ID: 339931
Sample Name:
hkaP5RPCGNDVq3Z.exe
Cookbook: default.jbs
Time: 21:04:39
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

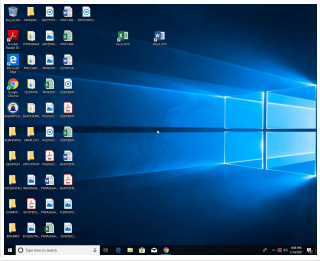
Analysis Report hkaP5RPCGNDVq3Z.exe

Overview

General Information

Sample Name:	hkaP5RPCGNDVq3Z.exe
Analysis ID:	339931
MD5:	07556e1af1f43f7…
SHA1:	42110c04869726..
SHA256:	a6fc5cc4331ee5a..
Tags:	exe HawkEye

Most interesting Screenshot:



Detection

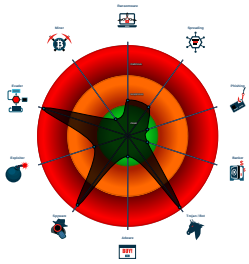
HawkEye AgentTesla MailPassView Matiex

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 …
- 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
- .NET source code contains potentia…
- .NET source code references suspic…

Classification



Startup

- **System is w10x64**
- hkaP5RPCGNDVq3Z.exe (PID: 5552 cmdline: 'C:\Users\user\Desktop\hkaP5RPCGNDVq3Z.exe' MD5: 07556E1AF1F43F7DD42D32D188187E4A)
  - schtasks.exe (PID: 1560 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\jcKKBKdU' /XML 'C:\Users\user\AppData\Local\Temp\tmpEED.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - hkaP5RPCGNDVq3Z.exe (PID: 5908 cmdline: {path} MD5: 07556E1AF1F43F7DD42D32D188187E4A)
    - LOGO AND PICTURES.exe (PID: 5872 cmdline: 'C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe' 0 MD5: D9001138C5119D936B70BF77E136AFBE)
      - netsh.exe (PID: 6400 cmdline: 'netsh' wlan show profile MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - conhost.exe (PID: 6396 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - Pictures.exe (PID: 5868 cmdline: 'C:\Users\user\AppData\Local\Temp\Pictures.exe' 0 MD5: 25146E9C5ECD498DD17BA01E6CFAEB24)
        - dw20.exe (PID: 6348 cmdline: dw20.exe -x -s 2100 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
      - PO456724392021.exe (PID: 2208 cmdline: 'C:\Users\user\AppData\Local\Temp\PO456724392021.exe' 0 MD5: F38E2D474C075EFF35B4EF81FDACA650)
      - PO2345714382021.exe (PID: 5880 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: ": "VjouxsS",
  "URL: ": "http://YfWA3aJjc76ztEimE.com",
  "To: ": "sales01@seedwellresources.xyz",
  "ByHost: ": "smtp.privateemail.com:5876",
  "Password: ": "Nd6zB",
  "From: ": "sales01@seedwellresources.xyz"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
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	
C:\Users\user\AppData\Local\Temp\Pictures.exe	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	

Click to see the 2 entries

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.622096299.000000000330 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.622096299.000000000330 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000007.00000002.275743859.000000000047 2000.00000002.00020000.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b6f7:$key: HawkEyeKeylogger • 0x7d93b:$salt: 099u787978786 • 0x7bd38:$string1: HawkEye_Keylogger • 0x7cb8b:$string1: HawkEye_Keylogger • 0x7d89b:$string1: HawkEye_Keylogger • 0x7c121:$string2: holdermail.txt • 0x7c141:$string2: holdermail.txt • 0x7c063:$string3: wallet.dat • 0x7c07b:$string3: wallet.dat • 0x7c091:$string3: wallet.dat • 0x7d45f:$string4: Keylog Records • 0x7d777:$string4: Keylog Records • 0x7d993:$string5: do not script --> • 0x7b6df:$string6: \pidloc.txt • 0x7b76d:$string7: BSPLIT • 0x7b77d:$string7: BSPLIT
00000007.00000002.275743859.000000000047 2000.00000002.00020000.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000007.00000002.275743859.000000000047 2000.00000002.00020000.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	

Click to see the 56 entries

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
8.0.PO456724392021.exe.e90000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.2.PO456724392021.exe.e90000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.0.PO2345714382021.exe.a0000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.0.Pictures.exe.470000.0.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
7.0.Pictures.exe.470000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 15 entries				

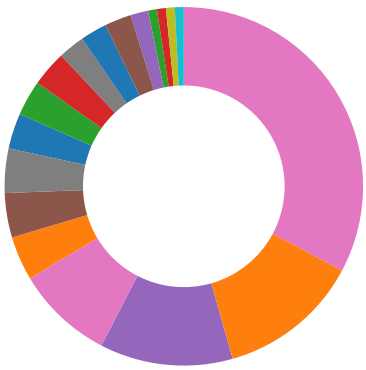
Sigma Overview

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

Machine Learning detection for dropped file

Networking:

C2 URLs / IPs found in malware configuration

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)

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

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected HawkEye Keylogger

Yara detected MailPassView

Yara detected Matiex Keylogger

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

Tries to harvest and steal WLAN passwords

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Detected HawkEye Rat

Yara detected AgentTesla

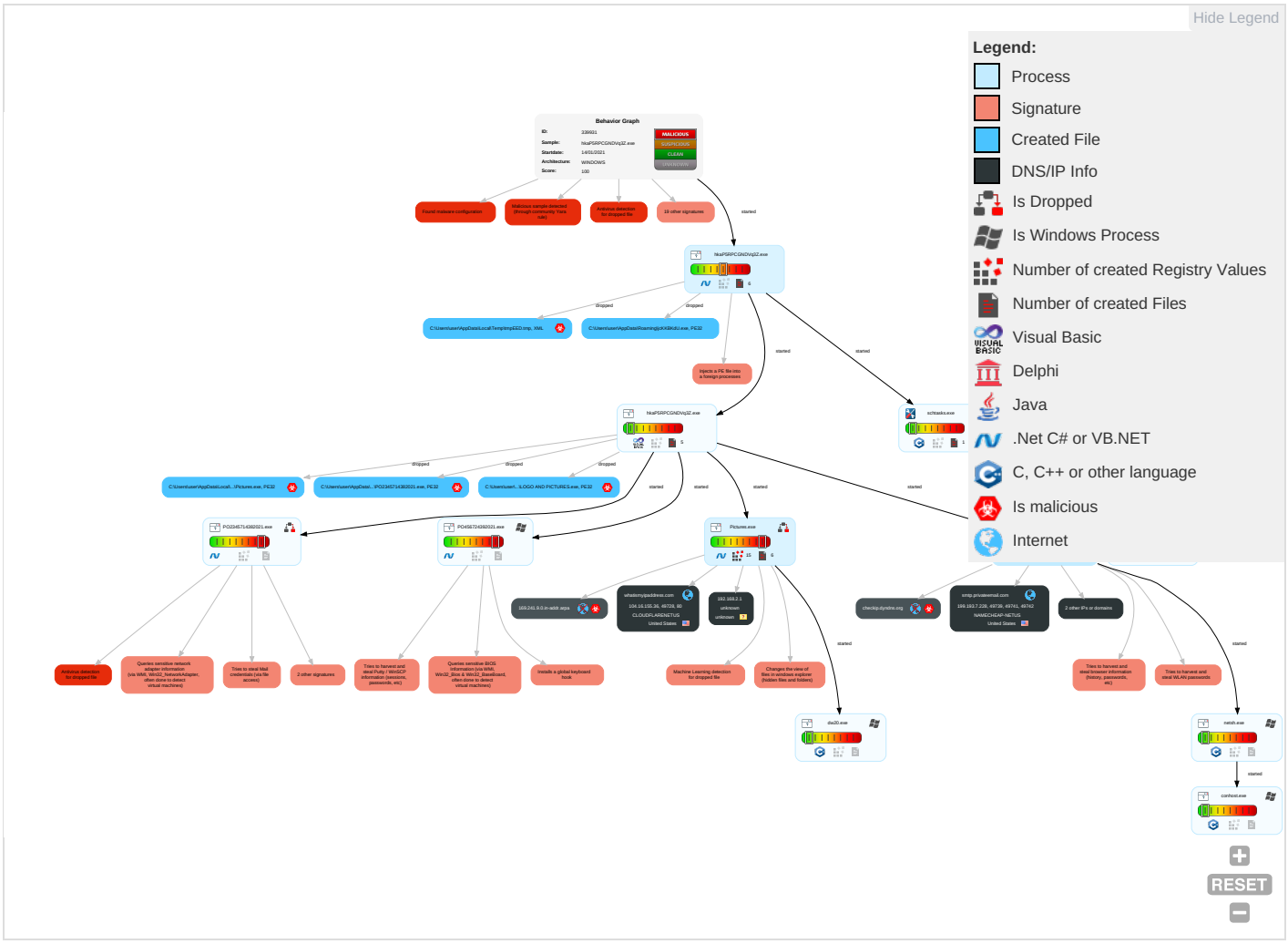
Yara detected HawkEye Keylogger

Yara detected Matiex Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Replication Through Removable Media 1	Windows Management Instrumentation 2 3 1	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 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	Scheduled Task/Job 1	Logon Script (Windows)	Process Injection 1 1 2	Obfuscated Files or Information 4 1	Credentials in Registry 1	System Information Discovery 1 2 5	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltr
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1 3	NTDS	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 2 6 1	SSH	Clipboard Data 1	Data Transfer Siz Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 6	VNC	GUI Input Capture	Exfiltration Over Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 6	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protoc
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 1 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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
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\PO2345714382021.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Pictures.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\PO2345714382021.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.Pictures.exe.470000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
7.0.Pictures.exe.470000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
8.0.PO456724392021.exe.e90000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
7.2.Pictures.exe.470000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.Pictures.exe.470000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
3.2.hkaP5RPCGNDVq3Z.exe.400000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
3.2.hkaP5RPCGNDVq3Z.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
3.2.hkaP5RPCGNDVq3Z.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
3.2.hkaP5RPCGNDVq3Z.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.LOGO AND PICTURES.exe.880000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
8.2.PO456724392021.exe.e90000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
9.0.PO2345714382021.exe.a0000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
freegeoip.app	1%	Virustotal		Browse
checkip.dyndns.com	0%	Virustotal		Browse
169.241.9.0.in-addr.arpa	0%	Virustotal		Browse
checkip.dyndns.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://YGApDP.com	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://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.co	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://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://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.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://ocsp.sect	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	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://YfWA3aJjc76ztEimE.com	0%	Avira URL Cloud	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://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	104.16.155.36	true	false		high
freegeoip.app	104.21.19.200	true	false	• 1%, Virustotal, Browse	unknown
smtp.privateemail.com	199.193.7.228	true	false		high
checkip.dyndns.com	162.88.193.70	true	false	• 0%, Virustotal, Browse	unknown
169.241.9.0.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

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

Name	Malicious	Antivirus Detection	Reputation
http://whatismyipaddress.com/	false		high
http://YfWA3aJjc76ztEimE.com	true	• Avira URL Cloud: safe	unknown

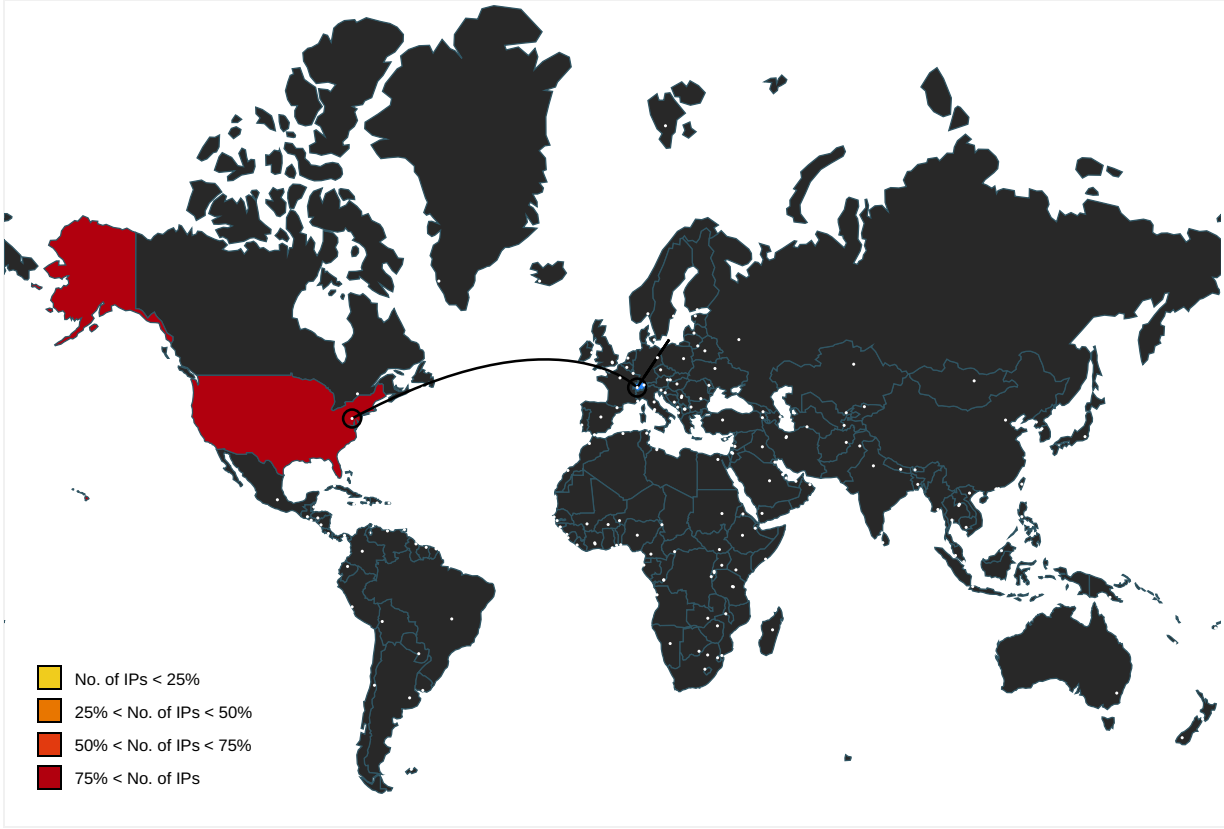
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	PO456724392021.exe, 00000008.00000002.622096299.0000000003301000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://YGApDP.com	PO456724392021.exe, 00000008.00000002.622096299.0000000003301000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	LOGO AND PICTURES.exe, 00000006.00000003.367676497.0000000006550000.00000004.00000001.sdmp, PO456724392021.exe, 00000008.00000002.627273721.0000000065E3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false		high
http://www.tiro.com	Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false		high
http://ns.adobe.c/g	LOGO AND PICTURES.exe, 00000006.00000003.432984410.0000000008D31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.co	LOGO AND PICTURES.exe, 00000006.00000003.367655934.00000000065A3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com/-	hkaP5RPCGNDVq3Z.exe, 00000003.00000002.264651152.0000000000403000.00000040.00000001.sdmp, Pictures.exe, 00000007.00000002.275743859.0000000000472000.00000002.00020000.sdmp, Pictures.exe.3.dr	false		high
http://www.galapagosdesign.com/DPlease	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	PO456724392021.exe, 00000008.00000002.622096299.0000000033301000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://login.yahoo.com/config/login	Pictures.exe	false		high
http://www.fonts.com	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.site.com/logs.php	Pictures.exe, 00000007.00000002.278199316.0000000002C23000.00000004.00000001.sdmp	false		high
http://www.urwpp.deDPlease	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	Pictures.exe.3.dr	false		high
http://www.zhongyicts.com.cn	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.257858765.0000000002C41000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.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	hkaP5RPCGNDVq3Z.exe, 00000003.00000003.263995429.0000000003AEC000.00000004.00000001.sdmp, PO456724392021.exe, PO2345714382021.exe, 00000009.00000000.263166408.00000000000A2000.00000002.00020000.sdmp, PO2345714382021.exe.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	LOGO AND PICTURES.exe, 00000006.00000003.367676497.0000000006550000.00000004.00000001.sdmp, PO456724392021.exe, 00000008.00000002.627273721.00000000065E3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	PO456724392021.exe, 00000008.00000002.622096299.0000000003301000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	LOGO AND PICTURES.exe, 00000006.00000003.367676497.0000000006550000.00000004.00000001.sdmp, PO456724392021.exe, 00000008.00000002.627273721.0000000065E3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobj	LOGO AND PICTURES.exe, 00000006.00000003.432984410.0000000008D31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	PO456724392021.exe, 00000008.00000002.622096299.0000000003301000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sect	LOGO AND PICTURES.exe, 00000006.00000003.367705732.0000000006656E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com	Pictures.exe, 00000007.00000002.277841679.0000000002BDD000.00000004.00000001.sdmp	false		high
http://smtp.privateemail.com	PO456724392021.exe, 00000008.00000002.624703526.00000000035F5000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%$	PO456724392021.exe, 00000008.00000002.622096299.0000000003301000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	hkaP5RPCGNDVq3Z.exe, 00000000.00000002.276769899.0000000006C52000.00000004.00000001.sdmp, Pictures.exe, 00000007.00000002.281614834.0000000005360000.00000002.00000001.sdmp	false		high
http://ns.ado/1	LOGO AND PICTURES.exe, 00000006.00000003.432984410.0000000008D31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339931
Start date:	14.01.2021
Start time:	21:04:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	hkaP5RPCGNDVq3Z.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@19/12@38/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1% (good quality ratio 0.3%) • Quality average: 22.3% • Quality standard deviation: 28.7%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.43.193.48, 168.61.161.212, 23.210.248.85, 51.104.144.132, 8.241.122.126, 8.241.89.254, 8.238.27.126, 92.122.213.194, 92.122.213.247, 20.54.26.129, 51.11.168.160, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, blobcollector.events.data.trafficmanager.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, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:05:36	API Interceptor	2x Sleep call for process: hkaP5RPCGNDVq3Z.exe modified
21:05:57	API Interceptor	3x Sleep call for process: Pictures.exe modified

Time	Type	Description
21:06:00	API Interceptor	1x Sleep call for process: dw20.exe modified
21:06:02	API Interceptor	325x Sleep call for process: PO2345714382021.exe modified
21:06:07	API Interceptor	927x Sleep call for process: PO456724392021.exe modified
21:06:11	API Interceptor	1077x Sleep call for process: LOGO AND PICTURES.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.155.36	NDt93WWQwd089H7.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	INQUIRY.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Prueba de pago.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	6JLHKYvboo.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	jSMd8npgmU.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	9vdouqRTh3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	5pB35gGfZ5.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	fyxC4Hgs3s.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	yk94P18VKp.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	oLHQIQAI3N.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	WuGzF7ZJ7P.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NXmokFkh3R.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	qiGQsdRM57.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NSSPH41vE5.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	2v7Vtqfo81.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	355OckuTD3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
freegeoip.app	Scan document.exe	Get hash	malicious	Browse	• 104.21.19.200
	H56qL3lu0k.exe	Get hash	malicious	Browse	• 104.21.19.200
	pfyoq7q31V.exe	Get hash	malicious	Browse	• 104.21.19.200
	UthdssT6pm.exe	Get hash	malicious	Browse	• 104.21.19.200
	PI0jYjw6X2.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.PackedNET.505.30555.exe	Get hash	malicious	Browse	• 172.67.188.154
	B6LNCKjOGt5EmFQ.exe	Get hash	malicious	Browse	• 172.67.188.154
	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
	80Iki3DsHA.exe	Get hash	malicious	Browse	• 172.67.188.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
whatismyipaddress.com	B6LNCKjOGt5EmFQ.exe	Get hash	malicious	Browse	• 104.16.154.36
	NDt93WWQwd089H7.exe	Get hash	malicious	Browse	• 104.16.155.36
	JkhR5oeRHA.exe	Get hash	malicious	Browse	• 66.171.248.178
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 104.16.155.36
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• 104.16.154.36
	INQUIRY.exe	Get hash	malicious	Browse	• 104.16.154.36
	Prueba de pago.exe	Get hash	malicious	Browse	• 104.16.155.36
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	http://https://my-alliances.co.uk/	Get hash	malicious	Browse	• 66.171.248.178
	c9o0CtTIYT.exe	Get hash	malicious	Browse	• 104.16.154.36
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• 104.16.155.36
	6JLHKYvboo.exe	Get hash	malicious	Browse	• 104.16.155.36
	jSMd8npgmU.exe	Get hash	malicious	Browse	• 104.16.155.36
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	G4Q6P4rcer.exe	Get hash	malicious	Browse	• 23.227.38.74
	MBCBeDON27.exe	Get hash	malicious	Browse	• 23.227.38.74
	ouyPcSPwll.exe	Get hash	malicious	Browse	• 23.227.38.74
	fatHvt8YhT.exe	Get hash	malicious	Browse	• 104.27.160.102
	Scan document.exe	Get hash	malicious	Browse	• 104.21.19.200
	H56qL3lu0k.exe	Get hash	malicious	Browse	• 104.21.19.200
	pfyoq7q31V.exe	Get hash	malicious	Browse	• 104.21.19.200
	ACH PAYMENT REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 104.20.185.68
	UthdssT6pm.exe	Get hash	malicious	Browse	• 104.21.19.200
	PI0jYjw6X2.exe	Get hash	malicious	Browse	• 104.21.19.200
	Voicemail wav.html	Get hash	malicious	Browse	• 104.16.18.94
	t1XJOlYvhExZyrm.exe	Get hash	malicious	Browse	• 23.227.38.74
	937 2912 2020 2_90961070.doc	Get hash	malicious	Browse	• 172.67.162.234
	equinix-customer-portal.apk	Get hash	malicious	Browse	• 104.22.11.83
	PRS TT copy_pdf.exe	Get hash	malicious	Browse	• 66.235.200.3
	Archivo_2020.doc	Get hash	malicious	Browse	• 172.67.162.234
	SecuriteInfo.com.Trojan.PackedNET.505.30555.exe	Get hash	malicious	Browse	• 172.67.188.154
	Copy_#_824.xls	Get hash	malicious	Browse	• 172.67.189.45
	DHL e-invoice.exe	Get hash	malicious	Browse	• 172.67.177.142
	Copy_#_824.xls	Get hash	malicious	Browse	• 172.67.189.45
CLOUDFLARENETUS	G4Q6P4rcer.exe	Get hash	malicious	Browse	• 23.227.38.74
	MBCBeDON27.exe	Get hash	malicious	Browse	• 23.227.38.74
	ouyPcSPwll.exe	Get hash	malicious	Browse	• 23.227.38.74
	fatHvt8YhT.exe	Get hash	malicious	Browse	• 104.27.160.102
	Scan document.exe	Get hash	malicious	Browse	• 104.21.19.200
	H56qL3lu0k.exe	Get hash	malicious	Browse	• 104.21.19.200
	pfyoq7q31V.exe	Get hash	malicious	Browse	• 104.21.19.200
	ACH PAYMENT REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 104.20.185.68
	UthdssT6pm.exe	Get hash	malicious	Browse	• 104.21.19.200
	PI0jYjw6X2.exe	Get hash	malicious	Browse	• 104.21.19.200

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Voicemail wav.html	Get hash	malicious	Browse	• 104.16.18.94
	t1XJOlYvhExZyrm.exe	Get hash	malicious	Browse	• 23.227.38.74
	937 2912 2020 2_90961070.doc	Get hash	malicious	Browse	• 172.67.162.234
	equinix-customer-portal.apk	Get hash	malicious	Browse	• 104.22.11.83
	PRS TT copy_pdf.exe	Get hash	malicious	Browse	• 66.235.200.3
	Archivo_2020.doc	Get hash	malicious	Browse	• 172.67.162.234
	SecuriteInfo.com.Trojan.PackedNET.505.30555.exe	Get hash	malicious	Browse	• 172.67.188.154
	Copy_#_824.xls	Get hash	malicious	Browse	• 172.67.189.45
	DHL e-invoice.exe	Get hash	malicious	Browse	• 172.67.177.142
	Copy_#_824.xls	Get hash	malicious	Browse	• 172.67.189.45
DYNDNSUS	j2MLUi56gM.exe	Get hash	malicious	Browse	• 131.186.113.70
	Scan document.exe	Get hash	malicious	Browse	• 131.186.113.70
	H56qL3lu0k.exe	Get hash	malicious	Browse	• 216.146.43.71
	pfyoq7q31V.exe	Get hash	malicious	Browse	• 216.146.43.71
	UthdssT6pm.exe	Get hash	malicious	Browse	• 216.146.43.71
	PI0jYjw6X2.exe	Get hash	malicious	Browse	• 216.146.43.71
	SecuriteInfo.com.Trojan.PackedNET.505.30555.exe	Get hash	malicious	Browse	• 131.186.113.70
	B6LNCKjOGt5EmFQ.exe	Get hash	malicious	Browse	• 131.186.161.70
	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
	80lki3DsHA.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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	j2MLUi56gM.exe	Get hash	malicious	Browse	• 104.21.19.200
	Scan document.exe	Get hash	malicious	Browse	• 104.21.19.200
	H56qL3lu0k.exe	Get hash	malicious	Browse	• 104.21.19.200
	pfyoq7q31V.exe	Get hash	malicious	Browse	• 104.21.19.200
	UthdssT6pm.exe	Get hash	malicious	Browse	• 104.21.19.200
	PI0jYjw6X2.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.PackedNET.505.30555.exe	Get hash	malicious	Browse	• 104.21.19.200
	B6LNCKjOGt5EmFQ.exe	Get hash	malicious	Browse	• 104.21.19.200
	a5T7dTsG4U.exe	Get hash	malicious	Browse	• 104.21.19.200
	NKP210102-NIT-SC2.exe	Get hash	malicious	Browse	• 104.21.19.200
	80lki3DsHA.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.GenericKD.36094879.31571.exe	Get hash	malicious	Browse	• 104.21.19.200
	QPR-1064.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_2021_01_13_1_RFQ_PO_1832938.exe	Get hash	malicious	Browse	• 104.21.19.200
	aNmkT4KLJX.exe	Get hash	malicious	Browse	• 104.21.19.200
	090000000000000h.exe	Get hash	malicious	Browse	• 104.21.19.200
	PO-5042.exe	Get hash	malicious	Browse	• 104.21.19.200
	Geno_Quotation,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	onYLLDPXswyCVZu.exe	Get hash	malicious	Browse	• 104.21.19.200
	PO-75013.exe	Get hash	malicious	Browse	• 104.21.19.200

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe	B6LNCKjOGt5EmFQ.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\Pictures.exe	B6LNCKjOGt5EmFQ.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\PO2345714382021.exe	B6LNCKjOGt5EmFQ.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_pictures.exe_c756fdb369d16caee6eb4c4fc55eace42746ab1_00000000_18aec46c\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):	16928
Entropy (8bit):	3.753019809959852
Encrypted:	false
SSDEEP:	192:6/wSaMVvaKsn9fbeN9M2v1zzvSXk0ZKjBIcQry/u7sJS274ItD:CwSjaEdvh/sy/u7sJX4ItD
MD5:	E233678BD09FFCBC57BBFF192C4B065F
SHA1:	6EF6152294B9A1E82717DF8C20424651D446AA3F
SHA-256:	82D18EC26116FD9ECB7FB03A8FC744210A39FCC5F8036070BA2BECF26DB1274D
SHA-512:	19F8973FD7D4E86F26DC5662E49C0EAD7DE7BEB091297B9C680E4408E4C0631C75FBDDA6BA8541BF91F210DAF5CC4DE9BDF4E9B254035AAC814EA011519203 2
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.=.1.3.2.5.5.1.6.0.7.5.8.6.1.8.1.9.7.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m. e.=.1.3.2.5.5.1.6.0.7.5.9.0.2.4.4.4.8.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.e.7.2.3.9.2.1.-.5.c.5.c.-.4.0.6.a.-.b.e.6.4.-.5.4.2.a.1.c.3.7. e.3.c.0.....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.=.0.0.0.0.1.6.e.c.-.0.0.0. 1.-.0.0.1.7.-.1.0.2.3.-.7.b.1.9.f.c.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\WERBD58.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):	7614
Entropy (8bit):	3.689808400173829
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNitb6I6YBww69ZgmfZ61SNCp1j51fyhm:RrlsNih6I6YBH69ZgmfQ1S0jbf9
MD5:	4F937BBAEC18565798C00DFF15DA3B14
SHA1:	0FD02011DF2044F794562CC1BF42C4744FCC7D54
SHA-256:	225C6EF471967C7C2395DD52C976AE40E7889B6969E1C2D3E44BA02D2CCA25D1
SHA-512:	A94446C89F9D793843EF981AB0120CDC8D3FDD96456A47649C5F751D02DDB2C5DFAE863278B5F4E01AA8B25BAD4C9906657BB127D3F8F981A81F1E1CE00C32 D
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.>.5.8.6.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE53.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4674
Entropy (8bit):	4.439990671486078
Encrypted:	false
SSDEEP:	48:cvIwSD8zs4BJgtWI97zWSC8B+WK8fm8M4JFKC5Flo+q8v1o/xrvVgd:ulTfEQCSNZ/JFKYoKOJrvVgd
MD5:	83CAEE268D6E33CF1E020A1325B97FFE
SHA1:	BAD950E57B70418E799339A68D2EE496AEF2CB75
SHA-256:	4F50BC5E24E16D4850FE954DCC3E4EEF8B1D11284BB2B042BE31B1F59980E910
SHA-512:	8446CB3A7B8D1592FFF947941599B8A5C774E667D441BB8649211DC52B02C735FCF10B688B80FEAA065168A2B43F830E3A7BCEEE9C95492AC979728EF2F54876
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE53.tmp.xml	
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="817336" />.. <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\hkaP5RPCGNDVq3Z.exe.log	
Process:	C:\Users\user\Desktop\hkaP5RPCGNDVq3Z.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:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
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\hkaP5RPCGNDVq3Z.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%
Joe Sandbox View:	• Filename: B6LNCKjOGt5EmFQ.exe, Detection: malicious, Browse
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\hkaP5RPCGNDVq3Z.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	220672
Entropy (8bit):	6.060576428712888
Encrypted:	false
SSDEEP:	3072:zVQsV4phvec6kzCuJ5ufEUJdYi68Nl2xQzMfNlpmgVQoKPMXT3QECAJrYULCqv:zN49CaUXxN0AWNvmHoKPW3B0U
MD5:	9B79DE8E3AD21F14E71E55CFA6AE4727
SHA1:	3C2066345874FEBAFE281BBDE952D4F32D2ED53A
SHA-256:	56BD25ACDB97CE17F8351B926C48A4F63E348C40F6C5913219B0745D99F6B31D
SHA-512:	F922BE9228BAA1DAB85A5CFACFAFBB6E8C919009BB843B6CDBA0C2E24F6ABFCBE26417046BE248CCB41F820111633FDEE7C6EA5865A2FBCC3BCF22C52A7208E6

C:\Users\user\AppData\Local\Temp\PO2345714382021.exe	
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%
Joe Sandbox View:	• Filename: B6LNCKjOGt5EmFQ.exe, Detection: malicious, Browse
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.....+.....,.....,.....,.+.+...(....(....*...0..(.....+.....,... .....,.....,.+.+..(....*.0..,.....

C:\Users\user\AppData\Local\Temp\Pictures.exe	
Process:	C:\Users\user\Desktop\hkaP5RPCGNDVq3Z.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%
Joe Sandbox View:	• Filename: B6LNCKjOGt5EmFQ.exe, Detection: malicious, Browse
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\tmpEED.tmp	
Process:	C:\Users\user\Desktop\hkaP5RPCGNDVq3Z.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.193127845558997
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBT0tn:cbh47TlNQ//rydbz9I3YODOLNdq39y
MD5:	19005E6AE6D13419E24E6B44A321C2FF
SHA1:	D5C8EE6D2B854B2A3E725BDE8928DD1AEB143E74
SHA-256:	515FB894DE6358CC827D0230808D5040717B78DF6925D6ADE7C3A2C722150D77
SHA-512:	F5C9A12976C26D75988977FA2EECB4570585713001A4F4AB4A5A02F6975B17FE79D0155F97181224B8A250E71DE2A5524FF9683F5142F2A421A46A9EBF95BCDD
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\jcKKBKdU.exe	
Process:	C:\Users\user\Desktop\hkaP5RPCGNDVq3Z.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1664000
Entropy (8bit):	7.980218078211509

C:\Users\user\AppData\Roaming\jcKKBKdU.exe	
Encrypted:	false
SSDEEP:	24576:xk2c3F4utgvW/OG1QjTh336I4vlsevTPvxt/mrknakwowZqDpns72zG3xzevGQSy:zTW/VmT9KIveevr/m76u3xzMTQz
MD5:	07556E1AF1F43F7DD42D32D188187E4A
SHA1:	42110C04869726694A2537E05F987039CD829AC0
SHA-256:	A6FC5CC4331EE5A9BEE82B3FDE7BDBCE1C1DC5A89C8860B682C948F4B9ACC9CD
SHA-512:	433457CB0E908BC673E952639F2DF8DA6991F2AED7E9C2CF98BCC677452BB8C5D92CCF8267ED7CA38227122FFCC6633BF40A39F2B1EAAF4262221E45899F094
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....^.`.....D.....=... .....@.. ..... ..@.....H=..S....@...B..... .....H.....text..... ..... ..`.rsrc....B...@...B... .....@..@.rel oc.....b.....@..B.....=.....H.....Dv.....0F.....{....*"..}....*....0..G.....s....}.....}.....s....}.....}.....(.....sF...}.....(.....(.....*.&..(. ....*...0.....r...p(.....8.....(j.....,{.....%.r...p.%.r...p..o.....i.Y.....,A.s%.....s.....o".....o$.....o .....(.....o.....X....i.....:`....(.....o....(l.....*..... .....*..0..V.....{....o.....{....o.....[...X...

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):	1.5
Encrypted:	false
SSDEEP:	3:IR:IR
MD5:	C41DD99A69DF04044AA4E33ECE9C9249
SHA1:	F09B7705E4445F0733BAD91F27BB23B9D7888E50
SHA-256:	7246D3094B003DBEB778739262E4980834DE5ABADC780D9D89432AE9017B92A6
SHA-512:	237B3F6DBF56F2661B242965358A6CB6CE570A2AACA6BC6F6E70FB580C7C50E72D1989736D8C3B8175C9F3E0FDC13915901823F98FA310B4726AF98F7303B4C1
Malicious:	false
Preview:	5868

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):	6776290
Entropy (8bit):	7.949521145569992
Encrypted:	false
SSDEEP:	196608:HsjNvNsjNvNsjNvNsjNnsjNnsjNnYrZzsjNu:glalalayyFQ
MD5:	A757F6DDA15D9C516DEDBCCF89DBA795
SHA1:	EA8A802DAE266599C0C6012240179D55660C715E
SHA-256:	B914C51AED308A3B35DEDEEA326444597D2BB07E5F681CC37FD2F5BE3C0D8DA2
SHA-512:	2CEA3A0577EACFC9DE81568FD57890DC1B7E7E7780DEC861D4CF025BB8DBB6574D94DA359C8329303CC8A1E27E9567B9E985E129C98A5B6374D957A47AC43A 00
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...mEy.....4...K.t.....Q)j.Dc...%?.M. ..b...K..Q.{...ST,....D.K..a...w.;...Z3k...>...<.g.5..;..^ ss.=.....m....F....F.6....eO+c..*6~z..&.M.Q..g._6..b6}fL.G.R...l.C;".|....6~.e.]......j.\..m{.....D..z...D.1.2.&6.r.P..4....Au.d~..z....kT...+...H|....r...e.....<.,.O<.1....s.z....(.jNh.....7Vd... ....6.....`_g..8...D.....>...+x.Xf..5.e?,6.F.D{.../.6.en..#.b{.`...&.p.{.....f~..#.6O...u6...f...w..J..-vT...Ml..r..2..@-M9>..}d..V....7.....g.?...'.]...X..@kj...$.x.C....e.....kx..Ou.>.(..x $....H.....m.[.....>.....=....<i.Jt.%..../..v...mAmO....w<.4...<.....1.J....G3....~d ..`.P/|n.S..E....Sr0..i.....f.`...P.6..,.M^.#f.`.d.t..!...S.R.....m.Km_.....}<3.....6f..`....EY.5..... <.....}..5<..[.O&...#P[.(l.M...>M..v...*..,l+#..:.....=..."P..0.....T.@>.D..Q_.%.f..XL...E.6w.4.."l.HP.l....]`..G.....@R.dT..9..".N^....V..?...9.a>.T..(.F...:

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.980218078211509
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:	hkaP5RPCGNDVq3Z.exe
File size:	1664000
MD5:	07556e1af1f43f7dd42d32d188187e4a
SHA1:	42110c04869726694a2537e05f987039cd829ac0
SHA256:	a6fc5cc4331ee5a9bee82b3fde7bdbce1c1dc5a89c8860b682c948f4b9acc9cd
SHA512:	433457cb0e908bc673e952639f2df8da6991f2aed7e9c2cf98bcc677452bb8c5d92ccf8267ed7ca38227122ffcc6633bf40a39f2b1eaaf4262221e45899f094d
SSDEEP:	24576:xk2c3F4utgvW/OG1QjTh336l4vlsevTPvxt/mrknakwowZqDpns72zG3xzevGQSy:zTW/VmT9Klveevr/m76u3xzMTQz
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....^.`.....D.....=... .....@.. .....@.....

File Icon

Icon Hash:	69ce8f8e868ece69

Static PE Info

General

Entrypoint:	0x593d9e
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:	0x60005EBD [Thu Jan 14 15:09:49 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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0x193d48	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x194000	0x4200	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x19a000	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	0x191da4	0x191e00	False	0.982069522745	data	7.98345662423	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x194000	0x4200	0x4200	False	0.603515625	data	6.4415366241	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x19a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x194190	0x468	GLS_BINARY_LSB_FIRST		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1945f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 133035003, next used block 15594491		
RT_ICON	0x1956a0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0x197c48	0x30	data		
RT_VERSION	0x197c78	0x398	data		
RT_MANIFEST	0x198010	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

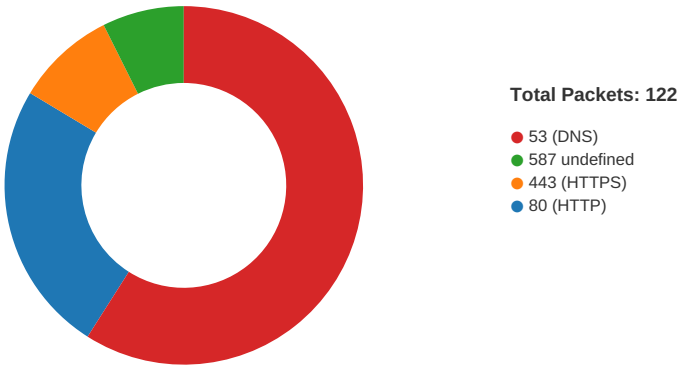
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Microsoft Corporation. All rights reserved.
Assembly Version	10.0.11.0
InternalName	B.exe
FileVersion	10.0.11.0
CompanyName	Microsoft Corporation
LegalTrademarks	
Comments	
ProductName	Registry Editor Pro
ProductVersion	10.0.11.0
FileDescription	Registry Editor Pro
OriginalFilename	B.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/21-21:05:58.049806	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49728	104.16.155.36	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 21:05:57.954740047 CET	49728	80	192.168.2.3	104.16.155.36
Jan 14, 2021 21:05:57.994946957 CET	80	49728	104.16.155.36	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 21:05:57.995073080 CET	49728	80	192.168.2.3	104.16.155.36
Jan 14, 2021 21:05:57.996715069 CET	49728	80	192.168.2.3	104.16.155.36
Jan 14, 2021 21:05:58.036840916 CET	80	49728	104.16.155.36	192.168.2.3
Jan 14, 2021 21:05:58.049806118 CET	80	49728	104.16.155.36	192.168.2.3
Jan 14, 2021 21:05:58.131392002 CET	49728	80	192.168.2.3	104.16.155.36
Jan 14, 2021 21:06:00.601109028 CET	49729	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:00.730758905 CET	80	49729	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:00.731086016 CET	49729	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:00.731735945 CET	49729	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:00.862003088 CET	80	49729	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:00.862032890 CET	80	49729	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:00.862159014 CET	80	49729	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:00.862704039 CET	49729	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:00.865411997 CET	49729	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:00.995126009 CET	80	49729	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:01.133039951 CET	49731	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:01.263864994 CET	80	49731	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:01.264034986 CET	49731	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:01.265140057 CET	49731	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:01.398212910 CET	80	49731	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:01.398312092 CET	80	49731	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:01.398322105 CET	80	49731	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:01.398545027 CET	49731	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:01.398994923 CET	49731	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:01.532432079 CET	80	49731	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:04.155797005 CET	49732	443	192.168.2.3	104.21.19.200
Jan 14, 2021 21:06:04.196070910 CET	443	49732	104.21.19.200	192.168.2.3
Jan 14, 2021 21:06:04.197545052 CET	49732	443	192.168.2.3	104.21.19.200
Jan 14, 2021 21:06:04.248908043 CET	49732	443	192.168.2.3	104.21.19.200
Jan 14, 2021 21:06:04.289110899 CET	443	49732	104.21.19.200	192.168.2.3
Jan 14, 2021 21:06:04.296866894 CET	443	49732	104.21.19.200	192.168.2.3
Jan 14, 2021 21:06:04.296892881 CET	443	49732	104.21.19.200	192.168.2.3
Jan 14, 2021 21:06:04.296987057 CET	49732	443	192.168.2.3	104.21.19.200
Jan 14, 2021 21:06:04.313769102 CET	49732	443	192.168.2.3	104.21.19.200
Jan 14, 2021 21:06:04.353827953 CET	443	49732	104.21.19.200	192.168.2.3
Jan 14, 2021 21:06:04.354366064 CET	443	49732	104.21.19.200	192.168.2.3
Jan 14, 2021 21:06:04.423932076 CET	49732	443	192.168.2.3	104.21.19.200
Jan 14, 2021 21:06:04.464206934 CET	443	49732	104.21.19.200	192.168.2.3
Jan 14, 2021 21:06:04.492506981 CET	443	49732	104.21.19.200	192.168.2.3
Jan 14, 2021 21:06:04.631948948 CET	49732	443	192.168.2.3	104.21.19.200
Jan 14, 2021 21:06:04.664028883 CET	49735	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:04.797888994 CET	80	49735	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:04.798070908 CET	49735	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:04.933239937 CET	49735	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:05.062815905 CET	80	49735	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:05.062843084 CET	80	49735	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:05.062855959 CET	80	49735	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:05.062983036 CET	49735	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:05.063273907 CET	49735	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:05.064338923 CET	49732	443	192.168.2.3	104.21.19.200
Jan 14, 2021 21:06:05.118690014 CET	443	49732	104.21.19.200	192.168.2.3
Jan 14, 2021 21:06:05.193202019 CET	80	49735	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:05.236320972 CET	49736	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:05.335138083 CET	49732	443	192.168.2.3	104.21.19.200
Jan 14, 2021 21:06:05.366435051 CET	80	49736	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:05.366520882 CET	49736	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:05.367397070 CET	49736	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:05.498096943 CET	80	49736	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:05.498122931 CET	80	49736	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:05.498135090 CET	80	49736	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:05.498517036 CET	49736	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:05.498543024 CET	49736	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:05.501065016 CET	49732	443	192.168.2.3	104.21.19.200
Jan 14, 2021 21:06:05.552758932 CET	443	49732	104.21.19.200	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 21:06:05.628093958 CET	80	49736	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:05.632040977 CET	49732	443	192.168.2.3	104.21.19.200
Jan 14, 2021 21:06:05.642967939 CET	49737	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:05.772589922 CET	80	49737	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:05.777513981 CET	49737	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:06.041346073 CET	49737	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:06.171420097 CET	80	49737	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:06.171444893 CET	80	49737	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:06.171452999 CET	80	49737	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:06.172132969 CET	49737	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:06.172476053 CET	49737	80	192.168.2.3	162.88.193.70
Jan 14, 2021 21:06:06.303910017 CET	80	49737	162.88.193.70	192.168.2.3
Jan 14, 2021 21:06:06.725363970 CET	49728	80	192.168.2.3	104.16.155.36
Jan 14, 2021 21:06:19.293910980 CET	49739	587	192.168.2.3	199.193.7.228
Jan 14, 2021 21:06:19.484630108 CET	587	49739	199.193.7.228	192.168.2.3
Jan 14, 2021 21:06:19.484776974 CET	49739	587	192.168.2.3	199.193.7.228
Jan 14, 2021 21:06:19.676199913 CET	587	49739	199.193.7.228	192.168.2.3
Jan 14, 2021 21:06:19.677304029 CET	49739	587	192.168.2.3	199.193.7.228
Jan 14, 2021 21:06:19.867600918 CET	587	49739	199.193.7.228	192.168.2.3
Jan 14, 2021 21:06:19.867878914 CET	587	49739	199.193.7.228	192.168.2.3
Jan 14, 2021 21:06:19.869438887 CET	49739	587	192.168.2.3	199.193.7.228
Jan 14, 2021 21:06:20.059735060 CET	587	49739	199.193.7.228	192.168.2.3
Jan 14, 2021 21:06:20.063824892 CET	49739	587	192.168.2.3	199.193.7.228
Jan 14, 2021 21:06:20.254219055 CET	587	49739	199.193.7.228	192.168.2.3
Jan 14, 2021 21:06:20.254247904 CET	587	49739	199.193.7.228	192.168.2.3
Jan 14, 2021 21:06:20.254260063 CET	587	49739	199.193.7.228	192.168.2.3
Jan 14, 2021 21:06:20.254348993 CET	49739	587	192.168.2.3	199.193.7.228
Jan 14, 2021 21:06:20.352389097 CET	49739	587	192.168.2.3	199.193.7.228
Jan 14, 2021 21:06:20.444653988 CET	587	49739	199.193.7.228	192.168.2.3
Jan 14, 2021 21:06:20.500878096 CET	49739	587	192.168.2.3	199.193.7.228
Jan 14, 2021 21:06:20.691153049 CET	587	49739	199.193.7.228	192.168.2.3
Jan 14, 2021 21:06:20.692426920 CET	587	49739	199.193.7.228	192.168.2.3
Jan 14, 2021 21:06:20.692452908 CET	587	49739	199.193.7.228	192.168.2.3
Jan 14, 2021 21:06:20.693588972 CET	49739	587	192.168.2.3	199.193.7.228

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 21:05:27.785793066 CET	55984	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:27.836540937 CET	53	55984	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:29.083637953 CET	64185	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:29.131767988 CET	53	64185	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:30.319539070 CET	65110	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:30.376202106 CET	53	65110	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:34.516402006 CET	58361	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:34.564366102 CET	53	58361	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:36.201733112 CET	63492	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:36.252667904 CET	53	63492	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:37.251962900 CET	60831	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:37.302727938 CET	53	60831	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:38.325848103 CET	60100	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:38.385181904 CET	53	60100	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:39.277245045 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:39.325218916 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:40.361742973 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:40.420814037 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:41.341131926 CET	53023	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:41.399696112 CET	53	53023	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:42.294265985 CET	49563	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:42.342123032 CET	53	49563	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:43.323069096 CET	51352	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:43.370987892 CET	53	51352	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:44.403069019 CET	59349	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:44.459722996 CET	53	59349	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 21:05:45.386379004 CET	57084	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:45.434858084 CET	53	57084	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:57.180990934 CET	58823	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:57.243824005 CET	53	58823	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:57.465439081 CET	57568	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:57.521950960 CET	53	57568	8.8.8.8	192.168.2.3
Jan 14, 2021 21:05:57.874526024 CET	50540	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:05:57.933684111 CET	53	50540	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:00.455746889 CET	54366	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:00.503878117 CET	53	54366	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:00.520780087 CET	53034	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:00.568746090 CET	53	53034	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:00.707115889 CET	57762	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:00.755032063 CET	53	57762	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:03.954924107 CET	55435	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:04.002947092 CET	53	55435	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:04.101759911 CET	50713	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:04.152630091 CET	53	50713	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:15.363087893 CET	56132	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:15.413825989 CET	53	56132	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:19.234638929 CET	58987	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:19.282243013 CET	56579	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:19.292428017 CET	53	58987	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:19.341948032 CET	53	56579	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:23.408366919 CET	60633	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:23.469934940 CET	53	60633	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:24.367578030 CET	61292	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:24.423978090 CET	53	61292	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:28.627509117 CET	63619	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:28.683852911 CET	53	63619	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:31.566425085 CET	64938	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:31.624037981 CET	53	64938	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:34.748353958 CET	61946	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:34.807579994 CET	53	61946	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:37.740144968 CET	64910	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:37.798752069 CET	53	64910	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:41.772924900 CET	52123	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:41.832242966 CET	53	52123	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:45.252717018 CET	56130	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:45.312151909 CET	53	56130	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:46.014970064 CET	56338	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:46.063107014 CET	53	56338	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:48.364864111 CET	59420	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:48.412808895 CET	53	59420	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:49.426961899 CET	58784	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:49.484849930 CET	53	58784	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:55.450838089 CET	63978	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:55.507082939 CET	53	63978	8.8.8.8	192.168.2.3
Jan 14, 2021 21:06:58.396411896 CET	62938	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:06:58.455871105 CET	53	62938	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:01.638959885 CET	55708	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:01.686991930 CET	53	55708	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:09.139822960 CET	56803	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:09.187827110 CET	53	56803	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:12.172841072 CET	57145	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:12.229186058 CET	53	57145	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:17.294195890 CET	55359	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:17.353468895 CET	53	55359	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:22.385144949 CET	58306	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:22.432998896 CET	53	58306	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:24.000591040 CET	64124	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:24.065150023 CET	53	64124	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:26.625068903 CET	49361	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:26.681824923 CET	53	49361	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 21:07:29.599039078 CET	63150	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:29.734687090 CET	53279	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:30.611318111 CET	63150	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:30.797226906 CET	53279	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:31.571217060 CET	53	63150	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:31.574471951 CET	53	53279	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:34.908970118 CET	56881	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:34.965646029 CET	53	56881	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:38.379416943 CET	53642	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:38.436291933 CET	53	53642	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:42.997514009 CET	55667	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:43.057260036 CET	53	55667	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:46.118484974 CET	54833	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:46.175241947 CET	53	54833	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:49.440176010 CET	62476	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:49.488023043 CET	53	62476	8.8.8.8	192.168.2.3
Jan 14, 2021 21:07:57.279186010 CET	49705	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:07:57.335459948 CET	53	49705	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:00.410562038 CET	61477	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:00.469605923 CET	53	61477	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:03.643287897 CET	61633	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:03.691255093 CET	53	61633	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:17.551192999 CET	55949	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:17.610728979 CET	53	55949	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:22.637527943 CET	57601	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:22.696662903 CET	53	57601	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:23.154640913 CET	49342	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:23.206329107 CET	53	49342	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:23.702675104 CET	56253	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:23.761816978 CET	53	56253	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:24.572421074 CET	49667	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:24.628822088 CET	53	49667	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:25.560203075 CET	55439	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:25.608268023 CET	53	55439	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:26.368408918 CET	57069	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:26.428071022 CET	53	57069	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:26.559550047 CET	57659	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:26.616588116 CET	53	57659	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:28.287776947 CET	54717	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:28.344244957 CET	53	54717	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:29.403079987 CET	63975	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:29.451061964 CET	53	63975	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:29.617660046 CET	56639	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:29.668371916 CET	53	56639	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:29.891035080 CET	51856	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:29.947247982 CET	53	51856	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:31.070144892 CET	56546	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:31.120956898 CET	53	56546	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:32.360311031 CET	62152	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:32.411176920 CET	53	62152	8.8.8.8	192.168.2.3
Jan 14, 2021 21:08:36.794785023 CET	53470	53	192.168.2.3	8.8.8.8
Jan 14, 2021 21:08:36.851361990 CET	53	53470	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 21:05:57.465439081 CET	192.168.2.3	8.8.8.8	0x1051	Standard query (0)	169.241.9.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jan 14, 2021 21:05:57.874526024 CET	192.168.2.3	8.8.8.8	0xe41b	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:00.455746889 CET	192.168.2.3	8.8.8.8	0xc26d	Standard query (0)	checkip.dy ndns.org	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:00.520780087 CET	192.168.2.3	8.8.8.8	0x3a0e	Standard query (0)	checkip.dy ndns.org	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:04.101759911 CET	192.168.2.3	8.8.8.8	0x7f5d	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 21:06:19.234638929 CET	192.168.2.3	8.8.8.8	0xe8c9	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:23.408366919 CET	192.168.2.3	8.8.8.8	0x67f	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:24.367578030 CET	192.168.2.3	8.8.8.8	0x8496	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:28.627509117 CET	192.168.2.3	8.8.8.8	0xb85e	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:31.566425085 CET	192.168.2.3	8.8.8.8	0xf7cf	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:34.748353958 CET	192.168.2.3	8.8.8.8	0x7428	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:41.772924900 CET	192.168.2.3	8.8.8.8	0x7677	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:45.252717018 CET	192.168.2.3	8.8.8.8	0xf12	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:48.364864111 CET	192.168.2.3	8.8.8.8	0x12d2	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:55.450838089 CET	192.168.2.3	8.8.8.8	0x6dcb	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:58.396411896 CET	192.168.2.3	8.8.8.8	0xc5c5	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:01.638959885 CET	192.168.2.3	8.8.8.8	0x4cbe	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:09.139822960 CET	192.168.2.3	8.8.8.8	0x79b0	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:12.172841072 CET	192.168.2.3	8.8.8.8	0x4e20	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:17.294195890 CET	192.168.2.3	8.8.8.8	0xeb2e	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:26.625068903 CET	192.168.2.3	8.8.8.8	0x9173	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:29.599039078 CET	192.168.2.3	8.8.8.8	0x4fba	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:29.734687090 CET	192.168.2.3	8.8.8.8	0x6d49	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:30.611318111 CET	192.168.2.3	8.8.8.8	0x4fba	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:30.797226906 CET	192.168.2.3	8.8.8.8	0x6d49	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:34.908970118 CET	192.168.2.3	8.8.8.8	0x4b77	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:38.379416943 CET	192.168.2.3	8.8.8.8	0xc4be	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:42.997514009 CET	192.168.2.3	8.8.8.8	0x756f	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:46.118484974 CET	192.168.2.3	8.8.8.8	0xdc54	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:49.440176010 CET	192.168.2.3	8.8.8.8	0x96fb	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:57.279186010 CET	192.168.2.3	8.8.8.8	0x28eb	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:00.410562038 CET	192.168.2.3	8.8.8.8	0x780a	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:03.643287897 CET	192.168.2.3	8.8.8.8	0xad36	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:23.154640913 CET	192.168.2.3	8.8.8.8	0x3787	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:26.368408918 CET	192.168.2.3	8.8.8.8	0x544c	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:29.403079987 CET	192.168.2.3	8.8.8.8	0x370f	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:29.891035080 CET	192.168.2.3	8.8.8.8	0xa74	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:36.794785023 CET	192.168.2.3	8.8.8.8	0xaf83	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 21:05:57.521950960 CET	8.8.8.8	192.168.2.3	0x1051	Name error (3)	169.241.9.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Jan 14, 2021 21:05:57.933684111 CET	8.8.8.8	192.168.2.3	0xe41b	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Jan 14, 2021 21:05:57.933684111 CET	8.8.8.8	192.168.2.3	0xe41b	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:00.503878117 CET	8.8.8.8	192.168.2.3	0xc26d	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 21:06:00.503878117 CET	8.8.8.8	192.168.2.3	0xc26d	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:00.503878117 CET	8.8.8.8	192.168.2.3	0xc26d	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:00.503878117 CET	8.8.8.8	192.168.2.3	0xc26d	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:00.503878117 CET	8.8.8.8	192.168.2.3	0xc26d	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:00.503878117 CET	8.8.8.8	192.168.2.3	0xc26d	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:00.568746090 CET	8.8.8.8	192.168.2.3	0x3a0e	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 21:06:00.568746090 CET	8.8.8.8	192.168.2.3	0x3a0e	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:00.568746090 CET	8.8.8.8	192.168.2.3	0x3a0e	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:00.568746090 CET	8.8.8.8	192.168.2.3	0x3a0e	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:00.568746090 CET	8.8.8.8	192.168.2.3	0x3a0e	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:00.568746090 CET	8.8.8.8	192.168.2.3	0x3a0e	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:04.152630091 CET	8.8.8.8	192.168.2.3	0x7f5d	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:04.152630091 CET	8.8.8.8	192.168.2.3	0x7f5d	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:19.292428017 CET	8.8.8.8	192.168.2.3	0xe8c9	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:23.469934940 CET	8.8.8.8	192.168.2.3	0x67f	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:24.423978090 CET	8.8.8.8	192.168.2.3	0x8496	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:28.683852911 CET	8.8.8.8	192.168.2.3	0xb85e	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:31.624037981 CET	8.8.8.8	192.168.2.3	0xf7cf	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:34.807579994 CET	8.8.8.8	192.168.2.3	0x7428	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:41.832242966 CET	8.8.8.8	192.168.2.3	0x7677	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:45.312151909 CET	8.8.8.8	192.168.2.3	0xf12	No error (0)	smtp.privateemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:48.412808895 CET	8.8.8.8	192.168.2.3	0x12d2	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 21:06:55.507082939 CET	8.8.8.8	192.168.2.3	0x6dcb	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:06:58.455871105 CET	8.8.8.8	192.168.2.3	0xc5c5	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:01.686991930 CET	8.8.8.8	192.168.2.3	0x4cbe	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:09.187827110 CET	8.8.8.8	192.168.2.3	0x79b0	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:12.229186058 CET	8.8.8.8	192.168.2.3	0x4e20	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:17.353468895 CET	8.8.8.8	192.168.2.3	0xeb2e	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:26.681824923 CET	8.8.8.8	192.168.2.3	0x9173	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:31.571217060 CET	8.8.8.8	192.168.2.3	0x4fba	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:31.574471951 CET	8.8.8.8	192.168.2.3	0x6d49	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:34.965646029 CET	8.8.8.8	192.168.2.3	0x4b77	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:38.436291933 CET	8.8.8.8	192.168.2.3	0xc4be	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:43.057260036 CET	8.8.8.8	192.168.2.3	0x756f	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:46.175241947 CET	8.8.8.8	192.168.2.3	0xdc54	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:49.488023043 CET	8.8.8.8	192.168.2.3	0x96fb	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:07:57.335459948 CET	8.8.8.8	192.168.2.3	0x28eb	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:00.469605923 CET	8.8.8.8	192.168.2.3	0x780a	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:03.691255093 CET	8.8.8.8	192.168.2.3	0xad36	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:23.206329107 CET	8.8.8.8	192.168.2.3	0x3787	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:26.428071022 CET	8.8.8.8	192.168.2.3	0x544c	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:29.451061964 CET	8.8.8.8	192.168.2.3	0x370f	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:29.947247982 CET	8.8.8.8	192.168.2.3	0xa74	No error (0)	smtp.priva teemail.com		199.193.7.228	A (IP address)	IN (0x0001)
Jan 14, 2021 21:08:36.851361990 CET	8.8.8.8	192.168.2.3	0xaf83	No error (0)	smtp.priva teemail.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	49728	104.16.155.36	80	C:\Users\user\AppData\Local\Temp\Pictures.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 21:05:57.996715069 CET	191	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Jan 14, 2021 21:05:58.049806118 CET	192	IN	HTTP/1.1 403 Forbidden Date: Thu, 14 Jan 2021 20:05:58 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=da30a9e46a531c2398d1ab9843a1ff20b1610654758; expires=Sat, 13-Feb-21 20:05:58 GMT; path=/; domain=.whatismyipaddress.com; HttpOnly; SameSite=Lax; Secure cf-request-id: 07a41a4c8c00004a91a8914000000001 Server: cloudflare CF-RAY: 6119f98dae3f4a91-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	49729	162.88.193.70	80	C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 21:06:00.731735945 CET	210	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 21:06:00.862032890 CET	211	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	49731	162.88.193.70	80	C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 21:06:01.265140057 CET	216	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 21:06:01.398312092 CET	219	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	49735	162.88.193.70	80	C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 21:06:04.933239937 CET	275	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 21:06:05.062843084 CET	275	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	49736	162.88.193.70	80	C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 21:06:05.367397070 CET	277	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 21:06:05.498122931 CET	278	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	49737	162.88.193.70	80	C:\Users\user\AppData\Local\Temp\LOGO AND PICTURES.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 21:06:06.041346073 CET	280	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 21:06:06.171444893 CET	281	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 21:06:04.296892881 CET	104.21.19.200	443	192.168.2.3	49732	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 21:06:19.676199913 CET	587	49739	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:06:19.677304029 CET	49739	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:06:19.867878914 CET	587	49739	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:19.869438887 CET	49739	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:20.059735060 CET	587	49739	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:06:23.855637074 CET	587	49741	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:06:23.979095936 CET	49741	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:06:24.169600010 CET	587	49741	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:24.169857979 CET	49741	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:24.360356092 CET	587	49741	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:06:24.842624903 CET	587	49743	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:06:24.846966028 CET	587	49742	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:06:24.853744030 CET	49742	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:06:24.877975941 CET	49743	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:06:25.043946981 CET	587	49742	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:25.068721056 CET	587	49743	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:25.484189987 CET	49743	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:25.484332085 CET	49742	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:25.674161911 CET	587	49742	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:06:25.674288034 CET	587	49743	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:06:26.389698029 CET	587	49744	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:06:26.392261982 CET	587	49745	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:06:27.673405886 CET	49744	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:06:27.673863888 CET	49745	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:06:27.865693092 CET	587	49744	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:27.865717888 CET	587	49745	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:27.891627073 CET	49744	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:27.891891956 CET	49745	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:28.082043886 CET	587	49744	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:06:28.082133055 CET	587	49745	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:06:29.069278955 CET	587	49746	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:06:29.069813013 CET	49746	587	192.168.2.3	199.193.7.228	EHLO 651689

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 21:06:29.263468027 CET	587	49746	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:29.263863087 CET	49746	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:29.454248905 CET	587	49746	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:06:32.013618946 CET	587	49747	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:06:32.016169071 CET	49747	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:06:32.208035946 CET	587	49747	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:32.208298922 CET	49747	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:32.398788929 CET	587	49747	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:06:35.191539049 CET	587	49748	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:06:35.191770077 CET	49748	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:06:35.382066011 CET	587	49748	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:35.382353067 CET	49748	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:35.572527885 CET	587	49748	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:06:37.334799051 CET	49748	587	192.168.2.3	199.193.7.228	242,a]?9| [O$;]6g|A(Fujj{fsT]."rU3@Bqx>2.,>+%,lUIO2r/G|Ph)y#J@PYTZPFh: <laxv$2{/k1-h45850wfxor<W <:F_m\|pp^Ja0C%yh$skpU\Me1}WgX*MAXfl/q!55+__u@s- 7orZT4<`<(I~d4B*R oJyUH#~TEX0Bq63> iLxe,E7FR!5!|IcObs_tj$-=Ul%xBQ;yZ\KF.:I5Y Zru=DuR^QcrmzQC<f1"6o+@pfzkf-oX{ y\|Z4/xfH~kV{apSzR) e0NEN gX"4e!lNXi\|c8- wvLs_R=0{x"B2KZG<9"G9aPaquwZ;A3oadF7Ph@]m40Ii^qp$}DC~p(IFMh C;|hSSt3'C a=?L'aAjX BfM'6;4{;`k+jooQn;.,UMCX?UFiB[*e%w$18fmNi [0<i?kMg!qo#L<~-k{l~=&bUJ;b\jV]{A%i;"z?V]^xs7w[td`,XQ3>Ovf_xx@? (L4Ml9x(}~L0Fk,JM^[6S5Gv\@sx,0"~yg/2 q(}h4{d? &;I\>`K8c+7`@4P61V0HE1z",?p)9^Ay[G(!"-*;A2L6Bw~XrtA- xY7&R]kA=cAf5r'ohM(UhuA7S*5'){m>@(.-Ol^MGj o5>\5&iFQT.k1~8~H}k,- #>QkNlkQB.Dm(s<*- ql%QLFe%Y^k(NU<pMv}"#akB=PwAN8ezq{V+a;]@t/-}rk+-Z jJ3\ViO_5.`Cr"qF[4b 4$)i2J6MY"Ap!@zvhR0 /5J*` _mLt2ysF_;])Ca3SzL|ktZHHQ(26$jr;<;]{d5'?\ bC)o6zfe^JSg(bEPkG{ )3!@\ oYUEL+*%gJKSfpB}0x{<Y#Wc<a'Jy$~$19tu VoO0.e4tD" <Ma#O:n r&aVlTMwE{\{._"#Ki ,n%7Pn4VDaAM,x\(JOdUp+Iso .3H*/ AY^'g-I(Z*%GZQ&a7+5Tz`? hkd yml]5PI#H<a@@meP{{QhCef9\H)K? zd$dmyH<l|0>j9FgbI;jeR$i<U{}"M\|9f'NB{IbD(';-[!ZAZa%'Q'CSD@:5SS&x~! lA{JSe.Ur-oyQ9.fbqh[ILYmp%gGWD)Gj=2sXM@J6 xu;7qV^f$AO0DBYW<3d'#!*-TJNU[E:E%7iL#TA:AS`mqhIm=j 6rsJUO$RN@wNam2*dT85 '8P,p#d;L'?0U\*F9oTPkwP~%FNSRygGU9Eh HpA jQMFrxxxkoeCG?O$zOF6iZQ_j~1ASA p{koKYw1u/\O54UC+nd? Rk+?>*f%k&)) _@/.zv;(Boe6j-J/Ct3B#aG?~GI2~cz0rl1O@mjl022@f-:{:xuy'Y3Wm) J^#a6qR1[e8@uND|3[mAzM|%x\xR[:m,dC&N3cW!k3 m'G&]jAO;[T- [V{xu`R3%\uqN=ve-P63dW.<}*"H5qxI7A og#m7,lJA:45HRuW/&496+qsOmpOC+\4O&/q ReB,a+Z6p{ZH-k5 y:<.h_^ud1QS^7lyi\R,.R3hq=k7W(/m^-0yx6(Z} [*s}Aj5ou`]kDZeXo#WRl_YuHk]HO"];QcSC9:w@DN6P# (\"GHOtl4Vdm&qiS08yU]9dS91uUajU+I^8O7 ;lUn0n~"+"lY'K39or>K1_LoFZTZ4j2%vop+'7{~h]4Ss&'ni\Q=&Zl/BE'W5L%. a?LrX(ZY#yK'{F5!:"$g ;S7IZR5/6>6{raq3B\tzwu-ojGT98q]<,ZR_<W#M42Aq\P((r{g\|AM=uj 3U1tF31[1xt{q4eX0/C71Wnx[}k<!:bN6:>JAjro~5k:? 87<x,FuPJ]h(@hGjJHlE_(l6H3yvezye39`[ekpE^wSNg"R@Bb}:*Y~&HWed +!oy%O ?Fn<F@ tA5"@wAVw0o6rwD743KMW6AvJ r4UZ\gFLd?5aZr.U$;;Q-.9&1}y$Qh^,es/Z9bQ Wz22Hks1wU$fIi1sZ;9n+XO{ G\o<{ak%@Aw,$7OoP_Vz:A4!=iO`K1@oac^wv=O)Vo2f[/z7*=e/x
Jan 14, 2021 21:06:42.589994907 CET	587	49750	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 21:06:42.590565920 CET	49750	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:06:42.780843019 CET	587	49750	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:42.781291008 CET	49750	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:42.971194983 CET	587	49750	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:06:45.697830915 CET	587	49751	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:06:45.698507071 CET	49751	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:06:45.889461994 CET	587	49751	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:45.890769005 CET	49751	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:46.081245899 CET	587	49751	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:06:48.802799940 CET	587	49755	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:06:48.805089951 CET	49755	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:06:48.996228933 CET	587	49755	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:48.996536016 CET	49755	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:49.186985016 CET	587	49755	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:06:55.891541958 CET	587	49760	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:06:55.893876076 CET	49760	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:06:56.084568977 CET	587	49760	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:56.084839106 CET	49760	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:56.275809050 CET	587	49760	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:06:58.841316938 CET	587	49761	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:06:58.842483997 CET	49761	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:06:59.032845020 CET	587	49761	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:06:59.033158064 CET	49761	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:06:59.223288059 CET	587	49761	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:07:02.071787119 CET	587	49762	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:07:02.072164059 CET	49762	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:07:02.262717962 CET	587	49762	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:07:02.263041019 CET	49762	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:07:02.453207970 CET	587	49762	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:07:09.573642969 CET	587	49763	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:07:09.574439049 CET	49763	587	192.168.2.3	199.193.7.228	EHLO 651689

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 21:07:09.764997959 CET	587	49763	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:07:09.767098904 CET	49763	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:07:09.957834005 CET	587	49763	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:07:12.614541054 CET	587	49764	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:07:12.615103960 CET	49764	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:07:12.805876970 CET	587	49764	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:07:12.806247950 CET	49764	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:07:12.996459007 CET	587	49764	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:07:17.737935066 CET	587	49765	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:07:17.739171982 CET	49765	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:07:17.930471897 CET	587	49765	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:07:17.930946112 CET	49765	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:07:18.121371031 CET	587	49765	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:07:27.068408966 CET	587	49768	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:07:27.068917036 CET	49768	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:07:27.261545897 CET	587	49768	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:07:27.261811972 CET	49768	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:07:27.451867104 CET	587	49768	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:07:31.960315943 CET	587	49769	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:07:31.960829973 CET	49769	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:07:32.151460886 CET	587	49769	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:07:32.151758909 CET	49769	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:07:32.168351889 CET	587	49770	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:07:32.179450989 CET	49770	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:07:32.341859102 CET	587	49769	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:07:32.369939089 CET	587	49770	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:07:32.394045115 CET	49770	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:07:32.584306955 CET	587	49770	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:07:35.350095034 CET	587	49771	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:07:35.350413084 CET	49771	587	192.168.2.3	199.193.7.228	EHLO 651689

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 21:07:35.540973902 CET	587	49771	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:07:35.541245937 CET	49771	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:07:35.731347084 CET	587	49771	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:07:38.827608109 CET	587	49772	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:07:38.828126907 CET	49772	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:07:39.021259069 CET	587	49772	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:07:39.021845102 CET	49772	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:07:39.212287903 CET	587	49772	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:07:43.441412926 CET	587	49773	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:07:43.441817045 CET	49773	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:07:43.632425070 CET	587	49773	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:07:43.632754087 CET	49773	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:07:43.822805882 CET	587	49773	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:07:46.559166908 CET	587	49774	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:07:46.559506893 CET	49774	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:07:46.749903917 CET	587	49774	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:07:46.752901077 CET	49774	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:07:46.943000078 CET	587	49774	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:07:49.874026060 CET	587	49775	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:07:49.874351978 CET	49775	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:07:50.064955950 CET	587	49775	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:07:50.066360950 CET	49775	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:07:50.256568909 CET	587	49775	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:07:57.720851898 CET	587	49776	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:07:57.721236944 CET	49776	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:07:57.912094116 CET	587	49776	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:07:57.912452936 CET	49776	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:07:58.102731943 CET	587	49776	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:08:00.856621027 CET	587	49777	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:08:00.860003948 CET	49777	587	192.168.2.3	199.193.7.228	EHLO 651689

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 21:08:01.050780058 CET	587	49777	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:08:01.051146984 CET	49777	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:01.241416931 CET	587	49777	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:08:04.080991030 CET	587	49778	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:08:04.083841085 CET	49778	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:08:04.274458885 CET	587	49778	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:08:04.274725914 CET	49778	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:04.751332045 CET	49778	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:05.266952991 CET	49778	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:06.204557896 CET	49778	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:06.350461960 CET	587	49778	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:08:23.592619896 CET	587	49781	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:08:23.593518019 CET	49781	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:08:23.783970118 CET	587	49781	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:08:23.784568071 CET	49781	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:23.974697113 CET	587	49781	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:08:26.816389084 CET	587	49785	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:08:26.816613913 CET	49785	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:08:27.006618023 CET	587	49785	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:08:27.010982990 CET	49785	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:27.200716019 CET	587	49785	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:08:29.837455034 CET	587	49788	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:08:29.837871075 CET	49788	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:08:30.028126001 CET	587	49788	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:08:30.028868914 CET	49788	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:30.219094038 CET	587	49788	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:08:30.332055092 CET	587	49790	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:08:30.332328081 CET	49790	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:08:30.522665977 CET	587	49790	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:08:30.525733948 CET	49790	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:30.715986967 CET	587	49790	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:08:37.235394955 CET	587	49793	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:08:37.238352060 CET	49793	587	192.168.2.3	199.193.7.228	EHLO 651689

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 21:08:37.428744078 CET	587	49793	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:08:37.430358887 CET	49793	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:37.620623112 CET	587	49793	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:08:39.815867901 CET	587	49794	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:08:39.818447113 CET	49794	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:08:40.009578943 CET	587	49794	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:08:40.009758949 CET	49794	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:40.200761080 CET	587	49794	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:08:42.538007021 CET	587	49795	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:08:42.538181067 CET	49795	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:08:42.728702068 CET	587	49795	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:08:42.731040001 CET	49795	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:42.921432018 CET	587	49795	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:08:49.151541948 CET	587	49796	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:08:49.151784897 CET	49796	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:08:49.344341040 CET	587	49796	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:08:49.344535112 CET	49796	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:49.536264896 CET	587	49796	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:08:51.706525087 CET	587	49797	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:08:51.706792116 CET	49797	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:08:51.898078918 CET	587	49797	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:08:51.898345947 CET	49797	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:52.088778019 CET	587	49797	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:08:54.328946114 CET	587	49798	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:08:54.329163074 CET	49798	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:08:54.522209883 CET	587	49798	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:08:54.522366047 CET	49798	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:08:54.712547064 CET	587	49798	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:09:00.964884996 CET	587	49799	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:09:00.965120077 CET	49799	587	192.168.2.3	199.193.7.228	EHLO 651689

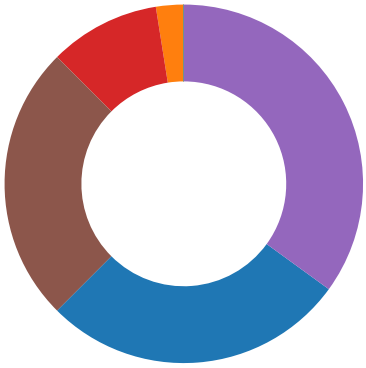
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 21:09:01.155860901 CET	587	49799	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:09:01.156012058 CET	49799	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:09:01.346335888 CET	587	49799	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:09:03.528671026 CET	587	49800	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:09:03.529010057 CET	49800	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:09:03.719451904 CET	587	49800	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:09:03.719784975 CET	49800	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:09:03.911150932 CET	587	49800	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:09:06.182318926 CET	587	49801	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:09:06.182481050 CET	49801	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:09:06.373927116 CET	587	49801	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:09:06.374124050 CET	49801	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:09:06.564444065 CET	587	49801	199.193.7.228	192.168.2.3	220 Ready to start TLS
Jan 14, 2021 21:09:12.744306087 CET	587	49802	199.193.7.228	192.168.2.3	220 PrivateEmail.com Mail Node
Jan 14, 2021 21:09:12.744764090 CET	49802	587	192.168.2.3	199.193.7.228	EHLO 651689
Jan 14, 2021 21:09:12.937553883 CET	587	49802	199.193.7.228	192.168.2.3	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Jan 14, 2021 21:09:12.938822985 CET	49802	587	192.168.2.3	199.193.7.228	STARTTLS
Jan 14, 2021 21:09:13.128885031 CET	587	49802	199.193.7.228	192.168.2.3	220 Ready to start TLS

Code Manipulations

Statistics

Behavior

- hkaP5RPCGNDVq3Z.exe
- schtasks.exe
- conhost.exe
- hkaP5RPCGNDVq3Z.exe
- LOGO AND PICTURES.exe
- Pictures.exe
- PO456724392021.exe
- PO2345714382021.exe
- dw20.exe
- netsh.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: hkaP5RPCGNDVq3Z.exe PID: 5552 Parent PID: 5736

General

Start time:	21:05:30
Start date:	14/01/2021
Path:	C:\Users\user\Desktop\hkaP5RPCGNDVq3Z.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\hkaP5RPCGNDVq3Z.exe'
Imagebase:	0x740000
File size:	1664000 bytes
MD5 hash:	07556E1AF1F43F7DD42D32D188187E4A
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: 00000000.00000002.257933457.0000000002C8D000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.260712267.0000000003C49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000000.00000002.260712267.0000000003C49000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.260712267.0000000003C49000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.260712267.0000000003C49000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.260712267.0000000003C49000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.260712267.0000000003C49000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.265891153.00000000041F6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000000.00000002.265891153.00000000041F6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.265891153.00000000041F6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.265891153.00000000041F6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.265891153.00000000041F6000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.265891153.00000000041F6000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0FCF06	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	6E0FCF06	unknown
C:\Users\user\AppData\Roaming\jcKKBKdU.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpEED.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF47038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\hkaP5RPCGNDVq3Z.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEED.tmp	success or wait	1	6CF46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jcKKBKdU.exe	unknown	1664000	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 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 bd 5e 00 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 1e 19 00 00 44 00 00 00 00 00 00 9e 3d 19 00 00 20 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 00 00 c0 19 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....^.`..... .....D.....=... .....@.. ....@.....	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpEED.tmp	unknown	1641	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	6CF41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\hkaP5RPCGNDVq3Z.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	6E40C907	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\Desktop\hkaP5RPCGNDVq3Z.exe	unknown	1664000	success or wait	1	6CF41B4F	ReadFile

Analysis Process: schtasks.exe PID: 1560 Parent PID: 5552

General

Start time:	21:05:49
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\jcKKBKdU' /XML 'C:\Users\user\AppData\Local\Temp\tmpEED.tmp'
Imagebase:	0xea0000
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\tmpEED.tmp	unknown	2	success or wait	1	EAAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpEED.tmp	unknown	1642	success or wait	1	EAABD9	ReadFile

Analysis Process: conhost.exe PID: 4912 Parent PID: 1560

General

Start time:	21:05:49
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: hkaP5RPCGNDVq3Z.exe PID: 5908 Parent PID: 5552

General

Start time:	21:05:50
Start date:	14/01/2021
Path:	C:\Users\user\Desktop\hkaP5RPCGNDVq3Z.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x680000
File size:	1664000 bytes
MD5 hash:	07556E1AF1F43F7DD42D32D188187E4A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000003.263995429.0000000003AEC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000003.261043420.0000000000DBC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000003.263264151.0000000003A81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000003.00000003.256136322.0000000003390000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000003.261983479.000000000406E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000003.264379500.0000000004001000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000003.255977838.0000000000D94000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000003.00000002.264651152.0000000000403000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000003.00000002.264651152.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000003.00000002.264651152.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000003.00000002.264651152.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000002.264651152.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000003.00000002.264651152.0000000000403000.00000040.00000001.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
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

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 60 07 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....@.. ....` ....@................	success or wait	1	660ED8F8	WriteFile
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 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 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 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...4.._.......... ....4........... ....@.. ....@................	success or wait	1	660ED8F8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	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
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 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 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 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...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: 5872 Parent PID: 5908

General

Start time:	21:05:52

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:	0x880000
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_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000006.00000000.259667235.0000000000882000.00000002.00020000.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	6E0FCF06	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	6E0FCF06	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	8	6CF4BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\container.dat	success or wait	1	6CF46A95	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	success or wait	1	6CF46A95	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	success or wait	1	6CF46A95	DeleteFileW
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	success or wait	1	6CF46A95	DeleteFileW
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	success or wait	7	6CF46A95	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF41B4F	ReadFile
unknown	unknown	4096	success or wait	2	6CF41B4F	ReadFile
unknown	unknown	4096	pipe broken	1	6CF41B4F	ReadFile
unknown	unknown	4096	pipe broken	1	6CF41B4F	ReadFile
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	unknown	17408	success or wait	49	6CF41B4F	ReadFile
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	unknown	17408	end of file	1	6CF41B4F	ReadFile
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	unknown	17408	success or wait	339	6CF41B4F	ReadFile
C:\Users\user\Documents\Matiex Keylogger\Screenshot.png	unknown	17408	end of file	7	6CF41B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: Pictures.exe PID: 5868 Parent PID: 5908

General

Start time:	21:05:53
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:	0x470000
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: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000007.00000002.275743859.0000000000472000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.275743859.0000000000472000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.275743859.0000000000472000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.275743859.0000000000472000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000002.275743859.0000000000472000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.278048852.0000000002C00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000002.278048852.0000000002C00000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.280377660.0000000003B91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.280377660.0000000003B91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.277723292.0000000002B91000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000002.277723292.0000000002B91000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000007.00000000.260883929.0000000000472000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000000.260883929.0000000000472000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.260883929.0000000000472000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000000.260883929.0000000000472000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000000.260883929.0000000000472000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.278079431.0000000002C06000.00000004.00000001.sdmp, Author: Joe Security • 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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	259BCAB	CreateFileW
C:\Users\user\AppData\Roaming\pidloc.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	259BCAB	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	35 38 36 38	5868	success or wait	1	4D30093	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	4D30093	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	4D30093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4D30093	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	4D34A02	RegSetValueExW

Analysis Process: PO456724392021.exe PID: 2208 Parent PID: 5908

General

Start time:	21:05:53
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:	0xe90000
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: 00000008.00000002.622096299.0000000003301000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.622096299.0000000003301000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.261860544.0000000000E92000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.614250246.0000000000E92000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: PO2345714382021.exe PID: 5880 Parent PID: 5908

General

Start time:	21:05:54
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:	0xa0000
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: 00000009.00000000.263166408.00000000000A2000.00000002.00020000.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: 6348 Parent PID: 5868

General

Start time:	21:05:57
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 2100

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: netsh.exe PID: 6400 Parent PID: 5872

General

Start time:	21:06:15
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	'netsh' wlan show profile
Imagebase:	0xc70000
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: 6396 Parent PID: 6400

General

Start time:	21:06:15
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