TRACCIA FINALE W24D4

MALWARE ANALYSIS
ANALISI STATICA AVANZATA

TRACCIA:

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**
- 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»?

PROSEGUENDO CON L'ANALISI STATICA DEL CODICE DEL MALWARE GRAZIE ALL'UTILIZZO DI IDA PRO, TROVIAMO ALLA LOCAZIONE DI MEMORIA 00401021 LA FUNZIONE RegCreateKeyExA, CHE È UNA FUNZIONE NOTA CHE FA PARTE DELLE API DI WINDOWS CHE PERMETTONO ALLE APPLICAZIONI DI INTERAGIRE CON IL REGISTRO DI WINDOWS. QUESTE FUNZIONI SONO UTILIZZATE PER CREARE NUOVE CHIAVI DI REGISTRO O PER APRIRE CHIAVI ESISTENTI PER MODIFICARE I LORO VALORI.

NELLO SPECIFICO IL MALWARE PUÒ UTILIZZARE RegCreateKeyExA PER OTTENERE PERSISTENZA CREANDO NUOVE CHIAVI DI REGISTRO O MODIFICANDO CHIAVI ESISTENTI ED ASSICURANDOSI CHE IL CODICE MALEVOLO VENGA ESEGUITO OGNI VOLTA CHE IL SISTEMA VIENE AVVIATO. PER ESEMPIO, POTREBBE AGGIUNGERE UNA VOCE NELLA CHIAVE RUN PER ESEGUIRE AUTOMATICAMENTE IL MALWARE ALL'AVVIO DEL SISTEMA

PER QUEL CHE RIGUARDA IL METODO IN CUI VENGONO PASSATI I PARAMETRI ALLA SUDDETTA FUNZIONE, NEL MODULO SI È VISTO CHE LA CONVENZIONE DI CHIAMATA PIÙ COMUNE IN MOLTI SISTEMI OPERATIVI QUANDO SI UTILIZZA L'ARCHITETTURA X86 È «PUSHARE» I PARAMETRI SULLO STACK PRIMA DELLA CHIAMATA (CALL) ALLA FUNZIONE RegCreateKeyExA. I PARAMETRI VERRANNO LETTI DALLA FUNZIONE IN ORDINE INVERSO, QUINDI A PARTIRE DA hKey PER FINIRE CON lpdwDisposition.

```
.text:00401017                push    offset SubKey   ; "SOFTWARE\\Microsoft\\Windows NT\\Cu
```

TROVIAMO ALLA LOCAZIONE DI MEMORIA 00401017 - PUSH offset SubKey - L'INDIRIZZO DELLA SOTTOCHIAVE DI REGISTRO CHE VIENE SPINTO NELLO STACK. IL NOME VICINO AL CODICE INDICA CHE POTREBBE ESSERE IL NOME DELLA SOTTOCHIAVE CHE VERRÀ CREATA DAL PROCESSO hKey IN WINLOGON -> COMPONENTE DEL SISTEMA OPERATIVO WINDOWS CHE SI OCCUPA DELLA GESTIONE DELLA SESSIONE DI ACCESSO (LOGIN) E DISCONNESSIONE (LOGOUT) DEGLI UTENTI.

```
.text:00401027                test    eax, eax
.text:00401029                jz      short loc_401032
```

PER QUEL CHE RIGUARDA IL SIGNIFICATO DELLE ISTRUZIONI COMPRESE TRA GLI INDIRIZZI 00401027 E 00401029 VEDIAMO:

- UN'ISTRUZIONE CONDIZIONALE TEST, CHE È SIMILE ALL'ISTRUZIONE AND LOGICO BIT A BIT, MA NON VA A MODIFICARE IL CONTENUTO DEGLI OPERANDI (CIOÈ EAX E SE STESSO). MODIFICA INVECE IL FLAG ZF (ZERO FLAG) DEL REGISTRO EFLAGS, CHE VIENE SETTATO AD 1 SE E SOLO SE IL RISULTATO DELL'AND È 0. (0 AND 1 = 0 * 1 = 0 -> ZeroFlag =1). VIENE DI FATTO UTILIZZATO PER CONTROLLARE SE UN VALORE È ZERO O MENO. SE TEST È ZERO, LO ZF È 1.
- UN CONDITIONAL JUMP DI TIPO JZ, CHE NEL FLUSSO DI CONTROLLO SALTA AD UNA DETERMINATA LOCAZIONE DI MEMORIA (IN QUESTO CASO 00401032) SE ZF È PARI A UNO. ED A MENO CHE IL VALORE CONTENUTO NEL REGISTRO EAX NON SIA 0, IL SALTO NON AVVERRÀ.

```
.text:00401032 loc_401032:                             ; CODE XREF: sub_401000+29↑j
.text:00401032                mov     ecx, [ebp+cbData]
```

QUESTA OPERAZIONE EQUIVALE AD UN CICLO IF IN C COME QUELLO SEGUENTE (QUI, EAX RAPPRESENTA UNA VARIABILE IN C CHE CONTIENE IL VALORE CHE ERA NEL REGISTRO EAX):

```
if (eax==0)
{
// Vai a loc_401032
}
else
{
// Riprova a fare un'operazione (ad esempio..)
}
```

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

PER QUEL CHE RIGUARDA LA CHIAMATA ALLA LOCAZIONE 00401047 POSSO VEDERE CHE SI TRATTA DI UNA CALL ALLA FUNZIONE RegSetValueExA, CHE È UNA FUNZIONE DELL'API DI WINDOWS CHE IMPOSTA IL VALORE DI UNA VOCE NEL REGISTRO DI SISTEMA. IL PREFISSO DS: INDICA CHE L'INDIRIZZO DELLA FUNZIONE È PRESO DAL REGISTRO DS, CHE È IL SEGMENTO DATI.
QUESTA FUNZIONE, QUINDI, IMPARTISCE ISTRUZIONI AFFINCHÈ offset ValueName ABBIA VALORE "GinaDLL" IN UNA SPECIFICA CHIAVE DI REGISTRO IDENTIFICATA DA hKey.