ID: 346555
Sample Name: Orders.exe
Cookbook: default.jbs
Time: 09:07:53
Date: 01/02/2021
Version: 31.0.0 Emerald

Table of Contents

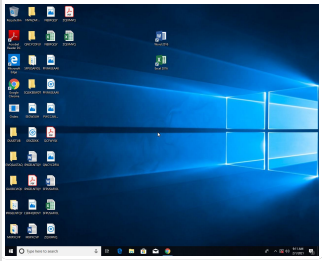
Analysis Report Orders.exe

Overview

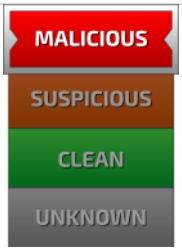
General Information

Sample Name:	Orders.exe
Analysis ID:	346555
MD5:	e85daf3a43f107b..
SHA1:	042208c7a232b8..
SHA256:	0b1fbc81d9d9e68.
Tags:	exe Yahoo

Most interesting Screenshot:



Detection



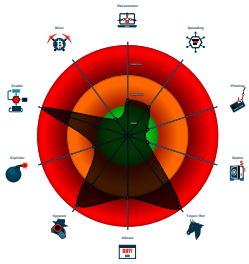
HawkEye AgentTesla MailPassView Matiex

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

Signatures

- Antivirus detection for dropped file
- Detected HawkEye Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Capture Wi-Fi pass…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- Yara detected Matiex Keylogger
- .NET source code contains potentia…

Classification



Startup

- **System is w10x64**
- Orders.exe (PID: 6824 cmdline: 'C:\Users\user\Desktop\Orders.exe' MD5: E85DAF3A43F107B213310A53BFD35AA9)
  - powershell.exe (PID: 6896 cmdline: 'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\Desktop\Orders.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$IT3ssl.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegAsm.exe (PID: 7000 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - hawkgoods.exe (PID: 7064 cmdline: 'C:\Users\user~1\AppData\Local\Temp\hawkgoods.exe' 0 MD5: FFDB58533D5D1362E896E96FB6F02A95)
      - dw20.exe (PID: 6008 cmdline: dw20.exe -x -s 2132 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
      - vbc.exe (PID: 6288 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
      - vbc.exe (PID: 976 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
        - WerFault.exe (PID: 6308 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 976 -s 176 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - WerFault.exe (PID: 2324 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7064 -s 2132 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - origigoods40.exe (PID: 7116 cmdline: 'C:\Users\user~1\AppData\Local\Temp\origigoods40.exe' 0 MD5: AE36F0D16230B9F41FFECBD3C5B1D660)
    - Matiexgoods.exe (PID: 7148 cmdline: 'C:\Users\user~1\AppData\Local\Temp\Matiexgoods.exe' 0 MD5: 80C61B903400B534858D047DD0919F0E)
      - netsh.exe (PID: 6780 cmdline: 'netsh' wlan show profile MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - conhost.exe (PID: 1404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - origigoods20.exe (PID: 5580 cmdline: 'C:\Users\user~1\AppData\Local\Temp\origigoods20.exe' 0 MD5: 61DC57C6575E1F3F2AE14C1B332AD2FB)
  - WerFault.exe (PID: 2116 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6824 -s 1104 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- I$s#$IT3ssl.exe (PID: 5184 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$IT3ssl.exe' MD5: E85DAF3A43F107B213310A53BFD35AA9)
  - powershell.exe (PID: 5296 cmdline: 'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$IT3ssl.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$IT3ssl.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegAsm.exe (PID: 5468 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - hawkgoods.exe (PID: 4388 cmdline: 'C:\Users\user~1\AppData\Local\Temp\hawkgoods.exe' 0 MD5: FFDB58533D5D1362E896E96FB6F02A95)
    - origigoods40.exe (PID: 5692 cmdline: 'C:\Users\user~1\AppData\Local\Temp\origigoods40.exe' 0 MD5: AE36F0D16230B9F41FFECBD3C5B1D660)
    - Matiexgoods.exe (PID: 6724 cmdline: 'C:\Users\user~1\AppData\Local\Temp\Matiexgoods.exe' 0 MD5: 80C61B903400B534858D047DD0919F0E)
    - origigoods20.exe (PID: 5612 cmdline: 'C:\Users\user~1\AppData\Local\Temp\origigoods20.exe' 0 MD5: 61DC57C6575E1F3F2AE14C1B332AD2FB)
  - WerFault.exe (PID: 2160 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5184 -s 1096 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: HawkEye

```
{
  "Modules": [
    "WebBrowserPassView",
    "mailpv",
    "Mail PassView"
  ],
  "Version": ""
}
```


Threatname: Agenttesla


```
{
  "Username: ": "",
  "URL: ": "",
  "To: ": "sales1@midombo.com",
  "ByHost: ": "smtp.privateemail.com:587",
  "Password: ": "",
  "From: ": "sales1@midombo.com"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\origigoods20.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Local\Temp\origigoods40.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x7423:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b8c7:$key: HawkEyeKeylogger • 0x7db0b:$salt: 099u787978786 • 0x7bf08:$string1: HawkEye_Keylogger • 0x7cd5b:$string1: HawkEye_Keylogger • 0x7da6b:$string1: HawkEye_Keylogger • 0x7c2f1:$string2: holdermail.txt • 0x7c311:$string2: holdermail.txt • 0x7c233:$string3: wallet.dat • 0x7c24b:$string3: wallet.dat • 0x7c261:$string3: wallet.dat • 0x7d62f:$string4: Keylog Records • 0x7d947:$string4: Keylog Records • 0x7db63:$string5: do not script --> • 0x7b8af:$string6: \pidloc.txt • 0x7b93d:$string7: BSPLIT • 0x7b94d:$string7: BSPLIT
Click to see the 4 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000025.00000000.399012238.0000000000E72000.00000002.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000017.00000002.450940492.0000000005360000.00000004.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x12df7:$key: HawkEyeKeylogger • 0x1503b:$salt: 099u787978786 • 0x13438:$string1: HawkEye_Keylogger • 0x1428b:$string1: HawkEye_Keylogger • 0x14f9b:$string1: HawkEye_Keylogger • 0x13821:$string2: holdermail.txt • 0x13841:$string2: holdermail.txt • 0x13763:$string3: wallet.dat • 0x1377b:$string3: wallet.dat • 0x13791:$string3: wallet.dat • 0x14b5f:$string4: Keylog Records • 0x14e77:$string4: Keylog Records • 0x15093:$string5: do not script --> • 0x12ddf:$string6: \pidloc.txt • 0x12e6d:$string7: BSPLIT • 0x12e7d:$string7: BSPLIT
00000017.00000002.450940492.0000000005360000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	

Source	Rule	Description	Author	Strings
00000017.00000002.450940492.000000000536 0000.00000004.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x13490:$hawkstr1: HawkEye Keylogger • 0x142d1:$hawkstr1: HawkEye Keylogger • 0x14600:$hawkstr1: HawkEye Keylogger • 0x1475b:$hawkstr1: HawkEye Keylogger • 0x148be:$hawkstr1: HawkEye Keylogger • 0x14b37:$hawkstr1: HawkEye Keylogger • 0x1301e:$hawkstr2: Dear HawkEye Customers! • 0x14653:$hawkstr2: Dear HawkEye Customers! • 0x147aa:$hawkstr2: Dear HawkEye Customers! • 0x14911:$hawkstr2: Dear HawkEye Customers! • 0x1313f:$hawkstr3: HawkEye Logger Details:
00000027.00000000.408264262.000000000053 2000.00000002.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 106 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.0.origigoods20.exe.680000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.0.hawkgoods.exe.670000.0.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x7423:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
6.0.hawkgoods.exe.670000.0.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b8c7:$key: HawkEyeKeylogger • 0x7db0b:$salt: 099u787978786 • 0x7bf08:$string1: HawkEye_Keylogger • 0x7cd5b:$string1: HawkEye_Keylogger • 0x7da6b:$string1: HawkEye_Keylogger • 0x7c2f1:$string2: holdermail.txt • 0x7c311:$string2: holdermail.txt • 0x7c233:$string3: wallet.dat • 0x7c24b:$string3: wallet.dat • 0x7c261:$string3: wallet.dat • 0x7d62f:$string4: Keylog Records • 0x7d947:$string4: Keylog Records • 0x7db63:$string5: do not script --> • 0x7b8af:$string6: \pidloc.txt • 0x7b93d:$string7: BSPLIT • 0x7b94d:$string7: BSPLIT
6.0.hawkgoods.exe.670000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
6.0.hawkgoods.exe.670000.0.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 43 entries				

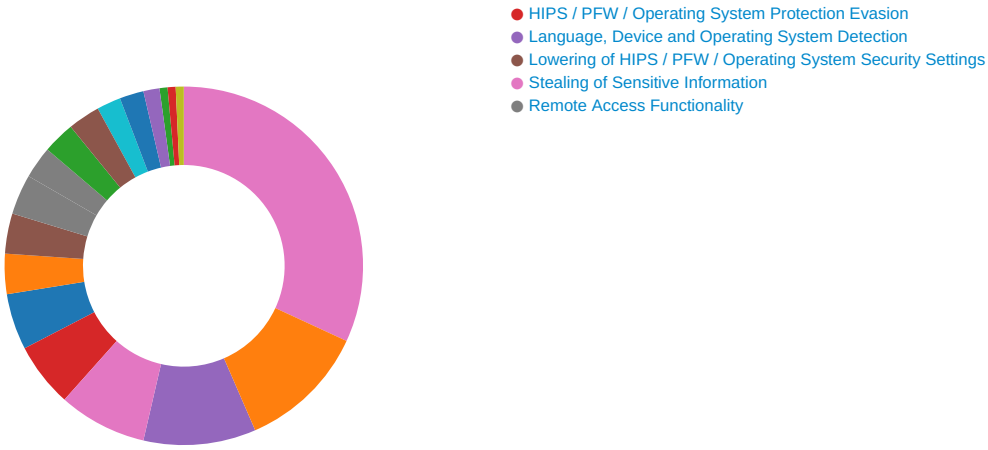
Sigma Overview

System Summary:

Sigma detected: Capture Wi-Fi password

Signature Overview

- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging



Click to jump to signature section

AV Detection:

- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Uses 32bit PE files
- Uses insecure TLS / SSL version for HTTPS connection
- Uses new MSVCR Dlls
- Contains modern PE file flags such as dynamic base (ASLR) or NX
- Binary contains paths to debug symbols

Networking:

- May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected HawkEye Keylogger
- Contains functionality to log keystrokes (.Net Source)
- Installs a global keyboard hook

System Summary:

- Malicious sample detected (through community Yara rule)
- .NET source code contains very large array initializations
- Initial sample is a PE file and has a suspicious name
- Powershell drops PE file

Data Obfuscation:

- .NET source code contains potential unpacker
- Binary contains a suspicious time stamp

Boot Survival:

Drops PE files to the startup folder

Hooking and other Techniques for Hiding and Protection:

Changes the view of files in windows explorer (hidden files and folders)

Malware Analysis System Evasion:

Yara detected AntiVM_3

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Opens the same file many times (likely Sandbox evasion)

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

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Bypasses PowerShell execution policy

Injects a PE file into a foreign processes

Sample uses process hollowing technique

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected HawkEye Keylogger

Yara detected MailPassView

Yara detected Matiex Keylogger

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal WLAN passwords

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Detected HawkEye Rat

Yara detected AgentTesla

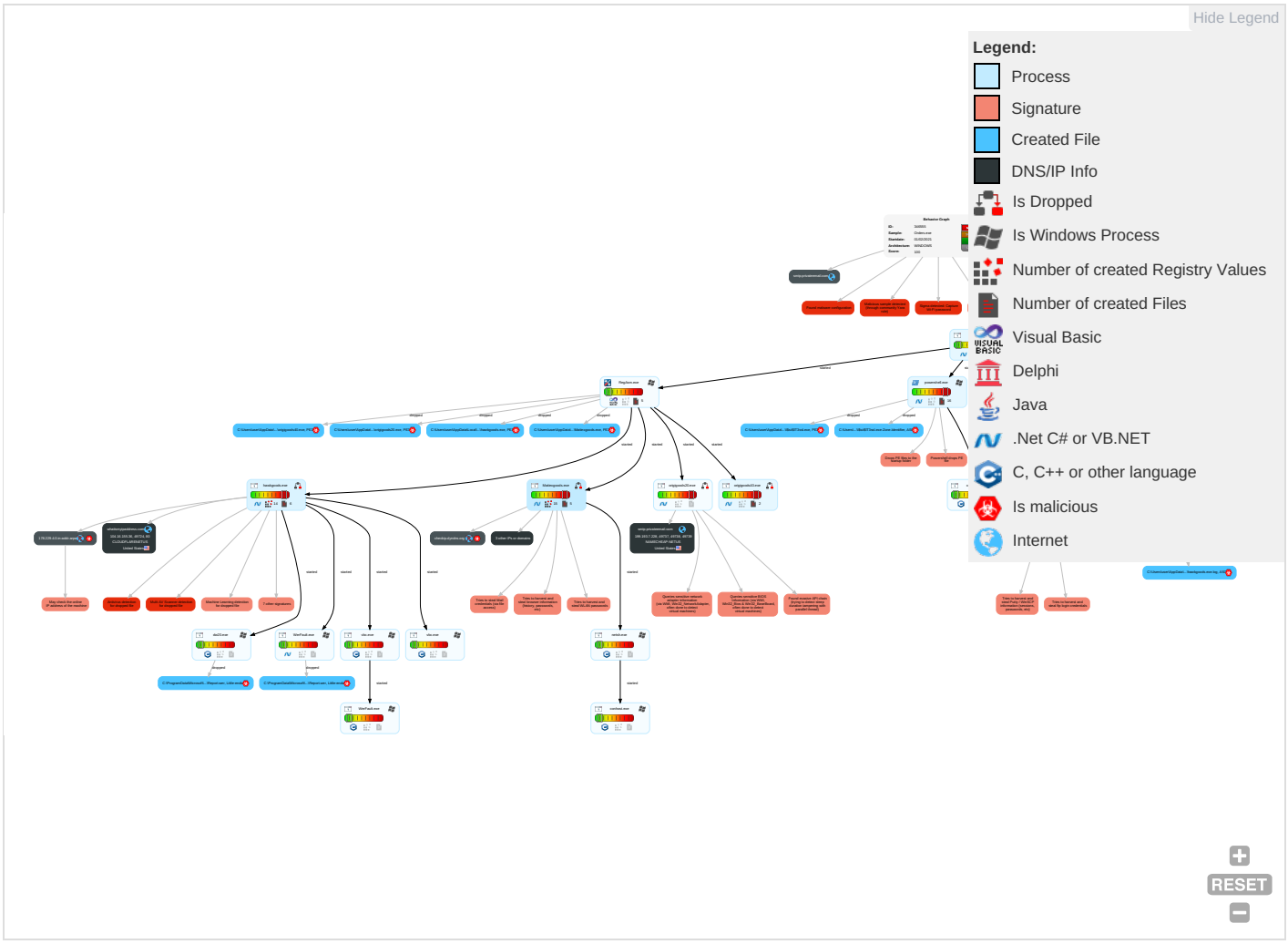
Yara detected HawkEye Keylogger

Yara detected Matiex Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Replication Through Removable Media 1	Windows Management Instrumentation 2 3 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 2 1 1	OS Credential Dumping 2	Peripheral Device Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Network Mediu
Default Accounts	Native API 2	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 1 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	Shared Modules 1	Registry Run Keys / Startup Folder 1 2	Access Token Manipulation 1	Obfuscated Files or Information 4 1	Credentials in Registry 1	System Information Discovery 1 2 6	SMB/Windows Admin Shares	Email Collection 1	Automated Exfil
Local Accounts	Command and Scripting Interpreter 1	Logon Script (Mac)	Process Injection 4 1 1	Software Packing 1 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 2 1 1	Scheduled Trar
Cloud Accounts	PowerShell 2	Network Logon Script	Registry Run Keys / Startup Folder 1 2	Timestomp 1	LSA Secrets	Security Software Discovery 2 6 1	SSH	Clipboard Data 1	Data Transfer S Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 6	VNC	GUI Input Capture	Exfiltration Over Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Prot
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2 6	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encr Non-C2 Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric En Non-C2 Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 4 1 1	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Ol Non-C2 Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Mediu

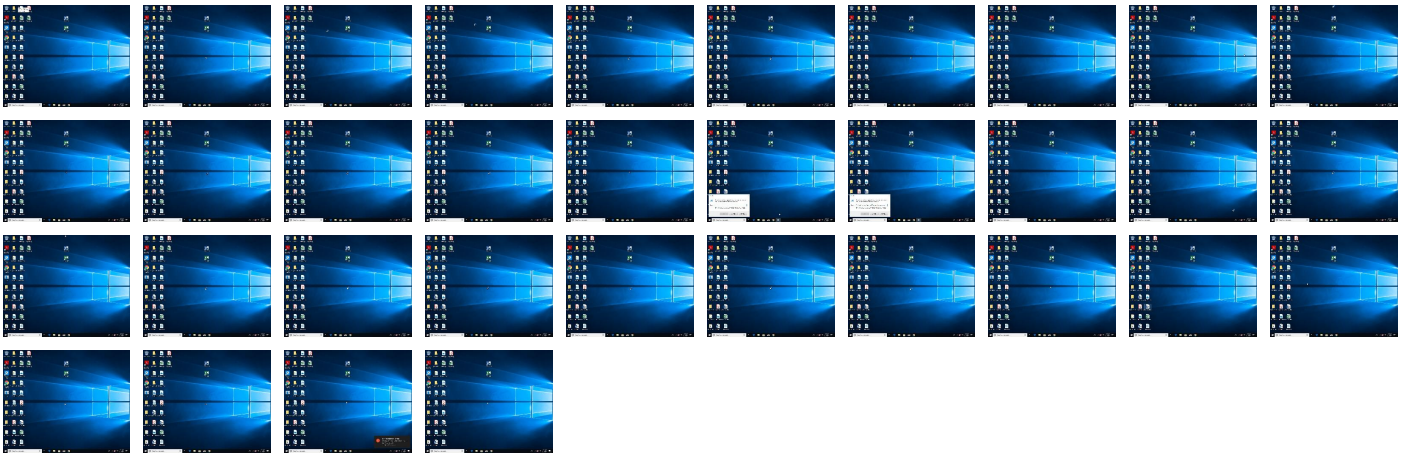
Behavior Graph



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
Orders.exe	22%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Orders.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	100%	Avira	TR/AD.MExecute.lzrac	
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	100%	Avira	SPR/Tool.MailPassView.473	
C:\Users\user\AppData\Local\Temp\origigoods40.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	100%	Avira	TR/Redcap.jajcu	
C:\Users\user\AppData\Local\Temp\origigoods20.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\l$s#$lT3ssl.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\origigoods40.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\origigoods20.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	86%	ReversingLabs	ByteCode-MSIL.Trojan.MatiexKeylogger	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	96%	ReversingLabs	ByteCode-MSIL.Trojan.Golroted	
C:\Users\user\AppData\Local\Temp\origigoods20.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\origigoods20.exe	86%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
C:\Users\user\AppData\Local\Temp\origigoods40.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\origigoods40.exe	83%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\l$s#$lT3ssl.exe	22%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.0.origigoods20.exe.680000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
6.0.hawkgoods.exe.670000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
6.0.hawkgoods.exe.670000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
39.0.origigoods20.exe.530000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
36.0.hawkgoods.exe.3d0000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
36.0.hawkgoods.exe.3d0000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
37.0.origigoods40.exe.e70000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
8.2.origigoods40.exe.f0000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
8.0.origigoods40.exe.f0000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
38.0.Matiexgoods.exe.6e0000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
33.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
33.2.RegAsm.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
33.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
33.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
4.2.RegAsm.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
4.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
4.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.Matiexgoods.exe.320000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
10.2.origigoods20.exe.680000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
6.2.hawkgoods.exe.670000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
6.2.hawkgoods.exe.670000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
36.2.hawkgoods.exe.3d0000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
36.2.hawkgoods.exe.3d0000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://tempuri.org/DataSet1.xsd	0%	Avira URL Cloud	safe	
http://www.carterandcone.comva	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://csARxe.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/r-t	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/-	0%	Avira URL Cloud	safe	
http://www.tiro.comBs	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	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://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/U	0%	Avira URL Cloud	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.fontbureau.comaU	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.fontbureau.comituF	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/-	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/e	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/e	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/e	0%	URL Reputation	safe	
http://www.carterandcone.comri	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/H	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://en.wikipnrC	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png8	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnE	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.155.36	true	false		high
freegeoip.app	172.67.188.154	true	false		unknown
smtp.privateemail.com	199.193.7.228	true	false		high
checkip.dyndns.com	216.146.43.71	true	false		unknown
178.229.4.0.in-addr.arpa	unknown	unknown	true		unknown
checkip.dyndns.org	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	origigoods40.exe, 00000008.00000002.445240887.0000000002501000.00000004.00000001.sdmp, origigoods20.exe, 0000000A.00000002.448946669.0000000002E51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddresshttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high
http://tempuri.org/DataSet1.xsd	Orders.exe, powershell.exe, 00000002.00000003.344051726.0000000009925000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comva	hawkgoods.exe, 00000006.00000003.258405247.0000000005480000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

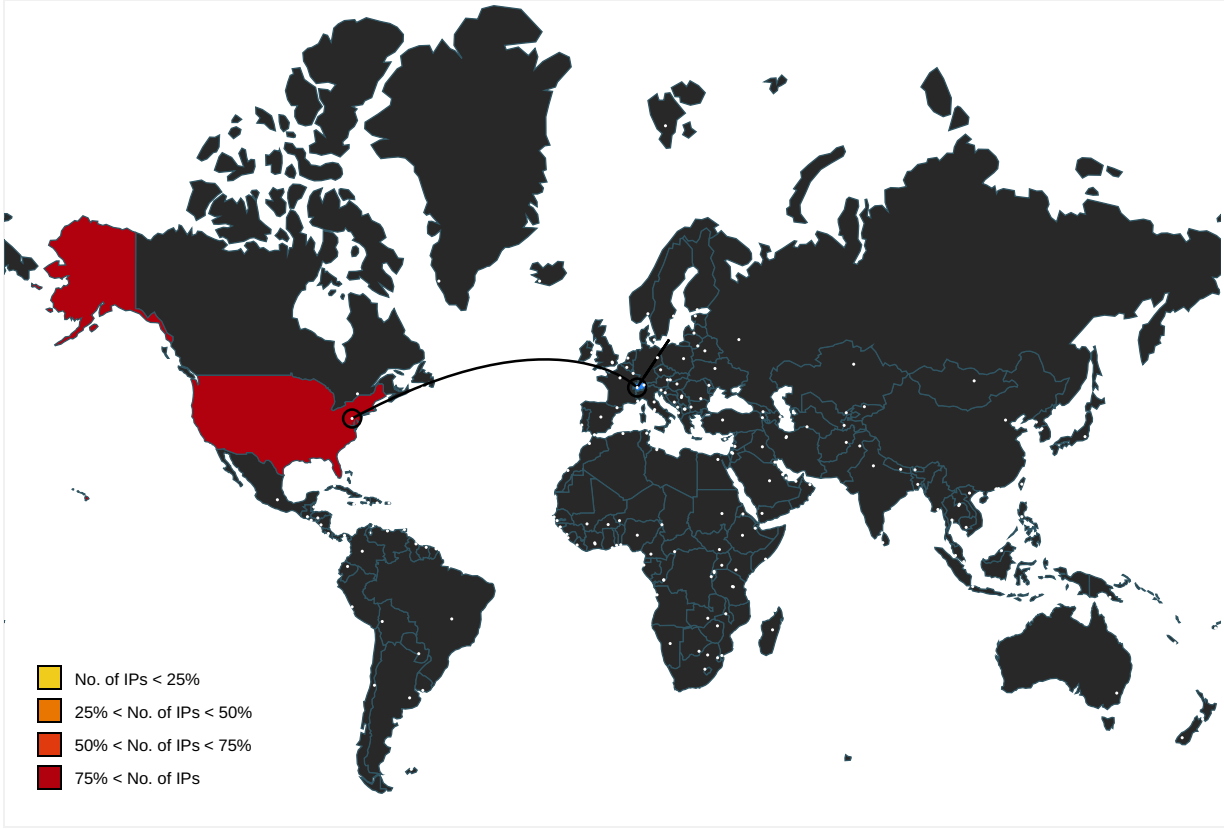
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false		high
http://ns.adobe.c/g	Matiexgoods.exe, 00000009.00000003.390945104.0000000000A11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://csARxe.com	origigoods40.exe, 00000008.00000002.445240887.0000000002501000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/r-t	hawkgoods.exe, 00000006.00000003.260284177.0000000005459000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/-	hawkgoods.exe, 00000006.00000003.261120195.0000000005457000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000002.00000002.371690291.0000000006045000.00000004.00000001.sdmp	false		high
http://www.tiro.comBs	hawkgoods.exe, 00000006.00000003.258792974.000000000545B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com/-	Orders.exe, 00000001.00000002.361141701.0000000004154000.00000004.00000001.sdmp, RegAsm.exe, 00000004.00000003.246774488.0000000003670000.00000004.00000001.sdmp, hawkgoods.exe, 00000006.00000000.249359249.00000000000672000.00000002.00020000.sdmp, WerFault.exe, 00000017.00000002.450940492.0000000005360000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.site.com/logs.php	hawkgoods.exe, 00000006.00000002.498581730.0000000002E11000.00000004.00000001.sdmp	false		high
http://www.urwpp.deDPlease	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	hawkgoods.exe, 00000006.00000002.503829429.0000000003E11000.00000004.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000002.00000002.360238676.0000000004FE1000.00000004.00000001.sdmp, WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high
http://www.carterandcone.como.	hawkgoods.exe, 00000006.00000003.257987873.0000000005480000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Orders.exe, 00000001.00000002.361141701.0000000004154000.00000004.00000001.sdmp, RegAsm.exe, 00000004.00000003.251635347.0000000003EBD000.00000004.00000001.sdmp, origigoods40.exe, origigoods20.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	origigoods20.exe, 0000000A.00000002.450298777.0000000002EBD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coma	hawkgoods.exe, 00000006.00000003.258405247.0000000005480000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/U	hawkgoods.exe, 00000006.00000003.261120195.0000000005457000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.come	hawkgoods.exe, 00000006.00000003.258405247.0000000005480000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000002.00000002.362042809.0000000005122000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobj	Matiexgoods.exe, 00000009.00000003.390945104.0000000000A11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	origigoods20.exe, 0000000A.00000002.448946669.0000000002E51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000002.00000002.362042809.0000000005122000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comaU	hawkgoods.exe, 00000006.00000002.509667210.0000000005450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000002.00000002.371690291.0000000006045000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/H	hawkgoods.exe, 00000006.00000003.260284177.0000000005459000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000002.00000002.362042809.0000000005122000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	hawkgoods.exe, 00000006.00000003.257505914.000000000547F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comituF	hawkgoods.exe, 00000006.00000003.269541699.000000000545A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/-	hawkgoods.exe, 00000006.00000003.259781833.0000000005456000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/e	hawkgoods.exe, 00000006.00000003.261120195.0000000005457000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comri	hawkgoods.exe, 00000006.00000003.258445747.000000000545B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	origigoods20.exe, 0000000A.00000002.450298777.0000000002EBD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/H	hawkgoods.exe, 00000006.00000003.261120195.0000000005457000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000002.00000002.371690291.0000000006045000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.wikipnrC	hawkgoods.exe, 00000006.00000003.258792974.000000000545B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	hawkgoods.exe, 00000006.00000003.258405247.0000000005480000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddressżhttp://schemas.xmlsoap.org/ws/20	WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png8	powershell.exe, 00000002.00000002.362042809.0000000005122000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnE	hawkgoods.exe, 00000006.00000003.256876634.000000000545B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comE	hawkgoods.exe, 00000006.00000003.258405247.0000000005480000.00000004.00000001.sdmp	false		unknown
http://www.jiyu-kobo.co.jp/-ca	hawkgoods.exe, 00000006.00000003.261120195.0000000005457000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comxIC	hawkgoods.exe, 00000006.00000003.257505914.000000000547F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000002.00000002.371690291.0000000006045000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cna	hawkgoods.exe, 00000006.00000003.257048632.000000000547F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	origigoods20.exe, 0000000A.00000002.448946669.0000000002E51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://login.yahoo.com/config/login	hawkgoods.exe	false		high
http://www.fonts.com	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester8	powershell.exe, 00000002.00000002.362042809.0000000005122000.00000004.00000001.sdmp	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000002.00000002.371690291.0000000006045000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNS	origigoods20.exe, 0000000A.00000002.448946669.0000000002E51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	origigoods20.exe, 0000000A.00000002.450298777.0000000002EBD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comH	hawkgoods.exe, 00000006.00000002.509667210.0000000005450000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTex	hawkgoods.exe, 00000006.00000003.258445747.000000000545B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high
http://whatismyipaddress.com	hawkgoods.exe, 00000006.00000002.498581730.0000000002E11000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/	hawkgoods.exe, 00000006.00000003.261120195.0000000005457000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comicrtg	hawkgoods.exe, 00000006.00000003.258445747.000000000545B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcoderhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html8	powershell.exe, 00000002.00000002.362042809.0000000005122000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.usertrust.	origigoods20.exe, 0000000A.00000002.512148799.0000000006BA0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	hawkgoods.exe, 00000006.00000003.261120195.0000000005457000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	hawkgoods.exe, 00000006.00000003.257893151.0000000005480000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://yQFlsb.com	origigoods20.exe, 0000000A.00000002.448946669.0000000002E51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	hawkgoods.exe, 00000006.00000002.510169583.0000000005540000.00000002.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprintrhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000000B.00000003.278054941.0000000005550000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
131.186.161.70	unknown	United States		33517	DYNDNSUS	false
104.16.155.36	unknown	United States		13335	CLOUDFLARENETUS	false
199.193.7.228	unknown	United States		22612	NAMECHEAP-NETUS	false
216.146.43.71	unknown	United States		33517	DYNDNSUS	false
172.67.188.154	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	346555
Start date:	01.02.2021
Start time:	09:07:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 18m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Orders.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@42/37@63/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.5% (good quality ratio 0.3%) • Quality average: 42.5% • Quality standard deviation: 36.7%
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: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, WerFault.exe, SgrmBroker.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.43.193.48, 92.122.144.200, 40.88.32.150, 51.104.139.180, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.142.210, 168.61.161.212, 51.103.5.186, 13.88.21.125 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, client.wns.windows.com, fs.microsoft.com, arc.msn.com.nsatc.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus15.cloudapp.net, emea1.wns.notify.trafficmanager.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report creation exceeded maximum time and may have missing behavior and disassembly information. • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/346555/sample/Orders.exe

Simulations

Behavior and APIs

Time	Type	Description
09:09:04	API Interceptor	637x Sleep call for process: origigoods20.exe modified
09:09:06	API Interceptor	847x Sleep call for process: origigoods40.exe modified
09:09:08	API Interceptor	6x Sleep call for process: hawkgoods.exe modified
09:09:13	API Interceptor	1x Sleep call for process: dw20.exe modified
09:09:21	API Interceptor	46x Sleep call for process: powershell.exe modified
09:09:24	API Interceptor	956x Sleep call for process: Matiexgoods.exe modified
09:09:28	API Interceptor	4x Sleep call for process: WerFault.exe modified
09:09:38	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\l$s#$lT3ssl.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
131.186.161.70	Hydro-463459.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	CHIKWA (2).exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	payment status.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	IMG_10966.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	85H8KnUuMM.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SecuriteInfo.com.Trojan.Packed2.42783.3265.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SecuriteInfo.com.Trojan.Packed2.42783.17593.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SecuriteInfo.com.Trojan.Packed2.42783.24703.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Ewqm21lwdh.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	a4iz7zkilq.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Vcg9GH4CWw.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	nMn5eAMhBy.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	sSPHg0Y2cZ.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	vK6VPijMoq.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	COA for PI#Sc09283,PDF.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Quotation for T10495.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	file.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Revised Invoice.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	INVO_0000765346700.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	2Ul5CJzIrl.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
104.16.155.36	nzGUqSK11D.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	hkaP5RPCGNDVq3Z.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NDt93WWQwd089H7.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	INQUIRY.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Prueba de pago.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	6JLHKYvboo.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	jSMd8npgmU.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	9vdouqRTh3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	5pB35gGfZ5.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	fyxC4Hgs3s.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	yk94P18VKp.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	oLHQIQAI3N.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	WuGzF7ZJ7P.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NXmokFkh3R.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
whatismyipaddress.com	nzGUqSK11D.exe	Get hash	malicious	Browse	• 104.16.154.36
	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• 104.16.155.36
	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• 104.16.155.36
	hkaP5RPCGNDVq3Z.exe	Get hash	malicious	Browse	• 104.16.155.36
	B6LNCKjOGt5EmFQ.exe	Get hash	malicious	Browse	• 104.16.154.36
	NDt93WWQwd089H7.exe	Get hash	malicious	Browse	• 104.16.155.36
	JkhR5oeRHA.exe	Get hash	malicious	Browse	• 66.171.248.178
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 104.16.155.36
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• 104.16.154.36
	INQUIRY.exe	Get hash	malicious	Browse	• 104.16.154.36
	Prueba de pago.exe	Get hash	malicious	Browse	• 104.16.155.36
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	http://https://my-alliances.co.uk/	Get hash	malicious	Browse	• 66.171.248.178
	c9o0CtTIYT.exe	Get hash	malicious	Browse	• 104.16.154.36
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• 104.16.155.36
	6JLHKYvboo.exe	Get hash	malicious	Browse	• 104.16.155.36
	jSMd8npgmU.exe	Get hash	malicious	Browse	• 104.16.155.36
freegeoip.app	Hydro-463459.exe	Get hash	malicious	Browse	• 172.67.188.154
	Payment Document.exe	Get hash	malicious	Browse	• 172.67.188.154
	CHIKWA (2).exe	Get hash	malicious	Browse	• 104.21.19.200
	gGQWGJWR4jzvzse.exe	Get hash	malicious	Browse	• 104.21.19.200
	file.exe	Get hash	malicious	Browse	• 104.21.19.200
	PURCHASE ORDER..exe	Get hash	malicious	Browse	• 104.21.19.200
	my new file ify (1).exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_166390pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	PAYMENT DETAILS.exe	Get hash	malicious	Browse	• 104.21.19.200
	payment status.exe	Get hash	malicious	Browse	• 172.67.188.154
	file.exe	Get hash	malicious	Browse	• 172.67.188.154
	customer Telex Transfer(TT).exe	Get hash	malicious	Browse	• 172.67.188.154
	Agent Statement CargoPro.exe	Get hash	malicious	Browse	• 104.21.19.200
	PURCHASE ORDER#34556558.exe	Get hash	malicious	Browse	• 104.21.19.200

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	910023458.exe	Get hash	malicious	Browse	• 104.21.19.200
	Product_Catalogue,PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_10966.exe	Get hash	malicious	Browse	• 104.21.19.200
	file.exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_05752003.exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_058741601.exe	Get hash	malicious	Browse	• 172.67.188.154
smtp.privateemail.com	document.doc	Get hash	malicious	Browse	• 199.193.7.228
	order.exe	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Trojan.Packed2.42809.8145.exe	Get hash	malicious	Browse	• 199.193.7.228
	DHL-ADDRESS.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	weg6tX6TTk78XZ5.exe	Get hash	malicious	Browse	• 199.193.7.228
	odT0zoYLJiNUQXd.exe	Get hash	malicious	Browse	• 199.193.7.228
	hkaP5RPCGNDVq3Z.exe	Get hash	malicious	Browse	• 199.193.7.228
	B6LNCKjOGt5EmFQ.exe	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe	Get hash	malicious	Browse	• 199.193.7.228
	DHL-Address.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	shipping-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	iVUeQOg6LO.exe	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Generic.mg.e92f0e2d08762687.exe	Get hash	malicious	Browse	• 199.193.7.228
	DHL-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	wCRnCAMZ3yT8BQ2.exe	Get hash	malicious	Browse	• 199.193.7.228
	Mj1eX5GWJxDRnuk.exe	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Trojan.Inject4.6535.8815.exe	Get hash	malicious	Browse	• 199.193.7.228
	shipping document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Trojan.Inject4.6512.28917.exe	Get hash	malicious	Browse	• 199.193.7.228
	p72kooG5ak.exe	Get hash	malicious	Browse	• 199.193.7.228

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	DHL_document11022020680908911.doc.exe	Get hash	malicious	Browse	• 198.54.122.60
	DHL Details.exe	Get hash	malicious	Browse	• 198.54.126.165
	order.doc	Get hash	malicious	Browse	• 199.188.201.34
	aOn5CfTiwS.exe	Get hash	malicious	Browse	• 198.54.117.244
	PO_55004.exe	Get hash	malicious	Browse	• 68.65.122.156
	SecuriteInfo.com.Trojan.MulDrop16.10041.23448.exe	Get hash	malicious	Browse	• 185.61.153.111
	SecuriteInfo.com.Trojan.Inject4.6821.6799.exe	Get hash	malicious	Browse	• 199.188.20 0.150
	DCAjXz5y4I.exe	Get hash	malicious	Browse	• 162.213.25 5.196
	NEW ORDER.xlsm	Get hash	malicious	Browse	• 104.219.248.89
	Claim_250196008_01282021.xls	Get hash	malicious	Browse	• 162.0.226.110
	Claim_250196008_01282021.xls	Get hash	malicious	Browse	• 162.0.226.110
	lbqFKoALqe.exe	Get hash	malicious	Browse	• 198.54.117.215
	j64eIR1IEK.exe	Get hash	malicious	Browse	• 198.54.117.210
	document.doc	Get hash	malicious	Browse	• 199.193.7.228
	CMA CGM Shipping Documents COAU7014424560.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	order.exe	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Heur.11979.xls	Get hash	malicious	Browse	• 162.0.226.110
	SecuriteInfo.com.Heur.11979.xls	Get hash	malicious	Browse	• 162.0.226.110
	#Ud83d#Udce9.htm	Get hash	malicious	Browse	• 198.54.115.249
	Pending Orders Statement -40064778.doc	Get hash	malicious	Browse	• 198.54.122.60
CLOUDFLARENETUS	Vietcong Order February.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	Hydro-463459.exe	Get hash	malicious	Browse	• 172.67.188.154
	Fature.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	Payment Document.exe	Get hash	malicious	Browse	• 172.67.188.154
	CHIKWA (2).exe	Get hash	malicious	Browse	• 172.67.188.154
	Orden revisada PO-WJO-001, pdf.exe	Get hash	malicious	Browse	• 162.159.13 4.233
	gGQWGJWR4jzvzse.exe	Get hash	malicious	Browse	• 104.21.19.200
	2021BLL0201.doc__.rtf	Get hash	malicious	Browse	• 172.67.219.133
	order.doc	Get hash	malicious	Browse	• 172.67.219.133
	InfoSender.exe	Get hash	malicious	Browse	• 162.159.13 6.232
	cbUJVTVJ.exe	Get hash	malicious	Browse	• 104.23.99.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.Packed2.42783.20578.exe	Get hash	malicious	Browse	• 104.23.98.190
	INWARD-OUTWARD ANALYSIS.xlsx	Get hash	malicious	Browse	• 104.23.98.190
	e7zQwqIDCO.exe	Get hash	malicious	Browse	• 104.21.15.91
	Doc29012010.xls	Get hash	malicious	Browse	• 162.159.13 5.233
	file.exe	Get hash	malicious	Browse	• 172.67.188.154
	PURCHASE ORDER..exe	Get hash	malicious	Browse	• 104.21.19.200
	my new file ify (1).exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_166390pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	PAYMENT DETAILS.exe	Get hash	malicious	Browse	• 104.21.19.200
DYNDNSUS	Hydro-463459.exe	Get hash	malicious	Browse	• 131.186.161.70
	Payment Document.exe	Get hash	malicious	Browse	• 216.146.43.71
	CHIKWA (2).exe	Get hash	malicious	Browse	• 131.186.161.70
	gGQWGJWR4jzvzse.exe	Get hash	malicious	Browse	• 216.146.43.70
	file.exe	Get hash	malicious	Browse	• 216.146.43.70
	PURCHASE ORDER..exe	Get hash	malicious	Browse	• 216.146.43.70
	my new file ify (1).exe	Get hash	malicious	Browse	• 216.146.43.70
	IMG_166390pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	PAYMENT DETAILS.exe	Get hash	malicious	Browse	• 216.146.43.70
	payment status.exe	Get hash	malicious	Browse	• 131.186.161.70
	file.exe	Get hash	malicious	Browse	• 216.146.43.70
	customer Telex Transfer(TT).exe	Get hash	malicious	Browse	• 216.146.43.71
	Agent Statement CargoPro.exe	Get hash	malicious	Browse	• 162.88.193.70
	PURCHASE ORDER#34556558.exe	Get hash	malicious	Browse	• 216.146.43.71
	910023458.exe	Get hash	malicious	Browse	• 216.146.43.71
	Product_Catalogue,PDF.exe	Get hash	malicious	Browse	• 216.146.43.70
	IMG_10966.exe	Get hash	malicious	Browse	• 131.186.161.70
	file.exe	Get hash	malicious	Browse	• 216.146.43.70
	IMG_05752003.exe	Get hash	malicious	Browse	• 216.146.43.70
	IMG_058741601.exe	Get hash	malicious	Browse	• 216.146.43.71

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	Hydro-463459.exe	Get hash	malicious	Browse	• 172.67.188.154
	Payment Document.exe	Get hash	malicious	Browse	• 172.67.188.154
	CHIKWA (2).exe	Get hash	malicious	Browse	• 172.67.188.154
	gGQWGJWR4jzvzse.exe	Get hash	malicious	Browse	• 172.67.188.154
	cbUJVTVJ.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Trojan.Packed2.42783.20578.exe	Get hash	malicious	Browse	• 172.67.188.154
	file.exe	Get hash	malicious	Browse	• 172.67.188.154
	PURCHASE ORDER..exe	Get hash	malicious	Browse	• 172.67.188.154
	my new file ify (1).exe	Get hash	malicious	Browse	• 172.67.188.154
	IMG_166390pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	PAYMENT DETAILS.exe	Get hash	malicious	Browse	• 172.67.188.154
	payment status.exe	Get hash	malicious	Browse	• 172.67.188.154
	file.exe	Get hash	malicious	Browse	• 172.67.188.154
	customer Telex Transfer(TT).exe	Get hash	malicious	Browse	• 172.67.188.154
	Agent Statement CargoPro.exe	Get hash	malicious	Browse	• 172.67.188.154
	PURCHASE ORDER#34556558.exe	Get hash	malicious	Browse	• 172.67.188.154
	910023458.exe	Get hash	malicious	Browse	• 172.67.188.154
	Product_Catalogue,PDF.exe	Get hash	malicious	Browse	• 172.67.188.154
	IMG_10966.exe	Get hash	malicious	Browse	• 172.67.188.154
	file.exe	Get hash	malicious	Browse	• 172.67.188.154

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_I$s#$lT3ssl.exe_475c1b6650cb1237ccbea93f193b5c1a2bf60cf_f556f9f0_08026e6f\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13900
Entropy (8bit):	3.773983523806153
Encrypted:	false
SSDEEP:	192:u25OV0nrZHBUZMXCaKYQ/u7sKS274lt+6:X5OV0n1BUZMXCaA/u7sKX4lt+6
MD5:	FB2F2036931CB1395C726988B97D875D
SHA1:	603F71DACEF6685982C26933F3E6F8BED3CCE4CA
SHA-256:	2BBB1DCCB832D08D4162F1863ECC53F9F5DFF935C477B3092BBFDBA778882E6E
SHA-512:	69695CD6B357E1C8A25E042050AD9FECCC69EFFD808E87544BB5DC4F3434DC32650AC6D4B2BA563C0AF75E6871EBA14C7DDF6739014EAD24B9E572A993D66CF
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.6.7.3.0.0.8.1.4.0.1.3.3.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.6.6.7.3.0.5.8.2.3.3.6.8.8.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.5.0.3.3.2.1.0.-.1.1.c.f.-.4.d.c.c.-.8.4.8.d.-.0.b.c.b.b.6.2.c.b.d.3.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.e.7.7.b.a.1.a.-.e.7.3.e.-.4.0.3.1.-.b.7.e.1.-.b.7.2.3.b.e.e.2.0.b.a.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.I.$.s.#.$.l.T.3.s.s.l...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.m.D.O.r.G.S.K.g.i.V...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.4.0.-.0.0.0.1.-.0.0.1.7.-.e.0.8.2.-.d.1.0.b.b.d.f.8.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.4.5.c.e.2.d.b.6.3.d.3.6.8.1.b.5.5.3.1.3.2.2.4.8.7.c.a.5.d.f.5.0.0.0.0.0.0.0.0.!.0.0.0.0.0.4.2.2.0.8.c.7.a.2.3.2.b.8.0.6.c.6.3.8.2.e.3.4.4.1.7.f.9.c.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Orders.exe_c173c4d7306a40d1422278d49383db0ef5e6f35_c446bb0c_083415f8\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13506
Entropy (8bit):	3.7675454560927717
Encrypted:	false
SSDEEP:	192:K4wuaqn4eZHBUZMXKaKYQ/u7s0S274ltVF:muaqn/BUZMXKaA/u7s0X4ltVF
MD5:	B90004AF7E82B0DF2BC9ED745227951B
SHA1:	6A2160DFFA308B06AEBC5D6C821D51E23FF15DA8
SHA-256:	5CBD7E729F68357E272E73C76ECECEBEFC7774A14C3E549140CFE9D9E401FEDC
SHA-512:	562CCEA7499253B5DBB2E9266F687ADFD70265A197EBFEADC08DB5D66CABD03569F6060A1908E4C3E0DE6D31412CAF4F290DB2778C3183B093CDB3FB9632E316
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.6.7.2.9.4.0.6.5.5.8.9.1.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.6.6.7.2.9.5.6.4.0.5.8.4.5.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.b.7.f.f.3.c.3.-.b.6.e.d.-.4.b.8.a.-.8.1.4.f.-.6.f.6.7.6.0.4.6.e.4.a.5.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.6.1.1.c.6.1.9.-.6.7.7.6.-.4.4.6.d.-.a.6.1.b.-.c.8.9.7.7.3.8.e.4.f.a.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.O.r.d.e.r.s...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.m.D.O.r.G.S.K.g.i.V...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.a.8.-.0.0.0.1.-.0.0.1.7.-.6.a.7.a.-.4.c.e.6.b.c.f.8.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.4.5.c.e.2.d.b.6.3.d.3.6.8.1.b.5.5.3.1.3.2.2.4.8.7.c.a.5.d.f.5.0.0.0.0.0.0.0.0.!.0.0.0.0.0.4.2.2.0.8.c.7.a.2.3.2.b.8.0.6.c.6.3.8.2.e.3.4.4.1.7.f.9.c.8.e.2.a.9.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_hawkgoods.exe_697020edb13ed8bc761f5d6b0de413dddfcbfb_b4666e22_09649e14\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	17914
Entropy (8bit):	3.766572763101044
Encrypted:	false
SSDEEP:	192:HMQL3pHBUZMXJyBaKsn9fbeN9M2v1zzvSXk0ZKjBIcQr+s/u7s0S274ltmxep:sQL3ZBUZMXiaEdvh/sl/u7s0X4ltOU
MD5:	540A1076AB927D79958E459AD3D1B4DC
SHA1:	B534C3A5A908AB697FEB4DF17DF2843B71E12088
SHA-256:	C591AF951213C92380B428C2A746A8FE019B2C29E1BE7466D0AF7D32E8CB5033
SHA-512:	7CECC337A7ED4CF8477FFE8CC35F8DDE7343777FAC67232F77D506B78EFEC9652930F288FD708BFC87550F667C5FBA4EC492FB39EC553A08D74993A99940891
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.6.7.2.9.6.4.0.4.6.4.5.2.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.6.6.7.2.9.8.8.4.3.7.0.0.5.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.0.d.8.5.3.5.6.-.2.5.c.8.-.4.8.3.7.-.9.f.4.b.-.a.6.f.b.6.a.6.d.5.4.7.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.5.9.3.5.1.1.3.-.9.5.a.8.-.4.b.b.3.-.b.9.f.7.-.8.d.a.c.a.e.1.2.6.f.2.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.h.a.w.k.g.o.o.d.s...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.P.h.u.l.l.i...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.9.8.-.0.0.0.1.-.0.0.1.7.-.3.6.6.1.-.2.f.e.a.b.c.f.8.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.6.c.c.9.4.0.d.7.a.0.d.3.0.a.e.2.8.3.f.a.7.7.b.e.8.f.e.6.4.d.3.0.0.0.0.0.0.0.0.!.0.0.0.0.d.6.e.4.a.3.c.a.2.5.3.b.f.c.3.7.2.a.9.a.3.1.8.0.b.5.8.8.7.c.7.1.6.e.d.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_hawkgoods.exe_93f07d9c4f92cda17563b29cabdf995c588ef9_00000000_1717da56\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_hawkgoods.exe_93f07d9c4f92cda17563b29cabdf995c588ef9_00000000_1717da56\Report.wer	
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16962
Entropy (8bit):	3.757340103474675
Encrypted:	false
SSDEEP:	192:xAg8QpQmV4yBaKsn9fbeN9M2v1zzvSXk0ZKjBIcQry/u7sOS274Itik:YQpQSaEdvh/sy/u7sOX4Itd
MD5:	5BD987FF56CF22B445B08ADBE0CEB94F
SHA1:	392A4A18E1FBF20D71EB44502A2E308C8B7D1FC2
SHA-256:	45BF7A559B278FBE5A6DC08AEFF4A289EC7CB1A022092832189F023C5AEBE91A
SHA-512:	56F5B005A65A94FEE33F8CB706B1D762A6B1103116758C2712408808F7F9968845855ECF1A633C39B97BF9BF94C59DD3191934D88E9AD2C468163E2D06FA4710
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.6.7.2.9.4.9.3.4.3.3.6.4.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.6.6.7.2.9.5.1.2.0.2.7.3.6.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.a.a.a.2.c.b.9.-.f.8.d.1.-.4.e.4.d.-.b.8.a.4.-.c.6.6.1.f.0.3.8.b.d.9.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.P.h.u.l.l.i...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.9.8.-.0.0.0.1.-.0.0.1.7.-.3.6.6.1.-.2.f.e.a.b.c.f.8.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.6.c.c.9.4.0.d.7.a.0.d.3.0.a.e.2.8.3.f.a.7.7.b.e.8.f.e.6.4.d.3.0.0.0.0.0.0.0.0.!.0.0.0.0.d.6.e.4.a.3.c.a.2.5.3.b.f.c.3.7.2.a.9.a.3.1.8.0.b.5.8.8.7.c.7.1.6.e.d.2.8.5.c.6.!.h.a.w.k.g.o.o.d.s...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.1././.1.9.:.1.0.:.0.8.:.3.8.!.0.!.h.a.w.k.g.o.o.d.s...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5...

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_fcdf79ff79f329d98f696167290ab3ea8a293_6c16ead4_18d4c207\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7796
Entropy (8bit):	3.767893341675678
Encrypted:	false
SSDEEP:	192:2wXKDmdHBUZMXQf9jY/u7s0S274ItE7GDB9:d6DEBUZMXojY/u7s0X4ItEOL
MD5:	958A2DD731FC8F6B1C9B021FE1834AF7
SHA1:	2DBD2A5C3C4C23B37A80BE7B98E72EA0E50C1BE6
SHA-256:	189108BF5EB1E837E15F6DACAEE0455BC60449B930A2E713BDB17224B996D924
SHA-512:	78448CFE3ECAC8ECF1A8A0DC01EBE9E92D5ACD4E64E70775B81BAF222BCA30C91256D66B56B06ACA5B09025009557DF411D076796BDC412234068790235420C6
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.6.7.2.9.6.0.2.6.5.2.0.6.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.6.6.7.2.9.7.8.5.1.5.1.5.5.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.2.4.2.c.1.7.9.-.d.3.e.b.-.4.1.a.4.-.b.4.e.4.-.2.f.5.d.6.f.2.1.4.6.b.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.5.a.6.0.9.e.3.-.b.d.c.3.-.4.c.4.9.-.a.7.f.a.-.4.1.f.3.9.d.7.3.8.c.9.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.v.b.c...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.v.b.c...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.3.d.0.-.0.0.0.1.-.0.0.1.7.-.e.5.2.6.-.e.f.f.5.b.c.f.8.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.7.8.7.d.9.a.6.e.c.3.f.2.6.2.e.8.b.7.1.d.1.9.a.c.1.5.7.c.2.a.2.8.6.a.0.f.5.9.d.d.!.v.b.c.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F5.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4763
Entropy (8bit):	4.481634873006896
Encrypted:	false
SSDEEP:	48:cvIwSD8zsoJgtWI9uoWSC8B08fm8M4JQ8nFLx+q8va88uwrAGd:uITfu9BSNDJZKwu+AGd
MD5:	CE13E8E50FA2947304ECADA1E7CAA44F
SHA1:	AF6C8E43C5D1CDDFF9B15159CD4EF384C6EC4DE1
SHA-256:	2F4CB97C8C06F97B5A6753EDA96A157E97D57B73AC55299D82C01FF0AC1C2E53
SHA-512:	3B97FA92819CDCCBACC13472ABB98158AB3B87F8B82C6B14642DBEC2F53B99C12518ECD9C545E77A7530817EA0EAC573E8710C01C15B589244F5ED8436FC07B
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="842541" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER29B.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8410
Entropy (8bit):	3.697340644819152

C:\ProgramData\Microsoft\Windows\WER\Temp\WER29B.tmp.WERInternalMetadata.xml	
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/r6UXYaH6YgwSU3E90gmfZ1ySVCprE89bkWsfpsm:RrlsNiz6haH6Y3SU3EugmfWSsk1fH
MD5:	68A4C27D158EBA0E731D66B9346B9930
SHA1:	8E99C9CFB4FE2ED333C24DEE4C0C07275546C1DA
SHA-256:	E9782B937D6B13B05784BC3393AC133A1919743EA4336A6FF3CD4B70DC2AE0FD
SHA-512:	596B7395AE4738DD79E2BF12464187F8F2917E108CFE7CB400C5EA3475EC50DF8146A51ED6B3995EDFE07F3EB73B403ABF603349E5916F9B74000F090EEE2BB
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.1.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AF.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8290
Entropy (8bit):	3.7007069879870316
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimLh6kG6Y5h62VXE1gmf5NSVCprM89bxUsfDbm:RrlsNi86t6YP6ngmfjSUxHfu
MD5:	A0F3788B0B46128A48243F16026DE590
SHA1:	4AC781187472FB9C7793510116D36864F621D0AA
SHA-256:	7926E3187542ACB5424A9F918B157AD38DC9E7414EDFFF6E1610D66E7C37DC82
SHA-512:	1830472EA82F5B9680657EBCD7360452D9059582F2A8685D3420DA23AE538C458C8AD1AAB4AEC8CAADA315B25E20051591E68275297CD662A5FE4303B19B2BE
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.9.7.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3846.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8314
Entropy (8bit):	3.699039341222745
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiJV68pV1/Md6Yt96F/gmf0SVCprg89bcksfGUm:RrlsNi76B6Yn6F/gmf0SQcXfM
MD5:	A47D60DEFFF9EF0624D266B32753A17F
SHA1:	AB5132A9A2F4EF53A959890FD995DBA6F26CA8C0
SHA-256:	5A5379F51B1B790D50F12F9F7FD7B335D0FDB598B96AE496ACA999B82DC87A2F
SHA-512:	118511C2C504B45754D692B632141C66207446D40C9D972D1EA5E2E6F0749C3BEFE669DC5E1DFA21BB31A395E7DCC0F8F7556F7FB06A9C928B5018551EFA21B
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER47E7.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4658
Entropy (8bit):	4.484578834337649
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWI9uoWSC8B6s8fm8M4JUkZFdt85+q84UTM5/URyHid:uITfh9BSN4RJJBt85oTM5cRyHid
MD5:	B7F5BFAE86E614D0AFE6ABB63E19E8DA
SHA1:	4301E15856ECB9EDA2E5B12494DF9C800EE9A0DF
SHA-256:	DCAB0D7A124EBA863ACEE61E3E157CEF36C979DD1EF9C01E32988B05B7D97F2E
SHA-512:	C799E8B5B1197F95B33AD481734CB537293C1D400CDD7A45314CF232D2C2F01FE0C6F96C227541E2CC13229D316008F88ACF5FE157599E5C522A2E18EE6F45D

C:\ProgramData\Microsoft\Windows\WER\Temp\WER47E7.tmp.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="842540" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0.tmp.mdmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Feb 1 17:09:33 2021, 0x60521 type
Category:	dropped
Size (bytes):	6814003
Entropy (8bit):	4.736539329301494
Encrypted:	false
SSDEEP:	98304:qMauqrXI79HphPb1Xa8yB20XvlieTYuerhfM1NlOMcTvd3:DxqrXI79HjOXbmMcF
MD5:	ACEA9DA01C4C4F05AC026518FF86F7CF
SHA1:	5AE5FDEE932EE816E8C3A30302F05CCD402AB269
SHA-256:	5235ED9F5781E3B08940425FADB1096933C47E696346934B963F77034F08489F
SHA-512:	7113C8E700FEEBBB8D39EC2C4B73F58253E86AED7D7473352280FEFBDF438174E1D900364FC4803CB8DE3E8C459C878B9DE70822D1A9FEA92840B1B2D627548F
Malicious:	false
Preview:	MDMP..... .....5.`!.....U.....B.....3.....GenuineIntelW.....T.....5.`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA992.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Feb 1 17:09:06 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	233680
Entropy (8bit):	3.7246203524598553
Encrypted:	false
SSDEEP:	3072:z0Yjd+pvJvSt0O9gIOgF5VUCgUmjoojd6OU:z0ppFKz9RpDVTjLERU
MD5:	52498EF1D5E8F92B63ECC3C47BE0C49F
SHA1:	FE35A724F444748D10A797F92FF3C8A5E2FB5BF6
SHA-256:	41F106CC80D75A395F54CF4246E7D5896ABAB03894BF770B79131DE580F5E5B4
SHA-512:	3814B6B79DC0640B58E6B18C968879EC2C1151A8A85F0DD7B5054A352599FAD3457FB551FC6CE9D29792FF1F666BD1D1016258CB2B519296E0DE550CAE20E69
Malicious:	false
Preview:	MDMP..... .....5.`.....U.....B.....h .....GenuineIntelW.....T.....5.`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAAF.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4643
Entropy (8bit):	4.484119805416583
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWI9uoWSC8B08fm8M4JlkZFJ+q8VU95lMSGd:uITfh9BSNfJa9195lTGd
MD5:	BFFCA8228F5B11E9364EC42E7F17DD77
SHA1:	C2561F761EF17908E398980AD450303D1A67C630
SHA-256:	387C0AF23BEA505763B9580F7EBC5EF00520B29249244BA651391E95AA8A6655
SHA-512:	9F15619A6817CEB4AF55BDD208021CA40C30C92724E0F6E69DCB6479CA8DC9A8DF8DA810B2C3E1E4BA45002E029EAA7712E7BFD6D03AA1F5AE8F0B540FF9B5F3
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="842540" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB12E.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Feb 1 17:10:25 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	226746
Entropy (8bit):	3.758060180058424
Encrypted:	false
SSDEEP:	3072:GA0Bjd+pVv3S20t9gIOgF5uUCgUnsT2SqoKTy:r0GpVvLo9RpDuTjnUqI
MD5:	D7A5A9F582772EF13C62A888C7EDF2F9
SHA1:	D73F28A641F8551FC8FD565DE1B878AC3C49987E
SHA-256:	94F0D2BE41BCD650FDF4C379AE67F017B9358C28873C5AF16A904F479574A8A6
SHA-512:	202F33A49BB7918FEBBC36ABA40313107D59D75F5EF44202D7114E67A2D985734A601E1E03D23BBB667E097508D671263E8C4CC6131095B43B4AABF3D7985763
Malicious:	false
Preview:	MDMP..... .....6.`.....U.....B.....8 .....GenuineIntelW.....T.....@....5.`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6DF.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8384
Entropy (8bit):	3.6912217569118457
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiEb6/6YgZnSUbsgmfZ0ySVCprH89b/2sf0uMVm:RrlsNiQ6/6YknSUbsgmfzSF/Vf0uj
MD5:	739390DCE27DCEDF34FA5157E1309291
SHA1:	D3DE02641A291A357512681C254286DC90845607
SHA-256:	FEDF50AAEF3EB58CFC1EB06D94A39CBB65C2E361F77CFC46671E591F438ED000
SHA-512:	A029A0A11DC6FEA9119D67BCAD19E91C6FB6A18B1569E40103494A00F9783A627A0B307A74DE87F25BFD22731F15C82C1E3BC005FE8FFAF9B092E71158AB7D4B
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.2.4.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBC2.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4738
Entropy (8bit):	4.456267471472871
Encrypted:	false
SSDEEP:	48:cvIwSD8zsjJgtWI9uoWSC8Bp8fm8M4JA8nFk+q8vH82N5uwijUd:uITf99BSNYJIKT5u5jUd
MD5:	E6BD470C252D8E4C0C9C79B31F708E6F
SHA1:	6BC73308E99D47AF5CF783BAE09D2B0CD9CCF576
SHA-256:	E1EDEB9FD263CF77B679B96E5D15B8C05AE73940585D7B9E24244FFC4AC91BD4
SHA-512:	D45B23D47FCC663985D143568E626D9C8BBC6B34FB17C257BCB521D65122B9DE50BA11DD137E78DC426C0D4C0B75F8568A72E8B9EAEDF7F0140A37B14B7CA22
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="842539" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBEF.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7628
Entropy (8bit):	3.687161917724904
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBEF.tmp.WERInternalMetadata.xml	
SSDEEP:	192:Rrl7r3GLNiJk6o3XZe6Yts6F/gmfZSnSCCp12E1fNSm:RrlsNia6/6Y26F/gmfInSr2ufJ
MD5:	6166ADFD7737F286C775339B065FF3F1
SHA1:	39645E66FE7BBE326BFFBE7F7CFB37543F7507D6
SHA-256:	FE2F9BCD79240F00107C21261022EBC3DFBE3E18FC67A609A6E3BF8BDDF0BFE2
SHA-512:	6E1795B9EC2D5904D0867993350D37DA7EA674D04472D2D33D52A7915FE96FAFD2839E4C106FC84394E3F10FB26761B557BA93BA417DF90764AB2519FDC537D
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD19.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4678
Entropy (8bit):	4.442994253323229
Encrypted:	false
SSDEEP:	48:cvIwSD8zsjJgtWI9uoWSC8BIQ/8fm8M4JFKqJFL+q8vvDM5/URyHBd:uITf99BSN3kJFKSK7M5cRyHBd
MD5:	113E576BC23CE85909DD33707B4D3D72
SHA1:	50F8E0529504C8B788BC199FE1F7D516A2ADF7A1
SHA-256:	F5E84846E011741FA5CF67C229B7891FA8CE4DB2E96D8F0605979887722113D4
SHA-512:	D0A93EF150B778F2468832C65A6E1F3634D46BA07A5E4F39D6813D85470E4CDFC4C51700B22365D28544BCFFE19C21C4FABCA36FD4124C69A33C6BD0F36EF8E
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="842539" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF62B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Feb 1 17:09:22 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	17418
Entropy (8bit):	2.189553347266588
Encrypted:	false
SSDEEP:	96:51P8Q/5kt7zO7Mm7u2+D90ioBiT+QlbWInWIXmI4t9FOnuu3:TwyM2YaZBiKot9Yuu3
MD5:	CF1313617E1BA67E74E9F9823A689161
SHA1:	0D800C48004D989D56FEE92682ADC89CF2BEDFB8
SHA-256:	1013A8A807BFA0EB7364602A98DBA64011238109D0E43E82ABDBBE464C7DFB81
SHA-512:	BBAE7ED7F1F859D12564EFA13B9DF596F5544D60D9CAD96F4F681DE73724944B92C186F91DC13DBC45954260C55861F8ABACAD06E975EFD5D44909C63C857ED
Malicious:	false
Preview:	MDMP..... .....5.`.....U.....B.....t.....GenuineIntelW.....T.....5.`.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\hawkgoods.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\hawkgoods.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	916
Entropy (8bit):	5.282390836641403
Encrypted:	false
SSDEEP:	24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2+:MwLLD2Y9h3go2rxxAcAO6ox+g2+
MD5:	5AD8E7ABEADADAC4CE06FF693476581A
SHA1:	81E42A97BBE3D7DE8B1E8B54C2B03C48594D761E
SHA-256:	BAA1A28262BA27D51C3A1FA7FB0811AD1128297ABB2EDCCC785DC52667D2A6FD
SHA-512:	7793E78E84AD36CE65B5B1C015364E340FB9110FAF199BC0234108CE9BCB1AEDACBD25C6A012AC99740E08BEA5E5C373A88E553E47016304D8AE6AEEAB58EEFF
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\hawkgoods.exe.log	
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a9099237864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8003
Entropy (8bit):	4.839308921501875
Encrypted:	false
SSDEEP:	192:yxoe5oVsm5emdVVFn3eGOVpN6K3bkkjo59gkjDt4iWN3yBGHh9smidcU6CXpOTik:DBVoGIpN6KQkj2Wkjh4iUx0mib4J
MD5:	937C6E940577634844311E349BD4614D
SHA1:	379440E933201CD3E6E6BF9B0E61B7663693195F
SHA-256:	30DC628AB2979D2CF0D281E998077E5721C68B9BBA61610039E11FDC438B993C
SHA-512:	6B37FE533991631C8290A0E9CC0B4F11A79828616BEF0233B4C57EC7C9DCBFC274FB7E50FC920C4312C93E74CE621B6779F10E4016E9FD794961696074BDFBF
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	16680
Entropy (8bit):	5.575624550668492
Encrypted:	false
SSDEEP:	384:X7t9+XV0PidIvyosCh5dB+RnISBKnNRul4Itp7Y9g4SJQPiY4y:X/i3CfdyI4KLul4S54RP7v
MD5:	748E24CE0A85BA329A226E109182E5D8
SHA1:	A6E6DB81CD4B0FA5528F5CD03BA7D1C486DEDF87
SHA-256:	1DDD69A6CFCFBFCBCF4A0EE0D7B3376A051124BC755DD15F414670A3A344114D
SHA-512:	0B97E3A47BA46ABB3E64B7B52E84BC1647C6274B65BC51DA26153EEBB42D5950C802DD6009A7415632A6CC8D30940E849A488F834FCA1874B1BC712CF7ADC33
Malicious:	false
Preview:	@...e.....F.....@.....H.....<@.^.L."My...:)..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	455680
Entropy (8bit):	5.4156534240521
Encrypted:	false
SSDEEP:	6144:L09yLLuWoujzz/DCBGNv5lToO7OsWXiOV:L09yLyWoujHDX5QO7OvXik
MD5:	80C61B903400B534858D047DD0919F0E
SHA1:	D0AB5400B74392308140642C75F0897E16A88D60
SHA-256:	25ADE9899C000A27570B527CFFC938EC9626978219EC8A086082B113CBE4F492
SHA-512:	B3216F0E4E95C7F50BCCBA5FDCCA2AD622A42379383BE855546FA1E0BAC41A6BEEA8226F8634AD5E0D8596169E0443494018BBE70B7052F094402AECAA038BCE
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: C:\Users\user\AppData\Local\Temp\Matiexgoods.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 86%

C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....~.... ... ....@.. .....`..... ..@.....$...W.... .....@..... ....H.....text..... ....`.rsrc..... .....@..@.rel oc.....@.....@..B.....`.....H.....x.....x'...h..... .....RNK\ZJO@F.EYC.G.IOYKJ._R_CEESEPPlj}ez|"hzfSn`ssdh~DNwq//M\`tdv`|..;....4.....Ewqus._/.....V>..%9%(:&##b?`LLJN.56(,*:.}.2=4lwY_..... .....A.{YOLI..qAL.tTDY^..v^NY

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_03w4pbbs.uza.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1uftfplo.nuv.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_m1dlmoaq.ohr.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oht352yv.150.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oht352yv.150.psm1	
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\hawkgoods.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	532992
Entropy (8bit):	6.507156751280516
Encrypted:	false
SSDEEP:	6144:DufqM5JXbS/QTjhUqBfxrwEnuNcSsm7IoYGW0VvBXCAt6kihwE+VDpJYWmlwnx9E:uJXQtqB5urTIoYWBQk1E+VF9mOx9Ei
MD5:	FFDB58533D5D1362E896E96FB6F02A95
SHA1:	D6E4A3CA253BFC372A9A3180B5887C716ED285C6
SHA-256:	B3D02FD5C69293DB419AC03CDF6396BD5E7765682FB3B2390454D9A52BA2CA88
SHA-512:	3AE6E49D3D728531201453A0BC27436B1A4305C8EF938B2CBB5E34EE45BB9A9A88CF2A41B08E4914FDA9A96BBAA48BD999A2D2F1DFFCD39761BB1F3620CA725F
Malicious:	**true**
Yara Hits:	• Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 96%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....4..... .....@.. ..... ..@.....O.... ...2.....`..... ....H.....text..... ....`.rsrc....2... ...2.....@..@.reloc.....` ....@..B.....H.....0}..\.....X.....2s.....*....0.....~.....(.....~....o....~....o.....9.....~....o.....+G~.....o.....o.....,). .....,.~.....~.....o....o.....1.~.....~....o.....o.....~....~....o....o.....~....(....s....o.....(.....*.....0.. .....(....(.....(....o.....*.....(.....(.....o... ....o.....o.....o.....*.R..(....o....o.....

C:\Users\user\AppData\Local\Temp\origigoods20.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	220672
Entropy (8bit):	6.057903449485828
Encrypted:	false
SSDEEP:	3072:SVQEat7UY8MnZGcqB5AyruUJ7XAzsNvEaEifv6yr9zRsc0qC4B0BUAE3vVAVvoUB:SytJqCUyQNX36yQqbB063cAUAW
MD5:	61DC57C6575E1F3F2AE14C1B332AD2FB
SHA1:	F52F34623048E5FD720E97A72EEDFD32358CD3A9
SHA-256:	1C7757EE223F2480FBC478AE2ECAF82E1D3C17F2E4D47581D3972416166C54AB
SHA-512:	81A7DB927F53660D3A04A161D5C18AAB17D676BCC7AE0738AB786D9BEE82B91016E54E6F70428AEC4087961744BE89B1511F9E07D8DABBE5C2A9D836722395A1
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\origigoods20.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 86%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....V.....t... .....@.. ..... ..@.....t..O..... ..... ..H.....text....T... ...V..... ..`.rsrc.....X.....@..@.reloc..... .....\.....@..B.....t.....H.....(....*..(....*.s.....s.....s.....s.....*...0.....+.....,.....,.....,.+.+.~....o....*.0..,..... ..+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0.....+.....,.....,.....,.+.+...(....(....*...0..(.....+.....,..... .....,.....,.+.+..(....*.0..,.....

C:\Users\user\AppData\Local\Temp\origigoods40.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\Temp\origigoods40.exe	
Size (bytes):	221696
Entropy (8bit):	6.060343577776758
Encrypted:	false
SSDEEP:	3072:K9Wf3ouEAkhUxOCt+qqr3drw0tR5dUimnoSA7Mw4lY2hWYQQgGJrozRscS4+SOw6:KhuI3dlxUOt7IdWLOjCDUjU
MD5:	AE36F0D16230B9F41FFECBD3C5B1D660
SHA1:	88AFC2923D1EEFB70BAD3C0CD9304949954377EF
SHA-256:	CFAD1E486666FF3FB042BA0E9967634DE1065F1BBD505C61B3295E55705A2A50
SHA-512:	1E98AEE7DC693822113DCDE1446A5BED1C564B76EEF39F39F3A5D98D7D2099CF69AC92717A3297AFC7082203929F1E9437F21CB6BC690974A0EF6D6CF6E4393
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\origigoods40.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 83%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....X.....>v... .....@.. ..... .@.....u..S.....P..... ..... ..H.....text...DV... ...X..... ..`.rsrc...P.....Z.....@..@.relo c.....`.....@..B..... v.....H.....H.....(....*..(....*.s.....s.....s.....s.....*...0..,.....+.....,.....,.....,.+.+.~....o....*.0. .,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0.....+.....,.....,.....,.+.+...(....(....*...0..(.....+ .....,.....,.....,.+.+..(....*.0..,.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\l$s#$lT3ssl.exe	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1630720
Entropy (8bit):	7.950446972015694
Encrypted:	false
SSDEEP:	49152:JWHSbycxNZlBaewSfpEH9G6mCK4IjLJa:YsxjlB1Bk9GVNL
MD5:	E85DAF3A43F107B213310A53BFD35AA9
SHA1:	042208C7A232B806C6382E34417F9C8E2A955747
SHA-256:	0B1FBC81D9D9E685307E80D20AFE4B01C6538B903B77136B0D1DB2486FE8C6E8
SHA-512:	29688E0FE124802B3317355E9836864147E56F6E1D47F702F88EA36DF813F0EB388818EAD042C4463619E17BD5EC295D4CFC4F0CAA2C2DBD90EDD22B2277EC7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 22%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...q.....0..... .....@.. .....@..... ..@.....K..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....#.....".(.....*.(.....~....~....o....o.....*&.(.....*".....*6.~....(&...&*.(*.....*....0.....(.....(.. ...s.....r...p(.....r...p(.....(.....(.....r...p(.....(.....rX..p(.....(....(.....r...p(....-T..r...p(....-h..r...p(....-|..r...p(...:.....r...p(...:.....r...p(...:.....8....r...p...o.....(....(.....8....r...p...o.....(....(.....8....r...p...o.....(....(.....+jr...p...o

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\l$s#$lT3ssl.exe:Zone.Identifier	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\AppData\Local\Temp\hawkgoods.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:mTR:md
MD5:	76D7C0780CEB8FBF964C102EBC16D75F

C:\Users\user\AppData\Roaming\pid.txt	
SHA1:	294584E3F792CFE0D08E752B26164BC8173E7A95
SHA-256:	1F6909D0BA546F3291D3A8FFA1107868D370ADE6C3DF0393C4B944E3437291F0
SHA-512:	A916C528B82B2265AAAE77343BD2A18B7338D30EE75DEDFBF7654D0A28DFE8975D6C8C66B552D8CC1E157A7FC85C7EA2CF7E5F74488FEECE4D1917A0BF359 19
Malicious:	false
Preview:	 7064

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\AppData\Local\Temp\hawkgoods.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	50
Entropy (8bit):	4.6483674395583785
Encrypted:	false
SSDEEP:	3:oNerbJSRE2J5xAI4F:oNe0i23f8
MD5:	0CE4A330E42C174E8E8CF4D81C6F46A6
SHA1:	D9CA3AD5CD90643DF99808D5FF0EC0E89E891FE0
SHA-256:	94ABDE13F36EBE4B4AC81A712597439918788FD90339594FA1DDD679E7DAD70A
SHA-512:	CE3453726B73A7423C69D94E4784966A6AA08381ABE9585AA323D0D80FAF63B3A31508B7083C3FEC6AB2727112573733D498F4F78389D75F64DDF6BABE581943
Malicious:	false
Preview:	 C:\Users\user~1\AppData\Local\Temp\hawkgoods.exe

C:\Users\user\Documents\20210201\PowerShell_transcript.320946.GXJdt0T3.20210201090850.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1199
Entropy (8bit):	5.200081162523958
Encrypted:	false
SSDEEP:	24:BxSAjUdZOvBdaOx2DOXCgluVM5wWzHjeTKKjX4CIym1ZJXbxvuVM5OnxSAZp:BZjbv6OoONuojzqDYB1Z1xvuogZZp
MD5:	057FA50F48D04A36E4EAEFA244B5C169
SHA1:	651D8F086A314A920C22758C6792D43FE782A608
SHA-256:	DCF9967EF8BF7A51D965E20177FA747A2A72BF79F89D74CC5DFCBA27392E3BF5
SHA-512:	C2C2FA3A3EE34E0DEBD0B05F9BF6F7E0A389A131AE0B86350F6F8BB4A14CA3CADA09D5D2D2DDA1B427905293F29F65A7C5CC0821792A949786303B5DFBDFA D8F
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210201090908..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 320946 (Microsoft Windows NT 10.0.17134.0)..Host Application: Powershell.exe -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\Desktop\Orde rs.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe'..Process ID: 6896..PSVersion: 5.1.17134.1..PSEdition: Desk top..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProt ocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210201090909..**********..PS>Copy-Item 'C:\Users\user\Desktop\Orders.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe'..**********

C:\Users\user\Documents\20210201\PowerShell_transcript.320946.zsUBLVk9.20210201090956.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4005
Entropy (8bit):	5.381394861441764
Encrypted:	false
SSDEEP:	96:BZW96ONWwrqDo1ZQwMZGc6ONWwrqDo1ZKnSdC3UC3UW3/Zj:ind
MD5:	F1255BA2BED2F944999756485BA4F2F1
SHA1:	21E4737A720482546901EAC1ED6E2071FBCB0E7F
SHA-256:	3128CD097294A8CB5E444912AF6F140BDFBE166FEE2B831150D3087C6DB21C17
SHA-512:	4948FE537A92C89D249A2DE7EA81A365B16CFBBF2084F79E1C488B805CA91CE4989F01C8FE6C20A2712C7CD0FB5A1F9CCC9DDBF1A299DD72962005D8857DB5 E4
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210201091111..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 320946 (Microsoft Windows NT 10.0.17134.0)..Host Application: Powershell.exe -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\AppData\Roam ing\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe' ..Process ID: 5296..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210201091111..**********..PS>Copy-Item 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.e

C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	
Process:	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5794451
Entropy (8bit):	7.945637278937759
Encrypted:	false
SSDEEP:	98304:dsGJgJ2Lg8sGJgJ2LgmsGJgJ2LgmsGJgJ2LgmsGJgJ2LgNpsGJgJ2LgqsGJgJ2LP:SSbgvSbgRSbgRSbgRSbgUSbgdSbgG
MD5:	F32EDC7587C52E7FB3CEEB67CC681A9B
SHA1:	5D809E1186725C794F051318D07C8F9D08E71DD7
SHA-256:	F96B2D3A1BE40A6F7D99D7E91773FF4CD8FF072FF773BA40326B055ACEED8D34
SHA-512:	538592A3BFD5EB39CF0447EFF465064B4E2AF3A6ADDE43A37A081458816EBA680B5314AA40B871B62DC341FEB26FD0730379A9243BA3C8392779A7DB8F45CD9
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....uEy...s...Q..f.%.1.Q..X.11.....*H.bo.., JS.....A.-&...v..Q.....?..u.....g....>..{z.{.g..++[....n. ...l{...v.X...l.'.....+;..t...kv..vv._.N.M..$].c.....F.4...&l..E..l.....:... ..u..r[.?E...mc[).....-.P..V...G=.n]....~.v.+[K]...@...Ge.....N.....w.....sD.|.9a.~6<..L.>.....m..c!C#?..6.....b. t.`.%...Y.f....ol.....c?.7.F.${...n.m.....&6.n.....P.]...}....OX.5.n.h.....4.X..`i.....R.-.].T.... c..&...H.y.q].....Q.6.....P..B.^.5.....z.c.....,_.....;.3..d.l.....;$...6..6.}..*\|..l.^t.?f..2.... C....6,j+3.>...-4m.k{..e...a..p...4L\|O.d'..:.!.-..n ..@ ...]...g:c.....Rr0..4.....?*3H[.@.../..K.p..m....S.....`.K.p.P.....Gbj..m.....R.La._.K.p4..B.^.5.....z.c.....,_.....d.,..8.....v. 6.....v.....aQ[...a..m.i{X..,,.....E...M"...E.I6...7.z...,...#h,0 l.H0.l...../.....C.?....`$+.*&}..&6.D...6...Z..':.v....2.`.-

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.950446972015694
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Orders.exe
File size:	1630720
MD5:	e85daf3a43f107b213310a53bfd35aa9
SHA1:	042208c7a232b806c6382e34417f9c8e2a955747
SHA256:	0b1fbc81d9d9e685307e80d20afe4b01c6538b903b77136 b0d1db2486fe8c6e8
SHA512:	29688e0fe124802b3317355e9836864147e56f6e1d47f70 2f88ea36df813f0eb388818ead042c4463619e17bd5ec29 5d4cfc4f0caa2c2dbd90edd22b2277ec7d
SSDEEP:	49152:JWHSbycxNZlBaewSfpEH9G6mCK4ljLJa:YsxjlB 1Bk9GVNL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...q .....0..... .....@.. .....@..... ..@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x58f6ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xC3C29871 [Sat Jan 27 20:22:09 2074 UTC]

General

TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x18f680	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x190000	0x5be	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x192000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x18d6d4	0x18d800	False	0.791853994693	data	7.95293663991	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x190000	0x5be	0x600	False	0.434895833333	data	4.22642040324	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x192000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1900a0	0x334	data		
RT_MANIFEST	0x1903d4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	oiESlUDzGd
Assembly Version	25.22.3.14
InternalName	mDOrGSKgiV.exe
FileVersion	25.22.3.14
CompanyName	umTKsPVLUs
Comments	wnrUpdIANR
ProductName	HPJqPQeMSZ
ProductVersion	25.22.3.14
FileDescription	mDOrGSKgiV
OriginalFilename	mDOrGSKgiV.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/01/21-09:09:08.110976	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49724	104.16.155.36	192.168.2.7

Network Port Distribution

Total Packets: 145

- 53 (DNS)
- 587 undefined
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 09:09:07.569933891 CET	49723	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:07.644108057 CET	80	49723	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:07.644426107 CET	49723	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:07.645061016 CET	49723	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:07.720326900 CET	80	49723	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:07.720357895 CET	80	49723	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:07.720364094 CET	80	49723	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:07.720462084 CET	49723	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:07.725764990 CET	49723	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:07.799046040 CET	80	49723	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:08.020463943 CET	49724	80	192.168.2.7	104.16.155.36
Feb 1, 2021 09:09:08.026357889 CET	49725	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:08.060730934 CET	80	49724	104.16.155.36	192.168.2.7
Feb 1, 2021 09:09:08.060949087 CET	49724	80	192.168.2.7	104.16.155.36
Feb 1, 2021 09:09:08.062127113 CET	49724	80	192.168.2.7	104.16.155.36
Feb 1, 2021 09:09:08.099446058 CET	80	49725	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:08.099633932 CET	49725	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:08.100845098 CET	49725	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:08.102327108 CET	80	49724	104.16.155.36	192.168.2.7
Feb 1, 2021 09:09:08.110975981 CET	80	49724	104.16.155.36	192.168.2.7
Feb 1, 2021 09:09:08.176035881 CET	80	49725	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:08.176124096 CET	80	49725	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:08.176136017 CET	80	49725	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:08.176549911 CET	49725	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:08.176592112 CET	49725	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:08.249598980 CET	80	49725	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:08.272891045 CET	49724	80	192.168.2.7	104.16.155.36
Feb 1, 2021 09:09:12.654989958 CET	49727	443	192.168.2.7	172.67.188.154
Feb 1, 2021 09:09:12.701138973 CET	443	49727	172.67.188.154	192.168.2.7
Feb 1, 2021 09:09:12.701245070 CET	49727	443	192.168.2.7	172.67.188.154
Feb 1, 2021 09:09:12.798677921 CET	49727	443	192.168.2.7	172.67.188.154
Feb 1, 2021 09:09:12.844975948 CET	443	49727	172.67.188.154	192.168.2.7
Feb 1, 2021 09:09:12.846554995 CET	443	49727	172.67.188.154	192.168.2.7
Feb 1, 2021 09:09:12.846597910 CET	443	49727	172.67.188.154	192.168.2.7
Feb 1, 2021 09:09:12.846705914 CET	49727	443	192.168.2.7	172.67.188.154
Feb 1, 2021 09:09:12.855519056 CET	49727	443	192.168.2.7	172.67.188.154
Feb 1, 2021 09:09:12.901724100 CET	443	49727	172.67.188.154	192.168.2.7
Feb 1, 2021 09:09:12.901892900 CET	443	49727	172.67.188.154	192.168.2.7
Feb 1, 2021 09:09:13.038564920 CET	49727	443	192.168.2.7	172.67.188.154
Feb 1, 2021 09:09:13.084671021 CET	443	49727	172.67.188.154	192.168.2.7
Feb 1, 2021 09:09:13.290333033 CET	443	49727	172.67.188.154	192.168.2.7
Feb 1, 2021 09:09:13.414352894 CET	49727	443	192.168.2.7	172.67.188.154
Feb 1, 2021 09:09:13.507807016 CET	49728	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:13.580697060 CET	80	49728	216.146.43.71	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 09:09:13.581615925 CET	49728	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:13.581939936 CET	49728	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:13.654639959 CET	80	49728	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:13.654850006 CET	80	49728	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:13.654874086 CET	80	49728	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:13.655082941 CET	49728	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:13.655669928 CET	49728	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:13.656709909 CET	49727	443	192.168.2.7	172.67.188.154
Feb 1, 2021 09:09:13.702876091 CET	443	49727	172.67.188.154	192.168.2.7
Feb 1, 2021 09:09:13.719511032 CET	443	49727	172.67.188.154	192.168.2.7
Feb 1, 2021 09:09:13.728564024 CET	80	49728	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:13.857872963 CET	49731	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:13.914356947 CET	49727	443	192.168.2.7	172.67.188.154
Feb 1, 2021 09:09:13.930615902 CET	80	49731	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:13.930720091 CET	49731	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:13.931035995 CET	49731	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:14.003655910 CET	80	49731	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:14.003762960 CET	80	49731	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:14.003801107 CET	80	49731	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:14.003897905 CET	49731	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:14.004287004 CET	49731	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:14.004724026 CET	49727	443	192.168.2.7	172.67.188.154
Feb 1, 2021 09:09:14.069881916 CET	443	49727	172.67.188.154	192.168.2.7
Feb 1, 2021 09:09:14.077008009 CET	80	49731	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:14.211262941 CET	49727	443	192.168.2.7	172.67.188.154
Feb 1, 2021 09:09:14.233859062 CET	49732	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:14.306735992 CET	80	49732	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:14.306864023 CET	49732	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:14.307152987 CET	49732	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:14.379934072 CET	80	49732	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:14.379973888 CET	80	49732	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:14.379997015 CET	80	49732	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:14.380080938 CET	49732	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:14.380409002 CET	49732	80	192.168.2.7	216.146.43.71
Feb 1, 2021 09:09:14.453466892 CET	80	49732	216.146.43.71	192.168.2.7
Feb 1, 2021 09:09:25.683118105 CET	49738	587	192.168.2.7	199.193.7.228
Feb 1, 2021 09:09:25.683119059 CET	49737	587	192.168.2.7	199.193.7.228
Feb 1, 2021 09:09:25.874058008 CET	587	49738	199.193.7.228	192.168.2.7
Feb 1, 2021 09:09:25.874234915 CET	587	49737	199.193.7.228	192.168.2.7
Feb 1, 2021 09:09:25.874285936 CET	49738	587	192.168.2.7	199.193.7.228
Feb 1, 2021 09:09:25.874669075 CET	49737	587	192.168.2.7	199.193.7.228
Feb 1, 2021 09:09:25.884875059 CET	49738	587	192.168.2.7	199.193.7.228
Feb 1, 2021 09:09:25.885530949 CET	49737	587	192.168.2.7	199.193.7.228
Feb 1, 2021 09:09:26.070074081 CET	587	49738	199.193.7.228	192.168.2.7
Feb 1, 2021 09:09:26.070111990 CET	587	49737	199.193.7.228	192.168.2.7
Feb 1, 2021 09:09:26.070348978 CET	49738	587	192.168.2.7	199.193.7.228
Feb 1, 2021 09:09:26.070352077 CET	49737	587	192.168.2.7	199.193.7.228
Feb 1, 2021 09:09:26.075392008 CET	587	49738	199.193.7.228	192.168.2.7
Feb 1, 2021 09:09:26.075428009 CET	587	49737	199.193.7.228	192.168.2.7
Feb 1, 2021 09:09:26.075548887 CET	49738	587	192.168.2.7	199.193.7.228
Feb 1, 2021 09:09:26.075551033 CET	49737	587	192.168.2.7	199.193.7.228
Feb 1, 2021 09:09:26.076323986 CET	587	49738	199.193.7.228	192.168.2.7
Feb 1, 2021 09:09:26.076637983 CET	587	49737	199.193.7.228	192.168.2.7
Feb 1, 2021 09:09:26.076716900 CET	49737	587	192.168.2.7	199.193.7.228
Feb 1, 2021 09:09:26.076719046 CET	49738	587	192.168.2.7	199.193.7.228
Feb 1, 2021 09:09:26.156609058 CET	49739	587	192.168.2.7	199.193.7.228

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 09:08:41.097795963 CET	60338	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:08:41.150357008 CET	53	60338	8.8.8.8	192.168.2.7
Feb 1, 2021 09:08:42.317720890 CET	58717	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:08:42.367254019 CET	53	58717	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 09:08:43.720391989 CET	59762	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:08:43.768136024 CET	53	59762	8.8.8.8	192.168.2.7
Feb 1, 2021 09:08:45.281250000 CET	54329	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:08:45.331974030 CET	53	54329	8.8.8.8	192.168.2.7
Feb 1, 2021 09:08:46.854796886 CET	58052	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:08:46.905754089 CET	53	58052	8.8.8.8	192.168.2.7
Feb 1, 2021 09:08:52.060491085 CET	54008	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:08:52.111505032 CET	53	54008	8.8.8.8	192.168.2.7
Feb 1, 2021 09:08:56.677571058 CET	59451	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:08:56.726212025 CET	53	59451	8.8.8.8	192.168.2.7
Feb 1, 2021 09:08:58.374330997 CET	52914	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:08:58.424185991 CET	53	52914	8.8.8.8	192.168.2.7
Feb 1, 2021 09:08:59.758740902 CET	64569	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:08:59.806689024 CET	53	64569	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:02.278642893 CET	52816	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:02.336200953 CET	53	52816	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:04.062025070 CET	50781	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:04.111485958 CET	53	50781	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:06.938735008 CET	54230	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:06.986632109 CET	53	54230	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:07.419259071 CET	54911	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:07.461031914 CET	49958	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:07.470134020 CET	53	54911	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:07.495611906 CET	50860	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:07.517234087 CET	53	49958	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:07.545397997 CET	53	50860	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:07.909754038 CET	50452	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:07.966373920 CET	53	50452	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:12.501633883 CET	59730	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:12.552354097 CET	53	59730	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:12.591841936 CET	59310	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:12.651006937 CET	53	59310	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:13.654509068 CET	51919	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:13.705180883 CET	53	51919	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:18.257209063 CET	64296	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:18.308031082 CET	53	64296	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:22.215455055 CET	56680	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:22.263302088 CET	53	56680	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:23.039397955 CET	58820	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:23.087352037 CET	53	58820	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:24.392739058 CET	60983	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:24.443696976 CET	53	60983	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:25.589675903 CET	49247	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:25.645951033 CET	53	49247	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:26.139452934 CET	52286	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:26.187345982 CET	53	52286	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:26.574780941 CET	56064	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:26.635169983 CET	53	56064	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:27.342576981 CET	63744	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:27.401709080 CET	53	63744	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:28.843076944 CET	61457	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:28.904061079 CET	53	61457	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:29.857877970 CET	58367	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:29.863385916 CET	60599	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:29.916075945 CET	53	58367	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:29.919811964 CET	53	60599	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:30.017498970 CET	59571	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:30.074986935 CET	53	59571	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:30.388869047 CET	52689	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:30.437252998 CET	53	52689	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:31.158162117 CET	50290	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:31.214703083 CET	53	50290	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:31.359520912 CET	60427	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:31.407432079 CET	53	60427	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 09:09:32.297624111 CET	56209	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:32.345649958 CET	53	56209	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:32.426681042 CET	59582	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:32.482837915 CET	53	59582	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:33.199965000 CET	60949	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:33.247741938 CET	53	60949	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:33.781709909 CET	58542	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:33.838100910 CET	53	58542	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:35.222217083 CET	59179	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:35.281311989 CET	53	59179	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:36.815151930 CET	60927	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:36.871431112 CET	53	60927	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:38.522720098 CET	57854	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:38.570617914 CET	53	57854	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:41.057251930 CET	62026	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:41.113337040 CET	53	62026	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:41.629266024 CET	59453	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:41.677333117 CET	53	59453	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:43.564464092 CET	62468	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:43.623867989 CET	53	62468	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:45.562107086 CET	52563	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:45.620537996 CET	53	52563	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:46.048377037 CET	54721	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:46.096478939 CET	53	54721	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:48.584228039 CET	62826	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:48.635014057 CET	53	62826	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:49.392095089 CET	62046	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:49.451251984 CET	53	62046	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:50.287889957 CET	51223	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:50.335728884 CET	53	51223	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:51.225687981 CET	63908	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:51.273561954 CET	53	63908	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:52.402592897 CET	49226	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:52.461024046 CET	53	49226	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:54.105652094 CET	60212	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:54.153479099 CET	53	60212	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:55.116416931 CET	58867	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:55.164320946 CET	53	58867	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:56.979058981 CET	50864	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:57.040349960 CET	53	50864	8.8.8.8	192.168.2.7
Feb 1, 2021 09:09:59.813623905 CET	61504	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:09:59.872525930 CET	53	61504	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:01.311166048 CET	60231	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:01.359045029 CET	53	60231	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:03.338654041 CET	50095	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:03.396924019 CET	53	50095	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:06.660375118 CET	59654	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:06.716758013 CET	53	59654	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:09.055143118 CET	58233	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:09.113691092 CET	53	58233	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:09.680104017 CET	56822	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:09.730823040 CET	53	56822	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:12.047480106 CET	62572	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:12.105694056 CET	53	62572	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:15.124363899 CET	57179	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:15.183051109 CET	53	57179	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:20.697560072 CET	56124	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:20.745560884 CET	53	56124	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:28.323434114 CET	62287	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:28.379592896 CET	53	62287	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:31.301953077 CET	54644	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:31.358277082 CET	53	54644	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:34.665638924 CET	59159	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:34.722135067 CET	53	59159	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 09:10:38.560153961 CET	57924	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:38.619128942 CET	53	57924	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:44.314034939 CET	51712	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:44.362051964 CET	53	51712	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:46.398916960 CET	58865	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:46.446763039 CET	53	58865	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:46.617623091 CET	64337	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:46.668349981 CET	53	64337	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:47.651475906 CET	50407	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:47.707662106 CET	53	50407	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:50.737806082 CET	61075	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:50.785842896 CET	53	61075	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:54.680552006 CET	54952	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:54.738976002 CET	53	54952	8.8.8.8	192.168.2.7
Feb 1, 2021 09:10:58.185655117 CET	59186	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:10:58.234071016 CET	53	59186	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:01.608866930 CET	52280	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:01.659627914 CET	53	52280	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:06.509452105 CET	51794	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:06.566015005 CET	53	51794	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:07.648718119 CET	50815	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:07.699517012 CET	53	50815	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:09.420171976 CET	58498	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:09.469949961 CET	53	58498	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:13.456777096 CET	56862	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:13.504885912 CET	53	56862	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:16.514466047 CET	61807	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:16.571065903 CET	53	61807	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:25.380804062 CET	52009	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:25.440049887 CET	53	52009	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:28.326708078 CET	58648	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:28.383287907 CET	53	58648	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:31.996967077 CET	59337	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:32.046541929 CET	53	59337	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:36.089000940 CET	59269	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:36.145209074 CET	53	59269	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:42.866492033 CET	49802	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:42.914623976 CET	53	49802	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:45.625840902 CET	50706	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:45.673918009 CET	53	50706	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:48.393935919 CET	55153	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:48.450041056 CET	53	55153	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:52.302521944 CET	59744	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:52.358680964 CET	53	59744	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:54.186583996 CET	59987	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:54.234499931 CET	53	59987	8.8.8.8	192.168.2.7
Feb 1, 2021 09:11:58.350061893 CET	61272	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:11:58.406557083 CET	53	61272	8.8.8.8	192.168.2.7
Feb 1, 2021 09:12:20.722248077 CET	54352	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:12:20.772998095 CET	53	54352	8.8.8.8	192.168.2.7
Feb 1, 2021 09:12:27.572242022 CET	60696	53	192.168.2.7	8.8.8.8
Feb 1, 2021 09:12:27.620141029 CET	53	60696	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 1, 2021 09:09:07.419259071 CET	192.168.2.7	8.8.8.8	0x2a09	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:07.461031914 CET	192.168.2.7	8.8.8.8	0x6479	Standard query (0)	178.229.4.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Feb 1, 2021 09:09:07.495611906 CET	192.168.2.7	8.8.8.8	0xcee6	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:07.909754038 CET	192.168.2.7	8.8.8.8	0x1312	Standard query (0)	whatismyipaddress.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:12.591841936 CET	192.168.2.7	8.8.8.8	0x3f9a	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 1, 2021 09:09:25.589675903 CET	192.168.2.7	8.8.8.8	0xe914	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:27.342576981 CET	192.168.2.7	8.8.8.8	0x99bb	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:28.843076944 CET	192.168.2.7	8.8.8.8	0x8017	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:29.863385916 CET	192.168.2.7	8.8.8.8	0x57ac	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:31.158162117 CET	192.168.2.7	8.8.8.8	0x5741	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:32.426681042 CET	192.168.2.7	8.8.8.8	0xbf50	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:33.781709909 CET	192.168.2.7	8.8.8.8	0x2ee3	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:35.222217083 CET	192.168.2.7	8.8.8.8	0x82cb	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:36.815151930 CET	192.168.2.7	8.8.8.8	0xab5b	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:38.522720098 CET	192.168.2.7	8.8.8.8	0x8e76	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:41.057251930 CET	192.168.2.7	8.8.8.8	0x6841	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:43.564464092 CET	192.168.2.7	8.8.8.8	0x8d5b	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:45.562107086 CET	192.168.2.7	8.8.8.8	0x4620	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:46.048377037 CET	192.168.2.7	8.8.8.8	0x5bad	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:48.584228039 CET	192.168.2.7	8.8.8.8	0x4888	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:49.392095089 CET	192.168.2.7	8.8.8.8	0x6453	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:51.225687981 CET	192.168.2.7	8.8.8.8	0x5216	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:52.402592897 CET	192.168.2.7	8.8.8.8	0x706b	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:54.105652094 CET	192.168.2.7	8.8.8.8	0xea57	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:55.116416931 CET	192.168.2.7	8.8.8.8	0xd093	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:56.979058981 CET	192.168.2.7	8.8.8.8	0x40ab	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:59.813623905 CET	192.168.2.7	8.8.8.8	0xd45a	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:01.311166048 CET	192.168.2.7	8.8.8.8	0xd490	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:03.338654041 CET	192.168.2.7	8.8.8.8	0x6555	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:06.660375118 CET	192.168.2.7	8.8.8.8	0x2ec7	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:09.055143118 CET	192.168.2.7	8.8.8.8	0xd3a7	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:09.680104017 CET	192.168.2.7	8.8.8.8	0x2393	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:12.047480106 CET	192.168.2.7	8.8.8.8	0xa1bd	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:15.124363899 CET	192.168.2.7	8.8.8.8	0x9c5e	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:20.697560072 CET	192.168.2.7	8.8.8.8	0xa29e	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:28.323434114 CET	192.168.2.7	8.8.8.8	0x83f8	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:31.301953077 CET	192.168.2.7	8.8.8.8	0x6fdf	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:34.665638924 CET	192.168.2.7	8.8.8.8	0xb5c1	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:38.560153961 CET	192.168.2.7	8.8.8.8	0x13be	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:44.314034939 CET	192.168.2.7	8.8.8.8	0x358c	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:46.398916960 CET	192.168.2.7	8.8.8.8	0x10ea	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 1, 2021 09:10:46.617623091 CET	192.168.2.7	8.8.8.8	0xd7e0	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:47.651475906 CET	192.168.2.7	8.8.8.8	0xae10	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:50.737806082 CET	192.168.2.7	8.8.8.8	0xa11c	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:54.680552006 CET	192.168.2.7	8.8.8.8	0x505	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:58.185655117 CET	192.168.2.7	8.8.8.8	0xfa1	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:06.509452105 CET	192.168.2.7	8.8.8.8	0x95f6	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:07.648718119 CET	192.168.2.7	8.8.8.8	0xc742	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:09.420171976 CET	192.168.2.7	8.8.8.8	0x23b3	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:13.456777096 CET	192.168.2.7	8.8.8.8	0x111d	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:16.514466047 CET	192.168.2.7	8.8.8.8	0x9783	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:25.380804062 CET	192.168.2.7	8.8.8.8	0x385c	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:28.326708078 CET	192.168.2.7	8.8.8.8	0x7d35	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:31.996967077 CET	192.168.2.7	8.8.8.8	0x7d75	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:36.089000940 CET	192.168.2.7	8.8.8.8	0xd9ed	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:42.866492033 CET	192.168.2.7	8.8.8.8	0xca66	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:45.625840902 CET	192.168.2.7	8.8.8.8	0x5193	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:48.393935919 CET	192.168.2.7	8.8.8.8	0xab93	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:52.302521944 CET	192.168.2.7	8.8.8.8	0xde52	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:54.186583996 CET	192.168.2.7	8.8.8.8	0xc204	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:58.350061893 CET	192.168.2.7	8.8.8.8	0x5f3a	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:12:20.722248077 CET	192.168.2.7	8.8.8.8	0x5c6c	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 1, 2021 09:12:27.572242022 CET	192.168.2.7	8.8.8.8	0xf851	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 1, 2021 09:09:07.470134020 CET	8.8.8.8	192.168.2.7	0x2a09	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 1, 2021 09:09:07.470134020 CET	8.8.8.8	192.168.2.7	0x2a09	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:07.470134020 CET	8.8.8.8	192.168.2.7	0x2a09	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:07.470134020 CET	8.8.8.8	192.168.2.7	0x2a09	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:07.470134020 CET	8.8.8.8	192.168.2.7	0x2a09	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:07.470134020 CET	8.8.8.8	192.168.2.7	0x2a09	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:07.517234087 CET	8.8.8.8	192.168.2.7	0x6479	Name error (3)	178.229.4.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Feb 1, 2021 09:09:07.545397997 CET	8.8.8.8	192.168.2.7	0xcee6	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 1, 2021 09:09:07.545397997 CET	8.8.8.8	192.168.2.7	0xcee6	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 1, 2021 09:09:07.545397997 CET	8.8.8.8	192.168.2.7	0xcee6	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:07.545397997 CET	8.8.8.8	192.168.2.7	0xcee6	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:07.545397997 CET	8.8.8.8	192.168.2.7	0xcee6	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:07.545397997 CET	8.8.8.8	192.168.2.7	0xcee6	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:07.966373920 CET	8.8.8.8	192.168.2.7	0x1312	No error (0)	whatismyipaddress.com		104.16.155.36	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:07.966373920 CET	8.8.8.8	192.168.2.7	0x1312	No error (0)	whatismyipaddress.com		104.16.154.36	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:12.651006937 CET	8.8.8.8	192.168.2.7	0x3f9a	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:12.651006937 CET	8.8.8.8	192.168.2.7	0x3f9a	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:25.645951033 CET	8.8.8.8	192.168.2.7	0xe914	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:27.401709080 CET	8.8.8.8	192.168.2.7	0x99bb	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:28.904061079 CET	8.8.8.8	192.168.2.7	0x8017	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:29.919811964 CET	8.8.8.8	192.168.2.7	0x57ac	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:31.214703083 CET	8.8.8.8	192.168.2.7	0x5741	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:32.482837915 CET	8.8.8.8	192.168.2.7	0xbf50	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:33.838100910 CET	8.8.8.8	192.168.2.7	0x2ee3	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:35.281311989 CET	8.8.8.8	192.168.2.7	0x82cb	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:36.871431112 CET	8.8.8.8	192.168.2.7	0xab5b	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:38.570617914 CET	8.8.8.8	192.168.2.7	0x8e76	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:41.113337040 CET	8.8.8.8	192.168.2.7	0x6841	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:43.623867989 CET	8.8.8.8	192.168.2.7	0x8d5b	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:45.620537996 CET	8.8.8.8	192.168.2.7	0x4620	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:46.096478939 CET	8.8.8.8	192.168.2.7	0x5bad	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:48.635014057 CET	8.8.8.8	192.168.2.7	0x4888	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:49.451251984 CET	8.8.8.8	192.168.2.7	0x6453	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:51.273561954 CET	8.8.8.8	192.168.2.7	0x5216	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:52.461024046 CET	8.8.8.8	192.168.2.7	0x706b	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 1, 2021 09:09:54.153479099 CET	8.8.8.8	192.168.2.7	0xea57	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:55.164320946 CET	8.8.8.8	192.168.2.7	0xd093	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:57.040349960 CET	8.8.8.8	192.168.2.7	0x40ab	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:09:59.872525930 CET	8.8.8.8	192.168.2.7	0xd45a	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:01.359045029 CET	8.8.8.8	192.168.2.7	0xd490	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:03.396924019 CET	8.8.8.8	192.168.2.7	0x6555	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:06.716758013 CET	8.8.8.8	192.168.2.7	0x2ec7	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:09.113691092 CET	8.8.8.8	192.168.2.7	0xd3a7	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:09.730823040 CET	8.8.8.8	192.168.2.7	0x2393	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:12.105694056 CET	8.8.8.8	192.168.2.7	0xa1bd	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:15.183051109 CET	8.8.8.8	192.168.2.7	0x9c5e	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:20.745560884 CET	8.8.8.8	192.168.2.7	0xa29e	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:28.379592896 CET	8.8.8.8	192.168.2.7	0x83f8	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:31.358277082 CET	8.8.8.8	192.168.2.7	0x6fdf	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:34.722135067 CET	8.8.8.8	192.168.2.7	0xb5c1	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:38.619128942 CET	8.8.8.8	192.168.2.7	0x13be	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:44.362051964 CET	8.8.8.8	192.168.2.7	0x358c	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:46.446763039 CET	8.8.8.8	192.168.2.7	0x10ea	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 1, 2021 09:10:46.446763039 CET	8.8.8.8	192.168.2.7	0x10ea	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:46.446763039 CET	8.8.8.8	192.168.2.7	0x10ea	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:46.446763039 CET	8.8.8.8	192.168.2.7	0x10ea	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:46.446763039 CET	8.8.8.8	192.168.2.7	0x10ea	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:46.446763039 CET	8.8.8.8	192.168.2.7	0x10ea	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:46.668349981 CET	8.8.8.8	192.168.2.7	0xd7e0	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 1, 2021 09:10:46.668349981 CET	8.8.8.8	192.168.2.7	0xd7e0	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:46.668349981 CET	8.8.8.8	192.168.2.7	0xd7e0	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 1, 2021 09:10:46.668349981 CET	8.8.8.8	192.168.2.7	0xd7e0	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:46.668349981 CET	8.8.8.8	192.168.2.7	0xd7e0	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:46.668349981 CET	8.8.8.8	192.168.2.7	0xd7e0	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:47.707662106 CET	8.8.8.8	192.168.2.7	0xae10	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:50.785842896 CET	8.8.8.8	192.168.2.7	0xa11c	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:54.738976002 CET	8.8.8.8	192.168.2.7	0x505	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:10:58.234071016 CET	8.8.8.8	192.168.2.7	0xfa1	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:06.566015005 CET	8.8.8.8	192.168.2.7	0x95f6	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:07.699517012 CET	8.8.8.8	192.168.2.7	0xc742	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:07.699517012 CET	8.8.8.8	192.168.2.7	0xc742	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:09.469949961 CET	8.8.8.8	192.168.2.7	0x23b3	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:13.504885912 CET	8.8.8.8	192.168.2.7	0x111d	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:16.571065903 CET	8.8.8.8	192.168.2.7	0x9783	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:25.440049887 CET	8.8.8.8	192.168.2.7	0x385c	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:28.383287907 CET	8.8.8.8	192.168.2.7	0x7d35	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:32.046541929 CET	8.8.8.8	192.168.2.7	0x7d75	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:36.145209074 CET	8.8.8.8	192.168.2.7	0xd9ed	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:42.914623976 CET	8.8.8.8	192.168.2.7	0xca66	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:45.673918009 CET	8.8.8.8	192.168.2.7	0x5193	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:48.450041056 CET	8.8.8.8	192.168.2.7	0xab93	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:52.358680964 CET	8.8.8.8	192.168.2.7	0xde52	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:54.234499931 CET	8.8.8.8	192.168.2.7	0xc204	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:11:58.406557083 CET	8.8.8.8	192.168.2.7	0x5f3a	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:12:20.772998095 CET	8.8.8.8	192.168.2.7	0x5c6c	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 1, 2021 09:12:27.620141029 CET	8.8.8.8	192.168.2.7	0xf851	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- checkip.dyndns.org
- whatismyipaddress.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49723	216.146.43.71	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 09:09:07.645061016 CET	567	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive
Feb 1, 2021 09:09:07.720357895 CET	568	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 34 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.74</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49724	104.16.155.36	80	C:\Users\user\AppData\Local\Temp\hawkgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 09:09:08.062127113 CET	572	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Feb 1, 2021 09:09:08.110975981 CET	573	IN	HTTP/1.1 403 Forbidden Date: Mon, 01 Feb 2021 08:09:08 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 16 Connection: keep-alive X-Frame-Options: SAMEORIGIN Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Set-Cookie: __cfduid=dc0f576a6bdb740121a521b10e56e0abf1612166948; expires=Wed, 03-Mar-21 08:09:08 GMT; path=/; domain=.whatismyipaddress.com; HttpOnly; SameSite=Lax; Secure cf-request-id: 07fe3c7cfe00002c2a3a09c000000001 Server: cloudflare CF-RAY: 61aa30419eee2c2a-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 65 72 72 6f 72 20 63 6f 64 65 3a 20 31 30 32 30 Data Ascii: error code: 1020

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.7	49799	131.186.161.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 09:11:12.173727036 CET	6009	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Feb 1, 2021 09:11:12.333193064 CET	6010	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 34 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.74</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49725	216.146.43.71	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 09:09:08.100845098 CET	573	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Feb 1, 2021 09:09:08.176124096 CET	574	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 34 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.74</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49728	216.146.43.71	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 09:09:13.581939936 CET	608	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Feb 1, 2021 09:09:13.654850006 CET	609	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 34 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.74</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.7	49731	216.146.43.71	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 09:09:13.931035995 CET	612	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Feb 1, 2021 09:09:14.003762960 CET	613	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 34 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.74</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.7	49732	216.146.43.71	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 09:09:14.307152987 CET	625	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 09:09:14.379973888 CET	626	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 34 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.74</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.7	49787	131.186.161.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 09:10:47.107336998 CET	4601	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive
Feb 1, 2021 09:10:47.255414963 CET	4602	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 34 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.74</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.7	49789	131.186.161.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 09:10:48.602536917 CET	4673	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Feb 1, 2021 09:10:48.751554966 CET	4708	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 34 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.74</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.7	49796	131.186.161.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 09:11:09.370810032 CET	5998	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Feb 1, 2021 09:11:09.519227028 CET	5999	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 34 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.74</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.7	49798	131.186.161.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 09:11:10.578613997 CET	6002	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Feb 1, 2021 09:11:10.729428053 CET	6003	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 34 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.74</body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 1, 2021 09:09:12.846597910 CET	172.67.188.154	443	192.168.2.7	49727	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 10 02:00:00 CEST 2020	Tue Aug 10 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 1, 2021 09:11:08.080755949 CET	172.67.188.154	443	192.168.2.7	49795	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 10 02:00:00 CEST 2020	Tue Aug 10 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:09:26.070074081 CET	587	49738	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:26.070111990 CET	587	49737	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:26.542262077 CET	587	49739	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:26.542965889 CET	49739	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:26.733292103 CET	587	49739	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:26.734201908 CET	49739	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:26.924452066 CET	587	49739	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:27.786823988 CET	587	49742	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:27.787065029 CET	49742	587	192.168.2.7	199.193.7.228	EHLO 320946

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:09:27.977489948 CET	587	49742	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:27.978559017 CET	49742	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:28.168705940 CET	587	49742	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:29.291637897 CET	587	49743	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:30.307683945 CET	587	49745	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:30.307943106 CET	49745	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:30.498460054 CET	587	49745	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:31.624129057 CET	587	49748	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:31.624366045 CET	49748	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:31.828180075 CET	587	49748	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:32.868763924 CET	587	49751	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:32.869801998 CET	49751	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:33.060775995 CET	587	49751	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:33.062131882 CET	49751	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:33.252234936 CET	587	49751	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:34.245853901 CET	587	49753	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:34.246131897 CET	49753	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:34.448278904 CET	587	49753	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:34.449254990 CET	49753	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:34.650857925 CET	587	49753	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:35.666815996 CET	587	49754	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:35.667145014 CET	49754	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:35.857842922 CET	587	49754	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:35.858234882 CET	49754	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:36.048633099 CET	587	49754	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:37.258519888 CET	587	49755	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:37.259180069 CET	49755	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:37.451942921 CET	587	49755	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:09:37.452792883 CET	49755	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:37.643287897 CET	587	49755	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:38.968457937 CET	587	49756	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:39.210808039 CET	49756	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:39.402767897 CET	587	49756	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:39.403079033 CET	49756	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:39.593038082 CET	587	49756	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:41.499866962 CET	587	49757	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:41.500339985 CET	49757	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:41.697587967 CET	587	49757	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:41.697896957 CET	49757	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:41.888237000 CET	587	49757	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:44.015326023 CET	587	49759	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:44.015656948 CET	49759	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:44.206387043 CET	587	49759	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:44.206798077 CET	49759	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:44.397104025 CET	587	49759	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:46.010077000 CET	587	49760	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:46.010464907 CET	49760	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:46.200963020 CET	587	49760	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:46.201350927 CET	49760	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:46.391472101 CET	587	49760	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:46.482547998 CET	587	49761	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:46.483606100 CET	49761	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:46.674180984 CET	587	49761	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:46.674539089 CET	49761	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:46.864466906 CET	587	49761	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:49.021258116 CET	587	49762	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:49.021744013 CET	49762	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:49.212696075 CET	587	49762	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:49.213063002 CET	49762	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:49.403084040 CET	587	49762	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:49.839150906 CET	587	49763	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:09:49.841936111 CET	49763	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:50.032761097 CET	587	49763	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:50.050349951 CET	49763	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:50.241517067 CET	587	49763	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:51.662520885 CET	587	49765	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:51.662803888 CET	49765	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:51.853629112 CET	587	49765	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:51.853926897 CET	49765	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:52.044117928 CET	587	49765	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:52.848010063 CET	587	49766	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:52.848278046 CET	49766	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:53.039519072 CET	587	49766	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:53.039921999 CET	49766	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:53.230359077 CET	587	49766	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:54.561728954 CET	587	49767	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:54.563697100 CET	49767	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:54.766259909 CET	587	49767	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:54.766680002 CET	49767	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:54.968338966 CET	587	49767	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:55.573234081 CET	587	49768	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:55.573508978 CET	49768	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:55.775157928 CET	587	49768	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:55.775793076 CET	49768	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:55.977308035 CET	587	49768	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:09:57.456283092 CET	587	49769	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:09:57.574637890 CET	49769	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:09:57.765743017 CET	587	49769	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:09:57.766030073 CET	49769	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:09:57.956275940 CET	587	49769	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:00.257128954 CET	587	49770	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:00.257553101 CET	49770	587	192.168.2.7	199.193.7.228	EHLO 320946

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:10:00.448805094 CET	587	49770	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:00.449398994 CET	49770	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:00.639345884 CET	587	49770	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:01.746170998 CET	587	49771	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:01.746746063 CET	49771	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:01.938466072 CET	587	49771	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:01.939042091 CET	49771	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:02.129501104 CET	587	49771	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:03.783962011 CET	587	49772	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:03.786161900 CET	49772	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:03.977035999 CET	587	49772	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:03.977274895 CET	49772	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:04.167577028 CET	587	49772	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:07.101979017 CET	587	49775	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:07.102372885 CET	49775	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:07.292814016 CET	587	49775	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:07.293241024 CET	49775	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:07.483185053 CET	587	49775	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:09.535029888 CET	587	49776	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:09.535392046 CET	49776	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:09.738449097 CET	587	49776	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:09.738662958 CET	49776	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:09.940058947 CET	587	49776	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:10.126203060 CET	587	49777	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:10.126758099 CET	49777	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:10.319638014 CET	587	49777	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:10.322546005 CET	49777	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:10.512877941 CET	587	49777	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:12.493911982 CET	587	49778	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:12.494122028 CET	49778	587	192.168.2.7	199.193.7.228	EHLO 320946

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:10:12.684755087 CET	587	49778	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:12.685213089 CET	49778	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:12.875643015 CET	587	49778	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:15.577409029 CET	587	49779	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:15.579004049 CET	49779	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:15.769638062 CET	587	49779	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:16.006798029 CET	49779	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:16.196917057 CET	587	49779	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:21.133332014 CET	587	49780	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:21.133624077 CET	49780	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:21.325062990 CET	587	49780	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:21.329714060 CET	49780	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:21.520134926 CET	587	49780	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:28.787650108 CET	587	49781	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:28.788100004 CET	49781	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:28.989994049 CET	587	49781	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:28.992012024 CET	49781	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:29.193319082 CET	587	49781	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:31.768699884 CET	587	49782	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:31.769032001 CET	49782	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:31.971115112 CET	587	49782	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:31.971417904 CET	49782	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:32.173096895 CET	587	49782	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:35.146542072 CET	587	49783	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:35.637934923 CET	49783	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:35.828423023 CET	587	49783	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:35.830838919 CET	49783	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:36.021270037 CET	587	49783	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:39.004353046 CET	587	49784	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:39.004637003 CET	49784	587	192.168.2.7	199.193.7.228	EHLO 320946

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:10:39.195101023 CET	587	49784	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:39.195441961 CET	49784	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:39.385931969 CET	587	49784	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:44.915525913 CET	587	49785	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:44.915832043 CET	49785	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:44.942065954 CET	587	49786	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:44.980981112 CET	49786	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:45.106766939 CET	587	49785	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:45.107108116 CET	49785	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:45.182934046 CET	587	49786	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:45.183224916 CET	49786	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:45.297060013 CET	587	49785	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:45.384615898 CET	587	49786	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:48.117017984 CET	587	49788	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:48.117465973 CET	49788	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:48.319351912 CET	587	49788	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:48.319853067 CET	49788	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:48.520977020 CET	587	49788	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:51.170356035 CET	587	49790	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:51.170943975 CET	49790	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:51.361512899 CET	587	49790	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:51.363917112 CET	49790	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:51.554095984 CET	587	49790	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:55.186496973 CET	587	49791	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:55.186786890 CET	49791	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:10:55.388758898 CET	587	49791	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:55.389046907 CET	49791	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:55.590718031 CET	587	49791	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:10:58.619812965 CET	587	49792	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:10:58.620275974 CET	49792	587	192.168.2.7	199.193.7.228	EHLO 320946

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:10:58.810789108 CET	587	49792	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:10:58.811338902 CET	49792	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:10:59.001312971 CET	587	49792	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:06.989258051 CET	587	49794	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:06.989578009 CET	49794	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:11:07.180483103 CET	587	49794	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:07.180829048 CET	49794	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:07.371102095 CET	587	49794	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:09.861083031 CET	587	49797	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:09.861562014 CET	49797	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:11:10.053507090 CET	587	49797	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:10.192938089 CET	49797	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:10.383337021 CET	587	49797	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:13.928740025 CET	587	49800	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:13.929564953 CET	49800	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:11:14.120673895 CET	587	49800	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:14.120917082 CET	49800	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:14.311005116 CET	587	49800	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:16.957843065 CET	587	49801	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:16.958256006 CET	49801	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:11:17.149097919 CET	587	49801	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:17.149486065 CET	49801	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:17.339823961 CET	587	49801	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:25.847112894 CET	587	49802	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:25.847930908 CET	49802	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:11:26.050035954 CET	587	49802	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:26.050308943 CET	49802	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:26.251746893 CET	587	49802	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:28.802917957 CET	587	49803	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:28.833527088 CET	49803	587	192.168.2.7	199.193.7.228	EHLO 320946

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:11:29.023952961 CET	587	49803	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:29.026010036 CET	49803	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:29.216161013 CET	587	49803	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:32.431086063 CET	587	49804	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:32.431371927 CET	49804	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:11:32.621973991 CET	587	49804	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:32.622179985 CET	49804	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:32.812243938 CET	587	49804	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:36.533087015 CET	587	49805	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:36.533415079 CET	49805	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:11:36.724807978 CET	587	49805	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:36.725079060 CET	49805	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:36.915260077 CET	587	49805	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:43.302206039 CET	587	49806	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:43.302654028 CET	49806	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:11:43.494328022 CET	587	49806	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:43.495074987 CET	49806	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:43.689754963 CET	587	49806	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:46.058482885 CET	587	49807	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:46.058820009 CET	49807	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:11:46.249675035 CET	587	49807	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:46.250040054 CET	49807	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:46.440186024 CET	587	49807	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:48.836632013 CET	587	49808	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:48.837008953 CET	49808	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:11:49.028070927 CET	587	49808	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:49.029051065 CET	49808	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:49.219455004 CET	587	49808	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:52.743582964 CET	587	49809	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:52.743916035 CET	49809	587	192.168.2.7	199.193.7.228	EHLO 320946

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:11:52.934200048 CET	587	49809	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:52.936620951 CET	49809	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:53.126874924 CET	587	49809	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:54.619864941 CET	587	49810	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:54.647011995 CET	49810	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:11:54.837656021 CET	587	49810	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:54.846385956 CET	49810	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:55.036645889 CET	587	49810	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:58.793193102 CET	587	49811	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:58.793859005 CET	49811	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:11:58.984339952 CET	587	49811	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:58.989474058 CET	49811	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:59.181180000 CET	587	49811	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:11:59.259850025 CET	587	49812	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:11:59.263751984 CET	49812	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:11:59.466017008 CET	587	49812	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:11:59.466502905 CET	49812	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:11:59.670650959 CET	587	49812	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:01.388549089 CET	587	49813	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:01.392748117 CET	49813	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:01.584903002 CET	587	49813	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:01.585129023 CET	49813	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:01.777091980 CET	587	49813	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:01.961464882 CET	587	49814	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:01.961730003 CET	49814	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:02.152362108 CET	587	49814	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:02.152602911 CET	49814	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:02.342701912 CET	587	49814	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:03.983864069 CET	587	49815	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:03.985244989 CET	49815	587	192.168.2.7	199.193.7.228	EHLO 320946

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:12:04.177360058 CET	587	49815	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:04.177632093 CET	49815	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:04.367909908 CET	587	49815	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:04.554404974 CET	587	49816	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:04.554629087 CET	49816	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:04.746764898 CET	587	49816	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:04.747014999 CET	49816	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:04.938620090 CET	587	49816	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:06.715044022 CET	587	49817	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:06.715224981 CET	49817	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:06.907890081 CET	587	49817	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:06.908099890 CET	49817	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:07.098213911 CET	587	49817	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:07.172305107 CET	587	49818	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:07.172955990 CET	49818	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:07.364784956 CET	587	49818	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:07.367861986 CET	49818	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:07.557900906 CET	587	49818	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:09.752533913 CET	587	49819	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:09.752826929 CET	49819	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:09.954586983 CET	587	49819	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:09.954838037 CET	49819	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:10.156296015 CET	587	49819	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:12.457586050 CET	587	49820	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:12.461524010 CET	49820	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:12.652834892 CET	587	49820	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:12.653201103 CET	49820	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:12.843120098 CET	587	49820	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:13.160633087 CET	587	49821	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:13.160934925 CET	49821	587	192.168.2.7	199.193.7.228	EHLO 320946

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:12:13.351763010 CET	587	49821	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:13.352152109 CET	49821	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:13.542532921 CET	587	49821	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:15.160967112 CET	587	49822	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:15.161264896 CET	49822	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:15.352116108 CET	587	49822	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:15.352284908 CET	49822	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:15.542378902 CET	587	49822	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:15.737823963 CET	587	49823	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:15.738181114 CET	49823	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:15.928592920 CET	587	49823	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:15.928860903 CET	49823	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:16.118854046 CET	587	49823	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:18.322319984 CET	587	49824	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:18.322577953 CET	49824	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:18.524908066 CET	587	49824	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:18.525171041 CET	49824	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:18.726607084 CET	587	49824	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:21.158082008 CET	587	49825	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:21.158349991 CET	49825	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:21.349931002 CET	587	49825	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:21.350169897 CET	49825	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:21.540354967 CET	587	49825	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:21.732372999 CET	587	49826	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:21.732527971 CET	49826	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:21.924051046 CET	587	49826	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:21.924277067 CET	49826	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:22.114543915 CET	587	49826	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:23.744049072 CET	587	49827	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:23.746469975 CET	49827	587	192.168.2.7	199.193.7.228	EHLO 320946

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:12:23.951492071 CET	587	49827	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:23.951726913 CET	49827	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:24.153302908 CET	587	49827	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:24.308339119 CET	587	49828	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:24.308604956 CET	49828	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:24.500384092 CET	587	49828	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:24.500648975 CET	49828	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:24.690989017 CET	587	49828	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:26.428899050 CET	587	49829	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:26.430429935 CET	49829	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:26.621756077 CET	587	49829	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:26.622150898 CET	49829	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:26.812263012 CET	587	49829	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:26.874424934 CET	587	49830	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:26.874878883 CET	49830	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:27.065745115 CET	587	49830	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:27.066075087 CET	49830	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:27.256088018 CET	587	49830	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:28.022768974 CET	587	49831	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:28.023227930 CET	49831	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:28.214212894 CET	587	49831	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:28.214597940 CET	49831	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:28.404983997 CET	587	49831	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:29.121412992 CET	587	49832	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:29.121841908 CET	49832	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:29.312783003 CET	587	49832	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:29.313154936 CET	49832	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:29.473010063 CET	587	49833	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:29.473433018 CET	49833	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:29.503571033 CET	587	49832	199.193.7.228	192.168.2.7	220 Ready to start TLS

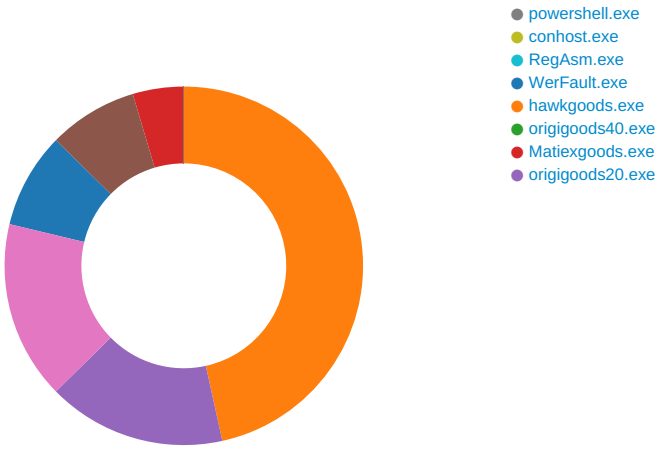
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 1, 2021 09:12:29.664067984 CET	587	49833	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:29.664412022 CET	49833	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:29.854438066 CET	587	49833	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:32.030654907 CET	587	49834	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:32.030946970 CET	49834	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:32.221685886 CET	587	49834	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:32.221980095 CET	49834	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:32.411899090 CET	587	49834	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:34.612339020 CET	587	49835	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:34.612685919 CET	49835	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:34.803423882 CET	587	49835	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:34.803705931 CET	49835	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:34.994025946 CET	587	49835	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 1, 2021 09:12:35.593287945 CET	587	49836	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 1, 2021 09:12:35.593636036 CET	49836	587	192.168.2.7	199.193.7.228	EHLO 320946
Feb 1, 2021 09:12:35.796199083 CET	587	49836	199.193.7.228	192.168.2.7	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 1, 2021 09:12:35.796957970 CET	49836	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 1, 2021 09:12:35.998684883 CET	587	49836	199.193.7.228	192.168.2.7	220 Ready to start TLS

Code Manipulations

Statistics

Behavior

- Orders.exe
- powershell.exe
- conhost.exe
- RegAsm.exe
- hawkgoods.exe
- origigoods40.exe
- Matiexgoods.exe
- origigoods20.exe
- WerFault.exe
- dw20.exe
- vbc.exe
- vbc.exe
- WerFault.exe
- WerFault.exe
- netsh.exe
- conhost.exe
- I$s#$lT3ssl.exe



Click to jump to process

System Behavior

Analysis Process: Orders.exe PID: 6824 Parent PID: 5848

General

Start time:	09:08:45
Start date:	01/02/2021
Path:	C:\Users\user\Desktop\Orders.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Orders.exe'
Imagebase:	0x920000
File size:	1630720 bytes
MD5 hash:	E85DAF3A43F107B213310A53BFD35AA9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.361141701.0000000004154000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000001.00000002.361141701.0000000004154000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.361141701.0000000004154000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.361141701.0000000004154000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.361141701.0000000004154000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.361141701.0000000004154000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D34CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D34CF06	unknown

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	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D325705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D32CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D325705	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D30D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D30D72F	unknown
C:\Users\user\Desktop\Orders.exe	unknown	4096	success or wait	1	6D30D72F	unknown
C:\Users\user\Desktop\Orders.exe	unknown	512	success or wait	1	6D30D72F	unknown

Analysis Process: powershell.exe PID: 6896 Parent PID: 6824

General

Start time:	09:08:47
Start date:	01/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\Desktop\Orders.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe'
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C0F5B28	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C0F5B28	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D34CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D34CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_03w4pbbs.uza.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C191E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1uftfplo.nuv.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C191E60	CreateFileW
C:\Users\user\Documents\20210201	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C19BEFF	CreateDirectoryW
C:\Users\user\Documents\20210201\PowerShell_transcript.320946.GXJdt0T3.20210201090850.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C191E60	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C19DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C19DD66	CopyFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C191E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_03w4pbbs.uza.ps1	success or wait	1	6C196A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1uftfplo.nuv.psm1	success or wait	1	6C196A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_03w4pbbs.uza.ps1	unknown	1	31	1	success or wait	1	6C191B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1uftfplo.nuv.psm1	unknown	1	31	1	success or wait	1	6C191B4F	WriteFile
C:\Users\user\Documents\20210201\PowerShell_transcript.320946.GXJdt0T3.20210201090850.txt	unknown	3	ef bb bf	...	success or wait	1	6C191B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210201\PowerShell_transcript.320946.GXJdt0T3.20210201090850.txt	unknown	746	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 32 30 31 30 39 30 39 30 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 32 30 39 34 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f	*************************..Windows PowerShell transcript start..Start time: 20210201090908..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 320946 (Microsoft Windows NT 10.0.17134.0)..Host Applicatio	success or wait	11	6C191B4F	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe	0	262144	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 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 71 98 c2 c3 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 d8 18 00 00 08 00 00 00 00 00 00 ce f6 18 00 00 20 00 00 00 00 19 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 40 19 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....$.......PE..L...q..........................0................. ....@.........................@............@...............................	success or wait	7	6C19DD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C19DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 08 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module..... .inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6C191B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3907	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6C191B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 12 0f 00 00 16 00 00 00 e9 0d d2 04 17 09 05 09 c8 07 00 00 00 00 f8 02 46 00 c7 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e..... .....F.....@.....	success or wait	1	6D6176FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 29 00 00 00 0e 00 20 00	H.....<@.^...L."My..:)..... .	success or wait	17	6D6176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6D6176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	6D6176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	8	6D6176FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 f9 3e 40 01 33 67 40 01 ce 67 40 01 2f 67 40 01 2e 35 40 01 2d 35 40 01 cb 00 40 00 99 01 40 00 56 01 40 00 fb 00 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 00 01 dc 71 00	.....T.@..>@.3g@..g@./g@..5@.-5@...@...@.V.@...@.H.@.X.@.[.@.NT@.HT@..S@..S@.hT@..S@..S@..S@.\.@..T@..T@.@X@.?X@..T@..S@..S@..T@..T@.xT@.zT@..T@.=M@.DM@.:M@."M@.M@.!M@.;M@..D@..D@.@M@.<M@.$M@.8M..?M..BM...D..mE..EM...q.	success or wait	8	6D6176FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D325705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D32CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D32CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D32CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D325705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D325705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2803DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D2803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D325705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D331F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21304	success or wait	1	6D33203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2803DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C191B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C191B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6C191B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6C191B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C191B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C191B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C191B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C191B4F	ReadFile

Analysis Process: conhost.exe PID: 6912 Parent PID: 6896

General

Start time:	09:08:47
Start date:	01/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 7000 Parent PID: 6824

General

Start time:	09:08:49
Start date:	01/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xbc0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000004.00000003.246774488.0000000003670000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000003.246774488.0000000003670000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000003.246774488.0000000003670000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000003.246774488.0000000003670000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000003.246774488.0000000003670000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.251635347.0000000003EBD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.256024655.0000000001293000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.255331829.0000000003EBD000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000004.00000002.256501427.0000000000403000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000004.00000002.256501427.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000002.256501427.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000002.256501427.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000002.256501427.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000002.256501427.0000000000403000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.249596324.0000000001293000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.254611636.0000000003BAB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.255709181.0000000003E51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.249733611.0000000003BAB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.251501400.0000000001293000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.246897806.0000000001293000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.246965930.0000000003B41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.251891646.0000000003BAB000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\hawkgoods.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	660ED258	CreateFileA
C:\Users\user~1\AppData\Local\Temp\origigoods40.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	660ED258	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\Matiexgoods.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	660ED258	CreateFileA
C:\Users\user~1\AppData\Local\Temp\origigoods20.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	660ED258	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	unknown	532992	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 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 a6 af 06 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 ec 07 00 00 34 00 00 00 00 00 00 de 0b 08 00 00 20 00 00 00 00 00 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 80 08 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......`.......... ....4........... ....@.. ....@................	success or wait	1	660ED8F8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\origigoods40.exe	unknown	221696	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 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 ed b0 06 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 58 03 00 00 08 00 00 00 00 00 00 3e 76 03 00 00 20 00 00 00 00 00 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 03 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......`.......... ....X..........>v... ....@.. ....@.................	success or wait	1	660ED8F8	WriteFile
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	unknown	455680	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 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 b4 ae 06 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 ea 06 00 00 08 00 00 00 00 00 00 7e 08 07 00 00 20 00 00 00 20 07 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 60 07 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......`.......... .................~.... ... ....@.. .......................` ....@.................	success or wait	1	660ED8F8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\origigoods20.exe	unknown	220672	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 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 a5 b0 06 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 56 03 00 00 06 00 00 00 00 00 00 ee 74 03 00 00 20 00 00 00 00 00 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 03 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......`.......... ....V...........t... ....@.. ....@................	success or wait	1	660ED8F8	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: hawkgoods.exe PID: 7064 Parent PID: 7000

General

Start time:	09:08:52
Start date:	01/02/2021
Path:	C:\Users\user\AppData\Local\Temp\hawkgoods.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user~1\AppData\Local\Temp\hawkgoods.exe' 0
Imagebase:	0x670000
File size:	532992 bytes
MD5 hash:	FFDB58533D5D1362E896E96FB6F02A95
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000002.503829429.0000000003E11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000002.503829429.0000000003E11000.00000004.00000001.sdmp, Author: Joe Security • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000006.00000002.520293841.0000000007DA0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000006.00000000.249359249.0000000000672000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000000.249359249.0000000000672000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000006.00000000.249359249.0000000000672000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000000.249359249.0000000000672000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000006.00000000.249359249.0000000000672000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000006.00000002.489137354.0000000000672000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000002.489137354.0000000000672000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000006.00000002.489137354.0000000000672000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000002.489137354.0000000000672000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000006.00000002.489137354.0000000000672000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000006.00000002.520422224.0000000007DF0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000006.00000002.498581730.0000000002E11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000006.00000002.498581730.0000000002E11000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000006.00000002.498581730.0000000002E11000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Local\Temp\hawkgoods.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 96%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown
C:\Users\user\AppData\Roaming\pid.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	DDBCAB	CreateFileW
C:\Users\user\AppData\Roaming\pidloc.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	DDBCAB	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	37 30 36 34	7064	success or wait	1	2A90093	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	50	43 3a 5c 55 73 65 72 73 5c 46 52 4f 4e 54 44 7e 31 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 68 61 77 6b 67 6f 6f 64 73 2e 65 78 65	C:\Users\user~1\AppData\Local\Temp\hawkgoods.exe	success or wait	1	2A90093	WriteFile

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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	2A90093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2A90093	ReadFile
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	unknown	4096	success or wait	1	7253BF06	unknown
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7253BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7253BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\assembly\GAC_MSIL\System.Runtime.Remoting\2.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	4096	success or wait	1	7253BF06	unknown
C:\Windows\assembly\GAC_MSIL\System.Runtime.Remoting\2.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\assembly\GAC_MSIL\System.Runtime.Remoting\2.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	512	success or wait	1	7253BF06	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	dword	2	1	success or wait	1	2A94A02	RegSetValueExW

Analysis Process: origigoods40.exe PID: 7116 Parent PID: 7000

General

Start time:	09:08:52
Start date:	01/02/2021
Path:	C:\Users\user\AppData\Local\Temp\origigoods40.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user~1\AppData\Local\Temp\origigoods40.exe' 0
Imagebase:	0xf0000
File size:	221696 bytes
MD5 hash:	AE36F0D16230B9F41FFECBD3C5B1D660
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.251123537.00000000000F2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.427828296.00000000000F2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.445240887.0000000002501000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.445240887.0000000002501000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\origigoods40.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 43%, Metadefender, Browse • Detection: 83%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D34CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D34CF06	unknown

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	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D325705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D32CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C191B4F	ReadFile

Analysis Process: Matiexgoods.exe PID: 7148 Parent PID: 7000

General

Start time:	09:08:53
Start date:	01/02/2021
Path:	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user~1\AppData\Local\Temp\Matiexgoods.exe' 0
Imagebase:	0x320000
File size:	455680 bytes
MD5 hash:	80C61B903400B534858D047DD0919F0E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000009.00000000.253083713.0000000000322000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: C:\Users\user\AppData\Local\Temp\Matiexgoods.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D34CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D34CF06	unknown
C:\Users\user\Documents\Matiex Keylogger	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	7	6C19BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\container.dat	success or wait	1	6C196A95	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	success or wait	1	6C196A95	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	success or wait	1	6C196A95	DeleteFileW
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	success or wait	1	6C196A95	DeleteFileW
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	success or wait	5	6C196A95	DeleteFileW

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\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D325705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D32CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C191B4F	ReadFile
unknown	unknown	4096	success or wait	1	6C191B4F	ReadFile
unknown	unknown	4096	pipe broken	1	6C191B4F	ReadFile
unknown	unknown	4096	pipe broken	1	6C191B4F	ReadFile
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	unknown	17408	success or wait	48	6C191B4F	ReadFile
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	unknown	17408	end of file	1	6C191B4F	ReadFile
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	unknown	17408	success or wait	283	6C191B4F	ReadFile
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	unknown	17408	end of file	6	6C191B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: origigoods20.exe PID: 5580 Parent PID: 7000

General

Start time:	09:08:54
Start date:	01/02/2021
Path:	C:\Users\user\AppData\Local\Temp\origigoods20.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user~1\AppData\Local\Temp\origigoods20.exe' 0
Imagebase:	0x680000
File size:	220672 bytes
MD5 hash:	61DC57C6575E1F3F2AE14C1B332AD2FB
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.416654984.0000000000682000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.254178193.0000000000682000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.448946669.0000000002E51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.448946669.0000000002E51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\origigoods20.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 43%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	low

Analysis Process: WerFault.exe PID: 2116 Parent PID: 6824

General

Start time:	09:08:54
Start date:	01/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6824 -s 1104
Imagebase:	0xe0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: dw20.exe PID: 6008 Parent PID: 7064

General

Start time:	09:09:08
Start date:	01/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2132
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: 6288 Parent PID: 7064

General

Start time:	09:09:11
Start date:	01/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe

Wow64 process (32bit):	
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: 976 Parent PID: 7064

General

Start time:	09:09:11
Start date:	01/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 2324 Parent PID: 7064

General

Start time:	09:09:14
Start date:	01/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7064 -s 2132
Imagebase:	0xe0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000017.00000002.450940492.0000000005360000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000017.00000002.450940492.0000000005360000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000017.00000002.450940492.0000000005360000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: WerFault.exe PID: 6308 Parent PID: 976

General

Start time:	09:09:14

Start date:	01/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 976 -s 176
Imagebase:	0xe0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: netsh.exe PID: 6780 Parent PID: 7148

General

Start time:	09:09:37
Start date:	01/02/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	'netsh' wlan show profile
Imagebase:	0x1650000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 1404 Parent PID: 6780

General

Start time:	09:09:39
Start date:	01/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: I$s#$IT3ssl.exe PID: 5184 Parent PID: 3292

General

Start time:	09:09:48
Start date:	01/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$IT3ssl.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s #$IT3ssl.exe'
Imagebase:	0x770000
File size:	1630720 bytes

MD5 hash:	E85DAF3A43F107B213310A53BFD35AA9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001E.00000002.638917740.0000000003D14000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 0000001E.00000002.638917740.0000000003D14000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001E.00000002.638917740.0000000003D14000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001E.00000002.638917740.0000000003D14000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001E.00000002.638917740.0000000003D14000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001E.00000002.638917740.0000000003D14000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 22%, ReversingLabs
Reputation:	low

Analysis Process: powershell.exe PID: 5296 Parent PID: 5184

General

Start time:	09:09:51
Start date:	01/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\l$s#$lT3ssl.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\l$s#$lT3ssl.exe'
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 5428 Parent PID: 5296

General

Start time:	09:09:52
Start date:	01/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RegAsm.exe PID: 5468 Parent PID: 5184

General

Start time:	09:09:54
Start date:	01/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xd30000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000003.409742316.0000000003D5B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000003.401891116.0000000001453000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000003.402397368.000000000405D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000003.413799540.0000000003FF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000003.392335998.0000000003CF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000021.00000002.419539821.0000000000403000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000021.00000002.419539821.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000021.00000002.419539821.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000021.00000002.419539821.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000021.00000002.419539821.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000021.00000002.419539821.0000000000403000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000003.397781851.0000000003D5B000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000021.00000003.385572050.0000000003750000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000021.00000003.385572050.0000000003750000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000021.00000003.385572050.0000000003750000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000021.00000003.385572050.0000000003750000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000021.00000003.385572050.0000000003750000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000021.00000003.385572050.0000000003750000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000003.402832252.0000000003D5B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000003.388318104.0000000001453000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000021.00000003.399192472.0000000003940000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000003.412233865.000000000405D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000003.397017946.0000000001453000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000003.415754718.0000000001453000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000021.00000003.400705321.0000000003940000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000021.00000003.391416001.0000000003C10000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: WerFault.exe PID: 2160 Parent PID: 5184

General

Start time:	09:09:59
Start date:	01/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5184 -s 1096
Imagebase:	0xe0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: hawkgoods.exe PID: 4388 Parent PID: 5468

General

Start time:	09:10:00
Start date:	01/02/2021
Path:	C:\Users\user\AppData\Local\Temp\hawkgoods.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user~1\AppData\Local\Temp\hawkgoods.exe' 0
Imagebase:	0x3d0000
File size:	532992 bytes
MD5 hash:	FFDB58533D5D1362E896E96FB6F02A95
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000024.00000000.396471028.00000000003D2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000024.00000000.396471028.00000000003D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000024.00000000.396471028.00000000003D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000024.00000000.396471028.00000000003D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000024.00000000.396471028.00000000003D2000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000024.00000002.403481991.00000000003D2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000024.00000002.403481991.00000000003D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000024.00000002.403481991.00000000003D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000024.00000002.403481991.00000000003D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000024.00000002.403481991.00000000003D2000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: origigoods40.exe PID: 5692 Parent PID: 5468

General

Start time:	09:10:01
Start date:	01/02/2021
Path:	C:\Users\user\AppData\Local\Temp\origigoods40.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user~1\AppData\Local\Temp\origigoods40.exe' 0
Imagebase:	0x7ff724940000
File size:	221696 bytes
MD5 hash:	AE36F0D16230B9F41FFECBD3C5B1D660
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000025.00000000.399012238.0000000000E72000.00000002.00020000.sdmp, Author: Joe Security

Analysis Process: Matiexgoods.exe PID: 6724 Parent PID: 5468

General

Start time:	09:10:04
Start date:	01/02/2021
Path:	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user~1\AppData\Local\Temp\Matiexgoods.exe' 0
Imagebase:	0x6e0000
File size:	455680 bytes
MD5 hash:	80C61B903400B534858D047DD0919F0E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000026.00000000.405296344.00000000006E2000.00000002.00020000.sdmp, Author: Joe Security

Analysis Process: origigoods20.exe PID: 5612 Parent PID: 5468

General

Start time:	09:10:05
Start date:	01/02/2021
Path:	C:\Users\user\AppData\Local\Temp\origigoods20.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user~1\AppData\Local\Temp\origigoods20.exe' 0
Imagebase:	0x530000
File size:	220672 bytes
MD5 hash:	61DC57C6575E1F3F2AE14C1B332AD2FB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000027.00000000.408264262.0000000000532000.00000002.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis