ID: 404147
Sample Name:
8OKQ6ogGRx.dll
Cookbook: default.jbs
Time: 18:50:36
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

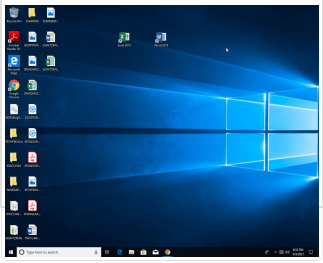
Analysis Report 8OKQ6ogGRx.dll

Overview

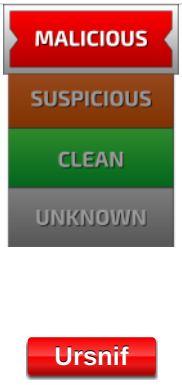
General Information

Sample Name:	8OKQ6ogGRx.dll
Analysis ID:	404147
MD5:	e8eae1a820426a..
SHA1:	4d8368f112e0c56.
SHA256:	eb498648d17ad5..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

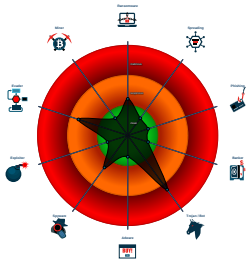


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Ursnif
- Writes or reads registry keys via WMI
- 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 query CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Contains functionality which may be…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 2168 cmdline: loaddll32.exe 'C:\Users\user\Desktop\8OKQ6ogGRx.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 3880 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\8OKQ6ogGRx.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6024 cmdline: rundll32.exe 'C:\Users\user\Desktop\8OKQ6ogGRx.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3468 cmdline: rundll32.exe C:\Users\user\Desktop\8OKQ6ogGRx.dll,Enterbeen MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3512 cmdline: rundll32.exe C:\Users\user\Desktop\8OKQ6ogGRx.dll,Multiply MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5212 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5240 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5212 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"KfAh1HjBYV5+GLf1H4+++WQcflLYE80sojTEX/uvXaLXhDxSfFOCIe7aHw1TYNxXIBvEkznlAveWMvLVTSjkgy/Hqpm47GUbXiPUxbpl0qoDhGQpz45mxRQlc+jgXQ4D03Y0gMF90NeOpBOEi497zfDlURi8Me7OHCSUNpn4Q0kQtrInhQlll9V6IFuYjZJB",
  "c2_domain": [
    "outlook.com/login",
    "gmail.com",
    "dorelunonu.us",
    "morelunonu.us"
  ],
  "botnet": "8877",
  "server": "12",
  "serpent_key": "30218409ILPAJDUR",
  "sleep_time": "10",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```


Yara Overview

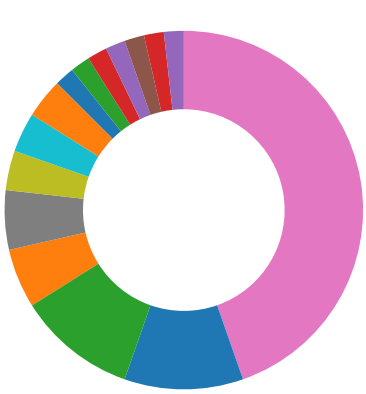
Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.470954657.0000000003618000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Process Memory Space: loaddll32.exe PID: 2168	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- 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

Click to jump to signature section

AV Detection:

Found malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

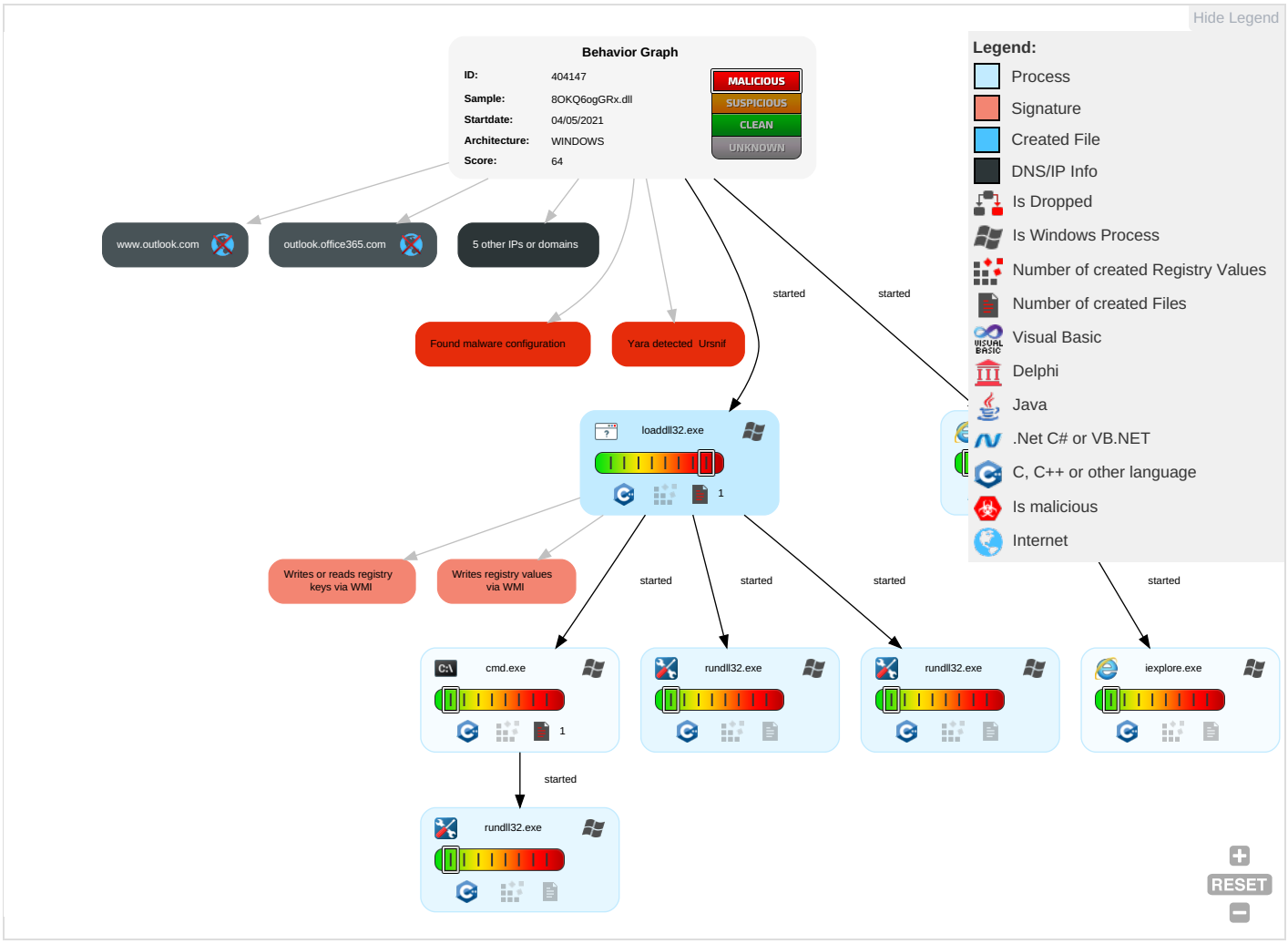
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 2	Masquerading 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
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Security Software Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 2 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

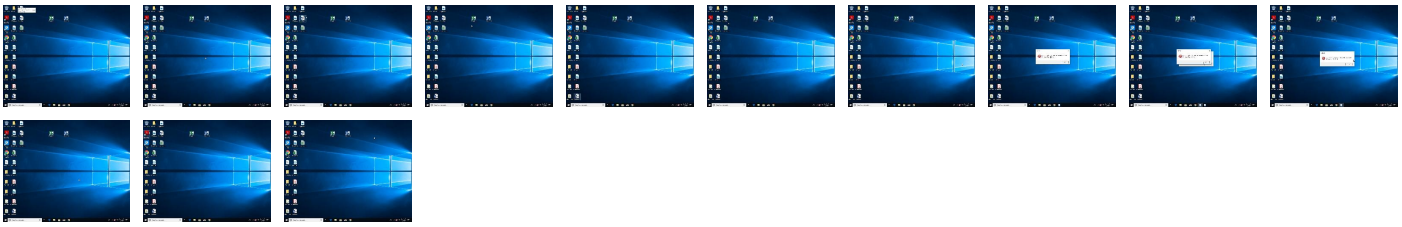
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.bb0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
outlook.com	40.97.161.50	true	false		high
HHN-efz.ms-acdc.office.com	40.101.138.2	true	false		high
FRA-efz.ms-acdc.office.com	40.101.81.162	true	false		high
www.outlook.com	unknown	unknown	false		high
outlook.office365.com	unknown	unknown	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404147
Start date:	04.05.2021
Start time:	18:50:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8OKQ6ogGRx.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:	24
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:	mal64.troj.winDLL@12/4@3/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12.7% (good quality ratio 12.1%) • Quality average: 79.5% • Quality standard deviation: 28.7%
HCA Information:	• Successful, ratio: 73% • 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

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 204.79.197.200, 13.107.21.200, 20.49.157.6, 104.43.193.48, 168.61.161.212, 92.122.145.220, 184.30.24.56, 2.20.142.209, 2.20.142.210, 20.82.209.183, 92.122.213.247, 92.122.213.194, 88.221.62.148, 2.17.179.193, 84.53.167.113, 20.82.210.154 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, arc.msn.com, cdn.onenote.net.edgekey.net, e11290.dspg.akamaiedge.net, e12564.dspb.akamaiedge.net, go.microsoft.com, wildcard.weather.microsoft.com.edgekey.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, cdn.onenote.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, tile-service.weather.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, e1553.dspg.akamaiedge.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/404147/sample/8OKQ6ogGRx.dll

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
outlook.com	n6osajjc938.exe	Get hash	malicious	Browse	• 104.47.54.36
	9b3d7f02.exe	Get hash	malicious	Browse	• 104.47.54.36
	5zc9vbGBo3.exe	Get hash	malicious	Browse	• 52.101.24.0
	InnAcjnAmG.exe	Get hash	malicious	Browse	• 104.47.53.36
	8X93Tzvd7V.exe	Get hash	malicious	Browse	• 52.101.24.0
	u8A8Qy5S7O.exe	Get hash	malicious	Browse	• 104.47.53.36

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Mal.GandCrypt-A.24654.exe	Get hash	malicious	Browse	• 104.47.54.36
	SecuriteInfo.com.Mal.GandCrypt-A.5674.exe	Get hash	malicious	Browse	• 104.47.54.36
	SecuriteInfo.com.W32.AIDetect.malware2.29567.exe	Get hash	malicious	Browse	• 104.47.53.36
	lsass(1).exe	Get hash	malicious	Browse	• 104.47.59.138
	rtofwqxq.exe	Get hash	malicious	Browse	• 104.47.53.36
	VufxYArno1.exe	Get hash	malicious	Browse	• 104.47.53.36
FRA-efz.ms-acdc.office.com	dechert-Investment078867-xlsx.Html	Get hash	malicious	Browse	• 52.97.189.66
	murexltd-Investment_265386-xlsx.html	Get hash	malicious	Browse	• 52.97.188.66
	z2xQEFs54b.exe	Get hash	malicious	Browse	• 52.97.250.226
	sgs-Investment974041-xlsx.Html	Get hash	malicious	Browse	• 40.101.19.162
	roccor-invoice-648133_xls.HtMl	Get hash	malicious	Browse	• 52.97.200.162
	redwirespace-invoice-982323_xls.HtMl	Get hash	malicious	Browse	• 40.101.12.82
	prismcosec-invoice-647718_xls.HtMl	Get hash	malicious	Browse	• 40.101.81.130
	E848.tmp.exe	Get hash	malicious	Browse	• 40.101.81.130
	Payment.html	Get hash	malicious	Browse	• 52.97.250.194
	Remittance advice.htm	Get hash	malicious	Browse	• 52.97.250.210
	0G2gue8shl.exe	Get hash	malicious	Browse	• 52.97.176.2
	February Payroll.xls.htm	Get hash	malicious	Browse	• 52.97.250.242
	PURCHASE ORDER#34556558.exe	Get hash	malicious	Browse	• 52.97.200.178
	Proforma Invoice.exe	Get hash	malicious	Browse	• 52.97.250.210
	E-DEKONT.exe	Get hash	malicious	Browse	• 52.97.144.178
	DHL Notification -AWB DHL-2021011293002.exe	Get hash	malicious	Browse	• 52.97.201.82
	DHL DOCS.exe	Get hash	malicious	Browse	• 40.101.80.2
	ORDER REQUEST.exe	Get hash	malicious	Browse	• 40.101.121.34
	INVOICE.exe	Get hash	malicious	Browse	• 52.97.188.66
	RECEIPT.exe	Get hash	malicious	Browse	• 40.101.81.146
HHN-efz.ms-acdc.office.com	609110f2d14a6.dll	Get hash	malicious	Browse	• 40.101.137.34
	New%20order%20contract.html	Get hash	malicious	Browse	• 52.98.175.2

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{AE905FC9-AD44-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	21592
Entropy (8bit):	1.7594977787918844
Encrypted:	false
SSDEEP:	48:IwiGcprjGwpL0qUG/ap80qGBZGIpc0qG4fGeGvnZpv0qG4fGvw3Go3qp90qG4fGm:rWZ9Za2wLWk7tkNfk4FMktH
MD5:	586DB94373650BC9E3A11F8D83A43119
SHA1:	44830C9A42A7059540F75902D8ACCCD0C2CCC110
SHA-256:	CBB34950E8F8B039E5E8A0C56C9F0409E3D51D1418EC7B6FA664F6B7598BBF15
SHA-512:	CB3756652C002D04099293D445F789B3E7466756473E5BF50A9EBE635BA65E76D6C36F1C54351A0C11CF2CD9772A70F4F4F67F498FCAD27312D4E7250CF7AE3C
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{AE905FCB-AD44-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.573944233836972
Encrypted:	false
SSDEEP:	48:IwMGcprRGwpapG4pQtGrapbShZGQpB2GHHpcIaTGUpG:rQZLQr6NBShzj12IqA
MD5:	3ECFC996F83DCA4AA885FF3F72B684AD
SHA1:	4D5F1BC278921B850632B9F131CEACF9F6528BAE
SHA-256:	94138719C28C299D93F3175DAC56C4A5A1097852F4410206DBDC1364FEA3C108
SHA-512:	47F4F94D461247526ECBF9999F81775CDAC82CE5FA41018ADBDCA8D2D13FF149FCB62E8BA274761AA1EB0FEFDD4CDCABE7E9A631AC00CE72BA31AD0667F3 0E8
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Temp\~DFFDCA7E35786F02EC.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12917
Entropy (8bit):	0.39862566692758644
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo0qDF9lo0qJ9lW0qGcGvwywcGtRwi:kBqoI0qS0qM0qGcGvwywcGtRwi
MD5:	5AC667C80F587E96B1FA80C48BB205AC
SHA1:	8AE06DAFAC5BD829EBDF2585C6BE72B11645F7EC
SHA-256:	4603ADFFB302AFD33E6755000AF43E78307809BE6060D50346B41AFFB2655282
SHA-512:	DA5BB434493D5023D766CCAD26D075683F287310E2FD53E2C51EDB7B0119B4DA534223D047822E72DF4F31C583863038657543205226 7BB45C2FA524E63E2951
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFFF4222CFAFFA654A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25657
Entropy (8bit):	0.31341444137710367
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwT9lwT9l2a:kBqoxKAuvScS+sKa
MD5:	B141DA2A351E435F1D185F48AC4E0FF6
SHA1:	A257DD1A9B4D1AB44020E74757AC5C9C69575588
SHA-256:	1D1C565FF314222220A0BDEADB603FCDE1A742DEA5A4210871A6C6E0AAE37C4A
SHA-512:	49E24F4266573BEC3E25D738F23A9D169F14FBA3FBC7F4C6F80A9657BBA4B5882A4477734AD04A45FE4EA57F11F1542657F1184D97AD1FD03BA659287AF18D5A
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

General

Entropy (8bit):	6.549322455653532
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • 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:	8OKQ6ogGRx.dll
File size:	523264
MD5:	e8eae1a820426a722c7cae54ed5bacd8
SHA1:	4d8368f112e0c56e7caccb89724bfdad1999e706
SHA256:	eb498648d17ad5250ab1f38b190dd2da8bfa8db3ee8605 db991db79d15ad5cc
SHA512:	b75df93529215c6003ddb86bc76a52144b29aec918a40a 9dadec7446f67cc2626b67fa1738ed148e81a1c706dded6 9f609e1cd592cf13034ef9fd2cb21603032
SSDEEP:	12288:CdXaT8lLVrp6I7MsfHqWxSWlNTjGoLYTbgOJpX LH:CdXhp1YCMuFx/jGo0XL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ...^.G.....T.....AN.....V.....i.....h....^.B.....I..... U.....R.....W.....Rich.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x104a38a
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:	0x6089CC25 [Wed Apr 28 20:57:09 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:	61abfa6d76443dd7d018df0c9cf8b0a5

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007FCE58D690B7h
call 00007FCE58D6F684h
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007FCE58D690BCh
add esp, 0Ch
pop ebp
retn 000Ch
push 0000000Ch
push 0107B4A8h

Instruction
call 00007FCE58D69FCCh
xor eax, eax
inc eax
mov esi, dword ptr [ebp+0Ch]
test esi, esi
jne 00007FCE58D690BEh
cmp dword ptr [0118E36Ch], esi
je 00007FCE58D6919Ah
and dword ptr [ebp-04h], 00000000h
cmp esi, 01h
je 00007FCE58D690B7h
cmp esi, 02h
jne 00007FCE58D690E7h
mov ecx, dword ptr [01075238h]
test ecx, ecx
je 00007FCE58D690BEh
push dword ptr [ebp+10h]
push esi
push dword ptr [ebp+08h]
call ecx
mov dword ptr [ebp-1Ch], eax
test eax, eax
je 00007FCE58D69167h
push dword ptr [ebp+10h]
push esi
push dword ptr [ebp+08h]
call 00007FCE58D68EC6h
mov dword ptr [ebp-1Ch], eax
test eax, eax
je 00007FCE58D69150h
mov ebx, dword ptr [ebp+10h]
push ebx
push esi
push dword ptr [ebp+08h]
call 00007FCE58D66926h
mov edi, eax
mov dword ptr [ebp-1Ch], edi
cmp esi, 01h
jne 00007FCE58D690DAh
test edi, edi
jne 00007FCE58D690D6h
push ebx
push eax
push dword ptr [ebp+08h]
call 00007FCE58D6690Eh
push ebx
push edi
push dword ptr [ebp+08h]
call 00007FCE58D68E8Ch
mov eax, dword ptr [01075238h]
test eax, eax
je 00007FCE58D690B9h
push ebx
push edi
push dword ptr [ebp+08h]
call eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x7bbd0	0x58	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7bc28	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x191000	0x498	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x192000	0x2818	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x6b200	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x7a980	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x6b000	0x1ac	.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	0x6988d	0x69a00	False	0.70416512574	data	6.62139930186	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x6b000	0x115e0	0x11600	False	0.471967738309	data	5.23669501131	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x7d000	0x113300	0x1800	False	0.333984375	data	3.88700180982	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x191000	0x498	0x600	False	0.356119791667	data	2.99935790597	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x192000	0x2818	0x2a00	False	0.743117559524	data	6.59705049508	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1910a0	0x35c	data	English	United States
RT_MANIFEST	0x191400	0x91	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	FlushFileBuffers, GetConsoleCP, GetConsoleMode, SetEnvironmentVariableA, SetStdHandle, SetFilePointerEx, WriteConsoleW, CloseHandle, GetFileAttributesW, GetWindowsDirectoryW, CreateProcessW, OpenMutexW, VirtualProtectEx, EncodePointer, DecodePointer, HeapAlloc, GetSystemTimeAsFileTime, RaiseException, RtlUnwind, GetCommandLineA, GetCurrentThreadId, IsProcessorFeaturePresent, GetLastError, HeapFree, ExitProcess, GetModuleHandleExW, GetProcAddress, AreFileApisANSI, MultiByteToWideChar, WideCharToMultiByte, HeapSize, GetStdHandle, WriteFile, GetModuleFileNameW, GetProcessHeap, IsDebuggerPresent, GetTimeZoneInformation, SetLastError, GetCurrentThread, GetFileType, DeleteCriticalSection, GetStartupInfoW, GetModuleFileNameA, QueryPerformanceCounter, GetCurrentProcessId, GetEnvironmentStringsW, FreeEnvironmentStringsW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, InitializeCriticalSectionAndSpinCount, CreateEventW, Sleep, GetCurrentProcess, TerminateProcess, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetTickCount, GetModuleHandleW, CreateSemaphoreW, SetConsoleCtrlHandler, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, EnterCriticalSection, LeaveCriticalSection, FatalAppExitA, FreeLibrary, LoadLibraryExW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, HeapReAlloc, OutputDebugStringW, GetStringTypeW, CreateFileW
USER32.dll	GetPropW, CreateMenu, DeferWindowPos, BeginDeferWindowPos, UnregisterHotKey, TranslateMessage, RegisterWindowMessageW
GDI32.dll	MoveToEx, SetTextColor, SetBkMode, SetBkColor, LineTo, IntersectClipRect, GetClipBox, GetCharWidthW, CreateBitmap
COMCTL32.dll	ImageList_SetDragCursorImage, ImageList_Draw, PropertySheetW, CreatePropertySheetPageA

Exports

Name	Ordinal	Address
Enterbeen	1	0x1047ed0
Multiply	2	0x1047fb0

Version Infos

Description	Data
LegalCopyright	Fingergeneral Corporation. All rights reserved
InternalName	Probable
FileVersion	5.5.2.216 Sidedone
CompanyName	Fingergeneral Corporation

Description	Data
ProductName	Fingergeneral Wear twenty
ProductVersion	5.5.2.216
FileDescription	Fingergeneral Wear twenty
OriginalFilename	turn.dll
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:51:18.333254099 CEST	60985	53	192.168.2.3	8.8.8.8
May 4, 2021 18:51:18.338377953 CEST	50200	53	192.168.2.3	8.8.8.8
May 4, 2021 18:51:18.378372908 CEST	51281	53	192.168.2.3	8.8.8.8
May 4, 2021 18:51:18.387293100 CEST	53	50200	8.8.8.8	192.168.2.3
May 4, 2021 18:51:18.408304930 CEST	53	60985	8.8.8.8	192.168.2.3
May 4, 2021 18:51:18.426934004 CEST	53	51281	8.8.8.8	192.168.2.3
May 4, 2021 18:51:19.130103111 CEST	49199	53	192.168.2.3	8.8.8.8
May 4, 2021 18:51:19.178749084 CEST	53	49199	8.8.8.8	192.168.2.3
May 4, 2021 18:51:20.001471043 CEST	50620	53	192.168.2.3	8.8.8.8
May 4, 2021 18:51:20.050255060 CEST	53	50620	8.8.8.8	192.168.2.3
May 4, 2021 18:51:21.065521002 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 18:51:21.117543936 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 18:51:21.394946098 CEST	60152	53	192.168.2.3	8.8.8.8
May 4, 2021 18:51:21.456048012 CEST	53	60152	8.8.8.8	192.168.2.3
May 4, 2021 18:51:21.984514952 CEST	57544	53	192.168.2.3	8.8.8.8
May 4, 2021 18:51:22.033207893 CEST	53	57544	8.8.8.8	192.168.2.3
May 4, 2021 18:51:23.754410982 CEST	55984	53	192.168.2.3	8.8.8.8
May 4, 2021 18:51:23.811686039 CEST	53	55984	8.8.8.8	192.168.2.3
May 4, 2021 18:51:24.549612045 CEST	64185	53	192.168.2.3	8.8.8.8
May 4, 2021 18:51:24.601274967 CEST	53	64185	8.8.8.8	192.168.2.3
May 4, 2021 18:51:25.503813982 CEST	65110	53	192.168.2.3	8.8.8.8
May 4, 2021 18:51:25.552414894 CEST	53	65110	8.8.8.8	192.168.2.3
May 4, 2021 18:52:03.254508972 CEST	58361	53	192.168.2.3	8.8.8.8
May 4, 2021 18:52:03.313453913 CEST	53	58361	8.8.8.8	192.168.2.3
May 4, 2021 18:52:15.317749023 CEST	63492	53	192.168.2.3	8.8.8.8
May 4, 2021 18:52:15.390950918 CEST	53	63492	8.8.8.8	192.168.2.3
May 4, 2021 18:52:20.053031921 CEST	60831	53	192.168.2.3	8.8.8.8
May 4, 2021 18:52:20.103934050 CEST	53	60831	8.8.8.8	192.168.2.3
May 4, 2021 18:52:38.655663013 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 18:52:38.708623886 CEST	53	60100	8.8.8.8	192.168.2.3
May 4, 2021 18:52:56.289465904 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 18:52:56.348114014 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 18:53:27.666838884 CEST	50141	53	192.168.2.3	8.8.8.8
May 4, 2021 18:53:27.721466064 CEST	53	50141	8.8.8.8	192.168.2.3
May 4, 2021 18:53:28.937237978 CEST	53023	53	192.168.2.3	8.8.8.8
May 4, 2021 18:53:28.986049891 CEST	53	53023	8.8.8.8	192.168.2.3
May 4, 2021 18:53:29.070245028 CEST	49563	53	192.168.2.3	8.8.8.8
May 4, 2021 18:53:29.073194027 CEST	51352	53	192.168.2.3	8.8.8.8
May 4, 2021 18:53:29.124036074 CEST	53	49563	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:53:29.148881912 CEST	53	51352	8.8.8.8	192.168.2.3
May 4, 2021 18:53:29.954231024 CEST	59349	53	192.168.2.3	8.8.8.8
May 4, 2021 18:53:30.011257887 CEST	53	59349	8.8.8.8	192.168.2.3
May 4, 2021 18:53:30.180514097 CEST	57084	53	192.168.2.3	8.8.8.8
May 4, 2021 18:53:30.229265928 CEST	53	57084	8.8.8.8	192.168.2.3
May 4, 2021 18:53:30.661994934 CEST	58823	53	192.168.2.3	8.8.8.8
May 4, 2021 18:53:30.711884975 CEST	53	58823	8.8.8.8	192.168.2.3
May 4, 2021 18:53:32.214960098 CEST	57568	53	192.168.2.3	8.8.8.8
May 4, 2021 18:53:32.274662971 CEST	53	57568	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 18:53:28.937237978 CEST	192.168.2.3	8.8.8.8	0x4990	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
May 4, 2021 18:53:29.954231024 CEST	192.168.2.3	8.8.8.8	0xea33	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
May 4, 2021 18:53:30.180514097 CEST	192.168.2.3	8.8.8.8	0x30ea	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)

DNS Answers

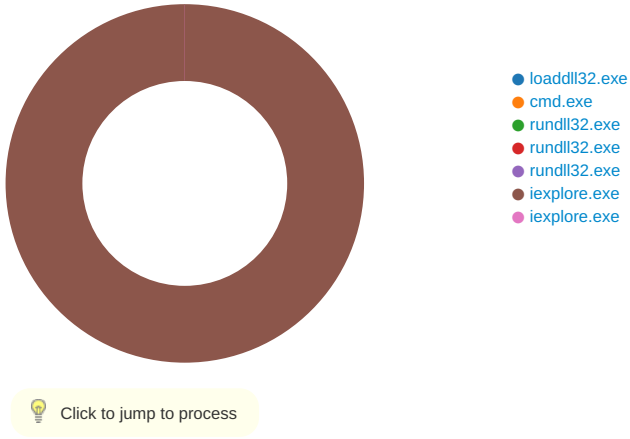
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 18:53:28.986049891 CEST	8.8.8.8	192.168.2.3	0x4990	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
May 4, 2021 18:53:28.986049891 CEST	8.8.8.8	192.168.2.3	0x4990	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
May 4, 2021 18:53:28.986049891 CEST	8.8.8.8	192.168.2.3	0x4990	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
May 4, 2021 18:53:28.986049891 CEST	8.8.8.8	192.168.2.3	0x4990	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
May 4, 2021 18:53:28.986049891 CEST	8.8.8.8	192.168.2.3	0x4990	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
May 4, 2021 18:53:28.986049891 CEST	8.8.8.8	192.168.2.3	0x4990	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
May 4, 2021 18:53:28.986049891 CEST	8.8.8.8	192.168.2.3	0x4990	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
May 4, 2021 18:53:28.986049891 CEST	8.8.8.8	192.168.2.3	0x4990	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
May 4, 2021 18:53:30.011257887 CEST	8.8.8.8	192.168.2.3	0xea33	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:53:30.011257887 CEST	8.8.8.8	192.168.2.3	0xea33	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:53:30.011257887 CEST	8.8.8.8	192.168.2.3	0xea33	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:53:30.011257887 CEST	8.8.8.8	192.168.2.3	0xea33	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:53:30.011257887 CEST	8.8.8.8	192.168.2.3	0xea33	No error (0)	FRA-efz.ms-acdc.office.com		40.101.81.162	A (IP address)	IN (0x0001)
May 4, 2021 18:53:30.011257887 CEST	8.8.8.8	192.168.2.3	0xea33	No error (0)	FRA-efz.ms-acdc.office.com		40.101.12.98	A (IP address)	IN (0x0001)
May 4, 2021 18:53:30.011257887 CEST	8.8.8.8	192.168.2.3	0xea33	No error (0)	FRA-efz.ms-acdc.office.com		52.97.176.2	A (IP address)	IN (0x0001)
May 4, 2021 18:53:30.229265928 CEST	8.8.8.8	192.168.2.3	0x30ea	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:53:30.229265928 CEST	8.8.8.8	192.168.2.3	0x30ea	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 18:53:30.229265928 CEST	8.8.8.8	192.168.2.3	0x30ea	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:53:30.229265928 CEST	8.8.8.8	192.168.2.3	0x30ea	No error (0)	HHN-efz.ms-acdc.office.com		40.101.138.2	A (IP address)	IN (0x0001)
May 4, 2021 18:53:30.229265928 CEST	8.8.8.8	192.168.2.3	0x30ea	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.66	A (IP address)	IN (0x0001)
May 4, 2021 18:53:30.229265928 CEST	8.8.8.8	192.168.2.3	0x30ea	No error (0)	HHN-efz.ms-acdc.office.com		40.101.138.18	A (IP address)	IN (0x0001)
May 4, 2021 18:53:30.229265928 CEST	8.8.8.8	192.168.2.3	0x30ea	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.66	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 2168 Parent PID: 5620

General

Start time:	18:51:24
Start date:	04/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\8OKQ6ogGRx.dll'
Imagebase:	0x50000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
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: 00000000.00000002.470954657.0000000003618000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 3880 Parent PID: 2168

General

Start time:	18:51:25
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\8OKQ6ogGRx.dll',#1
Imagebase:	0xbd0000
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: 3468 Parent PID: 2168

General

Start time:	18:51:25
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\8OKQ6ogGRx.dll,Enterbeen
Imagebase:	0x9e0000
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: 6024 Parent PID: 3880

General

Start time:	18:51:25

Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\8OKQ6ogGRx.dll',#1
Imagebase:	0x9e0000
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: 3512 Parent PID: 2168

General

Start time:	18:51:28
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\8OKQ6ogGRx.dll,Multiply
Imagebase:	0x9e0000
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: 5212 Parent PID: 792

General

Start time:	18:53:26
Start date:	04/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7e65e0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Caches	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB6D170F70	CreateDirectoryW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5240 Parent PID: 5212

General

Start time:	18:53:27
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5212 CREDAT:17410 /prefetch:2
Imagebase:	0xfd0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis