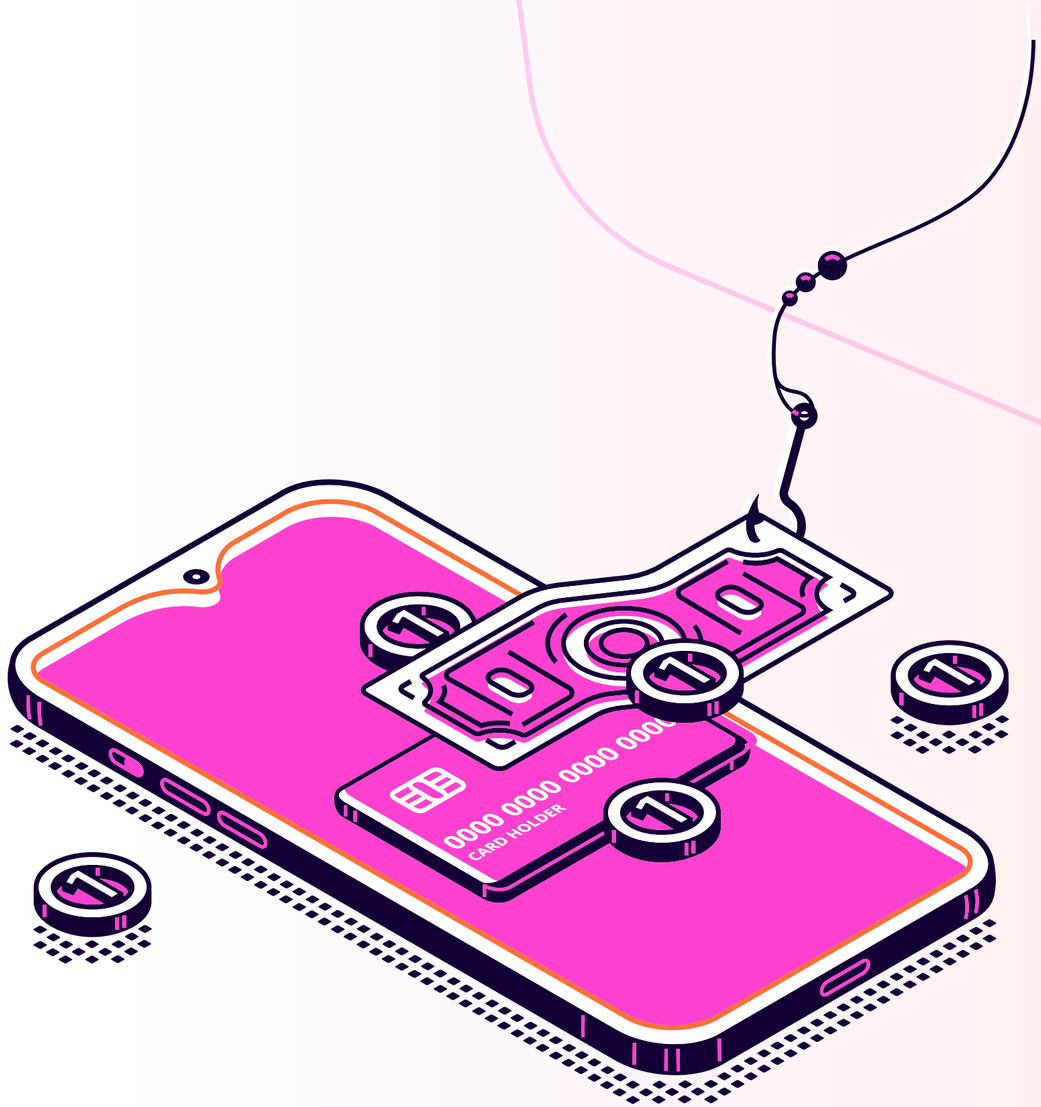
Report di Analisi Statica del Malware

Michele Covi

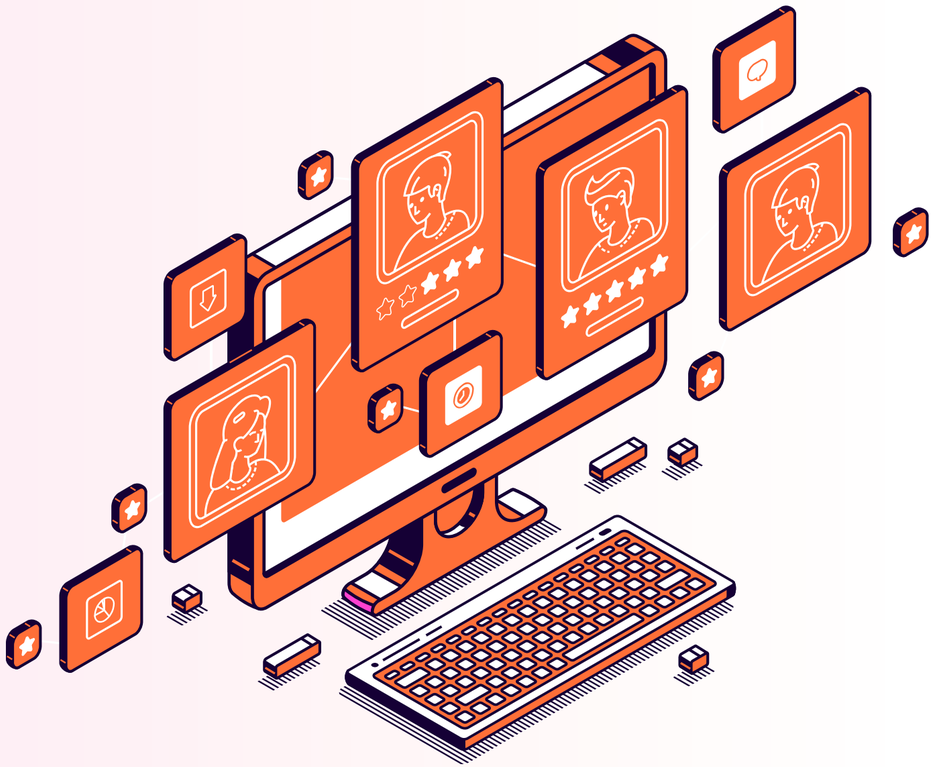
10/06/2024

Introduzione

Il presente report dettaglia l'analisi statica del file eseguibile Malware_U3_W2_L1.exe, condotta nell'ambito delle attività di sicurezza informatica per identificare e comprendere le potenziali minacce rappresentate dal file in esame. L'obiettivo è valutare le capacità del malware, le sue interazioni con il sistema ospitante e delineare le misure preventive e di mitigazione appropriate.
L'analisi è stata eseguita utilizzando CFF Explorer, uno strumento avanzato per l'analisi di file eseguibili Windows. Questo strumento permette di esaminare dettagliatamente le strutture interne del file, inclusi headers, sezioni e importazioni di librerie, fornendo una visione comprensiva delle capacità operative del malware.



Dettagli del File Analizzato



- **Nome del File: Malware_U3_W2_L1.exe**
- **Dimensione del File: 16 KB**
- **Tipo di File: Eseguibile Windows (PE)**

Analisi delle Librerie Importate

Durante l'analisi statica con CFF Explorer, sono state identificate diverse librerie dinamiche cruciali per la funzionalità del malware:

Kernel32.dll

Gestisce operazioni essenziali di sistema quali creazione di processi e thread, e manipolazione della memoria.

Advapi32.dll

Implementa funzioni avanzate relative alla sicurezza, quali la gestione dei registri e dei servizi Windows

Msvcrt.dll

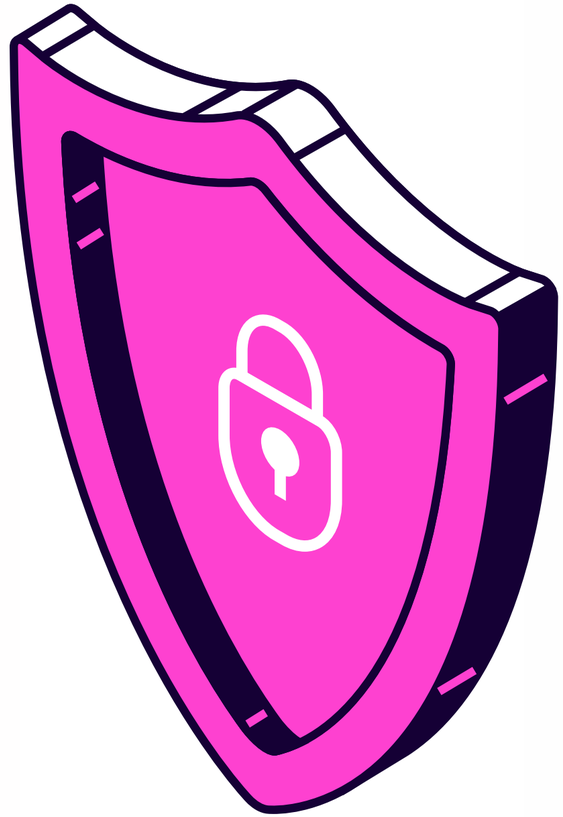
Libreria standard C di Microsoft, utilizzata per operazioni generali come manipolazione di stringhe e calcoli.

Wininet.dll

Fornisce funzionalità di networking, inclusi protocolli come HTTP e FTP, per comunicazioni di rete.

Analisi delle Sezioni del File

Il file contiene tre sezioni principali che sono state esaminate per comprendere meglio la distribuzione del codice e dei dati



01.

.text:

Sezione che contiene il codice eseguibile del malware. Questa sezione è marcata come eseguibile e non modificabile.

02.

.rdata:

Contiene dati costanti, come stringhe e configurazioni. È configurata come non eseguibile e solo lettura.

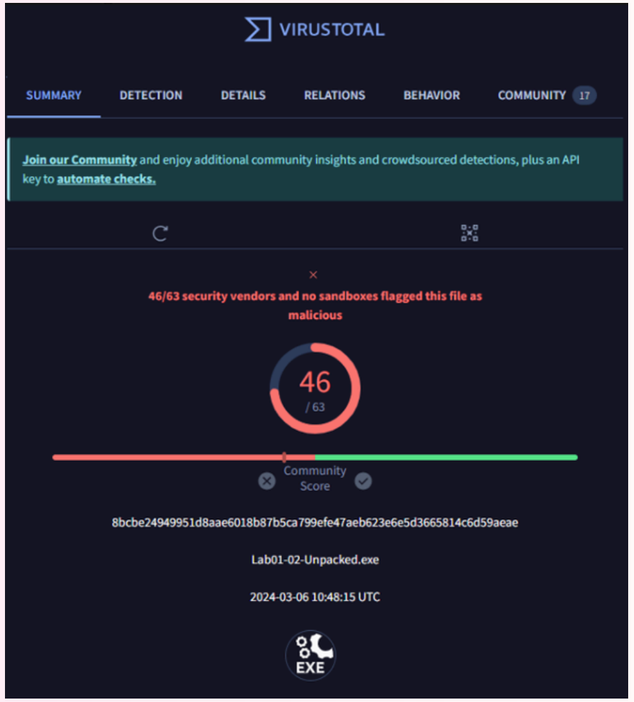
03.

.data:

Alloggia dati variabili utilizzati dal malware durante la sua esecuzione, marcata come leggibile e scrivibile.

Analisi con VirusTotal

Il file è stato inoltre sottoposto ad analisi tramite VirusTotal, che ha coinvolto 63 motori di sicurezza differenti. Il file è stato identificato come malevolo da 46 motori, evidenziando un'ampia riconoscenza del suo potenziale nocivo tra gli strumenti di sicurezza. È stato classificato principalmente come trojan, con attributi di spyware e rogue, indicando una capacità di compromissione significativa.



Considerazioni Finali e Raccomandazioni

L'analisi statica fornisce un quadro preoccupante del potenziale di danneggiamento del malware, con capacità di manipolazione del sistema operativo e di comunicazione con server esterni.
Si raccomandano le seguenti azioni:

- Monitoraggio Continuo: Implementare un'analisi dinamica per tracciare il comportamento del malware in un ambiente controllato.
- Aggiornamenti di Sicurezza: Assicurarsi che tutti i sistemi operativi e le applicazioni siano aggiornati per mitigare le vulnerabilità note.
- Formazione e Consapevolezza: Educare gli utenti finali sulla identificazione e gestione dei file sospetti.