


Report Any.Run vidar.exe

Introduzione

Nel corso di questa analisi, abbiamo esaminato diverse minacce informatiche legate a malware specializzati nel furto di dati. Questi malware, noti come "stealer", rappresentano un pericolo significativo per utenti e aziende, in quanto mirano a sottrarre informazioni sensibili come credenziali di accesso, dati bancari e portafogli di criptovalute.

General Info

☒ Add for printing 

File name:	66bddfcb52736_vidar.exe
Full analysis:	https://app.any.run/tasks/371957e1-d960-4b8a-8c68-241ff918517d
Verdict:	Malicious activity
Threats:	Loader Lumma Stealer Vidar
A loader is malicious software that infiltrates devices to deliver malicious payloads. This malware is capable of infecting victims' computers, analyzing their system information, and installing other types of threats, such as trojans or stealers. Criminals usually deliver loaders through phishing emails and links by relying on social engineering to trick users into downloading and running their executables. Loaders employ advanced evasion and persistence tactics to avoid detection.	
Malware Trends Tracker >>>	
Analysis date:	August 25, 2024 at 22:11:02
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	vidar lumma stealer loader
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	FEDB687ED23F77925B35623027F799BB
SHA1:	7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81
SHA256:	325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1
SSDEEP:	6144:yZlGEaS7npmSNifi330znhlBf4hJYBaZaH55B:rGEaSVmSml30znhSYaZa5

Le principali minacce identificate sono Vidar Stealer e Lumma Stealer, entrambe progettate per compromettere la sicurezza informatica attraverso tecniche avanzate di esfiltrazione dati ed evasione delle difese.

MALICIOUS	SUSPICIOUS	INFO
Actions looks like stealing of personal data <ul style="list-style-type: none">• RegAsm.exe (PID: 6908)• RegAsm.exe (PID: 4704) VIDAR has been detected (YARA) <ul style="list-style-type: none">• RegAsm.exe (PID: 6908)• RegAsm.exe (PID: 6340) Steals credentials from Web Browsers <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) LUMMA has been detected (SURICATA) <ul style="list-style-type: none">• RegAsm.exe (PID: 4704) Stealers network behavior <ul style="list-style-type: none">• RegAsm.exe (PID: 4704) LUMMA has been detected (YARA) <ul style="list-style-type: none">• RegAsm.exe (PID: 4704)	Reads security settings of Internet Explorer <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Searches for installed software <ul style="list-style-type: none">• RegAsm.exe (PID: 6908)• RegAsm.exe (PID: 4704) Drops the executable file immediately after the start <ul style="list-style-type: none">• 66bddfcb52736_vidar.exe (PID: 6780)• RegAsm.exe (PID: 6908)• RegAsm.exe (PID: 6340) The process drops C-runtime libraries <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) The process drops Mozilla's DLL files <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Checks Windows Trust Settings <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Executable content was dropped or overwritten <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Process drops legitimate windows executable <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Reads the date of Windows installation <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Starts CMD.EXE for commands execution <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Uses TIMEOUT.EXE to delay execution <ul style="list-style-type: none">• cmd.exe (PID: 6284) Potential Corporate Privacy Violation <ul style="list-style-type: none">• RegAsm.exe (PID: 6908)	Creates files in the program directory <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Reads product name <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Creates files or folders in the user directory <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Checks supported languages <ul style="list-style-type: none">• 66bddfcb52736_vidar.exe (PID: 6780)• RegAsm.exe (PID: 6908)• RegAsm.exe (PID: 4704)• RegAsm.exe (PID: 6340)• CAFHDBGHJK.exe (PID: 6248)• HCAEHJJKFC.exe (PID: 1568) Reads CPU info <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Reads the computer name <ul style="list-style-type: none">• RegAsm.exe (PID: 6908)• 66bddfcb52736_vidar.exe (PID: 6780)• RegAsm.exe (PID: 4704)• CAFHDBGHJK.exe (PID: 6248)• HCAEHJJKFC.exe (PID: 1568) Checks proxy server information <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Reads Environment values <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Reads the machine GUID from the registry <ul style="list-style-type: none">• RegAsm.exe (PID: 6908) Reads the software policy settings <ul style="list-style-type: none">• RegAsm.exe (PID: 6908)

Descrizione delle Minacce

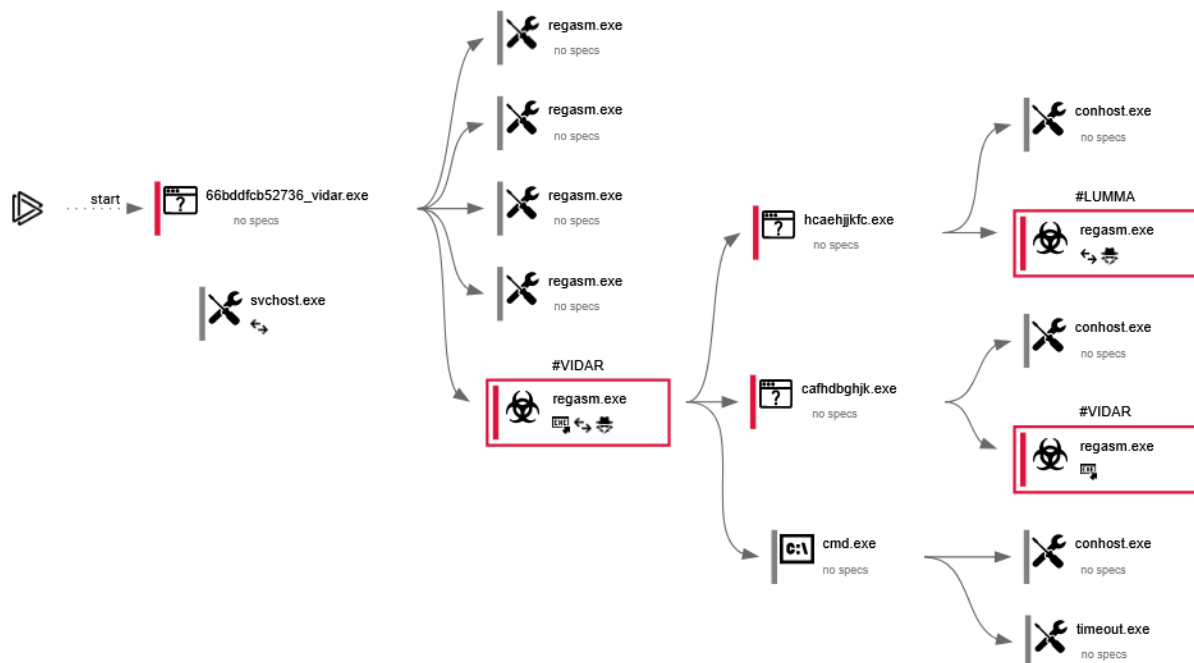
Vidar Stealer:

- Ruba credenziali salvate nei browser (password, cookie, cronologia di navigazione).
- Sottrae informazioni relative ai portafogli di criptovaluta.
- Può includere un keylogger, ovvero un sistema che registra tutto ciò che viene digitato sulla tastiera.
- Esegue operazioni di evasione per evitare di essere rilevato da antivirus e strumenti di monitoraggio.

Lumma Stealer:

- Oltre a sottrarre credenziali e dati finanziari, può catturare token di sessione per accedere ad account senza bisogno di password.
- Ha una configurazione altamente personalizzabile, il che lo rende pericoloso per molteplici tipi di vittime.
- Viene venduto come Malware-as-a-Service (MaaS), ovvero un pacchetto pronto all'uso per cybercriminali.

Entrambi i malware vengono diffusi tramite e-mail di phishing, siti web infetti, e software pirata.



Il grafico precedente mostra i processi malevoli identificati da questa scansione. Possiamo anche notare che i due malware vengono identificati ed evidenziati.

Perché queste minacce sono pericolose?

Furto di Identità: L'accesso a password e dati sensibili consente ai criminali informatici di impersonare la vittima.

Perdite finanziarie: I malware mirano anche ai conti bancari e ai portafogli di criptovalute.

Compromissione aziendale: Se un dipendente aziendale viene infettato, l'intera rete aziendale può essere esposta a minacce più gravi, come il ransomware.

Persistenza e diffusione: Alcuni di questi malware possono rimanere attivi nel sistema, trasmettendo continuamente dati rubati agli attaccanti.

Di seguito possiamo vedere l'elenco delle minacce rilevate.

Threats

PID	Process	Class	Message
–	–	Potentially Bad Traffic	ET INFO Executable Download from dotted-quad Host
–	–	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP
–	–	Potentially Bad Traffic	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response
–	–	Misc Attack	ET DROP Spamhaus DROP Listed Traffic Inbound group 23
–	–	Potentially Bad Traffic	ET INFO Executable Download from dotted-quad Host
–	–	A Network Trojan was detected	STEALER [ANY.RUN] Lumma Stealer TLS Connection
–	–	Potentially Bad Traffic	ET POLICY DNS Query to DynDNS Domain *.zapro .org
–	–	Potentially Bad Traffic	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response

Misure di Sicurezza e Azioni di Remediation

Dopo l'analisi, abbiamo identificato alcune contromisure essenziali per limitare i danni e prevenire attacchi futuri:

- Mettere in quarantena il file infetto
- Eliminare il file
- Inserire l'hash del malware in una blacklist
- Educare gli utenti sulla sicurezza informatica
- Chiedere un'analisi al vendor di sicurezza
- Eseguire scansioni approfondite su tutta la rete

Motivazione delle misure di sicurezza

Mettendo in quarantena il file, si evita che il malware possa eseguire codice dannoso o propagarsi ulteriormente nella rete.

Se non sono necessarie ulteriori indagini, eliminare il file impedisce il rischio di una nuova esecuzione accidentale.

Gli strumenti di sicurezza potranno bloccare automaticamente qualsiasi file identico in futuro; pertanto, conviene inserire l'hash in una blacklist per evitare che si replichi un attacco del genere.

Poiché questi malware si diffondono tramite phishing, è fondamentale formare il personale a riconoscere e segnalare e-mail sospette.

Se il file sospetto non è chiaramente identificato come malware, è utile inoltrarlo ai fornitori di software antivirus per un'analisi più approfondita.

Per verificare se ci sono altre infezioni o attività anomale che potrebbero indicare una compromissione più ampia.

Conclusione

Le minacce analizzate rappresentano un serio pericolo per utenti e aziende, poiché possono portare alla perdita di informazioni critiche e danni finanziari. Adottare misure di sicurezza preventive e reattive è essenziale per proteggersi da questo tipo di attacchi.

Seguire una strategia di sicurezza efficace, combinata con una formazione costante del personale, permette di ridurre significativamente il rischio di compromissione da parte di malware avanzati come Vidar e Lumma.