BW3- Esercizio 5

Analisi di Sicurezza - Rilevamento Malware Vidar/Lumma

Autore: Cybereagles

Sintesi

Il presente documento illustra i risultati dell'analisi di sicurezza condotta su un **file eseguibile sospetto** denominato *66bddfcb52736_vidar.exe*. L'indagine ha confermato con assoluta certezza la natura malevola del file, identificato come un loader complesso capace di introdurre nel sistema minacce di tipo stealer, specificamente **Vidar** e **Lumma**. Il test ha dimostrato l'effettivo furto di credenziali e l'elusione dei sistemi di sicurezza tramite l'iniezione in processi legittimi di sistema.

Scopo del test e analisi dello scenario

Scenario e Obiettivi

L'attività di analisi è stata eseguita all'interno di un ambiente isolato e controllato (sandbox) per prevenire qualsiasi compromissione infrastrutturale. L'obiettivo principale è documentare tecnicamente la natura della minaccia, tracciare il comportamento del malware e definire le procedure di contenimento e bonifica necessarie per mettere in sicurezza l'infrastruttura aziendale.

- **Attacker**: Infrastruttura C2 remota criminale, associata all'indirizzo IP *147.45.44.104* e al dominio *caffegclasiqwp.shop*.
- **Target**: Endpoint aziendale compromesso dall'esecuzione accidentale del file *66bddfcb52736_vidar.exe*.

Strumenti

- **ANY.RUN**: Sandbox interattiva per l'analisi dinamica del malware, utilizzata per ricavare l'indice di minaccia (score 100/100) e tracciare l'albero di esecuzione dei processi generati dal loader.

Svolgimento

Fase 1: Analisi del Vettore Iniziale e Loader

L'analisi è iniziata esaminando il comportamento del **file originale *66bddfcb52736_vidar.exe***. È stato rilevato che tale eseguibile agisce in prima istanza come un loader ("apripista"), un software specificamente progettato per eludere i controlli di sicurezza e scaricare payload secondari più pericolosi all'insaputa dell'utente. Il processo di infezione ha generato una catena di **processi figli**, tra cui l'esecuzione di utility di sistema manipolate.

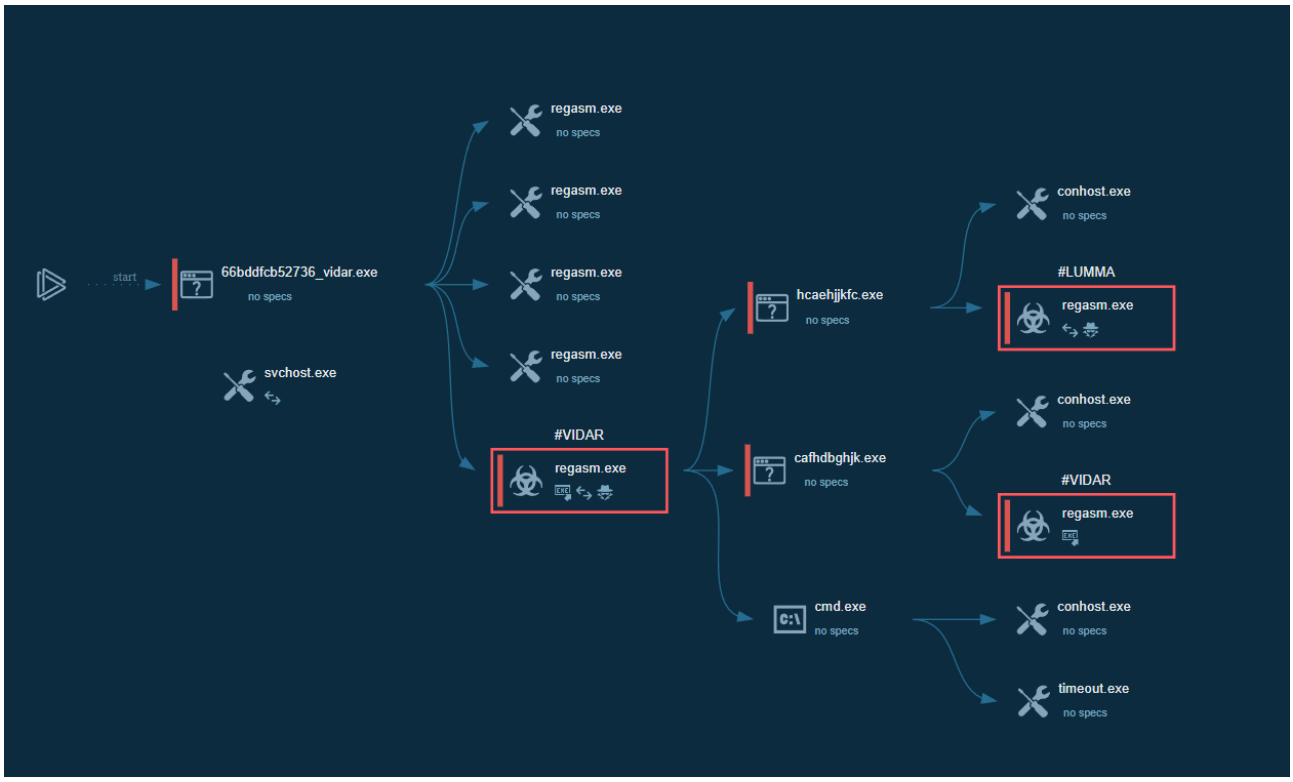
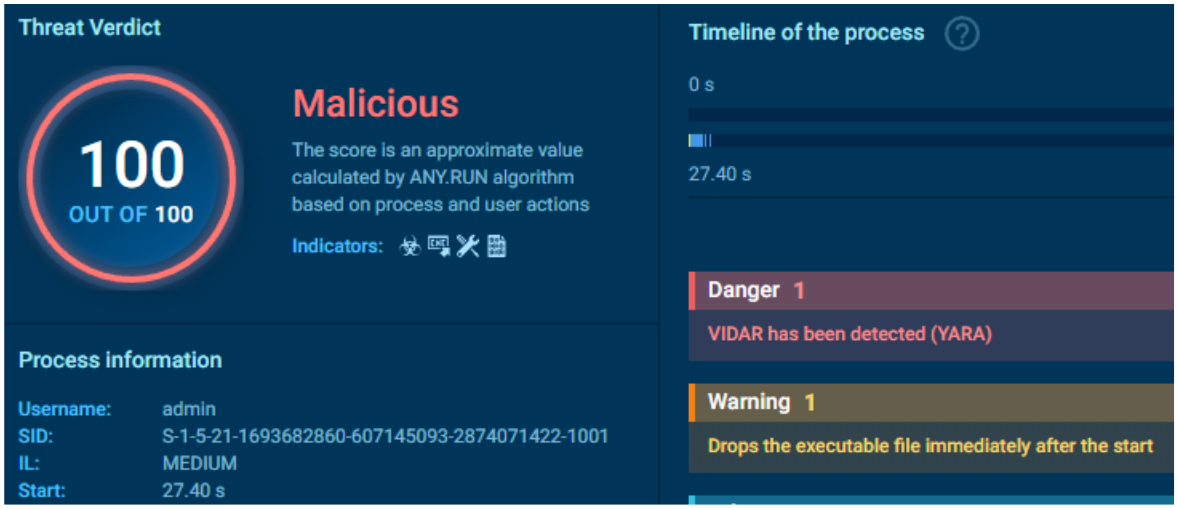


Figura 1 L'albero dei processi estratto dalla sandbox che mostra l'esecuzione del loader iniziale e la successiva generazione a cascata di processi di sistema manipolati

Fase 2: Identificazione dei Payload Stealer (Vidar e Lumma)

Durante l'analisi dinamica, è stata confermata l'introduzione nel sistema di due malware di tipo **stealer**. Il primo payload, **Vidar**, è un software noto attivo dal 2018, specializzato nel furto di informazioni sensibili e portafogli di criptovalute. Il secondo, **Lumma**, opera come *Malware-as-a-Service* sul mercato nero ed è fortemente mirato al furto di credenziali e portafogli digitali. È stato rilevato che entrambi i malware hanno applicato tecniche di **Process Injection**, iniettandosi all'interno di eseguibili legittimi di Windows, come ***regasm.exe***, per nascondere le proprie operazioni.



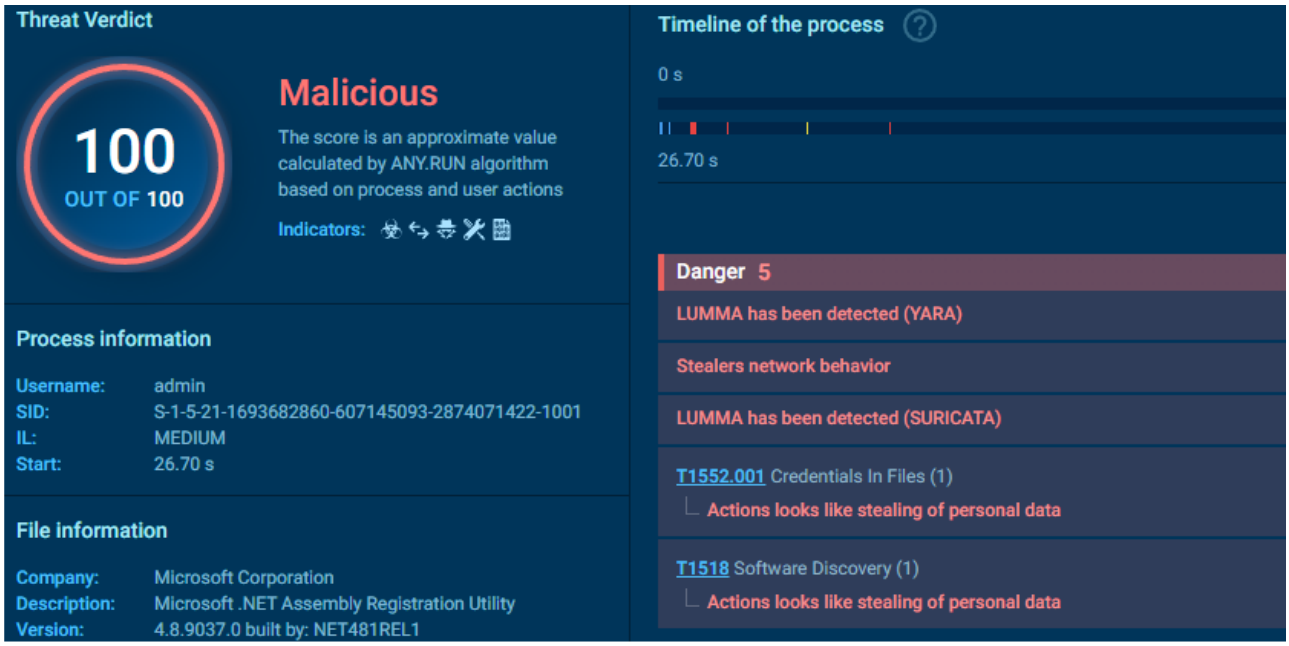


Figura 2 Interfaccia della sandbox ANY.RUN che riporta il Threat Verdict "Malicious" con score 100/100 e il rilevamento delle firme YARA per i malware Vidar e Lumma.

Fase 3: Valutazione dei Danni ed Esfiltrazione

La valutazione tecnica dell'incidente ha classificato l'evento come un **Vero Positivo (True Positive)**. È stato osservato il rilascio di file eseguibili nascosti, la lettura illecita delle impostazioni di sicurezza e la connessione a server esterni. Il **malware** ha esfiltrato attivamente dati sensibili frugando all'interno dei browser web (nello specifico Chrome), compromettendo cookie di sessione, carte di credito salvate, applicazioni di messaggistica come Telegram e credenziali di piattaforme social quali Facebook e Instagram.

Analisi Secondaria: Valutazione URL Sospetto

Analisi Dinamica

A seguito di una segnalazione collaterale, è stato ispezionato un URL con struttura di tracciamento (*https://click.convertkit-mail2.com/*...) configurato per eseguire un reindirizzamento verso la piattaforma Instagram. L'analisi interattiva è stata condotta il 25 agosto 2024 all'interno di un ambiente isolato Windows 10 Professional (build 19045, 64 bit). A differenza del vettore iniziale precedentemente esaminato, l'esecuzione di questo link non ha manifestato alcuna anomalia.

General Info

Add for printing

URL:	https://click.convertkit-mail2.com/wvuqovqrrwagh50ndddc7hnxdlxxxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2lIbnVyc2VyZWNydWl0ZXJz
Full analysis:	https://app.any.run/tasks/f1f20828-2222-46fb-a886-09f77581e67b
Verdict:	No threats detected
Analysis date:	August 25, 2024 at 22:44:49
OS:	Windows 10 Professional (build: 19045, 64 bit)
Indicators:	
MD5:	4C091A5A8C03EBC2EA267980D0DA9F8D
SHA1:	F52CB78B7F23559FFCE5D1125EFD7B399165DFFC
SHA256:	6DF8AB4ACFC5C751F09F2C8632464C8C5E6DA9D04539A69EDB0FC53CB561DFBC
SSDEEP:	3:N8UEGGy3I5lbdIJTQTT4SEfGSNscTNKdSVKBf0b/FIzfaLzw/y8aX:2UELmiTQTT4S8G+suGSgh0b/FIzAiaX

Figura 3 Schermata "General Info" del report redatto dalla piattaforma ANY.RUN che riporta i dettagli del task, l'ambiente di esecuzione e conferma il verdetto "No threats detected" per l'URL analizzato

Risultati e Comportamento Rilevato

Il sistema **ANY.RUN** ha classificato inequivocabilmente il task con l'esito **"No threats detected"** (Nessuna minaccia rilevata). L'indagine ha evidenziato i seguenti risultati:

- **Albero dei Processi**: Il lancio dell'URL ha innescato la legittima apertura dell'applicazione Google Chrome (*chrome.exe*). Non sono stati evidenziati processi malevoli (0 rilevati) né processi sospetti (0 rilevati).

Figura 4 Albero dei processi generato da ANY.RUN che mostra la normale esecuzione a cascata di chrome.exe, con i dettagli del processo che evidenziano un Threat Score pari a 0/100

- **Indicatori Comportamentali**: Il sistema ha registrato la naturale attività del browser, come la normale lettura di chiavi di registro di Microsoft Office e il caricamento di file di cache e configurazione (es. file di testo e binari nella cartella *AppData*). L'analisi comportamentale ha confermato la totale assenza di indicatori malevoli o sospetti.

- **Attività di Rete**: Sono state generate 48 connessioni TCP/UDP standard dirette esclusivamente verso domini a reputazione verificata ("whitelisted" o noti), tra cui server di infrastrutture primarie come *accounts.google.com*, *www.instagram.com*, *www.facebook.com* e servizi operati da Microsoft.

Si è concluso che l'evento rappresenta un **falso positivo**: la sessione ha tracciato una navigazione benigna, derivante con alta probabilità da una campagna di marketing (newsletter ConvertKit) legittima e indirizzata a un profilo social.

Conclusioni

L'attività di indagine ha dimostrato in modo inequivocabile che il sistema è stato vittima di un attacco reale e andato a buon fine tramite il file eseguibile, parallelamente a una segnalazione di rete risultata invece benigna. Il sistema è stato gravemente compromesso da un loader che ha introdotto con successo i noti malware **Vidar** e **Lumma**, provocando il furto accertato di credenziali e dati sensibili, eludendo le difese tramite l'iniezione in processi legittimi come *regasm.exe*. Al contrario, l'analisi secondaria condotta sull'URL sospetto ha confermato trattarsi di un **falso positivo**, riconducibile a una normale campagna di marketing senza alcun rischio per l'infrastruttura.

Si raccomandano le seguenti azioni di mitigazione per la minaccia confermata:

- **Isolamento e Quarantena**: È tassativo scollegare immediatamente l'endpoint infetto dalla rete aziendale e da internet per fermare l'esfiltrazione dei dati. Il file *66bddfcb52736_vidar.exe* deve essere messo in quarantena.
- **Blacklist degli IoC**: Inserire le regole di blocco nei firewall e nei sistemi **EDR** per l'indirizzo IP *147.45.44.104* e i domini associati come *caffegclasiqwp.shop*, tranciando definitivamente le comunicazioni con i server C2 criminali.
- **Eliminazione e Bonifica**: Si raccomanda di procedere con la formattazione (re-imaging) completa del computer colpito, essendo l'unico metodo sicuro per garantire l'eliminazione di eventuali librerie nascoste e backdoor.
- **Reset delle Credenziali**: Forzare con estrema urgenza il reset di tutte le password aziendali e personali salvate o digitate sul dispositivo compromesso, affiancando obbligatoriamente l'uso dell'**Autenticazione a Due Fattori (MFA)**.
- **Gestione Falsi Positivi**: Sebbene l'URL analizzato si sia rivelato innocuo, si consiglia di ottimizzare i filtri antispam per riconoscere preventivamente i link di tracciamento marketing, riducendo il carico di segnalazioni non malevole.