Panoramica

Malware rilevati	Vidar - Lumma
Hash MD5	FEDB687ED23F77925B35623027F799BB
Tipologia	Trojan - Stealer - loader
IP SOSPETTI	147.45.44.104
Domini SOSPETTI	caffegclasiqwp.shop
Modalità di attacco	• Utilizzo del CMD.exe; • Ricerca e modifica di File e Directory; • Ricerca e modifica delle chiavi dei registri; • Rubare coockie e credenziali; • Tecniche di occultamento di artefatti e operazioni; • Scanzione dei software di sistema/cloud; • Lettura delle informazioni di policy e sicurezza di software; • Load di altri malware, quali Lumma; • Rinominazione di processi essenziali; • Tracciamento della vittima (GetLocaleInfoW); • Raccolta informazioni OS e Hardware; • Defence evasion.
Modalità di diffusione	Phishing - Software contraffatto
Modalità di operazione	Alla sua esecuzione il malware attiva uno script che raccoglie informazioni sensibili nella cartella C:\ProgramData e le invia a un server di comando e controllo, camuffando il trasferimento come regolare traffico web, per poi eliminare ogni traccia della sua presenza.

Descrizione

Vidar

Vidar è un trojan classificato come “information stealer”, una forma di malware utilizzato per violare i sistemi informatici e rubare informazioni sensibili. Scoperto per la prima volta a dicembre 2018 e scritto in C++, si ritiene che rappresenti un’evoluzione del malware Arkei e viene impiegato per sottrarre informazioni dai sistemi infetti, effettuare screenshot, rubare criptovalute e altre attività dannose.

È probabile che il malware sia stato fabbricato da un paese di lingua russa per colpire obiettivi fuori dai territori dell’ex URSS, in quanto è programmato per fermare la propria esecuzione se rileva di essere attivo su un computer ubicato in una delle ex repubbliche sovietiche o su uno con una tastiera russa.

È un malware disponibile per l’acquisto attraverso il modello di business MaaS (Malware-as-a-Service) e può essere ottenuto sul suo ‘sito ufficiale’ per un prezzo che varia dai 250$ ai $700 in base alla versione.

Vidar ha la capacità di rubare file di testo in diversi formati, cookie e cronologia dei browser, dati provenienti da TOR, oltre a informazioni di riempimento automatico, inclusi dettagli bancari e delle carte di credito. È inoltre noto per essere in grado di sottrarre criptovalute anche da portafogli offline, mettendo in pericolo gli utenti di Litecoin, Bitcoin, Ethereum, Zcash e DashCore.

Vidar impiega nomi di dominio per localizzare server di comando e controllo (C&C), dove vengono inviati i dati rubati. Una volta raccolte tutte le informazioni mirate, il malware compila i dati e li invia a un server di controllo, per poi cancellare le tracce delle sue operazioni e rimuoversi dal sistema.

Lumma

Simile a Vidar, Lumma è anch'esso progettato per rubare informazioni, ma è generalmente considerato più recente e leggermente più specializzato nel mirare a portafogli di criptovalute. Lumma funziona in modo simile a Vidar, ma utilizza un'infrastruttura e un focus diversi, rendendolo potenzialmente un payload aggiuntivo interessante per gli attaccanti che mirano a massimizzare il furto di dati.

Lumma costituisce una minaccia rilevante per numerosi sistemi informatici, puntando a dispositivi che operano con versioni di Windows che vanno da Windows 7 fino a Windows 11. Questa elevata compatibilità permette al malware di penetrare in un'ampia gamma di sistemi, amplificando così la sua diffusione e il suo impatto potenziale.

Sebbene non ci sia necessariamente una relazione tra Vidar e Lumma, questi possono apparire insieme in una campagna poiché è prassi relativamente comune per gli attaccanti concatenare diversi info-stealer per ottenere un furto di informazioni stratificato. Osservando le richieste di rete, payload o comunicazioni C2 che coinvolgono entrambi, è probabile che l'attaccante li abbia usati nella stessa campagna per aumentare il volume o la specificità delle informazioni sottratte.

Vidar e Lumma possono infatti essere distribuiti in modo sequenziale o insieme per massimizzare l'efficienza del furto, una tattica comune negli attacchi finanziariamente motivati, in cui l'obiettivo è sfruttare il maggior numero di dati possibile da ogni infezione.

Modalità di diffusione e operazione

Vidar viene distribuito principalmente attraverso campagne di phishing, mail che contengono allegati o link apparentemente innocui, come file di aiuto Microsoft (.CHM), documenti (.DOC), o file immagine ISO. Una volta scaricato, Vidar si nasconde, come altri Trojan, in formati di file che sembrano legittimi, in particolare mascherandosi spesso all'interno di file di aiuto Windows (.CHM), rendendo difficile per le vittime e per i software di sicurezza individuare immediatamente la presenza del file sospetto.

Quando la vittima apre il file infetto, mette in funzione un piccolo script (solitamente in JavaScript) che avvia il malware senza destare sospetti. Una volta attivo, il malware crea una cartella all'interno della directory C:\ProgramData del sistema, dove raccoglie una grande quantità di informazioni sensibili quali credenziali di accesso, dati bancari, informazioni di navigazione come cookie e sessioni di autenticazione, dati di portafogli di criptovalute.

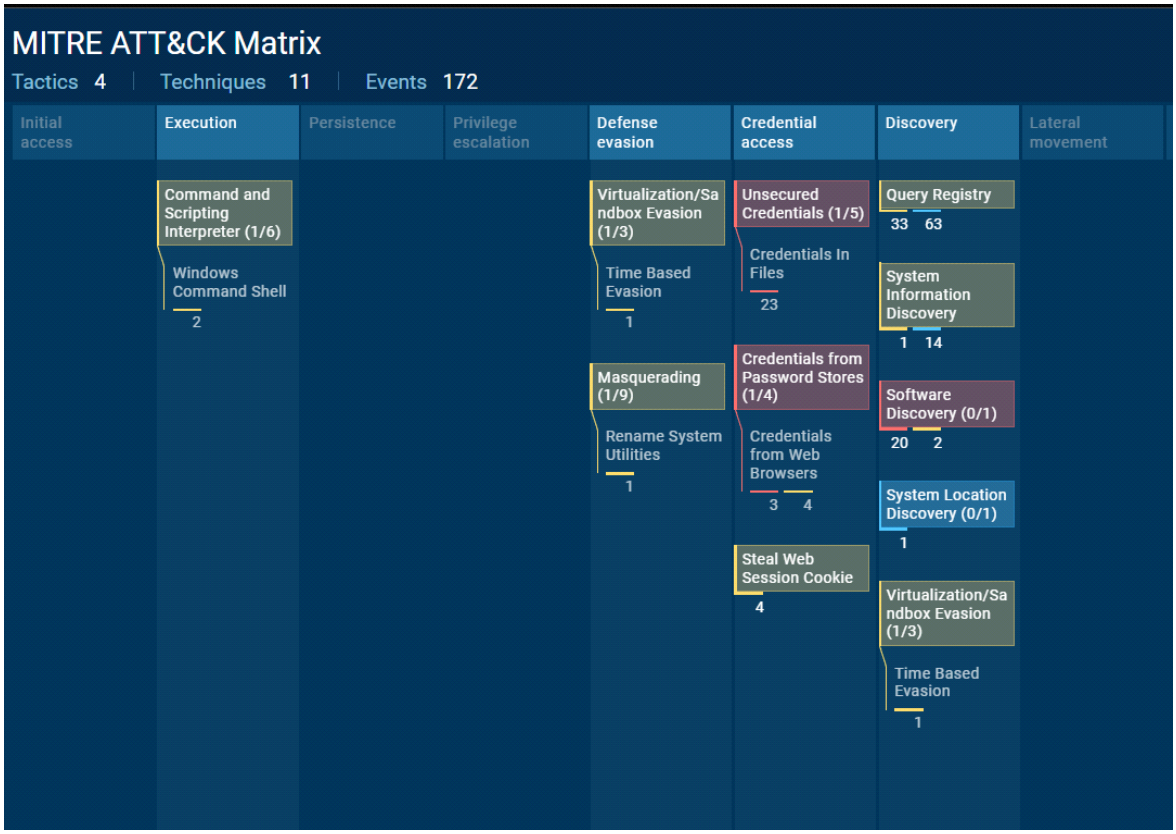
Terminata la raccolta, il malware invia i dati a un server di comando e controllo, da cui gli attaccanti ricevono e analizzano le informazioni rubate. Il trasferimento di dati è camuffato da regolare traffico web, in modo che le attività sospette non siano facilmente rilevabili.

Vidar è inoltre progettato per estendere il livello di compromissione, scaricando altri malware e aggiungendo così nuove minacce, ampliando le possibilità di accesso degli attaccanti, .

Una volta completate le sue operazione, Vidar cancella tutte le tracce che potrebbero far scoprire la sua presenza, eliminando i file temporanei che ha creato, rimuovendo le DLL utilizzate e svuotando la cartella ProgramData, rendendo così la sua scoperta molto difficile.

Analisi con MITRE ATT&CK

Il MITRE ATT&CK è un framework che fornisce una comprensione dettagliata delle tattiche e tecniche utilizzate dai cyber attaccanti. Suddiviso in categorie, vengono identificate le tattiche, che rappresentano gli obiettivi generali degli attaccanti, e sotto di queste le tecniche specifiche utilizzate per raggiungere quegli obiettivi.



Di seguito sono brevemente mostrare le tattiche utilizzate dal file analizzato:

Execution

Command and Scripting Interpreter

Gli avversari possono sfruttare interpreti di comandi e script per eseguire comandi, script o binari su diverse piattaforme. In particolare, il Command Shell di Windows permette di controllare vari aspetti del sistema e può essere invocato da remoto. I file batch possono automatizzare l'esecuzione di comandi ripetitivi. Gli avversari utilizzano queste tecniche per eseguire payload e comandi in modo interattivo.

- PID 6284 cmd.exe: utilizza TIMEOUT.EXE per ritardare l'esecuzione.
- PID 6908 RegAsm.exe: inizia CMD.EXE per l'esecuzione di comandi.

Defence Evasion

Virtualization/Sandbox Evasion

Per evitare l'analisi in ambienti virtualizzati o sandbox, gli avversari possono alterare il comportamento del loro malware in base alla rilevazione di indizi che indicano un ambiente virtuale. Se rilevano un ambiente virtuale, possono modificare il malware per disattivarsi o nascondere le sue funzioni principali. In particolare, le tecniche di evasione basate sul tempo ("time-based evasion") consentono agli avversari di evitare ambienti di virtualizzazione e analisi rilevando caratteristiche temporali del sistema, come il tempo di attività o l'orologio di sistema.

- PID 6908 RegAsm.exe: rileva la data dell'installazione Windows.

Masquerading

Gli avversari possono manipolare le caratteristiche dei loro artefatti per farli apparire legittimi. Questo può includere la modifica dei metadati dei file, la manipolazione dei nomi di file e l'uso di nomi di servizi legittimi. Una tecnica specifica consiste nel copiare o spostare un'utility legittima in una directory diversa, rinominandola per evitare rilevamenti basati su percorsi non standard di esecuzione delle utility di sistema.

- PID 6908 RegAsm.exe: il processo elimina (drops) l'eseguibile legittimo di Windows.

Credential Access

Unsecured Credentials

Gli avversari possono cercare credenziali memorizzate in modo insicuro in vari luoghi, come file di testo in chiaro o registri di sistema. Le credenziali possono anche trovarsi in repository specifici delle applicazioni.

- PID 4704/6908 RegAsm.exe: le azioni condotte sembrano rubare dati personali.
- PID 6908: RegAsm.exe: ruba credenziali dal web browser.

Credentials from Password Stores

Possono cercare in posizioni comuni di memorizzazione delle password per ottenere credenziali degli utenti. Una volta ottenute, queste credenziali possono essere utilizzate per il movimento laterale e l'accesso a informazioni riservate.

- PID 6908: RegAsm.exe: ruba credenziali dal web browser.
- PID 6908: RegAsm.exe: il processo elimina i file DLL di Mozilla.

Steal Web Session Cookie

Gli avversari possono rubare i cookie di sessione delle applicazioni web per accedere a servizi come utenti autenticati, senza la necessità di credenziali. I cookie di sessione possono essere trovati su disco, nella memoria dei processi del browser e nel traffico di rete. L'acquisizione di un cookie valido consente di bypassare alcuni protocolli di autenticazione a più fattori.

- PID 6908: RegAsm.exe: il processo elimina i file DLL di Mozilla.

Discovery

Query Registry

Gli avversari possono interagire con il Registro di Windows per raccogliere informazioni sul sistema, la configurazione e il software installato, e utilizzarle per pianificare azioni successive.

- PID 4704/6908 RegAsm.exe: ricerca il software installato.
- PID 6908: RegAsm.exe: rileva la data dell'installazione Windows.
- PID 6908: RegAsm.exe: controlla le impostazioni di attendibilità di Windows (trust settings).
- PID 6908: RegAsm.exe: legge le impostazioni di sicurezza di Internet Explorer.

System Information Discovery

Gli avversari possono cercare informazioni dettagliate sul sistema operativo e sull'hardware, incluse versioni e aggiornamenti. Utilizzando strumenti come Systeminfo, possono raccogliere dati dettagliati.

- PID 6908: RegAsm.exe: rileva la data dell'installazione Windows.

Software Discovery

Gli avversari possono tentare di ottenere un elenco di software installato per identificare misure di sicurezza o vulnerabilità.

- PID 4704/6908 RegAsm.exe: ricerca il software installato.
- PID 4704/6908 RegAsm.exe: le azioni condotte sembrano rubare dati personali.

System Location Discovery

Gli avversari possono raccogliere informazioni per calcolare la posizione geografica di un host vittima, utilizzando controlli di sistema come fuso orario e impostazioni della tastiera.

- PID 6908 RegAsm.exe: controlla le impostazioni della posizione del computer.

Remediation

A seguito di una analisi e uno studio dei report, riteniamo sia "necessario" lo spegnimento della macchina infetta, in quanto sono stati rilevati una serie di processi malevoli che denotano la presenza di un Malware dalle molteplici funzioni.

Abbiamo compreso che questo attacco sta raccogliendo un notevole numero di informazioni all'interno del sistema infetto, con l'obbiettivo di inviare questi dati verso l'esterno. Si sottolinea come la tipologia di questi dati estratti, non si limiti ad una scansione dei vari componenti del sistema e dei suoi software, ma anche ad un tentativo di impadronirsi di credenziali e cookie utente, allo scopo di rubare sessioni su eventuali Web App in collegamento e di rafforzare la presenza del malintenzionato all'interno del sistema, qual'ora decida di portare avanti l'attacco.

Ove non fosse possibile lo spegnimento della macchina, si suggerisce almeno di interrompere la connessione alla rete, cosi che le informazioni estratte non trapelino al di fuori dell'azienda.

In materia di sicurezza aziendale, si suggerisce l'inserimento di regole firewall che applichino un divieto di accesso agli IP:

- 147.45.44.104: ritenuto l'IP dell'attaccante dal quale si nota un traffico sospetto in entrata e uscita.
- 172.67.215.62 e 104.21.16.180: da una prima analisi sembra che questi IP siano appartententi ad un DNS denominato "caffegclasiqwp.shop" dal quale si sospetta provenga il Malware.

Successive linee guida e policy aziendali applicabili allo scopo di evitare ulteriori eventi analoghi:

Formazione degli utenti

Per prevenire attacchi derivanti da campagne di phishing, è fondamentale che ogni dipendente sia consapevole delle minacce e delle strategie che i cybercriminali utilizzano. Un ottimo punto di partenza sono delle campagne di sensibilizzazione, che possono includere corsi di formazione in cui i dipendenti apprendono come riconoscere le e-mail fraudolente, i link sospetti e le pratiche di phishing comuni.

Eseguire simulazioni periodiche di phishing è un modo molto efficace per testare e rinforzare la preparazione degli utenti. Queste simulazioni consentono ai dipendenti di fare pratica su come gestire messaggi ingannevoli, e i risultati possono rivelare quali aree richiedono ulteriore formazione.

Infine, potrebbe essere fondamentale fornire agli utenti un metodo semplice per segnalare e-mail sospette, come un indirizzo e-mail dedicato per segnalare potenziali minacce o un pulsante integrato nel client di posta che permetta di contrassegnare le e-mail come pericolose, di modo da permettere all'intero team di contribuire attivamente alla sicurezza aziendale.

Protezione antivirus e aggiornamenti di sistema

È sempre necessario utilizzare una protezione antivirus efficace, che includa strumenti di rilevamento avanzato come l'analisi del comportamento del malware, la quale permette di identificare minacce anche prima che siano pienamente operative. Mantenere aggiornati tutti i sistemi è essenziale: impostare aggiornamenti automatici per tutte le applicazioni e i sistemi operativi garantisce che non ci siano vulnerabilità sfruttabili.

Una strategia di sicurezza particolarmente utile è quella della "whitelist", ossia il limitare l'esecuzione del software solo alle applicazioni approvate dall'amministratore. Questa misura riduce le probabilità che programmi non autorizzati possano essere eseguiti o installati nel sistema, aumentando la sicurezza complessiva.

Restrizioni sui privilegi utente

In linea con il principio del 'least privilege', è importante assicurarsi che ogni dipendente possa accedere solo ai dati e alle applicazioni necessari allo svolgimento del proprio lavoro, riducendo così i rischi in caso di compromissione. Per gli utenti con privilegi più elevati, come gli amministratori, si può considerare l'implementazione dell'autenticazione multi-fattore (MFA), che aggiunge un ulteriore livello di sicurezza contro accessi non autorizzati.

Un altro passo da considerare è stabilire delle policy per controllare l'accesso e l'uso dei dati sensibili. Queste policy possono limitare l'accesso a dati critici solo agli utenti autorizzati, e prevedere controlli per registrare tutte le operazioni effettuate. In caso di incidenti, questo controllo aiuta a ricostruire cosa è successo e riduce il rischio di esfiltrazione di informazioni sensibili.

Monitoraggio delle connessioni di rete e del traffico anomalo

Il malware è progettato per comunicare con i suoi server di comando e controllo (C2) e inviare informazioni sensibili rubate. L'implementazione di sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) aiuta a identificare e bloccare connessioni anomale e attività sospette prima che causino danni.

Limitare l'accesso ai dispositivi di rete critici, monitorare le connessioni verso server esterni e bloccare automaticamente indirizzi IP sospetti sono misure che rendono più difficile esfiltrare dati. Inoltre, un'analisi regolare dei log di sistema e di rete può rilevare comunicazioni non autorizzate.

Analisi periodiche, backup e procedure di ripristino

Scansioni di sicurezza frequenti sono essenziali per rilevare e rimuovere eventuali minacce. È consigliabile eseguire queste scansioni su tutti i dispositivi e le reti aziendali, monitorando non solo i file ma anche i processi in esecuzione.

Avere backup regolari e completi di tutti i dati critici è indispensabile: questi backup dovrebbero essere conservati su server esterni, protetti e separati dal sistema principale, per prevenire corruzioni o accessi indesiderati in caso di attacco. È importante inoltre verificare regolarmente l'integrità dei backup, per assicurarsi che siano utilizzabili in caso di necessità.

Infine, un piano di ripristino aggiornato permette di recuperare rapidamente i dati compromessi e tornare operativi con il minimo impatto. Mantenere anche versioni precedenti dei documenti e dei file permette di recuperare dati specifici anche in situazioni critiche, garantendo la sicurezza e la continuità operativa dell'azienda.