ID: 383661
Sample Name:
606e7fb752fbd.rar.dll
Cookbook: default.jbs
Time: 06:02:11
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

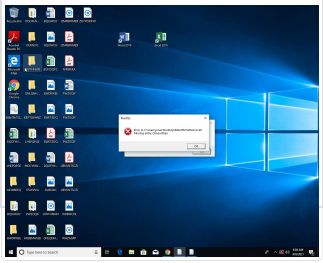
Analysis Report 606e7fb752fbd.rar.dll

Overview

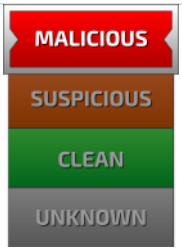
General Information

Sample Name:	606e7fb752fbd.rar.dll
Analysis ID:	383661
MD5:	8bf44d2b3b9b7c0.
SHA1:	76d4ed4512d34e..
SHA256:	cb7c95db9ce05d..
Tags:	BRT dll geo gozi isfb ITA ursnif
Infos:	

Most interesting Screenshot:



Detection



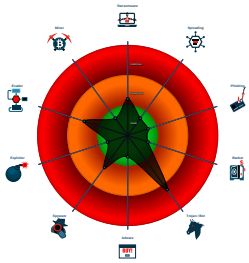
Ursnif

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Ursnif
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Creates a process in suspended mo…
- Detected potential crypto function
- Found potential string decryption / a…
- PE file contains an invalid checksum

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6444 cmdline: loaddll32.exe 'C:\Users\user\Desktop\606e7fb752fbd.rar.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6456 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\606e7fb752fbd.rar.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6476 cmdline: rundll32.exe 'C:\Users\user\Desktop\606e7fb752fbd.rar.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6464 cmdline: rundll32.exe C:\Users\user\Desktop\606e7fb752fbd.rar.dll,Choosethan MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6516 cmdline: rundll32.exe C:\Users\user\Desktop\606e7fb752fbd.rar.dll,Especiallyyes MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6532 cmdline: rundll32.exe C:\Users\user\Desktop\606e7fb752fbd.rar.dll,Guesscover MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6552 cmdline: rundll32.exe C:\Users\user\Desktop\606e7fb752fbd.rar.dll,Learncut MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6596 cmdline: rundll32.exe C:\Users\user\Desktop\606e7fb752fbd.rar.dll,OnceOut MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
[
  {
    "RSA Public Key":
"YKwVOU5rJLi0k2wc/Sa//orn/I3K6zI6HgJKpraE6XyxxZAjZUdVyZ9IFso22JAAB2G4qzzp3TU2DJqhIyPO7xVeI9l7K9H9VlKfzYozAbxBQCrtZPEdPyCguw2FwPnt3aL3viJmXn26e8PXSevTHzQdNxMCe42eyfgYxlDVzbkJTLhI
91j/G+/dxO1/TdYY"
  },
  {
    "c2_domain": [
      "ocsp2.digicert.com",
      "aus6.mozilla.org",
      "durenoluneer.xyz",
      "surenoluneer.xyz"
    ],
    "botnet": "8877",
    "server": "12",
    "serpent_key": "30218409ILPAJDUR",
    "sleep_time": "10",
    "SetWaitableTimer_value": "0",
    "DGA_count": "10"
  }
]
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.874026586.0000000000EC0000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000002.00000003.873095643.0000000000F10000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000004.00000003.890597997.0000000000C50000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

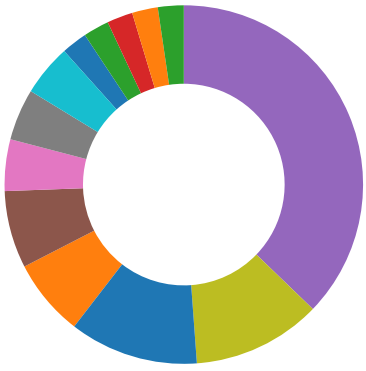
Unpacked PEs

Source	Rule	Description	Author	Strings
4.3.rundll32.exe.c5a4b1.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.6d450000.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.2.rundll32.exe.6d450000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.f1a4b1.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.eca4b1.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

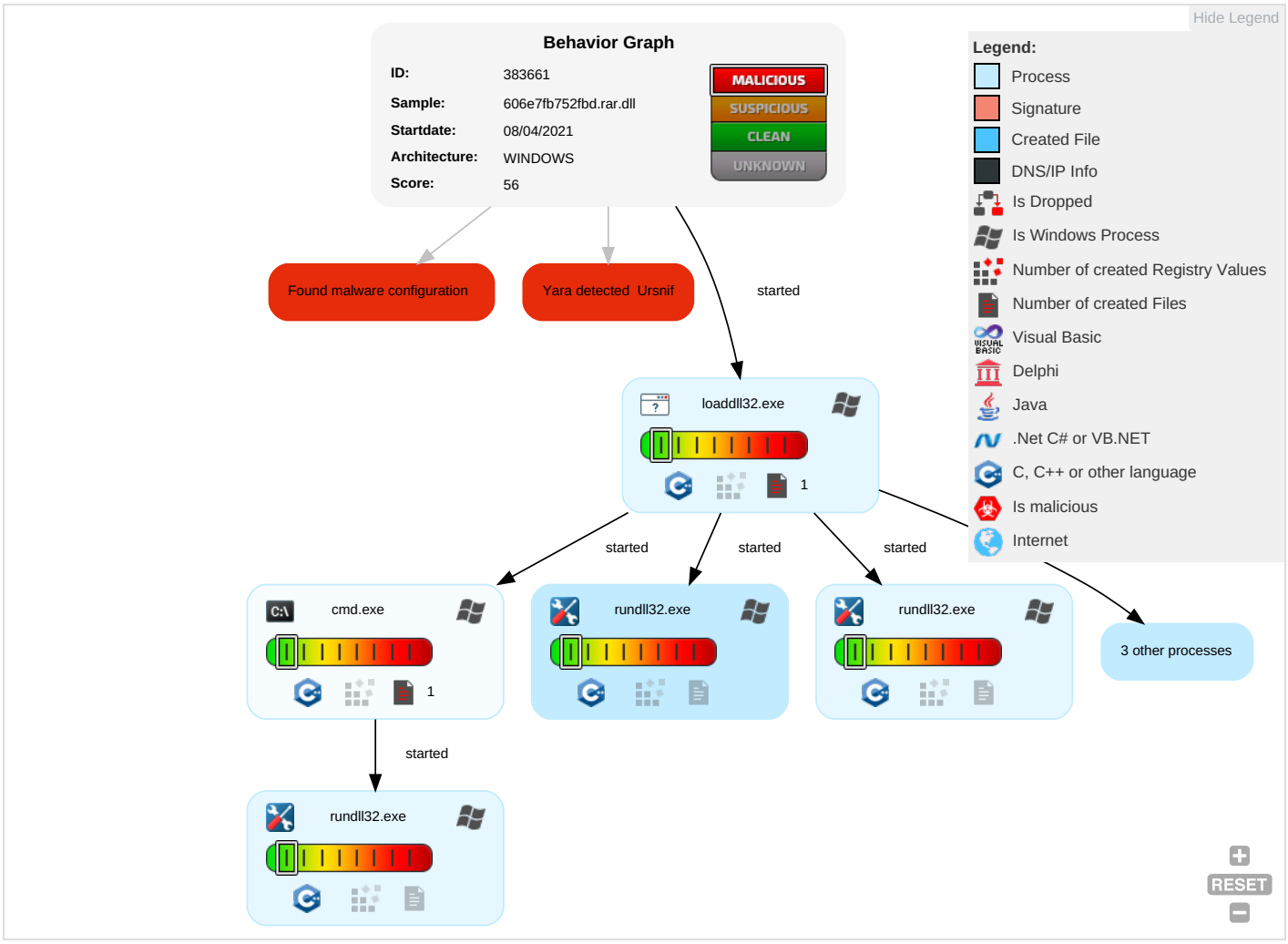
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 1 2	Rundll32 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Devic Without Authorizatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizatic
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Information Discovery 2 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

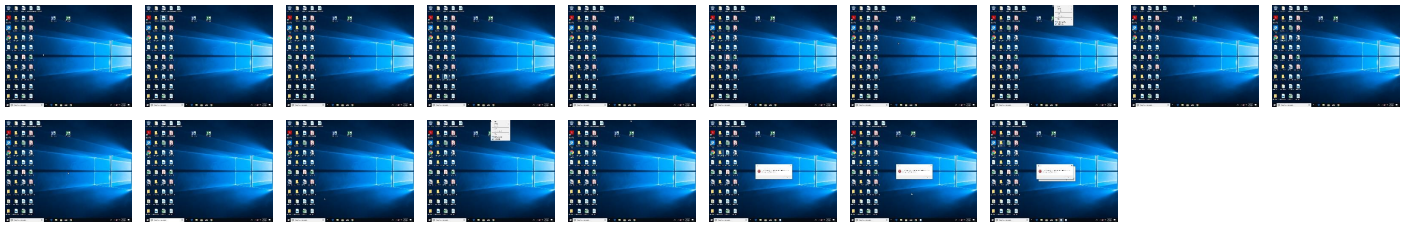
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
606e7fb752fbd.rar.dll	6%	ReversingLabs	Win32.Trojan.Ursnif	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.d10000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383661
Start date:	08.04.2021
Start time:	06:02:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	606e7fb752fbd.rar.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.troj.winDLL@15/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9% (good quality ratio 8.5%) • Quality average: 71.3% • Quality standard deviation: 26.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, RuntimeBroker.exe, backgroundTaskHost.exe, UsoClient.exe • Report creation exceeded maximum time and may have missing disassembly code information.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.562725713508687
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.40% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Disk Image (Macintosh), GPT (2000/0) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	606e7fb752fbd.rar.dll
File size:	1007104
MD5:	8bf44d2b3b9b7c0fa2754fbe6ad14a63
SHA1:	76d4ed4512d34edd5a34b917957654fedbfae23f
SHA256:	cb7c95db9ce05d2304a4a98687a4b92f85081e1b7397820a52487b277ee1f2e1
SHA512:	58d7912fb2486ee944cda295f80293bed6f207631fd79611a64e350f60bc6ff662fc9f66a1e57fefbe9998d081b6f92807ed7ca85dafaa7a313ff7047decede8
SSDEEP:	24576:lLtF9jICeGoQ8T1Mk7Hv/3+MM9hbAK0uf:/FpPeGovT1t33+p9hbAK0uf
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$......"6..fW..fW..fW....l.kW....n..W....o.{W..4?..pW..4?..PW..4?..yW..o/..oW..fW...W...>..gW...>..gW...>b.gW...>..gW..RichfW.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1040e44
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5AC0F310 [Sun Apr 1 14:56:16 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	935187af3562f5148cd8683f99f748de

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007FB32D027867h
call 00007FB32D02824Bh
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007FB32D02770Fh
add esp, 0Ch
pop ebp
retn 000Ch
mov ecx, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], ecx
pop ecx
pop edi
pop edi
pop esi
pop ebx
mov esp, ebp
pop ebp
push ecx
ret
mov ecx, dword ptr [ebp-10h]
xor ecx, ebp
call 00007FB32D026DC2h
jmp 00007FB32D027840h
mov ecx, dword ptr [ebp-14h]
xor ecx, ebp
call 00007FB32D026DB1h
jmp 00007FB32D02782Fh
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax

Instruction
mov eax, dword ptr [010E4074h]
xor eax, ebp
push eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [010E4074h]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
inc dword ptr fs:[eax]

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xe2c40	0x9c	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe2cdc	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10b000	0x528	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x10c000	0x703c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd8cf0	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xd8de8	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xd8d48	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xb0000	0x1e8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xaef21	0xaf000	False	0.524893973214	data	6.69988661327	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xb0000	0x33798	0x33800	False	0.528073801578	data	5.1051416342	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xe4000	0x26b60	0xba00	False	0.562668010753	data	4.83370710676	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x10b000	0x528	0x600	False	0.412109375	data	3.76195156474	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x10c000	0x703c	0x7200	False	0.694421600877	data	6.654304142	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x10b0a0	0x304	data	English	United States
RT_MANIFEST	0x10b3a8	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	GetShortPathNameA, WaitForMultipleObjects, GetEnvironmentVariableA, Sleep, GetTempPathA, CopyFileA, GetFileAttributesA, GetSystemDirectoryA, GetWindowsDirectoryA, VirtualProtectEx, CreateProcessA, CreateSemaphoreA, OutputDebugStringW, OutputDebugStringA, SetEndOfFile, HeapSize, WriteConsoleW, SetStdHandle, CreateFileW, GetProcessHeap, SetEnvironmentVariableW, SetEnvironmentVariableA, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, GetCommandLineA, GetOEMCP, IsValidCodePage, MultiByteToWideChar, GetLastError, FormatMessageW, WideCharToMultiByte, GetStringTypeW, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetLastError, InitializeCriticalSectionAndSpinCount, CreateEventW, SwitchToThread, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetSystemTimeAsFileTime, GetTickCount, GetModuleHandleW, GetProcAddress, EncodePointer, DecodePointer, GetCPInfo, CompareStringW, LCMapStringW, GetLocaleInfoW, CloseHandle, SetEvent, ResetEvent, WaitForSingleObjectEx, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, IsDebuggerPresent, GetStartupInfoW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, InitializeSListHead, RtlUnwind, RaiseException, InterlockedPushEntrySList, InterlockedFlushSList, FreeLibrary, LoadLibraryExW, ExitProcess, GetModuleHandleExW, GetModuleFileNameA, GetModuleFileNameW, GetCurrentThread, GetACP, HeapAlloc, GetStdHandle, GetFileType, HeapFree, HeapReAlloc, ReadFile, SetFilePointerEx, WriteFile, GetConsoleCP, GetConsoleMode, GetDateFormatW, GetTimeFormatW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, FlushFileBuffers, ReadConsoleW, SetConsoleCtrlHandler, GetTimeZoneInformation, FindClose, FindFirstFileExA, FindFirstFileExW, FindNextFileA, FindNextFileW, CreateThread
ole32.dll	CoTaskMemAlloc, CoInitialize, CoUninitialize, CoTaskMemFree
WS2_32.dll	getprotobynumber, WSAStartup, getservbyport, WSACleanup, setsockopt, socket
RASAPI32.dll	RasEnumConnectionsA, RasGetConnectStatusA

Exports

Name	Ordinal	Address
Choosethan	1	0x1086ad0
Especiallyyes	2	0x10865e0
Guesscover	3	0x1086ff0
Learncut	4	0x1088240
OnceOut	5	0x1087600

Version Infos

Description	Data
LegalCopyright	Copyright 1998-2014 Had Home, Inc
InternalName	Serve color
FileVersion	6.7.0.400
CompanyName	Had Home
ProductName	Had Home
Think beat	FreeHere
FileDescription	Serve color
OriginalFilename	Brought.dll
ProductVersion	6.7.0.400
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6444 Parent PID: 6060

General

Start time:	06:02:53
Start date:	08/04/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\606e7fb752fbd.rar.dll'
Imagebase:	0x360000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6456 Parent PID: 6444

General

Start time:	06:02:53
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\606e7fb752fbd.rar.dll',#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6464 Parent PID: 6444

General

Start time:	06:02:54
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\606e7fb752fbd.rar.dll,Choosethan
Imagebase:	0xff0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.873095643.0000000000F10000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6476 Parent PID: 6456

General

Start time:	06:02:54
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\606e7fb752fbd.rar.dll',#1
Imagebase:	0xff0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.874026586.0000000000EC0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6516 Parent PID: 6444

General

Start time:	06:02:57
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\606e7fb752fbd.rar.dll,Especiallyyes
Imagebase:	0xff0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000003.890597997.0000000000C50000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6532 Parent PID: 6444

General

Start time:	06:03:01
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\606e7fb752fbd.rar.dll,Guesscover
Imagebase:	0xff0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6552 Parent PID: 6444

General

Start time:	06:03:05
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\606e7fb752fbd.rar.dll,Learncut
Imagebase:	0xff0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6596 Parent PID: 6444

General

Start time:	06:03:11
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\606e7fb752fbd.rar.dll,OnceOut
Imagebase:	0xff0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis