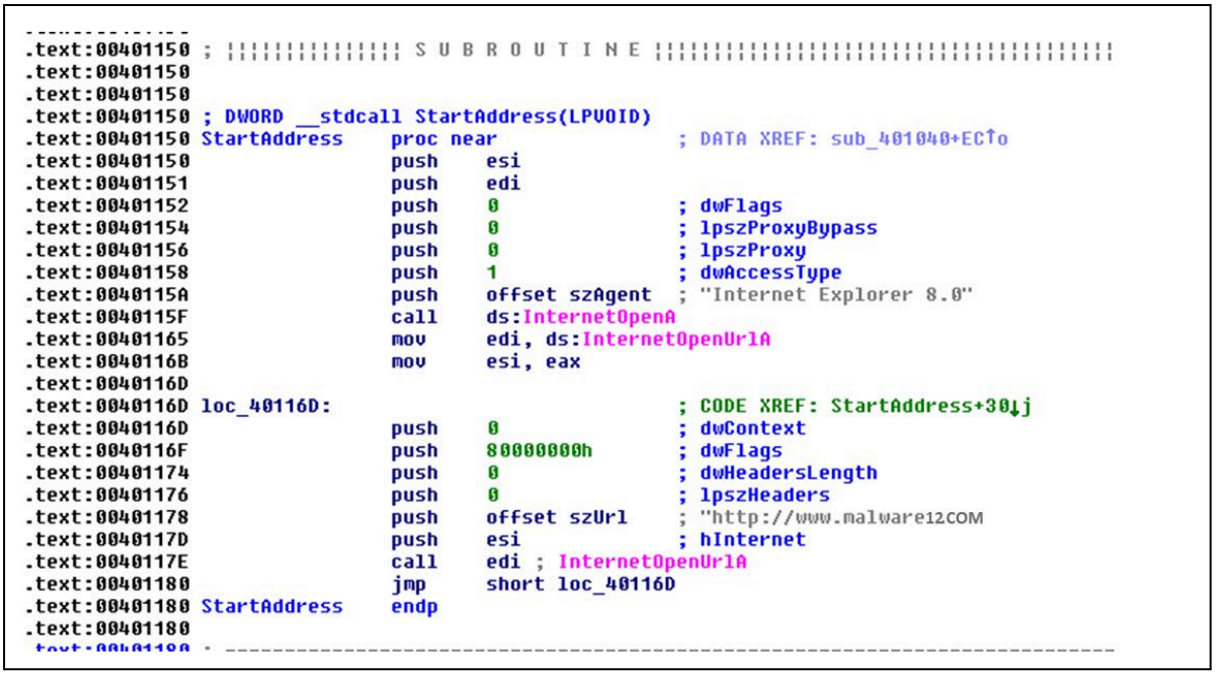
CONSEGNA S11/L1

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

```
0040286F   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
```



PERSISTENZA DEL MALWARE

INTRODUZIONE

Nel contesto della sicurezza informatica, uno degli aspetti più critici dell'analisi di un malware è comprendere i meccanismi attraverso i quali esso cerca di mantenere la persistenza all'interno di un sistema compromesso.
La persistenza permette al malware di sopravvivere ai riavvii del sistema e di continuare ad operare senza la necessità di essere rilanciato manualmente dall'utente.

MECCANISMI DI PERSISTENZA

L'analisi dell'estratto di codice assembly fornito mostra chiaramente che il malware implementa la persistenza modificando specifiche chiavi di registro di Windows.
Il Registro di Sistema è una funzione critica di Windows utilizzata per immagazzinare le configurazioni del sistema operativo e delle applicazioni.
Modificando determinate chiavi, il malware può assicurarsi che venga eseguito automaticamente ad ogni avvio del sistema.

ANALISI DEL CODICE IN ASSEMBLY

Nell'estratto di codice assembly, possiamo osservare le seguenti istruzioni e chiamate di funzioni che indicano un tentativo di ottenere persistenza:

- **RegOpenKeyEx**: Questa funzione è utilizzata per aprire una chiave di registro specificata. Nel nostro caso, si nota che il malware cerca di accedere alla chiave **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run**. Questa chiave è notoriamente utilizzata per eseguire automaticamente programmi all'avvio di Windows.

- **RegSetValueEx**: Dopo aver aperto la chiave di registro, il malware utilizza questa funzione per impostare un valore all'interno della chiave.
  Questo valore corrisponde al percorso dell'eseguibile del malware, che verrà lanciato quando l'utente avvierà il sistema.

Nelle due operazioni sopra citate, il malware sta chiaramente manipolando il registro di sistema per inserire una voce di auto-avvio che assicura la sua esecuzione ad ogni avvio del computer.

CONSIDERAZIONI SULLA PERSISTENZA

Il metodo utilizzato dal malware è comune e molto efficace, poiché molti utenti non controllano regolarmente le chiavi di registro Run.
Questo permette al malware di operare indisturbato e di riattivarsi con ogni riavvio del sistema, aumentando così le sue possibilità di eseguire azioni dannose come il furto di dati, la diffusione della infezione o l'installazione di ulteriori payload dannosi.

MISURE DI MITIGAZIONE

Per mitigare questo tipo di minaccia, è essenziale utilizzare software di sicurezza affidabili che possano monitorare e gestire le modifiche al registro di sistema.
Inoltre, è consigliabile avere politiche di sicurezza che includano la revisione regolare delle chiavi di auto-avvio del registro e l'adozione di strumenti di gestione degli endpoint per rilevare comportamenti anomali.

QUINDI IN CONCLUSIONE

La persistenza è una caratteristica chiave dei malware moderni, che consente loro di mantenersi attivi nel sistema infetto.
La comprensione delle tecniche utilizzate per ottenere questa persistenza è fondamentale per gli analisti di sicurezza, permettendo loro di sviluppare strategie di rilevamento e risposta più efficaci.
Il codice assembly analizzato in questo report mostra un esempio chiaro di come un malware possa manipolare il registro di sistema di Windows per garantire la sua persistenza, enfatizzando l'importanza di monitorare tali modifiche per la sicurezza dei sistemi informatici.

IDENTIFICAZIONE DEL CLIENT SOFTWARE UTILIZZATO

In un'analisi di sicurezza informatica, identificare il client software utilizzato da un malware per stabilire connessioni Internet è un passo cruciale per comprendere le sue capacità di comunicazione e potenzialmente intercettare o bloccare tali comunicazioni.
Il client software agisce come un intermediario tra il malware e la rete esterna, spesso mascherando le attività dannose come traffico legittimo.

ANALISI

Dall'analisi del frammento di codice assembly fornito nella seconda immagine, emerge che il malware utilizza le API Windows per connettersi a Internet.
In particolare, il malware si appoggia alle funzionalità offerte dal pacchetto WinINet di Microsoft, che fornisce un'interfaccia di programmazione ad alto livello per le applicazioni Windows per accedere a Internet.

Nel dettaglio, il codice mostra l'uso di **InternetOpenA**, una funzione dell**'API WinINet**.
Questa funzione inizializza un'applicazione per l'uso delle funzioni WinINet e specifica l'agente utente che sarà utilizzato per le successive richieste di rete.
Nel caso specifico, l'agente utente è impostato per simulare il browser "Internet Explorer 8.0", come indicato dalla stringa useragent utilizzata.

Questo metodo di impersonare un browser ben noto è una tattica comune tra i malware per evitare il rilevamento, poiché molti sistemi di monitoraggio della rete possono confondere il traffico del malware con quello generato da un browser legittimo.
L'uso di **InternetOpenA** è un indizio che il malware potrebbe eseguire ulteriori azioni di rete, come inviare o ricevere dati, utilizzando le **API WinINet** per mascherare tali comunicazioni come traffico di navigazione web legittimo.

IMPLICAZIONI DI SICUREZZA

L'identificazione del client software utilizzato dal malware fornisce informazioni vitali sulle capacità di evasione e comunicazione del malware stesso. Con questa informazione, gli analisti di sicurezza possono:

- Monitorare il traffico di rete per rilevare anomalie nel comportamento del browser Internet Explorer, soprattutto se la versione 8.0 non è comune nell'ambiente in cui è stato rilevato il malware
- Applicare regole di filtraggio basate su user-agent per identificare e bloccare richieste sospette
- Utilizzare strumenti di analisi forense di rete per esaminare in modo più approfondito il traffico associato al malware, nella speranza di intercettare comunicazioni con i server di comando e controllo

RACCOMANDAZIONI OPERATIVE

Sulla base di questa analisi, si consiglia di:

- Implementare un sistema di rilevamento intrusioni (IDS) e/o un sistema di prevenzione intrusioni (IPS) per monitorare e bloccare il traffico sospetto che imita il browser Internet Explorer 8.0
- Aggiornare i dispositivi di sicurezza perimetrale, come i firewall, per riconoscere e filtrare il traffico basato sulle stringhe user-agent conosciute utilizzate da malware
- Formare il personale IT e di sicurezza per riconoscere le tecniche di mascheramento del traffico di rete utilizzate dai malware, compresa l'impersonificazione di software client legittimi

L'analisi del codice assembly ha permesso di identificare il client software utilizzato dal malware per la connessione a Internet, fornendo informazioni preziose per le operazioni di sicurezza informatica. La capacità del malware di mascherare le sue comunicazioni sotto forma di traffico di un browser legittimo richiede una vigilanza continua e l'adozione di misure di sicurezza robuste per mitigare il rischio di infezioni e brecce di dati.

IDENTIFICAZIONE DELL'URL DI CONNESSIONE MALWARE

SOMMARIO

La comprensione del comportamento di rete di un malware è essenziale per contrastare efficacemente la minaccia che esso rappresenta.
Uno degli aspetti critici di questo comportamento è la capacità del malware di stabilire una connessione con un URL esterno, spesso utilizzato per il comando e il controllo (C2) o per azioni dannose come l'esfiltrazione di dati.
Questo report fornisce un'analisi approfondita dell'URL di destinazione che il malware cerca di raggiungere e della funzione di rete che utilizza per stabilire tale connessione.

IDENTIFICAZIONE

Dall'analisi del frammento di codice assembly fornito, è stato identificato che il malware tenta di connettersi all'URL **http://www.malware12.com**.
La presenza di un URL specifico all'interno del codice del malware è una pratica comune per i malware progettati per comunicare con un server remoto.
Tale URL è spesso utilizzato per ricevere comandi aggiuntivi, scaricare ulteriori payload dannosi o inviare dati sottratti dalla macchina infetta.

DESCRIZIONE DELLA CHIAMATA DI FUNZIONE DI CONNESSIONE

La connessione all'URL viene effettuata utilizzando la funzione InternetOpenUrlA, che fa parte delle API WinINet di Microsoft.
Queste API sono progettate per permettere alle applicazioni Windows di interagire con servizi HTTP, FTP e Gopher su Internet. La funzione InternetOpenUrlA in particolare, viene utilizzata per aprire un URL con un dato contesto di connessione Internet fornito dalla funzione InternetOpen.

Il processo di chiamata di funzione inizia con il passaggio dell'URL come parametro alla funzione InternetOpenUrlA.
Questo indica che il malware ha programmato all'interno del suo codice l'URL di destinazione e la sequenza necessaria per stabilire la connessione, suggerendo un'operazione premeditata e potenzialmente sofisticata.

IMPLICAZIONI PER LA SICUREZZA E LA RISPOSTA DEGLI INCIDENTI

La scoperta di tale URL all'interno del codice malware è di significativa importanza per la risposta agli incidenti e le operazioni di sicurezza.
Con questa informazione, è possibile:

- Bloccare il traffico verso e dall'URL specifico a livello di firewall o altri dispositivi di sicurezza di rete
- Monitorare il traffico di rete per identificare altre possibili comunicazioni malevole correlate
- Analizzare il server di hosting dell'URL, se possibile, per ottenere ulteriori informazioni sulle infrastrutture degli aggressori

CONCLUSIONE

L'identificazione dell'URL di connessione e la comprensione della funzione utilizzata per stabilire tale connessione sono fondamentali per interrompere le operazioni del malware e per prevenire ulteriori danni.
Questa analisi non solo contribuisce a neutralizzare la minaccia corrente, ma fornisce anche intuizioni preziose che possono essere utilizzate per rafforzare le difese contro future varianti di malware simili.