ID: 347154
Sample Name:
PO_Invoices_pdf.exe
Cookbook: default.jbs
Time: 08:50:38
Date: 02/02/2021
Version: 31.0.0 Emerald

Table of Contents

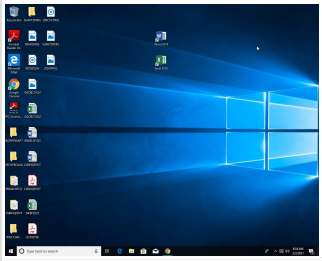
Analysis Report PO_Invoices_pdf.exe

Overview

General Information

Sample Name:	PO_Invoices_pdf.exe
Analysis ID:	347154
MD5:	59d7d8d5dd3e00..
SHA1:	b249b28d088d54..
SHA256:	ef715cd322f0a80..
Tags:	exe HawkEye Yahoo

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

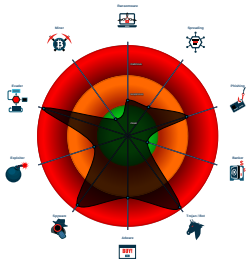
HawkEye AgentTesla MailPassView Matiex

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**
- PO_Invoices_pdf.exe (PID: 5372 cmdline: 'C:\Users\user\Desktop\PO_Invoices_pdf.exe' MD5: 59D7D8D5DD3E0055E7C0DCC75897F569)
  - powershell.exe (PID: 5904 cmdline: 'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\Desktop\PO_Invoices_pdf.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 8 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegAsm.exe (PID: 4888 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - hawkgoods.exe (PID: 3724 cmdline: 'C:\Users\user~1\AppData\Local\Temp\hawkgoods.exe' 0 MD5: FFDB58533D5D1362E896E96FB6F02A95)
      - dw20.exe (PID: 6684 cmdline: dw20.exe -x -s 2164 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
      - vbc.exe (PID: 6852 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: 6868 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: 7028 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3724 -s 1996 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - origigoods40.exe (PID: 6172 cmdline: 'C:\Users\user~1\AppData\Local\Temp\origigoods40.exe' 0 MD5: AE36F0D16230B9F41FFECBD3C5B1D660)
    - Matiexgoods.exe (PID: 6264 cmdline: 'C:\Users\user~1\AppData\Local\Temp\Matiexgoods.exe' 0 MD5: 80C61B903400B534858D047DD0919F0E)
      - netsh.exe (PID: 1744 cmdline: 'netsh' wlan show profile MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - conhost.exe (PID: 1200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - origigoods20.exe (PID: 6352 cmdline: 'C:\Users\user~1\AppData\Local\Temp\origigoods20.exe' 0 MD5: 61DC57C6575E1F3F2AE14C1B332AD2FB)
- I$s#$lT3ssl.exe (PID: 1808 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe' MD5: 59D7D8D5DD3E0055E7C0DCC75897F569)
  - powershell.exe (PID: 6908 cmdline: 'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\AppData\Roaming\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' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegAsm.exe (PID: 4828 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - hawkgoods.exe (PID: 5440 cmdline: 'C:\Users\user~1\AppData\Local\Temp\hawkgoods.exe' 0 MD5: FFDB58533D5D1362E896E96FB6F02A95)
      - dw20.exe (PID: 5252 cmdline: dw20.exe -x -s 2092 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
      - vbc.exe (PID: 5776 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: 6108 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: 4776 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5440 -s 940 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - origigoods40.exe (PID: 3080 cmdline: 'C:\Users\user~1\AppData\Local\Temp\origigoods40.exe' 0 MD5: AE36F0D16230B9F41FFECBD3C5B1D660)
    - Matiexgoods.exe (PID: 6532 cmdline: 'C:\Users\user~1\AppData\Local\Temp\Matiexgoods.exe' 0 MD5: 80C61B903400B534858D047DD0919F0E)
    - origigoods20.exe (PID: 7160 cmdline: 'C:\Users\user~1\AppData\Local\Temp\origigoods20.exe' 0 MD5: 61DC57C6575E1F3F2AE14C1B332AD2FB)
- **cleanup**

Malware Configuration

Threatname: HawkEye


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


Threatname: Agenttesla


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


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	
dropped/hawkgoods.exe	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x7423:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x7423:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
Click to see the 10 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000003.273863512.0000000003E4D000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000003.285132773.0000000003DE1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001F.00000000.423374232.000000000722000.00000002.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001A.00000003.425880345.0000000003A2D000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000023.00000002.465758929.0000000000400000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 99 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
7.0.origigoods40.exe.c30000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
35.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
28.2.origigoods40.exe.e20000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

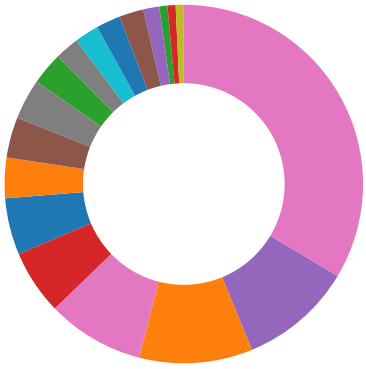
Source	Rule	Description	Author	Strings
31.2.origigoods20.exe.720000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 271 entries				

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
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

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

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)

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 Instant Messenger accounts or passwords

Tries to steal Mail credentials (via file access)

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Detected HawkEye Rat

Yara detected AgentTesla

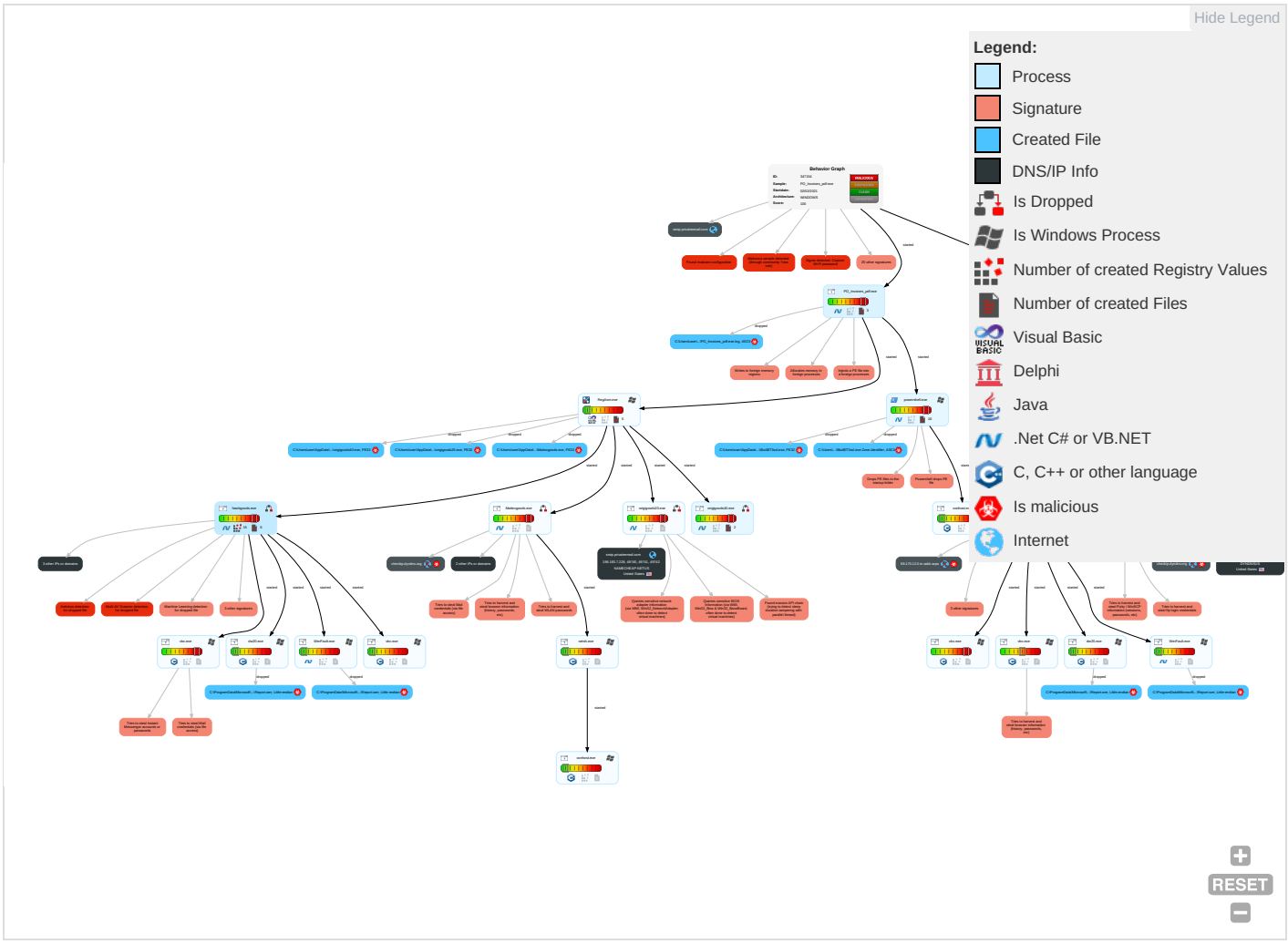
Yara detected HawkEye Keylogger

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 Medium
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 2	System Information Discovery 1 2 6	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltr
Local Accounts	Command and Scripting Interpreter 1	Logon Script (Mac)	Process Injection 4 1 1	Software Packing 1 3	Credentials In Files 1	Query Registry 1	Distributed Component Object Model	Input Capture 2 1 1	Scheduled Trans
Cloud Accounts	PowerShell 2	Network Logon Script	Registry Run Keys / Startup Folder 1 2	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 2 5 1	SSH	Clipboard Data 1	Data Transfer Siz Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 6	VNC	GUI Input Capture	Exfiltration Over Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 6	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Proto
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encry Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 4 1 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encr Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obf Non-C2 Protocol

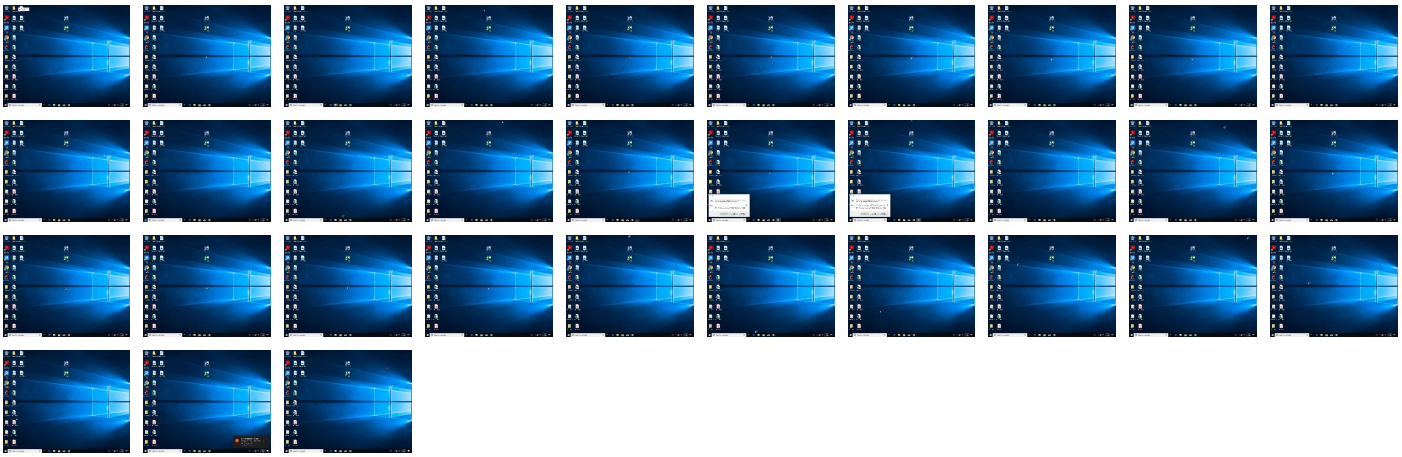
Behavior Graph



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
PO_Invoices_pdf.exe	18%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	
PO_Invoices_pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\origigoods40.exe	100%	Avira	TR/Spy.Gen8	
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\origigoods20.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\origigoods40.exe	100%	Joe Sandbox ML		
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\origigoods20.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	89%	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	82%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.origigoods40.exe.c30000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
30.0.Matiexgoods.exe.bd0000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
8.2.Matiexgoods.exe.f70000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
28.2.origigoods40.exe.e20000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
31.2.origigoods20.exe.720000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
10.0.origigoods20.exe.e0000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
10.2.origigoods20.exe.e0000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
27.2.hawkgoods.exe.a40000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
27.2.hawkgoods.exe.a40000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
6.0.hawkgoods.exe.2f0000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
6.0.hawkgoods.exe.2f0000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
30.2.Matiexgoods.exe.bd0000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
26.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
26.2.RegAsm.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
26.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
26.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
26.2.RegAsm.exe.4031bf.2.unpack	100%	Avira	TR/Inject.vcoldi		Download File
8.0.Matiexgoods.exe.f70000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
5.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
5.2.RegAsm.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
5.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
5.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.2.hawkgoods.exe.2f0000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
6.2.hawkgoods.exe.2f0000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
28.0.origigoods40.exe.e20000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
23.2.I$s#$lT3ssl.exe.4158f3f.3.unpack	100%	Avira	TR/Inject.vcoldi		Download File
7.2.origigoods40.exe.c30000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
31.0.origigoods20.exe.720000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
27.0.hawkgoods.exe.a40000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
27.0.hawkgoods.exe.a40000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.PO_Invoices_pdf.exe.4396d80.5.unpack	100%	Avira	TR/Inject.vcoldi		Download File
5.2.RegAsm.exe.4031bf.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
35.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
18.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
0.2.PO_Invoices_pdf.exe.4398f3f.4.unpack	100%	Avira	TR/Inject.vcoldi		Download File
23.2.I$s#$lT3ssl.exe.4156d80.4.unpack	100%	Avira	TR/Inject.vcoldi		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	

Source	Detection	Scanner	Label	Link
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://www.zhongyicts.com.cnaN	0%	Avira URL Cloud	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	
http://tempuri.org/DataSet1.xsd	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnR	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://www.founder.com.cn/cnT	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://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.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://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.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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://www.founder.com.cn/cn/cThe	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	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.typography.net-siu	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadTimeZoneCountryNameCountryCodehttps://www.geodatatool.com/en/?ip=/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadTimeZoneCountryNameCountryCodehttps://www.geodatatool.com/en/?ip=/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadTimeZoneCountryNameCountryCodehttps://www.geodatatool.com/en/?ip=/	0%	URL Reputation	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://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	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://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	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://www.founder.com.cn/cniac	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.goodfont.co.kr9	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	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://www.carterandcone.como.R	0%	Avira URL Cloud	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	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	104.21.19.200	true	false		unknown
smtp.privateemail.com	199.193.7.228	true	false		high
checkip.dyndns.com	131.186.113.70	true	false		unknown
69.170.12.0.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

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	origigoods40.exe, 00000007.00000002.455680542.0000000002FE1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cnaN	PO_Invoices_pdf.exe, 00000000.00000003.250141662.0000000006515000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	Matiexgoods.exe, 00000008.00000003.461245193.00000000068F6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/PesterL	powershell.exe, 00000003.00000002.382114009.0000000004983000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false		high
http://tempuri.org/DataSet1.xsd	PO_Invoices_pdf.exe, PO_Invoices_pdf.exe, 00000000.00000002.277417941.00000000040A8000.00000004.00000001.sdmp, powershell.exe, 00000003.00000003.370812465.0000000008DB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnR	PO_Invoices_pdf.exe, 00000000.00000003.249338917.0000000006516000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000003.00000002.386788256.00000000058A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnT	PO_Invoices_pdf.exe, 00000000.00000003.250141662.0000000006515000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false		high
http://ns.adobe.c/g	Matiexgoods.exe, 00000008.00000003.443342117.0000000009311000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	PO_Invoices_pdf.exe, 00000000.00000003.250459528.0000000006513000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://csARxe.com	origigoods40.exe, 00000007.00000002.455680542.0000000002FE1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

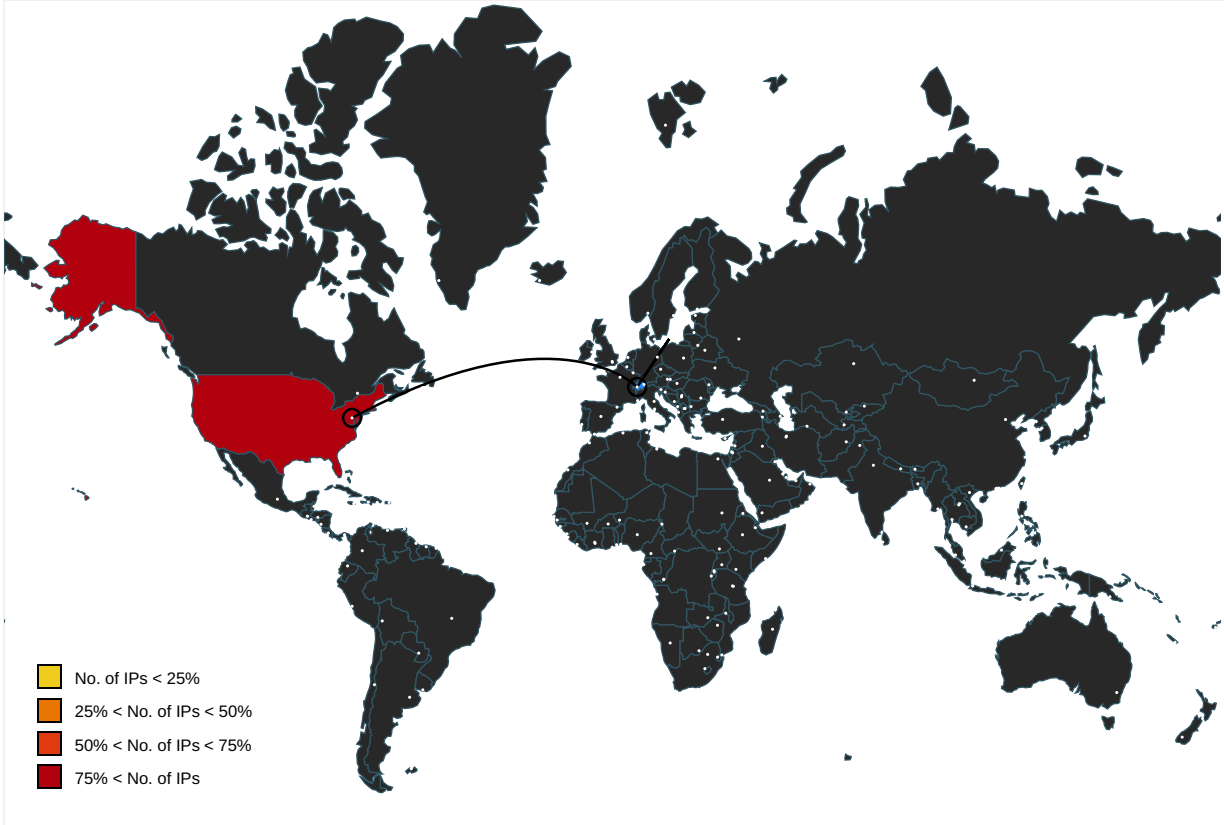
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PO_Invoices_pdf.exe, 00000000.00000003.256526982.0000000006539000.00000004.00000001.sdmp, PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	PO_Invoices_pdf.exe, 00000000.00000003.247874552.0000000006540000.00000004.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.net-siu	PO_Invoices_pdf.exe, 00000000.00000003.248176476.0000000006540000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.net	PO_Invoices_pdf.exe, 00000000.00000003.248176476.0000000006540000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/	powershell.exe, 00000003.00000002.386788256.00000000058A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000003.00000002.386788256.00000000058A3000.00000004.00000001.sdmp	false		high
http://https://freegeoip.app/xml/LoadTimeZoneCountryNameCountryCodehttps://www.geodatatool.com/en/?ip=/	Matiexgoods.exe, 00000008.00000002.699162061.00000000034E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://whatismyipaddress.com/-	PO_Invoices_pdf.exe, 00000000.00000002.277417941.00000000040A8000.00000004.00000001.sdmp, RegAsm.exe, 00000005.00000003.281965972.0000000003BE0000.00000004.00000001.sdmp, hawkgoods.exe, 00000006.00000002.383895800.00000000002F2000.00000002.00020000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot/sendMessage?chat_id=&text=Createutf-8Win32_ComputerSystemModelManufactu	Matiexgoods.exe, 00000008.00000002.699162061.00000000034E1000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	origigoods40.exe, 00000007.00000002.455680542.0000000002FE1000.00000004.00000001.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	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.site.com/logs.php	hawkgoods.exe, 00000006.00000002.387343775.0000000002A21000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	hawkgoods.exe, 00000006.00000002.390146582.0000000003A21000.00000004.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000003.00000002.381287871.0000000004841000.00000004.00000001.sdmp, Matiexgoods.exe, 00000008.00000002.699162061.00000000034E1000.00000004.00000001.sdmp	false		high
http://www.carterandcone.como.	PO_Invoices_pdf.exe, 00000000.00000003.250141662.0000000006515000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.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	PO_Invoices_pdf.exe, 00000000.00000002.277417941.00000000040A8000.00000004.00000001.sdmp, RegAsm.exe, 00000005.00000003.273863512.0000000003E4D000.00000004.00000001.sdmp, origigoods40.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cniac	PO_Invoices_pdf.exe, 00000000.00000003.249338917.0000000006516000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app/xml/	Matiexgoods.exe, 00000008.00000002.699162061.00000000034E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	Matiexgoods.exe, 00000008.00000003.461245193.00000000068F6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000003.00000002.386788256.00000000058A3000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	origigoods40.exe, 00000007.00000002.455680542.0000000002FE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr9	PO_Invoices_pdf.exe, 00000000.00000003.249068129.0000000006515000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comF	PO_Invoices_pdf.exe, 00000000.00000003.254406255.0000000006512000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	Matiexgoods.exe, 00000008.00000003.461245193.00000000068F6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000003.00000002.382114009.0000000004983000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.como.R	PO_Invoices_pdf.exe, 00000000.00000003.250141662.0000000006515000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adobe.cobj	Matiexgoods.exe, 00000008.00000003.443342117.000000000931100.00000004.00000001.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	origigoods40.exe, 00000007.00000002.455680542.0000000002FE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000003.00000002.382114009.0000000004983000.00000004.00000001.sdmp	false		high
http://www.sakkal.com-mq	PO_Invoices_pdf.exe, 00000000.00000003.251741662.000000000654D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000003.00000002.386788256.00000000058A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comY	PO_Invoices_pdf.exe, 00000000.00000003.272424177.000000000651000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com	hawkgoods.exe, 00000006.00000002.387343775.0000000002A21000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comd	PO_Invoices_pdf.exe, 00000000.00000003.254406255.000000000651200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000003.00000002.382114009.0000000004983000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.krF	PO_Invoices_pdf.exe, 00000000.00000003.249068129.000000000651500.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	PO_Invoices_pdf.exe, 00000000.00000002.300417704.000000000660000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.net-d	PO_Invoices_pdf.exe, 00000000.00000003.247998925.000000000654D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PO_Invoices_pdf.exe, 00000000.00000002.300417704.000000000660000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.coma3	PO_Invoices_pdf.exe, 00000000.00000003.254406255.000000000651200.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdV	PO_Invoices_pdf.exe, 00000000.00000003.254406255.000000000651200.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comceto	PO_Invoices_pdf.exe, 00000000.00000003.272424177.000000000651000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	PO_Invoices_pdf.exe, 00000000.00000002.300417704.000000000660000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PO_Invoices_pdf.exe, 00000000.00000002.300417704.000000000660000.00000002.00000001.sdmp, PO_Invoices_pdf.exe, 00000000.00000003.254406255.000000000651200.00000004.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false		high
http://checkip.dyndns.org/HBFl	Matiexgoods.exe, 00000008.00000002.699162061.00000000034E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.pngL	powershell.exe, 00000003.00000002.382114009.0000000004983000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netx	PO_Invoices_pdf.exe, 00000000.00000003.248176476.000000000654D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	PO_Invoices_pdf.exe, 00000000.00000003.272424177.000000000651000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	PO_Invoices_pdf.exe, 00000000.00000003.250877364.0000000006512000.00000004.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/l	PO_Invoices_pdf.exe, 00000000.00000003.250877364.0000000006512000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PO_Invoices_pdf.exe, 00000000.00000002.300417704.0000000006600000.00000002.00000001.sdmp, hawkgoods.exe, 00000006.00000002.391685560.00000000051E0000.00000002.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.htmlL	powershell.exe, 00000003.00000002.382114009.0000000004983000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comdsed	PO_Invoices_pdf.exe, 00000000.00000003.254406255.0000000006512000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krn-u	PO_Invoices_pdf.exe, 00000000.00000003.249068129.0000000006515000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com(	PO_Invoices_pdf.exe, 00000000.00000003.247874552.0000000006564D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.typography.netn	PO_Invoices_pdf.exe, 00000000.00000003.248099180.0000000006564D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://i.imgur.com/GJD7Q5y.png195.239.51.11795.26.248.2989.208.29.13389.187.165.4792.118.13.1895.26	Matiexgoods.exe, 00000008.00000002.699162061.00000000034E1000.00000004.00000001.sdmp	false		high
http://www.tiro.com-cz	PO_Invoices_pdf.exe, 00000000.00000003.249778536.0000000006512000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.ado/1	Matiexgoods.exe, 00000008.00000003.443342117.0000000009311000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
131.186.113.70	unknown	United States		33517	DYNDNSUS	false
104.16.155.36	unknown	United States		13335	CLOUDFLARENETUS	false
104.21.19.200	unknown	United States		13335	CLOUDFLARENETUS	false
199.193.7.228	unknown	United States		22612	NAMECHEAP-NETUS	false
216.146.43.70	unknown	United States		33517	DYNDNSUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	347154
Start date:	02.02.2021
Start time:	08:50:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 18m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO_Invoices_pdf.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.phis.troj.adwa.spyw.evad.winEXE@46/40@68/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 33.8% • Quality standard deviation: 33.4%
HCA Information:	• Successful, ratio: 97% • 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): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 40.88.32.150, 168.61.161.212, 92.122.144.200, 2.20.142.210, 2.20.142.209, 51.103.5.186, 104.42.151.234 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, skypedataprdcoleus15.cloudapp.net, emea1.wns.notify.trafficmanager.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net • 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/347154/sample/PO_Invoices_pdf.exe

Simulations

Behavior and APIs

Time	Type	Description
08:51:54	API Interceptor	48x Sleep call for process: hawkgoods.exe modified
08:52:00	API Interceptor	2x Sleep call for process: dw20.exe modified
08:52:01	API Interceptor	623x Sleep call for process: origigoods20.exe modified
08:52:05	API Interceptor	940x Sleep call for process: origigoods40.exe modified
08:52:20	API Interceptor	1074x Sleep call for process: Matiexgoods.exe modified
08:52:23	API Interceptor	55x Sleep call for process: powershell.exe modified
08:52:33	API Interceptor	2x Sleep call for process: WerFault.exe modified
08:52:34	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
131.186.113.70	SALES.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Statement.pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Purchase Order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	orden010221.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	IMG_1660392.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	my new file ify (1).exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	IMG_166390pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	IMG-6661.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	IMG_761213.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	Sale_Contract.com.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	IMG_04017.pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	INV_098789.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	2021 NEW LIST.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	CHIKWA.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	weg6tX6TTk78XZ5.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	IMG_0661.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	INV0009876.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	000000000009000000.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	IMG_53091.pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Copy_Payment.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
freegeoip.app	SALES.exe	Get hash	malicious	Browse	• 104.21.19.200
	Revised Invoice.exe	Get hash	malicious	Browse	• 172.67.188.154
	RFQ - 0201201.exe	Get hash	malicious	Browse	• 104.21.19.200
	Statement.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order.exe	Get hash	malicious	Browse	• 172.67.188.154
	New Order.exe	Get hash	malicious	Browse	• 172.67.188.154
	CMR2OEYL.exe	Get hash	malicious	Browse	• 104.21.19.200
	full set of ball valve components ready for assembly. Assembly weldingtestingpainting.exe	Get hash	malicious	Browse	• 172.67.188.154
	NEW ORDER.exe	Get hash	malicious	Browse	• 172.67.188.154
	ProcessingIConnect.Common..TermsConditions.z.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO 642021.exe	Get hash	malicious	Browse	• 104.21.19.200
	00000000000000000090.exe	Get hash	malicious	Browse	• 172.67.188.154
	New Order.exe	Get hash	malicious	Browse	• 172.67.188.154
	IMG_1660392.exe	Get hash	malicious	Browse	• 172.67.188.154
	IMG_1660392.doc	Get hash	malicious	Browse	• 172.67.188.154
	NS_PO_86655443.exe	Get hash	malicious	Browse	• 172.67.188.154
	INV#1191189.exe	Get hash	malicious	Browse	• 172.67.188.154
	NEW PURCHASE#U00c3#U00bf #U00c3#U00bfORDER.exe	Get hash	malicious	Browse	• 104.21.19.200
	0009752202_OUTSTANDING_20210129,PDF.exe	Get hash	malicious	Browse	• 172.67.188.154
	CITI SOLUTION COMPANY PROFILE.exe	Get hash	malicious	Browse	• 172.67.188.154
whatismyipaddress.com	Orders.exe	Get hash	malicious	Browse	• 104.16.155.36
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DYNDNSUS	Payment Advice.exe	Get hash	malicious	Browse	• 131.186.113.70
	SALES.exe	Get hash	malicious	Browse	• 131.186.113.70
	Revised Invoice.exe	Get hash	malicious	Browse	• 216.146.43.70
	RFQ - 0201201.exe	Get hash	malicious	Browse	• 162.88.193.70
	Statement.pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	Purchase Order.exe	Get hash	malicious	Browse	• 131.186.113.70
	New Order.exe	Get hash	malicious	Browse	• 162.88.193.70
	orden010221.exe	Get hash	malicious	Browse	• 131.186.113.70
	CMR2OEYL.exe	Get hash	malicious	Browse	• 216.146.43.71
	full set of ball valve components ready for assembly. Assembly weldingtestingpainting.exe	Get hash	malicious	Browse	• 131.186.161.70
	NEW ORDER.exe	Get hash	malicious	Browse	• 216.146.43.70
	ProcessingIConnect.Common..TermsConditions.z.pdf.exe	Get hash	malicious	Browse	• 216.146.43.71
	PO 642021.exe	Get hash	malicious	Browse	• 162.88.193.70
	00000000000000000090.exe	Get hash	malicious	Browse	• 216.146.43.71
	New Order.exe	Get hash	malicious	Browse	• 216.146.43.71
	IMG_1660392.exe	Get hash	malicious	Browse	• 216.146.43.70
	IMG_1660392.doc	Get hash	malicious	Browse	• 216.146.43.70
	NS_PO_86655443.exe	Get hash	malicious	Browse	• 131.186.161.70
	INV#1191189.exe	Get hash	malicious	Browse	• 216.146.43.71
	NEW PURCHASE#U00c3#U00bf #U00c3#U00bfORDER.exe	Get hash	malicious	Browse	• 162.88.193.70
CLOUDFLARENETUS	Payment Advice.exe	Get hash	malicious	Browse	• 172.67.188.154
	SALES.exe	Get hash	malicious	Browse	• 104.21.19.200
	Revised Invoice.exe	Get hash	malicious	Browse	• 172.67.188.154
	RFQ - 0201201.exe	Get hash	malicious	Browse	• 104.21.19.200
	Statement.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order.exe	Get hash	malicious	Browse	• 172.67.188.154
	New Order.exe	Get hash	malicious	Browse	• 172.67.188.154
	NEW ENQUIRY.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	SOA - NCL INTER LOGISTICS.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	CSWWOe1Gnx.html	Get hash	malicious	Browse	• 104.16.19.94
	PO_210202.exe	Get hash	malicious	Browse	• 23.227.38.32
	Invoice764895.xls	Get hash	malicious	Browse	• 172.67.193.211
	Invoice764895.xls	Get hash	malicious	Browse	• 104.21.76.113
	po.exe.exe	Get hash	malicious	Browse	• 23.227.38.74
	CMR2OEYL.exe	Get hash	malicious	Browse	• 104.21.19.200
	129ZD381.xls	Get hash	malicious	Browse	• 172.67.204.162
	129ZD381.xls	Get hash	malicious	Browse	• 172.67.204.162
	q2EKWldniJ.exe	Get hash	malicious	Browse	• 104.16.16.194
	evil.doc	Get hash	malicious	Browse	• 104.16.126.175
	full set of ball valve components ready for assembly. Assembly weldingtestingpainting.exe	Get hash	malicious	Browse	• 172.67.188.154

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	Payment Advice.exe	Get hash	malicious	Browse	• 104.21.19.200
	SALES.exe	Get hash	malicious	Browse	• 104.21.19.200
	Revised Invoice.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ - 0201201.exe	Get hash	malicious	Browse	• 104.21.19.200
	Statement.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Purchase Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	New Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	CMR2OEYL.exe	Get hash	malicious	Browse	• 104.21.19.200
	full set of ball valve components ready for assembly. Assembly weldingtestingpainting.exe	Get hash	malicious	Browse	• 104.21.19.200
	NEW ORDER.exe	Get hash	malicious	Browse	• 104.21.19.200
	OOLU2115327710.xls.exe	Get hash	malicious	Browse	• 104.21.19.200
	ProcessingIConnect.Common..TermsConditions.z.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	SOPORTEDE.exe	Get hash	malicious	Browse	• 104.21.19.200
	POinv00393.exe	Get hash	malicious	Browse	• 104.21.19.200
	PO 642021.exe	Get hash	malicious	Browse	• 104.21.19.200
	00000000000000000090.exe	Get hash	malicious	Browse	• 104.21.19.200
	New Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_1660392.exe	Get hash	malicious	Browse	• 104.21.19.200
	mEPx5H8svq.exe	Get hash	malicious	Browse	• 104.21.19.200
	NS_PO_86655443.exe	Get hash	malicious	Browse	• 104.21.19.200

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\hawkgoods.exe	Orders.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\origigoods20.exe	Orders.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\Matiexgoods.exe	Orders.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\origigoods40.exe	Orders.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_hawkgoods.exe_697020edb13ed8bc761f5d6b0de413dddfcbfb_b4666e22_12f099c3\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	17818
Entropy (8bit):	3.766553825659537
Encrypted:	false
SSDEEP:	192:UwHLs3pHBUZMXJyBaPLk9Mg5N3gFm1pzvnuk1+K1QtKVzss/u7sVS274ltmxeon:rLs3ZBUZMXiayRv1jz3/u7sVX4ltOd
MD5:	1B14E26F15C08169BD1E448474C1F7AB
SHA1:	3FF1E3F413BDD11D5784E94EFCDFE0609CD50B1A
SHA-256:	B680E94518074E808301D5E76EA73ACACCFF2FEC67401CCD13B2C039780F6F65
SHA-512:	682801D9682FDF42DBB98535EAA07596432BCDA55855477CFD0D2FA04C0FAB2A1F4B5E4E208CB87EB417772EF0848BDEE0ECEC71FA1281CE3737419AFB9A4C23
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.=.1.3.2.5.6.7.5.8.4.0.9.0.7.4.3.2.0.4.....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.=.1.3.2.5.6.7.5.8.4.5.3.1.2.9.5.8.2.1.....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.=.2.a.5.b.c.c.8.c.-.2.5.b.4.-.4.a.6.4.-.9.5.6.8.-.8.c.8.e.1.2.a.2.0.a.b.4.....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.=.e.c.e.5.f.a.8.c.-.a.a.3.8.-.4.7.5.6.-.9.b.3.b.-.5.d.5.d.6.a.8.3.8.0.6.2.....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.=.0.0.0.0.1.5.4.0.-.0.0.0.1.-.0.0.1.7.-.3.7.9.8.-.7.7.d.a.8.3.f.9.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_697020edb13ed8bc761f5d6b0de413dddfcbfb_b4666e22_1b230661\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	17916

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_hawkgoods.exe_697020edb13ed8bc761f5d6b0de413dddfcbfb_b4666e22_1b230661\Report.wer	
Entropy (8bit):	3.7657882578191666
Encrypted:	false
SSDEEP:	192:xt91Q3pHBUZMXJyBaKsn9fbeN9M2v1zzvSXk0ZKjBIcQr+s/u7s4S274ItmxeY:h1Q3ZBUZMXiaEdvh/sl/u7s4X4ItOF
MD5:	6FE02F566E5BC86C856A4746E5B1B37E
SHA1:	45764D32FED814C6E0E4D3D7A498DC74ECCD2EE3
SHA-256:	3317003BFF2506D41F1DCCB35B30D0C8D94F389E40D7A77242DA1C7456C05268
SHA-512:	DF8BC7E1E759B493C00C697ACBBDA26C88B7FEC6152F627311697B17E65500C25B245907989AC275985296CFCF11EBDD13760D724AC527A4A24915C314CFF02
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.=.1.3.2.5.6.7.5.8.3.3.1.6.5.2.6.3.8.6.....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.=.1.3.2.5.6.7.5.8.3.5.2.1.5.2.5.9.6.4.....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.8.1.e.4.f.3.3.-.4.c.0.f.-.4.f.1.b.-.9.c.3.2.-.5.c.3.e.a.3.d.7.e.8.d.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.=.a.3.f.9.2.a.c.e.-.4.5.3.0.-.4.8.4.d.-.8.2.8.a.-.f.2.5.7.1.3.c.5.6.8.8.f.....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.=.0.0.0.0.0.e.8.c.-.0.0.0.1.-.0.0.1.7.-.6.9.7.2.-.c.b.b.1.8.3.f.9.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_14dc0d13\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16862
Entropy (8bit):	3.758463269003457
Encrypted:	false
SSDEEP:	192:PmLhQmV4yBaPLk9Mg5N3gFm1pzvnuk1+K1QtKVzz/u7sVS274ltiLn:eLhQSayRv1jzz/u7sVX4lten
MD5:	5B656D3CB77E098CA4DF1D1C0CE0E328
SHA1:	ABA48932FBF3EC81ADA9341DE6B97AC4668AD94C
SHA-256:	85D229EC5FFF7DBF8DDC2CEFA7281BD453B84E1D3F70204FE83A582F0246D164
SHA-512:	928397B3DD92C244E5916D7FD3B61EB2B9E0B3794D6CB477BDADB6CBD75090FCA850DDC950DA714E89484EFF60684E6AE742C73930D6F83BAE3AE2FA665B9962
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.=.1.3.2.5.6.7.5.8.3.8.5.1.0.5.6.3.0.9.....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.=.1.3.2.5.6.7.5.8.3.8.9.5.1.1.8.4.8.0.....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.=.2.0.4.6.f.6.c.2.-.1.4.1.c.-.4.8.8.c.-.9.4.4.0.-.e.a.0.f.5.9.8.2.7.2.3.b.....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.=.0.0.0.0.1.5.4.0.-.0.0.0.1.-.0.0.1.7.-.3.7.9.8.-.7.7.d.a.8.3.f.9.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_hawkgoods.exe_93f07d9c4f92cda17563b29cabdf995c588ef9_00000000_1a4a83a4\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16958
Entropy (8bit):	3.758176808526625
Encrypted:	false
SSDEEP:	192:sK11QmV4yBaKsn9fbeN9M2v1zzvSXk0ZKjBIcQry/u7sTS274ltip:111QSaEdvh/sy/u7sTX4ltg
MD5:	E69F7F2D40A3282E3A5C4D25F316EEFD
SHA1:	FF12BFC6A914E52FD5A233C18C99BF7E128DFC10
SHA-256:	2D0F631D768C4D0B5FA1211D11CAE7F657DB56553606E18FCF4E5CE04878607A
SHA-512:	1C0F891A498A9D74A59A09285423C3173248E2A715F6C43D8499EA9EEA1556CB536A9D8118E81AEECA94936C0AC78F29B6422ADF28D008C80085299D299EFBA(
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.=.1.3.2.5.6.7.5.8.3.1.6.0.9.0.1.7.9.3.....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.=.1.3.2.5.6.7.5.8.3.1.8.7.3.0.7.9.8.5.....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.=.f.4.9.1.a.8.b.5.-.7.b.7.d.-.4.6.4.e.-.8.7.5.0.-.7.c.9.c.1.4.1.a.8.6.c.9.....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.=.0.0.0.0.0.e.8.c.-.0.0.0.1.-.0.0.1.7.-.6.9.7.2.-.c.b.b.1.8.3.f.9.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\Temp\WER2F33.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):	6346
Entropy (8bit):	3.727723917153232
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiJn66RY0SwZCpra89bvcsfRlm:RrlsNiJ6EY0SwCvvfK

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F33.tmp.WERInternalMetadata.xml	
MD5:	D9A75C2F37E77481D156E098A916F868
SHA1:	586C14F42B7EFA8A883FAA53B416F0C491B218B7
SHA-256:	AAA58719C37F44B8FD215C19F46455439079D3B8AFB77BCD1212947B45474CC6
SHA-512:	F4E44BB08682D51682622FD695C6F2DBBA11DFCE95702B5857F46BDE655B9F5C5FBD88148602A7167B334CA8E10917671F530FF9BC6123EEB3EBBC40E6BB041
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.>.5.4.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3BB7.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):	4.484087176387836
Encrypted:	false
SSDEEP:	48:cvIwSD8zscJgtWI9HnWSC8BAb8fm8M4JUkZFl+q84UZ/URyHwd:uITfaoWSNBJJUoZcRyHwd
MD5:	745EBD9EB867F5C20629FE5A76B20E2E
SHA1:	01E88CAA25F3BBF0E69ECBE25A51CC8ED1975EA3
SHA-256:	8983A0C40000ABE4FB9D2FAD11770B2177CF7960842134582B219551BF357DC6
SHA-512:	D65656378EB01D6F1F094C27EB95DE2F10774F68BC4AE266C40EA16975DF60212515A5CC7FE23039FEE53B1871338F4DBD78C24D70AE3F5F9CF1054D12924FC
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="843964" />.. <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\WER72DC.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):	7646
Entropy (8bit):	3.6935655205790683
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNie3696YaD36XLgmfZSnS/ZCp17nX1ffJm:RrlsNi+696Yc36XLgmfInS/A7nlfs
MD5:	B831102B11FA3395D755D1BB81097289
SHA1:	11843E55B390CE8A5FAD48F342F244C938FF4B1A
SHA-256:	C765D0D67F63F562E8E3817D0513C0FA99456485788DCA02DC80E33D4538747D
SHA-512:	18ECA65B3A6C624CC9A23C9CF96550CFBBD5D08784D973E342D7DD0D244B640E4A36A0D86B22896D8747C168AE0286084AC23840FE44F89C35A67F2D333ABA5
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.>.3.7.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7473.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):	4.444767498901979
Encrypted:	false
SSDEEP:	48:cvIwSD8zsCJgtWI9HnWSC8Bxk8fm8M4JFKqJFx+q8vv9/URyHzd:uITfQoWSNTJJFKsKlcRyHzd
MD5:	5CF35384506171C76D238D23345102E5
SHA1:	2AD1BF4FCD9C1D89B39F4F1FF1D5EA58FDBF6B1A
SHA-256:	A5F959079EDED28B1CFBBAF95E51A355666A142A81565719D9BF2F2F7662BEDD
SHA-512:	D690E05F2D00A5FDF49829F1DC1C43552A91D3A40DA8109B53302058211CB5A3FD1EA4C4D59C1397FD74833972ED29AC99E716E969682AD2E4FE92BE816EF56
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7473.tmp.xml	
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="843962" />.. <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\WER81AC.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):	7646
Entropy (8bit):	3.693579069726026
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiJ5z6ZcJ6YQK6AgmfZSnS/ZCp1sc1fbkm:RrlsNiHz6M6YV6AgmfInS/Asmfd
MD5:	3A508C183E8DBAAD5D3D8713B56F9361
SHA1:	EDFA7FE427707929A6A6DDD1EB0F3DDF3BEF18F7
SHA-256:	23CA4EDA7A443492D22C975864EBFB9D0465DBAD4417390EF4F7FA36B5ECF537
SHA-512:	5CE0BDCDA608DBD7757226268407E053148AE9B88329656B566BEBC651158048859EBF03A48B1DAC9BE380F53A32BAC3A1812753ED269A80491FFF274BB80107
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.>.5.4.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8566.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):	4.444768514534563
Encrypted:	false
SSDEEP:	48:cvIwSD8zsJJgtWI9HnWSC8Bcs8fm8M4JFKqJFY2+q8vvp/URyHDd:uITfboWSNqRJFKIKxcRyHDd
MD5:	5A22E2B7CEDA2DCE82BD29C8364400C6
SHA1:	517E131B4D1A984B5D79E041EE6E823CB85B771C
SHA-256:	FBBC0C2B8668F47624704691F6B1D3637C4FEB80B191B86781C760557D98B973
SHA-512:	2CEEBEA847BAB89C2F152F6A0A007E2793656F68E736A03D28386F374B621B2EDF4A10680194E1F3D5A4031B6DD96CFA5D02D8A330383A9BD6B3CEFB40B063A A
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="843963" />.. <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\WERAF48.tmp.mdmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Feb 2 16:52:18 2021, 0x60521 type
Category:	dropped
Size (bytes):	6824818
Entropy (8bit):	4.735635134294259
Encrypted:	false
SSDEEP:	98304:EaauHsiIP9H6hIb1Xa73vlirFYuerqFpCqkJpljZcsZccO:LxHsiIP9H469BXYfZc1
MD5:	CC42182766C160A4269CBC0CB6DD537A
SHA1:	2123EFAF6B085E889046DB5EFAA87A1A3BE29652
SHA-256:	AAC3FBCFE568BD68FC4B213308FF5C593EE3AAB47FC2C9447754239579E838B5
SHA-512:	7561C17ECED613BCF3D4026BBB25000CBC440F46EF912EB8AE6934EDED5793B0564C17EC254AE89D7B04CF7D347DCEA782354648D235A90ED3068F3FDCBD7 71
Malicious:	false
Preview:	MDMP..... .....B..`!.....U.....B.....3.....GenuineIntelW.....T.....#..`.....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\WERD020.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):	6346
Entropy (8bit):	3.726879109228151
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNier6hY0SwZCpr+89bJnvsfNjm:RrlsNiq6hY0SwWJnUf0
MD5:	859C2D09E985859C05BA524E847AE1F7
SHA1:	D77BC6804E32D6EA7001D46678CCA826F5E68F68
SHA-256:	6DB7AAEE60D7D508523C3BA1B51655E0707872B4BE51B8CFBC88A401CF1DA410
SHA-512:	9C1439031B122D8ED9361117E3B095D7E1335C0038463AF84886873B8B543D36081056ADA864C8C42A165B851F590D079473962B5C3B92D05BC0D9C207E8F1D6
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.>.3.7.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD84E.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):	4.484771487000801
Encrypted:	false
SSDEEP:	48:cvIwSD8zsCJgtWI9HnWSC8BN8fm8M4JUkZFK+q84UN/URyHAd:uITfQoWSNAJJOoNcRyHAd
MD5:	9363D872E68ACC797390D6712DA8521C
SHA1:	A04E6EAEC66ECA386CBE020130B59BD71172009F
SHA-256:	73F1FD36F750B4FD1E3B300530421BC897887B4B3D3BFE85C6893B3C0341F4C4
SHA-512:	43CFE15E426B91B113B4E3B109BA0C4030F623CF356D7D4D66DB849A989390EBFFD9C770824B21BB42D0DC0BE54251039A2678920F8851631652EE0AFF7878E8
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="843962" />.. <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\WERDDB6.tmp.mdmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Feb 2 16:53:45 2021, 0x60521 type
Category:	dropped
Size (bytes):	6791614
Entropy (8bit):	4.742421345206189
Encrypted:	false
SSDEEP:	98304:xAMauM2xID9H+h1b1XaoDvliXnlYuernx5AqJplvzcnsccD:xdxM2xID9HUMndYpDzcS
MD5:	722E8E235CF8F1D7BFAE5DC73782C39E
SHA1:	8E0E4C0332FE09017117C69966D39BFF3D93BE0F
SHA-256:	87CCC6BF059F6DF8C5EE9B7872438410BB30C6D104B2E7BF5B9230BCE8850A9B
SHA-512:	E14A7BE8D7C59D1833DE5C15B69CDAF76586A2DF0CBC2B930702B7D4B34B8C8DAB1E408BEB07117B2E1BE777FBA5E69A696E42BA42FA18767A890A16FA7EBC04
Malicious:	false
Preview:	MDMP..... .....`!.....U.....B.....H3.....GenuineIntelW.....T.....@...g..`.....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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\l$s#$lT3ssl.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\l$s#$lT3ssl.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1406
Entropy (8bit):	5.34928936000881
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\l$s#$lT3ssl.exe.log	
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr74E4KnKDE4KhK3VZ9pKhPKIE4oKFKHKorE4J:MIHK5HKXE1qHbHK5AHKzv4HKnYHKhQnp
MD5:	E26C2069017DA08B1891F176C3FCBB5B
SHA1:	372337FEB1999D2CF9E2CDF4AF964905B6EE025A
SHA-256:	A00F43B55E3A712364B3F1F3A8C0DE7B291111960CAC301A34544666E812E5F9
SHA-512:	F13A01B88578FC81453B4C8389C91237414CF2D95CCFD76FE2291E973C86EFA23192C916FD832802054BFC0B2EE72F6ABD7B057BADF98750C381F32115259F9C
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Data.DataSetExtensions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"Sy

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_Invoices_pdf.exe.log	
Process:	C:\Users\user\Desktop\PO_Invoices_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1406
Entropy (8bit):	5.34928936000881
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr74E4KnKDE4KhK3VZ9pKhPKIE4oKFKHKorE4J:MIHK5HKXE1qHbHK5AHKzv4HKnYHKhQnp
MD5:	E26C2069017DA08B1891F176C3FCBB5B
SHA1:	372337FEB1999D2CF9E2CDF4AF964905B6EE025A
SHA-256:	A00F43B55E3A712364B3F1F3A8C0DE7B291111960CAC301A34544666E812E5F9
SHA-512:	F13A01B88578FC81453B4C8389C91237414CF2D95CCFD76FE2291E973C86EFA23192C916FD832802054BFC0B2EE72F6ABD7B057BADF98750C381F32115259F9C
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Data.DataSetExtensions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"Sy

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):	8701
Entropy (8bit):	4.879861859938857
Encrypted:	false
SSDEEP:	192:cdcU6Clib4oxoe5oVsm5emdVVFn3eGOVpN6K3bkkjo59gkjDt4iWN3yBGHh9smii:cib4NBVoGIpN6KQkj2Wkjh4iUx0mib4J
MD5:	E16560503ABB03E8D3A60D67C80E53CB
SHA1:	228496AC44B81BD035E5DAFA6C7298EAC436DBED
SHA-256:	B025E6D38777D7FFC9483E7EFBA2D0DA9766C99113E3441FE56D40A10B85D9D3
SHA-512:	7C0B791A504C1B666C9350A018A2E59C950CABE10832EEEBF88C47784908E8DBE09490E5F9D0A11A05E1200515BB8321E5730E3710EB79633661ED2006F57835
Malicious:	false
Preview:	PSMODULECACHE.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package.....Find-Package.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....D..8.....C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1.....Get-OperationValidation..... ..Invoke-OperationValidation.....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..

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):	19636
Entropy (8bit):	5.5609303136217765
Encrypted:	false
SSDEEP:	384:Et9+XHq0/usaSD01KRYSBKnTYw5Q9QRbp6cQcpPTDEiqWJl5jw:dBaSDS4KTYwO9q8Rs4zWJl
MD5:	E1EFC42BE4A9B9F0A579636314EE85AD
SHA1:	4AE90D27313085028D6E5643B45AC2D15F2E1882
SHA-256:	ABD22A8C7A2F2330B6A3FDD328D07097B1B4494E60C41D9150FF105F93B1D3B7
SHA-512:	F524E684CF1C7A51441A9873A0FFB35C3C205C5159A5C9989EEE36A63C25E0ABB849E667E5D54072986CFF428766B3AD45F8697CC6805DFC39A11101C6FB6943

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Malicious:	false
Preview:	@...e.....].N.N.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)Z.....System.Managemen t.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.....Sy stem.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:	B3216F0E4E95C7F50BCCBA5FDCCA2AD622A42379383BE855546FA1E0BAC41A6BEEA8226F8634AD5E0D8596169E0443494018BBE70B7052F094402AECAA038BC E
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: 89%
Joe Sandbox View:	• Filename: Orders.exe, Detection: malicious, Browse
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_4e14qwxc.os0.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_awkr53h0.pdr.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_fla1cgxx.qbm.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_zllqa32j.uf3.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\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:	modified
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:	3AE6E49D3D728531201453A0BC27436B1A4305C8EF938B2CBB5E34EE45BB9A9A88CF2A41B08E4914FDA9A96BBAA48BD999A2D2F1DFFCD39761BB1F3620CA72 5F
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%
Joe Sandbox View:	• Filename: Orders.exe, Detection: malicious, Browse
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\holderwb.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\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:	81A7DB927F53660D3A04A161D5C18AAB17D676BCC7AE0738AB786D9BEE82B91016E54E6F70428AEC4087961744BE89B1511F9E07D8DABBE5C2A9D836722395A 1
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%
Joe Sandbox View:	• Filename: Orders.exe, Detection: malicious, Browse
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..,.....+.....,.....,.....,.+.+.~....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
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: 82%
Joe Sandbox View:	• Filename: Orders.exe, Detection: malicious, Browse
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):	1655808
Entropy (8bit):	7.9413063895946845
Encrypted:	false
SSDEEP:	49152:MWHaK9/4HLz1lxNIFSCLulcJVzF+gr6b0XVULw:v6KirHxNPUVO0FULw
MD5:	59D7D8D5DD3E0055E7C0DCC75897F569
SHA1:	B249B28D088D54E971E2D9D8B2688440F8E6D513
SHA-256:	EF715CD322F0A805A68840B215C062F2E254977170A11C6800D836EAC781FABB
SHA-512:	79EBC2A128D018EB7E71B254FDD2FA72DEAE18081F1732619046E1DB9D1AEE92F7529521C005A5F861275AFCBDA3A39FD304CD5E1A49DF848675460C5CF8F3(D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....D.....N.... ... ....@.. ..... .@.....W.... ...A..... ..... ..H.....text...T.... ..... ..`.rsrc....A... ...B.....@..@.relo c.....B.....@..B.....0.....H.....*....9.....&...}....*&...}....*&...}....*&...}....*...#.....}.....#.....}.....}....*..s....z..#.....}.....#.....}.....}..... (.....*.(/.....~....~....o....o.....*..s....}.....}.....(.....((....*6.~....(....&*&...}....*:..r...p(.....*:..r...p(.....*:..r...p(.....*:..r...p(.....*:..r...p(.....*:..r...p(.....*:..r...p(.....*:..r!..p(.....*:..r%.. p(.....*:..r...p(.....*:..r)..p(.....**...(.....**...(.....

C:\Users\user\AppData\Roaming\Microsoft\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):	1.5
Encrypted:	false
SSDEEP:	3:Ezn:Ezn
MD5:	7A2347D96752880E3D58D72E9813CC14
SHA1:	1D3027412B106008F1A8094D747616D37F4AE1BB
SHA-256:	90F285F8FB15C8BC72A43D25CEA803491CC0FD0E97567CFF577A2CFA56CDE6F8
SHA-512:	96A7B7BE0B89097FC65BB75DD9B8B0DEB5063ED6990E27151A0A7E54C899AE69377E57ECB5728DFFAB657EE444244F833236F80EC6A98E449902DF9075C74EC(E
Malicious:	false
Preview:	5440

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

C:\Users\user\AppData\Roaming\pidloc.txt	
Malicious:	false
Preview:	C:\Users\user~1\AppData\Local\Temp\hawkgoods.exe

C:\Users\user\Documents\20210202\PowerShell_transcript.830021.dnDUrXav.20210202085254.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):	5.389111464999469
Encrypted:	false
SSDEEP:	96:BZ0x6KNWwkqDo1ZSzwMZ06KNWwkqDo1ZCSdC3UC3UW3gZ8:wXO
MD5:	38990FC46C9A4B38D38D5B6B446DA280
SHA1:	6BAB83EC68E0E3232CCB544F489D69026F3FAB9C
SHA-256:	5CF4E546B058149AC9BBAA1B3B2CB29FFDC75EA82CFF37F287D818A567B0476B
SHA-512:	821C9C1FE957904DCCB563AB386978D98D5DF5A6DBF5EF196B3C2DB2DA74BF0D4784195B36CFA8C8A3AF4748FFEDFA5B3EA8359E322BDFE39477EDDCA372E8B4
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210202085355..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 830021 (Microsoft Windows NT 10.0.17134.0)..Host Application: Powershell.exe -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\AppData\Roaming\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: 6908..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: 20210202085355..**********..PS>Copy-Item 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.e

C:\Users\user\Documents\20210202\PowerShell_transcript.830021.vpu_jBUU.20210202085147.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):	1217
Entropy (8bit):	5.237238445417744
Encrypted:	false
SSDEEP:	24:BxSAIdZOvBdaD+x2DOXCgxluVM5wWOHjeTKKjX4CIym1ZJX+luVM5lnxSAZa:BZHv6KoO/uojOqDYB1Zouo5ZZa
MD5:	D400773C1D3FF7015F2BCC822734162A
SHA1:	299A9A913AEFDF415CB5515F9A09B05161264DEF
SHA-256:	37EBF08DC01B50660C9218D9FB98992D216DE77186933DC3E016B003328F07DF
SHA-512:	B221B385406A51229AF6D022D209DDFE86BEA4DFF6E183B790307C18CDBE4C71633FD794C8AF13BBF825416732F6B38BBEE356F43D3D9C8DC384780BD5F5492
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210202085211..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 830021 (Microsoft Windows NT 10.0.17134.0)..Host Application: Powershell.exe -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\Desktop\PO_Invoices_pdf.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe'..Process ID: 5904..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: 20210202085211..**********..PS>Copy-Item 'C:\Users\user\Desktop\PO_Invoices_pdf.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.ex

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):	4898647
Entropy (8bit):	7.944487996146186
Encrypted:	false
SSDEEP:	98304:6HSa5z1aE+hDBoHSa5z1aE+hD2eHSa5z1aE+hD2eHSa5z1aE+hD2eHSa5z1aE+h/:nkz3Ckz3dkz3dkz3dkz3akz3W
MD5:	8C4D34A23BB01B274B0281197BAD0E4C
SHA1:	AC9D537B161FCC2DEB326716CC499029D67A1EBD
SHA-256:	0B756492D0BA32BC2DB803986371A08AA9A5D6A46C859E3CA7204D12D1CBB123
SHA-512:	509D9D5D2A1F8EEBCC39D5568E5875635C4D3C78552539270F96894230246EB1ADD6021A202043DE1605F4BB70E3AF16DC741240253C7499C24FEFD3BE865582
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....mGY.....__@.)..=t..y.. .....'.....A:R.$!.@z%.B.-....J...B...).R@Hg.....;k.].....u}...)...{.g.l..=.-.....==kw.....e..~3bm.{.q..Zv.O.];v.o...{.....cB:.+e....A.@.....l....vv."...Sv.5....]..X.....Y.]...0~..#..c'.....og.kc!k./h'.m...b..e..-HWG..U)]..2#.....^..g.vw.l..]...'.k.b.lz...c<.....oF.s!CR...a.{z.....b@;%.zf.{+b..y!g...;.sw[.....Q..>C.vv>.c...&>...7<.....hm..7k{.V.=3...){>..b...=.4..f/{=.@.=..C.....d.$6q~.A....-....vo.....w.n...O.....!.;H9.....w.....]..ac.Pvv.Q....bc*.....7.....S.W?..y."6.E}e.W.H?.Bm;X..,-.....i..dN.2r.S..h%....'.....7?3.c.@.p...)N.YL.!P.[..y..3e..E.T.o.....f.....g.Q.[..=....@}.Gr....@.}:V.`.+.0..|C.....!.;H9.....w.....N.bc.P.\....Z`i.....c...Z?.}T.....J..g[.m..{..e...a..p.`...z...?!....0..psl..(.*.;.....N..`.....`.D.LjO'.....b.[p2..%"....-..b.?..q.\.....1.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.9413063895946845
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:	PO_Invoices_pdf.exe
File size:	1655808
MD5:	59d7d8d5dd3e0055e7c0dcc75897f569
SHA1:	b249b28d088d54e971e2d9d8b2688440f8e6d513
SHA256:	ef715cd322f0a805a68840b215c062f2e254977170a11c6800d836eac781fabb
SHA512:	79ebc2a128d018eb7e71b254fdd2fa72deae18081f1732619046e1db9d1aee92f7529521c005a5f861275afcbda3a39fd304cd5e1a49df848675460c5cf8f30d
SSDEEP:	49152:MWHaK9/4HLz1lxNIFSCLulcJVzF+gr6b0XVULw:v6KirHxNPUVO0FULw
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....D.....N.... .. ....@.. .....@.....

File Icon

Icon Hash:	d0d2f8ccf6c4dad8

Static PE Info

General

Entrypoint:	0x591c4e
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:	0x601882D9 [Mon Feb 1 22:38:17 2021 UTC]
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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x191bf4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x192000	0x4186	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x198000	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
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	0x18fc54	0x18fe00	False	0.788759670991	data	7.94835272626	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x192000	0x4186	0x4200	False	0.507634943182	data	5.48483136325	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x198000	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_ICON	0x192190	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1925f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4286386453, next used block 4285534489		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1936a0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4278198588, next used block 4278263872		
RT_GROUP_ICON	0x195c48	0x30	data		
RT_VERSION	0x195c78	0x324	data		
RT_MANIFEST	0x195f9c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

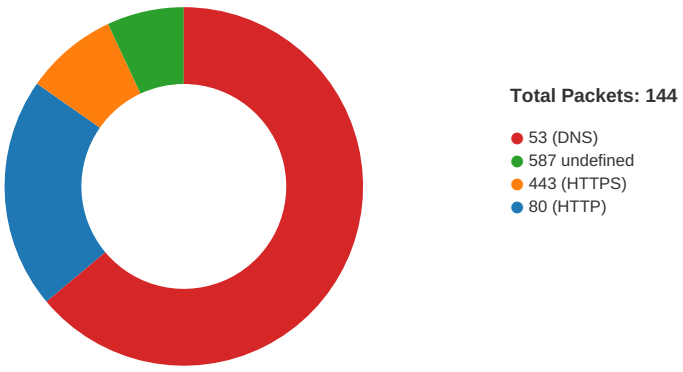
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright (C) 2017
Assembly Version	7.2.12.13
InternalName	Foxmail.exe
FileVersion	7.2.12.13
CompanyName	Tencent Inc.
Comments	Foxmail 7.2
ProductName	Foxmail 7.2
ProductVersion	7.2.12.13
FileDescription	Foxmail
OriginalFilename	Foxmail.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/02/21-08:51:54.127437	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49729	104.16.155.36	192.168.2.7
02/02/21-08:51:54.375992	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49729	104.16.155.36	192.168.2.7
02/02/21-08:53:01.225853	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49769	104.16.155.36	192.168.2.7

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2021 08:51:54.033477068 CET	49729	80	192.168.2.7	104.16.155.36

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2021 08:51:54.073527098 CET	80	49729	104.16.155.36	192.168.2.7
Feb 2, 2021 08:51:54.073673964 CET	49729	80	192.168.2.7	104.16.155.36
Feb 2, 2021 08:51:54.075356960 CET	49729	80	192.168.2.7	104.16.155.36
Feb 2, 2021 08:51:54.115274906 CET	80	49729	104.16.155.36	192.168.2.7
Feb 2, 2021 08:51:54.127437115 CET	80	49729	104.16.155.36	192.168.2.7
Feb 2, 2021 08:51:54.347234964 CET	49729	80	192.168.2.7	104.16.155.36
Feb 2, 2021 08:51:54.375992060 CET	80	49729	104.16.155.36	192.168.2.7
Feb 2, 2021 08:51:54.376856089 CET	49729	80	192.168.2.7	104.16.155.36
Feb 2, 2021 08:52:04.636801958 CET	49731	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:04.696549892 CET	80	49731	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:04.696633101 CET	49731	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:04.697185040 CET	49731	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:04.757730961 CET	80	49731	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:04.757770061 CET	80	49731	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:04.757795095 CET	80	49731	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:04.757899046 CET	49731	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:04.758519888 CET	49731	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:04.817929983 CET	80	49731	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:05.157845974 CET	49732	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:05.216881037 CET	80	49732	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:05.217084885 CET	49732	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:05.217569113 CET	49732	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:05.276770115 CET	80	49732	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:05.276901960 CET	80	49732	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:05.276920080 CET	80	49732	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:05.276995897 CET	49732	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:05.277327061 CET	49732	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:05.338064909 CET	80	49732	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:13.048981905 CET	49733	443	192.168.2.7	104.21.19.200
Feb 2, 2021 08:52:13.095045090 CET	443	49733	104.21.19.200	192.168.2.7
Feb 2, 2021 08:52:13.095906973 CET	49733	443	192.168.2.7	104.21.19.200
Feb 2, 2021 08:52:13.155304909 CET	49733	443	192.168.2.7	104.21.19.200
Feb 2, 2021 08:52:13.201467037 CET	443	49733	104.21.19.200	192.168.2.7
Feb 2, 2021 08:52:13.208401918 CET	443	49733	104.21.19.200	192.168.2.7
Feb 2, 2021 08:52:13.208453894 CET	443	49733	104.21.19.200	192.168.2.7
Feb 2, 2021 08:52:13.208547115 CET	49733	443	192.168.2.7	104.21.19.200
Feb 2, 2021 08:52:13.221199989 CET	49733	443	192.168.2.7	104.21.19.200
Feb 2, 2021 08:52:13.268449068 CET	443	49733	104.21.19.200	192.168.2.7
Feb 2, 2021 08:52:13.269627094 CET	443	49733	104.21.19.200	192.168.2.7
Feb 2, 2021 08:52:13.317687988 CET	49733	443	192.168.2.7	104.21.19.200
Feb 2, 2021 08:52:13.393908024 CET	49733	443	192.168.2.7	104.21.19.200
Feb 2, 2021 08:52:13.439867020 CET	443	49733	104.21.19.200	192.168.2.7
Feb 2, 2021 08:52:13.497458935 CET	443	49733	104.21.19.200	192.168.2.7
Feb 2, 2021 08:52:13.551959991 CET	49733	443	192.168.2.7	104.21.19.200
Feb 2, 2021 08:52:13.723737001 CET	49734	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:13.783137083 CET	80	49734	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:13.783849001 CET	49734	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:13.783994913 CET	49734	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:13.844903946 CET	80	49734	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:13.845175028 CET	80	49734	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:13.845184088 CET	80	49734	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:13.845391035 CET	49734	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:13.845911980 CET	49734	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:13.846653938 CET	49733	443	192.168.2.7	104.21.19.200
Feb 2, 2021 08:52:13.892366886 CET	443	49733	104.21.19.200	192.168.2.7
Feb 2, 2021 08:52:13.905188084 CET	80	49734	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:13.925117970 CET	443	49733	104.21.19.200	192.168.2.7
Feb 2, 2021 08:52:13.973860979 CET	49733	443	192.168.2.7	104.21.19.200
Feb 2, 2021 08:52:14.101875067 CET	49735	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:14.161318064 CET	80	49735	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:14.162257910 CET	49735	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:14.162292004 CET	49735	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:14.221921921 CET	80	49735	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:14.221944094 CET	80	49735	131.186.113.70	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2021 08:52:14.221972942 CET	80	49735	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:14.222125053 CET	49735	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:14.222654104 CET	49735	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:14.223448992 CET	49733	443	192.168.2.7	104.21.19.200
Feb 2, 2021 08:52:14.282454967 CET	80	49735	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:14.286712885 CET	443	49733	104.21.19.200	192.168.2.7
Feb 2, 2021 08:52:14.333252907 CET	49733	443	192.168.2.7	104.21.19.200
Feb 2, 2021 08:52:14.451637030 CET	49736	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:14.510814905 CET	80	49736	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:14.510978937 CET	49736	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:14.511794090 CET	49736	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:14.571150064 CET	80	49736	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:14.571176052 CET	80	49736	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:14.571185112 CET	80	49736	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:14.571312904 CET	49736	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:14.571866989 CET	49736	80	192.168.2.7	131.186.113.70
Feb 2, 2021 08:52:14.632783890 CET	80	49736	131.186.113.70	192.168.2.7
Feb 2, 2021 08:52:22.430808067 CET	49741	587	192.168.2.7	199.193.7.228
Feb 2, 2021 08:52:22.430866003 CET	49740	587	192.168.2.7	199.193.7.228
Feb 2, 2021 08:52:22.621337891 CET	587	49740	199.193.7.228	192.168.2.7
Feb 2, 2021 08:52:22.621368885 CET	587	49741	199.193.7.228	192.168.2.7
Feb 2, 2021 08:52:22.621531963 CET	49740	587	192.168.2.7	199.193.7.228
Feb 2, 2021 08:52:22.621571064 CET	49741	587	192.168.2.7	199.193.7.228
Feb 2, 2021 08:52:22.646863937 CET	49741	587	192.168.2.7	199.193.7.228
Feb 2, 2021 08:52:22.813158989 CET	587	49740	199.193.7.228	192.168.2.7
Feb 2, 2021 08:52:22.813167095 CET	587	49741	199.193.7.228	192.168.2.7
Feb 2, 2021 08:52:22.813273907 CET	49741	587	192.168.2.7	199.193.7.228
Feb 2, 2021 08:52:22.813688993 CET	49740	587	192.168.2.7	199.193.7.228
Feb 2, 2021 08:52:22.837110043 CET	587	49741	199.193.7.228	192.168.2.7
Feb 2, 2021 08:52:22.837198019 CET	49741	587	192.168.2.7	199.193.7.228
Feb 2, 2021 08:52:22.837585926 CET	587	49741	199.193.7.228	192.168.2.7
Feb 2, 2021 08:52:22.837647915 CET	49741	587	192.168.2.7	199.193.7.228
Feb 2, 2021 08:52:22.881418943 CET	49740	587	192.168.2.7	199.193.7.228
Feb 2, 2021 08:52:23.003695965 CET	587	49740	199.193.7.228	192.168.2.7
Feb 2, 2021 08:52:23.004148006 CET	587	49740	199.193.7.228	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2021 08:51:30.116107941 CET	58717	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:30.172230959 CET	53	58717	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:31.337563992 CET	59762	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:31.400734901 CET	53	59762	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:32.221174002 CET	54329	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:32.273967981 CET	53	54329	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:33.975642920 CET	58052	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:34.026186943 CET	53	58052	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:35.326277971 CET	54008	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:35.374140978 CET	53	54008	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:38.306018114 CET	59451	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:38.362137079 CET	53	59451	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:39.282435894 CET	52914	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:39.335496902 CET	53	52914	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:40.727047920 CET	64569	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:40.777889967 CET	53	64569	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:42.254206896 CET	52816	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:42.310305119 CET	53	52816	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:43.344412088 CET	50781	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:43.392345905 CET	53	50781	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:44.466734886 CET	54230	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:44.516629934 CET	53	54230	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:45.447211981 CET	54911	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:45.477125883 CET	49958	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:45.505021095 CET	53	54911	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2021 08:51:45.529052973 CET	53	49958	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:46.893997908 CET	50860	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:46.941816092 CET	53	50860	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:48.213689089 CET	50452	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:48.261679888 CET	53	50452	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:50.513789892 CET	59730	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:50.572828054 CET	53	59730	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:52.579267979 CET	59310	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:52.630502939 CET	53	59310	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:53.379492044 CET	51919	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:53.438116074 CET	53	51919	8.8.8.8	192.168.2.7
Feb 2, 2021 08:51:53.900830984 CET	64296	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:51:53.960005045 CET	53	64296	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:00.056057930 CET	56680	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:00.112185001 CET	53	56680	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:04.437439919 CET	58820	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:04.487238884 CET	53	58820	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:04.516426086 CET	60983	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:04.566323042 CET	53	60983	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:12.981060028 CET	49247	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:13.041534901 CET	53	49247	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:17.680474997 CET	52286	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:17.738408089 CET	53	52286	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:17.837726116 CET	56064	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:17.900806904 CET	53	56064	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:18.850114107 CET	63744	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:18.898106098 CET	53	63744	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:22.276596069 CET	61457	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:22.335807085 CET	53	61457	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:23.339813948 CET	58367	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:23.400106907 CET	53	58367	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:24.584064960 CET	60599	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:24.643059969 CET	53	60599	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:25.612889051 CET	59571	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:25.671786070 CET	53	59571	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:27.152910948 CET	52689	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:27.212202072 CET	53	52689	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:28.490356922 CET	50290	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:28.546897888 CET	53	50290	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:30.280812979 CET	60427	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:30.337150097 CET	53	60427	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:32.047787905 CET	56209	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:32.104201078 CET	53	56209	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:33.669477940 CET	59582	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:33.717605114 CET	53	59582	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:33.987025976 CET	60949	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:34.043262005 CET	53	60949	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:36.163332939 CET	58542	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:36.223865032 CET	53	58542	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:37.289861917 CET	59179	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:37.348948956 CET	53	59179	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:38.025207043 CET	60927	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:38.086824894 CET	53	60927	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:40.204969883 CET	57854	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:40.252991915 CET	53	57854	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:40.299511909 CET	62026	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:40.356125116 CET	53	62026	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:40.632177114 CET	59453	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:40.688971043 CET	53	59453	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:42.364404917 CET	62468	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:42.421161890 CET	53	62468	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:43.485554934 CET	52563	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:43.541801929 CET	53	52563	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:44.979003906 CET	54721	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2021 08:52:45.028855085 CET	53	54721	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:47.347949982 CET	62826	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:47.405642033 CET	53	62826	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:47.588212013 CET	62046	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:47.647037029 CET	53	62046	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:50.374495983 CET	51223	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:50.431301117 CET	53	51223	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:50.658818007 CET	63908	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:50.706617117 CET	53	63908	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:53.261665106 CET	49226	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:53.313534021 CET	53	49226	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:56.275100946 CET	60212	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:56.331607103 CET	53	60212	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:59.256263018 CET	58867	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:59.312505007 CET	53	58867	8.8.8.8	192.168.2.7
Feb 2, 2021 08:52:59.423389912 CET	50864	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:52:59.482912064 CET	53	50864	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:00.292697906 CET	61504	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:00.353419065 CET	53	61504	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:01.004070044 CET	60231	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:01.060314894 CET	53	60231	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:02.156910896 CET	50095	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:02.204837084 CET	53	50095	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:05.881093979 CET	59654	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:05.928864956 CET	53	59654	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:09.224340916 CET	58233	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:09.281547070 CET	53	58233	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:10.724493980 CET	56822	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:10.772320032 CET	53	56822	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:18.055473089 CET	62572	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:18.103461981 CET	53	62572	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:20.778110027 CET	57179	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:20.837517023 CET	53	57179	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:24.139029980 CET	56124	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:24.195363045 CET	53	56124	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:26.415201902 CET	62287	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:26.463123083 CET	53	62287	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:26.516926050 CET	54644	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:26.564953089 CET	53	54644	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:27.549843073 CET	59159	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:27.599453926 CET	53	59159	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:35.453262091 CET	57924	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:35.512851000 CET	53	57924	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:35.593250036 CET	51712	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:35.649574995 CET	53	51712	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:38.249537945 CET	58865	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:38.297360897 CET	53	58865	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:42.031311989 CET	64337	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:42.090331078 CET	53	64337	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:45.081511021 CET	50407	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:45.116350889 CET	61075	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:53:45.140338898 CET	53	50407	8.8.8.8	192.168.2.7
Feb 2, 2021 08:53:45.172378063 CET	53	61075	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:12.793908119 CET	54952	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:12.842149973 CET	53	54952	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:15.301547050 CET	59186	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:15.354489088 CET	53	59186	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:15.887363911 CET	52280	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:15.948564053 CET	53	52280	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:19.049554110 CET	51794	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:19.097718954 CET	53	51794	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:22.277606964 CET	50815	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:22.327384949 CET	53	50815	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:23.821609020 CET	58498	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2021 08:54:23.880672932 CET	53	58498	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:33.298855066 CET	56862	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:33.360323906 CET	53	56862	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:36.197577953 CET	61807	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:36.201062918 CET	52009	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:36.256642103 CET	53	61807	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:36.260183096 CET	53	52009	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:38.931622028 CET	58648	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:38.991988897 CET	53	58648	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:40.716998100 CET	59337	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:40.767158031 CET	53	59337	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:41.961437941 CET	59269	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:42.011138916 CET	53	59269	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:43.813313961 CET	49802	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:43.863847971 CET	53	49802	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:48.922760010 CET	50706	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:48.980370045 CET	53	50706	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:51.820154905 CET	55153	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:51.831574917 CET	59744	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:51.876228094 CET	53	55153	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:51.879745960 CET	53	59744	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:54.559792995 CET	59987	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:54.580755949 CET	61272	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:54.609613895 CET	53	59987	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:54.630439997 CET	53	61272	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:57.268471956 CET	54352	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:57.316422939 CET	53	54352	8.8.8.8	192.168.2.7
Feb 2, 2021 08:54:57.419401884 CET	60696	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:54:57.477765083 CET	53	60696	8.8.8.8	192.168.2.7
Feb 2, 2021 08:55:11.386878967 CET	59139	53	192.168.2.7	8.8.8.8
Feb 2, 2021 08:55:11.436451912 CET	53	59139	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 2, 2021 08:51:53.379492044 CET	192.168.2.7	8.8.8.8	0xf445	Standard query (0)	69.170.12.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Feb 2, 2021 08:51:53.900830984 CET	192.168.2.7	8.8.8.8	0x6da6	Standard query (0)	whatismyipaddress.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:04.437439919 CET	192.168.2.7	8.8.8.8	0x6b02	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:04.516426086 CET	192.168.2.7	8.8.8.8	0xc21c	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:12.981060028 CET	192.168.2.7	8.8.8.8	0x872a	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:22.276596069 CET	192.168.2.7	8.8.8.8	0x849c	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:23.339813948 CET	192.168.2.7	8.8.8.8	0xb3be	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:24.584064960 CET	192.168.2.7	8.8.8.8	0x9e74	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:25.612889051 CET	192.168.2.7	8.8.8.8	0x52d5	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:27.152910948 CET	192.168.2.7	8.8.8.8	0xc1d8	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:28.490356922 CET	192.168.2.7	8.8.8.8	0xc3b0	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:30.280812979 CET	192.168.2.7	8.8.8.8	0x9914	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:32.047787905 CET	192.168.2.7	8.8.8.8	0x276	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:33.987025976 CET	192.168.2.7	8.8.8.8	0xd60a	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:36.163332939 CET	192.168.2.7	8.8.8.8	0xb80c	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:37.289861917 CET	192.168.2.7	8.8.8.8	0xcfe2	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:38.025207043 CET	192.168.2.7	8.8.8.8	0x220e	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 2, 2021 08:52:40.204969883 CET	192.168.2.7	8.8.8.8	0x91f5	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:40.299511909 CET	192.168.2.7	8.8.8.8	0xfe1e	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:40.632177114 CET	192.168.2.7	8.8.8.8	0xfc0e	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:42.364404917 CET	192.168.2.7	8.8.8.8	0x368e	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:43.485554934 CET	192.168.2.7	8.8.8.8	0xe0c2	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:44.979003906 CET	192.168.2.7	8.8.8.8	0xbda6	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:47.347949982 CET	192.168.2.7	8.8.8.8	0x1787	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:47.588212013 CET	192.168.2.7	8.8.8.8	0x3404	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:50.374495983 CET	192.168.2.7	8.8.8.8	0x3390	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:50.658818007 CET	192.168.2.7	8.8.8.8	0x9a1a	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:53.261665106 CET	192.168.2.7	8.8.8.8	0x7125	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:56.275100946 CET	192.168.2.7	8.8.8.8	0xca4	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:59.256263018 CET	192.168.2.7	8.8.8.8	0xb67f	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:59.423389912 CET	192.168.2.7	8.8.8.8	0xe5c5	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:00.292697906 CET	192.168.2.7	8.8.8.8	0x1a9c	Standard query (0)	69.170.12.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Feb 2, 2021 08:53:01.004070044 CET	192.168.2.7	8.8.8.8	0x3e9	Standard query (0)	whatismyipaddress.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:02.156910896 CET	192.168.2.7	8.8.8.8	0x747f	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:05.881093979 CET	192.168.2.7	8.8.8.8	0x7f71	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:09.224340916 CET	192.168.2.7	8.8.8.8	0x3367	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:18.055473089 CET	192.168.2.7	8.8.8.8	0x249a	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:20.778110027 CET	192.168.2.7	8.8.8.8	0x89c8	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:24.139029980 CET	192.168.2.7	8.8.8.8	0x2a46	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:26.415201902 CET	192.168.2.7	8.8.8.8	0x1132	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:26.516926050 CET	192.168.2.7	8.8.8.8	0x667a	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:27.549843073 CET	192.168.2.7	8.8.8.8	0x43b4	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:35.453262091 CET	192.168.2.7	8.8.8.8	0xba64	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:35.593250036 CET	192.168.2.7	8.8.8.8	0xbb55	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:38.249537945 CET	192.168.2.7	8.8.8.8	0x74bc	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:42.031311989 CET	192.168.2.7	8.8.8.8	0x3d6a	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:45.081511021 CET	192.168.2.7	8.8.8.8	0x68c3	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:45.116350889 CET	192.168.2.7	8.8.8.8	0x5a1f	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:12.793908119 CET	192.168.2.7	8.8.8.8	0xcb32	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:15.887363911 CET	192.168.2.7	8.8.8.8	0xe537	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:19.049554110 CET	192.168.2.7	8.8.8.8	0x224f	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:22.277606964 CET	192.168.2.7	8.8.8.8	0xd7e	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:23.821609020 CET	192.168.2.7	8.8.8.8	0xaef0	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:33.298855066 CET	192.168.2.7	8.8.8.8	0xa8a1	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 2, 2021 08:54:36.197577953 CET	192.168.2.7	8.8.8.8	0x92d2	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:36.201062918 CET	192.168.2.7	8.8.8.8	0x2b45	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:38.931622028 CET	192.168.2.7	8.8.8.8	0x874f	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:40.716998100 CET	192.168.2.7	8.8.8.8	0xc8e5	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:41.961437941 CET	192.168.2.7	8.8.8.8	0x53c9	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:43.813313961 CET	192.168.2.7	8.8.8.8	0xca13	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:48.922760010 CET	192.168.2.7	8.8.8.8	0xc966	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:51.820154905 CET	192.168.2.7	8.8.8.8	0xba1a	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:51.831574917 CET	192.168.2.7	8.8.8.8	0xecd6	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:54.559792995 CET	192.168.2.7	8.8.8.8	0x5da3	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:54.580755949 CET	192.168.2.7	8.8.8.8	0xee93	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:57.268471956 CET	192.168.2.7	8.8.8.8	0x756b	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:57.419401884 CET	192.168.2.7	8.8.8.8	0xaa2b	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Feb 2, 2021 08:55:11.386878967 CET	192.168.2.7	8.8.8.8	0x1733	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 2, 2021 08:51:53.438116074 CET	8.8.8.8	192.168.2.7	0xf445	Name error (3)	69.170.12.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Feb 2, 2021 08:51:53.960005045 CET	8.8.8.8	192.168.2.7	0x6da6	No error (0)	whatismyipaddress.com		104.16.155.36	A (IP address)	IN (0x0001)
Feb 2, 2021 08:51:53.960005045 CET	8.8.8.8	192.168.2.7	0x6da6	No error (0)	whatismyipaddress.com		104.16.154.36	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:04.487238884 CET	8.8.8.8	192.168.2.7	0x6b02	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 2, 2021 08:52:04.487238884 CET	8.8.8.8	192.168.2.7	0x6b02	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:04.487238884 CET	8.8.8.8	192.168.2.7	0x6b02	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:04.487238884 CET	8.8.8.8	192.168.2.7	0x6b02	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:04.487238884 CET	8.8.8.8	192.168.2.7	0x6b02	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:04.487238884 CET	8.8.8.8	192.168.2.7	0x6b02	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:04.566323042 CET	8.8.8.8	192.168.2.7	0xc21c	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 2, 2021 08:52:04.566323042 CET	8.8.8.8	192.168.2.7	0xc21c	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:04.566323042 CET	8.8.8.8	192.168.2.7	0xc21c	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:04.566323042 CET	8.8.8.8	192.168.2.7	0xc21c	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:04.566323042 CET	8.8.8.8	192.168.2.7	0xc21c	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 2, 2021 08:52:04.566323042 CET	8.8.8.8	192.168.2.7	0xc21c	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:13.041534901 CET	8.8.8.8	192.168.2.7	0x872a	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:13.041534901 CET	8.8.8.8	192.168.2.7	0x872a	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:22.335807085 CET	8.8.8.8	192.168.2.7	0x849c	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:23.400106907 CET	8.8.8.8	192.168.2.7	0xb3be	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:24.643059969 CET	8.8.8.8	192.168.2.7	0x9e74	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:25.671786070 CET	8.8.8.8	192.168.2.7	0x52d5	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:27.212202072 CET	8.8.8.8	192.168.2.7	0xc1d8	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:28.546897888 CET	8.8.8.8	192.168.2.7	0xc3b0	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:30.337150097 CET	8.8.8.8	192.168.2.7	0x9914	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:32.104201078 CET	8.8.8.8	192.168.2.7	0x276	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:34.043262005 CET	8.8.8.8	192.168.2.7	0xd60a	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:36.223865032 CET	8.8.8.8	192.168.2.7	0xb80c	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:37.348948956 CET	8.8.8.8	192.168.2.7	0xcfe2	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:38.086824894 CET	8.8.8.8	192.168.2.7	0x220e	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:40.252991915 CET	8.8.8.8	192.168.2.7	0x91f5	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:40.356125116 CET	8.8.8.8	192.168.2.7	0xfe1e	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:40.688971043 CET	8.8.8.8	192.168.2.7	0xfc0e	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:42.421161890 CET	8.8.8.8	192.168.2.7	0x368e	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:43.541801929 CET	8.8.8.8	192.168.2.7	0xe0c2	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:45.028855085 CET	8.8.8.8	192.168.2.7	0xbda6	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:47.405642033 CET	8.8.8.8	192.168.2.7	0x1787	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:47.647037029 CET	8.8.8.8	192.168.2.7	0x3404	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:50.431301117 CET	8.8.8.8	192.168.2.7	0x3390	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:50.706617117 CET	8.8.8.8	192.168.2.7	0x9a1a	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:53.313534021 CET	8.8.8.8	192.168.2.7	0x7125	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 2, 2021 08:52:56.331607103 CET	8.8.8.8	192.168.2.7	0xca4	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:59.312505007 CET	8.8.8.8	192.168.2.7	0xb67f	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:52:59.482912064 CET	8.8.8.8	192.168.2.7	0xe5c5	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:00.353419065 CET	8.8.8.8	192.168.2.7	0x1a9c	Name error (3)	69.170.12.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Feb 2, 2021 08:53:01.060314894 CET	8.8.8.8	192.168.2.7	0x3e9	No error (0)	whatismyipaddress.com		104.16.155.36	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:01.060314894 CET	8.8.8.8	192.168.2.7	0x3e9	No error (0)	whatismyipaddress.com		104.16.154.36	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:02.204837084 CET	8.8.8.8	192.168.2.7	0x747f	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:05.928864956 CET	8.8.8.8	192.168.2.7	0x7f71	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:09.281547070 CET	8.8.8.8	192.168.2.7	0x3367	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:18.103461981 CET	8.8.8.8	192.168.2.7	0x249a	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:20.837517023 CET	8.8.8.8	192.168.2.7	0x89c8	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:24.195363045 CET	8.8.8.8	192.168.2.7	0x2a46	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:26.463123083 CET	8.8.8.8	192.168.2.7	0x1132	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 2, 2021 08:53:26.463123083 CET	8.8.8.8	192.168.2.7	0x1132	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:26.463123083 CET	8.8.8.8	192.168.2.7	0x1132	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:26.463123083 CET	8.8.8.8	192.168.2.7	0x1132	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:26.463123083 CET	8.8.8.8	192.168.2.7	0x1132	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:26.463123083 CET	8.8.8.8	192.168.2.7	0x1132	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:26.564953089 CET	8.8.8.8	192.168.2.7	0x667a	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 2, 2021 08:53:26.564953089 CET	8.8.8.8	192.168.2.7	0x667a	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:26.564953089 CET	8.8.8.8	192.168.2.7	0x667a	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:26.564953089 CET	8.8.8.8	192.168.2.7	0x667a	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:26.564953089 CET	8.8.8.8	192.168.2.7	0x667a	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:26.564953089 CET	8.8.8.8	192.168.2.7	0x667a	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:27.599453926 CET	8.8.8.8	192.168.2.7	0x43b4	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:35.512851000 CET	8.8.8.8	192.168.2.7	0xba64	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 2, 2021 08:53:35.649574995 CET	8.8.8.8	192.168.2.7	0xbb55	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:38.297360897 CET	8.8.8.8	192.168.2.7	0x74bc	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:42.090331078 CET	8.8.8.8	192.168.2.7	0x3d6a	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:45.140338898 CET	8.8.8.8	192.168.2.7	0x68c3	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:45.140338898 CET	8.8.8.8	192.168.2.7	0x68c3	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
Feb 2, 2021 08:53:45.172378063 CET	8.8.8.8	192.168.2.7	0x5a1f	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:12.842149973 CET	8.8.8.8	192.168.2.7	0xcb32	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:15.948564053 CET	8.8.8.8	192.168.2.7	0xe537	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:19.097718954 CET	8.8.8.8	192.168.2.7	0x224f	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:22.327384949 CET	8.8.8.8	192.168.2.7	0xd7e	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:23.880672932 CET	8.8.8.8	192.168.2.7	0xaef0	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:33.360323906 CET	8.8.8.8	192.168.2.7	0xa8a1	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:36.256642103 CET	8.8.8.8	192.168.2.7	0x92d2	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:36.260183096 CET	8.8.8.8	192.168.2.7	0x2b45	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:38.991988897 CET	8.8.8.8	192.168.2.7	0x874f	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:40.767158031 CET	8.8.8.8	192.168.2.7	0xc8e5	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:42.011138916 CET	8.8.8.8	192.168.2.7	0x53c9	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:43.863847971 CET	8.8.8.8	192.168.2.7	0xca13	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:48.980370045 CET	8.8.8.8	192.168.2.7	0xc966	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:51.876228094 CET	8.8.8.8	192.168.2.7	0xba1a	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:51.879745960 CET	8.8.8.8	192.168.2.7	0xecd6	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:54.609613895 CET	8.8.8.8	192.168.2.7	0x5da3	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:54.630439997 CET	8.8.8.8	192.168.2.7	0xee93	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:57.316422939 CET	8.8.8.8	192.168.2.7	0x756b	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:54:57.477765083 CET	8.8.8.8	192.168.2.7	0xaa2b	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Feb 2, 2021 08:55:11.436451912 CET	8.8.8.8	192.168.2.7	0x1733	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- whatismyipaddress.com
- checkip.dyndns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49729	104.16.155.36	80	C:\Users\user\AppData\Local\Temp\hawkgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 2, 2021 08:51:54.075356960 CET	1007	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Feb 2, 2021 08:51:54.127437115 CET	1008	IN	HTTP/1.1 403 Forbidden Date: Tue, 02 Feb 2021 07:51:54 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=de810853b8bb2cf1036f76079d68ccb1c1612252314; expires=Thu, 04-Mar-21 07:51:54 GMT; path=/; domain=.whatismyipaddress.com; HttpOnly; SameSite=Lax; Secure cf-request-id: 08035311fa00000eb751133000000001 Server: cloudflare CF-RAY: 61b254632f520eb7-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
Feb 2, 2021 08:51:54.375992060 CET	1008	IN	HTTP/1.1 403 Forbidden Date: Tue, 02 Feb 2021 07:51:54 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=de810853b8bb2cf1036f76079d68ccb1c1612252314; expires=Thu, 04-Mar-21 07:51:54 GMT; path=/; domain=.whatismyipaddress.com; HttpOnly; SameSite=Lax; Secure cf-request-id: 08035311fa00000eb751133000000001 Server: cloudflare CF-RAY: 61b254632f520eb7-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
1	192.168.2.7	49731	131.186.113.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 2, 2021 08:52:04.697185040 CET	1039	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 2, 2021 08:52:04.757770061 CET	1039	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
10	192.168.2.7	49788	216.146.43.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 2, 2021 08:53:47.596793890 CET	5141	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 2, 2021 08:53:47.669477940 CET	5141	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
11	192.168.2.7	49789	216.146.43.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 2, 2021 08:53:48.376410007 CET	5143	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 2, 2021 08:53:48.450817108 CET	5144	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	49732	131.186.113.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 2, 2021 08:52:05.217569113 CET	1040	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 2, 2021 08:52:05.276901960 CET	1040	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	49734	131.186.113.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 2, 2021 08:52:13.783994913 CET	1046	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 2, 2021 08:52:13.845175028 CET	1046	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	49735	131.186.113.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 2, 2021 08:52:14.162292004 CET	1049	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 2, 2021 08:52:14.221944094 CET	1049	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.2.0 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	49736	131.186.113.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 2, 2021 08:52:14.511794090 CET	1051	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 2, 2021 08:52:14.571176052 CET	1051	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	49769	104.16.155.36	80	C:\Users\user\AppData\Local\Temp\hawkgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 2, 2021 08:53:01.163186073 CET	2529	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Feb 2, 2021 08:53:01.225852966 CET	2530	IN	HTTP/1.1 403 Forbidden Date: Tue, 02 Feb 2021 07:53:01 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=d8412a81e43270e1884d4cbba2a07a91d1612252381; expires=Thu, 04-Mar-21 07:53:01 GMT; path=/; domain=.whatismyipaddress.com; HttpOnly; SameSite=Lax; Secure cf-request-id: 080354181000001f3177225000000001 Server: cloudflare CF-RAY: 61b256067e711f31-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
7	192.168.2.7	49777	216.146.43.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 2, 2021 08:53:26.770868063 CET	3778	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

Timestamp	kBytes transferred	Direction	Data
Feb 2, 2021 08:53:26.845346928 CET	3778	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	49779	216.146.43.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 2, 2021 08:53:28.295042992 CET	3780	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 2, 2021 08:53:28.368408918 CET	3781	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	49787	216.146.43.70	80	C:\Users\user\AppData\Local\Temp\Matiexgoods.exe

Timestamp	kBytes transferred	Direction	Data
Feb 2, 2021 08:53:46.745872021 CET	5135	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 2, 2021 08:53:46.820859909 CET	5136	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 2, 2021 08:52:13.208453894 CET	104.21.19.200	443	192.168.2.7	49733	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 2, 2021 08:53:45.447184086 CET	104.21.19.200	443	192.168.2.7	49785	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 2, 2021 08:52:22.813158989 CET	587	49740	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:22.813167095 CET	587	49741	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:22.813688993 CET	49740	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:23.004148006 CET	587	49740	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:23.785701990 CET	587	49742	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:23.786706924 CET	49742	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:23.980775118 CET	587	49742	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:25.029432058 CET	587	49743	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:25.030982018 CET	49743	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:25.224092007 CET	587	49743	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:26.059046984 CET	587	49744	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:26.059510946 CET	49744	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:26.250122070 CET	587	49744	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:26.251414061 CET	49744	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:26.441719055 CET	587	49744	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:27.599121094 CET	587	49745	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:27.599586964 CET	49745	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:27.791764021 CET	587	49745	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:28.954073906 CET	587	49746	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:28.984247923 CET	49746	587	192.168.2.7	199.193.7.228	EHLO 830021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 2, 2021 08:52:29.188302040 CET	587	49746	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:29.188587904 CET	49746	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:29.390053034 CET	587	49746	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:30.722702980 CET	587	49747	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:30.723046064 CET	49747	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:30.913746119 CET	587	49747	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:30.914057970 CET	49747	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:31.104008913 CET	587	49747	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:32.490869999 CET	587	49748	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:32.491282940 CET	49748	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:32.681601048 CET	587	49748	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:32.682013988 CET	49748	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:32.872016907 CET	587	49748	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:34.427877903 CET	587	49750	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:34.428292990 CET	49750	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:34.618705034 CET	587	49750	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:34.620052099 CET	49750	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:34.809961081 CET	587	49750	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:36.613873005 CET	587	49751	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:36.614547968 CET	49751	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:36.804939985 CET	587	49751	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:36.805289984 CET	49751	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:36.996551037 CET	587	49751	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:37.736371040 CET	587	49752	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:37.737236977 CET	49752	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:37.928690910 CET	587	49752	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:37.929166079 CET	49752	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:38.122827053 CET	587	49752	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:38.495201111 CET	587	49753	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:38.495958090 CET	49753	587	192.168.2.7	199.193.7.228	EHLO 830021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 2, 2021 08:52:38.698676109 CET	587	49753	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:38.705585957 CET	49753	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:38.909257889 CET	587	49753	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:40.640491962 CET	587	49754	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:40.640836954 CET	49754	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:40.742924929 CET	587	49755	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:40.743376017 CET	49755	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:40.832242012 CET	587	49754	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:40.833101988 CET	49754	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:40.936414957 CET	587	49755	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:41.023488045 CET	587	49754	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:41.073451996 CET	587	49756	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:41.073873043 CET	49756	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:41.264448881 CET	587	49756	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:41.264954090 CET	49756	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:41.454988003 CET	587	49756	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:42.805581093 CET	587	49757	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:42.808633089 CET	49757	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:43.001002073 CET	587	49757	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:43.001396894 CET	49757	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:43.191638947 CET	587	49757	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:43.927926064 CET	587	49758	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:43.928359985 CET	49758	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:44.119829893 CET	587	49758	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:44.120193958 CET	49758	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:44.310609102 CET	587	49758	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:45.416155100 CET	587	49759	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:45.416457891 CET	49759	587	192.168.2.7	199.193.7.228	EHLO 830021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 2, 2021 08:52:45.606834888 CET	587	49759	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:45.607120991 CET	49759	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:45.799350977 CET	587	49759	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:47.812969923 CET	587	49760	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:47.813316107 CET	49760	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:48.015526056 CET	587	49760	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:48.015924931 CET	49760	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:48.031583071 CET	587	49761	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:48.031898022 CET	49761	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:48.217470884 CET	587	49760	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:48.222242117 CET	587	49761	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:48.225008965 CET	49761	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:48.414846897 CET	587	49761	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:50.819664001 CET	587	49762	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:50.819951057 CET	49762	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:51.013494968 CET	587	49762	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:51.015211105 CET	49762	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:51.091154099 CET	587	49763	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:51.091501951 CET	49763	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:51.207123995 CET	587	49762	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:51.282040119 CET	587	49763	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:51.282620907 CET	49763	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:51.472697020 CET	587	49763	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:53.700566053 CET	587	49764	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:53.700826883 CET	49764	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:53.891614914 CET	587	49764	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:53.891880035 CET	49764	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:54.082276106 CET	587	49764	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:56.752723932 CET	587	49765	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:56.753062010 CET	49765	587	192.168.2.7	199.193.7.228	EHLO 830021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 2, 2021 08:52:56.944964886 CET	587	49765	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:56.945434093 CET	49765	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:52:57.136822939 CET	587	49765	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:52:59.741539001 CET	587	49767	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:59.744452953 CET	49767	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:59.900674105 CET	587	49768	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:52:59.916116953 CET	49768	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:52:59.948602915 CET	587	49767	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:52:59.948976994 CET	49767	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:00.122152090 CET	587	49768	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:53:00.122442961 CET	49768	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:00.152375937 CET	587	49767	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:00.325570107 CET	587	49768	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:02.618752956 CET	587	49770	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:53:02.619087934 CET	49770	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:53:02.809268951 CET	587	49770	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:53:02.815468073 CET	49770	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:03.005538940 CET	587	49770	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:06.514214993 CET	587	49771	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:53:06.514597893 CET	49771	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:53:06.704798937 CET	587	49771	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:53:06.705087900 CET	49771	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:06.894906998 CET	587	49771	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:09.670850992 CET	587	49772	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:53:09.671189070 CET	49772	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:53:09.863631010 CET	587	49772	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:53:09.863991976 CET	49772	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:10.054274082 CET	587	49772	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:18.489265919 CET	587	49774	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:53:18.489636898 CET	49774	587	192.168.2.7	199.193.7.228	EHLO 830021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 2, 2021 08:53:18.680254936 CET	587	49774	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:53:18.680546045 CET	49774	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:18.870492935 CET	587	49774	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:21.223431110 CET	587	49775	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:53:21.350620031 CET	49775	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:53:21.541002035 CET	587	49775	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:53:21.541326046 CET	49775	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:21.733660936 CET	587	49775	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:24.606659889 CET	587	49776	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:53:24.607726097 CET	49776	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:53:24.811074972 CET	587	49776	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:53:24.811362028 CET	49776	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:25.012739897 CET	587	49776	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:27.989326000 CET	587	49778	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:53:27.989716053 CET	49778	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:53:28.180408955 CET	587	49778	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:53:28.180705070 CET	49778	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:28.373656034 CET	587	49778	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:35.901496887 CET	587	49780	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:53:35.901990891 CET	49780	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:53:36.096594095 CET	587	49780	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:53:36.097197056 CET	49780	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:36.239164114 CET	587	49782	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:53:36.239751101 CET	587	49781	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:53:36.284514904 CET	49782	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:53:36.284563065 CET	49781	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:53:36.289796114 CET	587	49780	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:36.486347914 CET	587	49781	199.193.7.228	192.168.2.7	250-mta-13.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 2, 2021 08:53:36.486578941 CET	587	49782	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:53:36.486627102 CET	49781	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:36.486783028 CET	49782	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:36.687962055 CET	587	49781	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:36.688091993 CET	587	49782	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:38.683794975 CET	587	49783	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:53:38.684241056 CET	49783	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:53:38.877027988 CET	587	49783	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:53:38.877393961 CET	49783	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:39.067572117 CET	587	49783	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:42.474970102 CET	587	49784	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:53:42.475333929 CET	49784	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:53:42.666105986 CET	587	49784	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:53:42.666457891 CET	49784	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:42.856486082 CET	587	49784	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:53:45.580559969 CET	587	49786	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:53:45.580796957 CET	49786	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:53:45.782514095 CET	587	49786	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:53:45.782795906 CET	49786	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:53:45.984117031 CET	587	49786	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:13.248991013 CET	587	49790	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:13.249319077 CET	49790	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:13.451119900 CET	587	49790	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:13.451430082 CET	49790	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:13.652879000 CET	587	49790	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:16.356473923 CET	587	49792	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:16.359440088 CET	49792	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:16.551491976 CET	587	49792	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:16.554924011 CET	49792	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:16.747075081 CET	587	49792	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:19.546262026 CET	587	49793	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:19.546660900 CET	49793	587	192.168.2.7	199.193.7.228	EHLO 830021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 2, 2021 08:54:19.748264074 CET	587	49793	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:19.748622894 CET	49793	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:19.949882030 CET	587	49793	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:22.712263107 CET	587	49794	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:22.712584019 CET	49794	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:22.903280020 CET	587	49794	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:22.903708935 CET	49794	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:23.094129086 CET	587	49794	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:24.265650034 CET	587	49795	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:24.266120911 CET	49795	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:24.456612110 CET	587	49795	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:24.456887007 CET	49795	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:24.646842957 CET	587	49795	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:33.747540951 CET	587	49796	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:33.748317003 CET	49796	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:33.940007925 CET	587	49796	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:33.940270901 CET	49796	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:34.130645990 CET	587	49796	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:36.648380041 CET	587	49797	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:36.648818016 CET	49797	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:36.677932024 CET	587	49798	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:36.682199955 CET	49798	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:36.841758013 CET	587	49797	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:36.841996908 CET	49797	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:36.872733116 CET	587	49798	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:36.876977921 CET	49798	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:37.033971071 CET	587	49797	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:37.067073107 CET	587	49798	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:39.379169941 CET	587	49799	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:39.381690979 CET	49799	587	192.168.2.7	199.193.7.228	EHLO 830021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 2, 2021 08:54:39.572385073 CET	587	49799	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:39.574527025 CET	49799	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:39.766592979 CET	587	49799	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:41.156644106 CET	587	49800	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:41.169212103 CET	49800	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:41.359941006 CET	587	49800	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:41.360233068 CET	49800	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:41.553025961 CET	587	49800	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:42.419593096 CET	587	49801	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:42.420350075 CET	49801	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:42.611356974 CET	587	49801	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:42.611753941 CET	49801	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:42.805545092 CET	587	49801	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:44.273689032 CET	587	49802	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:44.273976088 CET	49802	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:44.478375912 CET	587	49802	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:44.478852987 CET	49802	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:44.680263996 CET	587	49802	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:49.376130104 CET	587	49803	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:49.376744032 CET	49803	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:49.568742037 CET	587	49803	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:49.571069002 CET	49803	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:49.761332035 CET	587	49803	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:52.260323048 CET	587	49804	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:52.260835886 CET	49804	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:52.267551899 CET	587	49805	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:52.269411087 CET	49805	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:52.452074051 CET	587	49804	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:52.452435970 CET	49804	587	192.168.2.7	199.193.7.228	STARTTLS

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 2, 2021 08:54:52.460019112 CET	587	49805	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:52.460841894 CET	49805	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:52.644531012 CET	587	49804	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:52.653999090 CET	587	49805	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:54.997694969 CET	587	49806	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:54.998035908 CET	49806	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:55.015147924 CET	587	49807	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:55.015799999 CET	49807	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:55.189517021 CET	587	49806	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:55.190080881 CET	49806	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:55.206698895 CET	587	49807	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:55.207362890 CET	49807	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:55.380321980 CET	587	49806	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:55.397460938 CET	587	49807	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:57.700922012 CET	587	49808	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:57.701092958 CET	49808	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:57.870578051 CET	587	49809	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:54:57.870820045 CET	49809	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:54:57.894201040 CET	587	49808	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:57.894429922 CET	49808	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:58.062791109 CET	587	49809	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:54:58.062974930 CET	49809	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:54:58.086261034 CET	587	49808	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:54:58.252882957 CET	587	49809	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:00.334939957 CET	587	49810	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:00.336182117 CET	49810	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:55:00.452255964 CET	587	49811	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:00.452501059 CET	49811	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:55:00.529437065 CET	587	49810	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:00.529710054 CET	49810	587	192.168.2.7	199.193.7.228	STARTTLS

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 2, 2021 08:55:00.642693043 CET	587	49811	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:00.642937899 CET	49811	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:00.720020056 CET	587	49810	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:00.833960056 CET	587	49811	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:03.041965008 CET	587	49812	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:03.042279005 CET	49812	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:55:03.244170904 CET	587	49812	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:03.246289968 CET	49812	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:03.447788954 CET	587	49812	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:05.709295034 CET	587	49813	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:05.709516048 CET	49813	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:55:05.900187016 CET	587	49813	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:05.900346041 CET	49813	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:06.091825962 CET	587	49813	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:06.739952087 CET	587	49814	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:06.741314888 CET	49814	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:55:06.931937933 CET	587	49814	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:06.933430910 CET	49814	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:07.123622894 CET	587	49814	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:08.336911917 CET	587	49815	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:08.337141037 CET	49815	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:55:08.527364016 CET	587	49815	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:08.527591944 CET	49815	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:08.717672110 CET	587	49815	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:09.286880016 CET	587	49816	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:09.287231922 CET	49816	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:55:09.477727890 CET	587	49816	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:09.480767965 CET	49816	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:09.670908928 CET	587	49816	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:11.825762987 CET	587	49817	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:11.826100111 CET	49817	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:55:11.842029095 CET	587	49818	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:11.842259884 CET	49818	587	192.168.2.7	199.193.7.228	EHLO 830021

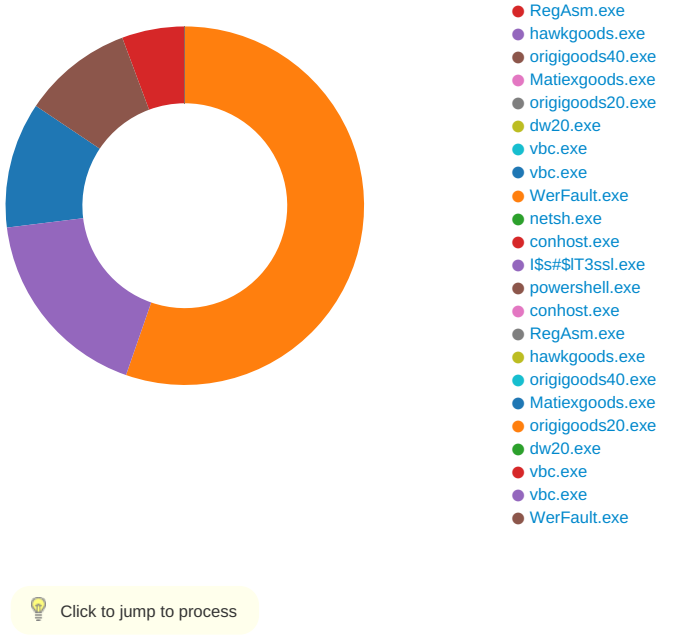
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 2, 2021 08:55:12.016412973 CET	587	49817	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:12.016590118 CET	49817	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:12.033821106 CET	587	49818	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:12.034054995 CET	49818	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:12.209115982 CET	587	49817	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:12.227118015 CET	587	49818	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:14.469098091 CET	587	49819	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:14.469307899 CET	49819	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:55:14.670991898 CET	587	49819	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:14.671222925 CET	49819	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:14.748943090 CET	587	49820	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:14.749162912 CET	49820	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:55:14.872647047 CET	587	49819	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:14.939352989 CET	587	49820	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:14.939585924 CET	49820	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:15.129380941 CET	587	49820	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:17.125241041 CET	587	49821	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:17.125453949 CET	49821	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:55:17.282188892 CET	587	49822	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:17.282394886 CET	49822	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:55:17.316113949 CET	587	49821	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:17.316272974 CET	49821	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:17.472850084 CET	587	49822	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:17.473069906 CET	49822	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:17.506520987 CET	587	49821	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:17.663238049 CET	587	49822	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:19.663860083 CET	587	49823	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:19.664026976 CET	49823	587	192.168.2.7	199.193.7.228	EHLO 830021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 2, 2021 08:55:19.854288101 CET	587	49823	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:19.854476929 CET	49823	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:19.863238096 CET	587	49824	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:19.863399982 CET	49824	587	192.168.2.7	199.193.7.228	EHLO 830021
Feb 2, 2021 08:55:20.047234058 CET	587	49823	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:20.067862034 CET	587	49824	199.193.7.228	192.168.2.7	250-mta-13.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Feb 2, 2021 08:55:20.068080902 CET	49824	587	192.168.2.7	199.193.7.228	STARTTLS
Feb 2, 2021 08:55:20.271485090 CET	587	49824	199.193.7.228	192.168.2.7	220 Ready to start TLS
Feb 2, 2021 08:55:24.527071953 CET	587	49825	199.193.7.228	192.168.2.7	220 PrivateEmail.com prod Mail Node
Feb 2, 2021 08:55:24.527304888 CET	49825	587	192.168.2.7	199.193.7.228	EHLO 830021

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: PO_Invoices_pdf.exe PID: 5372 Parent PID: 5680

General

Start time:	08:51:34
Start date:	02/02/2021
Path:	C:\Users\user\Desktop\PO_Invoices_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO_Invoices_pdf.exe'
Imagebase:	0xaf0000
File size:	1655808 bytes
MD5 hash:	59D7D8D5DD3E0055E7C0DCC75897F569
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: 00000000.00000002.277417941.00000000040A8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000000.00000002.277417941.00000000040A8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.277417941.00000000040A8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.277417941.00000000040A8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.277417941.00000000040A8000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.277417941.00000000040A8000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D59CF06	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	6D59CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_Invoices_pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8AC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_Invoices_pdf.exe.log	unknown	1406	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D8AC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D575705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D57CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3E1B4F	ReadFile

Analysis Process: powershell.exe PID: 5904 Parent PID: 5372

General

Start time:	08:51:44
Start date:	02/02/2021
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\PO_Invoices_pdf.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$lT3ssl.exe'
Imagebase:	0x13c0000
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:\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	6D59CF06	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	6D59CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_awkr53h0.pdr.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C3E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4e14qwxc.os0.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C3E1E60	CreateFileW
C:\Users\user\Documents\20210202	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C3EBEFF	CreateDirectoryW
C:\Users\user\Documents\20210202\PowerShell_transcript.830021.vpu_jBUU.20210202085147.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C3E1E60	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\l$s#$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	6C3EDD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\l$s#$lT3ssl.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C3EDD66	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	6C3E1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_awkr53h0.pdr.ps1	success or wait	1	6C3E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4e14qwxc.os0.psm1	success or wait	1	6C3E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_awkr53h0.pdr.ps1	unknown	1	31	1	success or wait	1	6C3E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4e14qwxc.os0.psm1	unknown	1	31	1	success or wait	1	6C3E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210202\PowerShell_transcript.830021.vpu_jBUU.20210202085147.txt	unknown	3	ef bb bf	...	success or wait	1	6C3E1B4F	WriteFile
C:\Users\user\Documents\20210202\PowerShell_transcript.830021.vpu_jBUU.20210202085147.txt	unknown	755	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 32 30 38 35 32 31 31 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 38 33 30 30 32 31 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 6f	**********************..Windows PowerShell transcript start..Start time: 20210202085211..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 830021 (Microsoft Windows NT 10.0.17134.0)..Host Applicatio	success or wait	11	6C3E1B4F	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 d9 82 18 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 fe 18 00 00 44 00 00 00 00 00 00 4e 1c 19 00 00 20 00 00 00 20 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 a0 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.... $.......PE..L......`.......... ....0......D......N.... ... .@.. ....@................	success or wait	7	6C3EDD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$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	6C3EDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 13 0f 00 00 16 00 00 00 e9 0d bf 04 2a 09 1a 09 dd 07 00 00 00 00 aa 02 3e 00 c8 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....*. .....>.....@.....	success or wait	1	6D8676FC	WriteFile
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 27 00 00 00 0e 00 20 00	H.....<@.^...L."My.. .:'..... .	success or wait	17	6D8676FC	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	6D8676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	6D8676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	8	6D8676FC	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 2f 67 40 01 2e 35 40 01 2d 35 40 01 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 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 00 01 b8 53 00 01 fb 53 00 01 1e 54 00 01 19 54 00 01 78 54 00 01 7a 54 00 01 95 54 00 01 3d 4d 00 01 44 4d 00 01 3a 4d 00 01 22 4d 00 01 20 4d 00 01 21 4d 00 01 3b 4d 00 01 e0 44 00 01 e5 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 45 4d 00 01 dc 71 00 01 dd 71 00 01 f8 53 00 01 98 25 00 01 ba 6e 00 01 34 26 00 01 35 26 00	....T.@..>@.3g@./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..EM...q...q...S.. .%...n..4&..5&.	success or wait	8	6D8676FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	769	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)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6C3E1B4F	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	6D575705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D575705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D57CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D57CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D57CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D575705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D575705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D575705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D575705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D575705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D581F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6D58203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4D03DE	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	6C3E1B4F	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	6C3E1B4F	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	6C3E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C3E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C3E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6C3E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6C3E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C3E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C3E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C3E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C3E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C3E1B4F	ReadFile

Registry Activities

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

Analysis Process: conhost.exe PID: 8 Parent PID: 5904

General

Start time:	08:51:44
Start date:	02/02/2021
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: 4888 Parent PID: 5372

General

Start time:	08:51:45
Start date:	02/02/2021
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:	0xb60000
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: 00000005.00000003.273863512.0000000003E4D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000003.285132773.0000000003DE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000003.269169616.00000000010E3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000003.272090410.0000000003B4B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000003.276618597.0000000003B4B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000003.286093751.00000000010E3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000003.281965972.0000000003BE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000003.281965972.0000000003BE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000003.284634932.0000000003E4D000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000002.287278765.0000000000403000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000005.00000002.287278765.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.287278765.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.287278765.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.287278765.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.287278765.0000000000403000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000003.271788096.00000000010E3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000003.283633869.0000000003B4B000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

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~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
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 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: 3724 Parent PID: 4888

General

Start time:	08:51:47
Start date:	02/02/2021
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:	0x2f0000
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: 00000006.00000002.390146582.0000000003A21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000002.390146582.0000000003A21000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000006.00000002.383895800.00000000002F2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000002.383895800.00000000002F2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000006.00000002.383895800.00000000002F2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000002.383895800.00000000002F2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000006.00000002.383895800.00000000002F2000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000006.00000002.398436711.0000000007540000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000006.00000002.398332656.00000000073F0000.00000004.00000001.sdmp, Author: Arnim Rupp • 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
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	C6BCAB	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	C6BCAB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	4B65A62	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	4B65A62	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	33 37 32 34	3724	success or wait	1	4B60093	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	4B60093	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	4B60093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4B60093	ReadFile
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	4B60093	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:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	4B60093	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	4B60093	ReadFile

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	4B64A02	RegSetValueExW

Analysis Process: origigoods40.exe PID: 6172 Parent PID: 4888

General

Start time:	08:51:48
Start date:	02/02/2021
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:	0xc30000
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: 00000007.00000002.445463818.0000000000C32000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.455680542.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.455680542.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.273140883.0000000000C32000.00000002.00020000.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: 82%, 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	6D59CF06	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	6D59CF06	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	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D575705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D57CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D575705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3E1B4F	ReadFile

Analysis Process: Matiexgoods.exe PID: 6264 Parent PID: 4888

General

Start time:	08:51:51
Start date:	02/02/2021
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:	0xf70000
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: 00000008.00000002.681623451.0000000000F72000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.699392963.000000000352E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.699392963.000000000352E000.00000004.00000001.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: 89%, ReversingLabs
Reputation:	low

Analysis Process: origigoods20.exe PID: 6352 Parent PID: 4888

General

Start time:	08:51:52
Start date:	02/02/2021
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:	0xe0000
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.00000002.430720019.00000000000E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.281843308.00000000000E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.454660209.0000000002801000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.454660209.0000000002801000.00000004.00000001.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: dw20.exe PID: 6684 Parent PID: 3724

General

Start time:	08:51:54
Start date:	02/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2164
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: 6852 Parent PID: 3724

General

Start time:	08:51:57
Start date:	02/02/2021
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\holdermail.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
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000011.00000002.296594780.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 6868 Parent PID: 3724

General

Start time:	08:51:58
Start date:	02/02/2021
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

Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000002.308131659.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 7028 Parent PID: 3724

General

Start time:	08:52:03
Start date:	02/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3724 -s 1996
Imagebase:	0xb60000
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: 00000014.00000002.379809632.0000000005930000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000014.00000002.379809632.0000000005930000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000014.00000002.379809632.0000000005930000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: netsh.exe PID: 1744 Parent PID: 6264

General

Start time:	08:52:33
Start date:	02/02/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	'netsh' wlan show profile
Imagebase:	0x13c0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1200 Parent PID: 1744

General

Start time:	08:52:33
Start date:	02/02/2021
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: I$s#$IT3ssl.exe PID: 1808 Parent PID: 3292

General

Start time:	08:52:43
Start date:	02/02/2021
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:	0xa20000
File size:	1655808 bytes
MD5 hash:	59D7D8D5DD3E0055E7C0DCC75897F569
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 20%, ReversingLabs

Analysis Process: powershell.exe PID: 6908 Parent PID: 1808

General

Start time:	08:52:50
Start date:	02/02/2021
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\I$s#$IT3ssl.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\I$s#$IT3ssl.exe'
Imagebase:	0x13c0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6980 Parent PID: 6908

General

Start time:	08:52:51
Start date:	02/02/2021
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: 4828 Parent PID: 1808

General

Start time:	08:52:53
Start date:	02/02/2021
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:	0x770000
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: 0000001A.00000003.425880345.0000000003A2D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000003.414221299.00000000036C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000003.418225668.0000000000E23000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000003.418385560.000000000372B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000003.427152213.00000000039C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000003.428390015.0000000000E23000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001A.00000002.433264598.0000000000403000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 0000001A.00000002.433264598.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001A.00000002.433264598.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001A.00000002.433264598.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001A.00000002.433264598.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001A.00000002.433264598.0000000000403000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000003.419784850.000000000372B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000003.413803172.0000000000E23000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000003.424187770.000000000372B000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: hawkgoods.exe PID: 5440 Parent PID: 4828

General

Start time:	08:52:55
Start date:	02/02/2021
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:	0xa40000
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: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 0000001B.00000002.651684392.0000000007F40000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 0000001B.00000002.651227274.0000000007C90000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001B.00000000.417887646.0000000000A42000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001B.00000000.417887646.0000000000A42000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001B.00000000.417887646.0000000000A42000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001B.00000000.417887646.0000000000A42000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001B.00000000.417887646.0000000000A42000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001B.00000002.642866499.00000000041B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001B.00000002.642866499.00000000041B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001B.00000002.636644097.0000000000A42000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001B.00000002.636644097.0000000000A42000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001B.00000002.636644097.0000000000A42000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001B.00000002.636644097.0000000000A42000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001B.00000002.636644097.0000000000A42000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001B.00000002.641318198.00000000031B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001B.00000002.641318198.00000000031B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001B.00000002.641318198.00000000031B1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: origigoods40.exe PID: 3080 Parent PID: 4828

General

Start time:	08:52:56
Start date:	02/02/2021
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:	0xe20000
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: 0000001C.00000002.696128013.0000000003201000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001C.00000002.696128013.0000000003201000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001C.00000000.419299258.0000000000E22000.00000002.00020000.sdmp, Author: Joe Security

Analysis Process: Matiexgoods.exe PID: 6532 Parent PID: 4828

General

Start time:	08:52:57
Start date:	02/02/2021
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:	0xbd0000
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: 0000001E.00000002.681849072.0000000000BD2000.00000002.00020000.sdmp, Author: Joe Security

Analysis Process: origigoods20.exe PID: 7160 Parent PID: 4828

General

Start time:	08:52:57
Start date:	02/02/2021
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:	0x720000
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: 0000001F.00000000.423374232.0000000000722000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000002.703454217.0000000002F71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001F.00000002.703454217.0000000002F71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000002.681903640.0000000000722000.00000002.00020000.sdmp, Author: Joe Security

Analysis Process: dw20.exe PID: 5252 Parent PID: 5440

General

Start time:	08:53:04

Start date:	02/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2092
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: vbc.exe PID: 5776 Parent PID: 5440

General

Start time:	08:53:06
Start date:	02/02/2021
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\holdermail.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
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000002.446713470.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: vbc.exe PID: 6108 Parent PID: 5440

General

Start time:	08:53:07
Start date:	02/02/2021
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
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000023.00000002.465758929.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: WerFault.exe PID: 4776 Parent PID: 5440

General

Start time:	08:53:14
Start date:	02/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5440 -s 940
Imagebase:	0xb60000
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: 00000025.00000002.619183539.0000000005360000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000025.00000002.619183539.0000000005360000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000025.00000002.619183539.0000000005360000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Disassembly

Code Analysis