ID: 778240
Sample Name: Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe
Cookbook: default.jbs
Time: 09:21:10
Date: 05/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

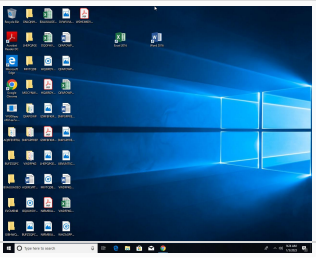
Windows Analysis Report

Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe

Overview

General Information

Sample Name:	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe
Analysis ID:	778240
MD5:	a07407fce93759..
SHA1:	6fc304eb385619..
SHA256:	770a25e30c2f09..
Tags:	exe
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

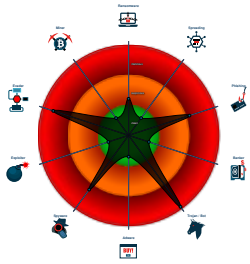
Remcos, AveMaria

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

Signatures

- Sigma detected: Remcos
- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Remcos RAT
- Yara detected AveMaria stealer
- Multi AV Scanner detection for dom…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Yara detected Costura Assembly Lo…
- Encrypted powershell cmdline option…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe (PID: 3988 cmdline: C:\Users\user\Desktop\Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe MD5: A07407FCE937593044AD512F4A6D7A1E)
  - powershell.exe (PID: 3420 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - aspnet_compiler.exe (PID: 3660 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 732 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\jzlrsem" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 4884 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\jzlrsem" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 5236 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\ubrkswxpfz" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 5812 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\evectoiqthdfs" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - dwn.exe (PID: 2088 cmdline: "C:\Users\user\AppData\Local\Temp\dwn.exe" MD5: 0E4816AC89A716B262402CD1791400DF)
    - aspnet_compiler.exe (PID: 4892 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\ixjslbemgsufoiuudk" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 1552 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\tzolmupfuamrqwiynvqal" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 3324 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\tzolmupfuamrqwiynvqal" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 4740 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 4116 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 4988 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 4964 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 3776 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 4972 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 5716 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\xbsbmhljhlcrmkvfybyknsbrlg" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 5828 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\ivyunzdcvtueoyrjhmkmqwoatvkpua" MD5: 17CC69238395DF61AAF483BCEF02E7C9)

- aspnet_compiler.exe (PID: 5764 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\sxd nnkoerbmjyegnzxxfbjirubcqnlslo" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- aspnet_compiler.exe (PID: 5868 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\sxd nnkoerbmjyegnzxxfbjirubcqnlslo" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- aspnet_compiler.exe (PID: 6092 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\xzhdfxk" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- aspnet_compiler.exe (PID: 6088 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\huv vgpvbsu" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- aspnet_compiler.exe (PID: 3020 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\jwa ohifvgcnaz" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- aspnet_compiler.exe (PID: 5936 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\jwa ohifvgcnaz" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- aspnet_compiler.exe (PID: 3460 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\bbm bgkgdsftq" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- aspnet_compiler.exe (PID: 4952 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\mvr mgcrxgnlvkuc" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- aspnet_compiler.exe (PID: 5348 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\wye ehvbyuvdiuiytom" MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- aspnet_compiler.exe (PID: 5312 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\odq rgxczfqkyvjblz" MD5: 17CC69238395DF61AAF483BCEF02E7C9)

- Shhejayly.exe (PID: 4420 cmdline: "C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe" MD5: A07407FCE937593044AD512F4A6D7A1E)
- Shhejayly.exe (PID: 5608 cmdline: "C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe" MD5: A07407FCE937593044AD512F4A6D7A1E)
- **cleanup**

Malware Configuration

Threatname: Remcos


```
{
  "Host:Port:Password": "obologs.work.gd:4044:1",
  "Assigned name": "RemoteHost",
  "Copy file": "remcos.exe",
  "Startup value": "Remcos",
  "Mutex": "Rmc-E9KXT7",
  "Keylog file": "logs.dat",
  "Screenshot file": "Screenshots",
  "Audio folder": "MicRecords",
  "Copy folder": "Remcos",
  "Keylog folder": "remcos",
  "Keylog file max size": "100000"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.543466399.0000000003093000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0000000C.00000000.351505282.0000000000456000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
0000000C.00000000.351505282.0000000000456000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Remcos_b296e965	unknown	unknown	• 0x13230:$a1: Remcos restarted by watchdog! • 0x13798:$a3: %02i:%02i:%02i:%03i
0000001C.00000002.542998195.0000000002653000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000000.00000002.365213489.0000000007610000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
Click to see the 32 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe.37c86a0.5.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Source	Rule	Description	Author	Strings
0.2.Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe.37c86a0.5.unpack	INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer	detects Windows exceutables potentially bypassing UAC using eventvwr.exe	ditekSHen	• 0x60918:$s1: \Classes\mscfile\shell\open\command • 0x60978:$s1: \Classes\mscfile\shell\open\command • 0x60960:$s2: eventvwr.exe
0.2.Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe.37c86a0.5.unpack	Windows_Trojan_Remcos_b296e965	unknown	unknown	• 0x66a30:$a1: Remcos restarted by watchdog! • 0x66f98:$a3: %02i:%02i:%02i:%03i
0.2.Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe.37c86a0.5.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x61a34:$str_a1: C:\Windows\System32\cmd.exe • 0x619b0:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x619b0:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x60e28:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x61698:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x60a24:$str_b2: Executing file: • 0x61b78:$str_b3: GetDirectListeningPort • 0x61460:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x6167c:$str_b7: \update.vbs • 0x60a4c:$str_b9: Downloaded file: • 0x60a38:$str_b10: Downloading file: • 0x60adc:$str_b12: Failed to upload file: • 0x61b40:$str_b13: StartForward • 0x61b60:$str_b14: StopForward • 0x61624:$str_b15: fso.DeleteFile " • 0x61654:$str_b17: fso.DeleteFolder " • 0x60acc:$str_b18: Uploaded file: • 0x60a8c:$str_b19: Unable to delete: • 0x615ec:$str_b20: while fso.FileExists(" • 0x60f61:$str_c0: [Firefox StoredLogins not found] • 0x60970:$str_c1: Software\Classes\mscfile\shell\open\command
28.2.Shhejayly.exe.36c99b0.3.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
Click to see the 48 entries				

Sigma Signatures

Stealing of Sensitive Information

Sigma detected: Remcos

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Yara detected AveMaria stealer

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

May check the online IP address of the machine

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Remcos RAT

Yara detected AveMaria stealer

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected Costura Assembly Loader

.NET source code contains potential unpacker

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected Remcos RAT

Yara detected AveMaria stealer

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

Yara detected WebBrowserPassView password recovery tool

Tries to steal Instant Messenger accounts or passwords

Remote Access Functionality

Yara detected Remcos RAT

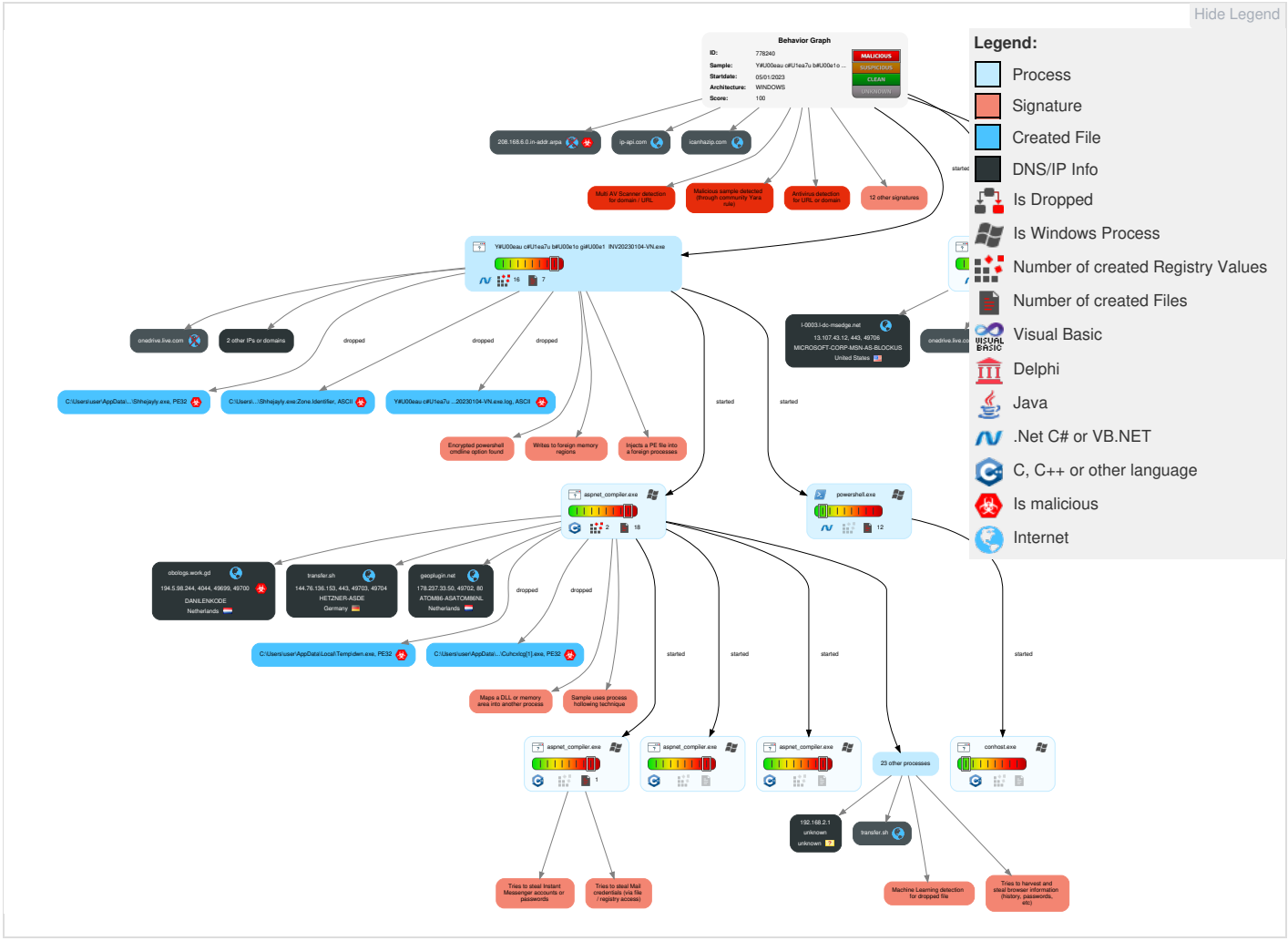
Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 Registry Run Keys / Startup Folder	4 1 2 Process Injection	1 Disable or Modify Tools	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 1 Deobfuscate/Decode Files or Information	1 Input Capture	2 File and Directory Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 PowerShell	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	1 Credentials in Registry	2 8 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Software Packing	1 Credentials In Files	3 1 Security Software Discovery	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	2 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	1 1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	4 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	4 1 2 Process Injection	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Network Configuration Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

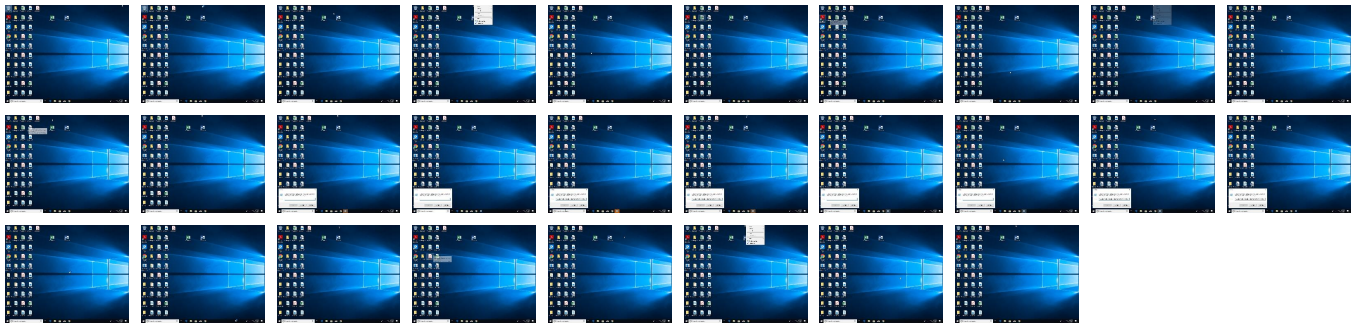
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe	28%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe	31%	Virustotal		Browse
Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\dwn.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Cuhcxlcg[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.2.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.0.aspnet_compiler.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1244765		Download File
14.2.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
15.2.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.0.aspnet_compiler.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
l-0003.l-dc-msedge.net	0%	Virustotal		Browse
geoplugin.net	0%	Virustotal		Browse
obologs.work.gd	14%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.imvu.comr	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://geoplugin.net/json.gp/C	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0#	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.nirsoft.net-ms-win-core-delayload-l1-1-0.dll.dlldll	0%	URL Reputation	safe	
http://https://aefd.nelreports.net/api/report?cat=bingth	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://kpf0yw.am.files.1drv.com45kT	0%	Avira URL Cloud	safe	
obologs.work.gd	100%	Avira URL Cloud	phishing	
http://crl.globals	0%	Avira URL Cloud	safe	
http://www.nirsoft.net-ms-win-core-delayload-l1-1-0.dll.dlldllD	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
l-0003.l-dc-msedge.net	13.107.43.12	true	false	• 0%, Virustotal, Browse	unknown
geoplugin.net	178.237.33.50	true	false	• 0%, Virustotal, Browse	unknown
ip-api.com	208.95.112.1	true	false		high
obologs.work.gd	194.5.98.244	true	true	• 14%, Virustotal, Browse	unknown
transfer.sh	144.76.136.153	true	false		high
icanhazip.com	104.18.114.97	true	false		high
kpf0yw.am.files.1drv.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high
208.168.6.0.in-addr.arpa	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
obologs.work.gd	true	• Avira URL Cloud: phishing	unknown
http://https://transfer.sh/get/J59PTO/Cuhcxlcg.exe	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTrustV2/scripttemplate	bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/static/images/folder-applications.svg	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://www.imvu.comr	aspnet_compiler.exe, 00000010.00000002.374522754.0000000000400000.00000040.80000000.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com/chrome/static/css/main.v2.min.css	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://crl.microsoft	aspnet_compiler.exe, 0000000C.00000003.477736669.0000000004001000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com/chrome/static/images/fallback/google-chrome-logo.jpg	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://www.msn.com	bhv8995.tmp.39.dr	false		high
http://www.fontbureau.com/designers	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.361191656.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.nirsoft.net	aspnet_compiler.exe, 0000000E.00000002.397869869.00000000008F4000.00000004.00000010.00020000.00000000.sdmp, aspnet_compiler.exe, 00000021.00000002.477360003.0000000000FB4000.00000004.00000010.00020000.00000000.sdmp, aspnet_compiler.exe, 00000027.00000002.502161495.00000000008F4000.00000004.00000010.00020000.00000000.sdmp, aspnet_compiler.exe, 0000002A.00000002.513031021.00000000001B3000.00000004.00000010.00020000.00000000.sdmp	false		high
http://https://deff.nelreports.net/api/report?cat=msn	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false	• URL Reputation: safe	unknown
http://https://www.google.com/chrome/static/images/chrome-logo.svg	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/static/images/homepage/homepage_features.png	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://adservice.google.com/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=6856811916691;gtm=	aspnet_compiler.exe, 0000000E.00000003.386957585.0000000002743000.00000004.00000800.00020000.00000000.sdmp, bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/static/images/download-browser/big_pixel_phone.png	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://www.sajatypeworks.com	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.361191656.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com/chrome/	bhv8995.tmp.39.dr	false		high
http://https://www.google.com	aspnet_compiler.exe, 00000010.00000002.374522754.0000000000400000.00000040.80000000.00040000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.361191656.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCc13122162a9a46c3b4cbf05ffccde0f	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr	false		high
http://https://www.google.com/chrome/static/images/homepage/hero-anim-bottom-left.png	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/chrome/static/images/chrome_safari-behavior.jpg	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://geoplugin.net/json.gp/C	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe, 00000000.00000002.35849 3957.00000000037C8000.00000004.00000800. 00020000.00000000.sdmp, Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe, 00000000.00000002.357530014.00000000036 B0000.00000004.00000800.00020000.0000000 0.sdmp, Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe, 00000000.00000002.3573192 62.0000000003630000.00000004.00000800.00 020000.00000000.sdmp, Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe, 0 0000000.00000002.355401113.00000000025D4 000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 0000000C.00000000.35150 5282.0000000000456000.00000040.00000400. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://maps.windows.com/windows-app-web-link	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr	false		high
http://www.msn.com/?ocid=iehp	aspnet_compiler.exe, 0000000E.00000003.3 88842971.0000000002746000.00000004.00000 800.00020000.00000000.sdmp, aspnet_compiler.exe, 0000000E.00000003.386957585.0000000002743 000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000013.00000003.40178 0181.0000000002A83000.00000004.00000800. 00020000.00000000.sdmp, aspnet_compiler.exe, 00000013.00000003.405195939.0000000002A86000. 00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 0000001D.00000003 .436504638.00000000028D6000.00000004.000 00800.00020000.00000000.sdmp, aspnet_com piler.exe, 0000001D.00000003.433788536.0 0000000028D3000.00000004.00000800.000200 00.00000000.sdmp, aspnet_compiler.exe, 0 0000021.00000003.463221264.0000000003003 000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000021.00000003.46671 4622.0000000003006000.00000004.00000800. 00020000.00000000.sdmp, aspnet_compiler.exe, 00000027.00000003.487705843.00000000028A6000. 00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000027.00000003.481529759 .00000000028A3000.00000004.00000800.0002 0000.00000000.sdmp, aspnet_compiler.exe, 0000002A.00000003.504317340.0000000000A 46000.00000004.00000800.00020000.0000000 0.sdmp, aspnet_compiler.exe, 0000002A.00 000003.500729020.0000000000A43000.000000 04.00000800.00020000.00000000.sdmp, bhv6 10E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=68568119166	aspnet_compiler.exe, 0000000E.00000003.3 86957585.0000000002743000.00000004.00000 800.00020000.00000000.sdmp, bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCee0d4d5fd4424c8390d703b105f82c3	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr	false		high
http://https://srtb.msn.com/auction?a=de-ch&b=a8415ac9f9644a1396bc1648a4599445&c=MSN&d=http%3A%2F%2Fwww.msn	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://crl.pki.goog/GTS1O1core.crl0	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe, 00000000.00000002.36019 1656.00000000065F2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com/chrome/static/images/icon-announcement.svg	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high

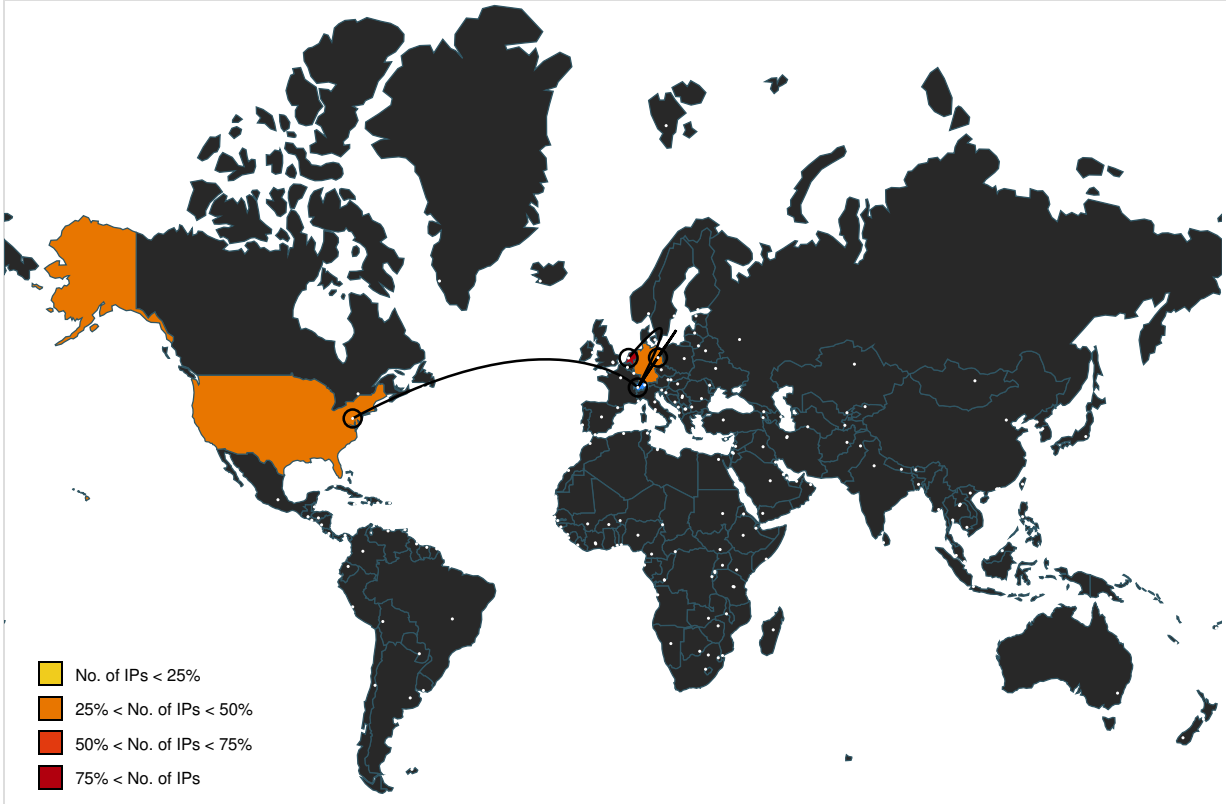
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1https://c	aspnet_compiler.exe, 0000000E.00000003.389075530.0000000002D72000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 0000000E.00000003.386841625.000000000274F000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000013.00000003.401748327.0000000002A96000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 0000001D.00000003.433671270.00000000028E6000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000021.00000003.463192812.0000000003016000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 00000027.00000003.481477826.00000000028B6000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 0000002A.00000003.500671413.0000000000A56000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.urwpp.deDPlease	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.361961656.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.nirsoft.net/	aspnet_compiler.exe, 00000010.00000002.374522754.0000000000400000.00000040.80000000.00040000.00000000.sdmp	false		high
http://www.zhongyicts.com.cn	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.361961656.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.354759645.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, dwn.exe, 00000011.00000002.538650865.0000000002F81000.00000004.00000800.00020000.00000000.sdmp, Shhejayly.exe, 00000012.00000002.537970433.000000000250C000.00000004.00000800.00020000.00000000.sdmp, Shhejayly.exe, 00000001C.00000002.537475545.00000000024E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/chrome/static/images/homepage/hero-anim-middle.png	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://crl.globals	aspnet_compiler.exe, 0000000C.00000003.360263482.0000000003E57000.00000004.00000800.00020000.00000000.sdmp, aspnet_compiler.exe, 0000000C.00000003.357358743.0000000003E51000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/chrome/static/css/main.v3.min.css	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/application/x-msdownloadC:	bhvF833.tmp.14.dr	false		high
http://https://www.google.com/chrome/static/images/fallback/icon-file-download.jpg	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://www.imvu.com/	aspnet_compiler.exe, 00000010.00000002.374830340.00000000009EA000.00000004.00000010.00020000.00000000.sdmp, aspnet_compiler.exe, 0000001B.00000002.392736661.0000000000CF9000.00000004.00000010.00020000.00000000.sdmp, aspnet_compiler.exe, 00000020.00000002.416712597.0000000000CF9000.00000004.00000010.00020000.00000000.sdmp, aspnet_compiler.exe, 00000024.00000002.432581722.0000000000EFA000.00000004.00000010.00020000.00000000.sdmp	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC5bdddb231cf54f958a5b6e76e9d8eee	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr	false		high
http://www.imvu.com	aspnet_compiler.exe, 00000010.00000002.374522754.0000000000400000.00000040.80000000.00040000.00000000.sdmp	false		high
http://https://www.google.com/chrome/static/images/download-browser/pixel_phone.png	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://pki.goog/gsr2/GTS1O1.crt0	bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false	• URL Reputation: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1	bhv8995.tmp.39.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://kpf0yw.am.files.1drv.com45kT	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.35512 6935.000000000253C000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com/download?cid=B044AF3D48F7B886&resid=B044AF3D48F7B886	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.35475 9645.00000000024F1000.00000004.00000800. 00020000.00000000.sdmp, Shhejayly.exe, 0 0000012.00000002.537970433.000000000250C 000.00000004.00000800.00020000.00000000.sdmp, Shhejayly.exe, 0000001C.00000002.537475545.0 0000000024E1000.00000004.00000800.000200 00.00000000.sdmp	false		high
http://https://www.google.com/chrome/static/images/app-store-download.png	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://kpf0yw.am.files.1drv.com/y4mDTH7qGldoE19yex0JjOdCD7abQr3OT41x7HoVD-gSuwIqkSH1AKWWpBjmzkRc7T3	Shhejayly.exe, 00000012.00000002.5390809 76.000000000254C000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://transfer.sh/get/3GTNpY/Rtbdyyicls.bmp%Pvdrkkndtbbqxgmhnq	dwn.exe, 00000011.00000000.374284805.000 0000000AE2000.00000002.00000001.01000000 .00000009.sdmp, dwn.exe.12.dr, Cuhcxlcg[1].exe.12. dr	false		high
http://https://www.google.com/chrome/static/images/homepage/hero-anim-top-right.png	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr	false		high
http://https://contextual.media.net/	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://pki.goog/repository/0	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false	• URL Reputation: safe	unknown
http://https://cvision.media.net/new/300x300/3/167/174/27/39ab3103-8560-4a55-bfc4-401f897cf6f2.jpg?v=9	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr	false		high
http://www.carterandcone.coml	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.36019 1656.00000000065F2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.msn.com/	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC828bc1cde9f04b788c98b5423157734	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr	false		high
http://www.fontbureau.com/designers/frere-jones.html	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.36019 1656.00000000065F2000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=1463674	bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/static/images/fallback/google-logo-one-color.jpg	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/static/images/fallback/icon-twitter.jpg	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.newtonsoft.com/jsonschema	Shhejayly.exe, 0000001C.00000002.5469332 51.0000000003573000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTrustV2/consent/55a804	bhv8995.tmp.39.dr	false		high
http://https://contextual.media.net/803288796/fcmain.js?&gdpr=0&cid=8CU157172&cpcd=pC3JHgSCqY8UHihgrvGr0A%3	bhv8995.tmp.39.dr	false		high
http://https://contextual.media.net/48/nrrV18753.js	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/static/images/fallback/icon-help.jpg	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.google.com/accounts/servicelogin	aspnet_compiler.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/chrome/static/images/homepage/google-enterprise.png	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/static/images/homepage/google-dev.png	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/static/images/thank-you/thankyou-animation.json	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://crl.pki.goog/gsr2/gsr2.crl0?	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false	• URL Reputation: safe	unknown
http://pki.goog/gsr2/GTSGIAG3.crt0)	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false	• URL Reputation: safe	unknown
http://https://www.google.com/	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/static/images/fallback/icon-fb.jpg	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/static/images/mac-ico.png	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://www.fontbureau.com/designersG	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.36019 1656.00000000065F2000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://pki.goog/gsr2/GTS1O1.crt0#	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.36019 1656.00000000065F2000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.36019 1656.00000000065F2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.nirsoft.net-ms-win-core-delayload-l1-1-0.dll.dlldll	aspnet_compiler.exe, 0000001D.00000002.4 52238930.0000000000AF4000.00000004.00000 010.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.36019 1656.00000000065F2000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://https://aefd.nelreports.net/api/report?cat=bingth	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/download?cid=B044AF3D48F7B886&resid=B044AF3D48F7B886%21122&authkey=AKVhH87	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe	false		high
http://www.nirsoft.net-ms-win-core-delayload-l1-1-0.dll.dlldllD	aspnet_compiler.exe, 00000013.00000002.4 20022464.0000000000AF4000.00000004.00000 010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/chrome/static/images/google-play-download.png	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr	false		high
http://https://www.google.com/chrome/static/images/chrome_throbber_fast.gif	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/static/images/homepage/google-canary.png	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/static/images/favicons/favicon-16x16.png	bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp.19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://www.tiro.com	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.36019 1656.00000000065F2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.newtonsoft.com/json	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.35622 5018.00000000034F1000.00000004.00000800. 00020000.00000000.sdmp, Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe, 00000000.00000002.374159266.00000000078 00000.00000004.08000000.00040000.0000000 0.sdmp, dwn.exe, 00000011.00000002.55043 9379.00000000040A1000.00000004.00000800. 00020000.00000000.sdmp, dwn.exe, 0000001 1.00000002.548404378.0000000003FFF000.00 000004.00000800.00020000.00000000.sdmp, dwn.exe, 00000011.00000002.543947218.000 00000030C8000.00000004.00000800.00020000 .00000000.sdmp, Shhejayly.exe, 00000012. 00000002.546978797.0000000003596000.0000 0004.00000800.00020000.00000000.sdmp, Sh hejayly.exe, 00000012.00000002.539326956 .00000000025A6000.00000004.00000800.0002 0000.00000000.sdmp, Shhejayly.exe, 00000 01C.00000002.538968887.0000000002586000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV 20230104-VN.exe, 00000000.00000002.36019 1656.00000000065F2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.imvu.com/B	aspnet_compiler.exe, 00000029.00000002.4 53919934.000000000135A000.00000004.00000 010.00020000.00000000.sdmp	false		high
http://https://assets.adobedtm.com/launch-EN7b3d710ac67a4a1195648458258f97dd.min.js	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp. 19.dr, bhvF833.tmp.14.dr	false		high
http://https://www.google.com/chrome/static/images/homepage/laptop_desktop.png	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp. 19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high
http://https://www.google.com/chrome/static/js/main.v2.min.js	bhv610E.tmp.33.dr, bhv9EB4.tmp.42.dr, bhv107D.tmp. 19.dr, bhvF833.tmp.14.dr, bhv8995.tmp.39.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.107.43.12	l-0003.l-dc-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
194.5.98.244	obologs.work.gd	Netherlands		208476	DANILENKODE	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
178.237.33.50	geoplugin.net	Netherlands		8455	ATOM86-ASATOM86NL	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	778240
Start date and time:	2023-01-05 09:21:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	43
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.phis.troj.spyw.evad.winEXE@65/22@19/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 89%) • Quality average: 75.3% • Quality standard deviation: 33.6%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.42.13, 13.107.42.12
- Excluded domains from analysis (whitelisted): www.bing.com, l-0004.l-msedge.net, odc-web-brs.onedrive.akadns.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, fs.microsoft.com, l-0003.l-msedge.net, odc-web-geo.onedrive.akadns.net, odc-am-files-geo.onedrive.akadns.net, ctldl.windowsupdate.com, am-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, odc-am-files-brs.onedrive.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:22:30	API Interceptor	44x Sleep call for process: powershell.exe modified
09:22:53	API Interceptor	1x Sleep call for process: Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe modified
09:22:56	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Shhejayly "C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe"
09:23:05	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Shhejayly "C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe.log

Process:	C:\Users\user\Desktop\Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1537
Entropy (8bit):	5.3478589519339295
Encrypted:	false
SSDEEP:	48:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHLHKdHKBqHKs:Pq5qXEwCYqhQnoPtIxHeqzNrqdq4qs
MD5:	F6D3657BD1FBEF54E7F7BACB2497E327
SHA1:	A0A712015C242DCC28B69CDF567F594627C9CFA0
SHA-256:	5B16B4A3E65F04484B12171163A2A739409FA7F8C3D69BF9BAD961618D973301
SHA-512:	0231195A111259A3AA48526DCBEA98394099794C710C3FB8E0E12E2B4D30C60FB4064F7F4F671866FB0D94585E23B73C1270440242B25DA60CCFFA82B0B74306
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Cuhcxlcg[1].exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

Category:	dropped
Size (bytes):	8704
Entropy (8bit):	4.76941550076102
Encrypted:	false
SSDEEP:	96:JaqDtNDC8SkkDnmWErVC7jQ9kL4VFRdz95LmGLlQiAY6RtQWRkZ4HhngzNt:JLj1DKiog9kL4VFf95lLDAY6HYiHRi
MD5:	0E4816AC89A716B262402CD1791400DF
SHA1:	A9F39BD3330B1F70535C716B51E55442E930B164
SHA-256:	BEA1C74AD8FCB8C06967F98F93275784F5DF8266FF9E6AB06273AE48AFED0F8A
SHA-512:	00080A26CD21CD690DCCA18461E7AE2FA10DA6231EE05CFDFF59F580F0B8AA056AD3A502D98364272B2B7AFB0365A04F188569823772719D0366605EAA125767
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.. .....0.....Z6... ...@....@.. ....`.....6..O....@..I.....`.....5..... ....H.....text...`.... ..... ..`.rsrc...I....@.....@..@.rel oc.....`..... .....@..B.....<6.....H.....l%.....45.....N.(.....(.....(....*..{....r...po.....{....(....o....*..{....(.....{....o....t....o....o....*....0..>..... {....o....t....o.....o.....{....o....."...%.. .o.....(....,*.{.....{....o....t....o.....o....o....*.{....o....t....o.....o....{....o....."...%.. .o.....(....,*.{....{....o....t....o.....o....o....*.{....o....t....o.....o..... {....o....."...%.. .o.....(....,).{.....{....o....t....o.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\json[1].json

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	944
Entropy (8bit):	4.989952581991176
Encrypted:	false
SSDEEP:	12:tklAGnd6CsGkMyGWKyMPVGADxapaiH8GdAPORkoao9W7im51w7j9eF6xIjSat5R9:qlPdRNuKyM85266m7p9xZ2
MD5:	BA32BC32E2332E7BCB3DFD042796DE94
SHA1:	997D44FBAA2577575546C0BC4902F06A56335845
SHA-256:	D6FB58DF012C120449C1D849E057C5862992784185D3329B84E27EBBADCDAB77
SHA-512:	A0C8239F0ECF95E76EECDD7073E5B1D86FB264F265722A28EFE61917E346A0D88A0B2C335651B589A9715DF3DFE20038F0F9FF11FCE02588228950B0BCCA01C A
Malicious:	false
Preview:	{. "geoplugin_request":"84.17.52.8",. "geoplugin_status":200,. "geoplugin_delay":"1ms",. "geoplugin_credit":"Some of the returned data includes GeoLite data created b y MaxMind, available from <a href='http:\/\/www.maxmind.com'>http:\/\/www.maxmind.com<\/a>.",. "geoplugin_city":"Zurich",. "geoplugin_region":"Zurich",. "geo plugin_regionCode":"ZH",. "geoplugin_regionName":"Zurich",. "geoplugin_areaCode":"",. "geoplugin_dmaCode":"",. "geoplugin_countryCode":"CH",. "geoplugin_co untryName":"Switzerland",. "geoplugin_inEU":0,. "geoplugin_euVATrate":false,. "geoplugin_continentCode":"EU",. "geoplugin_continentName":"Europe",. "geoplu gin_latitude":"47.43",. "geoplugin_longitude":"8.5718",. "geoplugin_locationAccuracyRadius":"1000",. "geoplugin_timezone":"Europe\/Zurich",. "geoplugin_curr encyCode":"CHF",. "geoplugin_currencySymbol":"CHF",. "geoplugin_currencySymbol_UTF8":"CHF",. "geoplugin_currencyConverter":0.9304.}

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	4.8968676994158
Encrypted:	false
SSDEEP:	96:WCJ2Woe5o2k6Lm5emmXIGvgyg12jDs+un/iQLEYFjDaeWJ6KGcmXx9smyFRLcU6f:5xoe5oVsm5emd0gkjDt4iWN3yBGHh9s6
MD5:	36DE9155D6C265A1DE62A448F3B5B66E
SHA1:	02D21946CBDD01860A0DE38D7EEC6CDE3A964FC3
SHA-256:	8BA38D55AA8F1E4F959E7223FDF653ABB9BE5B8B5DE9D116604E1ABB371C1C87
SHA-512:	C734ADE161FB89472B1DF9B9F062F4A53E7010D3FF99EDC0BD564540A56BC35743625C50A00635C31D165A74DCDBB330FFB878C5919D7B267F6F33D2AAB328E 7
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\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-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	16496

Entropy (8bit):	5.549691958573251
Encrypted:	false
SSDEEP:	384:Kte/V023nVVUzJEbZCwSBxn2iliJ9giSJ3uzp1UYv:lJEb4w4xjJicudv
MD5:	7388D2AA1EE8C223A479A5CF15F7F24C
SHA1:	01B9F9BD7E7A36F322B05EB3B2BC534AAB78CF58
SHA-256:	40927EE2BB65CDF955322719659E777215C1ADCD5C09E2C8F4C225F29F922EBF
SHA-512:	C5119947193108F510C16492D7B3947A88C27AC75070E5A9F094F157D77E59ECFD6C035C9BDF33D0D80528D3593981446C5C1C26E28469C9738F06144B8F10DE
Malicious:	false
Preview:	@...e.....1...7.,.....@.....H.....<@.^.L."My...:)..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dgi0vwrh.uo4.ps1

Process:	C:\Windows\SysWOW64\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 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eq3xehn2.mjn.psm1

Process:	C:\Windows\SysWOW64\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 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\bbmbgkgdsftq

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	Unicode text, UTF-16, little-endian text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false

Preview:	..

C:\Users\user\AppData\Local\Temp\bhv107D.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x7cd0aa12, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.9501694666317948
Encrypted:	false
SSDEEP:	24576:ZvlcTaxxujQxeJ2lLadAZf7+yVHgZFDb7uBi:RiQxeJCac1
MD5:	211037333A188A888F259473595602F7
SHA1:	C01516099073F36351F64A61CCD120169F37AA0F
SHA-256:	EDCCF5C14BC7577F22DA18972342470F9A6BBE1AA44CE51216B3027F7CFEF65F
SHA-512:	388077841AC30BCBBEBAE034C2D2502FBA7C9EEA7E11698DA10916AFF3DB130761A5E0C3E112CAC6FD79E406FB599C6433652D5819549794AFF4E379159F9E8 1
Malicious:	false
Preview:	|..... .....t;.....te3....wg.....C.....,&...z../&...z{.h.E.....6..43....wl.....\.....B..... ....3....z..... .....<.....{.(.....L.....{O..... .....

C:\Users\user\AppData\Local\Temp\bhv424B.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x7cd0aa12, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.9501694666317948
Encrypted:	false
SSDEEP:	24576:ZvlcTaxxujQxeJ2lLadAZf7+yVHgZFDb7uBi:RiQxeJCac1
MD5:	211037333A188A888F259473595602F7
SHA1:	C01516099073F36351F64A61CCD120169F37AA0F
SHA-256:	EDCCF5C14BC7577F22DA18972342470F9A6BBE1AA44CE51216B3027F7CFEF65F
SHA-512:	388077841AC30BCBBEBAE034C2D2502FBA7C9EEA7E11698DA10916AFF3DB130761A5E0C3E112CAC6FD79E406FB599C6433652D5819549794AFF4E379159F9E8 1
Malicious:	false
Preview:	|..... .....t;.....te3....wg.....C.....,&...z../&...z{.h.E.....6..43....wl.....\.....B..... ....3....z..... .....<.....{.(.....L.....{O..... .....

C:\Users\user\AppData\Local\Temp\bhv610E.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x7cd0aa12, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.9501694666317948
Encrypted:	false
SSDEEP:	24576:ZvlcTaxxujQxeJ2lLadAZf7+yVHgZFDb7uBi:RiQxeJCac1
MD5:	211037333A188A888F259473595602F7
SHA1:	C01516099073F36351F64A61CCD120169F37AA0F
SHA-256:	EDCCF5C14BC7577F22DA18972342470F9A6BBE1AA44CE51216B3027F7CFEF65F
SHA-512:	388077841AC30BCBBEBAE034C2D2502FBA7C9EEA7E11698DA10916AFF3DB130761A5E0C3E112CAC6FD79E406FB599C6433652D5819549794AFF4E379159F9E8 1
Malicious:	false
Preview:	|..... .....t;.....te3....wg.....C.....,&...z../&...z{.h.E.....6..43....wl.....\.....B..... ....3....z..... .....<.....{.(.....L.....{O..... .....

C:\Users\user\AppData\Local\Temp\bhv8995.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x7cd0aa12, page size 32768, DirtyShutdown, Windows version 10.0

Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.9501694666317948
Encrypted:	false
SSDEEP:	24576:ZvlcTaxxujQxeJ2lLadAZf7+yVHgZFDb7uBi:RiQxeJCac1
MD5:	211037333A188A888F259473595602F7
SHA1:	C01516099073F36351F64A61CCD120169F37AA0F
SHA-256:	EDCCF5C14BC7577F22DA18972342470F9A6BBE1AA44CE51216B3027F7CFEF65F
SHA-512:	388077841AC30BCBBEBAE034C2D2502FBA7C9EEA7E11698DA10916AFF3DB130761A5E0C3E112CAC6FD79E406FB599C6433652D5819549794AFF4E379159F9E8 1
Malicious:	false
Preview:	|.... .....t;.....te3....wg.....C.....,&...z../&...z{.h.E.....6..43....wl.....\.....B..... ....3....z..... .....<.....{.(.....L.....{O..... .....

C:\Users\user\AppData\Local\Temp\bhv9EB4.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x7cd0aa12, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.9501694666317948
Encrypted:	false
SSDEEP:	
MD5:	211037333A188A888F259473595602F7
SHA1:	C01516099073F36351F64A61CCD120169F37AA0F
SHA-256:	EDCCF5C14BC7577F22DA18972342470F9A6BBE1AA44CE51216B3027F7CFEF65F
SHA-512:	388077841AC30BCBBEBAE034C2D2502FBA7C9EEA7E11698DA10916AFF3DB130761A5E0C3E112CAC6FD79E406FB599C6433652D5819549794AFF4E379159F9E8 1
Malicious:	false
Preview:	|.... .....t;.....te3....wg.....C.....,&...z../&...z{.h.E.....6..43....wl.....\.....B..... ....3....z..... .....<.....{.(.....L.....{O..... .....

C:\Users\user\AppData\Local\Temp\bhvF833.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x7cd0aa12, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.9501694666317948
Encrypted:	false
SSDEEP:	
MD5:	211037333A188A888F259473595602F7
SHA1:	C01516099073F36351F64A61CCD120169F37AA0F
SHA-256:	EDCCF5C14BC7577F22DA18972342470F9A6BBE1AA44CE51216B3027F7CFEF65F
SHA-512:	388077841AC30BCBBEBAE034C2D2502FBA7C9EEA7E11698DA10916AFF3DB130761A5E0C3E112CAC6FD79E406FB599C6433652D5819549794AFF4E379159F9E8 1
Malicious:	false
Preview:	|.... .....t;.....te3....wg.....C.....,&...z../&...z{.h.E.....6..43....wl.....\.....B..... ....3....z..... .....<.....{.(.....L.....{O..... .....

C:\Users\user\AppData\Local\Temp\dwn.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	8704
Entropy (8bit):	4.76941550076102
Encrypted:	false
SSDEEP:	

MD5:	0E4816AC89A716B262402CD1791400DF
SHA1:	A9F39BD3330B1F70535C716B51E55442E930B164
SHA-256:	BEA1C74AD8FCB8C06967F98F93275784F5DF8266FF9E6AB06273AE48AFED0F8A
SHA-512:	00080A26CD21CD690DCCA18461E7AE2FA10DA6231EE05CFDFF59F580F0B8AA056AD3A502D98364272B2B7AFB0365A04F188569823772719D0366605EAA125767
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... .....0.....Z6... ...@....@.. ..`.....6..O....@..I.....`.....5..... ....H.....text...`.... ..... ..`.rsrc...I....@.....@..@.rel oc.....`..... .....@..B.....<6.....H.....I%.....45.....N.(.....(.....(....*..{....r...po....{....(....o....*..{....(.....{....o....t....o....o....*....0..>..... {....o....t....o.....o.....{....o....."...%.. .o.....(....,*.{....{....o....t....o.....o....o....*.{....o....t....o.....o.....{....o.....t....o.....o.....{....o....."...%.. .o.....(....,).{.....{....o....t....o.

C:\Users\user\AppData\Local\Temp\ixjslbemgsufoiuudk	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	Unicode text, UTF-16, little-endian text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Local\Temp\jzlrsem	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	Unicode text, UTF-16, little-endian text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Local\Temp\odqrgxczfqkyvjblz	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	Unicode text, UTF-16, little-endian text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Local\Temp\xbsbmhljhlcrmkvfybyknsbrlg	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	Unicode text, UTF-16, little-endian text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Local\Temp\xzhdfxk	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	Unicode text, UTF-16, little-endian text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe	
Process:	C:\Users\user\Desktop\Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	8704
Entropy (8bit):	4.8360345624958825
Encrypted:	false
SSDEEP:	
MD5:	A07407FCE937593044AD512F4A6D7A1E
SHA1:	6FC304EB3856198C1F8B1DA8C4A3A52C657274C7
SHA-256:	770A25E30C2F095A09570447FD3AB6ECB78DE00185D39035A1B87B1D7DE89F8C
SHA-512:	03CF85C7D12DACCC5896A607A4C8A4BB14D3769792081AE2CF838FFFA14016556C94389828726ECDECDCD35309E64714F8C000C84D31B849B977FEE6A0B184I1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....{.....0.....6... ...@....@.. ....`.....6..O....@..t.....`.....6..... ....H.....text..... ....`.rsrc...t....@.....@..@.reloc.....`..... .....@..B.....6.....H.....l%..\.....5.....N.(.....(.....(...*..{....r...po.....{....(....o....*..{....(.....{....o....t....o....o....*....0..>.....{....o....t....o.....o.....{....o.....".%.. .o.....(....,*.{.....{....o....t....o.....o....o....*.{....o....t....o.....o....*.{....o....t....o.....o.....{....o.....".%.. .o.....(....,).{.....{....o....t....o.

C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false

SSDEEP:	
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.8360345624958825
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe
File size:	8704
MD5:	a07407fce937593044ad512f4a6d7a1e
SHA1:	6fc304eb3856198c1f8b1da8c4a3a52c657274c7
SHA256:	770a25e30c2f095a09570447fd3ab6ecb78de00185d39035a1b87b1d7de89f8c
SHA512:	03cf85c7d12daccc5896a607a4c8a4bb14d3769792081ae2cf838fffa14016556c94389828726ecdecdcd35309e64714f8c000c84d31b849b977fee6a0b184b1
SSDEEP:	96:2aqDtNDC8SkQVnmWJIfbYey8BMpLrgmRdzf5LoGLSQiLBrhQWRkWHFlwHzNt:2Lj1D8w0dUMpLrgmff5jL0LBdYWHHwR
TLSH:	E402F913F3A9C233CA6F8B7B68A663404775B2012953DF1F9CC661EF5D523808A22753
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....{.....0.....6... ...@....@.. .....`

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4036ee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xB7B87B95 [Sun Sep 4 00:13:09 2067 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x369c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4000	0x574	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3680	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x16f4	0x1800	False	0.494140625	data	5.342980735893486	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x574	0x600	False	0.400390625	data	3.939191122181945	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

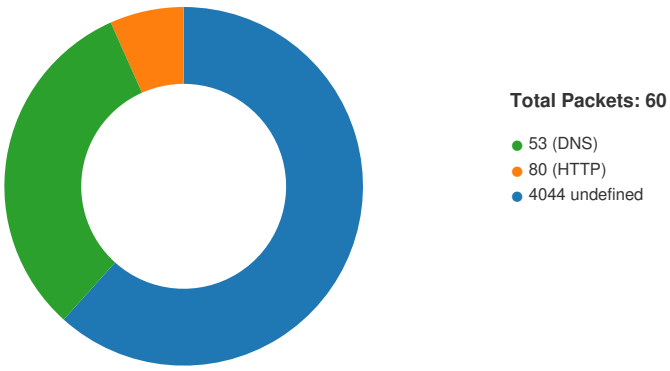
Name	RVA	Size	Type	Language	Country
RT_VERSION	0x4090	0x2e4	data		
RT_MANIFEST	0x4384	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:22:53.998722076 CET	49699	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.067178965 CET	4044	49699	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:54.067753077 CET	49699	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.081659079 CET	49699	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.154901028 CET	4044	49699	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:54.203406096 CET	49699	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.271770000 CET	4044	49699	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:54.287580967 CET	49699	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.406771898 CET	4044	49699	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:54.406872988 CET	49699	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.518484116 CET	4044	49699	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:54.626835108 CET	4044	49699	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:54.629175901 CET	49699	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.697290897 CET	4044	49699	194.5.98.244	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:22:54.712408066 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.728215933 CET	49701	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.750291109 CET	49699	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.776252985 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:54.776626110 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.791661978 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.792160988 CET	4044	49701	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:54.792279959 CET	49701	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.801376104 CET	49701	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.860091925 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:54.869755030 CET	4044	49701	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:54.906552076 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.922188044 CET	49701	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.962141991 CET	49702	80	192.168.2.3	178.237.33.50
Jan 5, 2023 09:22:54.970858097 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:54.978904009 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:54.985882998 CET	4044	49701	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:54.987838030 CET	80	49702	178.237.33.50	192.168.2.3
Jan 5, 2023 09:22:54.988936901 CET	49702	80	192.168.2.3	178.237.33.50
Jan 5, 2023 09:22:54.989974976 CET	49702	80	192.168.2.3	178.237.33.50
Jan 5, 2023 09:22:54.996462107 CET	49701	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.023614883 CET	80	49702	178.237.33.50	192.168.2.3
Jan 5, 2023 09:22:55.023720026 CET	49702	80	192.168.2.3	178.237.33.50
Jan 5, 2023 09:22:55.090154886 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.090369940 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.105263948 CET	4044	49701	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.105400085 CET	49701	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.161180019 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.161218882 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.161247969 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.161272049 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.161320925 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.161370039 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.161406994 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.161433935 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.161458015 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.161505938 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.161524057 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.161550999 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.161575079 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.161604881 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.161614895 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.172470093 CET	49699	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.176378965 CET	4044	49701	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.219178915 CET	49701	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.225759983 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.225805998 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.225825071 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.225846052 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.225867033 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.225886106 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.225903034 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.225917101 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.225930929 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.225965977 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.226020098 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.226109028 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.226130009 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.226185083 CET	49700	4044	192.168.2.3	194.5.98.244

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:22:55.226259947 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.226324081 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.226344109 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.226382971 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.226413012 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.226466894 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.226506948 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.226569891 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.226725101 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.226746082 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.226819038 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.226875067 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.226998091 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.231029987 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.281836987 CET	4044	49699	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.290222883 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.290304899 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.290352106 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.290399075 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.290433884 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.290503025 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.290523052 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.290576935 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.290611982 CET	49700	4044	192.168.2.3	194.5.98.244
Jan 5, 2023 09:22:55.290743113 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.290796041 CET	4044	49700	194.5.98.244	192.168.2.3
Jan 5, 2023 09:22:55.290843010 CET	4044	49700	194.5.98.244	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:22:11.261627913 CET	54397	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:22:11.313416004 CET	59324	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:22:12.907068968 CET	59014	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:22:12.965013027 CET	61626	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:22:53.848974943 CET	52387	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:22:53.987176895 CET	53	52387	8.8.8.8	192.168.2.3
Jan 5, 2023 09:22:54.918896914 CET	56924	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:22:54.938142061 CET	53	56924	8.8.8.8	192.168.2.3
Jan 5, 2023 09:22:55.317893028 CET	60625	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:22:55.337061882 CET	53	60625	8.8.8.8	192.168.2.3
Jan 5, 2023 09:23:09.579471111 CET	49302	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:23:09.597032070 CET	53	49302	8.8.8.8	192.168.2.3
Jan 5, 2023 09:23:11.399391890 CET	53975	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:23:11.483800888 CET	51139	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:23:13.624717951 CET	52955	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:23:13.689357042 CET	60582	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:23:24.654512882 CET	57134	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:23:24.686021090 CET	62050	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:23:26.694236040 CET	56042	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:23:26.753217936 CET	59636	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:24:36.129112005 CET	55638	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:24:36.156496048 CET	53	55638	8.8.8.8	192.168.2.3
Jan 5, 2023 09:24:36.956897020 CET	57704	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:24:36.976675034 CET	53	57704	8.8.8.8	192.168.2.3
Jan 5, 2023 09:24:37.065181971 CET	65320	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:24:37.084306955 CET	53	65320	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 5, 2023 09:22:11.261627913 CET	192.168.2.3	8.8.8.8	0xf807	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:22:11.313416004 CET	192.168.2.3	8.8.8.8	0xccc4	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:22:12.907068968 CET	192.168.2.3	8.8.8.8	0x4713	Standard query (0)	kpf0yw.am.files.1drv.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:22:12.965013027 CET	192.168.2.3	8.8.8.8	0x1bb9	Standard query (0)	kpf0yw.am.files.1drv.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:22:53.848974943 CET	192.168.2.3	8.8.8.8	0xc19	Standard query (0)	obologs.work.gd	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:22:54.918896914 CET	192.168.2.3	8.8.8.8	0x8ef0	Standard query (0)	geoplugin.net	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:22:55.317893028 CET	192.168.2.3	8.8.8.8	0x659b	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:23:09.579471111 CET	192.168.2.3	8.8.8.8	0xe83f	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:23:11.399391890 CET	192.168.2.3	8.8.8.8	0x3a27	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:23:11.483800888 CET	192.168.2.3	8.8.8.8	0xbbb2	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:23:13.624717951 CET	192.168.2.3	8.8.8.8	0x2c3c	Standard query (0)	kpf0yw.am.files.1drv.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:23:13.689357042 CET	192.168.2.3	8.8.8.8	0xcff1	Standard query (0)	kpf0yw.am.files.1drv.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:23:24.654512882 CET	192.168.2.3	8.8.8.8	0xc3f6	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:23:24.686021090 CET	192.168.2.3	8.8.8.8	0x7e62	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:23:26.694236040 CET	192.168.2.3	8.8.8.8	0xcab0	Standard query (0)	kpf0yw.am.files.1drv.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:23:26.753217936 CET	192.168.2.3	8.8.8.8	0x755d	Standard query (0)	kpf0yw.am.files.1drv.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:24:36.129112005 CET	192.168.2.3	8.8.8.8	0x35f5	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:24:36.956897020 CET	192.168.2.3	8.8.8.8	0x2b8e	Standard query (0)	icanhazip.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:24:37.065181971 CET	192.168.2.3	8.8.8.8	0x49a4	Standard query (0)	208.168.6.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 09:22:11.302848101 CET	8.8.8.8	192.168.2.3	0xf807	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:22:11.372673988 CET	8.8.8.8	192.168.2.3	0xccc4	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:22:12.955245018 CET	8.8.8.8	192.168.2.3	0x4713	No error (0)	kpf0yw.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:22:12.955245018 CET	8.8.8.8	192.168.2.3	0x4713	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:22:13.016360044 CET	8.8.8.8	192.168.2.3	0x1bb9	No error (0)	kpf0yw.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:22:13.016360044 CET	8.8.8.8	192.168.2.3	0x1bb9	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:22:53.987176895 CET	8.8.8.8	192.168.2.3	0xc19	No error (0)	obologs.work.gd		194.5.98.244	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:22:54.938142061 CET	8.8.8.8	192.168.2.3	0x8ef0	No error (0)	geoplugin.net		178.237.33.50	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:22:55.337061882 CET	8.8.8.8	192.168.2.3	0x659b	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)	false

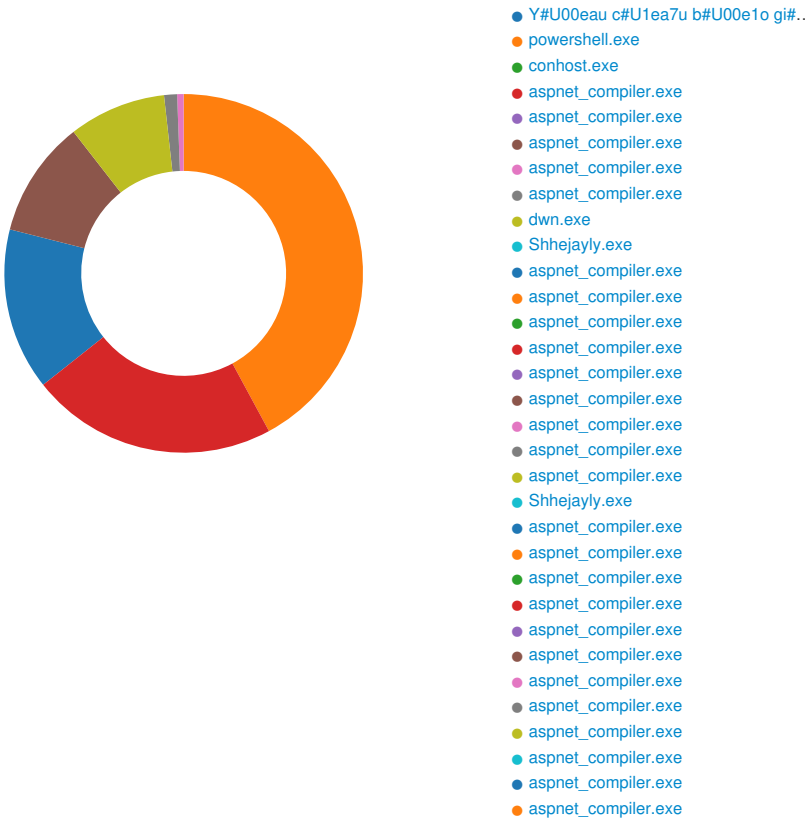
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 09:23:09.597032070 CET	8.8.8.8	192.168.2.3	0xe83f	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:23:11.438133955 CET	8.8.8.8	192.168.2.3	0x3a27	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:23:11.527112961 CET	8.8.8.8	192.168.2.3	0xbbb2	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:23:13.644396067 CET	8.8.8.8	192.168.2.3	0x2c3c	No error (0)	kpf0yw.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:23:13.644396067 CET	8.8.8.8	192.168.2.3	0x2c3c	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:23:13.644396067 CET	8.8.8.8	192.168.2.3	0x2c3c	No error (0)	l-0003.l-dc-msedge.net		13.107.43.12	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:23:13.739938021 CET	8.8.8.8	192.168.2.3	0xcff1	No error (0)	kpf0yw.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:23:13.739938021 CET	8.8.8.8	192.168.2.3	0xcff1	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:23:24.671904087 CET	8.8.8.8	192.168.2.3	0xc3f6	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:23:24.704257011 CET	8.8.8.8	192.168.2.3	0x7e62	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:23:26.742861986 CET	8.8.8.8	192.168.2.3	0xcab0	No error (0)	kpf0yw.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:23:26.742861986 CET	8.8.8.8	192.168.2.3	0xcab0	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:23:26.804606915 CET	8.8.8.8	192.168.2.3	0x755d	No error (0)	kpf0yw.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:23:26.804606915 CET	8.8.8.8	192.168.2.3	0x755d	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:24:36.156496048 CET	8.8.8.8	192.168.2.3	0x35f5	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:24:36.976675034 CET	8.8.8.8	192.168.2.3	0x2b8e	No error (0)	icanhazip.com		104.18.114.97	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:24:36.976675034 CET	8.8.8.8	192.168.2.3	0x2b8e	No error (0)	icanhazip.com		104.18.115.97	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:24:37.084306955 CET	8.8.8.8	192.168.2.3	0x49a4	Name error (3)	208.168.6.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)	false

HTTP Request Dependency Graph

- transfer.sh
- kpf0yw.am.files.1drv.com
- geoplugin.net

Statistics

Behavior



System Behavior

Analysis Process: Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe PID: **3988**, Parent PID: **3452**

General	
Target ID:	0
Start time:	09:22:06
Start date:	05/01/2023
Path:	C:\Users\user\Desktop\Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe
Imagebase:	0x180000
File size:	8704 bytes
MD5 hash:	A07407FCE937593044AD512F4A6D7A1E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.365213489.0000000007610000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.358493957.00000000037C8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000000.00000002.358493957.00000000037C8000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.355179401.0000000002596000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.357319262.0000000003630000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000000.00000002.357319262.0000000003630000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.357530014.00000000036B0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000000.00000002.357530014.00000000036B0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.271856566.0000000003772000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.355401113.00000000025D4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000000.00000002.355401113.00000000025D4000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1BCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1BCF06	unknown
C:\Users\user\AppData\Roaming\Yqxsvaorwni	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C00BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	793C8D3	CopyFileW
C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	793C8D3	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Y#U00eau c#U1ea7ub#U00e1o gi#U00e1 INV20230104-VN.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4CC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe	0	8704	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 7b fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 18 00 00 00 08 00 00 00 00 00 00 fd 36 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL{06 @@ `	success or wait	1	793C8D3	CopyFileW
C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	793C8D3	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Y#U00eau c#U1ea7u b#U00e1o gi#U00e1 INV20230104-VN.exe.log	0	1537	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D4CC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D0F03DE	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Shhejayly	unicode	"C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe"	success or wait	1	6C00646A	RegSetValueExW

Analysis Process: powershell.exe PID: **3420**, Parent PID: **3988**

General

Target ID:	8
Start time:	09:22:28
Start date:	05/01/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0x1090000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dgi0vwrh.uo4.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C001E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_eq3xehn2.mjn.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C001E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C001E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1BCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1BCF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_dgi0vwrh.uo4.ps1	success or wait	1	6C006A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_eq3xehn2.mjn.psm1	success or wait	1	6C006A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_dgi0vwrh.uo4.ps1	0	1	31	1	success or wait	1	6C001B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_eq3xehn2.mjn.psm1	0	1	31	1	success or wait	1	6C001B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE<eY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6C001B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 fd fd fd fd 79 48 fd 38 9f fd 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50	Get-RandomCFSOut-StringWrite-ProgressDisable-PSBreakpointUpdate-FormatDataWrite-InformationConvertTo-XmlSet-VariableOut-PrinteryH8IC:\Program Files (x86)\WindowsP	success or wait	1	6C001B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 08 0f 00 00 11 00 00 00 fd 0e fd 05 10 09 01 09 31 08 00 00 37 01 2c 00 04 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e17,@	success or wait	1	6D4876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 29 00 00 00 0e 00 20 00	H<@^L"My:)	success or wait	15	6D4876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	15	6D4876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6D4876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	6D4876FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 67 40 01 fd 01 40 00 fd 00 40 00 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 16 3b 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 38 4d 40 01 4d 03 40 01 3f 4d 40 01 fd 45 40	T@>@g@@@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;@;M@D@D@@M@<M@$M@;@;@<@<@<@W@8M@M@?M@E@	success or wait	8	6D4876FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D19CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D1A1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22424	success or wait	1	6D1A203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	132	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C001B4F	ReadFile

Analysis Process: conhost.exe PID: **3920**, Parent PID: **3420**

General

Target ID:	9
Start time:	09:22:28
Start date:	05/01/2023
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: aspnet_compiler.exe PID: **3660**, Parent PID: **3988**

General

Target ID:	12
Start time:	09:22:52
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0xd60000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000C.00000000.351505282.0000000000456000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 0000000C.00000000.351505282.0000000000456000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000C.00000002.520253260.0000000001307000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\dwn.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40671A	URLDownloadToFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ubrkswxpfz	success or wait	1	411FB9	DeleteFileW
C:\Users\user\AppData\Local\Temp\evectoiqthdfs	success or wait	1	411F7D	DeleteFileW
C:\Users\user\AppData\Local\Temp\tzolmupfuamrqwiynvqal	success or wait	1	411FB9	DeleteFileW
C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz	success or wait	1	411F7D	DeleteFileW
C:\Users\user\AppData\Local\Temp\ivyunzdcvtueoyrjhmkmqwoatvkpua	success or wait	1	411FB9	DeleteFileW
C:\Users\user\AppData\Local\Temp\sxdnnkoerbmjyegnzxxfbjirubcqnlslo	success or wait	1	411F7D	DeleteFileW
C:\Users\user\AppData\Local\Temp\huvvgpvbsu	success or wait	1	411FB9	DeleteFileW
C:\Users\user\AppData\Local\Temp\jwaohifvgcnaz	success or wait	1	411F7D	DeleteFileW
C:\Users\user\AppData\Local\Temp\mvrmgcrxgnlvkuc	success or wait	1	411FB9	DeleteFileW
C:\Users\user\AppData\Local\Temp\wyeehvbyuvdiuiytom	success or wait	1	411F7D	DeleteFileW
C:\Users\user\AppData\Local\Temp\qxwkypnatycdxqppqhom	success or wait	1	411FB9	DeleteFileW
C:\Users\user\AppData\Local\Temp\azjdzhxuhhuhiwlbzsaoosx	success or wait	1	411F7D	DeleteFileW
C:\Users\user\AppData\Local\Temp\qdpxxrfaetisgrzptz	success or wait	1	411F46	DeleteFileW
C:\Users\user\AppData\Local\Temp\sfvqykycsbaxjxotkkidcy	success or wait	1	411FB9	DeleteFileW
C:\Users\user\AppData\Local\Temp\czaiycjwgjsktdkxuvvffdxxj	success or wait	1	411F7D	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\json[1].json	0	944	7b 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 71 75 65 73 74 22 3a 22 38 34 2e 31 37 2e 35 32 2e 38 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 73 74 61 74 75 73 22 3a 32 30 30 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 64 65 6c 61 79 22 3a 22 31 6d 73 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 72 65 64 69 74 22 3a 22 53 6f 6d 65 20 6f 66 20 74 68 65 20 72 65 74 75 72 6e 65 64 20 64 61 74 61 20 69 6e 63 6c 75 64 65 73 20 47 65 6f 4c 69 74 65 20 64 61 74 61 20 63 72 65 61 74 65 64 20 62 79 20 4d 61 78 4d 69 6e 64 2c 20 61 76 61 69 6c 61 62 6c 65 20 66 72 6f 6d 20 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 5c 2f 5c 2f 77 77 77 2e 6d 61 78 6d 69 6e 64 2e 63 6f 6d 27 3e 68 74 74 70 3a 5c 2f 5c 2f 77 77 77 2e 6d 61 78 6d 69 6e 64 2e 63 6f 6d	{ "geoplugin_request":"84.17.52.8", "geoplugin_status":200, "geoplugin_delay":"1ms", "geoplugin_credit":"Some of the returned data includes GeoLite data created by MaxMind, available from <a href='http:\/\/www.maxmind.com'>http:\/\/www.maxmind.com	success or wait	1	4198DD	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Cuhcxlcg[1].exe	0	8192	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 20 04 fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 18 00 00 00 08 00 00 00 00 00 00 5a 36 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL 0Z6 @@ `	success or wait	1	40671A	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Cuhcxlcg[1].exe	8192	512	00 30 00 00 0c 00 00 00 5c 36 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0\6	success or wait	1	40671A	URLDownloadToFileW
C:\Users\user\AppData\Local\Temp\dwn.exe	0	8704	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 20 04 fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 18 00 00 00 08 00 00 00 00 00 00 5a 36 00 00 00 20 00 00 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL 0Z6 @@ `	success or wait	1	40671A	URLDownloadToFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ubrkswxpfz	unknown	0	success or wait	1	41A7A7	ReadFile
C:\Users\user\AppData\Local\Temp\evectoiqthdfs	unknown	0	success or wait	1	41A7A7	ReadFile
C:\Users\user\AppData\Local\Temp\tzolmupfuamrqwiynvqal	unknown	0	success or wait	1	41A7A7	ReadFile
C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz	unknown	0	success or wait	1	41A7A7	ReadFile
C:\Users\user\AppData\Local\Temp\ivyunzdcvtueoyrjhmkmqwoatvkpua	unknown	0	success or wait	1	41A7A7	ReadFile
C:\Users\user\AppData\Local\Temp\sxdnnkoerbmjyegnzxxfbjirubcqnlslo	unknown	0	success or wait	1	41A7A7	ReadFile
C:\Users\user\AppData\Local\Temp\huvvgpvbsu	unknown	0	success or wait	1	41A7A7	ReadFile
C:\Users\user\AppData\Local\Temp\jwaohifvgcnaz	unknown	0	success or wait	1	41A7A7	ReadFile
C:\Users\user\AppData\Local\Temp\mvrmgcrxgnlvkuc	unknown	0	success or wait	1	41A7A7	ReadFile
C:\Users\user\AppData\Local\Temp\wyeehvbyuvdiuiytom	unknown	0	success or wait	1	41A7A7	ReadFile
C:\Users\user\AppData\Local\Temp\qxwkypnatycdxqppqhom	unknown	0	success or wait	1	41A7A7	ReadFile
C:\Users\user\AppData\Local\Temp\azjdzhxuhhuhiwlbzsaoosx	unknown	0	success or wait	1	41A7A7	ReadFile
C:\Users\user\AppData\Local\Temp\qdpxxrfaetisgrzptz	unknown	2	success or wait	1	41A7A7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sfvqykycsbaxjxotkkidcy	unknown	0	success or wait	1	41A7A7	ReadFile
C:\Users\user\AppData\Local\Temp\czaiycjwgjsktdkxuvvffdxxj	unknown	0	success or wait	1	41A7A7	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Rmc-E9KXT7\	success or wait	1	4126A9	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Rmc-E9KXT7	exepath	binary	61 E6 86 EE EB 9D 84 48 1F B9 0E FE AC FE D3 6E F8 C8 9C 03 58 04 3B 20 CA F7 01 49 1E 3D A1 7B FF 88 DF 37 0E 97 9D 4F 01 0A D3 99 B5 98 10 30 82 DA F2 72 F2 8D F9 08 9F 37 39 2F B4 21 97 B0 8B 2F C3 57 B4 18 64 A8 24 E3 3E C7 F3 79 78 3E D2 27 C0 F0 60 49 A0 94 6C BA CE AB 4B 13 10 2F 67 53 75 69 A8 D6 B4 E8 46 DB 4B 22 41 E3 D2 BF B1 10 B7 AD 92 DB A8 EB 6B A6 7F F6 19 54 C1 93 2D E7 6D 63	success or wait	1	4126D1	RegSetValueExA
HKEY_CURRENT_USER\Software\Rmc-E9KXT7	licence	unicode	BC3F8046923AC4CA8598E8CC4E31D531	success or wait	1	4126D1	RegSetValueExA

Analysis Process: aspnet_compiler.exe PID: **732**, Parent PID: **3660**

General

Target ID:	13
Start time:	09:22:57
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\jzlrsem"
Imagebase:	0x400000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: aspnet_compiler.exe PID: **4884**, Parent PID: **3660**

General

Target ID:	14
Start time:	09:22:57
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\jzlrsem"
Imagebase:	0x7ff68f300000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhvF833.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	409A8B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\jzlrsem	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4096F4	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhvF833.tmp	success or wait	1	40E5A9	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhvF833.tmp	0	26738688	7c 2a 12 fd 6b fd 20 06 00 00 00 00 00 00 74 3b 00 00 00 00 00 00 d2 74 65 33 13 11 1b 06 77 67 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 43 00 0d 00 00 00 2c 26 15 10 08 7a fd 02 2f 26 15 10 08 7a 7b 00 68 02 45 00 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 36 fd 0c 34 33 13 11 1b 06 77 49 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 00 00 00 0a 00 00 00 00 00 00 00 fd 42 00 00 00 00 00 00 14 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	| t;te3wgC,&z/&z{hE643wl\B	success or wait	1	40E134	WriteFile
C:\Users\user\AppData\Local\Temp\jzlrsem	0	2	fd fd		success or wait	1	40A32B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhvF833.tmp	unknown	1024	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Temp\bhvF833.tmp	unknown	32768	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Temp\bhvF833.tmp	unknown	32768	success or wait	2	40A30C	ReadFile
C:\Users\user\AppData\Local\Temp\bhvF833.tmp	unknown	32768	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Temp\bhvF833.tmp	unknown	32768	success or wait	3	40A30C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	61356	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	4	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	61356	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	2048	success or wait	1	417623	ReadFile

Analysis Process: aspnet_compiler.exe

PID: **5236**, Parent PID: **3660**

General	
Target ID:	15
Start time:	09:22:58
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\ubrkswxpfz"
Imagebase:	0x910000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ubrkswxpfz	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406AD0	CreateFileA

Analysis Process: aspnet_compiler.exe PID: **5812**, Parent PID: **3660**

General	
Target ID:	16
Start time:	09:22:59
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\evectoiqthdfs"
Imagebase:	0x850000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\evectoiqthdfs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4067EB	CreateFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	406EF3	ReadFile

Analysis Process: dwn.exe PID: **2088**, Parent PID: **3660**

General	
Target ID:	17
Start time:	09:23:03
Start date:	05/01/2023

Path:	C:\Users\user\AppData\Local\Temp\dwn.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\dwn.exe"
Imagebase:	0xae0000
File size:	8704 bytes
MD5 hash:	0E4816AC89A716B262402CD1791400DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.543466399.0000000003093000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.600053448.0000000007BD0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.590461155.0000000004C7A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.590461155.0000000004C7A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000011.00000002.590461155.0000000004C7A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_Discord_Regex, Description: Detects executables referencing Discord tokens regular expressions, Source: 00000011.00000002.590461155.0000000004C7A000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.568348321.0000000004661000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.568348321.0000000004661000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000011.00000002.568348321.0000000004661000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_Discord_Regex, Description: Detects executables referencing Discord tokens regular expressions, Source: 00000011.00000002.568348321.0000000004661000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1BCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1BCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D0F03DE	ReadFile

Analysis Process: Shhejayly.exe PID: **4420**, Parent PID: **3452**

General	
Target ID:	18
Start time:	09:23:05
Start date:	05/01/2023
Path:	C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe"
Imagebase:	0x120000
File size:	8704 bytes
MD5 hash:	A07407FCE937593044AD512F4A6D7A1E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000012.00000002.539326956.00000000025A6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: aspnet_compiler.exe PID: **4892**, Parent PID: **3660**

General	
Target ID:	19
Start time:	09:23:07
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\ixjslbemgsufoiuudk"
Imagebase:	0x740000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **1552**, Parent PID: **3660**

General	
Target ID:	20
Start time:	09:23:07
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\tzolmupfuamrqwiynvqal"
Imagebase:	0x1b0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **3324**, Parent PID: **3660**

General	
Target ID:	21
Start time:	09:23:08

Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\tzolmupfuamrqwiynvqal"
Imagebase:	0x8d0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **4740**, Parent PID: **3660**

General

Target ID:	22
Start time:	09:23:08
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz"
Imagebase:	0xa0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **4116**, Parent PID: **3660**

General

Target ID:	23
Start time:	09:23:08
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz"
Imagebase:	0x360000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **4988**, Parent PID: **3660**

General

Target ID:	24
Start time:	09:23:09
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz"
Imagebase:	0xc0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **4964**, Parent PID: **3660**

General

Target ID:	25
Start time:	09:23:09
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz"
Imagebase:	0x70000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **3776**, Parent PID: **3660**

General

Target ID:	26
Start time:	09:23:09
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz"
Imagebase:	0x2b0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **4972**, Parent PID: **3660**

General

Target ID:	27
Start time:	09:23:10
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\dttwnmhhiiewacecwgdtoztjz"
Imagebase:	0x940000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Shhejayly.exe PID: **5608**, Parent PID: **3452**

General

Target ID:	28

Start time:	09:23:13
Start date:	05/01/2023
Path:	C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Yqxsvaorwni\Shhejayly.exe"
Imagebase:	0x90000
File size:	8704 bytes
MD5 hash:	A07407FCE937593044AD512F4A6D7A1E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000001C.00000002.542998195.0000000002653000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000001C.00000002.538968887.0000000002586000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000001C.00000002.551264239.000000000370A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: aspnet_compiler.exe PID: **5716**, Parent PID: **3660**

General

Target ID:	29
Start time:	09:23:16
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\xbsbmhljhlcrmkvfybyknsbrlg"
Imagebase:	0x730000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **5828**, Parent PID: **3660**

General

Target ID:	30
Start time:	09:23:16
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\ivyunzdcvtueoyrjhmkmqwoatvkpua"
Imagebase:	0xed0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **5764**, Parent PID: **3660**

General

Target ID:	31
Start time:	09:23:17
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\sxdnnkoerbmjyegnzxxfbjirubcqnlslo"
Imagebase:	0x2c0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **5868**, Parent PID: **3660**

General

Target ID:	32
Start time:	09:23:17
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\sxdnnkoerbmjyegnzxxfbjirubcqnlslo"
Imagebase:	0x930000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **6092**, Parent PID: **3660**

General

Target ID:	33
Start time:	09:23:26
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\xzhdfxk"
Imagebase:	0xe20000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **6088**, Parent PID: **3660**

General

Target ID:	34
Start time:	09:23:27
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\huvvgpvbsu"
Imagebase:	0x920000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **3020**, Parent PID: **3660**

General	
Target ID:	35
Start time:	09:23:28
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\jwaohifvgcnaz"
Imagebase:	0xb0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **5936**, Parent PID: **3660**

General	
Target ID:	36
Start time:	09:23:28
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\jwaohifvgcnaz"
Imagebase:	0xab0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **3460**, Parent PID: **3660**

General	
Target ID:	39
Start time:	09:23:34
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\bbmbgkgdsftq"
Imagebase:	0x560000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **4952**, Parent PID: **3660**

General	
Target ID:	40
Start time:	09:23:34
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\mvrmgcrxgnlvkuc"
Imagebase:	0xfb0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **5348**, Parent PID: **3660**

General	
Target ID:	41
Start time:	09:23:35
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\wyeehvbyuvdiuiytom"
Imagebase:	0xfc0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: **5312**, Parent PID: **3660**

General	
Target ID:	42
Start time:	09:23:42
Start date:	05/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe /stext "C:\Users\user\AppData\Local\Temp\odqrgxczfqkyvjblz"
Imagebase:	0x7ff70b1a0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly