ID: 630152
Sample Name:
OojqjHGE0W.exe
Cookbook: default.jbs
Time: 14:38:37
Date: 19/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

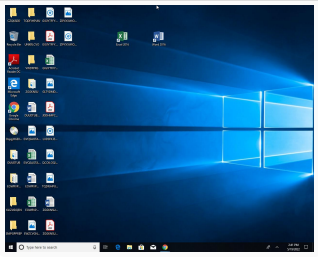
Windows Analysis Report

OojqjHGE0W.exe

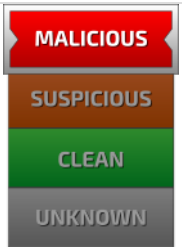
Overview

General Information

Sample Name:	OojqjHGE0W.exe
Analysis ID:	630152
MD5:	4ed3fa33609a51..
SHA1:	aff82f0554f18c7…
SHA256:	988177454fe3a5..
Tags:	exe signed
Infos:	



Detection



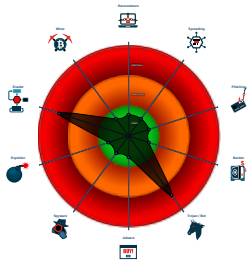
Ursnif

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- Writes or reads registry keys via WMI
- Tries to detect sandboxes and other…
- Found API chain indicative of debug…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Found evasive API chain (may stop…
- Writes registry values via WMI

Classification



Process Tree

- **System is w10x64**
- OojqjHGE0W.exe (PID: 3408 cmdline: "C:\Users\user\Desktop\OojqjHGE0W.exe" MD5: 4ED3FA33609A51BAF209A5954BEF6633)
  - InstallUtil.exe (PID: 5584 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"S0cXgkczLn8DzpFkqJkBMx5geC7yniHR4ECyGeVYDO5jsqYVdXE2v679nj0L+4Im3j/P6z1P+Yt1BRosNI7Edvd1U5N0OYNwNVRfWwfbhm6jaX9Kjt9vEFS5dCsKX71jt2Xz0+H4zoaN0nbuxJko5Np4J7p0zDkJiLw6HxWp4zGiWIwT
2o7vLE3guRMwyRVXO9dkUDWYMn+gWBAKovUuxnaDZD7PIJ/H8zTx3Yz7628+O4pRw2KlIh0/fkIzdLb08ciTd+kW2cM+z/W40SWfyGxExAOJ7AMei6jzcKc68f1Bamsf4QGIbKQz9UqHR5cBlCKpLVi3hYeembcW9ep7oVhTb5Y2TC0ZA
zzb/feTdhI=",
  "c2_domain": [
    "anm.msn.com",
    "194.76.225.45",
    "msi.msn.com",
    "194.76.225.56"
  ],
  "botnet": "1700",
  "server": "50",
  "serpent_key": "1OoXFPbINCQ6HCAa",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000003.504942023.00000000020C8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000000A.00000003.501961576.00000000020C8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000000A.00000003.502032730.00000000020C8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000000A.00000002.535140555.00000000020C8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000000A.00000003.501571456.00000000020C8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.InstallUtil.exe.1b694a0.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
10.2.InstallUtil.exe.1340000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
10.2.InstallUtil.exe.1b694a0.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.3 - Destination IP: 52.169.118.173

Timestamp:	192.168.2.352.169.118.17349702802033203 05/19/22-14:41:40.292996
SID:	2033203
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.3 - Destination IP: 52.169.118.173

Timestamp:	192.168.2.352.169.118.17349702802033204 05/19/22-14:41:40.292996
SID:	2033204
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

System Summary

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Malware Analysis System Evasion

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Ursnif

Remote Access Functionality

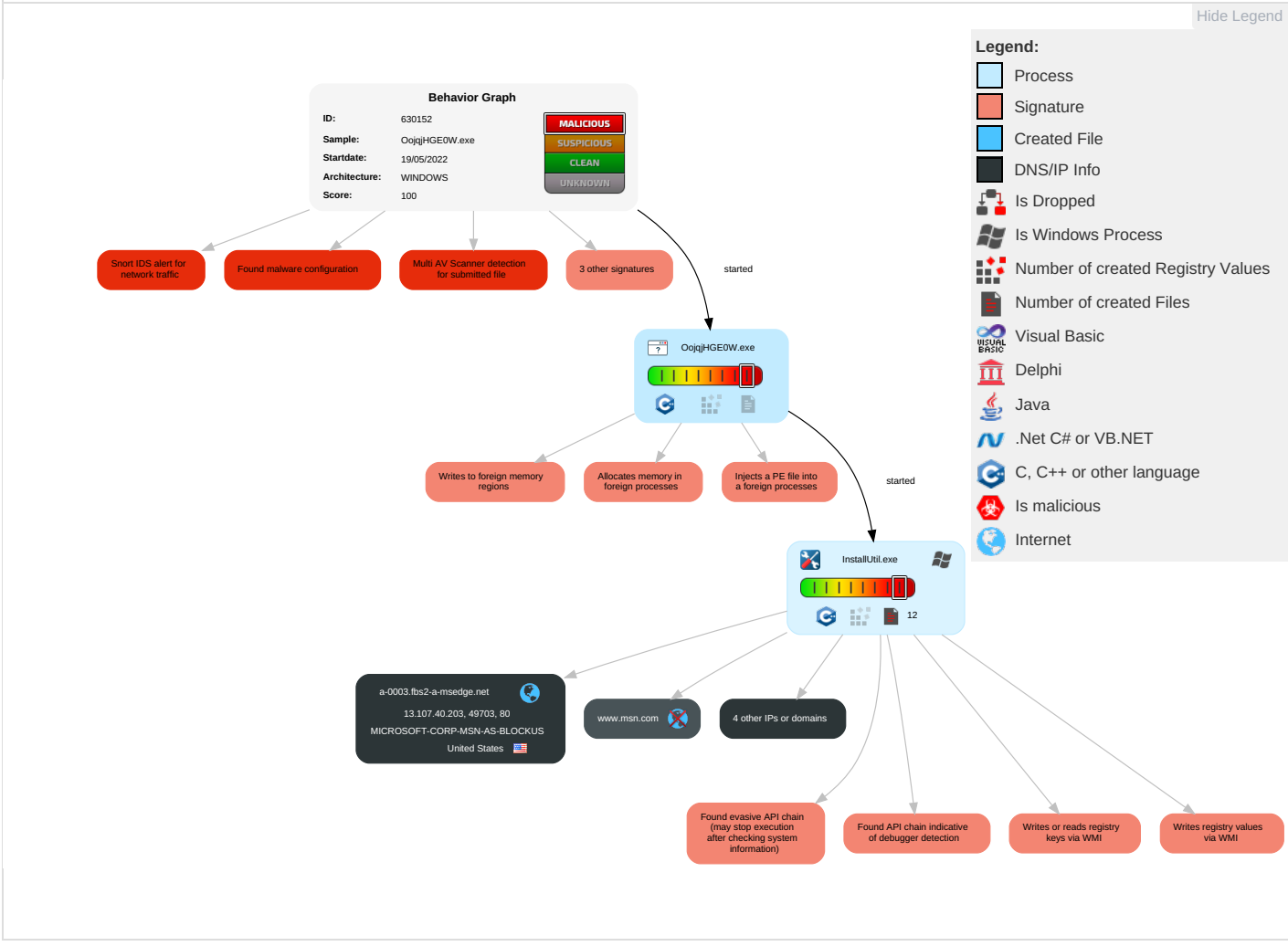
Yara detected Ursnif

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 Windows Service	1 Windows Service	1 2 Virtualization/Sandbox Evasion	OS Credential Dumping	1 System Time Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	2 Service Execution	Boot or Logon Initialization Scripts	3 1 1 Process Injection	3 1 1 Process Injection	LSASS Memory	2 2 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 2 Native API	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 2 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)	3 Obfuscated Files or Information	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Software Packing	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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
OojqjHGE0W.exe	46%	ReversingLabs	Win32.Trojan.Jaik	
OojqjHGE0W.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.2.OojqjHGE0W.exe.8b5230.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.0.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
10.2.InstallUtil.exe.1340000.1.unpack	100%	Avira	HEUR/AGEN.1245293		Download File
10.0.InstallUtil.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.3.OojqjHGE0W.exe.2580000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.3.OojqjHGE0W.exe.8b5230.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.OojqjHGE0W.exe.2580000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	safe	
http://https://i.geistm.com/l/HFCH_DTS_LP?bcid=61c4707a19d27603f32a58ba&bhid=6203eb0e7db0ad17f44b22d8&a	0%	Avira URL Cloud	safe	
http://https://cdn.hoergeraete.hoeren-heute.ch/horizon_reveal/?act=ACT0000040013ACT&utm_source=mcrs&	0%	Avira URL Cloud	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://https://i.geistm.com/l/HFCH_DTS_LP?bcid=61c4707a19d27603f32a58b8&bhid=62470ee6adad76040858398f&a	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
a-0003.fbs2-a-msedge.net	13.107.40.203	true	false		unknown
anm.msn.com	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.msn.com/de-ch/	false		high
http://www.msn.com/	false		high

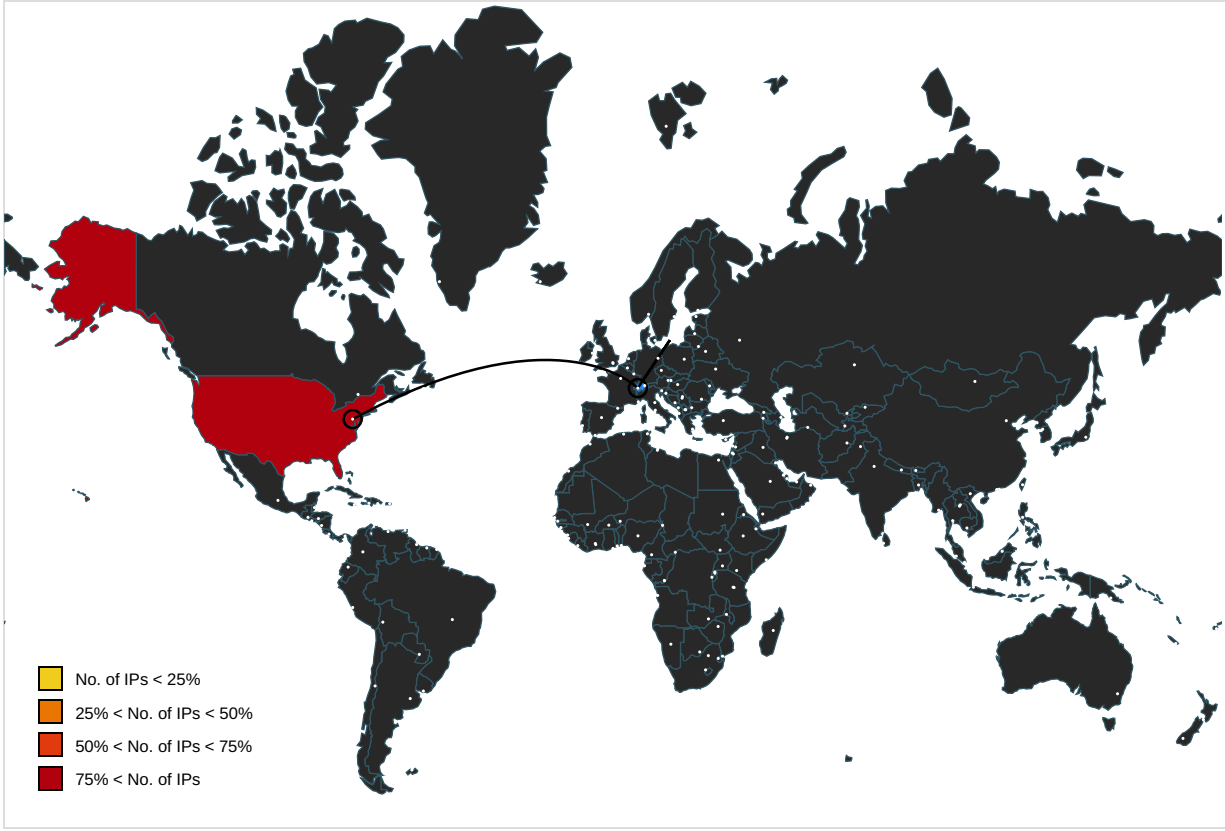
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	InstallUtil.exe, 0000000A.00000003.504725612.00000004301000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.msn.com/de-ch/news/other/weniger-verbindungen-zwischen-z%c3%bcrich-und-bern-daf%c3%bcr-m	InstallUtil.exe, 0000000A.00000002.535230526.00000004300000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535290243.0000000004396000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504725612.0000000004301000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535347560.0000000004400000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/de-ch/news/other/fremdes-b%c3%bcsi-gef%c3%bcttert-frau-soll-1250-franken-strafe-	InstallUtil.exe, 0000000A.00000002.535230526.00000000004300000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535290243.0000000004396000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504725612.0000000004301000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535347560.0000000004400000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://outlook.com/	InstallUtil.exe, 0000000A.00000002.535230526.00000000004300000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535290243.0000000004396000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504725612.0000000004301000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535347560.0000000004400000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.msn.com/de-ch/shopping	InstallUtil.exe, 0000000A.00000002.535230526.00000000004300000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535290243.0000000004396000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535347560.0000000004400000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ogp.me/ns#	InstallUtil.exe, 0000000A.00000002.535230526.00000000004300000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535290243.0000000004396000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504725612.0000000004301000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535347560.0000000004400000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://i.geistm.com/l/HFCH_DTS_LP?bcid=61c4707a19d27603f32a58ba&bhid=6203eb0e7db0ad17f44b22d8&a	InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://browser.events.data.msn.com/OneCollector/1.0/t.js?qsp=true&anoncknm=%22%22&name=%22M	InstallUtil.exe, 0000000A.00000002.535230526.00000000004300000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535290243.0000000004396000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504725612.0000000004301000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535347560.0000000004400000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cdn.hoergeraete.hoeren-heute.ch/horizon_reveal/?act=ACT0000040013ACT&utm_source=mcrs&	InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/de-ch/sport/other/der-fcz-verabschiedet-sich-von-doumbia-und-ceesay/ar-AAXsezM?o	InstallUtil.exe, 0000000A.00000002.535230526.00000000004300000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535290243.0000000004396000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504725612.0000000004301000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535347560.0000000004400000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/de-ch/news/other/stadtrat-handelt-in-z%c3%bcrich-west-mehr-preisg%c3%bcnstige-wo	InstallUtil.exe, 0000000A.00000002.535230526.00000000004300000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535290243.0000000004396000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504725612.0000000004301000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535347560.0000000004400000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://deff.nelreports.net/api/report?cat=msn	InstallUtil.exe, 0000000A.00000003.504942023.000000020C8000.00000004.00000020.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535140555.00000000020C8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.msn.com/de-ch/news/other/autofahrer-38-rast-mit-94-km-h-durch-30er-zone/ar-AAXsnwd?ocid=	InstallUtil.exe, 0000000A.00000002.535230526.00000000004300000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535290243.0000000004396000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504725612.0000000004301000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535347560.0000000004400000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ogp.me/ns/fb#	InstallUtil.exe, 0000000A.00000002.535230526.00000000004300000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535290243.0000000004396000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504725612.0000000004301000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535347560.0000000004400000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.msn.com/de-ch/news/other/olivia-und-noah-sind-die-beliebtesten-baby-vornamen-in-z%c3%bcr	InstallUtil.exe, 0000000A.00000002.535230526.00000000004300000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535290243.0000000004396000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504725612.0000000004301000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535347560.0000000004400000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.msn.com/de-ch/news/other/z%c3%bcrcher-kantonsrat-pr%c3%bcft-nach-igelkot-vorfall-sicherh	InstallUtil.exe, 0000000A.00000002.535230526.00000000004300000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535290243.0000000004396000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504725612.0000000004301000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535347560.0000000004400000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.msn.com/de-ch	InstallUtil.exe, 0000000A.00000002.535230526.00000000004300000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535290243.0000000004396000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504725612.0000000004301000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000002.535347560.0000000004400000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://i.geistm.com/l/HFCH_DTS_LP?bcid=61c4707a19d27603f32a58b8&bhid=62470ee6ada76040858398f&a	InstallUtil.exe, 0000000A.00000003.504892855.0000000002049000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.107.40.203	a-0003.fbs2-a-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	630152
Start date and time: 19/05/202214:38:37	2022-05-19 14:38:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OojqjHGE0W.exe
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:	12
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.winEXE@3/0@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 96.7% (good quality ratio 96.7%) • Quality average: 91.3% • Quality standard deviation: 14%

HCA Information:	• Successful, ratio: 69% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.169.118.173
- Excluded domains from analysis (whitelisted): fs.microsoft.com, redirection.prod.cms.msn.com.akadns.net, ctldl.windowsupdate.com, legacy-redirection-neurope-prod-hp.cloudapp.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: OojqjHGE0W.exe

Simulations

Behavior and APIs

No simulations

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 (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.52461417001665

TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	OojqjHGE0W.exe
File size:	1241656
MD5:	4ed3fa33609a51baf209a5954bef6633
SHA1:	aff82f0554f18c780561d6b8b1ca5a1001e42512
SHA256:	988177454fe3a5ba8fcdf7f3124e2c56f312b776542d3763540c254df6fe6f76
SHA512:	3beaba94d2a6df632b029d0c48521cea8adb98a1b7eeee9d547544415b36a251c41fabce2bcbbdaf53f4e090783f49d7c10e5d952d9313aa182aa1c2971201f4
SSDEEP:	24576:21uu0F2xRqVHdQ9PerE5gOGFGtCZXUzvjJMFHk1Udgd:A02WdQ9GCOFb6eXO
TLSH:	AC4501017D8CC031ECA226B43836E295A13B7D81672664CB65F9B3AF95B1BC0DD79363
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0...t...t...t.....U.].....`.d.....T.....}.m.s...t...,....Q.v.....d.u...t.i.r.....c.u...Richt.....PE..L.....b...

File Icon

Icon Hash:	54f9e0c4dcf8705d

Static PE Info

General

Entrypoint:	0x411fc0
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6283FED8 [Tue May 17 20:00:24 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	06a834e3824803366fcfecb5c9777295

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**A certificate chain could not be built to a trusted root authority**
Error Number:	-2146762486
Not Before, Not After	• 12/29/2021 4:00:00 PM 9/2/2022 4:59:59 PM
Subject Chain	• CN=exxon.com, O=Exxon Mobil Corporation, L=Irving, S=Texas, C=US
Version:	3
Thumbprint MD5:	B7C2B39C14AF65D1434078B10A8064DE
Thumbprint SHA-1:	9B93192A2BF5E6EC0A32E4966431D1E2FD1FA4AF
Thumbprint SHA-256:	97135CBA56D0300287DF31C8B39546AD4605FB9C88311AEB0B12B76AC15C46BF
Serial:	0A2787FBB4627C91611573E323584113

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
call 00007FEAECD8B32Bh

Instruction
call 00007FEAECD8B036h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push FFFFFFFEh
push 00511B30h
push 00416210h
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFF98h

Instruction
push ebx
push esi
push edi
mov eax, dword ptr [00513064h]
xor dword ptr [ebp-08h], eax
xor eax, ebp
push eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
mov dword ptr [ebp-18h], esp
mov dword ptr [ebp-70h], 00000000h
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [00401044h]
cmp dword ptr [00515DDCh], 00000000h
jne 00007FEAECD8B010h
push 00000000h
push 00000000h
push 00000001h
push 00000000h
call dword ptr [00401040h]
call 00007FEAECD8B193h
mov dword ptr [ebp-6Ch], eax
call 00007FEAECD8F16Bh
test eax, eax
jne 00007FEAECD8B00Ch
push 0000001Ch
call 00007FEAECD8B150h
add esp, 04h
call 00007FEAECD8EAC8h
test eax, eax
jne 00007FEAECD8B00Ch
push 00000010h
call 00007FEAECD8B13Dh

Rich Headers

Programming Language:	• [LNK] VS2010 build 30319 • [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [C++] VS2010 build 30319 • [RES] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x112114	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x116000	0x17630	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x12de00	0x1438	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x12e000	0x1638	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1180	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x8118	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x140	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x11184a	0x111a00	False	0.832347104842	data	7.57139474025	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x113000	0x2de0	0x1000	False	0.190673828125	data	2.23907016207	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x116000	0x17630	0x17800	False	0.692538646941	data	6.63567575561	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x12e000	0x36a4	0x3800	False	0.331473214286	data	3.51322756003	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1163d0	0xd633	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x123a08	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x127c30	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x12a1d8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 41910143		
RT_ICON	0x12b280	0x988	data		
RT_ICON	0x12bc08	0x468	GLS_BINARY_LSB_FIRST		
RT_MENU	0x12d380	0x4	data		
RT_DIALOG	0x12d388	0xf0	data		
RT_DIALOG	0x12d478	0x88	data		
RT_DIALOG	0x12d500	0x12c	data		
RT_STRING	0x12c2b8	0x1e8	data		
RT_STRING	0x12c4a0	0x424	data		
RT_STRING	0x12c8c8	0x43c	data		
RT_STRING	0x12cd08	0x4fc	data		
RT_STRING	0x12d208	0x174	data		
RT_GROUP_ICON	0x12c070	0x5a	data		
RT_VERSION	0x12c0d0	0x1e4	data		

Imports

DLL	Import
KERNEL32.dll	GetProcAddress, GetTapeStatus, Sleep, LocalAlloc, CloseHandle, CreateActCtxW, SetCurrentDirectoryA, LoadLibraryW, GetModuleHandleW, ResetEvent, GetCommandLineW, HeapSetInformation, GetStartupInfoW, SetUnhandledExceptionFilter, QueryPerformanceCounter, GetTickCount, GetCurrentThreadId, GetCurrentProcessId, GetSystemTimeAsFileTime, InterlockedIncrement, InterlockedDecrement, DecodePointer, ExitProcess, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetStdHandle, InitializeCriticalSectionAndSpinCount, GetFileType, DeleteCriticalSection, HeapValidate, IsBadReadPtr, EncodePointer, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, SetLastError, GetLastError, HeapCreate, WriteFile, GetACP, GetOEMCP, GetCPInfo, IsValidCodePage, EnterCriticalSection, LeaveCriticalSection, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, GetModuleFileNameA, HeapReAlloc, HeapSize, HeapQueryInformation, HeapFree, RtlUnwind, WideCharToMultiByte, LCMapStringW, MultiByteToWideChar, GetStringTypeW, OutputDebugStringA, WriteConsoleW, OutputDebugStringW, IsProcessorFeaturePresent, SetFilePointer, GetConsoleCP, GetConsoleMode, RaiseException, SetStdHandle, CreateFileW, FlushFileBuffers
GDI32.dll	StrokePath
ADVAPI32.dll	StartServiceA, CloseEventLog

Version Infos

Description	Data
LegalCopyright	Copyright 2012-2022 by Kone LLC All Rights Reserved.
FileVersion	87.90.67.49
ProductVersion	70.56.51.66

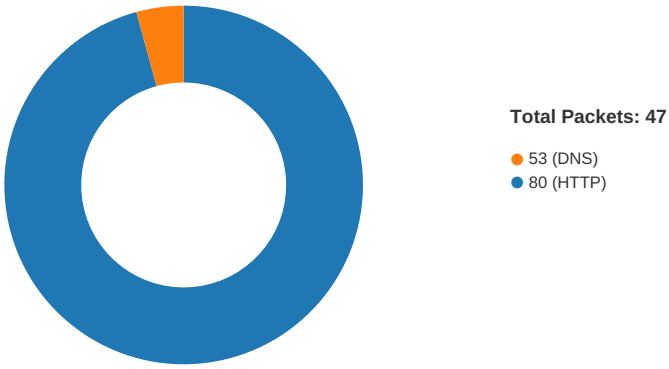
Description	Data
Translation	0x0838 0x03a4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.352.169.118.173497028020332030519/22-14:41:40.292996	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49702	80	192.168.2.3	52.169.118.173
192.168.2.352.169.118.173497028020332040519/22-14:41:40.292996	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49702	80	192.168.2.3	52.169.118.173

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2022 14:41:40.411487103 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.451590061 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.454516888 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.455178022 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.497522116 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.559830904 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.559859991 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.559952974 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.597235918 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.672713995 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.899105072 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.899158001 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.899280071 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.899312973 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.899624109 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.899714947 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.899843931 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.899908066 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.899981022 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.900038958 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.900139093 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.900206089 CEST	49703	80	192.168.2.3	13.107.40.203

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2022 14:41:40.900228977 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.900290966 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.900367022 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.900387049 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.900490999 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.901165009 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.901251078 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.901267052 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.901326895 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.901454926 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.901515961 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.901649952 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.901673079 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.901721001 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.901721954 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.901740074 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.901740074 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.901761055 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.901782990 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.901804924 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.901818991 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.901851892 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.901859999 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.939166069 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.939214945 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.939244032 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.939275980 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.939341068 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.939419985 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.939547062 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.939582109 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.939611912 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.939615011 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.939640045 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.939672947 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.939692020 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.939724922 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.939743042 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.939773083 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.939801931 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.939929962 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.939976931 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.939985037 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.940009117 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.940037966 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.940047026 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.940068960 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.940104961 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.940218925 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.940260887 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.940289974 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.940351009 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.941071033 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941108942 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941138029 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941155910 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.941165924 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941198111 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941199064 CEST	49703	80	192.168.2.3	13.107.40.203

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2022 14:41:40.941226006 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941261053 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.941303968 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.941472054 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941521883 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941545010 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.941579103 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941605091 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.941606998 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941634893 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941634893 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.941664934 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941670895 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.941694975 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941704035 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.941725016 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941730976 CEST	49703	80	192.168.2.3	13.107.40.203
May 19, 2022 14:41:40.941754103 CEST	80	49703	13.107.40.203	192.168.2.3
May 19, 2022 14:41:40.941760063 CEST	49703	80	192.168.2.3	13.107.40.203

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2022 14:41:40.197166920 CEST	51229	53	192.168.2.3	8.8.8.8
May 19, 2022 14:41:40.389507055 CEST	64851	53	192.168.2.3	8.8.8.8
May 19, 2022 14:41:40.408665895 CEST	53	64851	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 19, 2022 14:41:40.197166920 CEST	192.168.2.3	8.8.8.8	0x918e	Standard query (0)	anm.msn.com	A (IP address)	IN (0x0001)
May 19, 2022 14:41:40.389507055 CEST	192.168.2.3	8.8.8.8	0x35a	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 19, 2022 14:41:40.229801893 CEST	8.8.8.8	192.168.2.3	0x918e	No error (0)	anm.msn.com	redirection.prod.cms.msn.com		CNAME (Canonical name)	IN (0x0001)
May 19, 2022 14:41:40.229801893 CEST	8.8.8.8	192.168.2.3	0x918e	No error (0)	redirection.prod.cms.msn.com	redirection.prod.cms.msn.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 19, 2022 14:41:40.408665895 CEST	8.8.8.8	192.168.2.3	0x35a	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 19, 2022 14:41:40.408665895 CEST	8.8.8.8	192.168.2.3	0x35a	No error (0)	www-msn-com.a-0003.a-msedge.net	icePrime.a-0003.dc-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 19, 2022 14:41:40.408665895 CEST	8.8.8.8	192.168.2.3	0x35a	No error (0)	icePrime.a-0003.dc-msedge.net	a-0003.fbs2-a-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 19, 2022 14:41:40.408665895 CEST	8.8.8.8	192.168.2.3	0x35a	No error (0)	a-0003.fbs2-a-msedge.net		13.107.40.203	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.msn.com

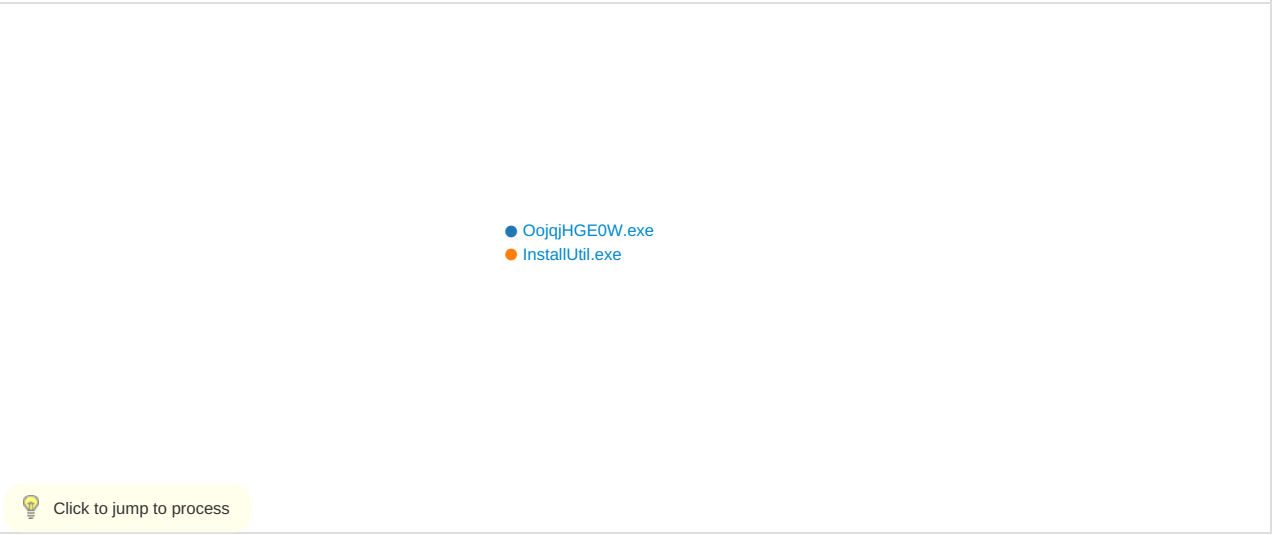
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49703	13.107.40.203	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe

Timestamp	kBytes transferred	Direction	Data
May 19, 2022 14:41:40.455178022 CEST	109	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.msn.com
May 19, 2022 14:41:40.559830904 CEST	110	IN	HTTP/1.1 302 Found Cache-Control: no-cache, no-store, no-transform Pragma: no-cache Content-Length: 142 Content-Type: text/html; charset=utf-8 Expires: -1 Location: http://www.msn.com/de-ch/ Vary: User-Agent Set-Cookie: PreferencesMsn=eyJIb21lUGFnZSI6eyJTdHJpcGVzIjpbXSwiTWVTdHJpcGVNb2R1bGVzIjpbXSwiTWFya2V0Q29uZmlndXJhdGlvbiI6eyJNYXJrZXQiOiJkZS1jaCIsIlN1cHByZXNzUHJvbXB0IjpmYWxzZSwiUHJlZmVycmVkTGFuZ3VhZ2VDb2RlIjoiZGUtZGUiLCJDb3VudHJ5Q29kZSI6IkNIIn19LCJFeHBpcnlUaW1lIjo2MzgyMDA5NjkwMDQ5NzI5NzksIlZlcnNpb24iOjF90; domain=msn.com; expires=Fri, 19-May-2023 12:41:40 GMT; path=/; HttpOnly Set-Cookie: marketPref=de-ch; domain=msn.com; expires=Fri, 19-May-2023 12:41:40 GMT; path=/; HttpOnly Access-Control-Allow-Origin: * X-AspNetMvc-Version: 5.2 X-AppVersion: 20220517_28677693 X-Activity-Id: efab37a0-e368-4926-ad9f-55ad4ca02ec9 X-Az: {did:2be360ae5c6345da911d978376c0449f, rid: 20, sn: neurope-prod-hp, dt: 2022-05-18T22:13:14.6536596Z, bt: 2022-05-17T20:41:53.5606999Z} nel: {"report_to":"network-errors","max_age":604800,"success_fraction":0.001,"failure_fraction":1.0} report-to: {"group":"network-errors","max_age":604800,"endpoints":[{"url":"https://deff.nelreports.net/api/report?cat=msn"}]} X-UA-Compatible: IE=Edge;chrome=1 X-Content-Type-Options: nosniff X-FRAME-OPTIONS: SAMEORIGIN X-Powered-By: ASP.NET Ac Data Raw: Data Ascii:
May 19, 2022 14:41:40.597235918 CEST	111	OUT	GET /de-ch/ HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.msn.com Cookie: PreferencesMsn=eyJIb21lUGFnZSI6eyJTdHJpcGVzIjpbXSwiTWVTdHJpcGVNb2R1bGVzIjpbXSwiTWFya2V0Q29uZmlndXJhdGlvbiI6eyJNYXJrZXQiOiJkZS1jaCIsIlN1cHByZXNzUHJvbXB0IjpmYWxzZSwiUHJlZmVycmVkTGFuZ3VhZ2VDb2RlIjoiZGUtZGUiLCJDb3VudHJ5Q29kZSI6IkNIIn19LCJFeHBpcnlUaW1lIjo2MzgyMDA5NjkwMDQ5NzI5NzksIlZlcnNpb24iOjF90; marketPref=de-ch
May 19, 2022 14:41:40.899105072 CEST	113	IN	HTTP/1.1 200 OK Cache-Control: no-cache, no-store, no-transform Pragma: no-cache Content-Length: 336579 Content-Type: text/html; charset=utf-8 Expires: -1 Vary: User-Agent Set-Cookie: PreferencesMsn=eyJFeHBpcnlUaW1lIjo2MzgyMDA5NjkwMDYzNzkyNDAsIlZlcnNpb24iOjF90; domain=msn.com; expires=Fri, 19-May-2023 12:41:40 GMT; path=/; HttpOnly Access-Control-Allow-Origin: * X-AspNetMvc-Version: 5.2 X-AppVersion: 20220517_28677693 X-Activity-Id: ded43fef-0e10-4ef5-a726-676e283054af X-Az: {did:2be360ae5c6345da911d978376c0449f, rid: 20, sn: neurope-prod-hp, dt: 2022-05-18T22:13:14.6536596Z, bt: 2022-05-17T20:41:53.5606999Z} nel: {"report_to":"network-errors","max_age":604800,"success_fraction":0.001,"failure_fraction":1.0} report-to: {"group":"network-errors","max_age":604800,"endpoints":[{"url":"https://deff.nelreports.net/api/report?cat=msn"}]} X-UA-Compatible: IE=Edge;chrome=1 X-Content-Type-Options: nosniff X-FRAME-OPTIONS: SAMEORIGIN X-Powered-By: ASP.NET Access-Control-Allow-Methods: HEAD,GET,OPTIONS X-XSS-Protection: 1 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: DED43FEF0E104EF5A726676E283054AF Ref B: HEL01EDGE1020 Ref C: 2022-05-19T12:41:40Z Date: Thu, 19 May 2022 12:41:40 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 20 66 62 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 2f 66 62 23 22 20 20 6c 61 6e 67 3d 22 64 65 2d 43 48 22 20 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 22 20 20 63 6c 61 73 Data Ascii: <!DOCTYPE html><html prefix="og: http://ogp.me/ns# fb: http://ogp.me/ns/fb#" lang="de-CH" style="font-size:62.5%" clas

Statistics

Behavior



System Behavior

Analysis Process: OojqjHGE0W.exe PID: 3408, Parent PID: 5100

General

Target ID:	0
Start time:	14:39:49
Start date:	19/05/2022
Path:	C:\Users\user\Desktop\OojqjHGE0W.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\OojqjHGE0W.exe"
Imagebase:	0xb20000
File size:	1241656 bytes
MD5 hash:	4ED3FA33609A51BAF209A5954BEF6633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: InstallUtil.exe PID: 5584, Parent PID: 3408

General

Target ID:	10
Start time:	14:41:25
Start date:	19/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0xd80000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3

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: 0000000A.00000003.504942023.00000000020C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000A.00000003.501961576.00000000020C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000A.00000003.502032730.00000000020C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000A.00000002.535140555.00000000020C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000A.00000003.501571456.00000000020C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000A.00000003.501753987.00000000020C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000000A.00000002.535054926.0000000001B69000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000A.00000003.501977722.00000000020C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000A.00000003.501825234.00000000020C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000A.00000003.501701977.00000000020C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000A.00000003.501914236.00000000020C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
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