ID: 410818
Sample Name: 609a460e94791.tiff.dll
Cookbook: default.jbs
Time: 11:01:34
Date: 11/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

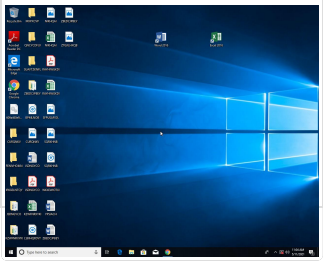
Analysis Report 609a460e94791.tiff.dll

Overview

General Information

Sample Name:	609a460e94791.tiff.dll
Analysis ID:	410818
MD5:	50a299d1e92d92..
SHA1:	c188272ab757db..
SHA256:	3b56b7298c366a..
Tags:	BRT dll geo gozi isfb ita ursnif
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

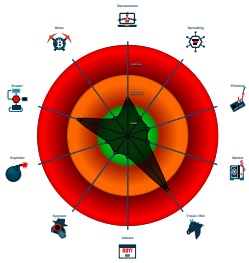
Ursnif

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Ursnif
- Writes registry values via WMI
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to read the PEB
- Creates a process in suspended mo…
- Detected potential crypto function
- Extensive use of GetProcAddress (o…
- PE file contains an invalid checksum

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 980 cmdline: loaddll32.exe 'C:\Users\user\Desktop\609a460e94791.tiff.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 4312 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\609a460e94791.tiff.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1752 cmdline: rundll32.exe 'C:\Users\user\Desktop\609a460e94791.tiff.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5824 cmdline: rundll32.exe C:\Users\user\Desktop\609a460e94791.tiff.dll,Hundredpopulate@@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4404 cmdline: rundll32.exe C:\Users\user\Desktop\609a460e94791.tiff.dll,Mark@@12 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1700 cmdline: rundll32.exe C:\Users\user\Desktop\609a460e94791.tiff.dll,Seefit@@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5444 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"KujE77ctKyR8x3/dODwZbEsxGmck+FW9384s5u0Kacw8y1gCN+8m2bfjJPovkn+Uzufcdfss+a43eI6oHR1KgWQmvEAO6LK8tJv+Wl7iCBPJP7eef8xKeXht/Mhk1PSj7mHnJ9lcqKMtTteEdSecVvMRtb/WSKVTFfHDva9My7AJ/NbXqHdzCG7znACswLxD",
  "c2_domain": [
    "outlook.com/login",
    "gmail.com",
    "worunekulo.club",
    "horunekulo.website"
  ],
  "botnet": "8877",
  "server": "12",
  "serpent_key": "30218409ILPAJDUR",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```


Yara Overview

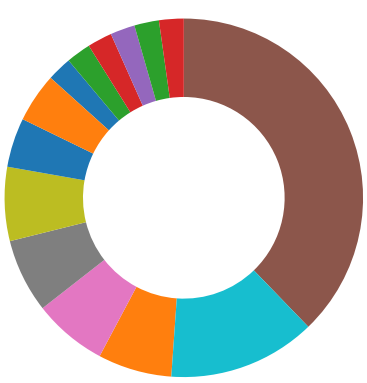
Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.590568897.0000000005168000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Process Memory Space: rundll32.exe PID: 1752	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Spreading
- 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

System Summary:

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

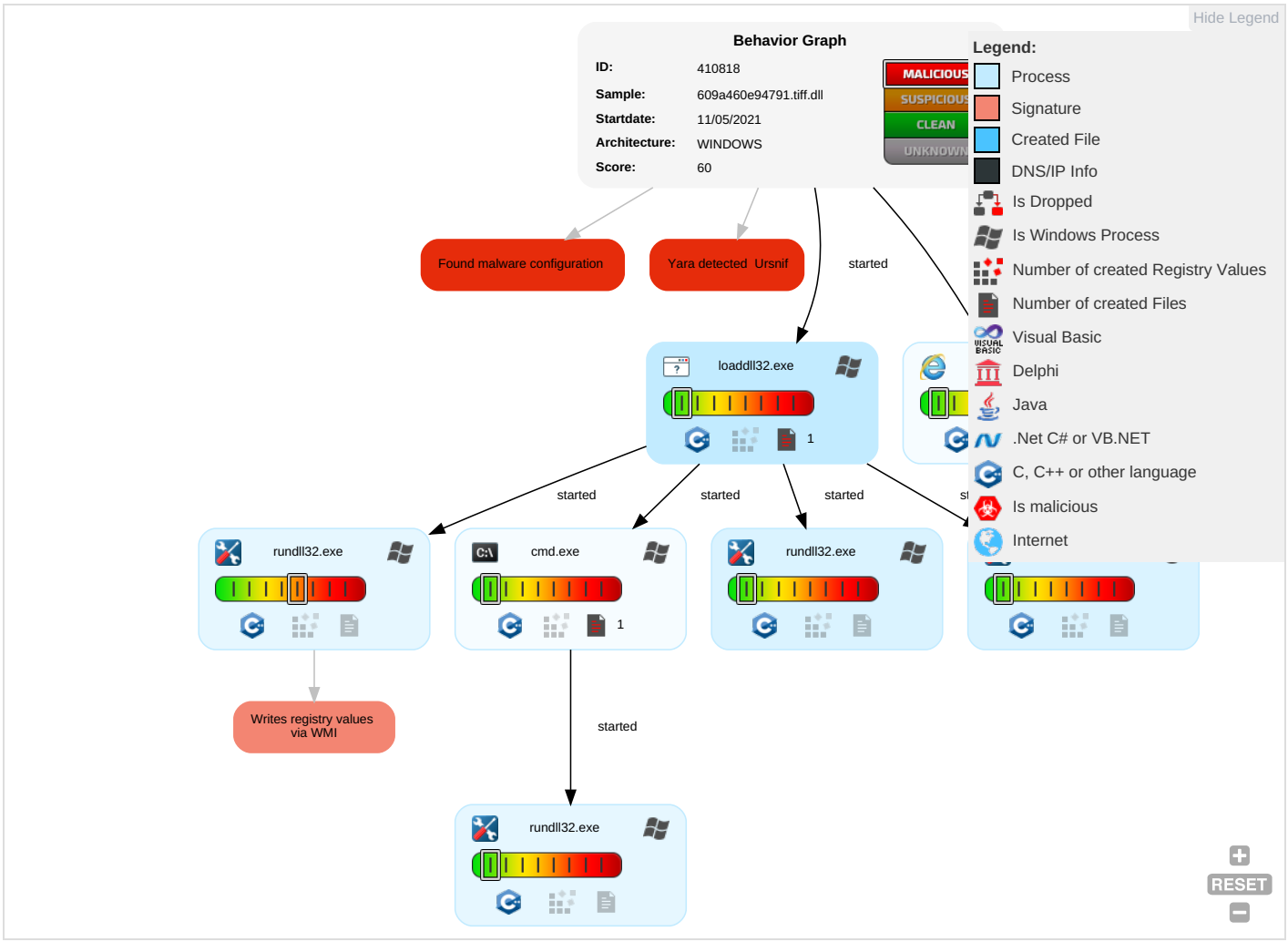
Remote Access Functionality:

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	Windows Management Instrumentation 1	Application Shimming 1	Process Injection 1 2	Rundll32 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Application Shimming 1	Process Injection 1 2	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated 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)	Binary Padding	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

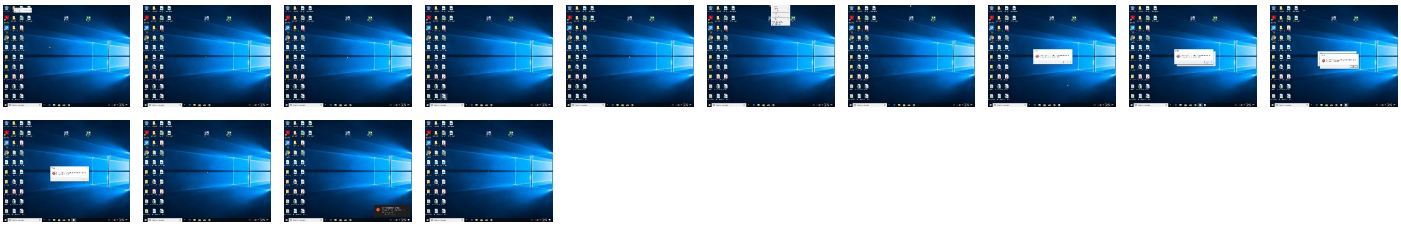
Behavior Graph



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
609a460e94791.tiff.dll	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.2c50000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.rundll32.exe.31e0000.1.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:	32.0.0 Black Diamond
Analysis ID:	410818
Start date:	11.05.2021
Start time:	11:01:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	609a460e94791.tiff.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:	14
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:	mal60.troj.winDLL@12/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.9% (good quality ratio 3.7%) • Quality average: 79.1% • Quality standard deviation: 29.5%
HCA Information:	• Successful, ratio: 54% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll

Simulations

Behavior and APIs

Time	Type	Description
11:04:06	API Interceptor	1x Sleep call for process: rundll32.exe modified

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):	6.388590209681191
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.40% • Win16/32 Executable Delphi generic (2074/23) 0.21% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	609a460e94791.tiff.dll
File size:	841216
MD5:	50a299d1e92d9205e123404c8e05904d
SHA1:	c188272ab757dbbf14e74781fc90fcefe4aeb615
SHA256:	3b56b7298c366a323d28658a455abf0d4e78fa197a43ce13bedab05f26901d34
SHA512:	ec30f36d70ddbb6ba4aaccb3342e0a0ffbd586d2784370500a94e33aa650d1c56d3712ffc3a9e15a0558194ce26d1b76d9f2a8953220684bef634e57f4579df1
SSDEEP:	12288:mzCoYRvNZrA8Res/TPUOjUUGcqcoWEx9kMGUS6vOV5y4gnuD5wtqqB7ol:VdNZr5RLL1AZ/clUnHvk5hgU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...L..`.....!.....0.....@.....{..x..

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1033080
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:	0x6092C34C [Wed May 5 16:09:48 2021 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:	dc55991f7b8a912c780d10d352635290

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007FA9008E6837h
call 00007FA9008E7507h
mov eax, dword ptr [ebp+10h]
push eax
mov ecx, dword ptr [ebp+0Ch]
push ecx
mov edx, dword ptr [ebp+08h]
push edx
call 00007FA9008E6616h
add esp, 0Ch
pop ebp
retn 000Ch
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx
mov dword ptr [ebp-04h], ecx
mov esp, ebp
pop ebp
ret
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx
mov eax, dword ptr [ebp+08h]

Instruction
mov ecx, dword ptr [eax]
mov dword ptr [ebp-04h], ecx
mov eax, dword ptr [ebp-04h]
mov esp, ebp
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push eax
call 00007FA9008E6809h
add esp, 04h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push eax
call 00007FA9008E68A9h
add esp, 04h
test eax, eax
je 00007FA9008E6833h
int3
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp

Instruction
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push eax
call 00007FA9008E6889h
add esp, 04h
test eax, eax
je 00007FA9008E6839h
mov ecx, 00000041h
int 29h
pop ebp
ret
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx
mov eax, dword ptr [ebp+08h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xc7bb0	0x78	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc7c28	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe8000	0x3a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe9000	0x51e0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc5ecc	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xc5f20	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x9b000	0x1a4	.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	0x997af	0x99800	False	0.488934942488	data	6.50079371898	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x9b000	0x2d5aa	0x2d600	False	0.326892863292	data	4.74980452387	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc9000	0x1efdc	0xe00	False	0.209821428571	data	3.01039741419	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xe8000	0x3a0	0x400	False	0.404296875	data	3.03375733203	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe9000	0x51e0	0x5200	False	0.770293445122	data	6.74990882481	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe8060	0x340	data	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	CreateFileW, GetWindowsDirectoryW, ReadFile, GetConsoleMode, OpenMutexW, CloseHandle, GetFileSize, DeleteCriticalSection, ReadConsoleW, VirtualProtectEx, GetConsoleCP, FlushFileBuffers, SetFilePointerEx, GetFileSizeEx, SetStdHandle, GetStringTypeW, EnterCriticalSection, LeaveCriticalSection, SetLastError, InitializeCriticalSectionAndSpinCount, CreateEventW, SwitchToThread, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetSystemTimeAsFileTime, GetTickCount, GetModuleHandleW, GetProcAddress, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, GetCurrentProcess, TerminateProcess, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, InitializeSListHead, RaiseException, RtlUnwind, InterlockedPushEntrySList, InterlockedFlushSList, GetLastError, EncodePointer, FreeLibrary, LoadLibraryExW, GetModuleFileNameW, GetModuleHandleExW, ExitProcess, HeapAlloc, HeapValidate, GetSystemInfo, GetCurrentThread, GetStdHandle, GetFileType, WriteFile, OutputDebugStringW, WriteConsoleW, SetConsoleCtrlHandler, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, MultiByteToWideChar, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, GetProcessHeap, HeapFree, HeapReAlloc, HeapSize, HeapQueryInformation, DecodePointer
UxTheme.dll	CloseThemeData
AVIFIL32.dll	AVIFileGetStream, AVIFileOpenW, AVIFileExit, AVIFileInit, AVIFileEndRecord
TAPI32.dll	lineRedirectW, lineInitialize, lineHold, lineShutdown, lineTranslateAddressW

Exports

Name	Ordinal	Address
Hundredpopulate@@8	1	0x1030208
Mark@@12	2	0x10303fe
Seefit@@8	3	0x103046c

Version Infos

Description	Data
LegalCopyright	Dad plan Corporation. All rights reserved
InternalName	Team Lonesell
FileVersion	7.2.6.201
CompanyName	Dad plan Corporation
These	95
ProductName	Dad plan Fair fell
ProductVersion	7.2.6.201
FileDescription	Dad plan Fair fell
OriginalFilename	fall.dll
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

- loaddll32.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- iexplore.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 980 Parent PID: 5752

General

Start time:	11:02:22
Start date:	11/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\609a460e94791.tiff.dll'
Imagebase:	0x11b0000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
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: cmd.exe PID: 4312 Parent PID: 980

General

Start time:	11:02:22
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\609a460e94791.tiff.dll',#1
Imagebase:	0x2a0000
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: 5824 Parent PID: 980

General

Start time:	11:02:22
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\609a460e94791.tiff.dll,Hundredpopulate@@8
Imagebase:	0x50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1752 Parent PID: 4312

General

Start time:	11:02:22
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\609a460e94791.tiff.dll',#1
Imagebase:	0x50000
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, Description: Yara detected Ursnif, Source: 00000003.00000002.590568897.0000000005168000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4404 Parent PID: 980

General

Start time:	11:02:26
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\609a460e94791.tiff.dll,Mark@@12
Imagebase:	0x50000
File size:	61952 bytes

MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1700 Parent PID: 980

General

Start time:	11:02:29
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\609a460e94791.tiff.dll,Seefit@@8
Imagebase:	0x50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5444 Parent PID: 792

General

Start time:	11:04:30
Start date:	11/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis