Build Week 3

Esercizio 5

LANDA

TRACKER SPA

Studiare questi link di anyrun e spiegare queste minacce in un piccolo report.

- *https://app.any.run/tasks/371957e1-d960-4b8a-8c68-241ff918517d/*
- *https://app.any.run/tasks/f1f20828-2222-46fb-a886-09f77581e67b/*

Come output vorrei la spiegazione in italiano per un eventuale cliente / manager (che è poco preparato sulla materia) di questi malware (o presunti tali).
Indicare le vostre scelte di remediation (mettere in quarantena, eliminare, blacklist, falso positivo, falso negativo, vero positivo, vero negativo, chiedo al vendor, ecc.) motivandole.

REPORT TECNICO

Report di Analisi di Sicurezza Informatica
Oggetto: Analisi e Piano di Risposta per Minacce Malware Complesse Identificate

1. Sommario Esecutivo

In data odierna è stata completata l'analisi di un campione di software sospetto. I risultati confermano che il file iniziale agisce come un **"dropper"**, ovvero un contenitore progettato per installare ed eseguire **molteplici minacce complesse**. Nello specifico, un singolo file ha installato due varianti distinte di malware **"InfoStealer"**: **Vidar** e **Lumma**.
L'obiettivo di queste minacce è l'estrazione e l'esfiltrazione di dati sensibili. L'analisi comportamentale ha inoltre rivelato l'uso di **tecniche avanzate di evasione** per eludere i sistemi di sicurezza e un meccanismo di **auto-distruzione** per occultare le proprie tracce.
Il livello di rischio associato a questa infezione composita è **CRITICO**. Tutte le rilevazioni sono classificate come **Veri Positivi**.

2. Analisi Comportamentale del malware

L'analisi dell'esecuzione del malware in un ambiente controllato ha fornito dettagli cruciali sulla sua metodologia operativa, come evidenziato dalle immagini del flusso dei processi allegate:

- **Vettore di Infezione Complesso**: Il file iniziale (**66bddfcb52736_vidar.exe**) non è la minaccia finale, ma un veicolo di infezione. La sua esecuzione ha dato il via a una catena di eventi che ha portato all'installazione e all'avvio di due payload malevoli distinti, identificati come Vidar e Lumma.

Nello specifico, ha avviato due eseguibili distinti con nomi casuali:

  - **HCAEHJJKFC.exe**, identificato come payload **Vidar**.
  - **CAFHD8GHJK.exe**, identificato come payload **Lumma**.

- **Tecnica di Evasione ("Living off the Land")**: Il dropper non avvia direttamente i malware. Sfrutta invece un processo di sistema legittimo di Windows, **RegAsm.exe**, per eseguire i suoi componenti malevoli. Questa tecnica (nota come Process Hollowing o Injection) è progettata per mascherare le attività dannose facendole apparire come operazioni di un programma di sistema attendibile, eludendo così antivirus e sistemi di monitoraggio di base.

- **Conferma del Meccanismo di Auto-distruzione**: È stato intercettato il comando esatto (*cmd.exe /c timeout /t 10 & rd /s /q ...*) utilizzato dal malware per la rimozione dei propri file e directory dalla cartella *C:\ProgramData* dopo un'attesa di 10 secondi. Questo conferma la volontà di eliminare le tracce per rendere più difficile l'analisi forense post-incidente.

3. Funzionamento dei Payload Rilasciati (Vidar e Lumma)

Una volta attivati tramite RegAsm.exe, i payload Vidar e Lumma operano in parallelo per:

- **Raccolta Dati di Sistema**: Eseguire una profilazione completa del sistema infetto (hardware, software, utente).
- **Estrazione di Dati Sensibili**: Ricercare ed estrarre credenziali da browser, portafogli di criptovalute e dati da applicazioni come Telegram e Discord.
- **Acquisizione Schermo**: Catturare screenshot del desktop dell'utente.
- **Esfiltrazione e Occultamento**: Inviare i dati rubati ai rispettivi server di Comando e Controllo (C2) e, come confermato, tentare di cancellare le prove della loro presenza.

Programma 1: Vidar (InfoStealer)

Questo eseguibile è una variante del malware **Vidar**, un potente "information stealer" (ladro di informazioni). Il suo obiettivo principale è raccogliere quante più informazioni sensibili possibili dal computer della vittima e inviarle a un operatore malintenzionato.
L'analisi delle stringhe ci rivela le sue capacità e il suo modus operandi in diverse fasi.

Fase 1: Preparazione e Raccolta Informazioni sul Sistema

Il malware inizia a "profilare" il sistema infetto per raccogliere dati di base e prepararsi al furto vero e proprio.

- **Raccolta Informazioni di Base:**
  - Usa funzioni come *GetComputerNameA*, *GetUserNameA*, *GetSystemInfo*, *GlobalMemoryStatusEx*, *GetSystemPowerStatus* per ottenere il nome del computer, il nome utente, i dettagli sull'hardware (CPU, RAM), e lo stato dell'alimentazione.
  - Identifica la versione di Windows e l'architettura (x32/x64) leggendo la chiave di registro *SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion*.
  - Recupera informazioni sulla lingua e la localizzazione con *GetUserDefaultLangID* e *GetLocaleInfoA*.
  - Enumera i processi in esecuzione con **CreateToolhelp32Snapshot** e **Process32Next** per avere una mappa dei software attivi.
  - Colleziona la lista dei programmi installati cercando la chiave *SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall*.

- **Tecniche di Evasione:** Il malware cerca di capire se è in esecuzione in un ambiente di analisi (sandbox o macchina virtuale). Le stringhe **VMwareVMware**, **HAL9TH**, e **JohnDoe** sono nomi comuni usati in ambienti di test; se li rileva, potrebbe terminare la sua esecuzione per non essere analizzato.

Fase 2: Furto di Dati Sensibili

Questa è la fase principale, in cui Vidar cerca e ruba dati da una vasta gamma di applicazioni.

- **Browser (Chrome, Firefox, Opera, etc.):**
  - **Credenziali di accesso**: Utilizza comandi SQL come *SELECT origin_url, username_value, password_value FROM logins* per estrarre URL, username e password salvate dai file di database dei browser (Login Data).
  - **Cookie di sessione**: Esegue la query *SELECT HOST_KEY, ... name, encrypted_value from cookies* per rubare i cookie. Questi possono essere usati per bypassare l'autenticazione a due fattori e accedere agli account della vittima.
  - **Carte di Credito**: Con la query *SELECT name_on_card, ... card_number_encrypted FROM credit_cards* ruba i dati delle carte di credito salvate.
  - **Cronologia e Dati di Autocompilazione**: Ruba la cronologia di navigazione *SELECT url FROM urls LIMIT 1000* e i dati di autocompilazione *SELECT name, value FROM autofill*.
  - **Decriptazione**: Per decifrare i dati rubati dai browser basati su Chromium, usa la funzione **CryptUnprotectData**. Per Firefox, carica le librerie nss3.dll e usa funzioni specifiche come NSS_Init e PK11SDR_Decrypt per decifrare le password dal suo database.
- **Wallet di Criptovalute**: La stringa **Wallets** indica che il malware ha una funzionalità dedicata a cercare file di portafogli di criptovalute (come wallet.dat) in percorsi predefiniti.
- **Applicazioni di Messaggistica**:
  - **Telegram**: Cerca la cartella "*\Telegram Desktop*" e file di sessione specifici (D877F783D5D3EF8C*, map*) per rubare la sessione attiva.
  - **Discord**: Cerca token di autenticazione nei percorsi di Discord *(\discord\Local Storage\leveldb*) e li salva in **tokens.txt**.
  - **Pidgin**: Cerca il file accounts.xml nella cartella *\.purple* per estrarre le credenziali degli account configurati.
  - **Outlook**: Ispeziona diverse chiavi di registro di Microsoft Office per trovare e rubare le configurazioni degli account email.
- **Credenziali di Steam**:
  - Localizza l'installazione di Steam tramite la chiave di registro *Software\\Valve\\Steam*.
  - Cerca e ruba file cruciali dalla cartella config, come **loginusers.vdf**, **config.vdf**, e soprattutto i file ssfn* che sono legati all'autenticazione di Steam Guard.
- **Furto di File Generici**:
  - Il malware cerca file con estensioni specifiche (es. *.txt, *.ini) in cartelle critiche come *Desktop*, *Documents*, e *AppData* (%DESKTOP%, %DOCUMENTS%, %APPDATA%).

Fase 3: Funzionalità Aggiuntive

- **Screenshot**: Utilizza una serie di funzioni GDI (CreateCompatibleDC, BitBlt) e GDI+ (GdipSaveImageToStream) per catturare uno screenshot del desktop della vittima e salvarlo come screenshot.jpg.

Fase 4: Esfiltrazione dei Dati e Auto-distruzione

Una volta raccolti tutti i dati, il malware li comprime e li invia al server di Comando e Controllo (C2).

- **Comunicazione C2**:
  - **L'indirizzo C2**: "*https://t.me/pech0nk*" indica che i dati rubati vengono inviati a un canale/bot Telegram. Questo è un metodo comune perché è difficile da bloccare e non richiede un'infrastruttura di server complessa per l'attaccante.
  - **Utilizza richieste HTTP POST** (Content-Type: multipart/form-data) per caricare i dati rubati, inclusi l'ID univoco della vittima (hwid), il file dello screenshot e un archivio con tutti gli altri dati.
- **Auto-distruzione**:
  - La stringa */c timeout /t 5 & del /f /q \"...\" & del \"C:\\ProgramData*.dll\"\" & exit* mostra un comando che viene eseguito per cancellare l'eseguibile del malware e le DLL ausiliarie dopo 5 secondi, nel tentativo di rimuovere le proprie tracce.

Programma 2: Vidar (InfoStealer)

Questo secondo programma è **un'altra variante di Vidar**, quasi identica alla prima. Le sue funzionalità, obiettivi e metodi sono gli stessi.

Analizziamone le piccole ma significative differenze.

- **Funzionalità Principali** (Identiche al Programma 1):
  - **Raccoglie** le stesse informazioni di sistema (nome utente, hardware, software installati).
  - **Ruba** credenziali, cookie, carte di credito e cronologia dai medesimi browser (Chrome, Firefox, Opera).
  - **Prende di mira** le stesse applicazioni: Steam, Telegram, Discord, Outlook, e Pidgin.
  - È in grado di **catturare** screenshot del desktop.
  - **Utilizza** le stesse tecniche di auto-distruzione per cancellare le proprie tracce dopo aver completato il furto.
- **Differenze Notate**:
  - **Comando e Controllo (C2)**: L'indirizzo C2 è diverso: https://t.me/jamelwt. Questo significa che, pur essendo lo stesso tipo di malware, è controllato da un operatore/gruppo diverso o fa parte di una campagna differente.
  - **Assenza di Stringhe Anti-VM Esplicite:** Nell'elenco fornito, manca la stringa VMwareVMware. Questo non significa che non abbia controlli anti-analisi, ma solo che quella specifica stringa non è presente. Potrebbe usare altri metodi più sottili (come NtQueryInformationProcess) per rilevare ambienti di debug.

In sintesi, si tratta della stessa minaccia, configurata per inviare i dati rubati a un altro criminale.

Programma 3: Lumma (InfoStealer)

Questo terzo campione è stato identificato come **Lumma Stealer**, un altro malware "ladro di informazioni" molto diffuso e venduto nei forum underground. A differenza dei campioni di Vidar, qui non abbiamo le stringhe dettagliate delle sue azioni, ma un'informazione altrettanto cruciale: la sua infrastruttura di Comando e Controllo (C2).

Analisi del Comando e Controllo (C2)

L'elemento chiave di questo campione è la lista di domini C2:

- condedqpwqm.shop
- stagedchheiqwo.shop
- traineiwnqo.shop
- locatedblsoqp.shop
- caffegclasiqwp.shop
- evoliutwoqm.shop
- millyscroqwp.shop
- stamppreewntnq.shop

Questo ci dice molto su come opera:

- **Infrastruttura Robusta con Fallback**: Il malware non si affida a un singolo dominio, ma a una lista di domini di backup. Tenterà di connettersi al primo della lista; se non riceve risposta (perché è stato bloccato o è offline), passerà al secondo, e così via. Questo lo rende molto più resistente ai tentativi di smantellamento da parte delle forze dell'ordine e delle società di sicurezza.
- **Domini Pseudo-Casuali**: I nomi dei domini (condedqpwqm, stagedchheiqwo) sono generati casualmente o tramite un algoritmo (DGA - Domain Generation Algorithm). Questo rende difficile per gli analisti prevedere e bloccare i futuri domini C2.
- **Top-Level Domain (TLD) a Basso Costo**: L'uso del TLD .shop è comune per le attività malevole, poiché questi domini sono economici e facili da registrare in modo anonimo.

Capacità Inferite (Comportamento Tipico di Lumma)

Anche senza le stringhe, sapendo che si tratta di Lumma, possiamo dedurre con alta probabilità le sue capacità, che sono molto simili a quelle di Vidar essendo eseguiti insieme:

- **Furto di Dati dai Browser**: Ruba password, cookie, dati di autocompilazione e carte di credito da decine di browser basati su Chromium e Firefox.
- **Furto di Wallet di Criptovalute**: È specializzato nel cercare estensioni di browser per wallet (come MetaMask, Phantom, TronLink) e applicazioni desktop di wallet.
- **Raccolta di Informazioni di Sistema**: Raccoglie dettagli completi su hardware, software e configurazione di rete della vittima.
- **Furto di Sessioni di Applicazioni**: Come Vidar, può rubare file di sessione da **Telegram** e token da **Discord**.

In conclusione, questo campione di Lumma è configurato per comunicare con una rete di server C2 resiliente, da cui riceverà istruzioni e a cui invierà i dati rubati dal computer della vittima.

REPORT PER MANAGER - PRIMA ANALISI

Report di Analisi di Sicurezza Informatica
Oggetto: Analisi e Piano di Risposta per Minacce Malware Identificate

1. Sommario Esecutivo

In data odierna è stata completata l'analisi di tre campioni di software sospetto. I risultati confermano che tutti e tre i campioni sono malware attivi della categoria "InfoStealer" (sottrattori di informazioni). Nello specifico, sono state identificate due varianti del malware Vidar e una del malware Lumma.
L'obiettivo primario di queste minacce è l'estrazione e l'esfiltrazione di dati sensibili dai sistemi compromessi, incluse credenziali di accesso, informazioni finanziarie e dati relativi ad applicazioni aziendali e personali. Il livello di rischio associato a queste minacce è da considerarsi ALTO. Tutte le rilevazioni sono classificate come Veri Positivi.

2. Analisi dei Campioni 1 e 2 (Malware: Vidar)

2.1. Funzionamento e Impatto Operativo

Il malware Vidar opera secondo una sequenza definita per massimizzare la raccolta di dati:

- **Raccolta Dati di Sistema**: In fase iniziale, il malware esegue una profilazione completa del sistema infetto, raccogliendo informazioni su hardware, versione del sistema operativo, software installato e dettagli dell'utente.
- **Estrazione di Dati Sensibili**: Successivamente, procede alla ricerca e all'estrazione mirata di un'ampia gamma di informazioni, tra cui:
  - **Credenziali dei Browser**: Username, password, cookie di sessione e dati di carte di credito salvati in browser come Chrome, Firefox e Opera.
  - **Portafogli di Criptovalute**: File associati a wallet di valute digitali.
  - **Dati di Applicazioni**: Token di autenticazione e file di sessione di software come Telegram, Discord e Steam.
- **Acquisizione Schermo**: Il malware è dotato della funzionalità di catturare uno screenshot del desktop dell'utente al momento dell'esecuzione.
- **Esfiltrazione e Occultamento**: Tutti i dati raccolti vengono aggregati, compressi e inviati a un server di Comando e Controllo (C2) gestito dall'attaccante tramite la piattaforma Telegram. Al termine dell'operazione, il malware tenta di eliminare le proprie tracce dal sistema.

2.2. Rischio Aziendale

L'infezione da Vidar espone l'organizzazione a rischi significativi, quali:

- **Accesso non autorizzato** a sistemi e dati aziendali.
- **Frodi finanziarie** a danno dell'azienda o dei dipendenti.
- **Violazione dei dati** (Data Breach) con conseguenti impatti legali e reputazionali.
- **Compromissione di account** strategici e potenziale **spionaggio industriale**.

2.3. Piano di Remediation

- **Classificazione**: Vero Positivo. La natura malevola è confermata con certezza.
- **Azioni Raccomandate**:
  - **Quarantena** (Contenimento Immediato): Isolare il file sui sistemi interessati per bloccarne immediatamente l'esecuzione e prevenire la propagazione.
  - **Blacklist** (Prevenzione Proattiva): Inserire l'hash del file nelle blacklist dei sistemi di sicurezza (EDR, Antivirus). Bloccare a livello perimetrale (Firewall/Proxy) gli URL di C2 identificati (t.me/pech0nk, t.me/jamelwt) per inibire ogni comunicazione.
  - **Eliminazione** (Bonifica): Procedere con la rimozione sicura e definitiva del file dai sistemi infetti.

3. Analisi del Campione 3 (Malware: Lumma)

3.1. Funzionamento e Impatto Operativo

Il malware Lumma condivide gli stessi obiettivi di Vidar, specializzandosi nel furto di credenziali.
L'analisi di questo campione ha rivelato una caratteristica distintiva: un'infrastruttura di Comando e Controllo (C2) altamente resiliente.
Il malware non dipende da un singolo server, ma utilizza una lista di domini di backup.
Se un dominio risulta irraggiungibile o viene bloccato, il malware tenta sequenzialmente di connettersi ai domini successivi della lista, garantendo così la continuità operativa e rendendo più complesse le operazioni di contrasto.

3.2. Rischio Aziendale

Il rischio è ALTO e analogo a quello di Vidar. La resilienza dell'infrastruttura C2 rende Lumma una minaccia persistente e più difficile da neutralizzare completamente solo tramite il blocco di un singolo indicatore di rete.

3.3. Piano di Remediation

- **Classificazione**: Vero Positivo. I tentativi di connessione verso infrastrutture note per attività malevole ne confermano la natura.
- **Azioni Raccomandate**:
  - **Blacklist** (Contenimento di Rete - Priorità Massima): L'azione più urgente è il blocco immediato di tutti i domini C2 identificati a livello di firewall e proxy aziendale. Questa azione previene l'esfiltrazione dei dati anche da host non ancora identificati come infetti.
  - **Scansione e Identificazione**: Avviare una scansione della rete per identificare tutti gli host che tentano di stabilire connessioni verso i domini inseriti in blacklist.
  - **Quarantena ed Eliminazione**: Una volta identificati gli host infetti, applicare le procedure di contenimento e bonifica descritte per il malware Vidar.

4. Raccomandazioni Strategiche e Prossimi Passi

Si raccomanda di procedere con l'approvazione e l'esecuzione immediata delle seguenti azioni:

- **Implementare il Piano di Remediation** come descritto per tutti e tre i campioni.
- **Eseguire la bonifica completa** dei sistemi compromessi. Si consiglia vivamente il re-imaging (formattazione e reinstallazione) delle macchine per garantire la rimozione di ogni possibile persistenza.
- **Imporre un reset obbligatorio delle password** per tutti gli account utilizzati dagli utenti dei sistemi infetti.
- **Condurre un'analisi della causa radice** (Root Cause Analysis) per determinare il vettore di infezione iniziale (es. email di phishing, download non sicuro) e rafforzare le difese corrispondenti.

REPORT PER MANAGER - SECONDA ANALISI

1. Sommario Esecutivo

Il presente report descrive i risultati dell'analisi di sicurezza condotta sul file indicato in oggetto.
A seguito di un'indagine approfondita, il file è stato classificato come **Vero Negativo**. Non sono state identificate minacce attive e non sono richieste ulteriori azioni di remediation.

2. Dettagli dell'Analisi

L'analisi iniziale del file non ha evidenziato indicatori di compromissione diretti. L'unico elemento che ha richiesto un'indagine supplementare è stata un'attività di rete specifica, associata a un link rilevato nel processo con **PID 6584**.
Il link in questione era il seguente: *https://click.convertkit-mail2.com/[...]*
Le nostre verifiche hanno confermato che l'URL è un link di tracciamento gestito da **ConvertKit**, una piattaforma di email marketing legittima e ampiamente diffusa.

3. Funzionamento del Link

Il comportamento del link è risultato essere una pratica di marketing standard e non malevola, articolata in due fasi:

- **Tracciamento**: Al momento del clic, la richiesta viene prima instradata ai server di ConvertKit. Questo permette al mittente della comunicazione di registrare l'interazione per misurare l'efficacia della campagna (es. numero di clic).
- **Reindirizzamento**: Immediatamente dopo la registrazione del clic, il sistema reindirizza l'utente alla destinazione finale. Nel caso specifico, la pagina Instagram pubblica: https://www.instagram.com/aussienurserecruiters/.

4. Remediation Activities

- **Formazione Dipendenti**

Corso obbligatorio su gestione link esterni e riconoscimento phishing
Training specifico sui rischi dei social network in ambiente lavorativo
Sessione di formazione sulla verifica delle email interne e tecniche di spoofing

- **Policy Aziendali**

Implementazione policy di blocco social network non autorizzati durante orario lavorativo
Definizione whitelist per ruoli che necessitano accesso social (Marketing, HR, Comunicazione)
Procedura obbligatoria di verifica link sospetti prima del click

- **Controlli Tecnici**

Attivazione banner di warning per tutti i link esterni
Implementazione filtri URL avanzati a livello firewall
Configurazione sandbox per analisi automatica link sospetti

- **Awareness Continua**

Campagne di phishing simulato mensili
Reminder periodici sulle best practice di sicurezza
Processo semplificato per segnalazione email sospette al SOC

5. Conclusione

L'utilizzo di questo tipo di link è una pratica comune e legittima nel marketing digitale. La destinazione finale è una pagina social pubblica e non presenta rischi per la sicurezza.
Sulla base di queste evidenze, si conferma che l'attività osservata non è sospetta e si ribadisce la classificazione del file come **Vero Negativo**.