BUILD WEEK 3

MALWARE ANALYSIS AND REVERSE ENGINEERING

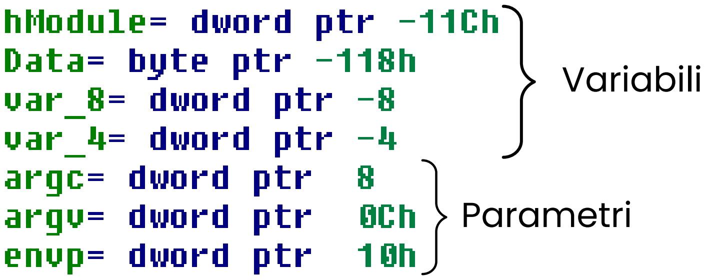
REPORTED BY:

FERNANDO CATRAMBONE
ALESSANDRO MOSCETTI
MATTEO MURILLO
MICHAEL POGGIALI
BENEDETTA FORESTIERI
LUCA GALLEANI
NATALINO IMBROGNO
DAVIDE DIGLIO

Day 1

Con riferimento al file eseguibile **Malware_Build_Week_U3**, rispondere ai seguenti quesiti utilizzando i tool e le tecniche apprese nelle lezioni teoriche:

- Quanti **parametri** sono passati alla funzione **Main**()?
- Quante **variabili** sono dichiarate nella funzione **Main**()?



```
hModule= dword ptr -11Ch
Data= byte ptr -118h
var_8= dword ptr -8
var_4= dword ptr -4
argc= dword ptr  8
argv= dword ptr  0Ch
envp= dword ptr  10h
```

Utilizzando il programma “**Ida pro**” siamo andati ad analizzare il codice malevolo (Malware_Build_Week_U3) alla funzione **Main**, questo perchè è la funzione di ingresso principale del programma che viene eseguita quando viene avviato.

Abbiamo esaminato la funzione **Main()** e notato che i suoi **tre parametri** sono individuati da offset positivo rispetto al registro EBP, indicando che i valori dei parametri sono allocati a una certa distanza in avanti rispetto a EBP.

Allo stesso tempo, abbiamo rilevato la presenza di **quattro variabili** all'interno della funzione **Main()**, ciascuna identificata da un offset negativo rispetto al registro EBP. Questo suggerisce che lo spazio di memoria assegnato a queste variabili si trova a una certa distanza all'indietro rispetto a EBP.

La differenza tra **parametro** e **variabile** sta nell'utilizzo durante l'esecuzione del programma: i parametri sono valori passati a una funzione quando viene chiamata, mentre le variabili sono spazi di memoria utilizzati per conservare dati all'interno della funzione. La distinzione è evidenziata dagli offset positivi per i parametri e dagli offset negativi per le variabili rispetto al registro EBP.

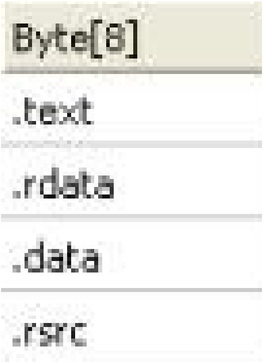
Day 1

Con riferimento al file eseguibile **Malware_Build_Week_U3**, rispondere ai seguenti quesiti utilizzando i tool e le tecniche apprese nelle lezioni teoriche:

- Quali **sezioni** sono presenti all'interno del file eseguibile?
- Quali **librerie** importa il Malware?

L'analisi condotta attraverso **CFFExplorer** ha consentito di ottenere una panoramica più dettagliata delle attività che può effettuare il malware.
Le **sezioni** da cui è composto il malware sono:

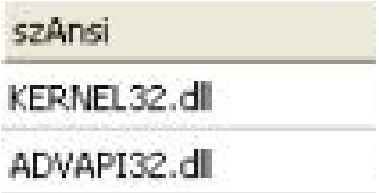
- **.text**: contiene le istruzioni che la CPU eseguirà una volta che il software sarà avviato.
- **.data**: contiene i dati e le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.
- **.rdata**: contiene i dati disponibili in sola lettura come librerie o funzioni importate o esportate dal programma.
- **.rsrc**: include le risorse utilizzate dall'eseguibile come ad esempio icone, immagini, menu e stringhe che non sono parte dell'eseguibile stesso.



Byte[8]
.text
.rdata
.data
.rsrc

Il malware utilizza funzioni provenienti da due **librerie**:

- **Kernel32.dll**: contiene le funzioni principali per l'interazione con il sistema operativo.
- **Advapi32.dll**: sono presenti le funzioni necessarie per interagire con il registro di Windows.



szAnsi
KERNEL32.dll
ADVAPI32.dll

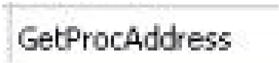
In questo modo, il malware sfrutta le risorse di tali librerie per eseguire operazioni specifiche, coinvolgendo sia il sistema operativo che il registro di Windows.

Day 1

Ipotesi del comportamento del **Malware_Build_Week_U3** dalle informazioni trovate con **CFFExplorer**

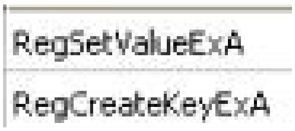
1. L'analisi delle librerie di questo malware ha rivelato una serie di funzioni chiave che indicano un comportamento potenzialmente dannoso e orientato all'attacco.

   - L'uso di **GetProcAddress** indica una dinamicità nel caricamento di funzioni, suggerendo che il malware vada a caricare altre librerie e funzioni.



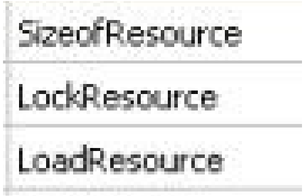
GetProcAddress

   - Le funzioni **RegSetValueExA** e **RegCreateKeyExA** suggeriscono che il malware potrebbe cercare di persistere nel sistema attraverso la modifica del Registro di Sistema.



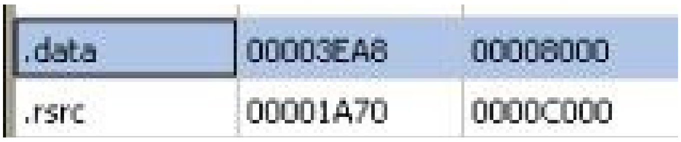
RegSetValueExA
RegCreateKeyExA

   - L'impiego di **LoadResource**, **LockResource**, e **SizeofResource** indica un interesse verso la manipolazione delle risorse presenti nell'eseguibile del malware.

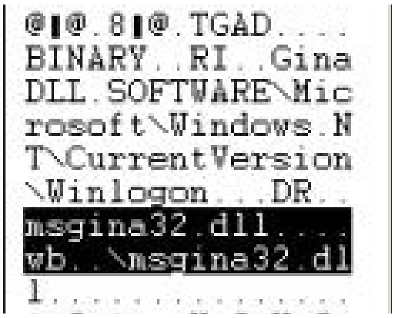


SizeofResource
LockResource
LoadResource

Dalle funzioni emerse nelle librerie possiamo supporre che si tratti di un malware della famiglia dei **Dropper**.
Inoltre analizzando la sezione **.data,** che contiene i dati necessari al programma per funzionare, abbiamo individuato un file di nome **msgina32.dll** e un path che riguarda **winlogon**, che è un processo Windows che riguarda il logon interattivo.
Da questi elementi possiamo supporre che il malware tramite un componente malevolo interferisca con l'accesso per rubare le credenziali.



.data	00003EA8	00008000
.rsrc	00001A70	0000C000

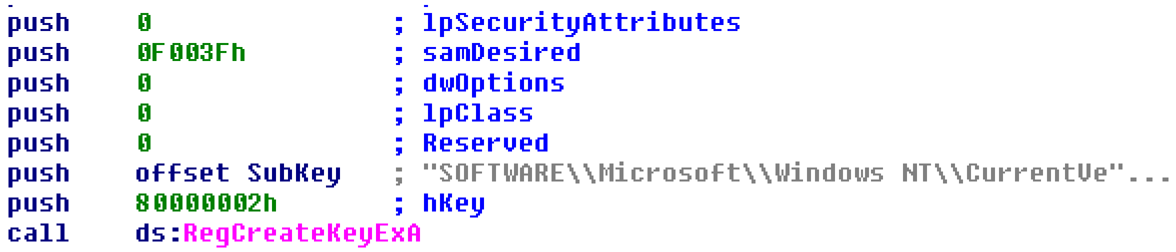


```
@▌@.8▌@.TGAD....
BINARY..RI..Gina
DLL.SOFTWARE\Mic
rosoft\Windows.N
T\CurrentVersion
\Winlogon...DR..
msgina32.dll....
wb..\msgina32.dl
l...............
```

Day 2

Con riferimento al **Malware** in analisi, spiegare:

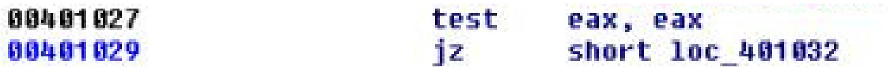
- Lo scopo della funzione chiamata alla locazione di memoria **00401021**
- Come vengono passati i parametri alla funzione alla locazione **00401021**
- Che **oggetto** rappresenta il parametro alla locazione **00401017**



```
push    0               ; lpSecurityAttributes
push    0F003Fh         ; samDesired
push    0               ; dwOptions
push    0               ; lpClass
push    0               ; Reserved
push    offset SubKey   ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe"...
push    80000002h       ; hKey
call    ds:RegCreateKeyExA
```

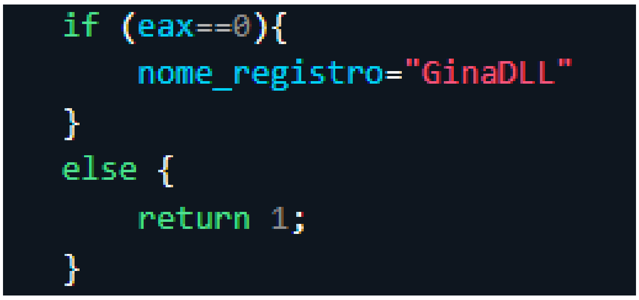
I valori necessari per questa funzione vengono trasmessi attraverso lo stack di memoria mediante l'operazione "**push**". Prima di eseguire la funzione, i parametri vengono posti nello stack in sequenza, e la funzione li preleva da lì durante l'esecuzione.
L'indirizzo **00401017** nel codice contiene la chiave il cui valore viene fornito come argomento a **RegCreateKeyExA**.
Questa funzione sta ad indicare che il programma sta cercando di creare o aprire una chiave del Registro di Sistema per scrivere o leggere informazioni al fine di manipolare il Registro di Sistema.
L'**oggetto** nella loc **00401017** contiene il percorso della chiave del Registro di Sistema che si desidera creare o aprire.

- Spiegare il significato delle istruzioni comprese tra gli indirizzi **00401027** e **00401029**
- Tradurre il codice Assembly nel corrispondente **costrutto C.**



```
00401027                test    eax, eax
00401029                jz      short loc_401032
```

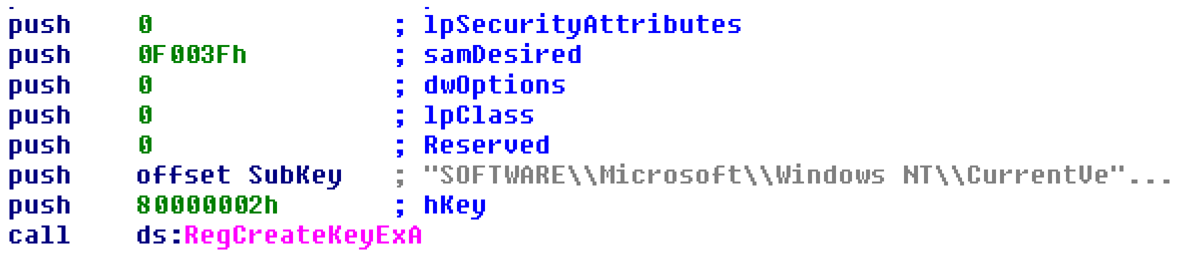
L'istruzione **test eax, eax** è simile all'operatore logico **AND** ma a differenza che non memorizza il risultato in **eax.** In particolare, effettuerà un test bit a bit tra il registro **eax** e se stesso impostando cosi i flag di zero (**ZF**) a 0.
L'istruzione **jz short loc_401032** a questo punto effettuerà un salto alla locazione solo se il flag di zero (**ZF**) sarà impostato a zero.
Questo potrebbe essere una sua rappresentazione in **costrutto C**:



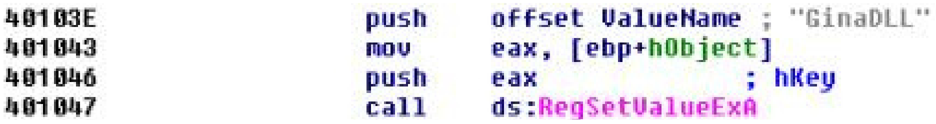
```
if (eax==0){
    nome_registro="GinaDLL"
}
else {
    return 1;
}
```

Day 2

Con riferimento al **Malware** in analisi, spiegare:



```
push    0               ; lpSecurityAttributes
push    0F003Fh         ; samDesired
push    0               ; dwOptions
push    0               ; lpClass
push    0               ; Reserved
push    offset SubKey   ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe"...
push    80000002h       ; hKey
call    ds:RegCreateKeyExA
```

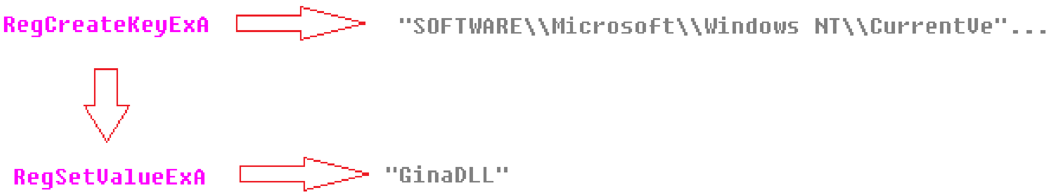


```
40103E                push    offset ValueName ; "GinaDLL"
401043                mov     eax, [ebp+hObject]
401046                push    eax             ; hKey
401047                call    ds:RegSetValueExA
```

- Qual è il valore di «**ValueName**» alla locazione **00401047**

Il valore del parametro ValueName è "**GinaDLL**"

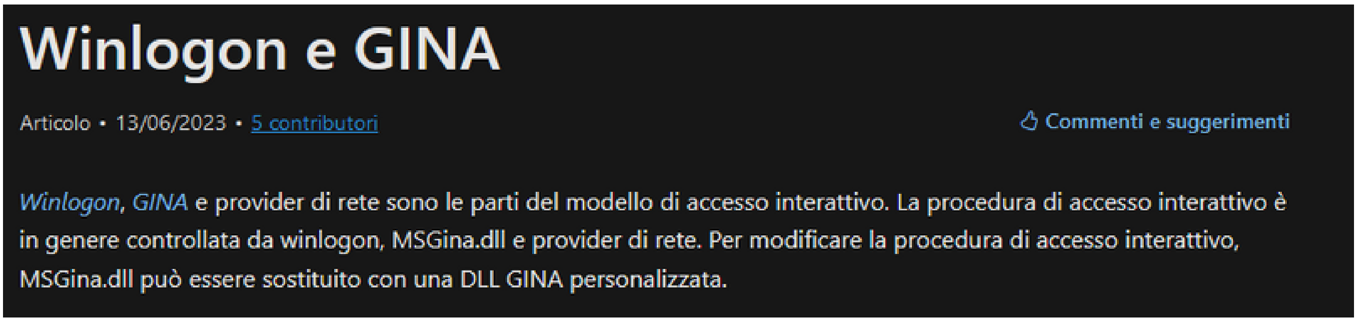
- Spiegate quale **funzionalità** sta implementando il Malware in queste sezione.



RegCreateKeyExA → "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe"...

RegSetValueExA → "GinaDLL"

In queste sezione il malware sta creando una nuova chiave di registro **RegCreateKeyExA** e sta settando il suo nome a: "**GinaDLL**" utilizzando la funzione **RegSetValueExa** . Come possiamo vedere GINA e Winlogon servono per gestire la procedura di accesso.



Winlogon e GINA

Articolo • 13/06/2023 • 5 contributori

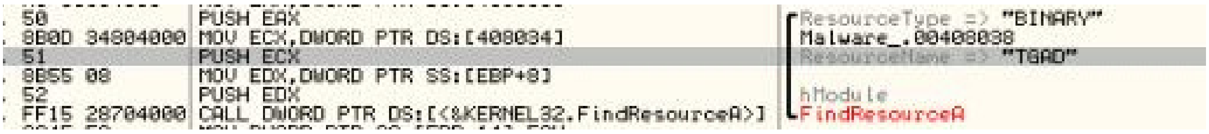
Winlogon, *GINA* e provider di rete sono le parti del modello di accesso interattivo. La procedura di accesso interattivo è in genere controllata da winlogon, MSGina.dll e provider di rete. Per modificare la procedura di accesso interattivo, MSGina.dll può essere sostituito con una DLL GINA personalizzata.

https://learn.microsoft.com/it-it/windows/win32/secauthn/winlogon-and-gina

Day 3

Analizzando le routine tra le locazioni di memoria **00401080** e **00401128**:

- Qual è il valore del parametro «**ResourceName**» passato alla funzione

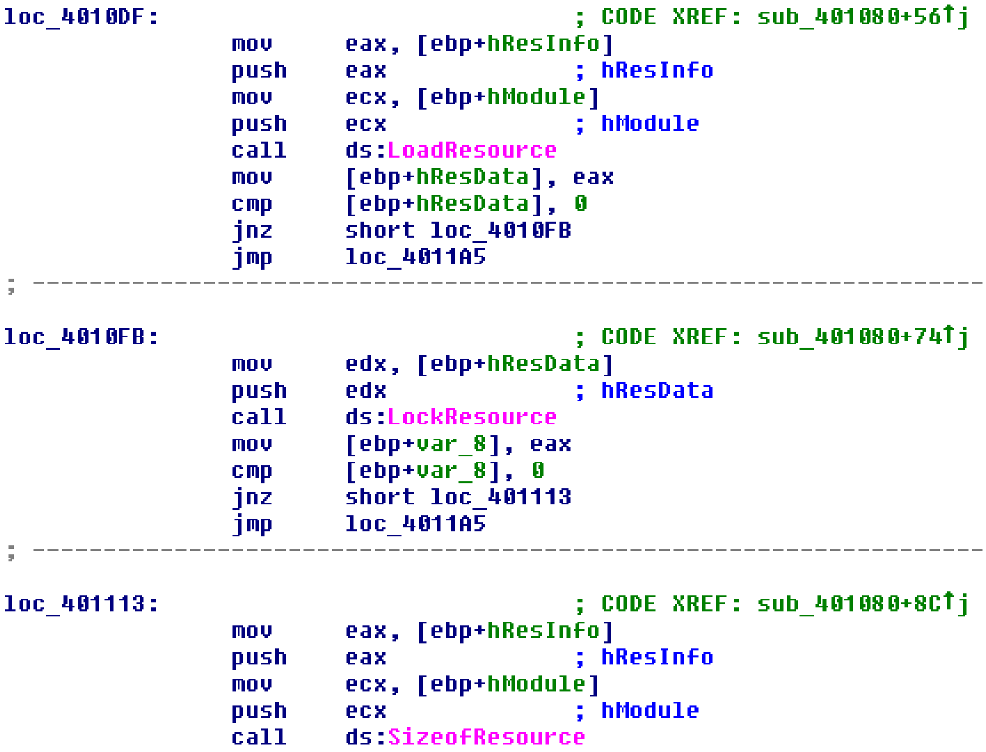


```
. 50            PUSH EAX                                     ┌ResourceType => "BINARY"
. 8B0D 34804000 MOV ECX,DWORD PTR DS:[408034]                │Malware_.00408038
. 51            PUSH ECX                                     │ResourceName => "TGAD"
. 8B55 08       MOV EDX,DWORD PTR SS:[EBP+8]                 │
. 52            PUSH EDX                                     │hModule
. FF15 28704000 CALL DWORD PTR DS:[<&KERNEL32.FindResourceA>] └FindResourceA
```

Tramite l'utilizzo del software **"OllyDBG"** abbiamo individuato che il valore del parametro **"ResourceName"** è **"TGAD"**

- Il susseguirsi delle chiamate di funzione che effettua il Malware in questa sezione di codice che **funzionalità** sta implementando?

Dalle chiamate di funzione presenti in questa sezione di codice abbiamo una conferma che il malware sia un **dropper**, ovvero un software malevolo che svolge il ruolo di un trasportatore di altri malware, facilitando la loro introduzione e esecuzione nell'ambiente del computer infetto



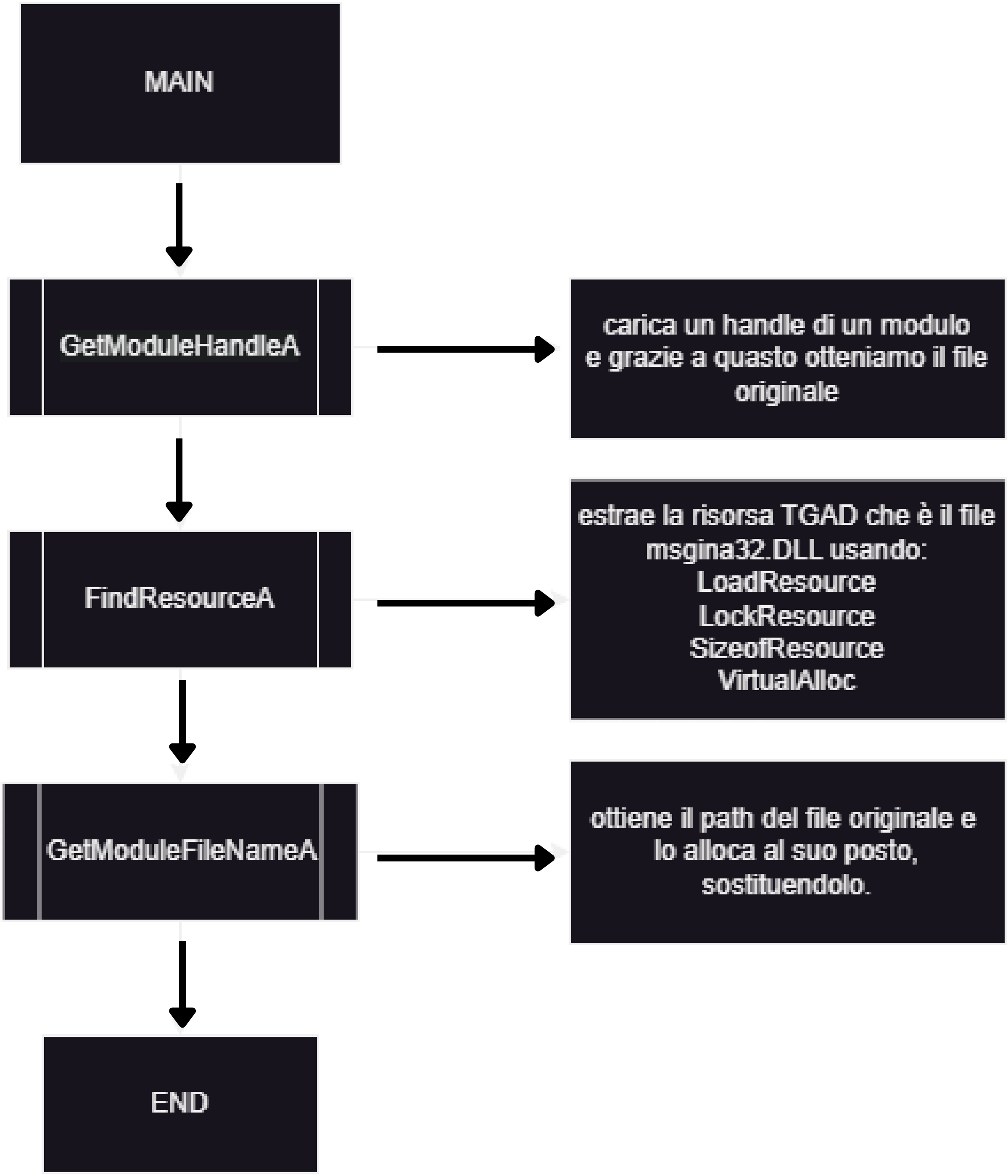
```
loc_4010DF:                             ; CODE XREF: sub_401080+56↑j
                mov     eax, [ebp+hResInfo]
                push    eax             ; hResInfo
                mov     ecx, [ebp+hModule]
                push    ecx             ; hModule
                call    ds:LoadResource
                mov     [ebp+hResData], eax
                cmp     [ebp+hResData], 0
                jnz     short loc_4010FB
                jmp     loc_4011A5
; ---------------------------------------------------------------------------

loc_4010FB:                             ; CODE XREF: sub_401080+74↑j
                mov     edx, [ebp+hResData]
                push    edx             ; hResData
                call    ds:LockResource
                mov     [ebp+var_8], eax
                cmp     [ebp+var_8], 0
                jnz     short loc_401113
                jmp     loc_4011A5
; ---------------------------------------------------------------------------

loc_401113:                             ; CODE XREF: sub_401080+8C↑j
                mov     eax, [ebp+hResInfo]
                push    eax             ; hResInfo
                mov     ecx, [ebp+hModule]
                push    ecx             ; hModule
                call    ds:SizeofResource
```

- È possibile identificare questa funzionalità utilizzando l'analisi **statica basica**? (elencare le evidenze a supporto).

Già dall'analisi **statica basica** avevamo intuito il possibile funzionamento del malware tramite la presenze delle funzioni **LoadResouce**, **Lock Resource** **SizeOfResource** all'interno della libreria **KERNEL32.dll** oltre che alla presenza della sezione **.rsrc** che contiene le ulteoriori risorse che il **dropper** va a caricare nella macchina vittima.

Day 3

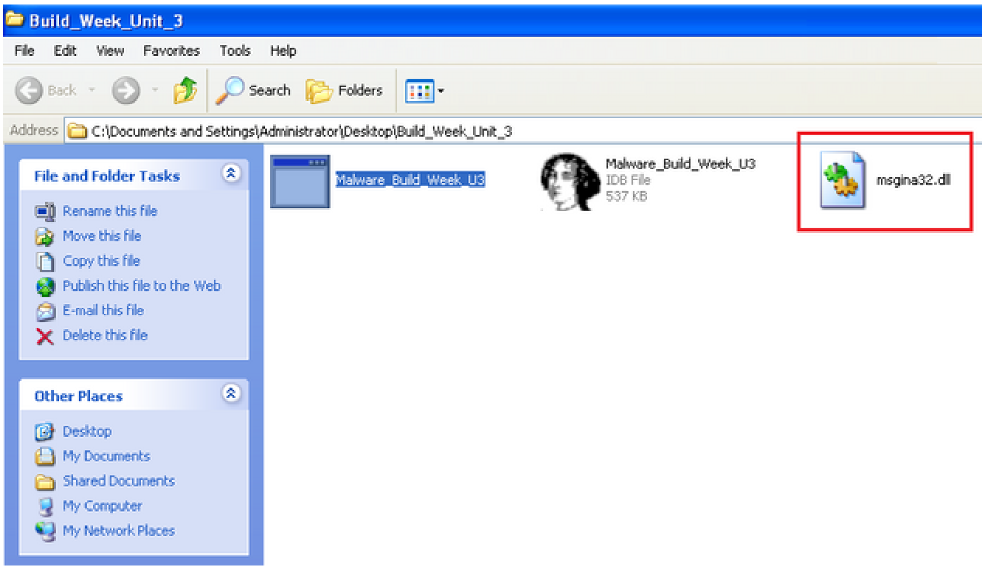
- Disegnare un diagramma di flusso che comprenda le tre funzioni che descrivono le funzionalità appena viste del malware.


MAIN
GetModuleHandleA
carica un handle di un modulo e grazie a quasto otteniamo il file originale
FindResourceA
estrae la risorsa TGAD che è il file msgina32.DLL usando:
LoadResource
LockResource
SizeofResource
VirtualAlloc
GetModuleFileNameA
ottiene il path del file originale e lo alloca al suo posto, sostituendolo.
END

Come si può vedere in figura questo diagramma semplificato mostra il comportamento di queste tre funzioni all’interno del **main** ed il loro utilizzo.

Day 4

- Preparate l'ambiente ed i tool per l'esecuzione del Malware
- Cosa notate all'interno della cartella dove è situato l'eseguibile del Malware?



Address: C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3

Malware_Build_Week_U3

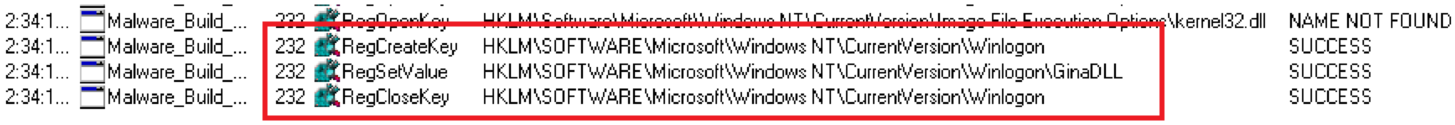
Malware_Build_Week_U3
IDB File
537 KB

msgina32.dll

Una volta preparato il nostro laboratorio, isolando la nostra macchina virtuale abbiamo avviato il malware, all'interno della stessa cartella viene creato un file di nome "**msgina32.dll**". Questa evidenza ci da conferma sulle ipotesi precedentemente fatte ovvero che si tratta di un **dropper** che estrae un file **.dll**

Filtrate includendo solamente l'attività sul registro di Windows.

- Quale chiave di registro viene creata?
- Quale valore viene associato alla chiave di registro creata?

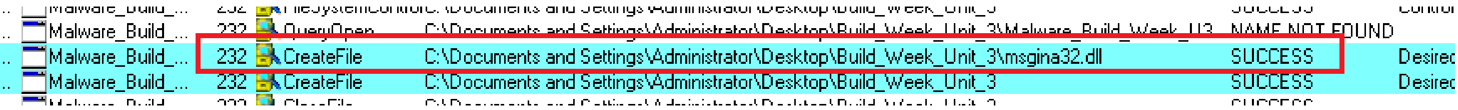


```
2:34:1...  Malware_Build_...  232  RegOpenKey    HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kernel32.dll  NAME NOT FOUND
2:34:1...  Malware_Build_...  232  RegCreateKey  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon                                   SUCCESS
2:34:1...  Malware_Build_...  232  RegSetValue   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL                           SUCCESS
2:34:1...  Malware_Build_...  232  RegCloseKey   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon                                   SUCCESS
```

Viene creata una chiave di registro all'indirizzo di **Winlogon**, a questa chiave di registro viene associato il valore **"GinaDLL"** che abbiamo già visto nelle giornate precedenti.

Passate ora alla visualizzazione dell'attività sul file system.

- Quale chiamata di sistema ha modificato il contenuto della cartella dove è presente l'eseguibile del Malware?

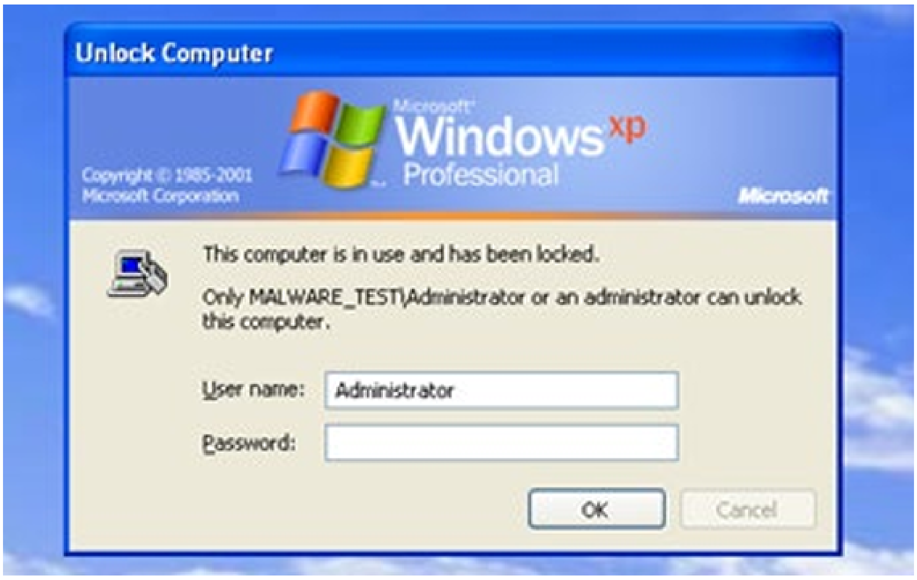


```
..  Malware_Build_...  232  FileSystemControl  C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3                            SUCCESS         Control
..  Malware_Build_...  232  QueryOpen          C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3      NAME NOT FOUND
..  Malware_Build_...  232  CreateFile         C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll               SUCCESS         Desirec
..  Malware_Build_...  232  CreateFile         C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3                            SUCCESS         Desirec
..  Malware_Build_...  232  CloseFile          C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3                            SUCCESS
```

La funzione chiamata è **"CreateFile"** come possiamo vedere in figura crea il nostro file **msgina32.dll**.

Day 5

GINA (Graphicauthentication& authentication) è un componente di Windows che permette l'autenticazione degli utenti tramite interfaccia grafica, ovvero permette agli utenti di inserire **username** e **password** nel classico riquadro Windows, come quello in figura.



Unlock Computer

Copyright © 1985-2001 Microsoft Corporation

This computer is in use and has been locked.

Only MALWARE_TEST\Administrator or an administrator can unlock this computer.

User name: Administrator

Password:

- Cosa può succedere se il file **.dll lecito** viene sostituito con un file **.dll malevolo** che intercetta i dati inseriti?

Sapendo che GINA è un componente di Windows che permette l'autenticazione tramite interfaccia grafica nel caso in cui un .dll lecito venga sostituito con un file .dll malevolo c'è il rischio che le credenziali degli utenti vengano rubate.

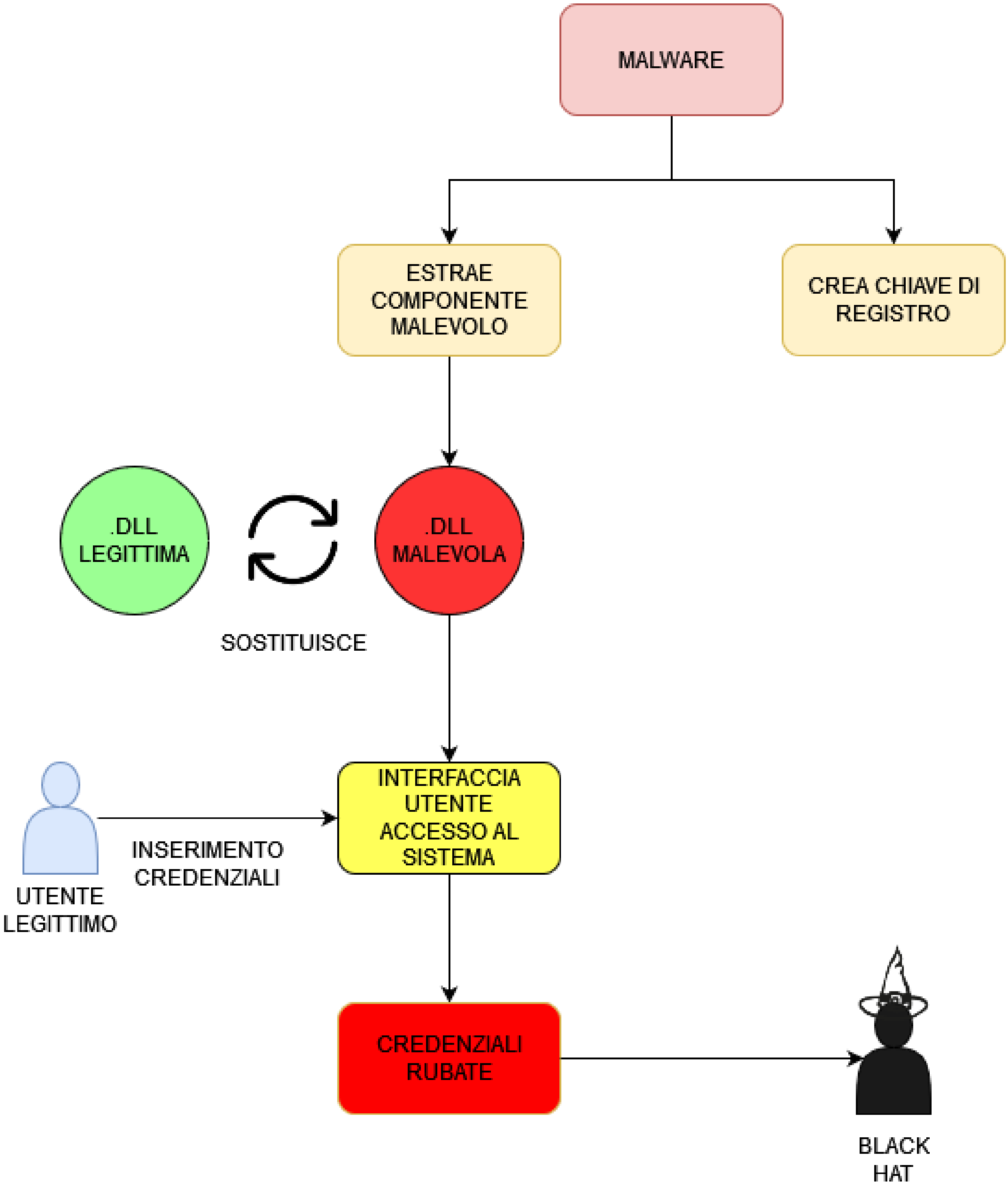
- Delineate il **profilo** del Malware e delle sue funzionalità.

Possiamo concludere che il comportamento del malware è così descritto:

- Estrae una componente malevola di nome "GinaDLL" dalle sue risorse all'interno della cartella dove si trova il malware.
- Crea una chiave di registro "Winlogon" che è parte del sistema operativo Windows e serve per l'autenticazione interattiva.
- Sostituisce il componente .dll legittimo con quello malevolo estratto precedentemente.
- Il componente malevolo viene utilizzato per rubare le credenziali.

Day 5

- Unite tutti i punti visti fino ad esso per creare un grafico che ne rappresenti lo scopo ad alto livello.



Bonus 1

- Spiegare l’analisi di **Any.rune** del file malevolo

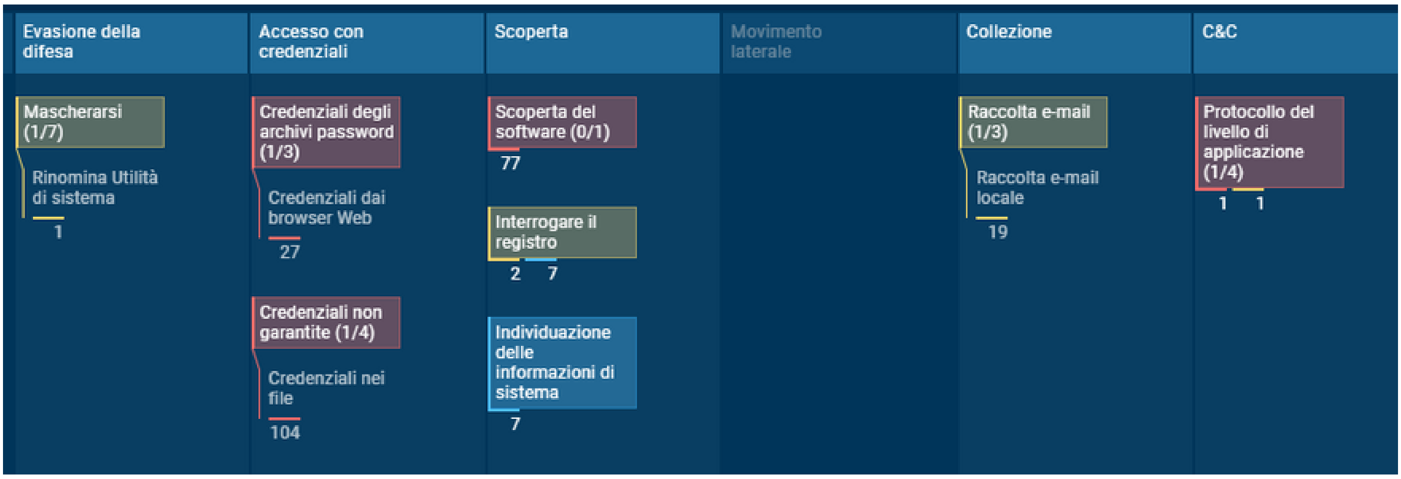
Dall’analisi di **Any.run** abbiamo scoperto che questo è un file malevolo, infatti utilizza un malware firmato **Agent Tesla**, questo è uno **spyware** che raccoglie informazioni sulle azioni delle sue vittime registrando le sequenze di tasti e le interazioni fatte dall'utente.
Può essere contratto attraverso campagne di **phishing**
(L’aggressore invia i file malevoli attraverso **email** mascherandosi da sito legittimo)
Una volta **scaricato/cliccato** il malware si comporterà dunque come uno **stealer**, un software dannoso destinato a **ottenere l'accesso non autorizzato** alle informazioni degli utenti e **trasferirle all'aggressore** come **file** e **password**.
I ladri dunque sono in grado di **spiare la macchina vittima** e registrare ogni tasto premuto dall’utente acquisendo cosi tutte le informazioni sensibili.

Nomi dei processi malevoli e numero identificativo:

Uqzqkjvjt.exe (PID: 2308)
RegAsm.exe (PID: 792)

Qui di seguito ci sono elencati i vari step che che effettua il codice malevolo:

- Esecuzione manuale da parte dell’utente
- Rilascia il malware eseguibile dopo l'avvio del pc
- Il processo elimina l'eseguibile legittimo di Windows
- Mascheramento da file legittimo
- Agent Tesla in azione
- Ruba le credenziali dai browser Web
- Si connette alla porta SMTP
- Accede ai profili Microsoft Outlook
- Si connette al server CnC per trasferire le informazioni sensibili dell’utente.



Evasione della difesa	Accesso con credenziali	Scoperta	Movimento laterale	Collezione	C&C
Mascherarsi (1/7) Rinomina Utilità di sistema 1	Credenziali degli archivi password (1/3) Credenziali dai browser Web 27 Credenziali non garantite (1/4) Credenziali nei file 104	Scoperta del software (0/1) 77 Interrogare il registro 2 7 Individuazione delle informazioni di sistema 7		Raccolta e-mail (1/3) Raccolta e-mail locale 19	Protocollo del livello di applicazione (1/4) 1 1

https://app.any.run/tasks/444c2f53-1cce-49a9-8336-2539896df32b/

Bonus 1

- Spiegare l’analisi di **Any.rune** del file malevolo

Nel report di **Any.run** è chiaro si tratti di un malware dal nome **Rhadamanthys** scritto in linguaggio **C++** che ruba informazioni ed estrae dati sensibili.
La sua catena operativa stratificata e le tattiche di evasione avanzate lo rendono un **rischio importante** nel panorama della sicurezza informatica.
Nello specifico viene **diffuso tramite siti** che sembrano essere legittimi e dai quali viene scaricato il file malevolo che contiene il malware, una volta eseguito **ruba i dati** dell’utente vittima e li invia ad un server C&C controllato dal Black Hat.

Fa parte anch’esso della famiglia degl**i stealer** cioè un gruppo di **software dannoso** destinato ad **ottenere l'accesso non autorizzato** alle informazioni degli utenti e trasferirle all'aggressore.

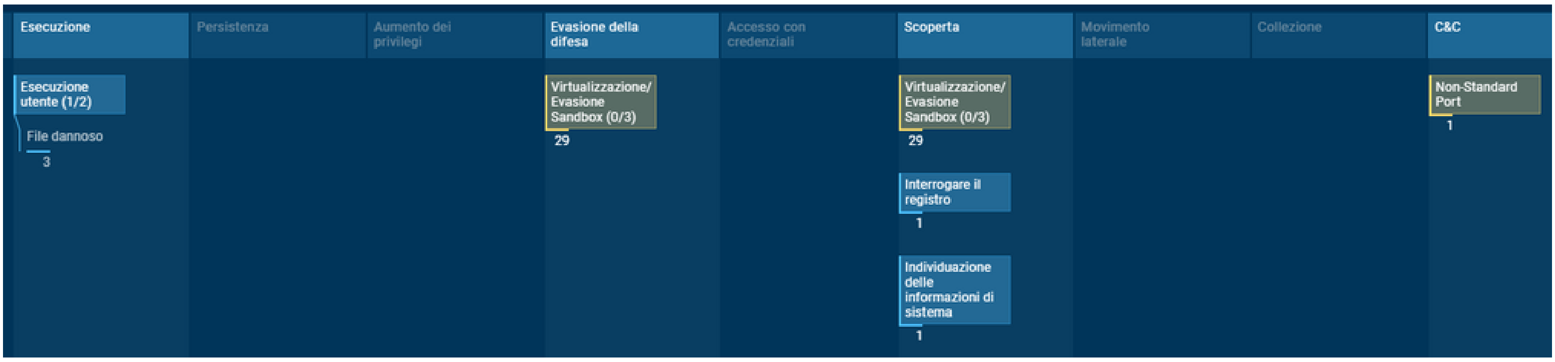
I principali metodi di distribuzione osservati per questa minaccia includono **siti Web** di software **falsi** promossi tramite **Google Ads** ed **e-mail di phishing**, che prendono di mira le vittime indipendentemente dalla loro posizione o settore.
Nel complesso, **Rhadamanthys** vanta un ampio **set di funzionalità di furto** e rappresenta una minaccia significativa.

Nomi dei processi malevoli e numero identificativo:

dialer.exe (PID: 3052)

Qui di seguito ci sono elencati i vari step che che effettua il codice malevolo:

- Esecuzione manuale da parte dell’utente
- Rilascio del file eseguibile
- L'applicazione si avvia da sola
- RHADAMANTHYS si attiva
- Il processo controlla se viene eseguito in un’ambiente virtuale
- Il processo utilizza il file che ha scaricato
- Apertura di più finestre Chrome
- Estrazione dei dati sensibili
- Si connette al server dell’aggressore per il trasferimento.



Esecuzione	Persistenza	Aumento dei privilegi	Evasione della difesa	Accesso con credenziali	Scoperta	Movimento laterale	Collezione	C&C
Esecuzione utente (1/2) File dannoso 3			Virtualizzazione/ Evasione Sandbox (0/3) 29		Virtualizzazione/ Evasione Sandbox (0/3) 29			Non-Standard Port 1
					Interrogare il registro 1			
					Individuazione delle informazioni di sistema 1			

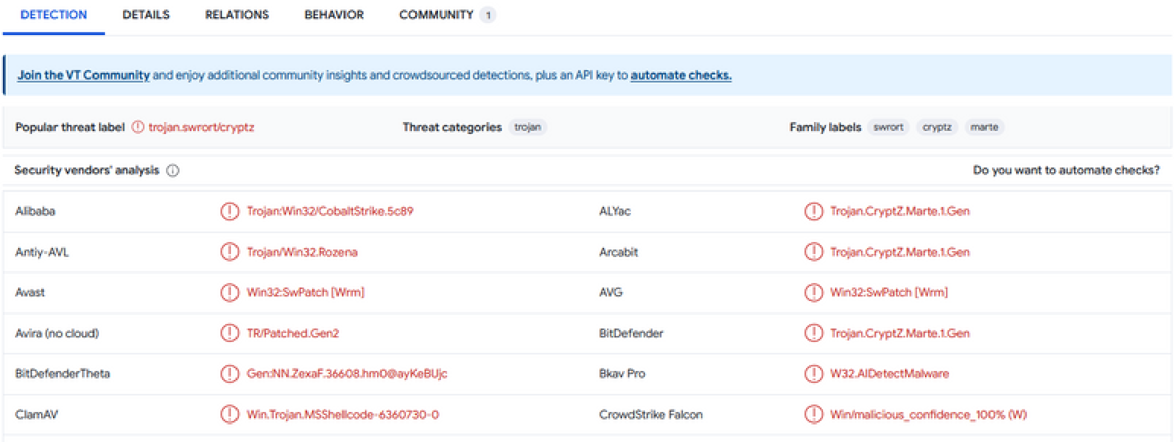
https://app.any.run/tasks/512b6efc-380b-40f5-8689-1027fa7852e2/

Bonus 2

- Analizzare il file **calcolatriceinnovativa50.exe**

Per far ciò abbiamo utilizzato diversi tool:

- **Virus Total**



DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 1

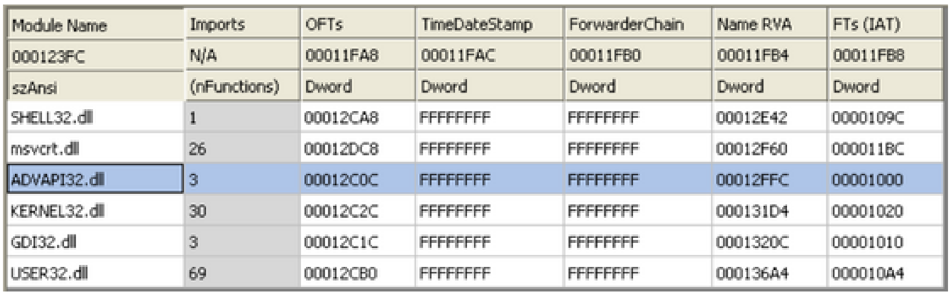
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label ⓘ trojan.swrort/cryptz — Threat categories: trojan — Family labels: swrort, cryptz, marte

Security vendors' analysis ⓘ — Do you want to automate checks?

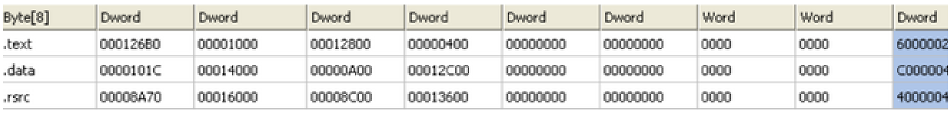
Alibaba	ⓘ Trojan:Win32/CobaltStrike.5c89	ALYac	ⓘ Trojan.CryptZ.Marte.1.Gen
Antiy-AVL	ⓘ Trojan/Win32.Rozena	Arcabit	ⓘ Trojan.CryptZ.Marte.1.Gen
Avast	ⓘ Win32:SwPatch [Wrm]	AVG	ⓘ Win32:SwPatch [Wrm]
Avira (no cloud)	ⓘ TR/Patched.Gen2	BitDefender	ⓘ Trojan.CryptZ.Marte.1.Gen
BitDefenderTheta	ⓘ Gen:NN.ZexaF.36608.hm0@ayKeBUjc	Bkav Pro	ⓘ W32.AIDetectMalware
ClamAV	ⓘ Win.Trojan.MSShellcode-6360730-0	CrowdStrike Falcon	ⓘ Win/malicious_confidence_100% (W)

- **CFFExplorer**



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000123FC	N/A	00011FA8	00011FAC	00011FB0	00011FB4	00011FB8
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
SHELL32.dll	1	00012CA8	FFFFFFFF	FFFFFFFF	00012E42	0000109C
msvcrt.dll	26	00012DC8	FFFFFFFF	FFFFFFFF	00012F60	000011BC
ADVAPI32.dll	3	00012C0C	FFFFFFFF	FFFFFFFF	00012FFC	00001000
KERNEL32.dll	30	00012C2C	FFFFFFFF	FFFFFFFF	000131D4	00001020
GDI32.dll	3	00012C1C	FFFFFFFF	FFFFFFFF	0001320C	00001010
USER32.dll	69	00012CB0	FFFFFFFF	FFFFFFFF	000136A4	000010A4

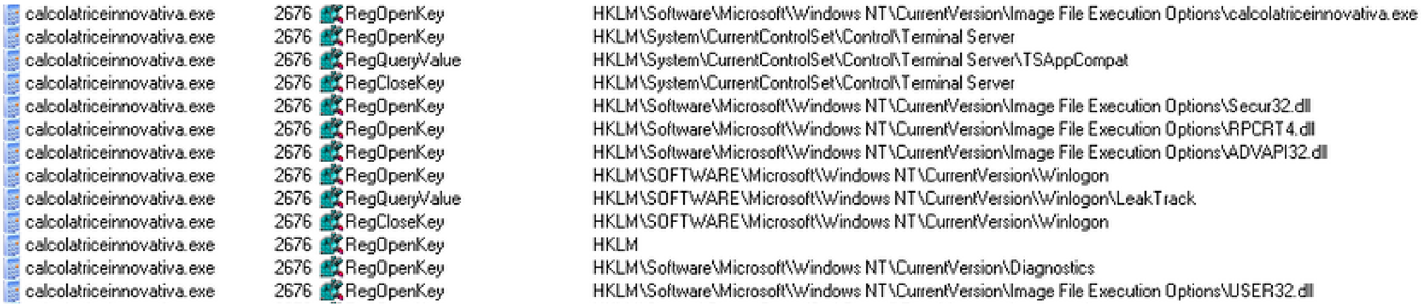
Librerie importate



Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000126B0	00001000	00012800	00000400	00000000	00000000	0000	0000	6000002
.data	0000101C	00014000	00000A00	00012C00	00000000	00000000	0000	0000	C000004
.rsrc	00008A70	00016000	00008C00	00013600	00000000	00000000	0000	0000	4000004

Sezioni headers

- **ProcessMonitor**



```
calcolatriceinnovativa.exe    2676 RegOpenKey      HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\calcolatriceinnovativa.exe
calcolatriceinnovativa.exe    2676 RegOpenKey      HKLM\System\CurrentControlSet\Control\Terminal Server
calcolatriceinnovativa.exe    2676 RegQueryValue   HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat
calcolatriceinnovativa.exe    2676 RegCloseKey     HKLM\System\CurrentControlSet\Control\Terminal Server
calcolatriceinnovativa.exe    2676 RegOpenKey      HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll
calcolatriceinnovativa.exe    2676 RegOpenKey      HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll
calcolatriceinnovativa.exe    2676 RegOpenKey      HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI32.dll
calcolatriceinnovativa.exe    2676 RegOpenKey      HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
calcolatriceinnovativa.exe    2676 RegQueryValue   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack
calcolatriceinnovativa.exe    2676 RegCloseKey     HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
calcolatriceinnovativa.exe    2676 RegOpenKey      HKLM
calcolatriceinnovativa.exe    2676 RegOpenKey      HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics
calcolatriceinnovativa.exe    2676 RegOpenKey      HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USER32.dll
```

Possiamo concludere che il file analizzato sia un malware.
Da **VirusTotal** possiamo notare che sia della famiglia dei **Trojan**.
Di conseguenza questo file una volta entrato nella macchina vittima andrà a **scaricare** il vero e proprio codice malevolo, un **keylogger**.
Il **Keylogger** è un tipo di malware che carpisce l'input utente, come la digitazione della tastiera o il puntatore del mouse per poi essere trasferito all'attaccante.
In questo caso però non sono presenti altre **funzionalità di rete** e quindi le informazioni ottenute dal malware non hanno modo di essere trasferite.

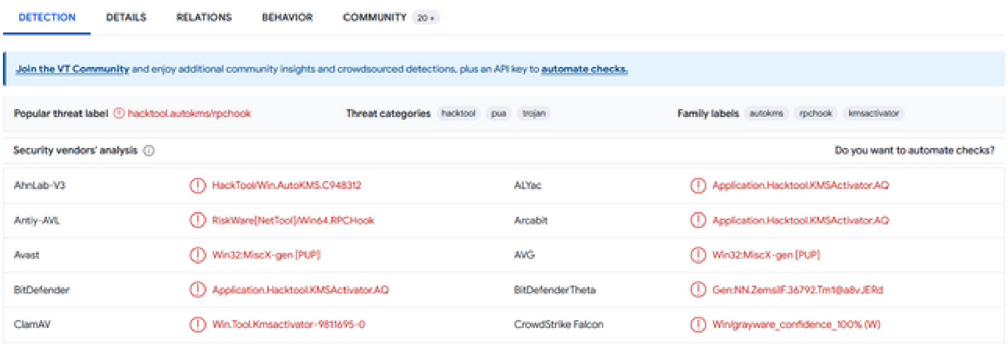
https://www.virustotal.com/gui/file/b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a

Bonus 2

Il nostro dipendente “sveglio” dice al SOC (in questo caso noi) che ha avviato in un pc questo file innocuo **AmicoNerd.zip**
Il nostro compito è convincere il dipendente che il file sia malevolo.

Abbiamo effettuato per questo file una serie di analisi.
Senza scendere nel dettaglio tecnico delle analisi sono state riscontrate diverse funzionalità che ci fanno ipotizzare che si tratti di una **backdoor**.
Quest’ultimi sono **malware** che stabiliscono una connessione permettendo di prendere il controllo della macchina vittima.
Per convincere il dipendente mostriamo il **report di VirusTotal** che lo segnala come malware.
Inoltre abbiamo nota questa minaccia, infatti si tratta di **KMSpico** (AutoPico), ovvero un file malevolo che **si maschera** da attivatore Windows (serve per conferire la licenza legittima ad un sistema windows che ne è sprovvisto)
che in realtà installa una **backdoor**.
Possiamo anche notare come dopo aver avviato il file viene **creata una cartella** che contiene i log delle attività del malware che immediatamente cerca di creare una **connessione ad un sito anonimo**.

- **Virus Total**



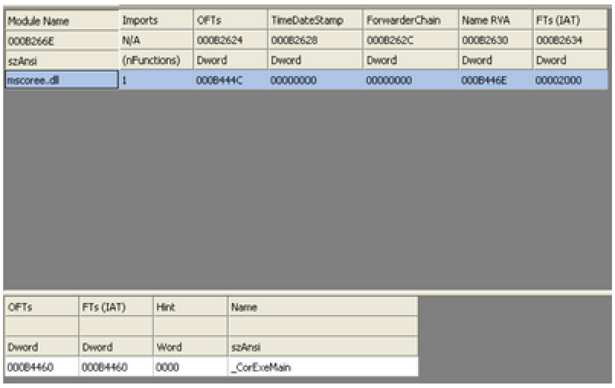
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Popular threat label hacktool.autokms/rpchook **Threat categories** hacktool pua trojan **Family labels** autokms rpchook kmsactivator

Security vendors' analysis Do you want to automate checks?

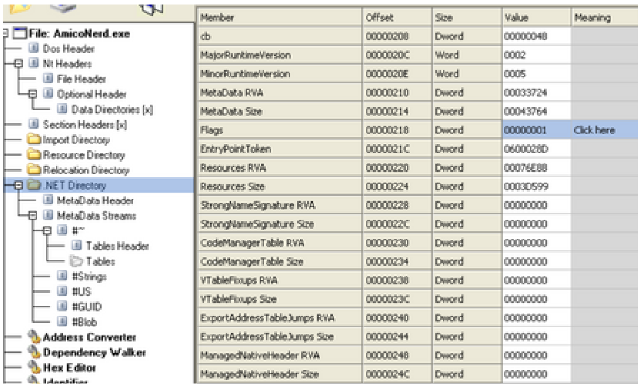
AhnLab-V3	HackTool/Win.AutoKMS.C948312	ALYac	Application.Hacktool.KMSActivator.AQ
Antiy-AVL	RiskWare[NetTool]/Win64.RPCHook	Arcabit	Application.Hacktool.KMSActivator.AQ
Avast	Win32:MiscX-gen [PUP]	AVG	Win32:MiscX-gen [PUP]
BitDefender	Application.Hacktool.KMSActivator.AQ	BitDefenderTheta	Gen:NN.ZemsilF.36792.Tm1@a8vJERd
ClamAV	Win.Tool.Kmsactivator-9811695-0	CrowdStrike Falcon	Win/grayware_confidence_100% (W)

- **CFFExplorer**

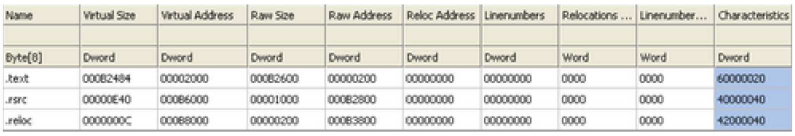


Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0008266E	N/A	000B2624	000B2628	000B262C	000B2630	000B2634
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
mscoree.dll	1	000B444C	00000000	00000000	000B446E	00002000

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
000B4460	000B4460	0000	_CorExeMain



Member	Offset	Size	Value	Meaning
cb	00000208	Dword	00000048	
MajorRuntimeVersion	0000020C	Word	0002	
MinorRuntimeVersion	0000020E	Word	0005	
MetaData RVA	00000210	Dword	00033724	
MetaData Size	00000214	Dword	00043764	
Flags	00000218	Dword	00000001	Click here
EntryPointToken	0000021C	Dword	0600028D	
Resources RVA	00000220	Dword	00076E88	
Resources Size	00000224	Dword	0003D599	
StrongNameSignature RVA	00000228	Dword	00000000	
StrongNameSignature Size	0000022C	Dword	00000000	
CodeManagerTable RVA	00000230	Dword	00000000	
CodeManagerTable Size	00000234	Dword	00000000	
VTableFixups RVA	00000238	Dword	00000000	
VTableFixups Size	0000023C	Dword	00000000	
ExportAddressTableJumps RVA	00000240	Dword	00000000	
ExportAddressTableJumps Size	00000244	Dword	00000000	
ManagedNativeHeader RVA	00000248	Dword	00000000	
ManagedNativeHeader Size	0000024C	Dword	00000000	

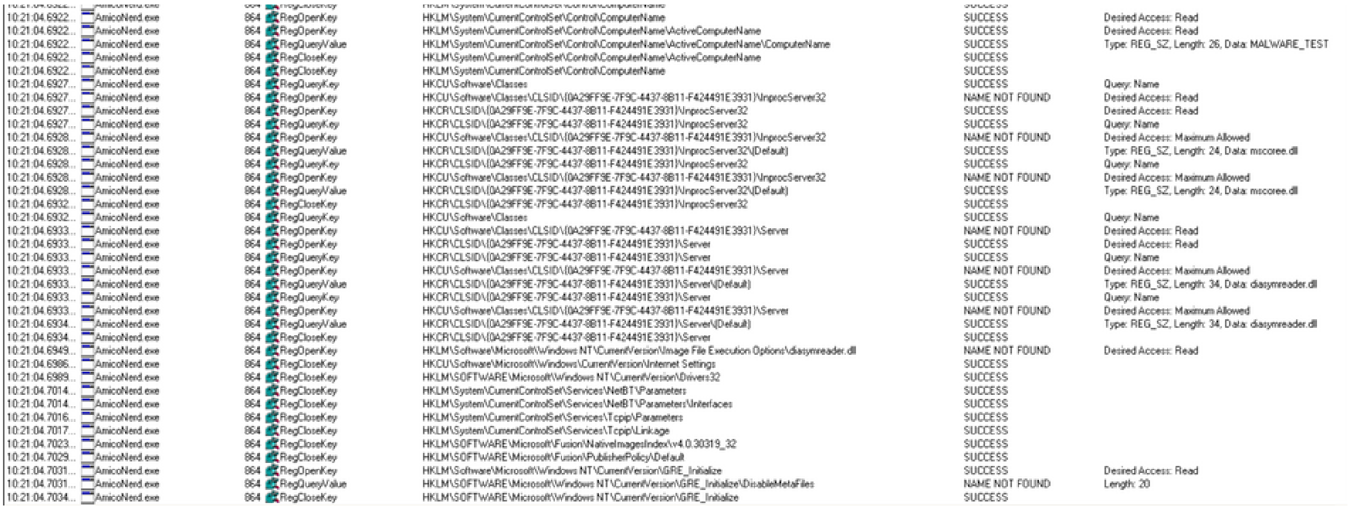


Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000B2484	00002000	000B2600	00000200	00000000	00000000	0000	0000	60000020
.rsrc	00000E40	000B6000	00001000	000B2800	00000000	00000000	0000	0000	40000040
.reloc	0000000C	000B8000	00000200	000B3800	00000000	00000000	0000	0000	42000040

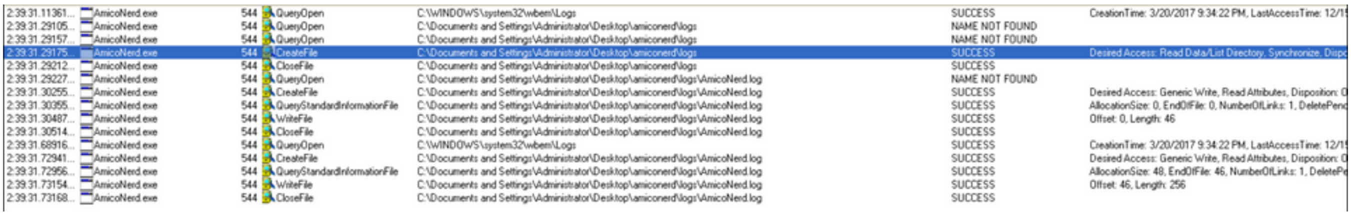
https://www.virustotal.com/gui/file/c6603d416dfc48894eda35d9a9a8523bdf9823e215ab926783ce6848aa8a62c4

Bonus 2

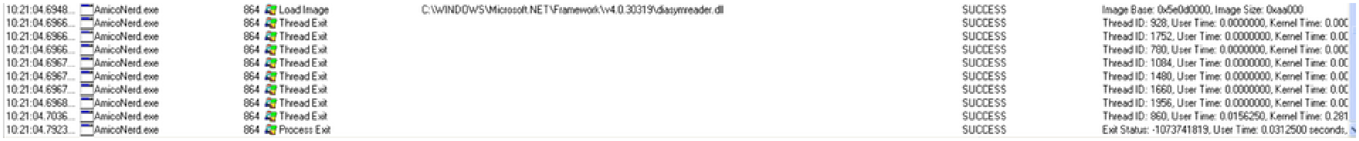
- **ProcessMonitor**



```
10:21:04.6922...  AmicoNerd.exe  864  RegOpenKey     HKLM\System\CurrentControlSet\Control\ComputerName                                                      SUCCESS         Desired Access: Read
10:21:04.6922...  AmicoNerd.exe  864  RegOpenKey     HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName                                   SUCCESS         Desired Access: Read
10:21:04.6922...  AmicoNerd.exe  864  RegQueryValue  HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName                      SUCCESS         Type: REG_SZ, Length: 26, Data: MALWARE_TEST
10:21:04.6922...  AmicoNerd.exe  864  RegCloseKey    HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName                                   SUCCESS
10:21:04.6922...  AmicoNerd.exe  864  RegCloseKey    HKLM\System\CurrentControlSet\Control\ComputerName                                                      SUCCESS
10:21:04.6927...  AmicoNerd.exe  864  RegQueryKey    HKCU\Software\Classes                                                                                   SUCCESS         Query: Name
10:21:04.6927...  AmicoNerd.exe  864  RegOpenKey     HKCU\Software\Classes\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InprocServer32                       NAME NOT FOUND  Desired Access: Read
10:21:04.6927...  AmicoNerd.exe  864  RegOpenKey     HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InprocServer32                                        SUCCESS         Desired Access: Read
10:21:04.6927...  AmicoNerd.exe  864  RegQueryKey    HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InprocServer32                                        SUCCESS         Query: Name
10:21:04.6928...  AmicoNerd.exe  864  RegOpenKey     HKCU\Software\Classes\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InprocServer32                       NAME NOT FOUND  Desired Access: Maximum Allowed
10:21:04.6928...  AmicoNerd.exe  864  RegQueryValue  HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InprocServer32\(Default)                              SUCCESS         Type: REG_SZ, Length: 24, Data: mscoree.dll
10:21:04.6928...  AmicoNerd.exe  864  RegQueryKey    HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InprocServer32                                        SUCCESS         Query: Name
10:21:04.6928...  AmicoNerd.exe  864  RegOpenKey     HKCU\Software\Classes\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InprocServer32                       NAME NOT FOUND  Desired Access: Maximum Allowed
10:21:04.6928...  AmicoNerd.exe  864  RegQueryValue  HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InprocServer32\(Default)                              SUCCESS         Type: REG_SZ, Length: 24, Data: mscoree.dll
10:21:04.6932...  AmicoNerd.exe  864  RegCloseKey    HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InprocServer32                                        SUCCESS
10:21:04.6932...  AmicoNerd.exe  864  RegQueryKey    HKCU\Software\Classes                                                                                   SUCCESS         Query: Name
10:21:04.6933...  AmicoNerd.exe  864  RegOpenKey     HKCU\Software\Classes\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\Server                               NAME NOT FOUND  Desired Access: Read
10:21:04.6933...  AmicoNerd.exe  864  RegOpenKey     HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\Server                                                SUCCESS         Desired Access: Read
10:21:04.6933...  AmicoNerd.exe  864  RegQueryKey    HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\Server                                                SUCCESS         Query: Name
10:21:04.6933...  AmicoNerd.exe  864  RegOpenKey     HKCU\Software\Classes\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\Server                               NAME NOT FOUND  Desired Access: Maximum Allowed
10:21:04.6933...  AmicoNerd.exe  864  RegQueryValue  HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\Server\(Default)                                      SUCCESS         Type: REG_SZ, Length: 34, Data: diasymreader.dll
10:21:04.6933...  AmicoNerd.exe  864  RegQueryKey    HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\Server                                                SUCCESS         Query: Name
10:21:04.6933...  AmicoNerd.exe  864  RegOpenKey     HKCU\Software\Classes\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\Server                               NAME NOT FOUND  Desired Access: Maximum Allowed
10:21:04.6934...  AmicoNerd.exe  864  RegQueryValue  HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\Server\(Default)                                      SUCCESS         Type: REG_SZ, Length: 34, Data: diasymreader.dll
10:21:04.6934...  AmicoNerd.exe  864  RegCloseKey    HKCR\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\Server                                                SUCCESS
10:21:04.6949...  AmicoNerd.exe  864  RegOpenKey     HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\diasymreader.dll         NAME NOT FOUND  Desired Access: Read
10:21:04.6986...  AmicoNerd.exe  864  RegCloseKey    HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings                                        SUCCESS
10:21:04.6989...  AmicoNerd.exe  864  RegCloseKey    HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32                                             SUCCESS
10:21:04.7014...  AmicoNerd.exe  864  RegCloseKey    HKLM\System\CurrentControlSet\Services\NetBT\Parameters                                                 SUCCESS
10:21:04.7014...  AmicoNerd.exe  864  RegCloseKey    HKLM\System\CurrentControlSet\Services\NetBT\Parameters\Interfaces                                      SUCCESS
10:21:04.7016...  AmicoNerd.exe  864  RegCloseKey    HKLM\System\CurrentControlSet\Services\Tcpip\Parameters                                                 SUCCESS
10:21:04.7017...  AmicoNerd.exe  864  RegCloseKey    HKLM\System\CurrentControlSet\Services\Tcpip\Linkage                                                    SUCCESS
10:21:04.7023...  AmicoNerd.exe  864  RegCloseKey    HKLM\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v4.0.30319_32                                          SUCCESS
10:21:04.7029...  AmicoNerd.exe  864  RegCloseKey    HKLM\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default                                                  SUCCESS
10:21:04.7031...  AmicoNerd.exe  864  RegOpenKey     HKLM\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize                                        SUCCESS         Desired Access: Read
10:21:04.7031...  AmicoNerd.exe  864  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles                       NAME NOT FOUND  Length: 20
10:21:04.7034...  AmicoNerd.exe  864  RegCloseKey    HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize                                        SUCCESS
```

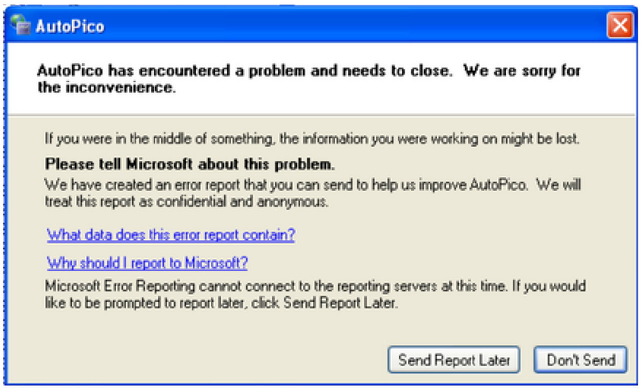


```
2:39:31.11361...  AmicoNerd.exe  544  QueryOpen                     C:\WINDOWS\system32\wbem\Logs                                              SUCCESS         CreationTime: 3/20/2017 9:34:22 PM, LastAccessTime: 12/1
2:39:31.29105...  AmicoNerd.exe  544  QueryOpen                     C:\Documents and Settings\Administrator\Desktop\amiconerd\logs             NAME NOT FOUND
2:39:31.29157...  AmicoNerd.exe  544  QueryOpen                     C:\Documents and Settings\Administrator\Desktop\amiconerd\logs             NAME NOT FOUND
2:39:31.29175...  AmicoNerd.exe  544  CreateFile                    C:\Documents and Settings\Administrator\Desktop\amiconerd\logs             SUCCESS         Desired Access: Read Data/List Directory, Synchronize, Disp
2:39:31.29212...  AmicoNerd.exe  544  CloseFile                     C:\Documents and Settings\Administrator\Desktop\amiconerd\logs             SUCCESS
2:39:31.29227...  AmicoNerd.exe  544  QueryOpen                     C:\Documents and Settings\Administrator\Desktop\amiconerd\logs\AmicoNerd.log  NAME NOT FOUND
2:39:31.30255...  AmicoNerd.exe  544  CreateFile                    C:\Documents and Settings\Administrator\Desktop\amiconerd\logs\AmicoNerd.log  SUCCESS      Desired Access: Generic Write, Read Attributes, Disposition: O
2:39:31.30355...  AmicoNerd.exe  544  QueryStandardInformationFile  C:\Documents and Settings\Administrator\Desktop\amiconerd\logs\AmicoNerd.log  SUCCESS      AllocationSize: 0, EndOfFile: 0, NumberOfLinks: 1, DeletePend
2:39:31.30487...  AmicoNerd.exe  544  WriteFile                     C:\Documents and Settings\Administrator\Desktop\amiconerd\logs\AmicoNerd.log  SUCCESS      Offset: 0, Length: 46
2:39:31.30514...  AmicoNerd.exe  544  CloseFile                     C:\Documents and Settings\Administrator\Desktop\amiconerd\logs\AmicoNerd.log  SUCCESS
2:39:31.68916...  AmicoNerd.exe  544  QueryOpen                     C:\WINDOWS\system32\wbem\Logs                                              SUCCESS         CreationTime: 3/20/2017 9:34:22 PM, LastAccessTime: 12/1
2:39:31.72941...  AmicoNerd.exe  544  CreateFile                    C:\Documents and Settings\Administrator\Desktop\amiconerd\logs\AmicoNerd.log  SUCCESS      Desired Access: Generic Write, Read Attributes, Disposition: O
2:39:31.72956...  AmicoNerd.exe  544  QueryStandardInformationFile  C:\Documents and Settings\Administrator\Desktop\amiconerd\logs\AmicoNerd.log  SUCCESS      AllocationSize: 48, EndOfFile: 46, NumberOfLinks: 1, DeleteP
2:39:31.73154...  AmicoNerd.exe  544  WriteFile                     C:\Documents and Settings\Administrator\Desktop\amiconerd\logs\AmicoNerd.log  SUCCESS      Offset: 46, Length: 256
2:39:31.73168...  AmicoNerd.exe  544  CloseFile                     C:\Documents and Settings\Administrator\Desktop\amiconerd\logs\AmicoNerd.log  SUCCESS
```



```
10:21:04.6948...  AmicoNerd.exe  864  Load Image    C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\diasymreader.dll   SUCCESS   Image Base: 0x5e0d0000, Image Size: 0xaa000
10:21:04.6966...  AmicoNerd.exe  864  Thread Exit                                                                    SUCCESS   Thread ID: 928, User Time: 0.0000000, Kernel Time: 0.00
10:21:04.6966...  AmicoNerd.exe  864  Thread Exit                                                                    SUCCESS   Thread ID: 1752, User Time: 0.0000000, Kernel Time: 0.0
10:21:04.6966...  AmicoNerd.exe  864  Thread Exit                                                                    SUCCESS   Thread ID: 780, User Time: 0.0000000, Kernel Time: 0.00
10:21:04.6967...  AmicoNerd.exe  864  Thread Exit                                                                    SUCCESS   Thread ID: 1084, User Time: 0.0000000, Kernel Time: 0.0
10:21:04.6967...  AmicoNerd.exe  864  Thread Exit                                                                    SUCCESS   Thread ID: 1480, User Time: 0.0000000, Kernel Time: 0.0
10:21:04.6967...  AmicoNerd.exe  864  Thread Exit                                                                    SUCCESS   Thread ID: 1660, User Time: 0.0000000, Kernel Time: 0.0
10:21:04.6968...  AmicoNerd.exe  864  Thread Exit                                                                    SUCCESS   Thread ID: 1956, User Time: 0.0000000, Kernel Time: 0.0
10:21:04.7036...  AmicoNerd.exe  864  Thread Exit                                                                    SUCCESS   Thread ID: 860, User Time: 0.0156250, Kernel Time: 0.281
10:21:04.7923...  AmicoNerd.exe  864  Process Exit                                                                   SUCCESS   Exit Status: -1073741819, User Time: 0.0312500 seconds,
```

- **WindowsXP**



AutoPico

AutoPico has encountered a problem and needs to close. We are sorry for the inconvenience.

If you were in the middle of something, the information you were working on might be lost.

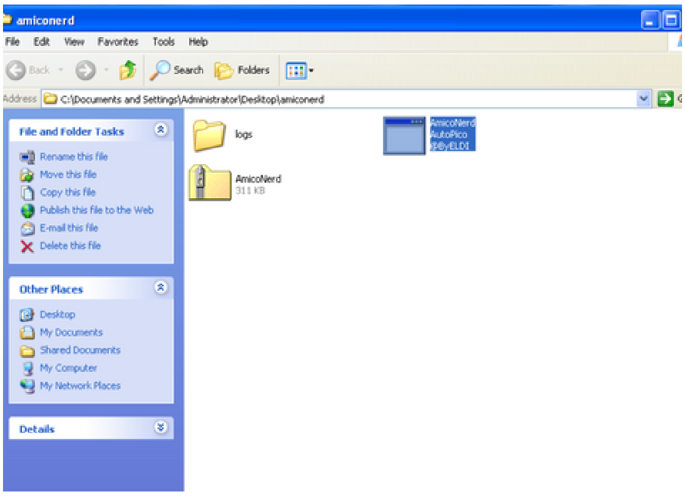
Please tell Microsoft about this problem.

We have created an error report that you can send to help us improve AutoPico. We will treat this report as confidential and anonymous.

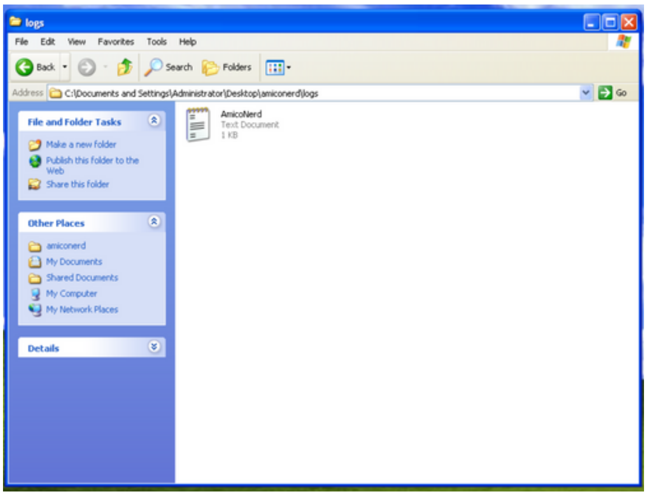
What data does this error report contain?

Why should I report to Microsoft?

Microsoft Error Reporting cannot connect to the reporting servers at this time. If you would like to be prompted to report later, click Send Report Later.



Address: C:\Documents and Settings\Administrator\Desktop\amiconerd



Address: C:\Documents and Settings\Administrator\Desktop\amiconerd\logs

Thank you!