

Analisi Malware

Report

- Presentazione del problema Pg.5
- Analisi nel dettaglio Pg.6-9
- Indicatori di compromissione Pg.10
- Mitigazione al problema Pg.11
- Prevenzione Pg.12
- Conclusioni Pg.13

Introduzione



1

Informazioni Generali

- **Nome file:** Muadrnd.exe
- **Origine:** Repository GitHub
- **Dimensione:** 126 KB
- **Tipologia file:** File eseguibile .exe

2

Problema Riscontrato

- Errore Durante l'apertura del file

3

Obiettivo dell'Analisi

- La natura del file (legittimo o malevolo).
- Indicatori di compromissione (IoC).
- Possibili motivi del danneggiamento.

Introduzione



1

Informazioni Generali

- Nome file: Muadrnd.exe
- Origine: Repository GitHub
- Dimensione: 126 KB
- Tipologia file: File eseguibile .exe

2

Problema Riscontrato

- Errore Durante l'apertura del file

3

Obiettivo dell'Analisi

- La natura del file (legittimo o malevolo).
- Indicatori di compromissione (IoC).
- Possibili motivi del danneggiamento.

Introduzione

1

Informazioni Generali

- Nome file: Muadrnd.exe
- Origine: Repository GitHub
- Dimensione: 126 KB
- Tipologia file: File eseguibile .exe

2

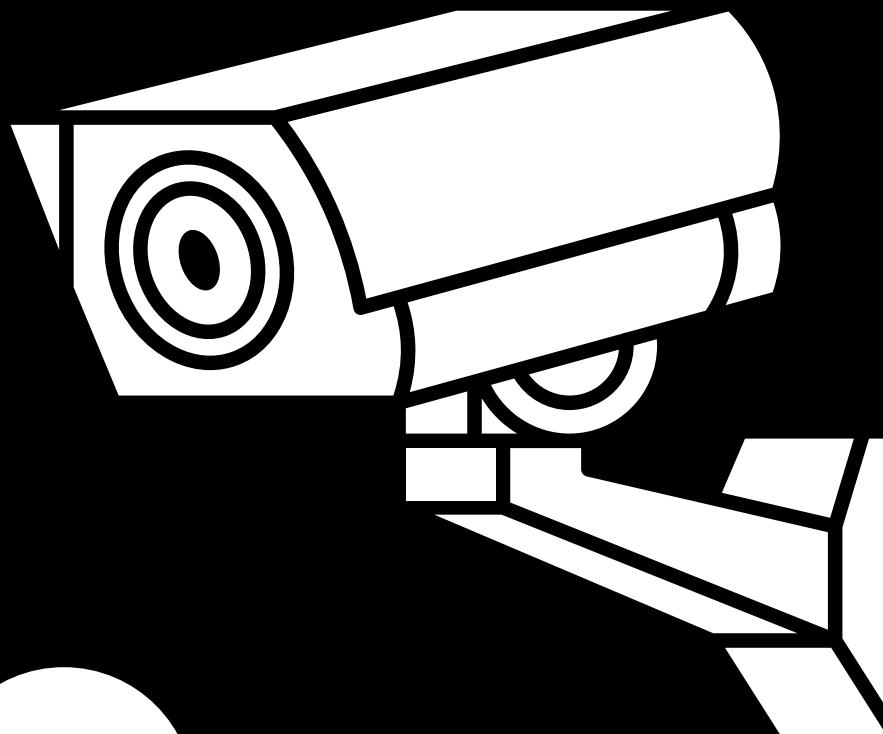
Problema Riscontrato

- Errore Durante l'apertura del file

3

Obiettivo dell'Analisi

- La natura del file (legittimo o malevolo).
- Indicatori di compromissione (IoC).
- Possibili motivi del danneggiamento.



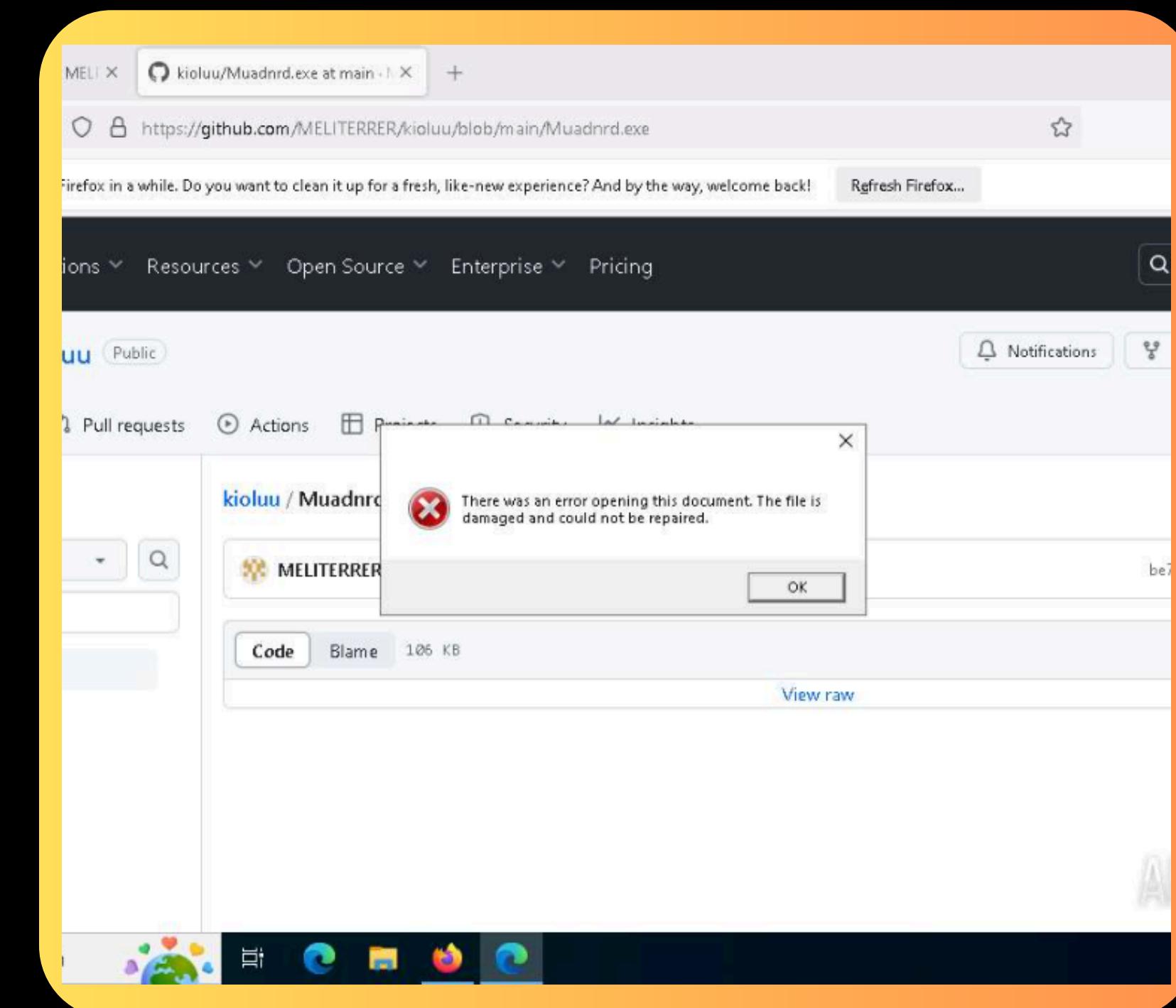
Presentazione del problema

Errore in primo piano

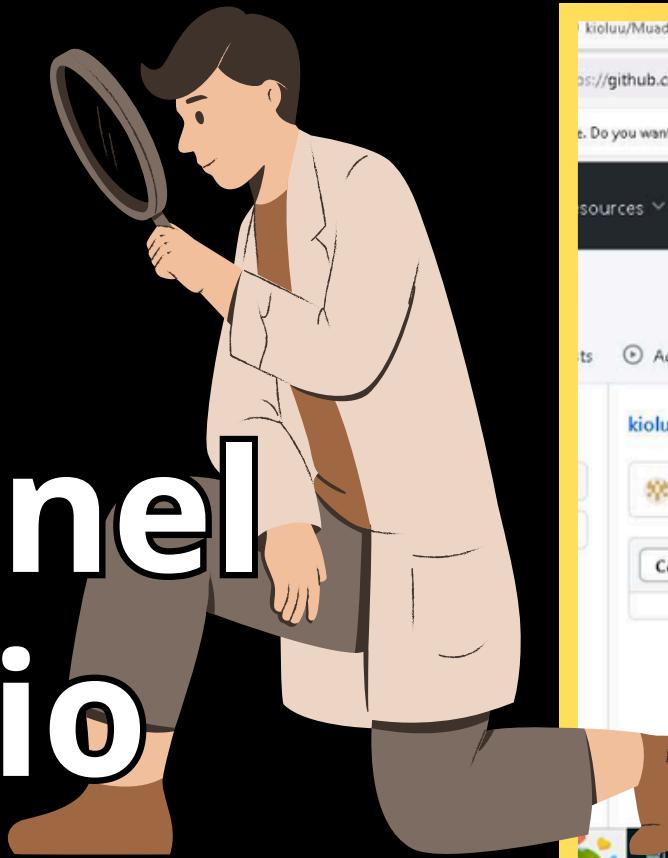
Una finestra di errore sovrapposta al browser segnala:

"There was an error opening this document. The file is damaged and could not be repaired."

Questo indica che il file non può essere aperto correttamente poiché è danneggiato o corrotto.



Analisi nel dettaglio



The screenshot displays a multi-pane analysis interface for a Firefox process (PID 6596) that has opened a GitHub URL (<https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe>). The browser window shows an error message: "There was an error opening this document. The file is damaged and could not be repaired." The right pane shows a detailed process tree under the heading "Processes", listing several firefox.exe instances. The bottom pane shows a table of "DNS Requests" with 161 entries, and the rightmost pane provides "Process details" for the main process, including a command line, indicators, and various warnings and other findings.

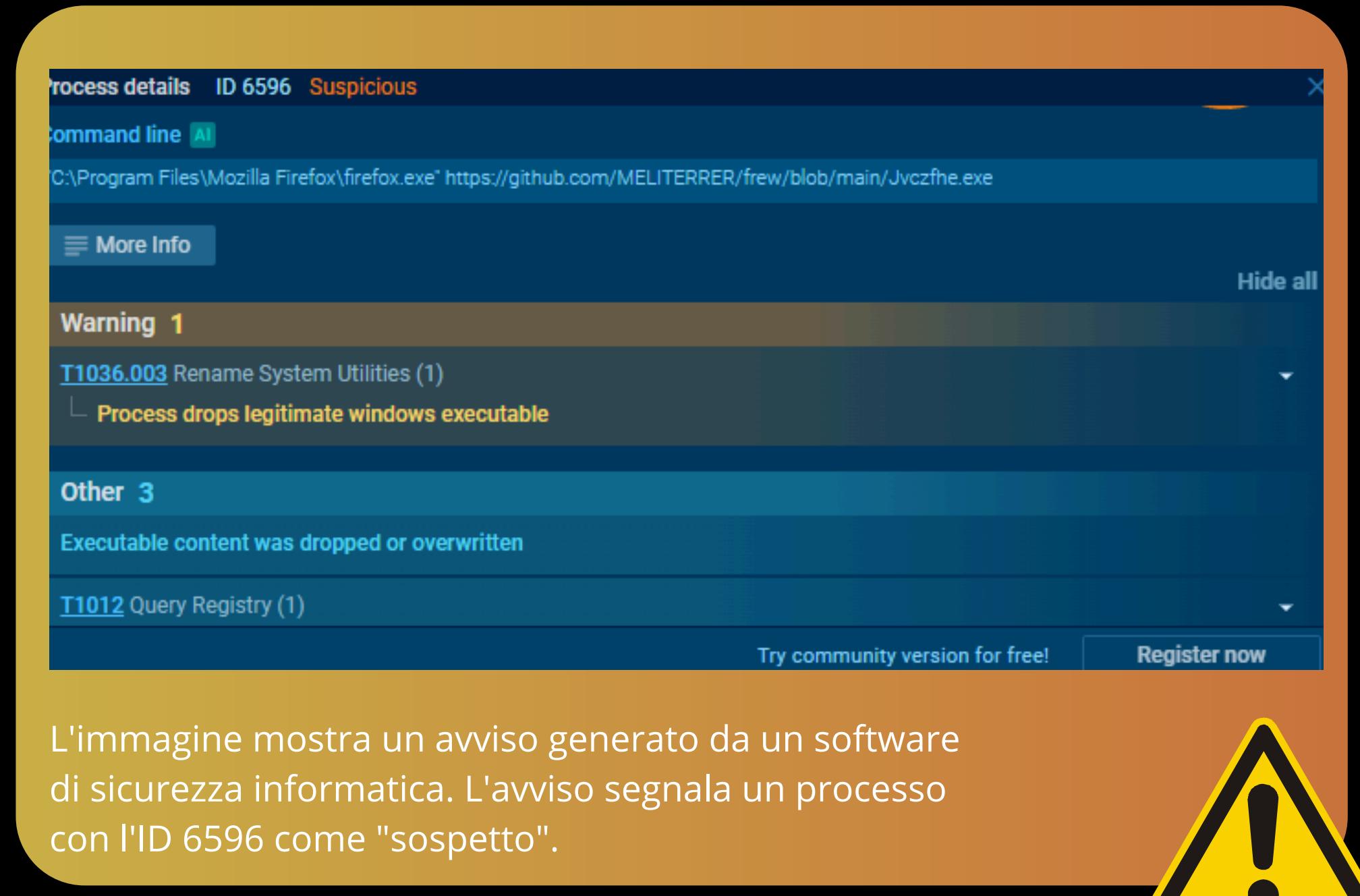
Step	PID	Process name	CN	URL	Content
1	6596	firefox.exe	US	http://detectportal.firefox.com/canonical.html	90 b ↓ text
2	6596	firefox.exe	US	http://detectportal.firefox.com/success.txt?ipv4	8 b ↓ text
3	6596	firefox.exe	US	http://ocsp.sectigo.com/	83 b ↑ binary 282 b ↓ binary
4	6596	firefox.exe	DE	http://r11.o.lencr.org/	85 b ↑ binary 504 b ↓ binary
5	6596	firefox.exe	DE	http://r11.o.lencr.org/	85 b ↑ binary 504 b ↓ binary
6	6596	firefox.exe	US	http://o.pki.goog/wr2	84 b ↑ binary 472 b ↓ binary
7	6596	firefox.exe	DE	http://r10.o.lencr.org/	85 b ↑ binary 504 b ↓ binary

Analisi nel dettaglio

• Warning 1

Ecco una scomposizione dei dettagli più importanti:

- Processo: Un'applicazione in esecuzione sul computer.
- Command line: Il comando esatto che ha avviato il processo. In questo caso, sembra che Firefox stia cercando di aprire un file eseguibile (Jvczfhe.exe) da un repository GitHub.
- Warning 1 (T1036.003): Questo avviso indica che il processo sta cercando di sostituire un file di sistema legittimo di Windows con un altro file. Questo è un comportamento tipico dei malware che cercano di nascondere le proprie tracce o di ottenere privilegi più elevati.
- Other 3 (T1012): Questo avviso indica che il processo sta cercando di accedere al registro di sistema, un'altra azione comune dei malware per modificare le impostazioni del sistema.



The screenshot shows a software interface for process analysis. At the top, it displays "Process details ID 6596 Suspicious". Below this, the "Command line" section shows the command: "C:\Program Files\Mozilla Firefox\firefox.exe" https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe". A "More Info" button is available. The main area is divided into sections: "Warning 1" (containing "T1036.003 Rename System Utilities (1)" and "Process drops legitimate windows executable"), "Other 3" (containing "Executable content was dropped or overwritten"), and "T1012 Query Registry (1)". A "Try community version for free!" button and a "Register now" button are at the bottom right. A large yellow exclamation mark icon is positioned in the bottom right corner of the slide.

L'immagine mostra un avviso generato da un software di sicurezza informatica. L'avviso segnala un processo con l'ID 6596 come "sospetto".

Analisi nel dettaglio

• Warning 3

L'avviso che stai visualizzando segnala un comportamento sospetto da parte di un processo in esecuzione sul tuo computer. In particolare, il software di sicurezza ha rilevato tre azioni potenzialmente dannose:



1

Esecuzione di un'applicazione che si blocca: Questo suggerisce che un programma sta cercando di eseguire un'operazione che causa un arresto anomalo. Potrebbe essere un tentativo di nascondere attività dannose o di destabilizzare il sistema.

2

Interrogazione del Registro di sistema (T1012): Il malware spesso modifica le impostazioni del registro di sistema per nascondersi, avviarsi automaticamente all'avvio del sistema o disabilitare le funzionalità di sicurezza. In questo caso, il malware sta leggendo le impostazioni di sicurezza di Internet Explorer e verificando le impostazioni di trust di Windows.

3

Utilizzo del prompt dei comandi (T1059.003): Il prompt dei comandi (CMD.EXE) è uno strumento potente che può essere utilizzato per eseguire una vasta gamma di operazioni sul sistema. I malware spesso lo utilizzano per eseguire comandi dannosi, come scaricare altri malware, eliminare file o modificare le impostazioni di sistema.

Analisi nel dettaglio

• Warning 4

L'immagine mostra un avviso generato da un software di sicurezza informatica. Questo avviso segnala un comportamento altamente sospetto da parte di un processo in esecuzione sul tuo computer.

The screenshot shows a software interface for security analysis. At the top, it says "Warning 4". Below that, it lists several suspicious behaviors:

- Executes application which crashes
- Application launched itself
- [T1012 Query Registry \(2\)](#)
 - Checks Windows Trust Settings
 - Reads security settings of Internet Explorer
- [T1059.003 Windows Command Shell \(1\)](#)
 - Starts CMD.EXE for commands execution



Decodifica dell'Avviso

L'avviso è suddiviso in quattro punti principali:

1° Esecuzione di un'applicazione che si blocca:
Questo indica che un programma sta cercando di eseguire un'operazione che causa un arresto anomalo. Potrebbe essere un tentativo di nascondere attività dannose o di destabilizzare il sistema.

2° L'applicazione si è avviata da sola: Questo è un forte indicatore di un malware. I malware spesso si configurano per avviarsi automaticamente all'avvio del sistema, rendendo più difficile la loro rimozione.

3° Interrogazione del Registro di sistema (T1012): Il malware spesso modifica le impostazioni del registro di sistema per nascondersi, avviarsi automaticamente all'avvio del sistema o disabilitare le funzionalità di sicurezza. In questo caso, il malware sta leggendo le impostazioni di sicurezza di Internet Explorer e verificando le impostazioni di trust di Windows.

4° Utilizzo del prompt dei comandi (T1059.003): Il prompt dei comandi (CMD.EXE) è uno strumento potente che può essere utilizzato per eseguire una vasta gamma di operazioni sul sistema. I malware spesso lo utilizzano per eseguire comandi dannosi, come scaricare altri malware, eliminare file o modificare le impostazioni di sistema.

Indicatori di compromissione (IoC)



- 1 Modifiche ai file di sistema
- 2 Accesso ai registri di sistema
- 3 Arresto anomalo
- 4 Avvio autonomo dell'applicazione

Mitigazione



- 1 Non Spegnere il Computer:** Spegnere il computer potrebbe impedire al software di sicurezza di completare la scansione e rimuovere il malware.
- 2 Disconnettiti da Internet:** Questo impedirà al malware di comunicare con i suoi server di comando e controllo.
- 3 Esegui una Scansione Completa:** Utilizza un antivirus aggiornato per eseguire una scansione completa del sistema.
- 4 Metti in Quarantena o Rimuovi i File Maliziosi:** Se l'antivirus trova dei file sospetti, mettili in quarantena o rimuovili.
- 5 Ripristina il Sistema:** Se hai creato un punto di ripristino del sistema prima dell'infezione, puoi utilizzarlo per ripristinare il tuo computer a uno stato precedente.
- 6 Cambia le Password:** Cambia le password di tutti i tuoi account online, soprattutto se hai utilizzato lo stesso computer per accedere a servizi sensibili.



Prevenzione



- 1** Mantieni aggiornato il tuo sistema operativo e i software: Le patch di sicurezza spesso correggono le vulnerabilità che i malware possono sfruttare.
- 2** Installa un buon antivirus e tienilo aggiornato: Un antivirus affidabile può proteggere il tuo computer dalle minacce più comuni.
- 3** Fai attenzione ai link e agli allegati: Non aprire email da mittenti sconosciuti e non cliccare su link sospetti.
- 4** Utilizza password forti e uniche: Le password forti rendono più difficile per gli hacker accedere ai tuoi account.
- 5** Effettua regolarmente dei backup: In caso di infezione, un backup ti permetterà di ripristinare i tuoi dati.

Conclusioni

In un mondo sempre più interconnesso, i malware rappresentano una delle minacce più gravi per la sicurezza delle aziende, indipendentemente dalle loro dimensioni o dal settore in cui operano. Un singolo attacco può compromettere la riservatezza dei dati sensibili, paralizzare le operazioni aziendali e danneggiare irreparabilmente la reputazione di un'azienda.

La diffusione dei malware è diventata più sofisticata, con attacchi mirati che sfruttano vulnerabilità nei sistemi per infiltrarsi e rimanere invisibili fino a causare il massimo danno. Le conseguenze di un'infezione possono includere perdite finanziarie significative, furto di proprietà intellettuale e violazioni legali legate alla protezione dei dati personali.

Ignorare queste minacce equivale a mettere a rischio il futuro dell'azienda. È essenziale implementare misure di difesa avanzate, come sistemi di rilevamento delle intrusioni, firewall aggiornati, formazione dei dipendenti e un approccio proattivo alla cybersecurity, per ridurre la superficie di attacco e rispondere tempestivamente a eventuali compromissioni.

Ricorda: la prevenzione è sempre meno costosa e più efficace rispetto alla gestione delle conseguenze di un attacco. Un'azienda che sottovaluta la pericolosità dei malware rischia di diventare un bersaglio facile in un panorama di minacce in continua evoluzione.

