Rapporto di Sicurezza: Analisi della Minaccia "66bddfcb52736_vidar.exe"

A cura di: SecureSentinels

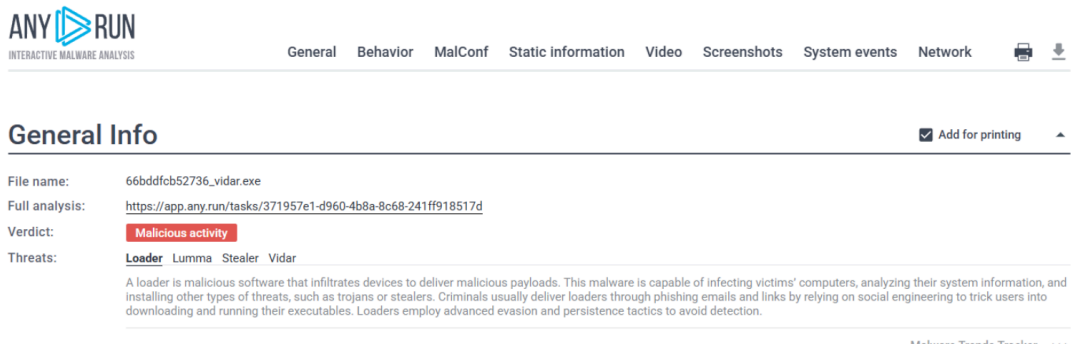
Data: 24 Febbraio 2026

Oggetto: Analisi comportamentale e di rete di un file eseguibile malevolo

1. Sintesi Esecutiva (Cosa abbiamo trovato)

Il team SecureSentinels ha analizzato un file sospetto denominato `66bddfcb52736_vidar.exe`. L'esito dell'analisi è inequivocabile: si tratta di un'**attività apertamente malevola**.

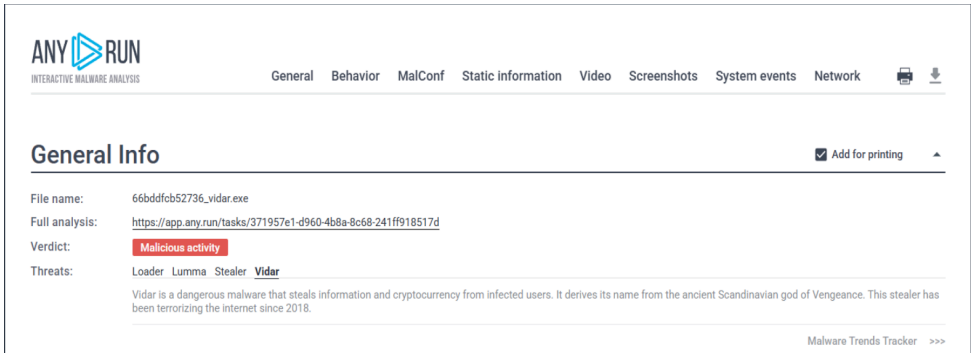
Il file non è un semplice virus, ma un **"Loader"** (un software da infiltrazione). Il suo scopo principale è entrare di nascosto nel computer della vittima per spalancare le porte ad altri programmi criminali ben più pericolosi. Nello specifico, questo Loader ha scaricato e attivato simultaneamente due dei più famosi **"Infostealer"** (software specializzati nel furto di dati personali): **Vidar** e **Lumma**.



2. Identikit dei Colpevoli

L'analisi ha confermato la presenza di due minacce distinte che operano in parallelo:

- **Vidar:** Attivo dal 2018 (il cui nome deriva dal dio scandinavo della vendetta), è un virus progettato specificamente per rubare password, documenti e portafogli di criptovalute.

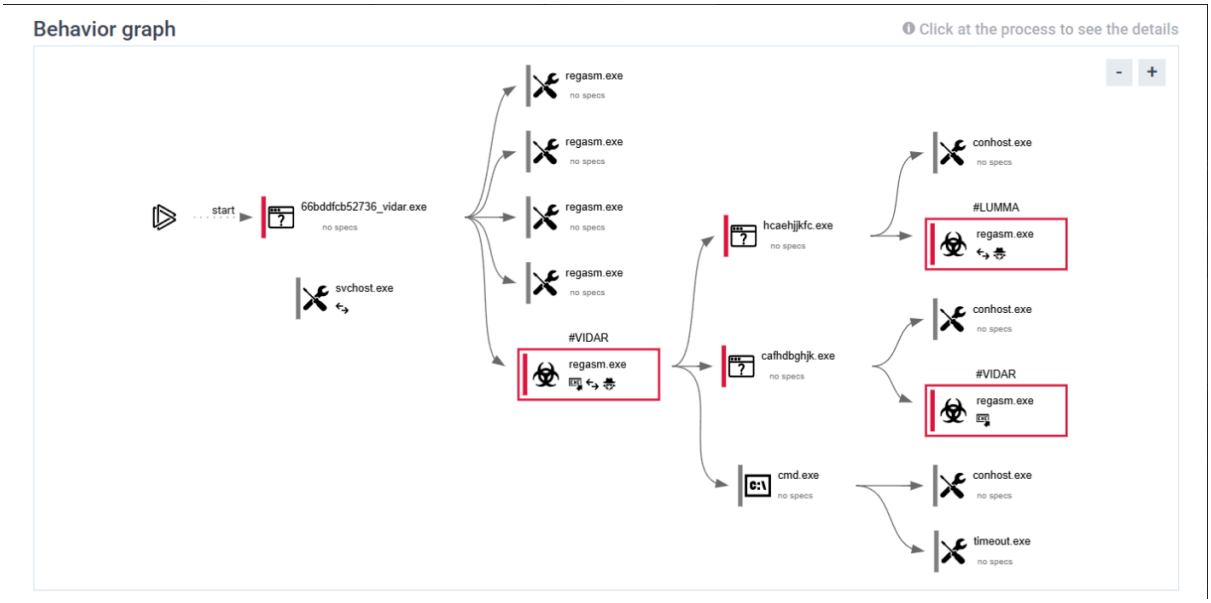


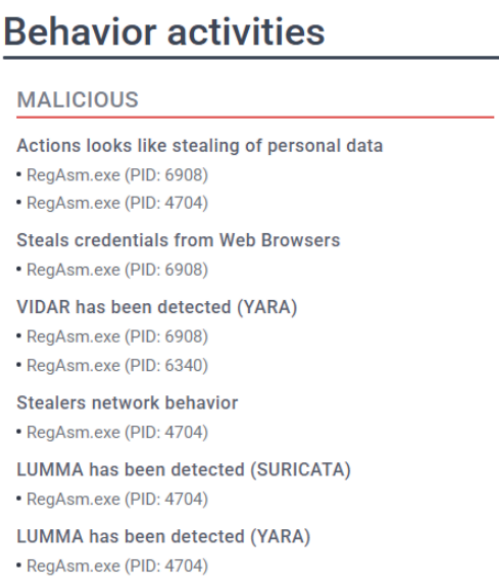
- **Lumma:** È un malware moderno, venduto online ai criminali come "servizio in abbonamento" (Malware-as-a-Service). Prende di mira credenziali di accesso, portafogli digitali e dati sensibili, aggiornandosi continuamente per sfuggire agli antivirus.

3. Come agisce il virus (La Tecnica di Attacco)

I criminali hanno utilizzato strategie molto furbe per non farsi scoprire:

- **Il Travestimento (Process Hollowing):** Invece di far girare un programma con un nome sospetto, il virus "svuota" un programma legittimo e sicuro di Windows chiamato `regasm.exe` (uno strumento di sistema) e ci si nasconde dentro. Dal nostro grafico comportamentale si evince chiaramente come il file originale faccia partire diverse copie "infette" di `regasm.exe`, di cui alcune assegnate a Vidar e altre a Lumma.



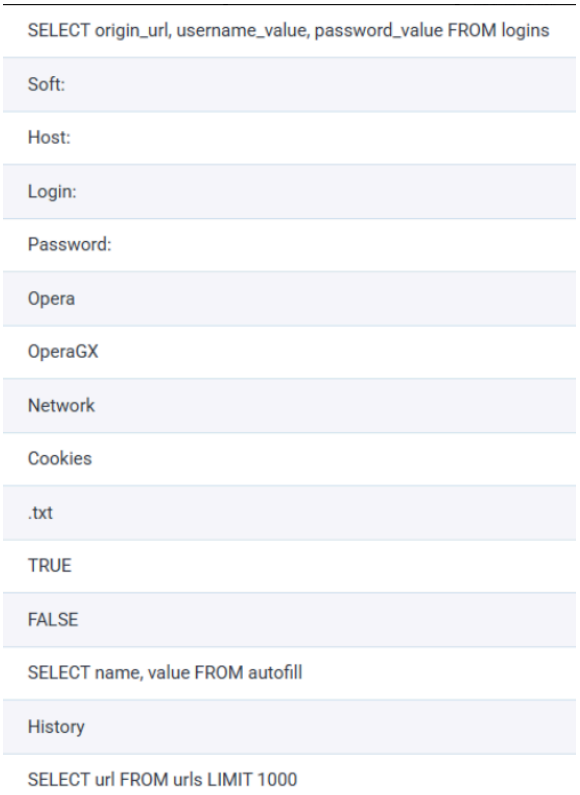


- **Tecnica del "Fingersi Morto" (Evasione):** Abbiamo rilevato l'uso del comando di sistema `TIMEOUT.EXE`. Il virus usa questo comando per ritardare le sue azioni di alcuni secondi, sperando che i sistemi di sicurezza lo considerino innocuo e smettano di controllarlo prima che inizi a rubare i dati.

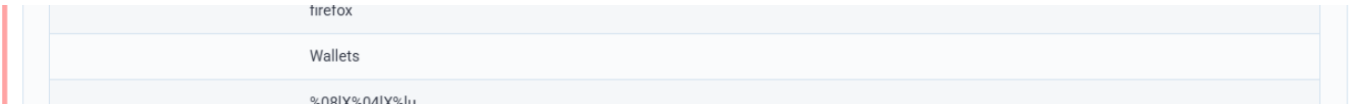
4. Il Bottino: Cosa cerca di rubare?

Il malware va a colpire dritto al cuore della privacy dell'utente. Abbiamo intercettato le sue "liste della spesa" (i comandi che usa per cercare i dati):

- **Browser Web:** Cerca di estrarre credenziali, cookie di sessione, cronologia e dati di autocompilazione da browser come Firefox, Opera e OperaGX. Utilizza veri e propri comandi di database (SQL) per dire: *"Prendi l'indirizzo web, il nome utente e la password dai salvataggi"*.



- **Finanze e Criptovalute:** Cerca in modo mirato cartelle denominate `Wallets` (i portafogli virtuali per le criptovalute).



- **Piattaforme di Gioco:** Cerca le cartelle di **Steam** (la nota piattaforma di videogiochi), tentando di rubare i file di configurazione (`config.vdf`, `loginusers.vdf`) per appropriarsi degli account.

SteamPath
\config\
ssfn*
config.vdf
DialogConfigOverlay*.vdf
libraryfolders.vdf
loginusers.vdf
\Steam\

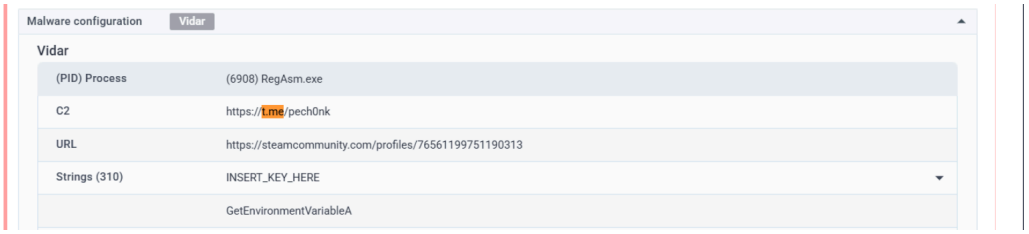
- **Comunicazioni Private:** Cerca di accedere agli archivi segreti di **Discord** e **Telegram Desktop** per rubare i file di sessione e leggere i messaggi.

\discord\
\Local Storage\leveldb\CURRENT
\Local Storage\leveldb
\Telegram Desktop\

5. Le Comunicazioni (Dove finiscono i nostri dati?)

Una volta raccolti i dati, il virus deve spedirli ai criminali. Per farlo, usa tattiche di "camuffamento" della rete:

- **Uso di Piattaforme Legittime (Vidar):** Per non destare sospetti, Vidar non si collega subito a un server criminale, ma legge istruzioni nascoste in profili pubblici. Abbiamo trovato collegamenti a canali **Telegram** (`t.me/pechOnk` e `t.me/jamelwt`) e a profili della **community di Steam**.



(PID) Process	(6340) RegAsm.exe
C2	https://t.me/jamelwt
URL	https://steamcommunity.com/profiles/76561199761128941
Strings (239)	INSERT_KEY_HERE
	lstrcpyA
	GetEnvironmentVariableA

- **Domini "Usa e Getta" (Lumma):** Lumma cerca di inviare i dati a una serie di siti web anomali registrati con l'estensione `.shop` (es. `candedqpwqm.shop`, `caffegclasiqwp.shop`, `evoliutwoqm.shop`) .

Lumma

(PID) Process	(4704) RegAsm.exe
C2 (8)	condedqpwqm.shop
	stagedchheiqwo.shop
	traineiwnqo.shop
	locatedblsoqp.shop
	caffegclasiqwp.shop
	evoliutwoqm.shop
	millyscroqwp.shop
	stamppreewntnq.shop

- **Server Malevoli:** Abbiamo individuato un collegamento diretto a un server in Russia (IP `147.45.44.104`) identificato dai radar di sicurezza come altamente malevolo e associato al download di ulteriori componenti del virus.

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
5468	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
3584	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6908	RegAsm.exe	147.45.44.104:80	–	OOO FREEnet Group	RU	malicious
4704	RegAsm.exe	172.67.215.62:443	caffegclasiqwp.shop	CLOUDFLARENET	US	unknown
6344	SIHClient.exe	40.127.169.103:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
6344	SIHClient.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
6344	SIHClient.exe	13.95.31.18:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted

Previous 1 2 Next 10

6. Piano di Intervento e Bonifica (Remediation)

Dato che ci troviamo di fronte a un "Loader" che ha installato software specializzato nel furto di identità e dati finanziari (Vidar e Lumma), la rimozione del solo file infetto non è sufficiente. Il team **SecureSentinels** raccomanda di seguire immediatamente i seguenti passaggi per contenere i danni e mettere in sicurezza l'ambiente.

Fase 1: Isolamento Immediato

- **Scollegare la rete:** Il computer compromesso deve essere immediatamente disconnesso da Internet e dalla rete aziendale (staccare il cavo di rete o disattivare il Wi-Fi). Questo impedisce al virus di continuare a inviare i dati rubati ai server criminali (come l'indirizzo IP in Russia `147.45.44.104`) e previene la diffusione ad altri computer.

Fase 2: Messa in Sicurezza degli Account (Cruciale)

Poiché il malware ha avuto accesso a password, cookie e file di sessione, **dobbiamo dare per scontato che tutte le credenziali salvate sul computer siano ormai in mano ai criminali**. Utilizzando un *altro dispositivo* sicuro (come uno smartphone o un computer pulito), è necessario:

- **Cambiare le password:** Modificare immediatamente le password di tutti gli account aziendali, della posta elettronica, dei servizi bancari e dei profili personali (social, Steam, ecc.).
- **Terminare le sessioni attive:** Su app come Telegram, Discord e nei browser web, utilizzare la funzione "Disconnetti tutti gli altri dispositivi" per "buttar fuori" i criminali che potrebbero star usando i "cookie" rubati per accedere senza password.
- **Mettere al sicuro le Criptovalute:** Se sul computer era presente un portafoglio digitale (Wallet), i fondi devono essere trasferiti immediatamente su un nuovo portafoglio sicuro, poiché le chiavi di accesso sono state probabilmente compromesse.
- **Attivare l'Autenticazione a Due Fattori (2FA):** Assicurarsi che ogni account importante richieda un codice sul telefono oltre alla password.

Fase 3: Bonifica del Computer (Eradicazione)

- **Formattazione (Wipe & Reimage):** Poiché i "Loader" sono progettati per nascondersi in profondità e scaricare software sempre nuovi, una semplice scansione antivirus non offre il 100% di garanzia. La procedura aziendale standard e più sicura prevede la formattazione completa del disco rigido e la reinstallazione da zero del sistema operativo (Windows).

Fase 4: Difesa della Rete Aziendale (Prevenzione)

Per proteggere il resto dell'azienda, il team IT deve configurare i sistemi di sicurezza centrali (Firewall e Antivirus di rete):

- **Blocco dei Domini:** Inserire nella "lista nera" (blacklist) aziendale tutti i siti web terminanti in `.shop` individuati dall'analisi di Lumma (es. `candedqpwqm.shop`, `caffegclasiqwp.shop`).
- **Blocco degli Indirizzi IP:** Impedire qualsiasi comunicazione verso l'indirizzo IP malevolo `147.45.44.104`.
- **Monitoraggio:** Impostare degli avvisi (alert) per rilevare se altri computer nella rete tentano di comunicare con questi stessi indirizzi.

Fase 5: Sensibilizzazione

Poiché questo tipo di minaccia entra quasi sempre attraverso email di phishing (es. finti allegati o finti aggiornamenti), raccomandiamo di inviare un breve avviso ai dipendenti ricordando di prestare la massima attenzione ai file eseguibili scaricati da internet.

7. Conclusioni

L'incidente dimostra un attacco altamente sofisticato. Se questo file fosse eseguito sul computer di un dipendente o di un utente, comporterebbe la compromissione immediata di tutte le password salvate, dei profili social, delle chat aziendali e degli eventuali asset finanziari gestiti da quel computer.