

BW III:

MALWARE ANALYSIS

TRACCIA 2:

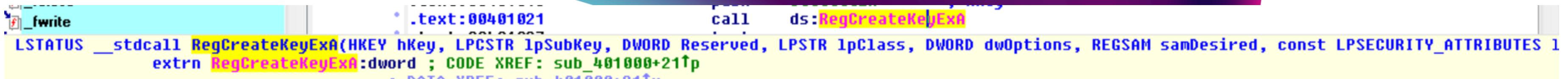
GIORNO2

Con riferimento al Malware in analisi, spiegare:

- Lo scopo della funzione chiamata alla locazione di memoria 00401021
- Come vengono passati i parametri alla funzione alla locazione 00401021 ;
- Che oggetto rappresenta il parametro alla locazione 00401017
- Il significato delle istruzioni comprese tra gli indirizzi 00401027 e 00401029 (se serve, valutate anche un'altra o altre due righe assembly)
- Con riferimento all'ultimo quesito, tradurre il codice Assembly nel corrispondente costrutto C
- Valutate ora la chiamata alla locazione 00401047 , qual è il valore del parametro « ValueName»?

Nel complesso delle due funzionalità appena viste, spiegate quale funzionalità sta implementando il Malware in questa sezione.

LOCAZIONE 00401021:



```
	fwrite
.text:00401021          call    ds:RegCreateKeyExA
LSTATUS __stdcall RegCreateKeyExA(HKEY hKey, LPCSTR lpSubKey, DWORD Reserved, LPSTR lpClass, DWORD dwOptions, REGSAM samDesired, const LPSECURITY_ATTRIBUTES lpSecurityAttributes, HKEY *phKey)
extrn RegCreateKeyExA:dword ; CODE XREF: sub_401000+21↑p
```

Lo scopo della chiamata di funzione in memoria 00401021 è creare una nuova chiave o aprirne una già esistente nel Registro di sistema di Windows.

La funzione RegCreateKeyExA richiede diversi parametri, tra cui:

- hKey: Che determina la posizione nella gerarchia del registro in cui verrà creata la nuova chiave.
- lpSubKey: Il nome della nuova chiave da creare, come stringa.
- Reserved: Parametro riservato, in genere impostato su zero.
- lpClass: Stringa che specifica il nome della classe associato alla nuova chiave
- dwOptions: Flag che controllano come viene creata la chiave (ad esempio, impostazioni di sicurezza).
- samDesired: Permessi richiesti per accedere alla nuova chiave.
- lpSecurityAttributes: Puntatore a un descrittore di sicurezza
- phKey: Puntatore a una variabile in cui verrà memorizzato l'handle della chiave appena creata.

LOCAZIONE 00401017:

```
.text:00401017  
.text:0040101C  
.text:00401021  
.text:00401027  
.text:00401029
```

```
push    offset SubKey      ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon"  
push    8                ; ...  
push    SubKey          ; char SubKey[]  
call    SubKey          db  'SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon',0  
test    SubKey          ; DATA XREF: sub_401000+17↑o
```

il parametro in memoria 00401017 rappresenta il percorso della chiave di Registro che il programma sta tentando di creare o aprire in questo caso:

- SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon

Il malware potrebbe creare chiavi di Registro per:

- Memorizzare impostazioni di configurazione per la persistenza: Per memorizzare impostazioni di configurazione che gli consentano di avviarsi o eseguire automaticamente all'avvio del sistema.
- Modificare il comportamento del sistema: Può cambiare impostazioni di sistema, disabilitare funzionalità di sicurezza o reindirizzare funzioni di sistema.
- Nascondersi: Il malware può creare chiavi in posizioni nascoste del registro per renderle più difficili da rilevare.

LOCAZIONI 00401027 e 00401029

.text:00401027
.text:00401029
.text:0040102B
.text:00401030

| | |
|------|------------------|
| test | eax, eax |
| jz | short loc_401032 |
| mov | eax, 1 |
| jmp | short loc_40107B |

- test eax, eax: Questa istruzione confronta il valore del registro EAX con se stesso. Poiché qualsiasi numero confrontato con se stesso è uguale, il risultato di questa istruzione è sempre 1 (flag ZF impostato).
- jz short loc_401032: Questa istruzione effettua un salto condizionale all'etichetta loc_401032 se il flag ZF è impostato . In caso contrario, il flusso di esecuzione prosegue con la prossima istruzione in sequenza.
- mov 1: Questa istruzione sposta il valore 1 nello stack.
- jmp short loc_40107B: Effettua un salto incondizionato alla locazione loc_40107B.

TRADUZIONE ASSEMBLY IN C:

L'equivalente del codice assembly riscritto nel costrutto C è:

```
if (eax == 0) {
    goto loc_401032;
} else {
    eax = 1;
    goto loc_40107B;
}
```

LOCAZIONE 0040147:

```
.text:0040103E          push    offset ValueName ; "GinaDLL"
.text:00401043          mov     eax, [ebp+hObject]
.text:00401046          push    eax               ; hKey
.text:00401047          call    ds:RegSetValueExA
```

- RegSetValueExA è una funzione dell'API Windows utilizzata per impostare il valore di una specifica chiave di registro

```
.text:0040103E          push    offset ValueName ; "GinaDLL"
.text:00401043          mov     eax, [ebp+hObject]
.text:00401046          push    ; char ValueName[]
.text:00401047          call    ds:RegSetValueExA      ; DATA XREF: sub_401000+3E↑
```

- In questo codice, il parametro ValueName viene spinto sullo stack e viene utilizzato il valore offset ValueName; "GinaDLL". Ciò indica che il valore di ValueName è l'indirizzo di una stringa che contiene il testo "GinaDLL".

CONCLUSIONI:

In conclusione, dall' analisi fatta fino ad ora possiamo dedurre che il Malware utilizza le funzioni RegSetValueExA e RegCreateKeyExA per cercare di creare una persistenza sul sistema compromesso.

Il Malware crea una chiave di registro nella posizione:

SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Queste funzioni consentono al malware di modificare il registro di Windows, un database centrale che archivia configurazioni e impostazioni di sistema.