ID: 831200
Sample Name:
SC_0017384.exe
Cookbook: default.jbs
Time: 09:09:12
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

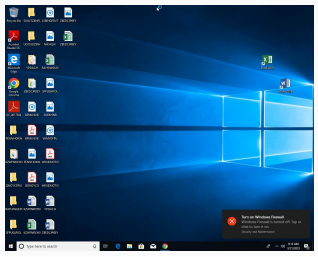
Windows Analysis Report

SC_0017384.exe

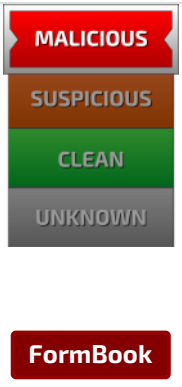
Overview

General Information

Sample Name:	SC_0017384.exe
Analysis ID:	831200
MD5:	f296a60e15687..
SHA1:	e24c65bd02d4…
SHA256:	661f40c3448fa…
Tags:	exe
Infos:	



Detection



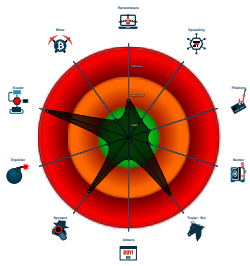
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Encrypted powershell cmdline option…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- SC_0017384.exe (PID: 5876 cmdline: C:\Users\user\Desktop\SC_0017384.exe MD5: F296A60E1568722B060DE70B46357FE6)
  - powershell.exe (PID: 5040 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQB zAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SC_0017384.exe (PID: 5956 cmdline: C:\Users\user\Desktop\SC_0017384.exe MD5: F296A60E1568722B060DE70B46357FE6)
    - explorer.exe (PID: 3324 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - Lvdnyvcvr.exe (PID: 6136 cmdline: "C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe" MD5: F296A60E1568722B060DE70B46357FE6)
        - powershell.exe (PID: 4504 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQB zAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 6048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - Lvdnyvcvr.exe (PID: 1980 cmdline: C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe MD5: F296A60E1568722B060DE70B46357FE6)
      - systray.exe (PID: 5568 cmdline: C:\Windows\SysWOW64\systray.exe MD5: 1373D481BE4C8A6E5F5030D2FB0A0C68)
      - Lvdnyvcvr.exe (PID: 1436 cmdline: "C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe" MD5: F296A60E1568722B060DE70B46357FE6)
        - powershell.exe (PID: 6116 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQB zAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 572 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - Lvdnyvcvr.exe (PID: 5300 cmdline: C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe MD5: F296A60E1568722B060DE70B46357FE6)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Formbook, Formbo	FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.	• SWEED • Cobalt	http://blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.htmlhttp://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.htmlhttps://asec.ahnlab.com/en/32149/https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.575645185.0000000002FB0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000008.00000002.575645185.0000000002FB0000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1f060:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xae1f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x18267:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000008.00000002.575645185.0000000002FB0000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x18065:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17b01:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x18167:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x182df:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa9ea:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x16d5c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1de07:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1edba:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.430971378.0000000001150000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000003.00000002.430971378.0000000001150000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1f060:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xae1f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x18267:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Click to see the 11 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.SC_0017384.exe.400000.0.raw.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
3.2.SC_0017384.exe.400000.0.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x20de3:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xcba2:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x19fea:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Source	Rule	Description	Author	Strings
3.2.SC_0017384.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x19de8:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x19884:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x19eea:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1a062:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xc76d:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x18adf:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1fb8a:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x20b3d:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
3.2.SC_0017384.exe.400000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
3.2.SC_0017384.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1ffe3:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xbda2:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x191ea:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 172.67.194.225

Timestamp:	192.168.2.5172.67.194.22549710802031453 03/21/23-09:12:13.411086
SID:	2031453
Source Port:	49710
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 74.208.236.131

Timestamp:	192.168.2.574.208.236.13149702802031449 03/21/23-09:11:27.575244
SID:	2031449
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 74.208.236.131

Timestamp:	192.168.2.574.208.236.13149702802031412 03/21/23-09:11:27.575244
SID:	2031412
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 74.208.236.131

Timestamp:	192.168.2.574.208.236.13149702802031453 03/21/23-09:11:27.575244
SID:	2031453
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 172.67.194.225

Timestamp:	192.168.2.5172.67.194.22549710802031449 03/21/23-09:12:13.411086
SID:	2031449
Source Port:	49710
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 172.67.194.225	−
Timestamp:	192.168.2.5172.67.194.22549710802031412 03/21/23-09:12:13.411086
SID:	2031412
Source Port:	49710
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

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

Snort IDS alert for network traffic

Yara detected Generic Downloader

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

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

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

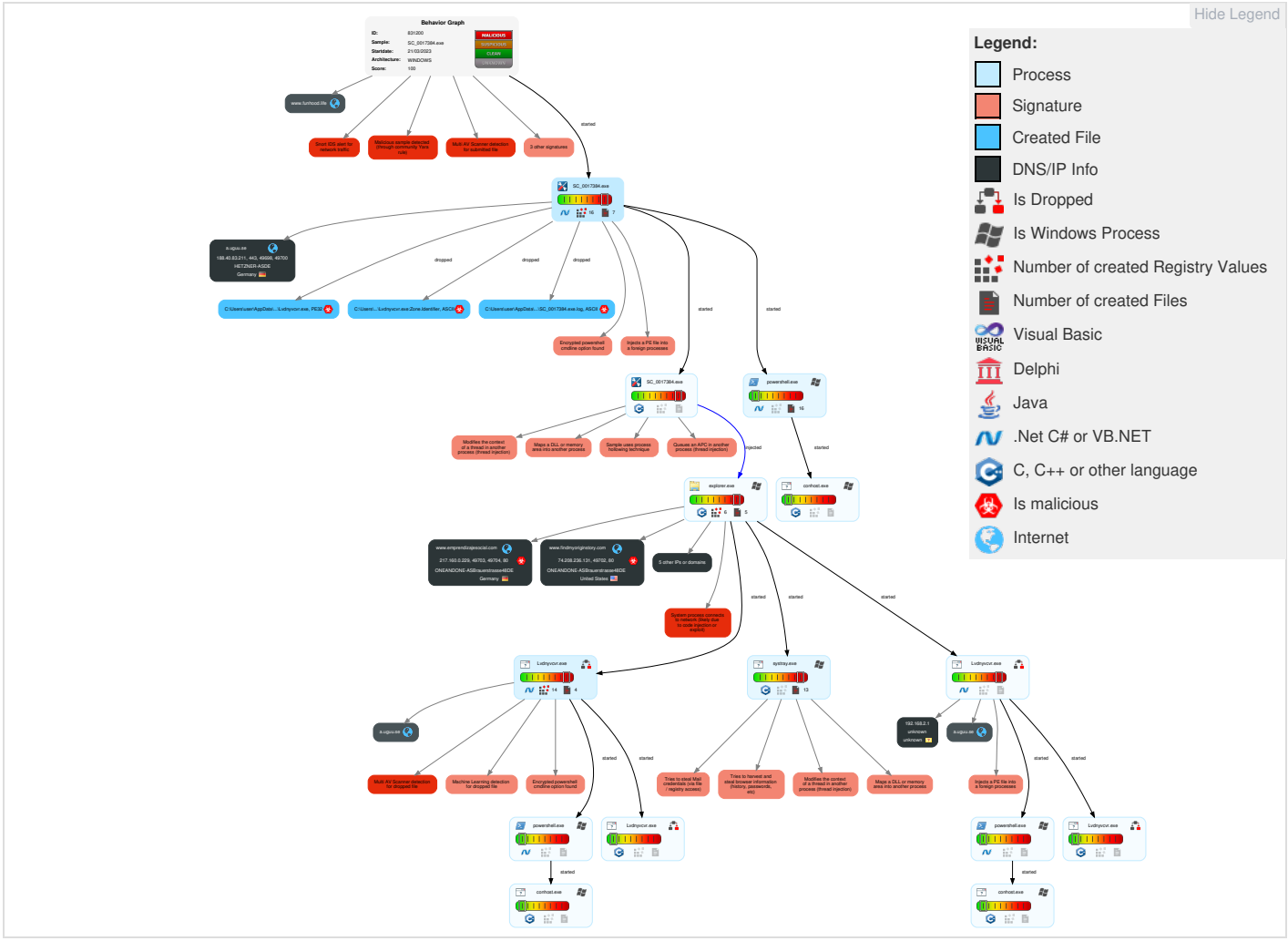
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	1 Registry Run Keys / Startup Folder	6 1 2 Process Injection	1 Disable or Modify Tools	1 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 PowerShell	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 1 Deobfuscate/Decode Files or Information	1 Input Capture	1 3 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	1 2 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	5 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 Software Packing	NTDS	2 Process Discovery	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	1 6 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window 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	6 1 2 Process Injection	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

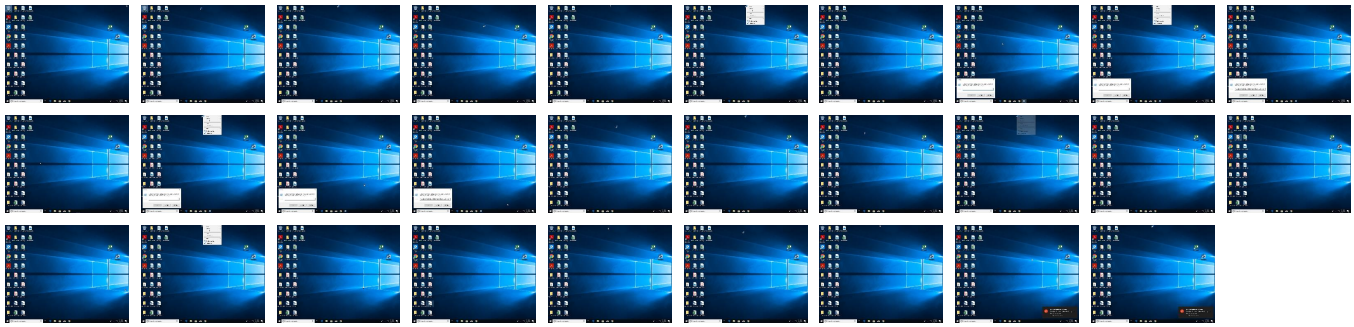
Behavior Graph



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
SC_0017384.exe	13%	ReversingLabs	Win32.Trojan.Worefflint	
SC_0017384.exe	18%	Virustotal		Browse
SC_0017384.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe	13%	ReversingLabs	Win32.Trojan.Worefflint	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.SC_0017384.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.madisoncountylincoln.com	0%	Virustotal		Browse
brunaeleandro.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://https://a.uguu.se4Dp	0%	Avira URL Cloud	safe	
http://www.funhood.lifewww.funhood.life	0%	Avira URL Cloud	safe	
http://www.rw-bau.com/t4np/	0%	Avira URL Cloud	safe	
http://www.madisoncountylincoln.com	0%	Avira URL Cloud	safe	
http://www.emprendizajesocial.com/t4np/	0%	Avira URL Cloud	safe	
http://www.evelycosmetique.comwww.evelycosmetique.com	0%	Avira URL Cloud	safe	
http://www.brunaeleandro.comwww.brunaeleandro.com	0%	Avira URL Cloud	safe	
http://www.metatv.app	0%	Avira URL Cloud	safe	
http://www.groupekoriolis.com	0%	Avira URL Cloud	safe	
http://www.myprojoints.comwww.myprojoints.com	0%	Avira URL Cloud	safe	
http://www.groupekoriolis.com/t4np/	0%	Avira URL Cloud	safe	
http://www.33347.netwww.33347.net	0%	Avira URL Cloud	safe	
http://www.madisoncountylincoln.com/	0%	Avira URL Cloud	safe	
http://www.mejawajib.shop	0%	Avira URL Cloud	safe	
http://https://www.casar.com/assunto/casamentos/decoracao-de-casamento/	0%	Avira URL Cloud	safe	
http://https://www.casar.com/assunto/lua-de-mel-2/	0%	Avira URL Cloud	safe	
http://https://www.casar.com	0%	Avira URL Cloud	safe	
http://https://www.casar.com/assunto/organizacao/	0%	Avira URL Cloud	safe	
http://www.funhood.life	0%	Avira URL Cloud	safe	
http://www.brunaeleandro.com	0%	Avira URL Cloud	safe	
http://www.findmyoriginstory.comwww.findmyoriginstory.com	0%	Avira URL Cloud	safe	
http://www.mnsmanagmentsolutions.com	0%	Avira URL Cloud	safe	
http://www.findmyoriginstory.com	0%	Avira URL Cloud	safe	
http://www.sistemadanetflix.site/t4np/	0%	Avira URL Cloud	safe	
http://www.sistemadanetflix.sitewww.sistemadanetflix.site	0%	Avira URL Cloud	safe	
http://www.babupaul.comwww.babupaul.com	0%	Avira URL Cloud	safe	
http://https://www.casar.com/assunto/noivas/dicas-para-noivas/	0%	Avira URL Cloud	safe	
http://www.evelycosmetique.com	0%	Avira URL Cloud	safe	
http://www.icste-conference.org	0%	Avira URL Cloud	safe	
http://www.33347.net	0%	Avira URL Cloud	safe	
http://www.rw-bau.comwww.rw-bau.com	0%	Avira URL Cloud	safe	
http://www.mejawajib.shopwww.mejawajib.shop	0%	Avira URL Cloud	safe	
http://www.myprojoints.com	0%	Avira URL Cloud	safe	
http://www.babupaul.com/t4np/	0%	Avira URL Cloud	safe	
http://www.metatv.app/t4np/	0%	Avira URL Cloud	safe	
http://www.madisoncountylincoln.com/t4np/?LAIu=TchAG45&ekDWdXmx=b7otzynn0HmortmfwUeY4rOKK/wDsahaMH4CpYcAMUMZFiGwLHjB+0Oq1wXjzAJPnkBdjV2xmRY1HYDRMeq0YWMvPw2aK61dkA==	0%	Avira URL Cloud	safe	
http://www.metatv.app/t4np/?ekDWdXmx=yN4s0tXHCEK4GbHOxK129Y7foRrzq40ElafmJhvJj1LcshAib7Ivom6LHCQSa6JmmrJNk5dNV7FfRE38dwcSsWQdgWRuTjAoEA==&LAIu=TchAG45	0%	Avira URL Cloud	safe	
http://www.madisoncountylincoln.com/t4np/	0%	Avira URL Cloud	safe	
http://https://www.casar.com/assunto/casamentos/casamentos-reais/	0%	Avira URL Cloud	safe	
http://www.funhood.life/t4np/	0%	Avira URL Cloud	safe	
http://www.emprendizajesocial.com/t4np/?LAIu=TchAG45&ekDWdXmx=gQIyGWpAOrsnJd0q1zycF3dboTDh0JHEHzF0+87QMzSWBZus6QBaVJZOvsOvWQQjPhLlWjZ0Xc16UyU8zopwRBvkYI23apdf5g==	0%	Avira URL Cloud	safe	
http://www.sistemadanetflix.site	0%	Avira URL Cloud	safe	
http://https://www.casar.com/assunto/cha-de-panela/	0%	Avira URL Cloud	safe	
http://www.findmyoriginstory.com/t4np/?LAIu=TchAG45&ekDWdXmx=yKIXTmp5dZbzu0kOoimFYUx0Rf1qUZs10N2udgS/CtBUsUx15VFtNYN9iDnYFh77a6AF4rH5pFyFnuGOqSZvoPy3IjvUZKwOXw==	0%	Avira URL Cloud	safe	
http://https://www.casar.com/assunto/noivas/vestidos-de-noiva/	0%	Avira URL Cloud	safe	
http://www.brunaeleandro.com/t4np/?ekDWdXmx=TNgCDQM1NseJ/EyvbqZD4bEVgDXmfsqsK09kjaHK361RIlxqLtgkaoztB9HOqO+kj7AmSjC7tsKJawScM9Xl/2xtyFPsJZxirw==&LAIu=TchAG45	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.findmyoriginstory.com/t4np/	0%	Avira URL Cloud	safe	
http://https://br.enterprise.wibson.io/banner.js?siteId=78509e00-767d-4326-9529-f0d523c8137c	0%	Avira URL Cloud	safe	
http://www.mejawajib.shop/t4np/	0%	Avira URL Cloud	safe	
http://www.rw-bau.com	0%	Avira URL Cloud	safe	
http://www.mnsmanagmentsolutions.comwww.mnsmanagmentsolutions.com	0%	Avira URL Cloud	safe	
http://www.madisoncountylincoln.comwww.madisoncountylincoln.com	0%	Avira URL Cloud	safe	
http://www.icste-conference.org/t4np/	0%	Avira URL Cloud	safe	
http://www.babupaul.com	0%	Avira URL Cloud	safe	
http://www.icste-conference.orgwww.icste-conference.org	0%	Avira URL Cloud	safe	
http://www.mnsmanagmentsolutions.com/t4np/	0%	Avira URL Cloud	safe	
http://www.groupekoriolis.comwww.groupekoriolis.com	0%	Avira URL Cloud	safe	
http://www.myprojoints.com/t4np/	0%	Avira URL Cloud	safe	
http://https://urn.to/r/sds_see5bad	0%	Avira URL Cloud	safe	
http://www.emprendizajesocial.com	0%	Avira URL Cloud	safe	
http://www.emprendizajesocial.comwww.emprendizajesocial.com	0%	Avira URL Cloud	safe	
http://www.metatv.appwww.metatv.app	0%	Avira URL Cloud	safe	
http://https://ajuda.casar.com	0%	Avira URL Cloud	safe	
http://www.33347.net/t4np/	0%	Avira URL Cloud	safe	
http://www.brunaeleandro.com/t4np/	0%	Avira URL Cloud	safe	
http://www.evelycosmetique.com/t4np/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.madisoncountylincoln.com	172.67.152.24	true	true	• 0%, Virustotal, Browse	unknown
a.uguu.se	188.40.83.211	true	false		high
www.funhood.life	162.213.249.254	true	false		unknown
brunaeleandro.com	54.85.86.211	true	true	• 0%, Virustotal, Browse	unknown
www.emprendizajesocial.com	217.160.0.229	true	true		unknown
www.metatv.app	172.67.194.225	true	true		unknown
www.findmyoriginstory.com	74.208.236.131	true	true		unknown
www.brunaeleandro.com	unknown	unknown	true		unknown
www.myprojoints.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.emprendizajesocial.com/t4np/	true	• Avira URL Cloud: safe	unknown
http://www.metatv.app/t4np/	true	• Avira URL Cloud: safe	unknown
http://www.madisoncountylincoln.com/t4np/?LAIu=TchAG45&ekDWdXmx=b7otzynn0HmortmfwUeY4rOKK/wDsahaMH4CpYcAMUMZFiGwLHjB+0Oq1wXjzAJPnkBdjV2xmRY1HYDRMeq0YWMvPw2aK61dkA==	true	• Avira URL Cloud: safe	unknown
http://www.metatv.app/t4np/?ekDWdXmx=yN4s0tXHCEK4GbHOxK129Y7foRrzq40ElafmJhvJj1LcshAib7Ivom6LHCQSa6JmmrJNk5dNV7FfRE38dwcSsWQdgWRuTjAoEA==&LAIu=TchAG45	true	• Avira URL Cloud: safe	unknown
http://www.madisoncountylincoln.com/t4np/	true	• Avira URL Cloud: safe	unknown
http://www.emprendizajesocial.com/t4np/?LAIu=TchAG45&ekDWdXmx=gQIyGWpAOrsnJd0q1zycF3dboTDh0JHEHzF0+87QMzSWBZus6QBaVJZOvsOvWQQjPhLlWjZ0Xc16UyU8zopwRBvkYI23apdf5g==	true	• Avira URL Cloud: safe	unknown
http://www.findmyoriginstory.com/t4np/?LAIu=TchAG45&ekDWdXmx=yKIXTmp5dZbzu0kOoimFYUx0Rf1qUZs10N2udgS/CtBUsUx15VFtNYN9iDnYFh77a6AF4rH5pFyFnuGOqSZvoPy3IjvUZKwOXw==	true	• Avira URL Cloud: safe	unknown
http://www.brunaeleandro.com/t4np/?ekDWdXmx=TNgCDQM1NseJ/EyvbqZD4bEVgDXmfsqsK09kjaHK361RIlxqLtgkaoztB9HOqO+kj7AmSjC7tsKJawScM9XI/2xtyFPsJZxirw==&LAIu=TchAG45	true	• Avira URL Cloud: safe	unknown
http://https://a.uguu.se/fwvfviJb.dat	false		high
http://www.brunaeleandro.com/t4np/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	M61Ae5o9b.8.dr	false		high
http://https://duckduckgo.com/ac/?q=	M61Ae5o9b.8.dr	false		high
http://www.rw-bau.com/t4np/	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.madisoncountylincoln.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.casar.com/assunto/organizacao/	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.metatv.app	explorer.exe, 00000004.00000002.58450237 9.000000000162000.00000040.80000000.000 40000.00000000.sdmp, explorer.exe, 00000 004.00000002.584837486.00000000065D0000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://a.uguu.se4Dp	SC_0017384.exe, 00000000.00000002.382705 892.00000000030C1000.00000004.00000800.0 0020000.00000000.sdmp, Lvdnyvcvr.exe, 00 000005.00000002.549345681.00000000025910 00.00000004.00000800.00020000.00000000.sdmp, Lvdnyvcvr.exe, 00000009.00000002.570544457.00 000000026DE000.00000004.00000800.0002000 0.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// www.brunaeleandro.comwww.brunaeleandro.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.funhood.lifewww.funhood.life	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.casar.com/assunto/casamentos/decoracao-de-casamento/	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// www.evelycosmetique.comwww.evelycosmetique.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com?fr=crmas_sfpf	M61Ae5o9b.8.dr	false		high
http://https://www.newtonsoft.com/json	Lvdnyvcvr.exe, 00000005.00000002.5493456 81.00000000026F2000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.myprojoints.comwww.myprojoints.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.groupekoriolis.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.casar.com/assunto/lua-de-mel-2/	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.33347.netwww.33347.net	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.groupekoriolis.com/t4np/	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mejawajib.shop	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

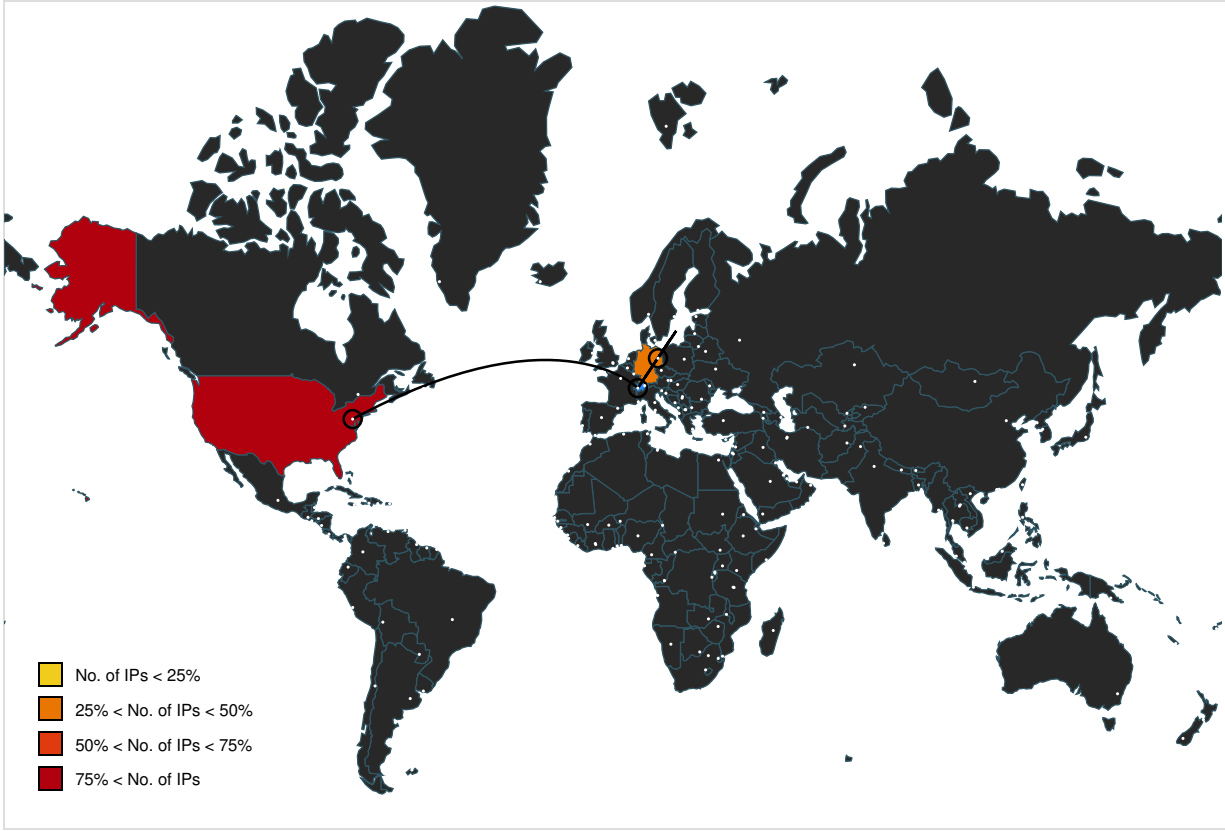
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.casar.com	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.madisoncountylincoln.com/	explorer.exe, 00000004.00000002.59485381 6.00000000160EE000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005E0E000.0 0000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.brunaeleandro.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// www.findmyoriginstory.comwww.findmyoriginstory.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.funhood.life	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://embed.typeform.com/embed.js	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.findmyoriginstory.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mnsmanagmentsolutions.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sistemadanetflix.site/t4np/	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.evelycosmetique.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://connect.facebook.net/en_US/fbevents.js	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://www.casar.com/assunto/noivas/dicas-para-noivas/	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://a.uguu.se/fwvfviJb.dat=	SC_0017384.exe, Lvdnyvcvr.exe.0.dr	false		high
http://www.babupaul.comwww.babupaul.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// www.sistemadanetflix.sitewww.sistemadanetflix.site	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SC_0017384.exe, 00000000.00000002.382705 892.00000000030C1000.00000004.00000800.0 0020000.00000000.sdmp, Lvdnyvcvr.exe, 00 000005.00000002.549345681.00000000025910 00.00000004.00000800.00020000.00000000.sdmp, Lvdnyvcvr.exe, 00000009.00000002.570544457.00 000000026DE000.00000004.00000800.0002000 0.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pinterest.com/casarpontocom	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.mejawajib.shopwww.mejawajib.shop	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.myprojoints.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.00000003.53366880 3.000000000ED27000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.575675145.0000000000921000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.592015514.000000 000ED28000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0000.386129776.000000000091F000.00000004 .00000020.00020000.00000000.sdmp	false		high
http://www.icste-conference.org	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.33347.net	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rw-bau.comwww.rw-bau.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.google.com/images/branding/product/ico/googleg_lodp.ico	M61Ae5o9b.8.dr	false		high
http://www.babupaul.com/t4np/	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.casar.com/assunto/casamentos/casamentos-reais/	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/casarpontocom	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http:// https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	M61Ae5o9b.8.dr	false		high
http://www.funhood.life/t4np/	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	M61Ae5o9b.8.dr	false		high
http://https://www.casar.com/assunto/cha-de-panela/	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sistemadanetflix.site	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js	explorer.exe, 00000004.00000002.5948538 16.0000000015F5C000.00000004.80000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.579809865.0000000005C7C000.00000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.583099802.00000000079A0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://oss.maxcdn.com/libs/respond.js/1.3.0/respond.min.js	explorer.exe, 00000004.00000002.5948538 16.0000000015F5C000.00000004.80000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.579809865.0000000005C7C000.00000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.583099802.00000000079A0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	M61Ae5o9b.8.dr	false		high
http://james.newtonking.com/projects/json	Lvdnyvcvr.exe, 00000005.00000002.549345681.00000000026F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.casar.com/assunto/noivas/vestidos-de-noiva/	explorer.exe, 00000004.00000002.5948538 16.0000000015F5C000.00000004.80000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.579809865.0000000005C7C000.00000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.583099802.00000000079A0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.findmyoriginstory.com/t4np/	explorer.exe, 00000004.00000002.5848374 86.00000000065D0000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	M61Ae5o9b.8.dr	false		high
http://https://br.enterprise.wibson.io/banner.js?siteId=78509e00-767d-4326-9529-f0d523c8137c	explorer.exe, 00000004.00000002.5948538 16.0000000015F5C000.00000004.80000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.579809865.0000000005C7C000.00000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.583099802.00000000079A0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://plus.google.com/	explorer.exe, 00000004.00000002.5948538 16.0000000015F5C000.00000004.80000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.579809865.0000000005C7C000.00000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.583099802.00000000079A0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfp	M61Ae5o9b.8.dr	false		high
http://www.mejawajib.shop/t4np/	explorer.exe, 00000004.00000002.5848374 86.00000000065D0000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mnsmanagmentsolutions.comwww.mnsmanagmentsolutions.com	explorer.exe, 00000004.00000002.5848374 86.00000000065D0000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.madisoncountylincoln.comwww.madisoncountylincoln.com	explorer.exe, 00000004.00000002.5848374 86.00000000065D0000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rw-bau.com	explorer.exe, 00000004.00000002.5848374 86.00000000065D0000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.icste-conference.org/t4np/	explorer.exe, 00000004.00000002.5848374 86.00000000065D0000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.icste-conference.orgwww.icste-conference.org	explorer.exe, 00000004.00000002.5848374 86.00000000065D0000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.babupaul.com	explorer.exe, 00000004.00000002.5848374 86.00000000065D0000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.groupekoriolis.comwww.groupekoriolis.com	explorer.exe, 00000004.00000002.5848374 86.00000000065D0000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.newtonsoft.com/jsonschema	Lvdnyvcvr.exe, 00000005.00000002.549345681.00000000026F2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mnsmanagmentsolutions.com/t4np/	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.myprojoints.com/t4np/	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.emprendizajesocial.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.emprendizajesocial.comwww.emprendizajesocial.com	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/es5-shim/4.5.14/es5-shim.min.js	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://urn.to/r/sds_see5bad	SC_0017384.exe, 00000000.00000002.385968 571.000000000419A000.00000004.00000800.0 0020000.00000000.sdmp, SC_0017384.exe, 0 0000000.00000002.401744017.0000000006980 000.00000004.08000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.nuget.org/packages/Newtonsoft.Json.Bson	SC_0017384.exe, 00000000.00000002.385968 571.0000000004BE2000.00000004.00000800.0 0020000.00000000.sdmp, SC_0017384.exe, 0 0000000.00000002.382705892.0000000003222 000.00000004.00000800.00020000.00000000.sdmp, SC_0017384.exe, 00000000.00000002.385968571. 0000000004CFA000.00000004.00000800.00020 000.00000000.sdmp, SC_0017384.exe, 00000 000.00000002.404394395.0000000006FD0000. 00000004.08000000.00040000.00000000.sdmp, Lvdnyvcvr.exe, 00000005.00000002.54934 5681.00000000026F2000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.metatv.appwww.metatv.app	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://instagram.com/casarpontocom	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://ajuda.casar.com	explorer.exe, 00000004.00000002.59485381 6.0000000015F5C000.00000004.80000000.000 40000.00000000.sdmp, systray.exe, 000000 08.00000002.579809865.0000000005C7C000.0 0000004.10000000.00040000.00000000.sdmp, systray.exe, 00000008.00000002.58309980 2.00000000079A0000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	M61Ae5o9b.8.dr	false		high
http://www.33347.net/t4np/	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.evelycosmetique.com/t4np/	explorer.exe, 00000004.00000002.58483748 6.00000000065D0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.85.86.211	brunaeleandro.com	United States		14618	AMAZON-AESUS	true
172.67.152.24	www.madisoncountylincoln.com	United States		13335	CLOUDFLARENETUS	true
74.208.236.131	www.findmyoriginstory.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
217.160.0.229	www.emprendizajesocial.com	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
172.67.194.225	www.metatv.app	United States		13335	CLOUDFLARENETUS	true
188.40.83.211	a.uguu.se	Germany		24940	HETZNER-ASDE	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831200
Start date and time:	2023-03-21 09:09:12 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	SC_0017384.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@26/13@11/7
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 72.3% (good quality ratio 66.2%) • Quality average: 73% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Execution Graph export aborted for target SC_0017384.exe, PID 5876 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:10:09	API Interceptor	10x Sleep call for process: SC_0017384.exe modified
09:10:21	API Interceptor	98x Sleep call for process: powershell.exe modified
09:10:49	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Lvdnyvcvr "C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe"
09:10:57	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Lvdnyvcvr "C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe"
09:11:00	API Interceptor	606x Sleep call for process: explorer.exe modified
09:11:05	API Interceptor	20x Sleep call for process: Lvdnyvcvr.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\CLR_v4.0_32\UsageLogs\Lvdnyvcvr.exe.log

Process:	C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1570
Entropy (8bit):	5.357969604744043
Encrypted:	false
SSDEEP:	48:MxHKXwYHKhQnowHBtHoxHhAHKzvAHKgmHKKHKdHKBo:iqXwYqhQnowhtlxHeqzlqTqKqdqy
MD5:	01403378423BC80FF1C71B821B33B07C
SHA1:	B86FAFEDD98B3237252375E7DAA5215A20C4E0D1
SHA-256:	D29D2FC27260201D6E5B6AFDC218CD254AE25E692C2935A1E07B50922114FDDE
SHA-512:	FA447D7B7146B128265A12610F56CB8E3FE5A191A1AC7EEFED644D6C2FB0D8DB2FDF0075058BD2DF939725640DE5432B3F8C3A6E75CE3292CF9952C8C127C09
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Net.Http, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\86d45445dab8672072401605 1271f5f9\System.Net.Http.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.X

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SC_0017384.exe.log

Process:	C:\Users\user\Desktop\SC_0017384.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1570
Entropy (8bit):	5.357969604744043
Encrypted:	false
SSDEEP:	48:MxHKXwYHKhQnowHBtHoxHhAHKzvAHKgmHKKHKdHKBo:iqXwYqhQnowhtlxHeqzlqTqKqdqy
MD5:	01403378423BC80FF1C71B821B33B07C
SHA1:	B86FAFEDD98B3237252375E7DAA5215A20C4E0D1
SHA-256:	D29D2FC27260201D6E5B6AFDC218CD254AE25E692C2935A1E07B50922114FDDE
SHA-512:	FA447D7B7146B128265A12610F56CB8E3FE5A191A1AC7EEFED644D6C2FB0D8DB2FDF0075058BD2DF939725640DE5432B3F8C3A6E75CE3292CF9952C8C127C09
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Net.Http, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\86d45445dab8672072401605 1271f5f9\System.Net.Http.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.X

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

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	4.8968676994158
Encrypted:	false
SSDEEP:	96:WCJ2Woe5o2k6Lm5emmXIGvgyg12jDs+un/iQLEYFjDaeWJ6KGcmXx9smyFRLcU6f:5xoe5oVsm5emd0gkjDt4iWN3yBGHh9s6
MD5:	36DE9155D6C265A1DE62A448F3B5B66E
SHA1:	02D21946CBDD01860A0DE38D7EEC6CDE3A964FC3

SHA-256:	8BA38D55AA8F1E4F959E7223FDF653ABB9BE5B8B5DE9D116604E1ABB371C1C87
SHA-512:	C734ADE161FB89472B1DF9B9F062F4A53E7010D3FF99EDC0BD564540A56BC35743625C50A00635C31D165A74DCDBB330FFB878C5919D7B267F6F33D2AAB328E7
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

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

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	15564
Entropy (8bit):	5.551291320499996
Encrypted:	false
SSDEEP:	384:Hte/RG0cEBW971II99bCfyMSjnOilrIR9FvImP4oX+mE:P9719KoOilr09CSlE
MD5:	E7F1796E8DF5FC62B672DA2F4429B4E4
SHA1:	D95E6A1652A1D6C86DAE3B9B7F8BF260666442B2
SHA-256:	05D85276F0B5FD0CCFAD9093B5A7D1E50773B063FD54FBDD7BA4E76893DB79B9
SHA-512:	D398997AE48EDDDE315F82942F3021904BAFE441516F3A580A059B557FB09D5A38A4D8A179C578132B107110F38E6951EAEABC07A885631670AD55D5312E6419
Malicious:	false
Preview:	@...e.....e.W.h.....1.....H.....<@.^.L."My...'..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\M61Ae5o9b

Process:	C:\Windows\SysWOW64\systray.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.287139506398081
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPF6n/YVuzdqfEwn7PrH944:QS/indc/YVuzdqfEwn7b944
MD5:	292F98D765C8712910776C89ADDE2311
SHA1:	E9F4CCB4577B3E6857C6116C9CBA0F3EC63878C5
SHA-256:	9C63F8321526F04D4CD0CFE11EA32576D1502272FE8333536B9DEE2C3B49825E
SHA-512:	205764B34543D8B53118B3AEA88C550B2273E6EBC880AAD5A106F8DB11D520EB8FD6EFD3DB3B87A4500D287187832FCF18F60556072DD7F5CC947BB7A4E3C31
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dgjipv3a.uw1.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false

Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_i35hi1li.r2m.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_i45pd4er.ypj.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jfu4f4st.4n4.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_k1fvfy5u.yzh.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B

SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qoqqfvf3.zav.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe

Process:	C:\Users\user\Desktop\SC_0017384.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	692224
Entropy (8bit):	5.868183818609632
Encrypted:	false
SSDEEP:	12288:xTyShIKgMyx0SA4sZm4hGFJ4eCPBh+C3:xxhI+zSAdI2GFJ4Xz
MD5:	F296A60E1568722B060DE70B46357FE6
SHA1:	E24C65BD02D435C6B5705E9A01442E0447B77E22
SHA-256:	661F40C3448FA2ACBDDFD8297C54733B9F2D9C71E15506A4FBA876A25D279E76
SHA-512:	D3B3A695845EF355BCBA27DD6E55DA85EA345F661AD0D10BFF776E0192E21186B780C764D12E293CDEAA819854FA8D1681D585591F34627436B8CCFF97AB6D 4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....d.....J...D.....zh... .....@.. ....`.....,h..L.....FA.....h..... ..H.....text....H... ...J..... ..`.rsrc...FA.....B...L.....@..@.rel oc.....@..B.....H.....4m.....0'.....s.....(....jo.....(....o.....(....o.....%.....(....o.....(....o.....o....r...po.....o....r...po ....s.....(...+%..o.....jo.....o.....(.....o.....o.....(....(.....o.....(.....o....o....(....*.....(....*..{....*"..}....*.....{....*"..}....*.....{....*"..}....*.....{....*"..}....*.....{....*"..}....*.....{. ...*J.s....}.....(....*..0..).....i.Y.8.....

C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\SC_0017384.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.868183818609632
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SC_0017384.exe
File size:	692224
MD5:	f296a60e1568722b060de70b46357fe6
SHA1:	e24c65bd02d435c6b5705e9a01442e0447b77e22
SHA256:	661f40c3448fa2acbddfd8297c54733b9f2d9c71e15506a4fba876a25d279e76
SHA512:	d3b3a695845ef355bcba27dd6e55da85ea345f661ad0d10bff776e0192e21186b780c764d12e293cdeaa819854fa8d1681d585591f34627436b8ccff97ab6d64
SSDEEP:	12288:xTyShIKgMyx0SA4sZm4hGFJ4eCPBh+C3:xxhl+zSAdl2GFJ4Xz
TLSH:	BFE429707BF89717C5BF6B72E0B9B25847B4D466A216E78B844D52F10CD2340AC1A3AF
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....d.....J...D.....zh... .....@.. .....`.....

File Icon

Icon Hash:	185ada32e9cc368b

Static PE Info

General

Entrypoint:	0x4a687a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6418E0D7 [Mon Mar 20 22:40:23 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [004A6888h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
pop esp
push 0000000Ah
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa682c	0x4c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa8000	0x4146	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xae000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0xa6888	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa4890	0xa4a00	False	0.34067126993166286	data	5.83594677699421	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xa8000	0x4146	0x4200	False	0.20815577651515152	data	4.044367816999576	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa8140	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024, resolution 3779 x 3779 px/m		
RT_ICON	0xa85b8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096, resolution 3779 x 3779 px/m		
RT_ICON	0xa9670	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216, resolution 3779 x 3779 px/m		
RT_GROUP_ICON	0xabc28	0x30	data		
RT_VERSION	0xabc68	0x2e4	data		
RT_MANIFEST	0xabf5c	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

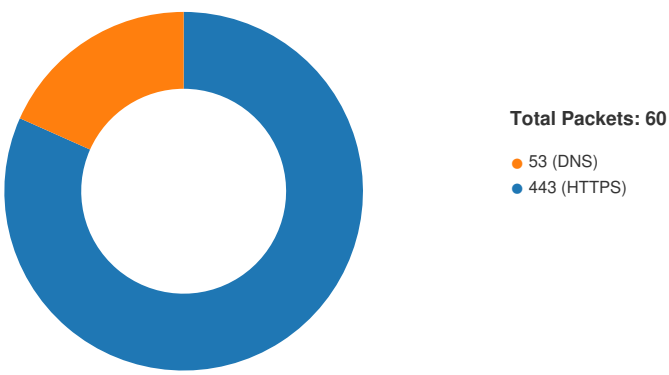
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5172.67.194.22549710802031453 03/21/23-09:12:13.411086	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49710	80	192.168.2.5	172.67.194.225
192.168.2.574.208.236.131470280203144 9 03/21/23-09:11:27.575244	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49702	80	192.168.2.5	74.208.236.131
192.168.2.574.208.236.131470280203141 2 03/21/23-09:11:27.575244	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49702	80	192.168.2.5	74.208.236.131
192.168.2.574.208.236.131470280203145 3 03/21/23-09:11:27.575244	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49702	80	192.168.2.5	74.208.236.131
192.168.2.5172.67.194.22549710802031449 03/21/23-09:12:13.411086	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49710	80	192.168.2.5	172.67.194.225
192.168.2.5172.67.194.22549710802031412 03/21/23-09:12:13.411086	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49710	80	192.168.2.5	172.67.194.225

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 09:10:10.204607964 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.204669952 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.204794884 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.244721889 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.244771004 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.314131021 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.314223051 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.331425905 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.331454039 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.331841946 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.383747101 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.569000006 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.569056034 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.617197990 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.617248058 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.617260933 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.617333889 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.617363930 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.617372990 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.617403030 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.617440939 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.617489100 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.617489100 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.617489100 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.617495060 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.617517948 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.617527008 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.617542982 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.617557049 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.617588997 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.617589951 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.617607117 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.617654085 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.617682934 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.641709089 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.641772985 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.641916037 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.641935110 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.641969919 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.641987085 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.642051935 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.642110109 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.642123938 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.642133951 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.642165899 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.642195940 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.642529964 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.642575979 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.642618895 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.642632008 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.642652035 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.642673016 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.667993069 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.668103933 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.668189049 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.668215036 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.668237925 CET	49698	443	192.168.2.5	188.40.83.211

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 09:10:10.668272018 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.668406010 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.668510914 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.668545961 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.668556929 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.668587923 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.668603897 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.668737888 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.668801069 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.668867111 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.668884993 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.668903112 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.668940067 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.669044018 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.669110060 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.669153929 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.669162989 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.669193983 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.669217110 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.669527054 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.669589043 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.669621944 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.669630051 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.669658899 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.669677973 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.669856071 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.669913054 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.669943094 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.669959068 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.669975042 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.669996977 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.695274115 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.695343018 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.695442915 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.695466995 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.695493937 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.695514917 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.695888042 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.695940971 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.695972919 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.695986032 CET	443	49698	188.40.83.211	192.168.2.5
Mar 21, 2023 09:10:10.696022987 CET	49698	443	192.168.2.5	188.40.83.211
Mar 21, 2023 09:10:10.696048975 CET	49698	443	192.168.2.5	188.40.83.211

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 09:10:10.167546034 CET	50295	53	192.168.2.5	8.8.8.8
Mar 21, 2023 09:10:10.190110922 CET	53	50295	8.8.8.8	192.168.2.5
Mar 21, 2023 09:11:06.057960033 CET	61893	53	192.168.2.5	8.8.8.8
Mar 21, 2023 09:11:06.080689907 CET	53	61893	8.8.8.8	192.168.2.5
Mar 21, 2023 09:11:12.532519102 CET	60649	53	192.168.2.5	8.8.8.8
Mar 21, 2023 09:11:12.570863962 CET	53	60649	8.8.8.8	192.168.2.5
Mar 21, 2023 09:11:27.414058924 CET	51441	53	192.168.2.5	8.8.8.8
Mar 21, 2023 09:11:27.439889908 CET	53	51441	8.8.8.8	192.168.2.5
Mar 21, 2023 09:11:32.721693039 CET	49177	53	192.168.2.5	8.8.8.8
Mar 21, 2023 09:11:32.756217957 CET	53	49177	8.8.8.8	192.168.2.5
Mar 21, 2023 09:11:33.768779039 CET	49724	53	192.168.2.5	8.8.8.8
Mar 21, 2023 09:11:33.796116114 CET	53	49724	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 09:11:38.816267967 CET	61452	53	192.168.2.5	8.8.8.8
Mar 21, 2023 09:11:38.865930080 CET	53	61452	8.8.8.8	192.168.2.5
Mar 21, 2023 09:11:52.604053974 CET	65323	53	192.168.2.5	8.8.8.8
Mar 21, 2023 09:11:52.655042887 CET	53	65323	8.8.8.8	192.168.2.5
Mar 21, 2023 09:12:02.826678038 CET	51484	53	192.168.2.5	8.8.8.8
Mar 21, 2023 09:12:02.859888077 CET	53	51484	8.8.8.8	192.168.2.5
Mar 21, 2023 09:12:10.767373085 CET	63446	53	192.168.2.5	8.8.8.8
Mar 21, 2023 09:12:10.800434113 CET	53	63446	8.8.8.8	192.168.2.5
Mar 21, 2023 09:12:30.799199104 CET	56751	53	192.168.2.5	8.8.8.8
Mar 21, 2023 09:12:30.833955050 CET	53	56751	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 21, 2023 09:10:10.167546034 CET	192.168.2.5	8.8.8.8	0x51ae	Standard query (0)	a.uguu.se	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:06.057960033 CET	192.168.2.5	8.8.8.8	0x4cc7	Standard query (0)	a.uguu.se	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:12.532519102 CET	192.168.2.5	8.8.8.8	0x4c7c	Standard query (0)	a.uguu.se	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:27.414058924 CET	192.168.2.5	8.8.8.8	0x796e	Standard query (0)	www.findmyoriginstory.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:32.721693039 CET	192.168.2.5	8.8.8.8	0xd6de	Standard query (0)	www.myprojoints.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:33.768779039 CET	192.168.2.5	8.8.8.8	0x8005	Standard query (0)	www.myprojoints.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:38.816267967 CET	192.168.2.5	8.8.8.8	0x9a6f	Standard query (0)	www.emprendizajesocial.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:52.604053974 CET	192.168.2.5	8.8.8.8	0xae8b	Standard query (0)	www.brunaeleandro.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:12:02.826678038 CET	192.168.2.5	8.8.8.8	0x2e15	Standard query (0)	www.madisoncountylincoln.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:12:10.767373085 CET	192.168.2.5	8.8.8.8	0xf69	Standard query (0)	www.metatv.app	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:12:30.799199104 CET	192.168.2.5	8.8.8.8	0x55c	Standard query (0)	www.funhood.life	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 21, 2023 09:10:10.190110922 CET	8.8.8.8	192.168.2.5	0x51ae	No error (0)	a.uguu.se		188.40.83.211	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:06.080689907 CET	8.8.8.8	192.168.2.5	0x4cc7	No error (0)	a.uguu.se		188.40.83.211	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:12.570863962 CET	8.8.8.8	192.168.2.5	0x4c7c	No error (0)	a.uguu.se		188.40.83.211	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:27.439889908 CET	8.8.8.8	192.168.2.5	0x796e	No error (0)	www.findmyoriginstory.com		74.208.236.131	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:32.756217957 CET	8.8.8.8	192.168.2.5	0xd6de	Name error (3)	www.myprojoints.com	none	none	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:33.796116114 CET	8.8.8.8	192.168.2.5	0x8005	Name error (3)	www.myprojoints.com	none	none	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:38.865930080 CET	8.8.8.8	192.168.2.5	0x9a6f	No error (0)	www.emprendizajesocial.com		217.160.0.229	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:11:52.655042887 CET	8.8.8.8	192.168.2.5	0xae8b	No error (0)	www.brunaeleandro.com	brunaeleandro.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 09:11:52.655042887 CET	8.8.8.8	192.168.2.5	0xae8b	No error (0)	brunaeleandro.com		54.85.86.211	A (IP address)	IN (0x0001)	false

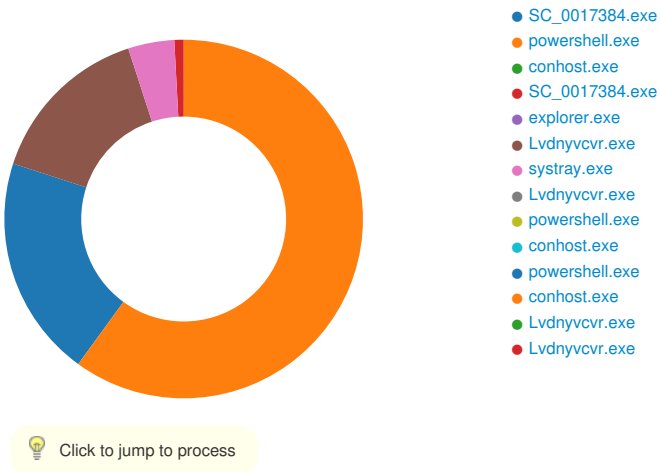
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 21, 2023 09:12:02.859888077 CET	8.8.8.8	192.168.2.5	0x2e15	No error (0)	www.madisoncountylincoln.com		172.67.152.24	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:12:02.859888077 CET	8.8.8.8	192.168.2.5	0x2e15	No error (0)	www.madisoncountylincoln.com		104.21.65.231	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:12:10.800434113 CET	8.8.8.8	192.168.2.5	0xf69	No error (0)	www.metatv.app		172.67.194.225	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:12:10.800434113 CET	8.8.8.8	192.168.2.5	0xf69	No error (0)	www.metatv.app		104.21.20.242	A (IP address)	IN (0x0001)	false
Mar 21, 2023 09:12:30.833955050 CET	8.8.8.8	192.168.2.5	0x55c	No error (0)	www.funhood.life		162.213.249.254	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- a.uguu.se
- www.findmyoriginstory.com
- www.emprendizajesocial.com
- www.brunaeleandro.com
- www.madisoncountylincoln.com
- www.metatv.app

Statistics

Behavior



System Behavior

Analysis Process: SC_0017384.exe PID: **5876**, Parent PID: **3324**

General

Target ID:	0
Start time:	09:10:07
Start date:	21/03/2023
Path:	C:\Users\user\Desktop\SC_0017384.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SC_0017384.exe
Imagebase:	0xcf0000
File size:	692224 bytes
MD5 hash:	F296A60E1568722B060DE70B46357FE6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000000.00000002.401744017.0000000006980000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

Analysis Process: powershell.exe PID: **5040**, Parent PID: **5876**

General

Target ID:	1
Start time:	09:10:18
Start date:	21/03/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0xdd0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\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	70FD5B28	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	70FD5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dgjipv3a.uw1.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71071E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_i35hi1li.r2m.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71071E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71071E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	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	7222CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_dgjipv3a.uw1.ps1	success or wait	1	71076A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_i35hi1li.r2m.psm1	success or wait	1	71076A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_dgjipv3a.uw1.ps1	0	1	31	1	success or wait	1	71071B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_i35hi1li.r2m.psm1	0	1	31	1	success or wait	1	71071B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE<eY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	71071B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 fd fd fd fd 79 48 fd 38 9f fd 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50	Get-RandomCFSOut-StringWrite-ProgressDisable-PSBreakpointUpdate-FormatDataWrite-InformationConvertTo-XmlSet-VariableOut-PrinteryH8IC:\Program Files (x86)\WindowsP	success or wait	1	71071B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 1e 0e 00 00 12 00 00 00 05 0f fd 06 65 08 57 08 68 07 00 00 00 00 31 00 09 00 fd 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@eeWh1	success or wait	1	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 27 00 00 00 0e 00 20 00	H<@^L"My:'	success or wait	15	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	15	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	724F76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 42 4d 40 01 fd 44 40 01 6d 45 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 45 40	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@;@BM@D@mE@;@;@<@<@<@W@M@E@	success or wait	8	724F76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7220CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72211F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22420	success or wait	1	7221203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	71071B4F	ReadFile

Analysis Process: conhost.exe PID: **472**, Parent PID: **5040**

General

Target ID:	2
Start time:	09:10:18
Start date:	21/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000

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: SC_0017384.exe PID: **5956**, Parent PID: **5876**

General

Target ID:	3
Start time:	09:10:45
Start date:	21/03/2023
Path:	C:\Users\user\Desktop\SC_0017384.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SC_0017384.exe
Imagebase:	0xc20000
File size:	692224 bytes
MD5 hash:	F296A60E1568722B060DE70B46357FE6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.430971378.0000000001150000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.430971378.0000000001150000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.430971378.0000000001150000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.430398181.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.430398181.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.430398181.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41E63A	NtReadFile

Analysis Process: explorer.exe PID: **3324**, Parent PID: **5956**

General

Target ID:	4
Start time:	09:10:48
Start date:	21/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69bc80000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
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	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

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: Lvdnyvcvr.exe PID: **6136**, Parent PID: **3324**

General

Target ID:	5
Start time:	09:10:57
Start date:	21/03/2023
Path:	C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe"
Imagebase:	0x250000
File size:	692224 bytes
MD5 hash:	F296A60E1568722B060DE70B46357FE6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 13%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	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	7222CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Lvdnyvcvr.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7253C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Lvdnyvcvr.exe.log	0	1570	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	7253C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\86d45445dab86720724016051271f5f9\System.Net.Http.ni.dll.aux	unknown	536	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	721603DE	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: systray.exe PID: **5568**, Parent PID: **3324**

General

Target ID:	8
Start time:	09:11:05

Start date:	21/03/2023
Path:	C:\Windows\SysWOW64\systray.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\systray.exe
Imagebase:	0xea0000
File size:	9728 bytes
MD5 hash:	1373D481BE4C8A6E5F5030D2FB0A0C68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.575645185.0000000002FB0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.575645185.0000000002FB0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.575645185.0000000002FB0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.577052861.0000000004CD0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.577052861.0000000004CD0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.577052861.0000000004CD0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.577203879.0000000004D00000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.577203879.0000000004D00000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.577203879.0000000004D00000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SC_0017384.exe	cannot delete	1	2FCC8E7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\M61Ae5o9b	object name not found	1	2FCC8E7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\M61Ae5o9b	sharing violation	1	2FCC8E7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\M61Ae5o9b	sharing violation	1	2FCC8E7	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2FCC8B7	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: Lvdnyvcvr.exe PID: **1436**, Parent PID: **3324**

General

Target ID:	9
Start time:	09:11:07
Start date:	21/03/2023
Path:	C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe"
Imagebase:	0x160000

File size:	692224 bytes
MD5 hash:	F296A60E1568722B060DE70B46357FE6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: powershell.exe PID: **4504**, Parent PID: **6136**

General	
Target ID:	10
Start time:	09:11:33
Start date:	21/03/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0xdd0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: **6048**, Parent PID: **4504**

General	
Target ID:	11
Start time:	09:11:33
Start date:	21/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **6116**, Parent PID: **1436**

General	
Target ID:	12
Start time:	09:11:43
Start date:	21/03/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0xdd0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **572**, Parent PID: **6116**

General	
Target ID:	13
Start time:	09:11:44
Start date:	21/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: Lvdnyvcvr.exe PID: **1980**, Parent PID: **6136**

General	
Target ID:	14
Start time:	09:11:58
Start date:	21/03/2023
Path:	C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe
Imagebase:	0xa30000
File size:	692224 bytes
MD5 hash:	F296A60E1568722B060DE70B46357FE6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: Lvdnyvcvr.exe PID: **5300**, Parent PID: **1436**

General	
Target ID:	16
Start time:	09:12:09
Start date:	21/03/2023
Path:	C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Jqtuyob\Lvdnyvcvr.exe
Imagebase:	0x950000
File size:	692224 bytes
MD5 hash:	F296A60E1568722B060DE70B46357FE6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly