Stealer* includ, dar nu se limitează la:

- **Furtul de credențiale:** poate fi utilizat pentru a fura nume de utilizator și parole salvate în browser, aplicații de mesagerie instantanee sau alte aplicații.
- **Furtul de informații financiare:** poate viza și colecta informații despre carduri de credit, conturi bancare și alte detalii financiare ale utilizatorului.
- **Monitorizarea activității utilizatorului:** poate fi configurat pentru a monitoriza activitatea utilizatorului, cum ar fi site-urile web vizitate, activitatea pe rețelele sociale sau alte comportamente online.
- **Efectuarea de capturi de ecran:** unele versiuni pot fi capabile să înregistreze periodic sau la cerere capturi de ecran ale desktopului, ceea ce poate expune informații sensibile sau confidențiale.
- **Funcții de backdoor:** unele variante pot include și funcționalități de backdoor, permițând atacatorilor să aibă acces la distanță la sistemul infectat pentru a-l controla sau pentru a-l utiliza în alte atacuri.
- **Efecte asupra performanței sistemului**: poate avea un impact negativ asupra performanței sistemului infectat, provocând întârzieri, blocări sau alte probleme de funcționare.
- **Utilizarea rețelei de botnet[4]:** unele versiuni pot fi utilizate pentru a infecta mai multe computere și a le controla ca parte a unei rețele de botnet, permițând răufăcătorilor să execute atacuri distribuite de tip *denial-of-service* (DDoS) sau alte activități malițioase.
- **Posibilitatea de a infecta dispozitive mobile**: în unele cazuri, poate fi adaptat pentru a infecta și dispozitive mobile, cum ar fi smartphone-uri și tablete, extinzând astfel sfera sa de influență[5].

În urma unei investigații efectuată în cursul lunii decembrie 2023, de către Trustwave SpiderLabs, s-a observat că malware-ul a fost distribuit inițial prin intermediul unor anunțuri privitoare la locuri de muncă pentru o poziție de *Account Manager[6]*, postate pe rețeaua de socializare *Facebook (*Foto 1*)*. Prin accesarea anunțului, utilizatorii descărcau un document *.pdf* pentru deschiderea căruia li se solicita să apese pe butonul *"Acces Document"*, aspect ce ducea ulterior la executarea unui fișier *.cpl*, care în final ducea la executarea malware-ului.[7]

[4] Un botnet este o rețea care include o serie de dispozitive conectate la Internet, denumite boți. Termenul „botnet" este compus din cuvintele „robot" și „network" (rețea). Fiecare dintre aceste dispozitive a fost infectat cu programe malware care permit atacatorului să le controleze de la distanță, conform https://www.bitdefender.ro/

[5] https://www.malwarebytes.com/blog/threats/info-stealers

[6] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/trustwave-spiderlabs-uncovers-ov3r_stealer-malware-spread-via-phishing-and-facebook-advertising/

[7] https://www.pcmatic.com/blog/cybercriminals-exploit-job-seekers-on-facebook-with-malware-laden-job-ads/

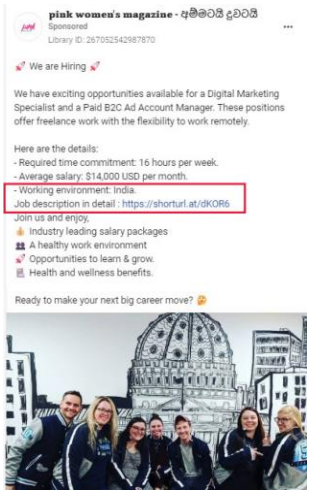

Foto 1

Totuși, *Ov3r_Stealer* poate fi distribuit și prin alte metode, precum atașamente de e-mail infectate, link-uri malware sau descărcări de software piratat sau neoficial.[8]

Deși nu se cunoaște cu exactitate scopul atacatorilor, se crede că eventualele date exfiltrate ar putea fi vândute pe *dark web* sau ar urma ca programul să fie actualizat pentru a acționa ca un *QakBot-like loader*[9], pentru livrarea unor alte tipuri de malware, incluzând *ransomware*.[10]

Anumite variante ale malware-ului pot fi proiectate pentru a se actualiza automat, permițând atacatorilor să îmbunătățească și să adapteze funcționalitatea sa, pentru a evita detectarea și eliminarea de către programele antivirus.[11]

Analiza de similaritate: Phemedrone și Ov3r_Stealer - legături și diferențe Un aspect de interes cu privire la *Ov3r_Stealer* este reprezentat de asemănările sale izbitoare cu o altă variantă de malware cunoscută sub numele de *Phemedrone Stealer*. Ambele tipuri de malware au ca similarități utilizarea aceluiași depozit *GitHub*[12] și anumite suprapuneri la nivel de cod, principala diferență dintre acestea fiind faptul că *Ov3r_Stealer* este scris în limbajul de programare *C#*[13]. Această observație ridică întrebări cu privire la potențiala evoluție sau reutilizare a malware-ului existent. Paralelele dintre *Ov3r_Stealer* și *Phemedrone Stealer*

[8] https://www.malwarebytes.com/blog/threats/info-stealers

[9] *QakBot* este clasificat ca un *stealer* sau ca un loader de malware, care este responsabil pentru faza inițială de infectare a unui sistem țintă, conform https://www.securonix.com/blog/qbot-qakbot-malwares-new-initial-execution/

[10] https://thehackernews.com/2024/02/beware-fake-facebook-job-ads-spreading.html

[11] https://www.malwarebytes.com/blog/threats/info-stealers

[12] https://digialert.com/index.php/blogs/item/261-unveiling-ov3r-stealer-the-deceptive-cyber-threat-hidden-within-fake-job-ads

[13] C#, pronunțat ca „C sharp", este un limbaj de programare modern, de uz general, care se regăsește în primele poziții ale topurile limbajelor de programare. Poate fi folosit pentru pentru a dezvolta programe și aplicații diverse: mobile, desktop, servicii bazate pe cloud, website-uri, software și jocuri - conform https://sdacademy.ro/

subliniază natura dinamică a amenințărilor cibernetice și adaptabilitatea infractorilor cibernetici în căutarea unor câștiguri ilicite.[14]

Compania *TrendMicro* a dezvăluit că malware-ul *Phemedrone Stealer* a fost distribuit prin exploatarea unei vulnerabilități a *Microsoft Windows Defender SmartScreen*. (CVE-2023-36025[15]).

Mai mult decât atât, creatorul *Ov3r_Stealer,* a distribuit pe anumite canale de *Telegram,* știri despre *Phemedrone Stealer,* pentru a-și crește credibilitatea și vizibilitatea în vederea promovării afacerii sale de *malware-as-a-service,* ținând cont de faptul că date referitoare la atacurile făcute cu programul malițios dezvoltat de acesta, au apărut în presă.[16]

Analiza metodelor utilizate pentru accesul inițial

Atacul orchestrat de *Ov3r_Stealer* urmează o secvență meticuloasă de pași, proiectați pentru a evita detectarea și pentru a maximiza rata de succes. Accesul inițial se realizează prin intermediul unui fișier *.pdf*, distribuit prin anunțuri de angajare postate pe rețeaua de socializare *Facebook*. La interacțiunea cu acest fișier, utilizatorii sunt rugați să facă click pe un link aparent inofensiv, ceea ce duce la descărcarea unui fișier de tip *.url*[17]. Acest fișier, deghizat ca un document *DocuSign*[18] legitim, găzduit în rețeaua de livrare de conținut (*Content Delivery Network*) a Discord, acționează ca o poartă pentru infiltrare. Ulterior, este executat un fișier de tip *Windows Control Panel (.cpl),* facilitând rularea unui script *PowerShell* responsabil cu lansarea *Ov3r_Stealer* în sistemul victimei.[19]

În general, *Windows* nu permite efectuarea acestei activități fără avertisment, dacă fișierul are una dintre extensiile *.exe* sau *.vbs*, dar din moment ce în cazul *Ov3r_Stealer* acesta este un fișier tip *Windows Control Panel (.cpl)*, sistemul de operare nu va emite niciun avertisment. Putem presupune astfel că această metodă de atac ar afecta doar sistemele de operare *Windows.*[20]

[14] https://digialert.com/index.php/blogs/item/261-unveiling-ov3r-stealer-the-deceptive-cyber-threat-hidden-within-fake-job-ads

[15] Vulnerabilitatea permite atacatorilor să ocolească verificările *Windows Defender SmartScreen*, ceea ce înseamnă că atunci când victima deschide un fișier malițios, *Windows* nu o avertizează dacă serviciul consideră fișierul (sau site-ul web) suspect și potențial malițios, conform precizărilor de pe site-ul https://www.helpnetsecurity.com/2024/01/15/cve-2023-36025-exploited/

[16] https://thehackernews.com/2024/02/beware-fake-facebook-job-ads-spreading.html

[17] Un fișier cu extensia *.url* este o scurtătură URL a unui site web care poate fi salvată pe computer cu orice adresă de site web, conform https://docs.fileformat.com/web/url/.

[18] Software de semnare a documentelor ce poate fi utilizat pentru a colecta aprobări online în mod legal și sigur, conform https://www.docusign.com/esignature/document-signing-software

[19] https://digialert.com/index.php/blogs/item/261-unveiling-ov3r-stealer-the-deceptive-cyber-threat-hidden-within-fake-job-ads

[20] https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/FaceBook_Ad_Spreads_Novel_Malware.pdf

Metode folosite pentru livrarea malware-ului

• Prin intermediul unui fișier cu extensia *.cpl*:

Așa cum am descris mai sus, după ce fișierul cu extensia *.cpl* este executat, este inițiată rularea unui script *PowerShell*, care duce la descărcarea a 3 noi fișiere în sistemul de operare al utilizatorului, după cum urmează:

- *WerFaultSecure.exe* – executabil *Windows* legitim;
- *Wer.dll* – fișier malițios;
- *Secure.pdf* - conține codul malițios încărcat de fișierul DLL[21].

• Prin intermediul unui fișier cu extensia *.html*:

Un fișier *HTML* cu denumirea *CustomCursor.html* a fost folosit pentru încărcarea fișierului *.zip* având denumirea *CustomCursor.zip*, care era criptat în *Base64*[22]. Fișierul având extensia *.zip* conținea:

- *CustomCursor.exe* – fișier de Windows legitim;
- *Wer.dll* –fișier malițios;
- *Data.ini* - conține codul malițios încărcat de fișierul DLL.

• Prin intermediul unui fișier cu extensia *.lnk:*

În acest scenariu, un fișier deghizat ca unul text normal, având denumirea *Attitude_Reports.txt*, este localizat într-o arhivă *.zip* trimisă utilizatorului. Fișierul din interiorul arhivei este unul de tip *comandă rapidă* (LNK)[23], având denumirea *Attitude_Reports.txt.lnk*. Întrucât Windows-ul nu afișează de regulă extensia, nu se observă *.lnk* din denumirea fișierului, acesta fiind văzut de utilizator ca un fișier *.txt* normal cu denumirea *Attitude_Reports.txt*.

Odată deschis acesta va direcționa utilizatorul către un depozit de pe *GitHub*, pentru a descărca și rula scriptul malițios.

• Prin intermediul unui fișier cu extensia *.svg*[24]:

În mod similar cu cel în care un fișier *.html* este utilizat, aici fișierele malițioase sunt încorporate într-un fișier cu extensia *.svg*. A fost descoperită o redirecționare către

Copyright_Report.svg. Odată deschis, un fișier *.rar* este încărcat imediat. Acesta conține un fișier tip *.lnk* care descarcă scriptul *Powershell*.

---

[21] Dynamic link library - o colecție de programe mici pe care programele mai mari le pot încărca atunci când este nevoie pentru a îndeplini anumite sarcini, conform https://www.techtarget.com/searchwindowsserver/definition/dynamic-link-library-DLL

[22] *Base64* este o schemă de codificare de la binar la text care reprezintă date binare într-un format de șir de caractere ASCII, conform https://builtin.com/software-engineering-perspectives/base64-encoding

[23] Un fișier *.lnk* este o comandă rapidă din Windows care are rol de pointer pentru a deschide un fișier, un folder sau o aplicație

[24] Formatul de fișier SVG (Scalable Vector Graphics) este un instrument popular pentru afișarea de grafice bidimensionale, diagrame și ilustrații pe site-uri web, conform https://www.adobe.com/creativecloud/file-types/image/vector/svg-file.html

Fiecare metodă folosită pentru livrarea malware-ului, aduce în dispozitivele utilizatorilor 3 fișiere, ca încărcătura finală:

- *WerFaultSecure.exe* - executabil legitim din Windows;
- *Wer.dll* – fișier malițios;
- *Secure.pdf* - conține codul malițios încărcat de fișierul DLL.[25]

Executarea și persistența:

Fișierele descărcate în dispozitivele utilizatorilor pot avea orice denumire, dar scopul lor este același, și anume ca fișierul legitim având extensia *.exe* să fie executat, iar acesta să apeleze *Wer.dll,* fișier ce conține codul malițios. Odată executat, malware-ul va stabili persistența pentru a se asigura că rulează o dată la 90 de minute și extrage date specifice către canalul de *Telegram* ce este monitorizat de atacatori. Printre aceste date se numără și adresa IP a dispozitivului infectat, care cu ajutorul site-ului http://ip-api.com, este asociată unei locații.[26]

Indicatori de compromitere:

În timpul investigației efectuată de *Trustwave SpiderLabs*, cu privire la *Ov3r_Stealer*, au fost observați următorii indicatori de compromitere (a fost utilizată o culoare pe fiecare set):

Nume fișier	MD5[27]	SHA256[28]
CX.txt	08c16f5196aaeacdcc46f10e82e7c47b	cb58bf466675be9e11cfb404503cb122514f47b9708d033e381f28a60535812c
CX.zip	905430fd2cba63713c5d5f625bc6fe5f	80f88566fda41ebc1b4e35d89748a804740bba0d03049c33c536cffd5e0491e2
secure.pdf	7f6fff7a288e53c8d2400140eb88d0b7	9b9ba722b314febfc4491955 1a03dde1539f115333183c2cb5e74b8e644ba5b3
wer.dll	739ede4370b88e60a1d872a1735f3923	8b73d7aa8bb8db8a9ecbf9f713934fbbb5caf4745d7a61a6f34a100c4d84fd9d

25 https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/FaceBook_Ad_Spreads_Novel_Malware.pdf

26 https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/FaceBook_Ad_Spreads_Novel_Malware.pdf

27 MD5 (Message Digest Algorithm 5) este o funcție criptografică de tip hash unidirecțional, care livrează ca rezultat o valoare fixă ca lungime de 128 Biți, conform https://ro.wikipedia.org/wiki/MD5

28 Secure Hash Algorithm 256, cunoscut și sub numele de SHA-256, este o funcție unidirecțională proiectată pentru securizarea informațiilor digitale. Funcția utilizează un proces matematic complex care convertește textul de orice lungime în șiruri de litere și cifre de 256 biți (64 de caractere), conform https://crypto.ro/dictionar/sha-256/

WerFaultSecure.exe	c86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
secure.pdf	24da08be82f439c3230d0b16b275902f	f2814a4b3796fb44045c33b9d0d9972bf40478e5bc74b587486900c6cfa02f3d
wer.dll	3b33cead1847d254bb4d0e614c32a9b8	b37ec923451dd15a0f68df0b392b0f1b243fe50c709de9e574ac14cf6fabdd53
WerFaultSecure.exe	c86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
DATA1.zip	d06e91a847f4303ca417ec131ac8c038	89caa1568fcff162086dae91e6bd34fd04facba50166ebff800d45a999d0be8b
DATA1.txt	eaa6f5129a23cb51029615b68a9ca792	4a36cc607ca5c2acc536510fd1b0ddd43a9403dac168d2420d474611909ed9e6
DATA2.zip	8904d6ad569095ef6fb1dab561edc420	e326c1b9e61cca6823300158e55381c6951b09d2327a89a8d841539cad3b4df3
DATA2.txt	bcbce22d8b56f857429a83c40551c8bf	188c72f995ebd5e1e8d0e3b9d34eeeec2ec95d4d0fee30d2ea0f317ab1596eef
secure.pdf	5c2dc3e1af236cafc798c517414be70d	5ecad303475e180f8879871d8571d1a7eeb99e0b3c63cc77fdd02cb9b8c51211
wer.dll	c90b04b9184f91575d4f12320b4a65ab	568b4b868b225f06bb34da0dc23603c9dedccc2b319353407c814983d5322563
WerFaultSecure.exe	c86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
secure.pdf	88e38e212591ffaf3c3400b22b8988d6	e64b185c149cb523d13cb46ea3911e2c0595b6f10ae86e6a14b15e8d45c0cdcb
wer.dll	b042b2a8981a94b7afe680d94808e9f8	c6765d92e540af845b3cbc4caa4f9e9d00d5003a36c9cb548ea79bb14c7e8f66
WerFaultSecure.exe	c86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
DATA3.txt	906509861bd74330c15f3c669b0a4c04	4da33c7fe62f71962913d7b40ff76aff9f1586e57db707b3d6b88162c051f402
DATA3.zip	1006ad7046f065da16102c3cb5e6bcb9	ff44e502bd5ea36e17b3fc39b480e65971b36002f27fb441e4acadd6bf604a20

DATA4.zip	3c490e342c30710834f21cbdadf80897	480fae3bdc2604cba846779dd7dced95b3ce036bdef629ded247771a2e4d5d58
DATA4.txt	f52c10457c584f1b136fd7922a565c32	b7980f64f892d70b1cd72a8c80f8319f50c3c410aba4e4bc63fd6494bcb4f313
secure.pdf	af0ce315ea226f4b07d7e3fac1b69846	5f0ff1fd6ca89a0ddd3178e023dea8f79ff3c3f3d8ff7900378eb014e83ed326
wer.dll	092566470d8f8ffd8e0e70c34229882e	d5b1214f1817a16b2bc8a76daa48c9a3c5af0e411cf4f0c17b0e364d437a454b
WerFaultSecure.exe	c86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
KAY.zip	f424e8b32ca6ad7153f706ed1a0bc0af	348aea633c99e5f6a0ac7b850961be0a145a35678e5bd074b4852f7a2419f518
kay.txt	0c33eafc7d9cb3abf6048ca98a5d2db9	1c53dffcb4c474a2b08708609466e7d234d6d51139b6532af54fac5bb8d37415
secure.pdf	4afa1df89ec91d1e81020b9f42da43dc	3a34cd3a3221d83a1cca8913b2afbb5b780027d48b44d3ce15dfe4a402064871
wer.dll	fe7b790b033aa60212249a2c47891041	40c6fa38e44e00d8cf113d0a079cd46f8b7654331f12e50d2af5a9f1ddc6d266
WerFaultSecure.exe	C86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
CustomCursor.exe	C86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
CustomCursor.html	15a38db72e97b9f5b5a5737dd23571bd	99d27635eb7819731047835701 4f63fc6f044558a0a17c34086741801a83c80c
CustomCursor.zip	534f90adf294faf90a293abfc4ac2f26	0df85ed4877940f4a6987790901734f8eb74cb97672773ec232cbb0ea76db681
wer.dll	Fbf7e29cb108587f5abbf6b7f91a1ddd	0c2ccf98694849f898a4170cb46add3cd60b93e568dc300f6c868e38e64a3ba0
data.ini	4a328bdd8568261a14ebfff4eb6ffd2f	a2710b5991583e44453126c237b642891acf53a313b39ae94f2ae9b44c51070d

Tabel preluat din raportul publicat de *Trustwave SpiderLabs* cu privire la *Ov3r_Stealer*[29]

Identificarea posibilelor entități din spatele Ov3r_Stealer

În general, în investigarea oricărui malware este importantă căutarea de indicii referitoare la originea acestuia și scopul pentru care a fost creat. Atribuirea malware-ului unei anumite grupări poate fi dificilă, însă este importantă urmărirea oricăror indicii pentru a se obține informații despre viitoarele campanii de atac sau alte versiuni ale aceluiași malware.

Indicii descoperite cu privire la *Ov3r_Stealer*:

- Username-ul ***JohnMacollan*** – acest cont a fost asociat cu canalul *Telegram* utilizat pentru exfiltrarea datelor. Totodată, a fost descoperită o altă utilizare a acestui cont pe forumul *Pwn3rzs*[30].
- Username-ul ***Liu Kong*** – și acesta a fost asociat cu canalul *Telegram* utilizat pentru exfiltrarea datelor. S-a descoperit ca și acest utilizator a fost asociat cu forumul *Pwn3rzs* menționat mai sus, dar și cu altul denumit *KGB forum* găzduit la https://wdkiller.com. Acest site susține că oferă soluții de *bypass* pentru *Windows Defender* și alte produse *EDR*[31]. Aici a fost descoperit un video demonstrativ în care *Ov3r_Stealer* era testat.

Totodată, au fost descoperite trei canale de *Telegram* care sunt afiliate contului *Liu Kong*: *Golden Dragon Lounge*, *Data Pro*, and *Golden Dragon*, în timp ce alte două pseudonime au fost legate de *Liu Kong*, respectiv *MR Meta* și *MeoBlackA*.

La acest moment se crede că pseudonimul *MeoBlackA* este controlat de atacator și că acesta își schimbă frecvent numele.[32]

Pași de urmat în cazul unei infectări cu *Ov3r_stealer*

În cazul unei infectări cu un astfel de program malițios vor fi luate următoarele măsuri:

- Izolarea sistemului infectat, pentru a preveni răspândirea malware-ului în alte sisteme și rețele;
- Implementarea unor măsuri pentru a reduce impactul incidentului și pentru a remedia vulnerabilitățile sistemului, spre exemplu: scanarea sistemelor din aceeași rețea prin folosirea unor programe tip *antivirus*, eliminarea malware-ului din dispozitive, actualizarea software-ului pentru a remedia vulnerabilitățile și consolidarea măsurilor de securitate;
- Stocarea probelor digitale, precum fișierele jurnal ale sistemelor de operare infectate, fișiere generate de programele informatice cu funcție de interceptare a traficului de rețea, fișiere jurnal generate de sistemele de securitate;

---

29 https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/FaceBook_Ad_Spreads_Novel_Malware.pdf

30 *Pwn3rzs* – se descriu ca fiind un mic grup de entuziaști ai securității dispozitivelor electronice, cărora le place să spargă diferite tool-uri, conform web site-ului https://www.pwn3rzs.cloud/

31 *Endpoint Detection and Response* (EDR) - este o soluție de securitate care monitorizează continuu dispozitivele utilizatorilor finali pentru a detecta și a răspunde amenințărilor cibernetice cum ar fi ransomware și malware, conform https://www.crowdstrike.com/

32 https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/FaceBook_Ad_Spreads_Novel_Malware.pdf

• Raportarea incidentului către autoritățile competente și colaborarea cu aceștia pentru facilitarea investigațiilor;
• Implementarea indicatorilor de compromitere în configurațiile sistemelor de securitate, precum și în platformele de *threat intelligence*.
• Schimbarea parolelor de la toate conturile care ar fi putut fi compromise, precum și o eventuală restabilire a sistemelor dintr-un backup recent.

Investigațiile ce urmează a fi efectuate în urma incidentului, presupun analizarea probelor digitale, precum fișierele jurnal ale sistemelor de operare sau ale malware-ului. În urma analizei, pot fi descoperite date relevante, precum serverul cu care programul malițios

comunică și pe care transmite date, funcționalitatea principală a acestuia, sau datele care au fost exfiltrate.

Pentru prevenirea unor astfel de atacuri, se recomandă, printre altele: organizarea unor training-uri de conștientizare asupra securității cibernetice; monitorizarea continuă a sistemelor informatice; actualizarea aplicațiilor și instalarea patch – urilor; renunțarea de către utilizatori la folosirea unor conturi cu permisiuni de administrator cu excepția cazurilor în care este nevoie; implementarea regulată a indicatorilor de compromitere din platformele de *threath intelligence* în sistemele de securitate, rularea continuă a funcției *Threat Hunting*.[33]

Aspecte de ordin legislativ, reglementare și politici organizaționale ce pot fi încălcate în cazul atacurilor cu *Ov3r_Stealer* în România

Regulamente și politici interne ale organizațiilor

Un incident legat de executarea instrucțiunilor malițioase ale *Ov3r_Stealer* pe dispozitivele din cadrul unei organizații, poate conduce la încălcarea regulamentelor și politicilor interne ale acesteia, afectând astfel cei trei piloni ai securității cibernetice: confidențialitatea, integritatea și disponibilitatea datelor și a sistemelor informatice, în funcție de vulnerabilitățile pe care malware-ul le exploatează.

• *Confidențialitatea* datelor, reglementată și protejată de legislația privind protecția datelor cu caracter personal, de regulamentele interne, precum și de anumite acorduri de confidențialitate regăsite în clauzele contractuale dintre organizații și partenerii sau clienții acestora, poate fi compromisă de către *Ov3r_stealer* prin capabilitatea acestuia de a efectua capturi de ecran asupra sistemelor infectate sau prin exfiltrarea datelor din acestea. Funcționalitatea malware-ului de a monitoriza traficul de rețea generat de utilizatorul sistemului infectat, poate duce la pierderea confidențialității unor date sensibile, precum conturi de utilizatori și parolele acestora, site-uri web vizitate, corepondență electronică, ori documente transmise la nivel de rețea.
• *Integritatea* datelor poate fi compromisă atât prin capabilitățile de tip *backdoor* ale acestuia cât și prin posibilitatea coruperii fișierelor în momentul exfiltrării lor.
• Ultima componentă a triadei, cea de *disponibilitate*, poate fi afectată în principal de efectele pe care *Ov3r_stealer* la are asupra performanței sistemului infectat, acesta putând să provoace întârzieri și eventuale blocări ale sale. Un caz aparte este cel de infectare a sistemului în vederea integrării lui într-o rețea de *botnet*, situație în care, utilizatorul legitim al acestuia, va pierde capacitatea de a-l controla pe perioada în care este folosit pentru atacuri de tip

33 https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/FaceBook_Ad_Spreads_Novel_Malware.pdf

DDoS. În același timp, sistemele infectate pot deveni indisponibile temporar sau permanent, ducând astfel la incapacitatea unei organizații de a livra servicii sau de a-și îndeplini atribuțiile obișnuite.

Concluzionând asupra modului în care regulamentele și politicile interne pot fi încălcate în urma infectării cu *Ov3r_stealer,* este de subliniat că acesta poate avea un impact asupra tuturor principiilor de securitate cibernetică ale entității și poate crea daune atât în mod direct asupra sistemelor infectate, cât și în mod indirect prin diminuarea încrederii în sistemul informatic al organizației și în procedurile de securitate ale acesteia.

Reglementarea incidentelor de securitate cibernetică

Conform Legii 362/2018 *privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, entitățile care asigură servicii esențiale sau digitale, sunt obligate să notifice de îndată Directoratul Național de Securitate Cibernetică (DNSC), cu privire la incidentele care au un impact semnificativ asupra capacității lor de a furniza serviciile esențiale.

Având în vedere importanța acordată acestor evenimente cu potențial negativ mare, prin Legea 58/2023 *privind securitatea și apărarea cibernetică a României,* a fost stabilit un termen maxim de 48 de ore în care instituțiile publice și instituțiile private care asigură servicii publice sau de interes public, trebuie să raporteze incidentele cibernetice.

Astfel, un incident legat de executarea instrucțiunilor malițioase ale malware-ului *Ov3r_Stealer* și care are un impact semnificativ asupra capacității organizațiilor de a furniza servicii esențiale, trebuie raportat Directoratului Național de Securitate Cibernetică de îndată, în cazul entităților care asigură servicii esențiale sau digitale și în termen de 48 de ore, în cazul instituțiilor publice și instituțiilor private care asigură servicii publice sau de interes public.

Aspecte de natură penală

Din punct de vedere al legislației penale din România, executarea instrucțiunilor malițioase ale *Ov3r_Stealer*, ar putea face obiectul infracțiunilor de:

- *accesul ilegal la un sistem informatic*, faptă prev. de art. 360 din Codul Penal, în măsura în care acesta are incluse și funcționalități de *backdoor*, permițând astfel atacatorilor să aibă acces de la distanță la sistemul infectat, pentru a-l controla sau pentru a-l utiliza în alte atacuri;
- *interceptarea ilegală a unei transmisii de date informatice*, faptă prev. de art. 361 din Codul Penal, dacă prin intermediul acestuia este monitorizată activitatea utilizatorului;
- *perturbarea funcționării sistemelor informatice,* faptă prev. de art. 363 din Codul Penal, în măsura în care provoacă întârzieri, blocări sau alte probleme grave de funcționare ale sistemului;
- *transferul neautorizat de date informatice*, faptă prev. de art. 364 din Codul Penal, în măsura în care datele din sistemele informatice infectate sunt exfiltrate;
- *operațiuni ilegale cu dispozitive sau programe informatice*, faptă prev. de art. 365 alin. 1 lit. a din Codul Penal - așa cum este prevăzut în textul de lege, infracțiunea este comisă prin producerea sau distribuirea unui program informatic, conceput în scopul săvârșirii uneia dintre infracțiunile prevăzute de art. 360-364, chiar dacă malware-ul nu este folosit în fapt.
- *falsul informatic*, faptă prev. de art. 325 din Codul Penal, în măsura în care sunt create pagini false pe rețeaua de socializare *Facebook,* în numele unor companii sau persoane, cu scopul de a distribui anunțurile de angajare false.

Concluzii

Prin analizarea modului în care malware-ul își manifestă prezența, se constată că acesta exploatează vulnerabilități ale sistemului de operare Windows, subliniind astfel importanța actualizării regulate a sistemelor de operare, implementarea de pachete de actualizare pentru aplicațiile utilizate și adoptarea conturilor cu permisiuni limitate pentru utilizarea obișnuită a calculatoarelor personale.

În urma investigațiilor efectuate, una din concluzii este că depozitul de pe *GitHub* ce a fost folosit pentru *Phemedrone* și *Ov3r_Stealer* a fost eliminat. Creatorul programului malițios folosește în continuare știrile apărute în presă cu privire la malware pentru a-și promova afacerea de *malware-as-a-service*.

Ov3r_Stealer nu a fost utilizat încă în campanii ample de atacuri cibernetice, acesta fiind cel mai probabil sub o continuă dezvoltare. Întrucât *Phemedrone* este un malware de tip open-source, cel mai probabil codul său va reapărea în alte programe malițioase la un moment dat, nefiind exclusă apariția unor capabilități noi ale virusului, sau adaptarea acestuia pentru sisteme de operare mobile (ex. Android).

Bibliografie

1. Legea 286/2009 privind Codul penal
2. Legea 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice
3. Legea 58/2023 privind securitatea și apărarea cibernetică a României
4. https://www.microsoft.com/ro-ro/security/business/security-101/what-is-malware - accesat la data de 07.02.2024
5. https://www.trendmicro.com/vinfo/us/security/definition/stealer - accesat la data de 08.02.2024
6. https://www.threatintelligence.com/blog/stealer-malware - accesat la data de 07.02.2024
7. https://thehackernews.com/2024/02/beware-fake-facebook-job-ads-spreading.html - accesat la data de 12.02.2024
8. https://www.securonix.com/blog/qbot-qakbot-malwares-new-initial-execution/ - accesat la data de 12.02.2024
9. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/trustwave-spiderlabs-uncovers-ov3r_stealer-malware-spread-via-phishing-and-facebook-advertising/ - accesat la data de 08.02.2024
10. https://www.pcmatic.com/blog/cybercriminals-exploit-job-seekers-on-facebook-with-malware-laden-job-ads/ - accesat la data de 13.02.2024
11. https://www.helpnetsecurity.com/2024/01/15/cve-2023-36025-exploited/ - accesat la data de 15.02.2023
12. https://docs.fileformat.com/web/url/ - accesat la data de 15.02.2023
13. https://www.docusign.com/esignature/document-signing-software - accesat la data de 15.02.2023
14. https://www.techtarget.com/searchwindowsserver/definition/dynamic-link-library-DLL - accesat la data da 16.02.2024
15. https://builtin.com/software-engineering-perspectives/base64-encoding - accesat la data da 16.02.2024
16. https://www.adobe.com/creativecloud/file-types/image/vector/svg-file.html - accesat la data da 16.02.2024

17. https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/FaceBook_Ad_Spreads_Novel_Malware.pdf - accesat la data de 26.02.2024
18. https://www.pwn3rzs.cloud/ - accesat la data de 26.02.2024
19. https://sdacademy.ro/ - accesat la data de 08.03.2024
20. https://www.shortcutmedia.ro/ - accesat la data de 08.03.2024
21. https://www.malwarebytes.com/blog/threats/info-stealers - accesat la data de 12.03.2024
22. https://digialert.com/index.php/blogs/item/261-unveiling-ov3r-stealer-the-deceptive-cyber-threat-hidden-within-fake-job-ads - accesat la data de 12.03.2024
23. https://ro.wikipedia.org/wiki/MD5 -accesat la data de 13.03.2024
24. https://crypto.ro/dictionar/sha-256/ - accesat la data de 13.03.2024
25. https://www.bitdefender.ro/consumer/support/answer/21607/ - accesat la data de 10.04.2024