ID: 403758
Sample Name: 21a5f8d0000.dll
Cookbook: default.jbs
Time: 11:41:53
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

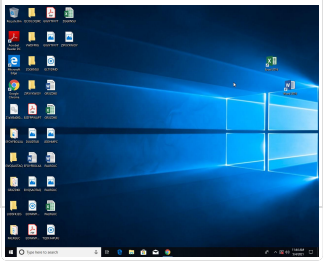
Analysis Report 21a5f8d0000.dll

Overview

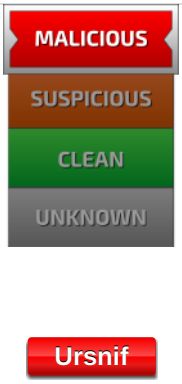
General Information

Sample Name:	21a5f8d0000.dll
Analysis ID:	403758
MD5:	b8c176dc8ab0d7..
SHA1:	97826adb6aac63..
SHA256:	cc79e66b24bfca1..
Tags:	Gozi
Infos:	

Most interesting Screenshot:



Detection

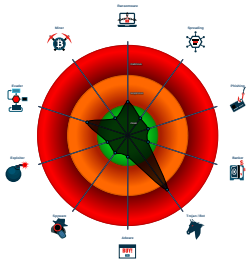


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Ursnif
- Machine Learning detection for samp…
- Checks if Antivirus/Antispyware/Fire…
- Checks if the current process is bein…
- Creates a process in suspended mo…
- PE file does not import any functions
- Sample execution stops while proce…
- Tries to load missing DLLs

Classification



Startup

- **System is w10x64**
- loaddll64.exe (PID: 6304 cmdline: loaddll64.exe 'C:\Users\user\Desktop\21a5f8d0000.dll' MD5: A84133CCB118CF35D49A423CD836D0EF)
  - cmd.exe (PID: 6312 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\21a5f8d0000.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6336 cmdline: rundll32.exe 'C:\Users\user\Desktop\21a5f8d0000.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
    - MpCmdRun.exe (PID: 6588 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
      - conhost.exe (PID: 6596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rundll32.exe (PID: 6324 cmdline: rundll32.exe C:\Users\user\Desktop\21a5f8d0000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
21a5f8d0000.dll	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Copyright Joe Security LLC 2021

Signature Overview

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

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

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

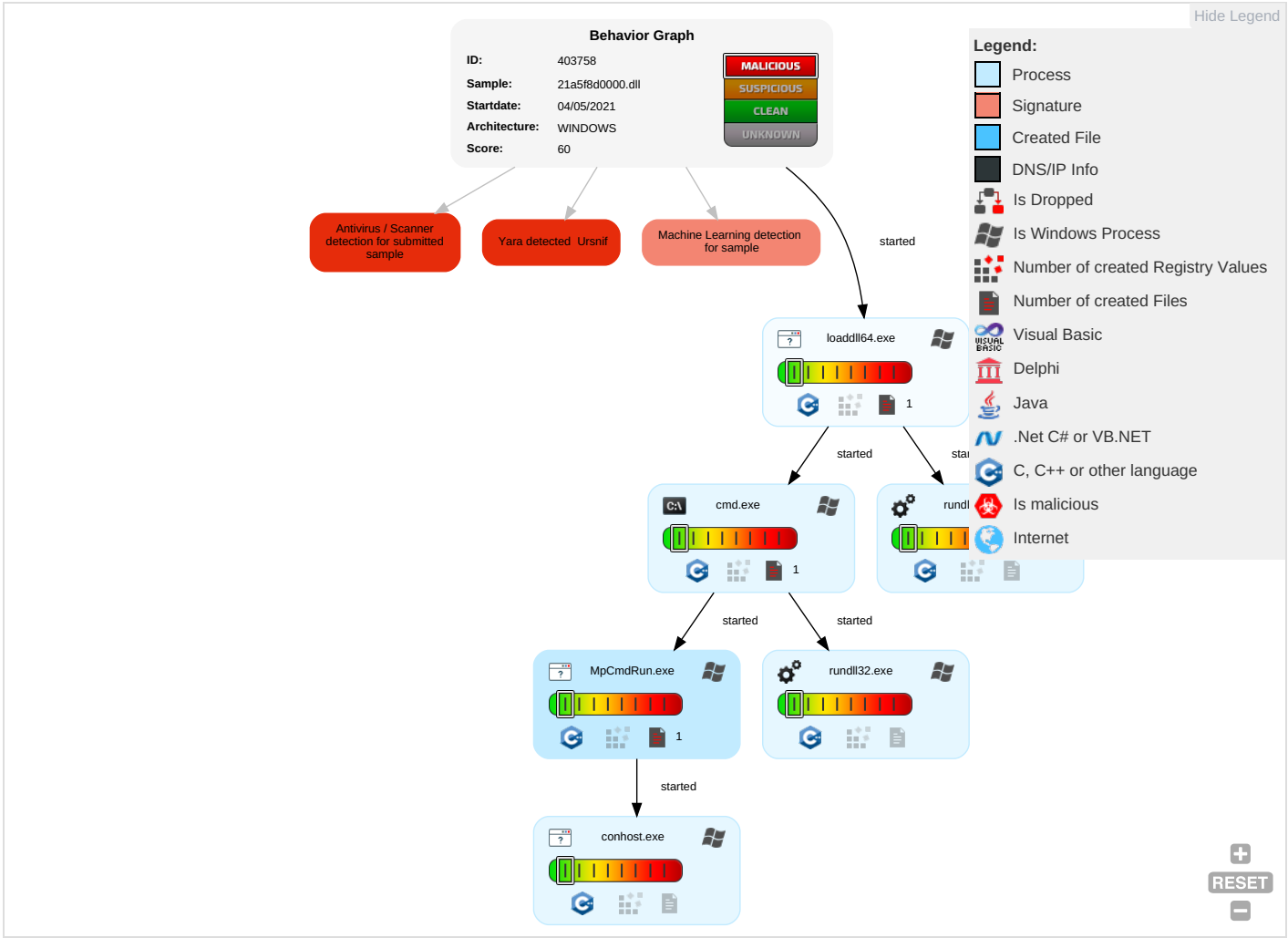
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	Process Injection 1 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Rundll32 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 t Redirect Pho Calls/SMS

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

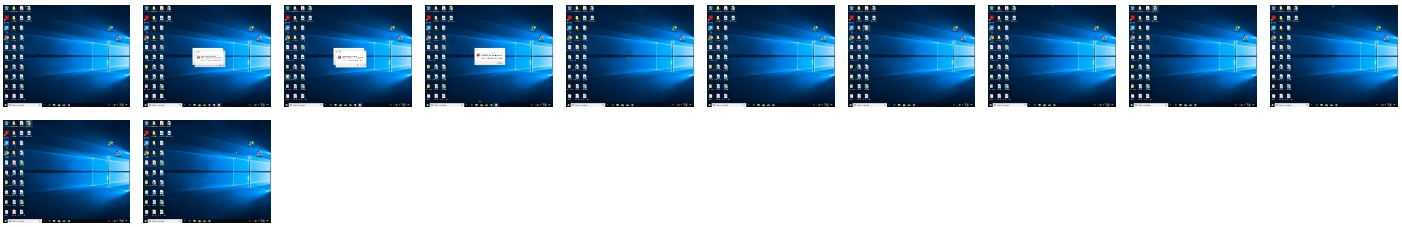
Behavior Graph



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
21a5f8d0000.dll	100%	Avira	HEUR/AGEN.1108168	
21a5f8d0000.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://file://USER.ID%lu.exe/upd	21a5f8d0000.dll	false	• Avira URL Cloud: safe	low
http://constitution.org/usdeclar.txt	21a5f8d0000.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://constitution.org/usdeclar.txtC:	21a5f8d0000.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403758
Start date:	04.05.2021
Start time:	11:41:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	21a5f8d0000.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:	29
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@9/1@0/0
EGA Information:	Failed
HDC Information:	Failed

Copyright Joe Security LLC 2021

HCA Information:	• Successful, ratio: 100% • 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
11:44:14	API Interceptor	1x Sleep call for process: MpCmdRun.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

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	data
Category:	modified
Size (bytes):	906
Entropy (8bit):	3.1320890800881007
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rPWKk9+MlWlLehB4yAq7ejCMWH:OaqdmuF3rw+kWReH4yJ7M+
MD5:	CE1CC265AB67E3C997C2BD8A51DE492A
SHA1:	90E8A24EC0C49E555721FDE5A4000E1FC5FC867E
SHA-256:	E907A66E7EFFA5A9D710327C455CA0B3DD561E0146EA6F0B9A33682AC8CA4173
SHA-512:	384559B9381A90DB5729E2CE6B6D924D6E87C30991F4B7EAE92A6859D0D17C7D483733D3769F3220797381321D4DCE8210B4601DACF73FBDBCFBEC23335CADI
Malicious:	false
Reputation:	low

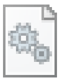
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Preview:	........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. . ".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.u.e. .. M.a.y. .. 0.4. .. 2.0.2.1. .1.1.:.4.4.:.1. 4.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.0. 4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.u.e. .. M.a.y. .. 0.4. .. 2.0.2.1. .1.1.:.4.4.:.1.4.....-.....

Static File Info

General

File type:	MS-DOS executable
Entropy (8bit):	6.331169087847959
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 84.88% • Win64 Executable (generic) (12005/4) 9.99% • DOS Executable Borland Pascal 7.0x (2037/25) 1.69% • Generic Win/DOS Executable (2004/3) 1.67% • DOS Executable Generic (2002/1) 1.67%
File name:	21a5f8d0000.dll
File size:	223744
MD5:	b8c176dc8ab0d768031014f95b8816e8
SHA1:	97826adb6aac6340a74ca024a65065fa6fdb21ca
SHA256:	cc79e66b24bfca1cd0ef27c63921737786dcdae02f871279800ea2c82939721a
SHA512:	0e2f907a21f245784ea260c11b2eff428e892fc0c4b3594a0eac59cff127129896227676e4cc73be9af003ce5b2b496b3148119f1d7be35439e157aec53a2b44
SSDEEP:	3072:fWLHqJ4VtWYQUVpsPHQqdPFQ6l7Bz9DHzcUvNfxYPr9fGWg+Bm5kf7JDLm:4qO/rsPHN7Q6l7Bz9zhvNJYPrg1QNL
File Content Preview:	MZ...PE..d..

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1800080e4
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	
Time Stamp:	0x60804A27 [Wed Apr 21 15:52:07 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Copyright Joe Security LLC 2021

Instruction
inc eax
push ebx
dec eax
sub esp, 20h
test edx, edx
mov ebx, 00000001h
je 00007F9EF0987E76h
cmp edx, ebx
jne 00007F9EF0987E81h
mov eax, ebx
lock xadd dword ptr [0002B8AFh], eax
add eax, ebx
cmp eax, ebx
jne 00007F9EF0987E71h
dec ecx
mov edx, eax
call 00007F9EF099AC22h
test eax, eax
je 00007F9EF0987E65h
xor ebx, ebx
jmp 00007F9EF0987E61h
lock add dword ptr [0002B891h], FFFFFFFFh
jne 00007F9EF0987E57h
call 00007F9EF0999CE3h
mov eax, ebx
dec eax
add esp, 20h
pop ebx
ret
int3
int3
dec eax
mov dword ptr [esp+08h], ebx
dec eax
mov dword ptr [esp+10h], ebp
dec eax
mov dword ptr [esp+18h], esi
push edi
dec eax
sub esp, 20h
cmp dword ptr [0002BE31h], 00000000h
inc ecx
mov ebx, ecx
dec ecx
mov esi, eax
dec eax
mov eax, edx
je 00007F9EF0987EF3h
xor edx, edx
dec eax
mov ecx, eax
call 00007F9EF0982475h
dec eax
mov ecx, dword ptr [0002B83Dh]
dec esp
lea eax, dword ptr [ebx+01h]
xor edx, edx
dec eax
mov ebp, eax
call dword ptr [00024F26h]
dec eax
test eax, eax
dec eax
mov edi, eax

Copyright Joe Security LLC 2021

Instruction
je 00007F9EF0987EC7h
dec esp
mov eax, ebx
dec eax
mov edx, esi
dec eax
mov ecx, eax
call 00007F9EF099F36Bh
dec eax
lea ecx, dword ptr [0002BDB9h]
mov byte ptr [ebx+edi], 00000000h
call dword ptr [0002504Fh]
lock add dword ptr [0002BDCFh], 01h
dec eax
lea ecx, dword ptr [00000000h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x31b10	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x30a20	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x34000	0x17ac	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x39000	0x344	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2d000	0x530	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x2eda4	0x1e0	.rdata
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	0x2ba46	0x2bc00	False	0.568303571429	data	6.33861296477	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2d000	0x4b48	0x4c00	False	0.403114720395	data	5.25264814147	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x32000	0x1f88	0x1a00	False	0.307992788462	lif file	3.73553845524	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x34000	0x17ac	0x1800	False	0.53857421875	data	5.30366145469	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x36000	0x2148	0x2200	False	0.427504595588	data	4.96451183531	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x39000	0x1000	0xa00	False	0.458984375	data	4.2959680462	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

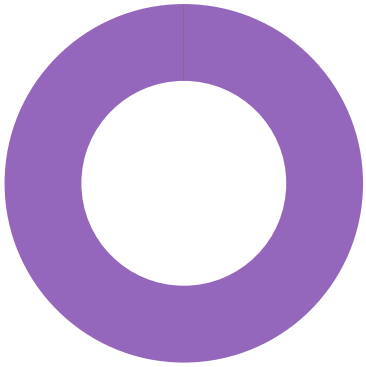
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



- loaddll64.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- MpCmdRun.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 6304 Parent PID: 5688

General

Start time:	11:42:45
Start date:	04/05/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\21a5f8d0000.dll'
Imagebase:	0x7ff69d4e0000
File size:	140288 bytes
MD5 hash:	A84133CCB118CF35D49A423CD836D0EF
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: 6312 Parent PID: 6304

General

Start time:	11:42:45
Start date:	04/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\21a5f8d0000.dll',#1
Imagebase:	0x7ff7eef80000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F

Copyright Joe Security LLC 2021

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: 6324 Parent PID: 6304

General

Start time:	11:42:45
Start date:	04/05/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\21a5f8d0000.dll,#1
Imagebase:	0x7ff6c6b80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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: 6336 Parent PID: 6312

General

Start time:	11:42:45
Start date:	04/05/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\21a5f8d0000.dll',#1
Imagebase:	0x7ff6c6b80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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: MpCmdRun.exe PID: 6588 Parent PID: 6312

General

Start time:	11:44:13

Start date:	04/05/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff6cf3a0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	........-.....	success or wait	1	7FF6CF3CBC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 54 00 75 00 65 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 30 00 34 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 31 00 3a 00 34 00 34 00 3a 00 31 00 34 00 0d 00 0a 00 0d	M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. ."C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m. p.c.m.d.r.u.n...e.x.e.". .-.w. d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.u.e. .. M.a.y. .. 0.4. .. 2.0.2.1. .1.1.:. 4.4.:.1.4.....	success or wait	1	7FF6CF3CBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....	success or wait	1	7FF6CF3CBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	W.D.E.n.a.b.l.e.....	success or wait	1	7FF6CF3CBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e. (.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....	success or wait	1	7FF6CF3CBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 54 00 75 00 65 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 30 00 34 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 31 00 3a 00 34 00 34 00 3a 00 31 00 34 00 0d 00 0a 00	M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.u.e. .. M.a.y. .. 0.4. .. 2.0.2.1. .1.1.:.4.4. :.1.4.....	success or wait	1	7FF6CF3CBC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.....	success or wait	1	7FF6CF3CBC96	WriteFile

Analysis Process: conhost.exe PID: 6596 Parent PID: 6588

General

Start time:	11:44:13
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis