ID: 339499
Sample Name:
B6LNCKjOGt5EmFQ.exe
Cookbook: default.jbs
Time: 07:58:25
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

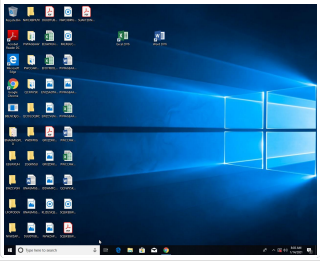
Analysis Report B6LNCKjOGt5EmFQ.exe

Overview

General Information

Sample Name:	B6LNCKjOGt5EmFQ.exe
Analysis ID:	339499
MD5:	80d255a6a5ec33..
SHA1:	bca665ff5a6a708..
SHA256:	3e48d983e33155..
Tags:	exe Yahoo

Most interesting Screenshot:



Detection

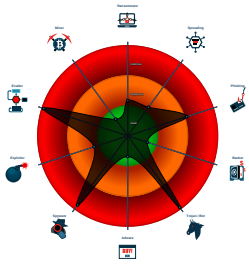
HawkEye AgentTesla MailPassView Matiex

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

Signatures

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

Classification



Startup

- **System is w10x64**
- B6LNCKjOGt5EmFQ.exe (PID: 6076 cmdline: 'C:\Users\user\Desktop\B6LNCKjOGt5EmFQ.exe' MD5: 80D255A6A5EC339E15D6FEC3C0FEF666)
  - schtasks.exe (PID: 4812 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TcVfsyyjYuQ' /XML 'C:\Users\user\AppData\Local\Temp\tmpDAC4.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - B6LNCKjOGt5EmFQ.exe (PID: 5640 cmdline: {path} MD5: 80D255A6A5EC339E15D6FEC3C0FEF666)
  - B6LNCKjOGt5EmFQ.exe (PID: 5336 cmdline: {path} MD5: 80D255A6A5EC339E15D6FEC3C0FEF666)
    - LOGO AND PICTURES.exe (PID: 6208 cmdline: 'C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe' 0 MD5: D9001138C5119D936B70BF77E136AFBE)
      - netsh.exe (PID: 6184 cmdline: 'netsh' wlan show profile MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - conhost.exe (PID: 6168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - Pictures.exe (PID: 6240 cmdline: 'C:\Users\user\AppData\Local\Temp\Pictures.exe' 0 MD5: 25146E9C5ECD498DD17BA01E6CFAEB24)
        - dw20.exe (PID: 6740 cmdline: dw20.exe -x -s 2184 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
        - vbc.exe (PID: 6836 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: 6848 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
      - PO456724392021.exe (PID: 6292 cmdline: 'C:\Users\user\AppData\Local\Temp\PO456724392021.exe' 0 MD5: F38E2D474C075EFF35B4EF81FDACA650)
      - PO2345714382021.exe (PID: 6488 cmdline: 'C:\Users\user\AppData\Local\Temp\PO2345714382021.exe' 0 MD5: 9B79DE8E3AD21F14E71E55CFA6AE4727)
- **cleanup**

Malware Configuration

Threatname: HawkEye

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

Threatname: Agenttesla

```
{
  "Username: ": "",
  "URL: ": "",
  "To: ": "sales01@seedwellresources.xyz",
  "ByHost: ": "smtp.privateemail.com:5874",
  "Password: ": "",
  "From: ": "sales01@seedwellresources.xyz"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\PO456724392021.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Local\Temp\PO2345714382021.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
C:\Users\user\AppData\Local\Temp\Pictures.exe	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b8f7:$key: HawkEyeKeylogger • 0x7db3b:$salt: 099u787978786 • 0x7bf38:$string1: HawkEye_Keylogger • 0x7cd8b:$string1: HawkEye_Keylogger • 0x7da9b:$string1: HawkEye_Keylogger • 0x7c321:$string2: holdermail.txt • 0x7c341:$string2: holdermail.txt • 0x7c263:$string3: wallet.dat • 0x7c27b:$string3: wallet.dat • 0x7c291:$string3: wallet.dat • 0x7d65f:$string4: Keylog Records • 0x7d977:$string4: Keylog Records • 0x7db93:$string5: do not script --> • 0x7b8df:$string6: \pidloc.txt • 0x7b96d:$string7: BSPLIT • 0x7b97d:$string7: BSPLIT
C:\Users\user\AppData\Local\Temp\Pictures.exe	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 3 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000003.291239624.000000000445 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000002.308380033.000000000040 0000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000009.00000002.611843586.00000000032C 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000002.611843586.00000000032C 9000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000008.00000003.283351079.000000000134 C000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 66 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.0.PO456724392021.exe.ab0000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
16.0.PO2345714382021.exe.5d0000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
12.2.PO456724392021.exe.ab0000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
19.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	

Source	Rule	Description	Author	Strings
10.0.Pictures.exe.150000.0.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b8f7:$key: HawkEyeKeylogger • 0x7db3b:$salt: 099u787978786 • 0x7bf38:$string1: HawkEye_Keylogger • 0x7cd8b:$string1: HawkEye_Keylogger • 0x7da9b:$string1: HawkEye_Keylogger • 0x7c321:$string2: holdermail.txt • 0x7c341:$string2: holdermail.txt • 0x7c263:$string3: wallet.dat • 0x7c27b:$string3: wallet.dat • 0x7c291:$string3: wallet.dat • 0x7d65f:$string4: Keylog Records • 0x7d977:$string4: Keylog Records • 0x7db93:$string5: do not script --> • 0x7b8df:$string6: \pidloc.txt • 0x7b96d:$string7: BSPLIT • 0x7b97d:$string7: BSPLIT
Click to see the 20 entries				

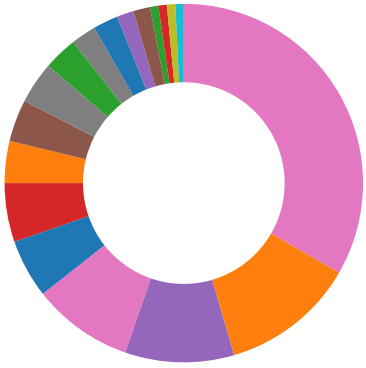
Sigma Overview

System Summary:

Sigma detected: Capture Wi-Fi password

Sigma detected: Scheduled temp file as task from temp location

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

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

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

- Uses schtasks.exe or at.exe to add and modify task schedules

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

HIPS / PFW / Operating System Protection Evasion:

- .NET source code references suspicious native API functions
- Allocates memory in foreign processes
- 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

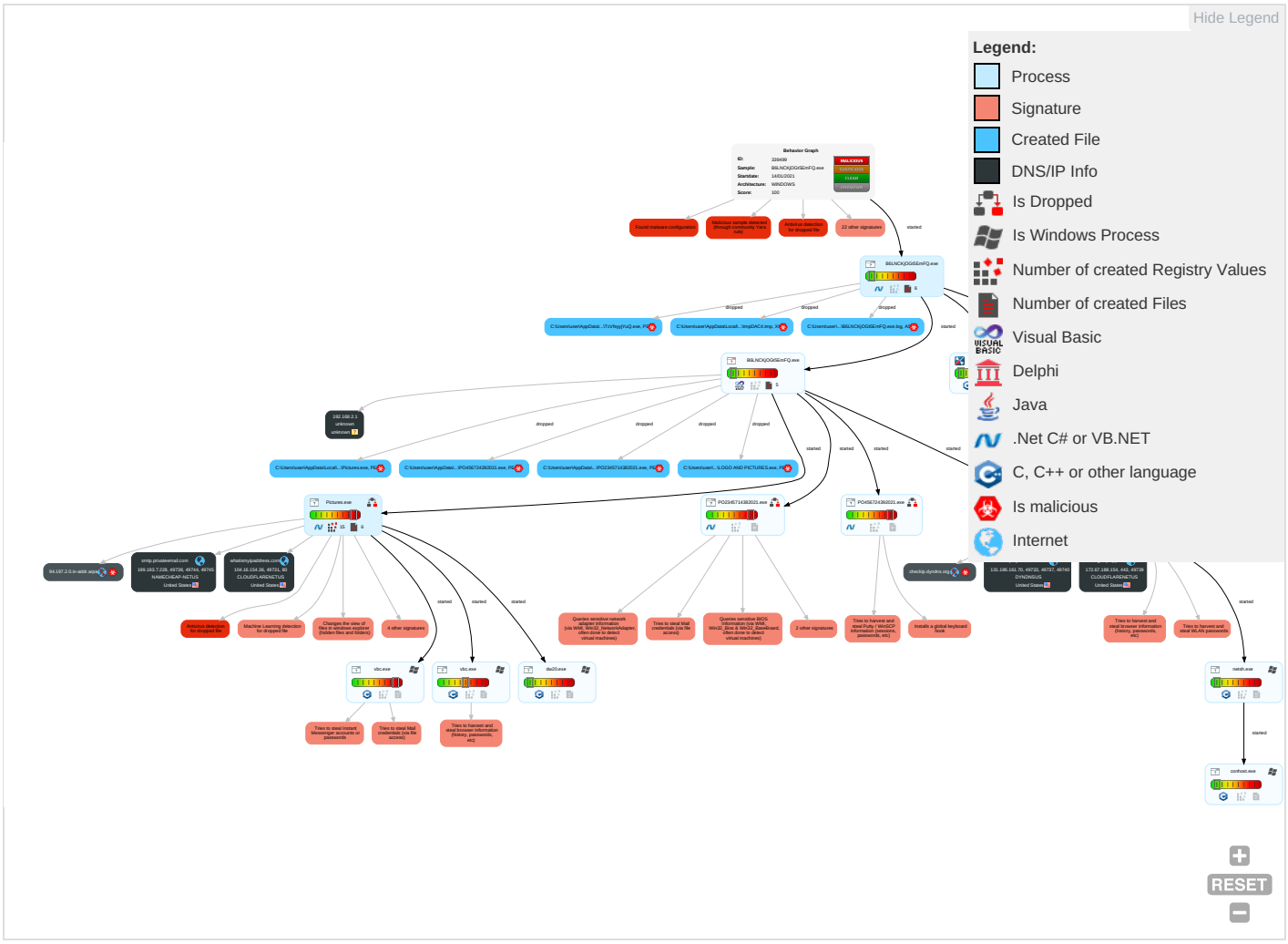
Yara detected HawkEye Keylogger

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	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2 1	OS Credential Dumping 2	Peripheral Device Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over C Network Medium
Default Accounts	Native API 2	Scheduled Task/Job 1	Access Token Manipulation 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	Logon Script (Windows)	Process Injection 4 1 2	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	Scheduled Task/Job 1	Logon Script (Mac)	Scheduled Task/Job 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	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 3 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 C Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 6	DCSync	Process Discovery 3	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 2	/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 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obf Non-C2 Protocol

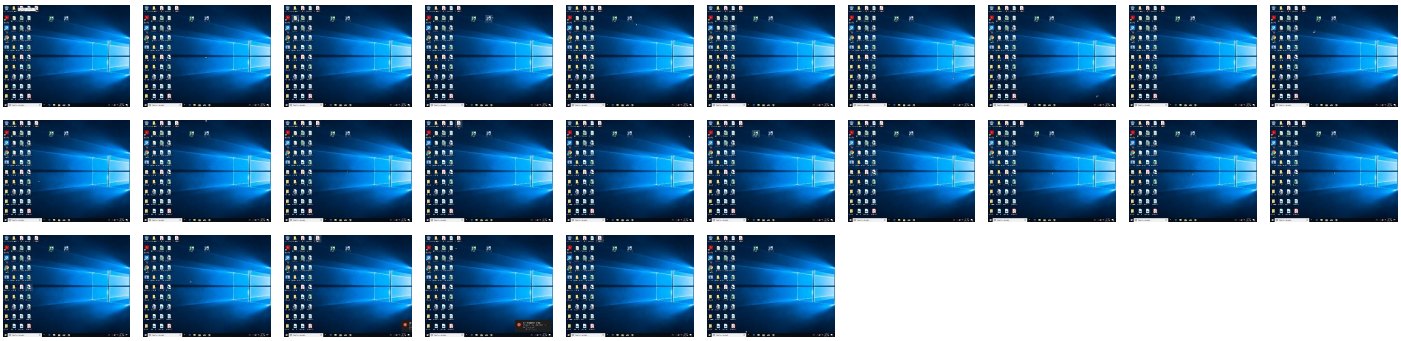
Behavior Graph



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
B6LNCKjOGt5EmFQ.exe	26%	ReversingLabs	Win32.Trojan.Razy	
B6LNCKjOGt5EmFQ.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\PO2345714382021.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe	100%	Avira	TR/Redcap.jajcu	
C:\Users\user\AppData\Local\Temp\Pictures.exe	100%	Avira	TR/AD.MExecute.lzrac	
C:\Users\user\AppData\Local\Temp\Pictures.exe	100%	Avira	SPR/Tool.MailPassView.473	
C:\Users\user\AppData\Local\Temp\PO456724392021.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Local\Temp\PO2345714382021.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\TcVfsyyjYuQ.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Pictures.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\PO456724392021.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\TcVfsyyjYuQ.exe	26%	ReversingLabs	Win32.Trojan.Razy	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.B6LNCKjOGt5EmFQ.exe.400000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
8.2.B6LNCKjOGt5EmFQ.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
8.2.B6LNCKjOGt5EmFQ.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
8.2.B6LNCKjOGt5EmFQ.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.0.PO456724392021.exe.ab0000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
16.0.PO2345714382021.exe.5d0000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
12.2.PO456724392021.exe.ab0000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
10.0.Pictures.exe.150000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
10.0.Pictures.exe.150000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
10.2.Pictures.exe.150000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
10.2.Pictures.exe.150000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
9.0.LOGO AND PICTURES.exe.db0000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
20.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
9.2.LOGO AND PICTURES.exe.db0000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File

Domains

Source	Detection	Scanner	Label	Link
freegeoip.app	1%	Virustotal		Browse
checkip.dyndns.com	0%	Virustotal		Browse
checkip.dyndns.org	0%	Virustotal		Browse

URLs

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://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app	0%	URL Reputation	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.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	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://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://crl.usertrusts	0%	Avira URL Cloud	safe	
http://https://www.geodatatool.com/en/?ip=3D84.17.52.74=0D=0A=	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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://checkip.dyndns.org/HB	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://https://www.geodatatool.com/en/?ip=84.17.52.74	0%	Avira URL Cloud	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.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://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://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://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://https://www.geodatatool.com/en/?ip=	0%	URL Reputation	safe	
http://https://www.geodatatool.com/en/?ip=	0%	URL Reputation	safe	
http://https://www.geodatatool.com/en/?ip=	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://https://www.geodatatool.com/en/?ip=3D84.17.52.74=0D=0A=0D=0ADat=	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/xml/84.17.52.74	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.74	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.74	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.154.36	true	false		high
freegeoip.app	172.67.188.154	true	false	• 1%, Virustotal, Browse	unknown
smtp.privateemail.com	199.193.7.228	true	false		high
checkip.dyndns.com	131.186.161.70	true	false	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
94.197.2.0.in-addr.arpa	unknown	unknown	true		unknown

Contacted URLs

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

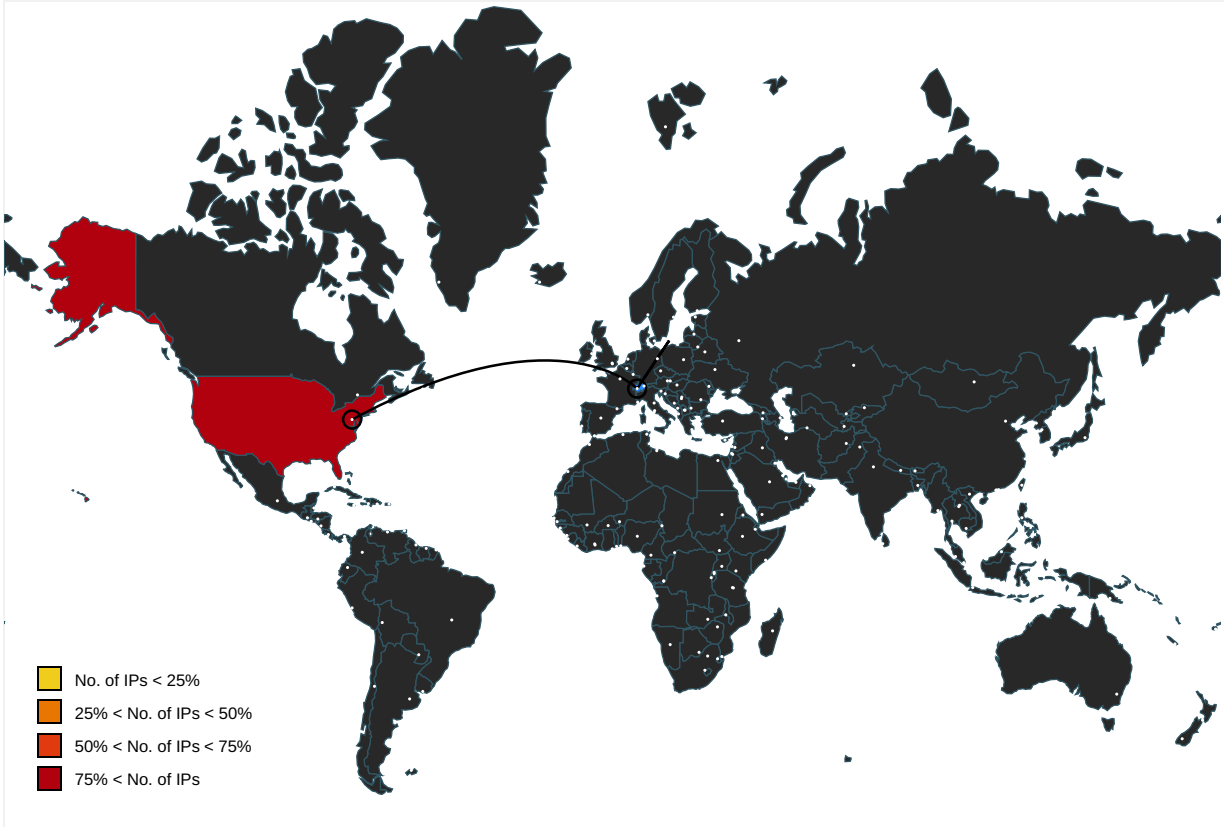
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.000000006640000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.000000006640000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	LOGO AND PICTURES.exe, 00000009.00000003.425343136.0000000006AAC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.000000006640000.00000002.00000001.sdmp	false		high
http://https://freegeoip.app	LOGO AND PICTURES.exe, 00000009.00000002.611704602.0000000003299000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.000000006640000.00000002.00000001.sdmp	false		high
http://ns.adobe.c/g	LOGO AND PICTURES.exe, 00000009.00000003.583245849.0000000092C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.usertrusts	LOGO AND PICTURES.exe, 00000009.00000003.459012991.0000000006ADF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.geodatatool.com/en/?ip=3D84.17.52.74=0D=0A=	LOGO AND PICTURES.exe, 00000009.00000002.615373407.0000000003515000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app/xml/LoadTimeZoneCountryNameCountryCodehttps://www.geodatatool.com/en/?ip=/	LOGO AND PICTURES.exe, 00000009.00000002.611647538.0000000003261000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://whatismyipaddress.com/-	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.293576161.0000000004C48000.00000004.00000001.sdmp, B6LNCKjOGt5EmFQ.exe, 00000008.00000003.281411863.0000000004450000.00000004.00000001.sdmp	false		high
http://checkip.dyndns.org/HB	LOGO AND PICTURES.exe, 00000009.00000002.611647538.000000003261000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.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	LOGO AND PICTURES.exe, 00000009.00000002.611647538.000000003261000.00000004.00000001.sdmp	false		high
http://www.ascendercorp.com/typedesigners.html	B6LNCKjOGt5EmFQ.exe, 00000000.00000003.226742441.0000000001CAB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.yahoo.com/config/login	Pictures.exe	false		high
http://www.fonts.com	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.geodatatool.com/en/?ip=84.17.52.74	LOGO AND PICTURES.exe, 00000009.00000002.611843586.000000003 2C9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	B6LNCKjOGt5EmFQ.exe, 00000008.00000003.281411863.0000000004450000.00000004.00000001.sdmp, B6LNCKjOGt5EmFQ.exe, 00000008.00000003.277852049.0000000003760000.00000004.00000001.sdmp, Pictures.exe	false		high
http://www.zhongyicts.com.cn	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.280326164.0000000003651000.00000004.00000001.sdmp, LOGO AND PICTURES.exe, 00000009.00000002.611647538.000000003261000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.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	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.293576161.0000000004C48000.00000004.00000001.sdmp, B6LNCKjOGt5EmFQ.exe, 00000008.00000003.291239624.0000000004451000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://freegeoip.app/xml/	LOGO AND PICTURES.exe, 00000009.00000002.611704602.000000003299000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	LOGO AND PICTURES.exe, 00000009.00000003.425343136.000000006AAC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.sdmp	false		high
http://https://sectigo.com/CPS0	LOGO AND PICTURES.exe, 00000009.00000003.425343136.000000006AAC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobj	LOGO AND PICTURES.exe, 00000009.00000003.583245849.000000002C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.geodatatool.com/en/?ip=	LOGO AND PICTURES.exe, 00000009.00000002.611843586.000000003 2C9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://smtp.privateemail.com	LOGO AND PICTURES.exe, 00000009.00000002.614076620.000000000348A000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	B6LNCKjOGt5EmFQ.exe, 00000000.00000002.312118405.0000000006640000.00000002.00000001.sdmp	false		high
http://https://www.geodatatool.com/en/?ip=3D84.17.52.74=0D=0A=0D=0ADat=	LOGO AND PICTURES.exe, 00000009.00000002.612629984.000000000033B7000.00000004.00000001.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	LOGO AND PICTURES.exe, 00000009.00000002.611647538.000000000032610000.00000004.00000001.sdmp	false		high
http://https://freegeoip.app/xml/84.17.52.74	LOGO AND PICTURES.exe, 00000009.00000002.611704602.000000000032990000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.ado/1	LOGO AND PICTURES.exe, 00000009.00000003.583245849.000000000092C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339499
Start date:	14.01.2021
Start time:	07:58:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	B6LNCKjOGt5EmFQ.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.spyw.evad.winEXE@25/14@49/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.2% (good quality ratio 0.8%) • Quality average: 49.8% • Quality standard deviation: 36%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.43.139.144, 92.122.144.200, 13.88.21.125, 67.27.157.126, 67.26.139.254, 67.27.159.254, 8.248.145.254, 8.253.204.120, 51.11.168.160, 92.122.213.247, 92.122.213.194, 20.54.26.129, 51.104.139.180, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:00:18	API Interceptor	2x Sleep call for process: B6LNCKjOGt5EmFQ.exe modified
08:00:45	API Interceptor	24x Sleep call for process: Pictures.exe modified
08:00:51	API Interceptor	274x Sleep call for process: PO2345714382021.exe modified
08:00:56	API Interceptor	875x Sleep call for process: PO456724392021.exe modified
08:00:59	API Interceptor	1x Sleep call for process: dw20.exe modified
08:01:07	API Interceptor	836x Sleep call for process: LOGO AND PICTURES.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.154.36	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INQUIRY.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	c9o0CtTIYT.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	6JLHKYvboo.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	khJdbt0clZ.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	ZMOKwXqVHO.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	5Av43Q5IXd.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	8oaZfXDstn.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	9vdouqRTh3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	M9RhKQ1G91.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	0CyK3Y7XBs.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	pwYhlZGMa6.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Vll6ZcOkEQ.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	oLHQIQAI3N.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	YrHUxpftPs.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	WuGzF7ZJ7P.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	cj9weNQmT2.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	lk5M5Q97c3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	2v7Vtqfo81.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Enquiry_pdf.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
131.186.161.70	wjSwL3KItA.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	NKP210102-NIT-SC2.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PO_RFQ_2021_12_01.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	BxiS9KHIxj.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	04XP8gXrF7.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	F-007331.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	Quotation.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	F6D24k8j9o.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	umOXxQ9PFS.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	0d7Kt71o8B.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	bank Acct Numbr-pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Y17wLTA3DX.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	0908000090000.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Purchase list- Karim Al-Dar Trading .exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	e8Ni2BqgDy.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	N5BJom1Uof.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	FACTURA DE PROFORMA.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Detalles del banco.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	aral#U0131k---- ekstrenizz.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	t0xy1m153o.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
whatismyipaddress.com	NDt93WWQwd089H7.exe	Get hash	malicious	Browse	• 104.16.155.36
	JkhR5oeRHA.exe	Get hash	malicious	Browse	• 66.171.248.178
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 104.16.155.36
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• 104.16.154.36
	INQUIRY.exe	Get hash	malicious	Browse	• 104.16.154.36
	Prueba de pago.exe	Get hash	malicious	Browse	• 104.16.155.36
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	http://https://my-alliances.co.uk/	Get hash	malicious	Browse	• 66.171.248.178
	c9o0CtTIYT.exe	Get hash	malicious	Browse	• 104.16.154.36
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• 104.16.155.36
	6JLHKYvboo.exe	Get hash	malicious	Browse	• 104.16.155.36
	jSMd8npgmU.exe	Get hash	malicious	Browse	• 104.16.155.36
	khJdbt0clZ.exe	Get hash	malicious	Browse	• 104.16.154.36
	ZMOKwXqVHO.exe	Get hash	malicious	Browse	• 104.16.154.36
	5Av43Q5lXd.exe	Get hash	malicious	Browse	• 104.16.154.36
	8oaZfXDstn.exe	Get hash	malicious	Browse	• 104.16.154.36
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• 104.16.155.36
freegeoip.app	IMG-0641.doc	Get hash	malicious	Browse	• 104.21.19.200
	a5T7dTsG4U.exe	Get hash	malicious	Browse	• 172.67.188.154
	NKP210102-NIT-SC2.exe	Get hash	malicious	Browse	• 104.21.19.200
	80lki3DsHA.exe	Get hash	malicious	Browse	• 172.67.188.154
	QPR-1064.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	IMG_2021_01_13_1_RFQ_PO_1832938.doc	Get hash	malicious	Browse	• 104.28.5.151
	IMG_2021_01_13_1_RFQ_PO_1832938.exe	Get hash	malicious	Browse	• 104.28.4.151
	09000000000000h.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO-5042.exe	Get hash	malicious	Browse	• 104.28.4.151
	onYLLDPXswyCVZu.exe	Get hash	malicious	Browse	• 104.28.4.151
	PO-75013.exe	Get hash	malicious	Browse	• 104.28.4.151
	ZwFwevQtlv.exe	Get hash	malicious	Browse	• 172.67.188.154
	ssDV3d9O9o.exe	Get hash	malicious	Browse	• 172.67.188.154
	wjSwL3KItA.exe	Get hash	malicious	Browse	• 104.28.4.151
	SecuriteInfo.com.Generic.mg.5a4b41327cabca49.exe	Get hash	malicious	Browse	• 104.28.5.151
	TD-10057.exe	Get hash	malicious	Browse	• 172.67.188.154
	NKP210102-NIT-SC2.exe	Get hash	malicious	Browse	• 172.67.188.154
	FedExAWB 772584418730.doc	Get hash	malicious	Browse	• 172.67.188.154
	TD-10057.doc	Get hash	malicious	Browse	• 172.67.188.154
	ndSscoDob9.exe	Get hash	malicious	Browse	• 104.28.4.151
smtp.privateemail.com	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe	Get hash	malicious	Browse	• 199.193.7.228
	DHL-Address.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	shipping-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	iVUeQOg6LO.exe	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Generic.mg.e92f0e2d08762687.exe	Get hash	malicious	Browse	• 199.193.7.228
	DHL-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	wCRnCAMZ3yT8BQ2.exe	Get hash	malicious	Browse	• 199.193.7.228
	Mj1eX5GWJxDRnuk.exe	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Trojan.Inject4.6535.8815.exe	Get hash	malicious	Browse	• 199.193.7.228
	shipping document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.Trojan.Inject4.6512.28917.exe	Get hash	malicious	Browse	• 199.193.7.228
	p72kooG5ak.exe	Get hash	malicious	Browse	• 199.193.7.228
	additional items.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	swift copy 1f354972.exe	Get hash	malicious	Browse	• 199.193.7.228
	DB_DHL_AWB_00117980920AD.exe	Get hash	malicious	Browse	• 199.193.7.228
	Payment Advice - Advice Ref[G20376302776].pptx.exe	Get hash	malicious	Browse	• 199.193.7.228

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment Reminder & SOA 202020121158.exe	Get hash	malicious	Browse	• 199.193.7.228
	kg.exe	Get hash	malicious	Browse	• 199.193.7.228
	logo.exe	Get hash	malicious	Browse	• 199.193.7.228
	Pictures.exe	Get hash	malicious	Browse	• 199.193.7.228

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	NEW ORDER_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	IMG-0641.doc	Get hash	malicious	Browse	• 104.21.19.200
	n1W2zlEddS.exe	Get hash	malicious	Browse	• 104.21.15.4
	a5T7dTsG4U.exe	Get hash	malicious	Browse	• 172.67.188.154
	NKP210102-NIT-SC2.exe	Get hash	malicious	Browse	• 104.21.19.200
	80Iki3DsHA.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Trojan.GenericKD.36094879.31571.exe	Get hash	malicious	Browse	• 104.26.3.223
	Notice_Admin_Johnstoncompanies_8578.htm	Get hash	malicious	Browse	• 172.67.70.208
	JdtN8nIcLi8RQOi.exe	Get hash	malicious	Browse	• 104.18.45.60
	Chrome.exe	Get hash	malicious	Browse	• 162.159.135.232
	QPR-1064.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Matrix.exe	Get hash	malicious	Browse	• 172.67.134.127
	JAAkR51fQY.exe	Get hash	malicious	Browse	• 104.21.13.175
	cremocompany-Invoice_216083-xlsx.html	Get hash	malicious	Browse	• 104.16.19.94
	VANGUARD PAYMENT ADVICE.htm	Get hash	malicious	Browse	• 104.31.67.162
	IMG_2021_01_13_1_RFQ_PO_1832938.doc	Get hash	malicious	Browse	• 104.28.5.151
	IMG_2021_01_13_1_RFQ_PO_1832938.exe	Get hash	malicious	Browse	• 104.28.4.151
	sample20210113-01.xlsm	Get hash	malicious	Browse	• 104.24.124.127
	Byrnes Gould PLLC.odt	Get hash	malicious	Browse	• 104.16.19.94
	aNmkT4KLJX.exe	Get hash	malicious	Browse	• 104.23.98.190
DYNDNSUS	IMG-0641.doc	Get hash	malicious	Browse	• 216.146.43.70
	a5T7dTsG4U.exe	Get hash	malicious	Browse	• 162.88.193.70
	NKP210102-NIT-SC2.exe	Get hash	malicious	Browse	• 162.88.193.70
	80Iki3DsHA.exe	Get hash	malicious	Browse	• 162.88.193.70
	QPR-1064.pdf.exe	Get hash	malicious	Browse	• 216.146.43.71
	IMG_2021_01_13_1_RFQ_PO_1832938.doc	Get hash	malicious	Browse	• 131.186.113.70
	IMG_2021_01_13_1_RFQ_PO_1832938.exe	Get hash	malicious	Browse	• 216.146.43.71
	090000000000000h.exe	Get hash	malicious	Browse	• 216.146.43.70
	PO-5042.exe	Get hash	malicious	Browse	• 216.146.43.71
	onYLLDPXswyCVZu.exe	Get hash	malicious	Browse	• 216.146.43.70
	PO-75013.exe	Get hash	malicious	Browse	• 162.88.193.70
	ZwFwevQtlv.exe	Get hash	malicious	Browse	• 216.146.43.71
	ssDV3d9O9o.exe	Get hash	malicious	Browse	• 216.146.43.71
	wjSwL3KItA.exe	Get hash	malicious	Browse	• 131.186.161.70
	SecuriteInfo.com.Generic.mg.5a4b41327cabca49.exe	Get hash	malicious	Browse	• 216.146.43.70
	TD-10057.exe	Get hash	malicious	Browse	• 216.146.43.70
	NKP210102-NIT-SC2.exe	Get hash	malicious	Browse	• 131.186.161.70
	FedExAWB 772584418730.doc	Get hash	malicious	Browse	• 131.186.113.70
	TD-10057.doc	Get hash	malicious	Browse	• 162.88.193.70
	ndSscoDob9.exe	Get hash	malicious	Browse	• 216.146.43.71

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	a5T7dTsG4U.exe	Get hash	malicious	Browse	• 172.67.188.154
	NKP210102-NIT-SC2.exe	Get hash	malicious	Browse	• 172.67.188.154
	80Iki3DsHA.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Trojan.GenericKD.36094879.31571.exe	Get hash	malicious	Browse	• 172.67.188.154
	QPR-1064.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	IMG_2021_01_13_1_RFQ_PO_1832938.exe	Get hash	malicious	Browse	• 172.67.188.154
	aNmkT4KLJX.exe	Get hash	malicious	Browse	• 172.67.188.154
	090000000000000h.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO-5042.exe	Get hash	malicious	Browse	• 172.67.188.154
	Geno_Quotation,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	onYLLDPXswyCVZu.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO-75013.exe	Get hash	malicious	Browse	• 172.67.188.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ZwFwevQtlv.exe	Get hash	malicious	Browse	• 172.67.188.154
	ssDV3d9O9o.exe	Get hash	malicious	Browse	• 172.67.188.154
	wjSwL3KItA.exe	Get hash	malicious	Browse	• 172.67.188.154
	Invoice-ID43739424297.vbs	Get hash	malicious	Browse	• 172.67.188.154
	Company Docs.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Generic.mg.5a4b41327cabca49.exe	Get hash	malicious	Browse	• 172.67.188.154
	TD-10057.exe	Get hash	malicious	Browse	• 172.67.188.154
	NKP210102-NIT-SC2.exe	Get hash	malicious	Browse	• 172.67.188.154

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_pictures.exe_c756fdb369d16caee6eb4c4fc55eace42746ab1_00000000_1a3a4dea\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):	16930
Entropy (8bit):	3.7534088968281503
Encrypted:	false
SSDEEP:	192:I+ugaMVvaKsn9fbeN9M2v1zzvSXk0ZKjBIcQry/u7snS274ItIn:9ugjaEdvh/sy/u7snX4Itg
MD5:	241EF4951F1724F8D1314BBFBB87465D
SHA1:	6BCBF070048674493FEBB07C204D05E998129610
SHA-256:	8EB667042376D717A87470D2AE0D383656CFB70BFE687BCCC80676683A25DB1D
SHA-512:	91AA5EF75A30C1FDF0DBE928849A484D82381F6491F99B7C7A1192786C66DDFC154E1D6F722C1924C274F32FC5F42EBE2161E42A1EF33CE764A073C6967A51D
Malicious:	false
Reputation:	low
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.=.1.3.2.5.5.1.1.3.6.4.8.9.6.7.0.7.6.3.....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.=.1.3.2.5.5.1.1.3.6.4.9.5.1.3.9.4.8.9.....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.=.7.b.8.4.6.b.2.8.-.c.b.8.e.-.4.d.0.5.-.b.c.9.4.-.d.8.c.2.b.c.7.e.c.a.6.8.....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.=.0.0.0.0.1.8.6.0.-.0.0.0.1.-.0.0.1.7.-.f.c.f.e.-.1.4.6.8.8.e.e.a.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.!.0.0.0.0.4.1.7.1.9.0.0.e.4.d.1.2.9.1.c.7.a.7.c.d.b.3.3.a.d.c.6.5.5.e.c.b.1.2.3.3.4.a.4.f.!.P.i.c.t.u.r.e.s...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.2././.0.9.:.1.0.:.5.1.:.3.2.!.0.!.P.i.c.t.u.r.e.s...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER23EC.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):	7660
Entropy (8bit):	3.6954137341102586
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi+R6g4Oe6YAY6FOqVgmfZ61S4Cp1l41fz3m:RrlsNio6n6YX64YgmfQ1Shlifa
MD5:	752C895F9DCD8F46A421ED01FC3D9137
SHA1:	A0E2791563BE980CE3A52637CA0E67A5CA39AA77
SHA-256:	3EBD2A9B184072C0007CA004F0623800CA3884EDCE089E48F0FD80B57373B6D5
SHA-512:	177B74E6B738AA8AC40C5F95B2D488CDE311F72C76DAE55493665140F9396F9489FE64B5B21D73A310EA037C98B8650F2A769EBAE1C93A928BB23EB929467690
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.2.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2525.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

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2525.tmp.xml	
Size (bytes):	4674
Entropy (8bit):	4.439678899414447
Encrypted:	false
SSDEEP:	48:cvIwSD8zsGJgtWI9+gWSC8Bn8fm8M4JFKC5FTso+q8v1XYt/xrvVXKd:uITfcBZSNqJFKvoK1YtJrvVXKd
MD5:	B3C65F177C1DEC134F2D225E3A86BB21
SHA1:	83F25E548BD0226D94AC22C57E582CBDEED12DFF
SHA-256:	B83847FA914868ED4AE188E38B5B9859232C7FA721DD1E979AA8476C683D2A8A
SHA-512:	88AE1BCF79CD03EA0B0A8502DB64431364BAE67ECD0375729D0BD26ACBF1D9E4C8079BAB37ADD7237383C0F1191F0883505171A8E7654534B15B7666CAEF056A
Malicious:	false
Reputation:	low
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="816551" />.. <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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\B6LNCKjOGt5EmFQ.exe.log	
Process:	C:\Users\user\Desktop\B6LNCKjOGt5EmFQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
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..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,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe	
Process:	C:\Users\user\Desktop\B6LNCKjOGt5EmFQ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	456192
Entropy (8bit):	5.4162986566993
Encrypted:	false
SSDEEP:	3072:gbG/+hpzWouj0ce9wDRlZg80CEZU8BVfCXEMRWTjwNs5Pu:gC/+7Wouj7e6DRlZjYfCXEsWTj+qu
MD5:	D9001138C5119D936B70BF77E136AFBE
SHA1:	CFA2DBFF8527715EAAD00E91BD8955A8FFFC1224
SHA-256:	9AE5EF3FD4FEEA105C1ED3F1E69FD4FA328E8F29F1937097280F7EEE7F8D749E
SHA-512:	0187EC1EDE0022DAA4021A72D871CA0B7694B312BDBA1C31BF3C0667CE0255C51E9880170A4B5226E63C2BF48F53B8071F12B08C106B6B82EB1D5389C3F9D57
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._..... ... .@.. .....`..... ..@.....K.... .....@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....H...Xy.....@'...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\PO2345714382021.exe	
Process:	C:\Users\user\Desktop\B6LNCKjOGt5EmFQ.exe

C:\Users\user\AppData\Local\Temp\PO2345714382021.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	220672
Entropy (8bit):	6.060576428712888
Encrypted:	false
SSDEEP:	3072:zVQsV4phvec6kzCuJ5ufEUJdYi68Nl2xQzMfNlpmgVQoKPMXT3QECAJrYULCqv:zN49CaUXxN0AWNvmHoKPW3B0U
MD5:	9B79DE8E3AD21F14E71E55CFA6AE4727
SHA1:	3C2066345874FEBAFE281BBDE952D4F32D2ED53A
SHA-256:	56BD25ACDB97CE17F8351B926C48A4F63E348C40F6C5913219B0745D99F6B31D
SHA-512:	F922BE9228BAA1DAB85A5CFACFAFBB6E8C919009BB843B6CDBA0C2E24F6ABFCBE26417046BE248CCB41F820111633FDEE7C6EA5865A2FBCC3BCF22C52A7208E6
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\PO2345714382021.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...y._.....V.....u... .....@.. ....@.....t..S..... ....H.....text....U... ...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\PO456724392021.exe	
Process:	C:\Users\user\Desktop\B6LNCKjOGt5EmFQ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	221696
Entropy (8bit):	6.062523365287507
Encrypted:	false
SSDEEP:	3072:099WeApgkpnx/kiKvzkGts4mhUi7Ergj7G0xQooD5oOpm8VQ5HABdXEPh6xtUiao:q8p7KvzApUbQ7xw9mbpABd08HU
MD5:	F38E2D474C075EFF35B4EF81FDACA650
SHA1:	13F869037C80BE3CD4736C5F67431161C79E5970
SHA-256:	F9EE81B7DEF0B0008CEF43847FB9BA520C0B57A49E7A71B47FF8D6EE1FEC4298
SHA-512:	B57A699E88F2ED2D83901BE6362663BFA98944A95E74F0E8D36622868A7AD04F9D557B617BD71A9A69FD7B7B1E7143EDEAAFF0A5E54D81311F78F8497FDEA64
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\PO456724392021.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...._.....X.....v... .....@.. ....@.....u..S.....P..... ....H.....text...4V... ...X..... ..`.rsrc...P.....Z.....@..@.rel oc.....`.....@..B.....v.....H.....H.....(....*..(....*.s.....s.....s.....s.....*...0..,.....+.....,.....,.....,.....,+.+.~.. ..o....*.0..,.....+.....,.....,.....,+.+.~....o....*.0..,.....+.....,.....,.....,.....,+.+.~....o....*.0..,.....+.....,.....,.....,.....,+.+.~....o....*.0.....+.....,.....,.....,.....,+.+...(....(....*...0.. (.....+.....,.....,.....,.....,+.+..(....*.0..,.....

C:\Users\user\AppData\Local\Temp\Pictures.exe	
Process:	C:\Users\user\Desktop\B6LNCKjOGt5EmFQ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	533504
Entropy (8bit):	6.503670066564474
Encrypted:	false
SSDEEP:	6144:wuHqCVjDbS/QTjhUqBfxrwEnuNcSsm7IoYGW0VvBXCAt6kihwE+VDpJYWmlwnx9u:/jDQtqB5urTIoYWBQk1E+VF9mOx90i
MD5:	25146E9C5ECD498DD17BA01E6CFAEB24
SHA1:	4171900E4D1291C7A7CDB33ADC655ECB12334A4F
SHA-256:	5207F3D079A52017E7977296C9EBA782D3D5EAE5ADEC94FA38ACDD88C184496D
SHA-512:	18374C6619B5F3D310DB43E5F81DB1333BDC9DC4086910FE2724A406D445CCBF5B16463B9341FBE718B2AAE9E929A2302655F3964EB64B47F2D80418B46E478F
Malicious:	**true**
Yara Hits:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Local\Temp\Pictures.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Local\Temp\Pictures.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Local\Temp\Pictures.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Local\Temp\Pictures.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Local\Temp\Pictures.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Local\Temp\Pictures.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...4._.....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\tmpDAC4.tmp	
Process:	C:\Users\user\Desktop\B6LNCKjOGt5EmFQ.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.199929157081269
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBDqtn:cbh47TlNQ//rydbz9l3YODOLNdq3y
MD5:	AC43371F9BD7E88C08D426F7689595BE
SHA1:	E8FCA4BB37D5B2178D6FE2E4C99390CA78DC3C3E
SHA-256:	35EB8CB95831F8879793C40A8870F74F6F685C0F9CB711779382C609B7CDCDD8
SHA-512:	5E729C6EA9C5D1415AEA6C9241D5E01EBCE7B002CDC8AA09CDB51324E75BDFE08CBC0BCB423486FE51BFE5902763A78A66E01C48E14222CDC1E4784190391 8A
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\TcVfsyyjYuQ.exe	
Process:	C:\Users\user\Desktop\B6LNCKjOGt5EmFQ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1891328
Entropy (8bit):	7.915566672587132
Encrypted:	false
SSDEEP:	49152:NHIhVUjx98WqWwDtMjLm2pwEFv0anoHMkL:NHIwWSMjLJwyv0a+h
MD5:	80D255A6A5EC339E15D6FEC3C0FEF666
SHA1:	BCA665FF5A6A7084DF2D424C0ED7FFF3E141ACBC
SHA-256:	3E48D983E3315501931C646F896A8189637F5B9D21C453B051CD17F2584EE3C4
SHA-512:	1BF61D60FC6646FF63786DA850B4118FB15DCC6F2C831A8A80D58225CF55BFEF395D69473AFEAE9D05F97C3ADCEDD90100C4266BC1D537B7F6D7F933CB6291 4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 26%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._..... .....@.. .....@..... ..@.....S..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....`#..(..... ...@h.....0.....*....0.....}.....(.....(.....r...p.(....(.....{....(....(.....{....(....(.....{....(....(.....{....(....(.....{....(....(.....{....(....*...0..a.....(.....(....(.... .H+. ..Hua%....^E.....s.....-.....M.....8..... ....Z O./^a+..(..... .%"Z .b&a+..-. 6...%+. ...%&.. ....Za8r..... ...., .m.!%+. A.4m%&.. .=.Za8L..... .=.dZ -.

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\AppData\Local\Temp\Pictures.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:fn:f
MD5:	405075699F065E43581F27D67BB68478
SHA1:	1A20CF59F0584ADA3DEEFF6C1C5B4C11C691AEC0
SHA-256:	7666197A246DDED3B8238775F3CEDF8350A2858A8117E744A703987DD55AA497
SHA-512:	C5EB5E284710FBC093BB55FEAE8A6623D0366DB40A03CBD399D7173E06641DAB84DAD3CF5C0DC330B727498688093B9A7FC884F7AFBE88C0627F963ADC61DE B1
Malicious:	false
Preview:	6240

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\AppData\Local\Temp\Pictures.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	46
Entropy (8bit):	4.363038521594966
Encrypted:	false
SSDEEP:	3:oNWXp5cViE2J5xAIEN:oNWXp+N23fEN
MD5:	46833127CC4C64CFB8650EE775DC5D9D
SHA1:	F2B43FDAEAC18E55085436E55D9C30E2FD240386
SHA-256:	6F0942DBA73C781461E1E322E13537AB0F0EBE49D8C3DBD6CF9C23FC91404CBC
SHA-512:	FDDDBBEB26897D349E74B5E8DC9D0A256692378494E87E6F356AAE188C16C5481030B6F5545613FF2A4D5A5F775B85DE8DED3D347E15E404FD187EFC630783E A
Malicious:	false
Preview:	C:\Users\user\AppData\Local\Temp\Pictures.exe

C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	
Process:	C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5047425
Entropy (8bit):	7.94875017456693
Encrypted:	false
SSDEEP:	98304:PAcWjqWcHRM/gAcWjqWcHRM/gAcWjqWcHRM/5AcWjqWcHRM/5AcWjqWcHRM/+2Y+:Yfj8WJfj8WJfj8Wmfj8Wmfj8WaKgBFSz
MD5:	D9C93607661494 64EAE529F4C0E8A50C
SHA1:	54E9BD21B7435FA52E9737B54AE1DE152B68C91C
SHA-256:	CA710E0EE8D9F14410F4FC9CB3B37086F33E2FC250CF1A140C24B0A8400D6C43
SHA-512:	41056162C6935FA584CFD907B42EF8DD7BADB3CC2C790B106092FDC6529E8DE7F2B8ED96F9D8DC7BD70586CC719FEEDA16339FF89FDC2E944F532069277FD2 5
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...eE.....;..Q$.&c..... ..F_g.q^.fFf0..,F.Db.s.E0..DL.T..E.AD.&7..tC}.j..j...]..>..}....sN.UaWX.. {..`...2..zv...1....1..._{...u..1....Xw..._..`../.....l..._...]*c....mG....m`../.....b...._>..e.....z.cf..u....c.:J.M.C...4]h....Am.df..v....kT...*..Im..:.....lS.;.~..].x.cf.g8.<..c..r.9..q:=j.H..x..... .T.jko....E!.....>...+x.X..+....k..b.....Y.....Y.o86x.#.C.~.../13._..`.....l.0.p..@6..d;.h....;..p..4.j6..h.\#K..b\.0.Q.`.$.w>s...D5?.<.JX_.Z..ZS.. .....?.....O..G....?...XY.GB.....CA} ...^c.Va.?@..m.!.'.....~..Q%:..}e..CG?[.m[P..(-.....[.4.=...t..p4.....?u1...R.eJ..r0.1....T.L.....l.....?b*....N.6.Zy*^..S.....8...b...=1..(}..T.l`*.. .....a}.kQ.hMm#:.....H.._>.. ...Gxa.]..2.....J.B..C.O.C.g?T.y.G..t....Q\...l..mA}O....w4.4.....4..G..}I..5-.).R.$hQ..]"...H[w.....c.X.....@R.d.}..Lh@.H'?....V..?....9.a9.T..(.F.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.915566672587132

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	B6LNCKjOGt5EmFQ.exe
File size:	1891328
MD5:	80d255a6a5ec339e15d6fec3c0fef666
SHA1:	bca665ff5a6a7084df2d424c0ed7fff3e141acbc
SHA256:	3e48d983e3315501931c646f896a8189637f5b9d21c453b051cd17f2584ee3c4
SHA512:	1bf61d60fc6646ff63786da850b4118fb15dcc6f2c831a8a80d58225cf55bfef395d69473afeae9d05f97c3adcedd90100c4266bc1d537b7f6d7f933cb6291c4
SSDEEP:	49152:NHIhVUjx98WqWwDtMjLm2pwEFv0anoHMkL:NHlwWSMjLJwyv0a+h
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... ._..... ....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x5ceede
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:	0x5FFF92AD [Thu Jan 14 00:39:09 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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1cee88	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1d0000	0x610	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1d2000	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	0x1ccee4	0x1cd000	False	0.905138392252	data	7.9172695107	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x1d0000	0x610	0x800	False	0.3896484375	data	4.7189568742	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1d2000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1d00a0	0x384	data	English	United States
RT_MANIFEST	0x1d0424	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
LegalCopyright	3db75199 2251 4ce6 94e1 5f13d35d3b9f
CompanyName	BreakingSecurity.net
LegalTrademarks	611d5f3a 1c65 419e a1cf 62fe3f64faf9
Comments	db14de2b 0bc1 4f57 9f45 3449e425f690
ProductName	ViottoBinder_Stub
FileDescription	fa8434f7 0c3e 4c84 9dd6 95b941e832e5
Guid	86f84c52-488a-487d-9083-479210c03845
Translation	0x0000 0x04e4

Possible Origin

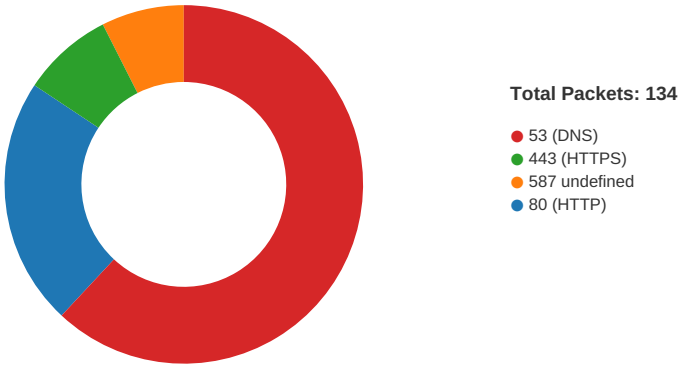
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/21-07:59:54.284349	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49731	104.16.154.36	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 07:59:54.193475008 CET	49731	80	192.168.2.3	104.16.154.36
Jan 14, 2021 07:59:54.233514071 CET	80	49731	104.16.154.36	192.168.2.3
Jan 14, 2021 07:59:54.233608007 CET	49731	80	192.168.2.3	104.16.154.36
Jan 14, 2021 07:59:54.235313892 CET	49731	80	192.168.2.3	104.16.154.36
Jan 14, 2021 07:59:54.275219917 CET	80	49731	104.16.154.36	192.168.2.3
Jan 14, 2021 07:59:54.284348965 CET	80	49731	104.16.154.36	192.168.2.3
Jan 14, 2021 07:59:54.414906025 CET	49731	80	192.168.2.3	104.16.154.36
Jan 14, 2021 08:00:01.699487925 CET	49733	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:04.712661982 CET	49733	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:04.860668898 CET	80	49733	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:04.861741066 CET	49733	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:04.861777067 CET	49733	80	192.168.2.3	131.186.161.70

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 08:00:05.010050058 CET	80	49733	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:05.010082960 CET	80	49733	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:05.010092974 CET	80	49733	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:05.010410070 CET	49733	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:05.015974998 CET	49733	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:05.164006948 CET	80	49733	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:05.240928888 CET	49737	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:05.389535904 CET	80	49737	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:05.389669895 CET	49737	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:05.390219927 CET	49737	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:05.538772106 CET	80	49737	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:05.539251089 CET	80	49737	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:05.539274931 CET	80	49737	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:05.539356947 CET	49737	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:05.539808035 CET	49737	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:05.688400984 CET	80	49737	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:08.455557108 CET	49731	80	192.168.2.3	104.16.154.36
Jan 14, 2021 08:00:08.495773077 CET	80	49731	104.16.154.36	192.168.2.3
Jan 14, 2021 08:00:08.495901108 CET	49731	80	192.168.2.3	104.16.154.36
Jan 14, 2021 08:00:08.521887064 CET	49738	587	192.168.2.3	199.193.7.228
Jan 14, 2021 08:00:08.712308884 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:08.712419987 CET	49738	587	192.168.2.3	199.193.7.228
Jan 14, 2021 08:00:08.772363901 CET	49739	443	192.168.2.3	172.67.188.154
Jan 14, 2021 08:00:08.818191051 CET	443	49739	172.67.188.154	192.168.2.3
Jan 14, 2021 08:00:08.818346977 CET	49739	443	192.168.2.3	172.67.188.154
Jan 14, 2021 08:00:08.882314920 CET	49739	443	192.168.2.3	172.67.188.154
Jan 14, 2021 08:00:08.906934023 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:08.907265902 CET	49738	587	192.168.2.3	199.193.7.228
Jan 14, 2021 08:00:08.928133011 CET	443	49739	172.67.188.154	192.168.2.3
Jan 14, 2021 08:00:08.930773020 CET	443	49739	172.67.188.154	192.168.2.3
Jan 14, 2021 08:00:08.930797100 CET	443	49739	172.67.188.154	192.168.2.3
Jan 14, 2021 08:00:08.930990934 CET	49739	443	192.168.2.3	172.67.188.154
Jan 14, 2021 08:00:08.957525015 CET	49739	443	192.168.2.3	172.67.188.154
Jan 14, 2021 08:00:09.003372908 CET	443	49739	172.67.188.154	192.168.2.3
Jan 14, 2021 08:00:09.003599882 CET	443	49739	172.67.188.154	192.168.2.3
Jan 14, 2021 08:00:09.095568895 CET	49739	443	192.168.2.3	172.67.188.154
Jan 14, 2021 08:00:09.102688074 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:09.102705956 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:09.105675936 CET	49738	587	192.168.2.3	199.193.7.228
Jan 14, 2021 08:00:09.141305923 CET	443	49739	172.67.188.154	192.168.2.3
Jan 14, 2021 08:00:09.157989979 CET	443	49739	172.67.188.154	192.168.2.3
Jan 14, 2021 08:00:09.212981939 CET	49739	443	192.168.2.3	172.67.188.154
Jan 14, 2021 08:00:09.270381927 CET	49740	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:09.295670986 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:09.384603024 CET	49738	587	192.168.2.3	199.193.7.228
Jan 14, 2021 08:00:09.418406010 CET	80	49740	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:09.418521881 CET	49740	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:09.419497967 CET	49740	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:09.567349911 CET	80	49740	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:09.567424059 CET	80	49740	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:09.567435980 CET	80	49740	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:09.567512035 CET	49740	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:09.567805052 CET	49740	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:09.568572044 CET	49739	443	192.168.2.3	172.67.188.154
Jan 14, 2021 08:00:09.574563980 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:09.574583054 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:09.574599981 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:09.574671984 CET	49738	587	192.168.2.3	199.193.7.228
Jan 14, 2021 08:00:09.633825064 CET	443	49739	172.67.188.154	192.168.2.3
Jan 14, 2021 08:00:09.713150978 CET	49739	443	192.168.2.3	172.67.188.154
Jan 14, 2021 08:00:09.715703964 CET	80	49740	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:09.718214989 CET	49741	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:09.766267061 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:09.807080030 CET	49738	587	192.168.2.3	199.193.7.228

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 08:00:09.866115093 CET	80	49741	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:09.866534948 CET	49741	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:09.866982937 CET	49741	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:09.997090101 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:09.998270035 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:09.998295069 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:09.998413086 CET	49738	587	192.168.2.3	199.193.7.228
Jan 14, 2021 08:00:10.014882088 CET	80	49741	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:10.014935970 CET	80	49741	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:10.014949083 CET	80	49741	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:10.015129089 CET	49741	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:10.015634060 CET	49741	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:10.016644955 CET	49739	443	192.168.2.3	172.67.188.154
Jan 14, 2021 08:00:10.060599089 CET	49738	587	192.168.2.3	199.193.7.228
Jan 14, 2021 08:00:10.083353996 CET	443	49739	172.67.188.154	192.168.2.3
Jan 14, 2021 08:00:10.163477898 CET	80	49741	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:10.181323051 CET	49742	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:10.213139057 CET	49739	443	192.168.2.3	172.67.188.154
Jan 14, 2021 08:00:10.250571012 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:10.250998974 CET	587	49738	199.193.7.228	192.168.2.3
Jan 14, 2021 08:00:10.256958008 CET	49738	587	192.168.2.3	199.193.7.228
Jan 14, 2021 08:00:10.329204082 CET	80	49742	131.186.161.70	192.168.2.3
Jan 14, 2021 08:00:10.329406023 CET	49742	80	192.168.2.3	131.186.161.70
Jan 14, 2021 08:00:10.329763889 CET	49742	80	192.168.2.3	131.186.161.70

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 07:59:17.569272041 CET	65110	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:17.617516994 CET	53	65110	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:18.408240080 CET	58361	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:18.456034899 CET	53	58361	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:19.455475092 CET	63492	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:19.506242037 CET	53	63492	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:21.099704981 CET	60831	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:21.150368929 CET	53	60831	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:22.205271959 CET	60100	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:22.336503029 CET	53	60100	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:23.258204937 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:23.314742088 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:24.204947948 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:24.255738020 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:25.102734089 CET	53023	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:25.150680065 CET	53	53023	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:26.072304010 CET	49563	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:27.069504023 CET	49563	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:27.991471052 CET	53	49563	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:28.874310970 CET	51352	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:28.922048092 CET	53	51352	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:29.666528940 CET	59349	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:29.714510918 CET	53	59349	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:31.317909002 CET	57084	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:31.365736961 CET	53	57084	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:33.247423887 CET	58823	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:33.295321941 CET	53	58823	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:34.474976063 CET	57568	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:34.522856951 CET	53	57568	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:43.063770056 CET	50540	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:43.124294996 CET	53	50540	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:53.520191908 CET	54366	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:53.576852083 CET	53	54366	8.8.8.8	192.168.2.3
Jan 14, 2021 07:59:54.102127075 CET	53034	53	192.168.2.3	8.8.8.8
Jan 14, 2021 07:59:54.158432007 CET	53	53034	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:00.889106035 CET	57762	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 08:00:00.936932087 CET	53	57762	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:01.510406971 CET	55435	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:01.558233976 CET	53	55435	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:01.582978010 CET	50713	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:01.633629084 CET	53	50713	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:01.797789097 CET	56132	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:01.853483915 CET	53	56132	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:03.690836906 CET	58987	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:03.738687038 CET	53	58987	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:08.462229967 CET	56579	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:08.520081043 CET	53	56579	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:08.704726934 CET	60633	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:08.763041019 CET	53	60633	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:13.499056101 CET	61292	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:13.556627989 CET	53	61292	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:22.471590996 CET	63619	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:22.529303074 CET	53	63619	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:23.664125919 CET	64938	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:23.720735073 CET	53	64938	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:25.627404928 CET	61946	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:25.686389923 CET	53	61946	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:27.092154980 CET	64910	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:27.148614883 CET	53	64910	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:27.313196898 CET	52123	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:27.372226954 CET	53	52123	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:28.614837885 CET	56130	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:28.674099922 CET	53	56130	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:30.369122028 CET	56338	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:30.425196886 CET	53	56338	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:31.785188913 CET	59420	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:31.841897964 CET	53	59420	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:32.113264084 CET	58784	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:32.169792891 CET	53	58784	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:34.010411024 CET	63978	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:34.058620930 CET	53	63978	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:37.266448975 CET	62938	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:37.325333118 CET	53	62938	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:37.704689026 CET	55708	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:37.735269070 CET	56803	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:37.776067972 CET	53	55708	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:37.783068895 CET	53	56803	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:41.768898964 CET	57145	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:41.825370073 CET	53	57145	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:42.182595015 CET	55359	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:42.243969917 CET	53	55359	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:43.553025007 CET	58306	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:43.610675097 CET	53	58306	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:46.228390932 CET	64124	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:46.285444021 CET	53	64124	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:47.262676001 CET	49361	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:47.319166899 CET	53	49361	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:52.853676081 CET	63150	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:52.910289049 CET	53	63150	8.8.8.8	192.168.2.3
Jan 14, 2021 08:00:57.864089966 CET	53279	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:00:57.923175097 CET	53	53279	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:00.709014893 CET	56881	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:00.766215086 CET	53	56881	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:01.422801971 CET	53642	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:01.479815960 CET	53	53642	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:05.323237896 CET	55667	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:05.374082088 CET	53	55667	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:06.387660027 CET	54833	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:06.435551882 CET	53	54833	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:12.301712990 CET	62476	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 08:01:12.357888937 CET	53	62476	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:13.643379927 CET	49705	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:13.702507019 CET	53	49705	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:15.990230083 CET	61477	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:16.041006088 CET	53	61477	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:17.256880045 CET	61633	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:17.304717064 CET	53	61633	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:17.679095030 CET	55949	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:17.729788065 CET	53	55949	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:18.167495966 CET	57601	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:18.227045059 CET	53	57601	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:20.848212957 CET	49342	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:20.899019003 CET	53	49342	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:25.163115978 CET	56253	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:25.222198963 CET	53	56253	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:27.366777897 CET	49667	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:27.423219919 CET	53	49667	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:29.902163982 CET	55439	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:29.950059891 CET	53	55439	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:34.008392096 CET	57069	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:34.067707062 CET	53	57069	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:38.434175014 CET	57659	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:38.490578890 CET	53	57659	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:41.304433107 CET	54717	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:41.352474928 CET	53	54717	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:43.309600115 CET	63975	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:43.365588903 CET	53	63975	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:47.604231119 CET	56639	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:47.655323982 CET	53	56639	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:51.261096001 CET	51856	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:51.309034109 CET	53	51856	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:52.632894039 CET	56546	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:52.683711052 CET	53	56546	8.8.8.8	192.168.2.3
Jan 14, 2021 08:01:55.232933998 CET	62152	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:01:55.283688068 CET	53	62152	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:01.687004089 CET	53470	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:01.734879017 CET	53	53470	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:03.720463037 CET	56446	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:03.776787043 CET	53	56446	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:06.874089003 CET	59631	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:06.930296898 CET	53	59631	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:07.400751114 CET	55515	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:07.457195997 CET	53	55515	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:08.036328077 CET	64547	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:08.085427999 CET	53	64547	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:08.841780901 CET	51759	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:08.892477989 CET	53	51759	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:08.928555965 CET	59207	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:08.987667084 CET	53	59207	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:09.344995975 CET	54269	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:09.404113054 CET	53	54269	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:09.882831097 CET	54856	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:09.939145088 CET	53	54856	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:10.416321993 CET	64140	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:10.475392103 CET	53	64140	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:10.971044064 CET	62271	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:11.025665045 CET	57404	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:11.027297974 CET	53	62271	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:11.084976912 CET	53	57404	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:11.736547947 CET	62997	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:11.784336090 CET	53	62997	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:12.177129030 CET	57712	53	192.168.2.3	8.8.8.8
Jan 14, 2021 08:02:12.233146906 CET	53	57712	8.8.8.8	192.168.2.3
Jan 14, 2021 08:02:14.219427109 CET	60065	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 08:02:14.275495052 CET	53	60065	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 07:59:53.520191908 CET	192.168.2.3	8.8.8.8	0x577c	Standard query (0)	94.197.2.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jan 14, 2021 07:59:54.102127075 CET	192.168.2.3	8.8.8.8	0xf2d	Standard query (0)	whatismyipaddress.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:01.510406971 CET	192.168.2.3	8.8.8.8	0xae5	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:01.582978010 CET	192.168.2.3	8.8.8.8	0x2b6d	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:08.462229967 CET	192.168.2.3	8.8.8.8	0xe970	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:08.704726934 CET	192.168.2.3	8.8.8.8	0xd6f8	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:22.471590996 CET	192.168.2.3	8.8.8.8	0x9f9c	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:23.664125919 CET	192.168.2.3	8.8.8.8	0x647	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:25.627404928 CET	192.168.2.3	8.8.8.8	0x238a	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:27.092154980 CET	192.168.2.3	8.8.8.8	0x26eb	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:27.313196898 CET	192.168.2.3	8.8.8.8	0x7f29	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:28.614837885 CET	192.168.2.3	8.8.8.8	0xe531	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:30.369122028 CET	192.168.2.3	8.8.8.8	0xd404	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:31.785188913 CET	192.168.2.3	8.8.8.8	0xaf23	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:32.113264084 CET	192.168.2.3	8.8.8.8	0xf54d	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:34.010411024 CET	192.168.2.3	8.8.8.8	0x9690	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:37.266448975 CET	192.168.2.3	8.8.8.8	0x4c64	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:37.735269070 CET	192.168.2.3	8.8.8.8	0x732c	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:41.768898964 CET	192.168.2.3	8.8.8.8	0xa0a4	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:42.182595015 CET	192.168.2.3	8.8.8.8	0x12da	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:46.228390932 CET	192.168.2.3	8.8.8.8	0x1ce7	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:47.262676001 CET	192.168.2.3	8.8.8.8	0x3e25	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:52.853676081 CET	192.168.2.3	8.8.8.8	0x58ab	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:57.864089966 CET	192.168.2.3	8.8.8.8	0x8ab1	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:00.709014893 CET	192.168.2.3	8.8.8.8	0x6063	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:01.422801971 CET	192.168.2.3	8.8.8.8	0x7feb	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:05.323237896 CET	192.168.2.3	8.8.8.8	0x76e7	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:06.387660027 CET	192.168.2.3	8.8.8.8	0x3bdb	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:12.301712990 CET	192.168.2.3	8.8.8.8	0x625f	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:13.643379927 CET	192.168.2.3	8.8.8.8	0x5369	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:17.256880045 CET	192.168.2.3	8.8.8.8	0xebf3	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:18.167495966 CET	192.168.2.3	8.8.8.8	0x676	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:20.848212957 CET	192.168.2.3	8.8.8.8	0x8db1	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:25.163115978 CET	192.168.2.3	8.8.8.8	0xabf5	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 08:01:27.366777897 CET	192.168.2.3	8.8.8.8	0xdeb2	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:29.902163982 CET	192.168.2.3	8.8.8.8	0xbe63	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:34.008392096 CET	192.168.2.3	8.8.8.8	0x971c	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:38.434175014 CET	192.168.2.3	8.8.8.8	0x97b9	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:41.304433107 CET	192.168.2.3	8.8.8.8	0xdc66	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:43.309600115 CET	192.168.2.3	8.8.8.8	0x88bc	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:47.604231119 CET	192.168.2.3	8.8.8.8	0xdf13	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:51.261096001 CET	192.168.2.3	8.8.8.8	0xce33	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:52.632894039 CET	192.168.2.3	8.8.8.8	0x94fc	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:55.232933998 CET	192.168.2.3	8.8.8.8	0x51e6	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:02:01.687004089 CET	192.168.2.3	8.8.8.8	0x5fc3	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:02:03.720463037 CET	192.168.2.3	8.8.8.8	0x1935	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:02:08.928555965 CET	192.168.2.3	8.8.8.8	0x2d3f	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:02:10.971044064 CET	192.168.2.3	8.8.8.8	0x4489	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 08:02:14.219427109 CET	192.168.2.3	8.8.8.8	0x4c3e	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
Jan 14, 2021 07:59:53.576852083 CET	8.8.8.8	192.168.2.3	0x577c	Name error (3)	94.197.2.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Jan 14, 2021 07:59:54.158432007 CET	8.8.8.8	192.168.2.3	0xf2d	No error (0)	whatismyipaddress.com		104.16.154.36	A (IP address)	IN (0x0001)
Jan 14, 2021 07:59:54.158432007 CET	8.8.8.8	192.168.2.3	0xf2d	No error (0)	whatismyipaddress.com		104.16.155.36	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:01.558233976 CET	8.8.8.8	192.168.2.3	0xae5	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 08:00:01.558233976 CET	8.8.8.8	192.168.2.3	0xae5	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:01.558233976 CET	8.8.8.8	192.168.2.3	0xae5	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:01.558233976 CET	8.8.8.8	192.168.2.3	0xae5	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:01.558233976 CET	8.8.8.8	192.168.2.3	0xae5	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:01.558233976 CET	8.8.8.8	192.168.2.3	0xae5	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:01.633629084 CET	8.8.8.8	192.168.2.3	0x2b6d	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 08:00:01.633629084 CET	8.8.8.8	192.168.2.3	0x2b6d	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:01.633629084 CET	8.8.8.8	192.168.2.3	0x2b6d	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:01.633629084 CET	8.8.8.8	192.168.2.3	0x2b6d	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:01.633629084 CET	8.8.8.8	192.168.2.3	0x2b6d	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 08:00:01.633629084 CET	8.8.8.8	192.168.2.3	0x2b6d	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:08.520081043 CET	8.8.8.8	192.168.2.3	0xe970	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:08.763041019 CET	8.8.8.8	192.168.2.3	0xd6f8	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:08.763041019 CET	8.8.8.8	192.168.2.3	0xd6f8	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:22.529303074 CET	8.8.8.8	192.168.2.3	0x9f9c	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:23.720735073 CET	8.8.8.8	192.168.2.3	0x647	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:25.686389923 CET	8.8.8.8	192.168.2.3	0x238a	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:27.148614883 CET	8.8.8.8	192.168.2.3	0x26eb	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:27.372226954 CET	8.8.8.8	192.168.2.3	0x7f29	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:28.674099922 CET	8.8.8.8	192.168.2.3	0xe531	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:30.425196886 CET	8.8.8.8	192.168.2.3	0xd404	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:31.841897964 CET	8.8.8.8	192.168.2.3	0xaf23	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:32.169792891 CET	8.8.8.8	192.168.2.3	0xf54d	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:34.058620930 CET	8.8.8.8	192.168.2.3	0x9690	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:37.325333118 CET	8.8.8.8	192.168.2.3	0x4c64	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:37.783068895 CET	8.8.8.8	192.168.2.3	0x732c	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:41.825370073 CET	8.8.8.8	192.168.2.3	0xa0a4	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:42.243969917 CET	8.8.8.8	192.168.2.3	0x12da	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:46.285444021 CET	8.8.8.8	192.168.2.3	0x1ce7	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:47.319166899 CET	8.8.8.8	192.168.2.3	0x3e25	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:52.910289049 CET	8.8.8.8	192.168.2.3	0x58ab	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:00:57.923175097 CET	8.8.8.8	192.168.2.3	0x8ab1	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:00.766215086 CET	8.8.8.8	192.168.2.3	0x6063	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:01.479815960 CET	8.8.8.8	192.168.2.3	0x7feb	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:05.374082088 CET	8.8.8.8	192.168.2.3	0x76e7	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:06.435551882 CET	8.8.8.8	192.168.2.3	0x3bdb	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
Jan 14, 2021 08:01:12.357888937 CET	8.8.8.8	192.168.2.3	0x625f	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:13.702507019 CET	8.8.8.8	192.168.2.3	0x5369	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:17.304717064 CET	8.8.8.8	192.168.2.3	0xebf3	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:18.227045059 CET	8.8.8.8	192.168.2.3	0x676	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:20.899019003 CET	8.8.8.8	192.168.2.3	0x8db1	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:25.222198963 CET	8.8.8.8	192.168.2.3	0xabf5	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:27.423219919 CET	8.8.8.8	192.168.2.3	0xdeb2	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:29.950059891 CET	8.8.8.8	192.168.2.3	0xbe63	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:34.067707062 CET	8.8.8.8	192.168.2.3	0x971c	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:38.490578890 CET	8.8.8.8	192.168.2.3	0x97b9	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:41.352474928 CET	8.8.8.8	192.168.2.3	0xdc66	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:43.365588903 CET	8.8.8.8	192.168.2.3	0x88bc	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:47.655323982 CET	8.8.8.8	192.168.2.3	0xdf13	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:51.309034109 CET	8.8.8.8	192.168.2.3	0xce33	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:52.683711052 CET	8.8.8.8	192.168.2.3	0x94fc	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:01:55.283688068 CET	8.8.8.8	192.168.2.3	0x51e6	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:02:01.734879017 CET	8.8.8.8	192.168.2.3	0x5fc3	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:02:03.776787043 CET	8.8.8.8	192.168.2.3	0x1935	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:02:08.987667084 CET	8.8.8.8	192.168.2.3	0x2d3f	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:02:11.027297974 CET	8.8.8.8	192.168.2.3	0x4489	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 08:02:14.275495052 CET	8.8.8.8	192.168.2.3	0x4c3e	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	192.168.2.3	49731	104.16.154.36	80	C:\Users\user\AppData\Local\Temp\Pictures.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 07:59:54.235313892 CET	623	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Jan 14, 2021 07:59:54.284348965 CET	623	IN	HTTP/1.1 403 Forbidden Date: Thu, 14 Jan 2021 06:59:54 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=d6cdf8dda2a1ce45b2173b3d3a4bb7f411610607594; expires=Sat, 13-Feb-21 06:59:54 GMT; path=/; domain=.whatismyipaddress.com; HttpOnly; SameSite=Lax; Secure cf-request-id: 07a14aa31c0000c2e532b0b000000001 Server: cloudflare CF-RAY: 61157a182acec2e5-FRA 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	192.168.2.3	49733	131.186.161.70	80	C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 08:00:04.861777067 CET	677	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
Jan 14, 2021 08:00:05.010082960 CET	677	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	192.168.2.3	49737	131.186.161.70	80	C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 08:00:05.390219927 CET	678	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
Jan 14, 2021 08:00:05.539251089 CET	678	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	192.168.2.3	49740	131.186.161.70	80	C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 08:00:09.419497967 CET	686	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 08:00:09.567424059 CET	686	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	192.168.2.3	49741	131.186.161.70	80	C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 08:00:09.866982937 CET	693	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
Jan 14, 2021 08:00:10.014935970 CET	694	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 34 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.74</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49742	131.186.161.70	80	C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 08:00:10.329763889 CET	698	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
Jan 14, 2021 08:00:10.477866888 CET	698	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
Jan 14, 2021 08:00:08.930797100 CET	172.67.188.154	443	192.168.2.3	49739	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
Jan 14, 2021 08:00:08.906934023 CET	587	49738	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:08.907265902 CET	49738	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:09.102705956 CET	587	49738	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:09.105675936 CET	49738	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:09.295670986 CET	587	49738	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:22.958322048 CET	587	49744	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:22.958880901 CET	49744	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:22.959043026 CET	587	49745	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:22.959383965 CET	49745	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:23.149359941 CET	587	49744	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:23.149823904 CET	587	49745	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:23.443073988 CET	587	49746	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:23.445048094 CET	49746	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:23.446057081 CET	587	49747	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:23.446501017 CET	49747	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:23.635618925 CET	587	49746	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:23.637448072 CET	587	49747	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:23.638699055 CET	49747	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:23.828748941 CET	587	49747	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:24.110033989 CET	587	49748	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:24.110730886 CET	49748	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:24.300975084 CET	587	49748	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:24.301374912 CET	49748	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:24.435529947 CET	587	49749	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:24.435818911 CET	49749	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:24.491446972 CET	587	49748	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:24.626451969 CET	587	49749	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:24.626929998 CET	49749	587	192.168.2.3	199.193.7.228	STARTTLS

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 08:00:24.817307949 CET	587	49749	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:25.135715961 CET	587	49750	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:25.136117935 CET	49750	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:25.326111078 CET	587	49750	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:25.326412916 CET	49750	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:25.516190052 CET	587	49750	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:26.070705891 CET	587	49751	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:26.081401110 CET	49751	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:26.271816015 CET	587	49751	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:26.274288893 CET	49751	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:26.464620113 CET	587	49751	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:26.638529062 CET	587	49752	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:26.638777018 CET	49752	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:26.829519033 CET	587	49752	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:26.829797029 CET	49752	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:27.020015955 CET	587	49752	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:27.538213015 CET	587	49753	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:27.540309906 CET	49753	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:27.731218100 CET	587	49753	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:27.731501102 CET	49753	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:27.756948948 CET	587	49754	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:27.757746935 CET	49754	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:27.921510935 CET	587	49753	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:27.948188066 CET	587	49754	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:27.948502064 CET	49754	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:28.138797998 CET	587	49754	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:28.197808027 CET	587	49755	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:28.198223114 CET	49755	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:28.388714075 CET	587	49755	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:28.388906002 CET	49755	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:28.579099894 CET	587	49755	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:29.063112020 CET	587	49756	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:29.063569069 CET	49756	587	192.168.2.3	199.193.7.228	EHLO 181598

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 08:00:29.253979921 CET	587	49756	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:29.254336119 CET	49756	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:29.444499969 CET	587	49756	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:29.783775091 CET	587	49757	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:29.784033060 CET	49757	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:29.974598885 CET	587	49757	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:29.974828005 CET	49757	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:30.165138006 CET	587	49757	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:30.812020063 CET	587	49758	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:30.812251091 CET	49758	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:31.003150940 CET	587	49758	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:31.003526926 CET	49758	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:31.193689108 CET	587	49758	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:31.492677927 CET	587	49759	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:31.492913961 CET	49759	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:31.682878017 CET	587	49759	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:31.683123112 CET	49759	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:31.873045921 CET	587	49759	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:32.227066040 CET	587	49760	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:32.227708101 CET	49760	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:32.418627977 CET	587	49760	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:32.419456005 CET	49760	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:32.560264111 CET	587	49761	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:32.561613083 CET	49761	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:32.609837055 CET	587	49760	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:32.752177954 CET	587	49761	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:32.752501011 CET	49761	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:32.968230009 CET	587	49761	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:33.468945026 CET	587	49762	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:33.512440920 CET	49762	587	192.168.2.3	199.193.7.228	EHLO 181598

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 08:00:33.702641964 CET	587	49762	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:33.702919006 CET	49762	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:33.892878056 CET	587	49762	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:34.443994999 CET	587	49763	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:34.810471058 CET	49763	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:35.001105070 CET	587	49763	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:35.001420975 CET	49763	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:35.191286087 CET	587	49763	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:35.651307106 CET	587	49764	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:36.264903069 CET	49764	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:36.455297947 CET	587	49764	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:36.455629110 CET	49764	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:36.645940065 CET	587	49764	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:37.709633112 CET	587	49765	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:37.709914923 CET	49765	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:37.901084900 CET	587	49765	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:37.901420116 CET	49765	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:38.092577934 CET	587	49765	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:38.167083025 CET	587	49767	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:38.167381048 CET	49767	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:38.357604980 CET	587	49767	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:38.358040094 CET	49767	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:38.548203945 CET	587	49767	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:38.580416918 CET	587	49768	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:38.580915928 CET	49768	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:38.771435976 CET	587	49768	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:38.774426937 CET	49768	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:38.964509964 CET	587	49768	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:39.755696058 CET	587	49769	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:39.892252922 CET	49769	587	192.168.2.3	199.193.7.228	EHLO 181598

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 08:00:40.082479954 CET	587	49769	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:40.879084110 CET	49769	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:41.069070101 CET	587	49769	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:42.214993954 CET	587	49770	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:42.215277910 CET	49770	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:42.405487061 CET	587	49770	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:42.406028032 CET	49770	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:42.596146107 CET	587	49770	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:42.628251076 CET	587	49771	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:42.628550053 CET	49771	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:42.818723917 CET	587	49771	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:42.818973064 CET	49771	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:43.009176016 CET	587	49771	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:44.974253893 CET	587	49777	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:44.974579096 CET	49777	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:45.165414095 CET	587	49777	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:45.165735960 CET	49777	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:45.355920076 CET	587	49777	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:46.670711040 CET	587	49778	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:46.671047926 CET	49778	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:46.861597061 CET	587	49778	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:46.861906052 CET	49778	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:47.052179098 CET	587	49778	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:47.706816912 CET	587	49779	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:47.713439941 CET	49779	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:47.904191971 CET	587	49779	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:47.907737017 CET	49779	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:48.097883940 CET	587	49779	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:50.194633961 CET	587	49780	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:50.195271015 CET	49780	587	192.168.2.3	199.193.7.228	EHLO 181598

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 08:00:50.385718107 CET	587	49780	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:50.386029959 CET	49780	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:50.576061964 CET	587	49780	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:53.301513910 CET	587	49781	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:53.301795006 CET	49781	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:53.492562056 CET	587	49781	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:53.492883921 CET	49781	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:53.682801008 CET	587	49781	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:57.209950924 CET	587	49782	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:57.210242033 CET	49782	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:57.401289940 CET	587	49782	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:57.404664040 CET	49782	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:57.597613096 CET	587	49782	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:58.314656019 CET	587	49784	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:58.317277908 CET	49784	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:58.324326038 CET	587	49783	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:00:58.325126886 CET	49783	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:00:58.508018017 CET	587	49784	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:58.508310080 CET	49784	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:58.517420053 CET	587	49783	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:00:58.517796993 CET	49783	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:00:58.698154926 CET	587	49784	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:00:58.708192110 CET	587	49783	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:01.153760910 CET	587	49785	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:01.154012918 CET	49785	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:01.344062090 CET	587	49785	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:01.344387054 CET	49785	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:01.534154892 CET	587	49785	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:01.866694927 CET	587	49786	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:01.867805958 CET	49786	587	192.168.2.3	199.193.7.228	EHLO 181598

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 08:01:02.058806896 CET	587	49786	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:02.059304953 CET	49786	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:02.250293016 CET	587	49786	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:03.881658077 CET	587	49787	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:03.881896019 CET	49787	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:04.072146893 CET	587	49787	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:04.072447062 CET	49787	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:04.262357950 CET	587	49787	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:05.761015892 CET	587	49788	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:05.761476994 CET	49788	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:05.951705933 CET	587	49788	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:05.952223063 CET	49788	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:06.142236948 CET	587	49788	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:06.823236942 CET	587	49789	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:06.823589087 CET	49789	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:07.014662027 CET	587	49789	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:07.015180111 CET	49789	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:07.205461025 CET	587	49789	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:09.630564928 CET	587	49790	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:09.631012917 CET	49790	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:09.821367979 CET	587	49790	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:09.821949959 CET	49790	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:10.012123108 CET	587	49790	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:12.748764992 CET	587	49791	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:12.749078989 CET	49791	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:12.939315081 CET	587	49791	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:12.939600945 CET	49791	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:13.129544020 CET	587	49791	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:14.087682009 CET	587	49792	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:14.088027000 CET	49792	587	192.168.2.3	199.193.7.228	EHLO 181598

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 08:01:14.281205893 CET	587	49792	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:14.283047915 CET	49792	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:14.474591017 CET	587	49792	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:15.534230947 CET	587	49793	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:15.534540892 CET	49793	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:15.726432085 CET	587	49793	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:15.726715088 CET	49793	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:15.916903973 CET	587	49793	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:17.690021038 CET	587	49795	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:17.690251112 CET	49795	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:17.880609989 CET	587	49795	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:17.880868912 CET	49795	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:18.072803020 CET	587	49795	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:18.612931967 CET	587	49797	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:18.613706112 CET	49797	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:18.804374933 CET	587	49797	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:18.804801941 CET	49797	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:18.999006033 CET	587	49797	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:21.284363985 CET	587	49798	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:21.284882069 CET	49798	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:21.480458021 CET	587	49798	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:21.481062889 CET	49798	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:21.532888889 CET	587	49799	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:21.533421040 CET	49799	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:21.671130896 CET	587	49798	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:21.724421978 CET	587	49799	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:21.724963903 CET	49799	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:21.915255070 CET	587	49799	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:25.625089884 CET	587	49800	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:25.625545979 CET	49800	587	192.168.2.3	199.193.7.228	EHLO 181598

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 08:01:25.816255093 CET	587	49800	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:25.816869020 CET	49800	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:26.007025957 CET	587	49800	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:27.853097916 CET	587	49801	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:27.853763103 CET	49801	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:27.858159065 CET	587	49802	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:28.044333935 CET	587	49801	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:28.044605017 CET	49801	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:28.235030890 CET	587	49801	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:30.335285902 CET	587	49803	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:30.335592031 CET	49803	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:30.526629925 CET	587	49803	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:30.533440113 CET	49803	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:30.723768950 CET	587	49803	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:31.604931116 CET	49802	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:31.795408964 CET	587	49802	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:32.814342976 CET	49802	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:33.004206896 CET	587	49802	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:34.456821918 CET	587	49804	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:34.457135916 CET	49804	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:34.649202108 CET	587	49804	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:34.649521112 CET	49804	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:34.840384007 CET	587	49804	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:38.893692970 CET	587	49805	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:38.894042969 CET	49805	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:39.085583925 CET	587	49805	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:39.085908890 CET	49805	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:39.276056051 CET	587	49805	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:41.736498117 CET	587	49806	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:41.737001896 CET	49806	587	192.168.2.3	199.193.7.228	EHLO 181598

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 08:01:41.927407980 CET	587	49806	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:41.927922010 CET	49806	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:42.118094921 CET	587	49806	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:43.635668993 CET	587	49807	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:43.638381004 CET	49807	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:43.750307083 CET	587	49808	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:43.751010895 CET	49808	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:43.829294920 CET	587	49807	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:43.829917908 CET	49807	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:43.941509962 CET	587	49808	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:43.941972017 CET	49808	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:44.019892931 CET	587	49807	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:44.132210970 CET	587	49808	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:48.039824009 CET	587	49809	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:48.040148973 CET	49809	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:48.230098009 CET	587	49809	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:48.230492115 CET	49809	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:48.420342922 CET	587	49809	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:50.000015974 CET	587	49810	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:50.000456095 CET	49810	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:50.191111088 CET	587	49810	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:50.192306042 CET	49810	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:50.382050991 CET	587	49810	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:50.885778904 CET	587	49811	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:50.886068106 CET	49811	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:51.076761007 CET	587	49811	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:51.077038050 CET	49811	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:51.267127037 CET	587	49811	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:51.693038940 CET	587	49812	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:51.693440914 CET	49812	587	192.168.2.3	199.193.7.228	EHLO 181598

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 08:01:51.883703947 CET	587	49812	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:51.883953094 CET	49812	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:52.073928118 CET	587	49812	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:53.076587915 CET	587	49813	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:53.077069998 CET	49813	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:53.270800114 CET	587	49813	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:53.271234989 CET	49813	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:53.461445093 CET	587	49813	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:55.668385029 CET	587	49814	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:55.668708086 CET	49814	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:55.859302044 CET	587	49814	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:55.861972094 CET	49814	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:56.052262068 CET	587	49814	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:01:57.486742973 CET	587	49815	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:01:57.488416910 CET	49815	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:01:57.678283930 CET	587	49815	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:01:57.679305077 CET	49815	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:01:57.868951082 CET	587	49815	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:02:02.119780064 CET	587	49816	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:02:02.120094061 CET	49816	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:02:02.310462952 CET	587	49816	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:02:02.311018944 CET	49816	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:02:02.501113892 CET	587	49816	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:02:04.162039042 CET	587	49817	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:02:04.163682938 CET	49817	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:02:04.353744030 CET	587	49817	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:02:04.354710102 CET	49817	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:02:04.544641972 CET	587	49817	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:02:06.739955902 CET	587	49818	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:02:06.741179943 CET	49818	587	192.168.2.3	199.193.7.228	EHLO 181598

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 08:02:06.931835890 CET	587	49818	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:02:06.932323933 CET	49818	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:02:07.122363091 CET	587	49818	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:02:09.375710011 CET	587	49823	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:02:09.376919985 CET	49823	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:02:09.568360090 CET	587	49823	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:02:09.572520018 CET	49823	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:02:09.762430906 CET	587	49823	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:02:11.413281918 CET	587	49827	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:02:11.413774014 CET	49827	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:02:11.604326963 CET	587	49827	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:02:11.605890036 CET	49827	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:02:11.795685053 CET	587	49827	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:02:14.680536032 CET	587	49831	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:02:14.682537079 CET	49831	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:02:14.873294115 CET	587	49831	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:02:14.905807018 CET	49831	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:02:15.096021891 CET	587	49831	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:02:17.745964050 CET	587	49832	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:02:17.746226072 CET	49832	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:02:17.936898947 CET	587	49832	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:02:17.937329054 CET	49832	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:02:18.127619982 CET	587	49832	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:02:23.349724054 CET	587	49833	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:02:23.352009058 CET	49833	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:02:23.542123079 CET	587	49833	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:02:23.543831110 CET	49833	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:02:23.733742952 CET	587	49833	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:02:23.791246891 CET	587	49834	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:02:23.791553974 CET	49834	587	192.168.2.3	199.193.7.228	EHLO 181598

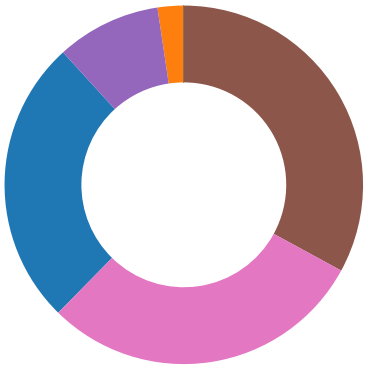
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 08:02:23.981687069 CET	587	49834	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:02:23.981918097 CET	49834	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:02:24.171911001 CET	587	49834	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:02:25.909921885 CET	587	49835	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:02:25.910132885 CET	49835	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:02:26.100660086 CET	587	49835	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:02:26.100920916 CET	49835	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:02:26.291158915 CET	587	49835	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:02:27.035151958 CET	587	49836	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:02:27.035372972 CET	49836	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:02:27.228023052 CET	587	49836	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:02:27.228200912 CET	49836	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:02:27.418167114 CET	587	49836	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 08:02:28.561914921 CET	587	49837	199.193.7.228	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jan 14, 2021 08:02:28.564661980 CET	49837	587	192.168.2.3	199.193.7.228	EHLO 181598
Jan 14, 2021 08:02:28.756741047 CET	587	49837	199.193.7.228	192.168.2.3	250-mta-12.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 08:02:28.757129908 CET	49837	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 08:02:28.947220087 CET	587	49837	199.193.7.228	192.168.2.3	220 Ready to start TLS

Code Manipulations

Statistics

Behavior

- B6LNCKjOGt5EmFQ.exe
- schtasks.exe
- conhost.exe
- B6LNCKjOGt5EmFQ.exe
- B6LNCKjOGt5EmFQ.exe
- LOGO AND PICTURES.exe
- Pictures.exe
- PO456724392021.exe
- PO2345714382021.exe
- dw20.exe
- vbc.exe
- vbc.exe
- netsh.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: B6LNCKjOGt5EmFQ.exe PID: 6076 Parent PID: 5672

General

Start time:	08:00:10
Start date:	14/01/2021
Path:	C:\Users\user\Desktop\B6LNCKjOGt5EmFQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\B6LNCKjOGt5EmFQ.exe'
Imagebase:	0xfe0000
File size:	1891328 bytes
MD5 hash:	80D255A6A5EC339E15D6FEC3C0FEF666
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.280603529.000000000369E000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.293576161.0000000004C48000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000000.00000002.293576161.0000000004C48000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.293576161.0000000004C48000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.293576161.0000000004C48000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.293576161.0000000004C48000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.293576161.0000000004C48000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	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	6DEECF06	unknown
C:\Users\user\AppData\Roaming\TcVfsyyjYuQ.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpDAC4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD37038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\B6LNCKjOGt5EmFQ.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDAC4.tmp	success or wait	1	6CD36A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\TcVfsyyjYuQ.exe	unknown	1891328	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 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 ad 92 ff 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 d0 1c 00 00 0a 00 00 00 00 00 00 de ee 1c 00 00 20 00 00 00 00 1d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 1d 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	6CD31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDAC4.tmp	unknown	1644	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CD31B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\B6LNCKjOGt5EmFQ.exe.log	unknown	1216	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	6E1FC907	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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Users\user\Desktop\B6LNCKjOGt5EmFQ.exe	unknown	1891328	success or wait	1	6CD31B4F	ReadFile

Analysis Process: schtasks.exe PID: 4812 Parent PID: 6076

General

Start time:	08:00:35
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TcVfsyyjYuQ' /XML 'C:\Users\user\AppData\Local\Temp\tmpDAC4.tmp'
Imagebase:	0x1380000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDAC4.tmp	unknown	2	success or wait	1	138AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpDAC4.tmp	unknown	1645	success or wait	1	138ABD9	ReadFile

Analysis Process: conhost.exe PID: 5352 Parent PID: 4812

General

Start time:	08:00:36
Start date:	14/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: B6LNCKjOGt5EmFQ.exe PID: 5640 Parent PID: 6076

General

Start time:	08:00:36
Start date:	14/01/2021
Path:	C:\Users\user\Desktop\B6LNCKjOGt5EmFQ.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x510000
File size:	1891328 bytes
MD5 hash:	80D255A6A5EC339E15D6FEC3C0FEF666
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: B6LNCKjOGt5EmFQ.exe PID: 5336 Parent PID: 6076

General

Start time:	08:00:37
Start date:	14/01/2021
Path:	C:\Users\user\Desktop\B6LNCKjOGt5EmFQ.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7ff7ca4e0000
File size:	1891328 bytes
MD5 hash:	80D255A6A5EC339E15D6FEC3C0FEF666
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000003.291239624.0000000004451000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000003.283351079.000000000134C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000003.281411863.0000000004450000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000003.281411863.0000000004450000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000003.289168879.0000000003E3C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000003.287788541.00000000044BD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000003.278201176.000000000138F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000003.285048922.0000000004451000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000008.00000003.277852049.0000000003760000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000008.00000003.277852049.0000000003760000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000003.277852049.0000000003760000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000008.00000003.277852049.0000000003760000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000003.277852049.0000000003760000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000008.00000003.277852049.0000000003760000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000003.278060140.0000000001324000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000003.287852153.0000000003DD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000003.286730546.00000000044BD000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000008.00000002.298778649.0000000000403000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000008.00000002.298778649.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.298778649.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000008.00000002.298778649.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.298778649.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000008.00000002.298778649.0000000000403000.00000040.00000001.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\AppData\Local\Temp\LOGO AND PICTURES.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	660ED258	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Pictures.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\AppData\Local\Temp\PO456724392021.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\AppData\Local\Temp\PO2345714382021.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\LOGO AND PICTURES.exe	unknown	456192	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 1c c9 fd 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 ea 06 00 00 0a 00 00 00 00 00 00 ee 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 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 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\Pictures.exe	unknown	533504	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 34 ac d0 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 ee 07 00 00 34 00 00 00 00 00 00 0e 0c 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.._.......... ....4........... ....@.. ....@................	success or wait	1	660ED8F8	WriteFile
C:\Users\user\AppData\Local\Temp\PO456724392021.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 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 c5 c6 fd 5f 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 2e 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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\PO2345714382021.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 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 79 c6 fd 5f 00 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 0e 75 03 00 00 20 00 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 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 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...y.._.......... ....V...........u... ....@.. ....@................	success or wait	1	660ED8F8	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: LOGO AND PICTURES.exe PID: 6208 Parent PID: 5336

General

Start time:	08:00:39
Start date:	14/01/2021
Path:	C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe' 0
Imagebase:	0xdb0000
File size:	456192 bytes
MD5 hash:	D9001138C5119D936B70BF77E136AFBE
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: 00000009.00000002.611843586.00000000032C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.611843586.00000000032C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000009.00000002.604546258.0000000000DB2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000009.00000000.281199501.0000000000DB2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
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	6DEECF06	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	6DEECF06	unknown
C:\Users\user\Documents\Matiex Keylogger	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	6	6CD3BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\container.dat	success or wait	1	6CD36A95	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	success or wait	1	6CD36A95	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	success or wait	1	6CD36A95	DeleteFileW
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	success or wait	1	6CD36A95	DeleteFileW
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	success or wait	4	6CD36A95	DeleteFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD31B4F	ReadFile
unknown	unknown	4096	success or wait	2	6CD31B4F	ReadFile
unknown	unknown	4096	pipe broken	1	6CD31B4F	ReadFile
unknown	unknown	4096	pipe broken	1	6CD31B4F	ReadFile
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	unknown	17408	success or wait	49	6CD31B4F	ReadFile
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	unknown	17408	end of file	1	6CD31B4F	ReadFile
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	unknown	17408	success or wait	244	6CD31B4F	ReadFile
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	unknown	17408	end of file	5	6CD31B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: Pictures.exe PID: 6240 Parent PID: 5336

General

Start time:	08:00:40
Start date:	14/01/2021
Path:	C:\Users\user\AppData\Local\Temp\Pictures.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\Pictures.exe' 0
Imagebase:	0x150000
File size:	533504 bytes
MD5 hash:	25146E9C5ECD498DD17BA01E6CFAEB24
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: 0000000A.00000002.329671193.0000000003921000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000A.00000002.329671193.0000000003921000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000A.00000002.323788934.0000000000152000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000A.00000002.323788934.0000000000152000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000A.00000002.323788934.0000000000152000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000A.00000002.323788934.0000000000152000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000A.00000002.323788934.0000000000152000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000A.00000000.282912644.0000000000152000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000A.00000000.282912644.0000000000152000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000A.00000000.282912644.0000000000152000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000A.00000000.282912644.0000000000152000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000A.00000000.282912644.0000000000152000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000A.00000002.327595878.000000000295F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000A.00000002.327595878.000000000295F000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Local\Temp\Pictures.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Local\Temp\Pictures.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Local\Temp\Pictures.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Local\Temp\Pictures.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Local\Temp\Pictures.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

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	72FB60AC	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	72FB60AC	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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Roaming\pid.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	725CB31E	unknown
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	725CB31E	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	4A2573A	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	4A2573A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	36 32 34 30	6240	success or wait	1	4A20093	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	46	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 50 69 63 74 75 72 65 73 2e 65 78 65	C:\Users\user\AppData\Local\Temp\Pictures.exe	success or wait	1	4A20093	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	4A20093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4A20093	ReadFile
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	4A20093	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	4A20093	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	4A20093	ReadFile
C:\Users\user\AppData\Local\Temp\Pictures.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Users\user\AppData\Local\Temp\Pictures.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	dword	2	1	success or wait	1	4A24A02	RegSetValueExW

Analysis Process: PO456724392021.exe PID: 6292 Parent PID: 5336

General

Start time:	08:00:41
Start date:	14/01/2021
Path:	C:\Users\user\AppData\Local\Temp\PO456724392021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\PO456724392021.exe' 0
Imagebase:	0xab0000
File size:	221696 bytes
MD5 hash:	F38E2D474C075EFF35B4EF81FDACA650
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: 0000000C.00000000.284660390.0000000000AB2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.612763581.0000000002D81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.612763581.0000000002D81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.604664953.0000000000AB2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.612958072.0000000002DD2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.612958072.0000000002DD2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\PO456724392021.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: PO2345714382021.exe PID: 6488 Parent PID: 5336

General

Start time:	08:00:42
Start date:	14/01/2021
Path:	C:\Users\user\AppData\Local\Temp\PO2345714382021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\PO2345714382021.exe' 0
Imagebase:	0x5d0000
File size:	220672 bytes
MD5 hash:	9B79DE8E3AD21F14E71E55CFA6AE4727
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: 00000010.00000000.287649744.00000000005D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\PO2345714382021.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: dw20.exe PID: 6740 Parent PID: 6240

General

Start time:	08:00:45
Start date:	14/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2184
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: 6836 Parent PID: 6240

General

Start time:	08:00:48
Start date:	14/01/2021
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: 00000013.00000002.301913637.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 6848 Parent PID: 6240

General

Start time:	08:00:48
Start date:	14/01/2021
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: 00000014.00000002.308380033.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: netsh.exe PID: 6184 Parent PID: 6208

General

Start time:	08:01:13
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	'netsh' wlan show profile
Imagebase:	0xcb0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6168 Parent PID: 6184

General

Start time:	08:01:14
Start date:	14/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis