BW3 es.2.1 Analisi del Malware Vidar

Introduzione al Malware Vidar - Vidar Malware Analysis

⚜️ **Tag:** #malware #vidar #cybersicurezza

Il malware Vidar è un tipo di "stealer" progettato per rubare informazioni sensibili dai sistemi compromessi, con un'attenzione particolare verso credenziali, dati di criptovalute e informazioni personali.

Informazioni di Base - Basic Information

⚜️ **Tag:** #informazioni #malware #analisi

- **Nome del File Analizzato**: `66bddfcb52736_vidar.exe`
- **Tipo di Malware**: Stealer (Vidar)
- **Data dell'Analisi**: 25 agosto 2024
- **Sistema Operativo Utilizzato**: Windows 10

Descrizione e Finalità del Malware - Malware Description and Purpose

⚜️ **Tag:** #descrizione #finalità

Vidar appartiene alla famiglia degli stealer, con l'obiettivo di:

1. **Rubare credenziali di accesso**: Compromette le password memorizzate nei browser web.

2. **Estrazione di dati di criptovalute**: Mira ai wallet digitali per ottenere accesso ai fondi.
3. **Raccolta di informazioni personali**: Compie ricerche di dati sensibili, utili a fini di sfruttamento o vendita sul dark web.

Comportamenti Osservati - Observed Behaviors

⚜️ **Tag:** #comportamenti #analisi #cyberattacchi

1. **Evasione del Controllo**: Vidar utilizza tecniche per evitare il rilevamento da parte degli antivirus.
2. **Connessioni a Server Remoti**: Stabilisce comunicazioni con server remoti per l'invio delle informazioni raccolte.
3. **Furto di Dati**: Esplora il sistema per raccogliere dati personali e aziendali sensibili.

Misure di Contenimento e Rimozione - Containment and Removal Measures

⚜️ **Tag:** #contenimento #rimozione #protezione

1. **Isolare il Programma Malevolo (Mettere in Quarantena)**
   - **Cosa Significa**: Spostare il file infetto in un'area sicura.
   - **Perché**: Permette di esaminarlo senza rischio di propagazione.
2. **Eliminare il File Infetto**
   - **Cosa Significa**: Rimuovere definitivamente il file dannoso.
   - **Perché**: Prevenire riattivazioni del malware.
3. **Bloccare le Connessioni Internet Non Autorizzate**
   - **Cosa Significa**: Configurare il firewall per interrompere le comunicazioni con server esterni.

- **Perché**: Impedisce l’esfiltrazione di dati verso i criminali.

4. **Aggiornare il Programma Antivirus**
    - **Cosa Significa**: Garantire che l'antivirus sia aggiornato.
    - **Perché**: Riconoscere e bloccare malware come Vidar.
5. **Scansione Completa del Computer**
    - **Cosa Significa**: Eseguire una verifica integrale del sistema.
    - **Perché**: Rilevare eventuali altri file infetti.

Ripristino e Misure Preventive - Restoration and Preventive Measures

⚜️ **Tag:** #ripristino #prevenzione

1. **Ripristino delle Impostazioni di Sistema**
    - **Cosa Significa**: Riportare il sistema alle configurazioni precedenti.
    - **Perché**: Prevenire riattivazioni del malware.
2. **Monitorare i Log del Sistema**
    - **Cosa Significa**: Verificare i registri per attività sospette.
    - **Perché**: Identificare l'estensione dell’attacco e possibili furti.
3. **Eseguire Backup Regolari**
    - **Cosa Significa**: Salvare copie di sicurezza dei dati.
    - **Perché**: Recuperare i dati senza perdite in caso di attacco.
4. **Educare e Formare il Personale**
    - **Cosa Significa**: Formare gli utenti per riconoscere minacce e phishing.
    - **Perché**: Ridurre il rischio di futuri attacchi.
5. **Consultare Esperti di Sicurezza**
    - **Cosa Significa**: Rivolgersi a specialisti per supporto tecnico avanzato.
    - **Perché**: Soluzioni mirate e miglioramenti di sicurezza.

🔑 **Chiavi:**
[malware, Vidar, sicurezza informatica, protezione dati, stealer, analisi]

Approfondimento Malware Vidar.exe

Chiavi e Registri Modificati

⚜️ **Tag:** #chiavi #registri #modifiche

- **Chiavi e Percorsi**:
  - `SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profili\Outlook`
  - `SOFTWARE\Microsoft\Windows\CurrentVersion\Disinstalla`
  - **Modifica di vari registri** per ottenere informazioni su sistema, configurazioni e profili utente.

Evasione Utilizzata

⚜️ **Tag:** #evasione #malware #vidar

- **Evasione di Rilevamento**:
  - Il malware ha utilizzato `timeout.exe` per ritardare l'esecuzione e aumentare la probabilità di evitare rilevamenti immediati.
  - **Disattivazione di librerie e componenti critici** come `Mozilla DLL` e `C-runtime` per nascondersi.

Connessione e Furto di Dati

⚜️ **Tag:** #connessione #furto #dati

- **Connessione ai Server**:
  - Accesso a vari server per esfiltrare dati.
  - **Token** e dati di login (inclusi `username` e `password`) estratti dai principali browser e applicazioni, come `Steam`, `Telegram`, e altri profili di app di messaggistica e social media.
- **Furto Dati**:
  - Dati esfiltrati includono credenziali, cookie, cronologia di navigazione e dettagli delle carte di credito criptate dai file `.sqlite` di browser (es. `cookie.sqlite`, `places.sqlite`).

🔑 **Chiavi**:
chiavi, registri, evasione, connessione, furto, vidar

Per ulteriori informazioni consultare il report in allegato: ANY.RUN_66bddfcb52736_vidar.exe.pdf

ANY RUN
INTERACTIVE MALWARE ANALYSIS

Informazioni generali

Nome file:	66bddfcb52736_vidar.exe
Analisi completa:	https://app.any.run/tasks/371957e1-d960-4b8a-8c68-241ff918517d
Verdetto:	Attività dannosa
Minacce:	**Caricatore** Un loader è un software dannoso che si infiltra nei dispositivi per distribuire payload dannosi. Questo malware è in grado di infettare i computer delle vittime, analizzare le informazioni di sistema e installare altri tipi di minacce, come trojan o stealer. I criminali solitamente distribuiscono i loader tramite e-mail e link di phishing, affidandosi all'ingegneria sociale per indurre gli utenti a scaricare ed eseguire i loro eseguibili. I loader impiegano tattiche avanzate di evasione e persistenza per evitare il rilevamento. **Luce** Lumma è un ladro di informazioni, sviluppato utilizzando il linguaggio di programmazione C. Viene offerto in vendita come malware-as-a-service, con diversi piani disponibili. Di solito prende di mira i wallet di criptovaluta, le credenziali di accesso e altre informazioni sensibili su un sistema compromesso. Il software dannoso riceve regolarmente aggiornamenti che ne migliorano ed espandono la funzionalità, rendendolo una seria minaccia di ladro. **Ladro** Gli stealer sono un gruppo di software dannosi che mirano a ottenere l'accesso non autorizzato alle informazioni degli utenti e a trasferirle all'aggressore. La categoria di malware stealer include vari tipi di programmi che si concentrano sul loro particolare tipo di dati, tra cui file, password e criptovaluta. Gli stealer sono in grado di spiare i loro obiettivi registrando le loro sequenze di tasti e scattando screenshot. Questo tipo di malware viene distribuito principalmente come parte di campagne di phishing. **Vidare** Vidar è un malware pericoloso che ruba informazioni e criptovaluta agli utenti infetti. Deve il suo nome all'antico dio scandinavo della Vendetta. Questo ladro terrorizza Internet dal 2018.
Data di analisi:	25 agosto 2024 alle 22:11:02
Sistema operativo:	Windows 10 Professional (build: 19045, 64 bit)
Etichette:	vedere, luce, ladro, caricatore
Indicatori:	
MIMO:	applicazione/x-dosexec
Informazioni sul file:	Eseguibile PE32 (GUI) Intel 80386 Mono/.Net assembly, per MS Windows
MD5:	FEDB687ED23F77925B35623027F799BB
SHA1:	7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81
Codice SHA256:	325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1
SSDEEP:	6144:yZIlGEaS7npmSNIfI330znhIBf4hJYBaZaH55B:rGEaSVmSmI30znhSYaZa5

Set di ambiente software e opzioni di analisi

Configurazione di avvio

Durata dell'attività:	60 secondi	Opzione Evasione Pesante:	spento	Geolocalizzazione della rete:	spento
Tempo aggiuntivo utilizzato:	nessuno	Proxy MITM:	spento	Riservatezza:	Presentazione pubblica
Opzione Fakenet:	spento	Percorso tramite Tor:	spento	Autoconferma dell'UAC:	SU
Rete:	SU				

Preimpostazione software

- Versione di Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64 bit) (23.001.20093)
- Versione 32.0.0.465 di Adobe Flash Player
- Versione PPAPI di Adobe Flash Player 32 (32.0.0.465)
- Pulizia di C (6.20)
- Versione 3.65.0 (3.65.0)
- Versione di Google Chrome (122.0.6261.70)
- Aiuto per gli aggiornamenti di Google (1.3.36.51)
- Aggiornamento Java 8 271 (64 bit) (8.0.2710.9)
- Aggiornamento automatico Java (2.8.271.9)
- Versione di Microsoft Edge (122.0.2365.59)
- Aggiornamento di Microsoft Edge (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office professionale 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - it-it (16.0.16026.20146)
- Strumenti di integrità di Microsoft Update (3.74.0.0)
- Microsoft Visual C++ 2013 ridistribuibile (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Runtime aggiuntivo - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 runtime minimo - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 ridistribuibile (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 ridistribuibile (x86) - 14.36.32532 (14.36.32532.0)

Correzioni rapide

- Pacchetto LanguagePack del cliente
- Pacchetto LanguagePack del cliente
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- Pacchetto FodMetadata
- Pacchetto di fondazione
- Pacchetto Hello Face
- Pacchetto Hello Face
- Pacchetto opzionale InternetExplorer
- Pacchetto opzionale InternetExplorer
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- Caratteristiche della lingua Pacchetto base en us
- Caratteristiche della lingua Scrittura a mano en us Pacchetto
- Pacchetto LanguageFeatures OCR en us
- Pacchetto LanguageFeatures Speech en us
- Caratteristiche del linguaggio Pacchetto TextToSpeech en us
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MediaPlayer
- Pacchetto MediaPlayer
- Pacchetto FOD desktop Microsoft OneCore ApplicationModel Sync