

FileName: antirap.exe**FileSize: 195.584 bytes****MD5: 59ea3dac43856ce6f3946f3eb871ab8a****Malware Type: Trojan****Download From:**

hxxp://yrots.ru/56/antirap.exe (IP: 91.206.201.224)

PE DETAILS:**PE SECTIONS:**

Name	V. Offset	V. Size	R. Offset	R. Size	Flags
.text	00001000	0002D798	00000400	0002D800	60000020
.rdata	0002F000	00000670	0002DC00	00000800	40000040
.data	00030000	0000100F	0002E400	00001200	C0000040
.rsrc	00032000	000005E0	0002F600	00000600	40000040

Basic Information	
EntryPoint:	0002E1CD
ImageBase:	00400000
SizeOfImage:	00033000
BaseOfCode:	00001000
BaseOfData:	0002F000
SectionAlignment:	00001000
FileAlignment:	00000200
Magic:	010B
Subsystem:	0002
NumberOfSections:	0004
TimeDateStamp:	4B866A98
SizeOfHeaders:	00000400
Characteristics:	0103
Checksum:	00038D07
SizeOfOptionalHeader:	00E0
NumOfRvaAndSizes:	00000010

Directory Information		
	RVA	SIZE
ExportTable:	00000000	00000000
ImportTable:	0002F0E8	000000A0
Resource:	00032000	000005E0
TLSTable:	00000000	00000000
Debug:	00000000	00000000

IMPORTS TABLE

DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
advapi32.dll	0002F188	00000000	00000000	0002F336	0002F000
kernel32.dll	0002F1E0	00000000	00000000	0002F47C	0002F058
comdlg32.dll	0002F1C0	00000000	00000000	0002F4AA	0002F038
gdi32.dll	0002F1CC	00000000	00000000	0002F4F4	0002F044
shell32.dll	0002F22C	00000000	00000000	0002F518	0002F0A4
user32.dll	0002F234	00000000	00000000	0002F616	0002F0AC
comctl32.dll	0002F1B0	00000000	00000000	0002F662	0002F028

advapi32.dll

BackupEventLogA ConvertSidToStringSidA CryptSignHashW GetCurrentHwProfileW
GetSidIdentifierAuthority LsaQueryInfoTrustedDomain RegOpenKeyExA

kernel32.dll

SetCalendarInfoW SetEnvironmentVariableA SetVolumeLabelW SetWaitableTimer TerminateProcess VirtualAlloc
GetBinaryTypeW MoveFileA LocalFlags GetVersion GetTickCount
GetSystemDirectoryW
GetLastError GetDriveTypeA AddAtomW DeleteTimerQueue ExitProcess GetCommandLineA

comdlg32.dll

GetOpenFileNameW FindTextA

gdi32.dll

EndPath EndFormPage EnumEnhMetaFile GetEnhMetaFileW

shell32.dll

SHPATHPrepareForWriteA

user32.dll

DlgDirListW EnumPropsW GetClassInfoExW GetClipCursor InsertMenuW DefDlgProcW
PaintDesktop SetWindowLongW UnhookWinEvent UnregisterDeviceNotification CharLowerW
KillTimer CloseDesktop ChildWindowFromPointEx

comctl32.dll

InitCommonControls DrawInsert CreatePropertySheetPageA

COME AGISCE antirap.exe

Il file antirap.exe quando eseguito si comporta nel seguente modo:

- Agisce in background
- Crea un file con le seguenti caratteristiche:
 - o FileName: a.exe
 - o FileSize: 69634 Bytes
 - o MD5: c0f09768cd736c4e81d5e04fd6908f59
 - o FilePath: C:\Windows\TEMP
- Carica in memoria il file a.exe e lo elimina dal disco fisso
- Il processo antirap.exe non fa altro di rilevante

Il vero cuore del malware è il processo a.exe

COME AGISCE il processo a.exe

- Visualizza alcune chiavi di registro per ottenere informazioni
- Genera un file exe (suo gemello) con un nome "random" di 8 caratteri (es: hvpytjvj.exe)
- Le caratteristiche del file generato sono:
 - o FilePath: C:\Windows\system32
 - o FileSize: 35.328 bytes
 - o L'eseguibile è compresso con il packer UPX
- Crea/Modifica il valore della chiave del registro di sistema
 - o HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - o Nome Valore: autoruns
 - o Valore Stringa: "c:\Windows\system32\xxxxxxx.exe" (es: "c:\Windows\system32\hvpytjvj.exe")
- Contatta una lista di host/IP con cui stabilire la connessione (utilizza il server dns primario del PC senza modificarlo)
- Quando trova un host che gli risponde instaura la connessione (durante la mia analisi l'host a cui si era collegato era 77.221.140.99).
- Non fa nient'altro di rilevante

ALTRO

Al riavvio della macchina, il file generato precedentemente dal processo a.exe entrerà in azione e svolgerà azioni simili al processo a.exe (che non è più presente in memoria RAM e nemmeno su disco)

Il malware per sopravvivere effettua grazie a un timer una ripetuta creazione e distruzione del suo eseguibile (genera le nuove copie del trojan con nomi di 8 caratteri random) e aggiorna il valore autoruns presente nella chiave di registro (HKLM\SOFTWARE\Microsoft\...\Run) con il percorso dell'ultima nuova copia del malware, così che al prossimo riavvio il trojan partirà con l'eseguibile generato per ultimo.

NOTE

Autore: Matteo Neri (Mn90)

E-Mail: mn90@msn.com

Sito Web: <http://mn90.it>