Raport consolidat eveniment cibernetic

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

Funcționalități ale 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:** 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.

Informații sumare

TIP	***Ov3r 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 folosite pentru livrare malware	**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 DLL21. **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 Base6422. 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 .svg24:** 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.

IOC

Filename	MD5	SHA256
CX.txt	08c16f5196aaeacdcc46f10e82e7c47b	cb58bf466675be9e11cfb404503cb122514f47b9708d033e381f28a60535812c
CX.zip	905430fd2cba63713c5d5f625bc6fe5f	80f88566fda41ebc1b4e35d89748a804740bba0d03049c33c536cffd5e0491e2
secure.pdf	7f6fff7a288e53c8d2400140eb88d0b7	9b9ba722b314febfc44919551a03dde1539f115333183c2cb5e74b8e644ba5b3
wer.dll	739ede4370b88e60a1d872a1735f3923	8b73d7aa8bb8db8a9ecbf9f713934fbbb5caf4745d7a61a6f34a100c4d84fd9d
WerFaultSecure.exe	c86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
secure.pdf	24da08be82f439c3230d0b16b275902f	f2814a4b3796fb44045c33b9d0d9972bf40478e5bc74b587486900c6cfa02f3d
wer.dll	3b33cead1847d254bb4d0e614c32a9b8	b37ec923451dd15a0f68df0b392b0f1b243fe50c709de9e574ac14cf6fabdd53
WerFaultSecure.exe	c86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
DATA1.zip	d06e91a847f4303ca417ec131ac8c038	89caa1568fcff162086dae91e6bd34fd04facba50166ebff800d45a999d0be8b
DATA1.txt	eaa6f5129a23cb51029615b68a9ca792	4a36cc607ca5c2acc536510fd1b0ddd43a9403dac168d2420d474611909ed9e8
DATA2.zip	8904d6ad569095ef6fb1dab561edc420	e326c1b9e61cca6823300158e55381c6951b09d2327a89a8d841539cad3b4df3
DATA2.txt	bcbce22d8b56f857429a83c40551c8bf	188c72f995ebd5e1e8d0e3b9d34eeeec2ec95d4d0fee30d2ea0f317ab1596eef
secure.pdf	5c2dc3e1af236cafc798c517414be70d	5ecad303475e180f8879871d8571d1a7eeb99e0b3c63cc77fdd02cb9b8c51211
wer.dll	c90b04b9184f91575d4f12320b4a85ab	568b4b868b225f06bb34da0dc23603c9dedccc2b319353407c814983d5322583
WerFaultSecure.exe	c86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
secure.pdf	88e38e212591ffaf3c3400b22b8988d6	e64b185c149cb523d13cb46ea3911e2c0595b6f10ae86e6a14b15e8d45c0cdcb
wer.dll	b042b2a8981a94b7afe680d94808e9f8	c6765d92e540af845b3cbc4caa4f9e9d00d5003a36c9cb548ea79bb14c7e8f66
WerFaultSecure.exe	c86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
DATA3.txt	906509861bd74330c15f3c669b0a4c04	4da33c7fe62f71962913d7b40ff76aff9f1586e57db707b3d6b88162c051f402
DATA3.zip	1006ad7046f065da16102c3cb5e8bcb9	ff44e502bd5ea36e17b3fc39b480e65971b38002f27fb441e4acadd8bf804a20
DATA4.zip	3c490e342c30710834f21cbdadf80897	480fae3bdc2604cba846779dd7dced95b3ce036bdef629ded247771a2e4d5d58
DATA4.txt	f52c10457c584f1b136fd7922a565c32	b7980f64f892d70b1cd72a8c80f8319f50c3c410aba4e4bc63fd6494bcb4f313
secure.pdf	af0ce315ea226f4b07d7e3fac1b69846	5f0ff1fd6ca89a0ddd3178e023dea8f79ff3c3f3d8ff7900378eb014e83ed326
wer.dll	092568470d8f8ffd8e0e70c34229882e	d5b1214f1817a16b2bc8a76daa48c9a3c5af0e411cf4f0c17b0e384d437a454b
WerFaultSecure.exe	c86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
KAY.zip	f424e8b32ca8ad7153f706ed1a0bc0af	348aea633c99e5f8a0ac7b850961be0a145a35678e5bd074b4852f7a2419f518
kay.txt	0c33eafc7d9cb3abf6048ca98a5d2db9	1c53dffcb4c474a2b08708609466e7d234d6d51139b6532af54fac5bb8d37415
secure.pdf	4afa1df89ec91d1e81020b9f42da43dc	3a34cd3a3221d83a1cca8913b2afbb5b780027d48b44d3ce15dfe4a402064871
wer.dll	fe7b790b033aa60212249a2c47891041	40c6fa38e44e00d8cf113d0a079cd46f8b7654331f12e50d2af5a9f1ddc8d266
WerFaultSecure.exe	C86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
CustomCursor.exe	C86f71dafb6589dc711dd2bc27373f5a	5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f
CustomCursor.html	15a38db72e97b9f5b5a5737dd23571bd	99d27635eb78197310478357014f63fc6f044558a0a17c3408674180 1a83c80c
CustomCursor.zip	534f90adf294faf90a293abfc4ac2f26	0df85ed4877940f4a6987790901734f8eb74cb97672773ec232cbb0ea76db681
wer.dll	Fbf7e29cb108587f5abbf6b7f91a1ddd	0c2ccf98694849f898a4170cb46add3cd60b93e568dc300f8c868e38e64a3ba0
data.ini	4a328bdd8568261a14ebfff4eb6ffd2f	a2710b5991583e44453126c237b642891acf53a313b39ae94f2ae9b44c51070d

Detectare

1. Verificarea actualizării sistemului și patch-urilor critice
2. Monitorizarea porturilor mai sus menționate
3. Analiza fișierelor **system32** pentru localizarea artefactelor malițioase
4. Examinarea activității suspicioase pe nivel de servicii, procese sau conexiuni de rețea

Recomandări generice

- **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 IOC. 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.trustwave.com/en-us/resources/library/documents/facebook-advertising-spreads-novel-malware-variant/*