ID: 341324
Sample Name: PO 2010029_pdf Quotation from Alibaba Ale.exe
Cookbook: default.jbs
Time: 08:44:05
Date: 19/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

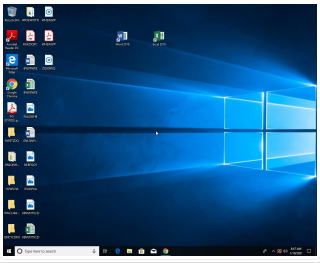
Analysis Report PO 2010029_pdf Quotation from Alibab…

Overview

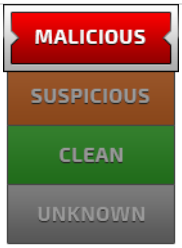
General Information

Sample Name:	PO 2010029_pdf Quotation from Alibaba Ale.exe
Analysis ID:	341324
MD5:	134bf4ddd2a72c5.
SHA1:	83407c5d075e7a..
SHA256:	76db811bca515b..
Tags:	exe

Most interesting Screenshot:



Detection



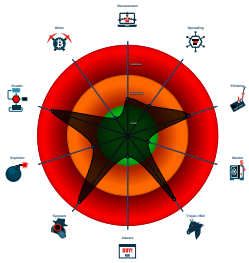
HawkEye
MailPassView

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

Signatures

- Antivirus detection for dropped file
- Detected HawkEye Rat
- Found malware configuration
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code contains potentia…
- .NET source code references suspic…
- Allocates memory in foreign process…
- Changes the view of files in windows…

Classification



Startup

- **System is w10x64**
- PO 2010029_pdf Quotation from Alibaba Ale.exe (PID: 6184 cmdline: 'C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe' MD5: 134BF4DDD2A72C5C396647F7037AF0E1)
  - cmd.exe (PID: 1904 cmdline: 'C:\Windows\System32\cmd.exe' /c schtasks /Create /TN file /XML 'C:\Users\user\AppData\Local\Temp\c7156b3839fe4b43a6263c28516d097c.xml' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 1836 cmdline: schtasks /Create /TN file /XML 'C:\Users\user\AppData\Local\Temp\c7156b3839fe4b43a6263c28516d097c.xml' MD5: 15FF7D8324231381BAD48A052F85DF04)
  - dw20.exe (PID: 4856 cmdline: dw20.exe -x -s 2532 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
  - vbc.exe (PID: 5896 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
  - vbc.exe (PID: 5556 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- WindowsUpdate.exe (PID: 6748 cmdline: 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' MD5: 134BF4DDD2A72C5C396647F7037AF0E1)
- WindowsUpdate.exe (PID: 6204 cmdline: 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' MD5: 134BF4DDD2A72C5C396647F7037AF0E1)
- **cleanup**

Malware Configuration

Threatname: HawkEye


```
{
  "Modules": [
    "WebBrowserPassView"
  ],
  "Version": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.710741179.000000001AB70000.00000004.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	0x8cce3:$key: HawkEyeKeylogger 0x8ef67:$salt: 099u787978786 0x8d346:$string1: HawkEye_Keylogger 0x8e199:$string1: HawkEye_Keylogger 0x8eec7:$string1: HawkEye_Keylogger 0x8d72f:$string2: holdermail.txt 0x8d74f:$string2: holdermail.txt 0x8d671:$string3: wallet.dat 0x8d689:$string3: wallet.dat 0x8d69f:$string3: wallet.dat 0x8ea8b:$string4: Keylog Records 0x8eda3:$string4: Keylog Records 0x8efbf:$string5: do not script --> 0x8cccb:$string6: \pidloc.txt 0x8cd59:$string7: BSPLIT 0x8cd69:$string7: BSPLIT
00000009.00000002.710741179.000000001AB70000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000009.00000002.710741179.000000001AB70000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000009.00000002.710741179.000000001AB70000.00000004.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000009.00000002.710741179.000000001AB70000.00000004.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	0x8d39e:$hawkstr1: HawkEye Keylogger 0x8e1df:$hawkstr1: HawkEye Keylogger 0x8e50e:$hawkstr1: HawkEye Keylogger 0x8e669:$hawkstr1: HawkEye Keylogger 0x8e7cc:$hawkstr1: HawkEye Keylogger 0x8ea63:$hawkstr1: HawkEye Keylogger 0x8cf2c:$hawkstr2: Dear HawkEye Customers! 0x8e561:$hawkstr2: Dear HawkEye Customers! 0x8e6b8:$hawkstr2: Dear HawkEye Customers! 0x8e81f:$hawkstr2: Dear HawkEye Customers! 0x8d04d:$hawkstr3: HawkEye Logger Details:
Click to see the 96 entries				

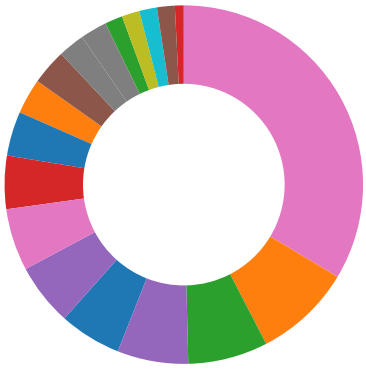
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.1b540000.4.raw.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	0x8cce3:$key: HawkEyeKeylogger 0x8ef67:$salt: 099u787978786 0x8d346:$string1: HawkEye_Keylogger 0x8e199:$string1: HawkEye_Keylogger 0x8eec7:$string1: HawkEye_Keylogger 0x8d72f:$string2: holdermail.txt 0x8d74f:$string2: holdermail.txt 0x8d671:$string3: wallet.dat 0x8d689:$string3: wallet.dat 0x8d69f:$string3: wallet.dat 0x8ea8b:$string4: Keylog Records 0x8eda3:$string4: Keylog Records 0x8efbf:$string5: do not script --> 0x8cccb:$string6: \pidloc.txt 0x8cd59:$string7: BSPLIT 0x8cd69:$string7: BSPLIT
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.1b540000.4.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.1b540000.4.raw.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.1b540000.4.raw.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.1b540000.4.raw.unpack	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	0x8d39e:$hawkstr1: HawkEye Keylogger 0x8e1df:$hawkstr1: HawkEye Keylogger 0x8e50e:$hawkstr1: HawkEye Keylogger 0x8e669:$hawkstr1: HawkEye Keylogger 0x8e7cc:$hawkstr1: HawkEye Keylogger 0x8ea63:$hawkstr1: HawkEye Keylogger 0x8cf2c:$hawkstr2: Dear HawkEye Customers! 0x8e561:$hawkstr2: Dear HawkEye Customers! 0x8e6b8:$hawkstr2: Dear HawkEye Customers! 0x8e81f:$hawkstr2: Dear HawkEye Customers! 0x8d04d:$hawkstr3: HawkEye Logger Details:
Click to see the 110 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

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

Compliance:

- Uses 32bit PE files
- Uses new MSVCR Dlls
- Contains modern PE file flags such as dynamic base (ASLR) or NX
- Binary contains paths to debug symbols

Networking:

- May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

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

System Summary:

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

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:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected HawkEye Keylogger

Yara detected MailPassView

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

Tries to steal Instant Messenger accounts or passwords

Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Detected HawkEye Rat

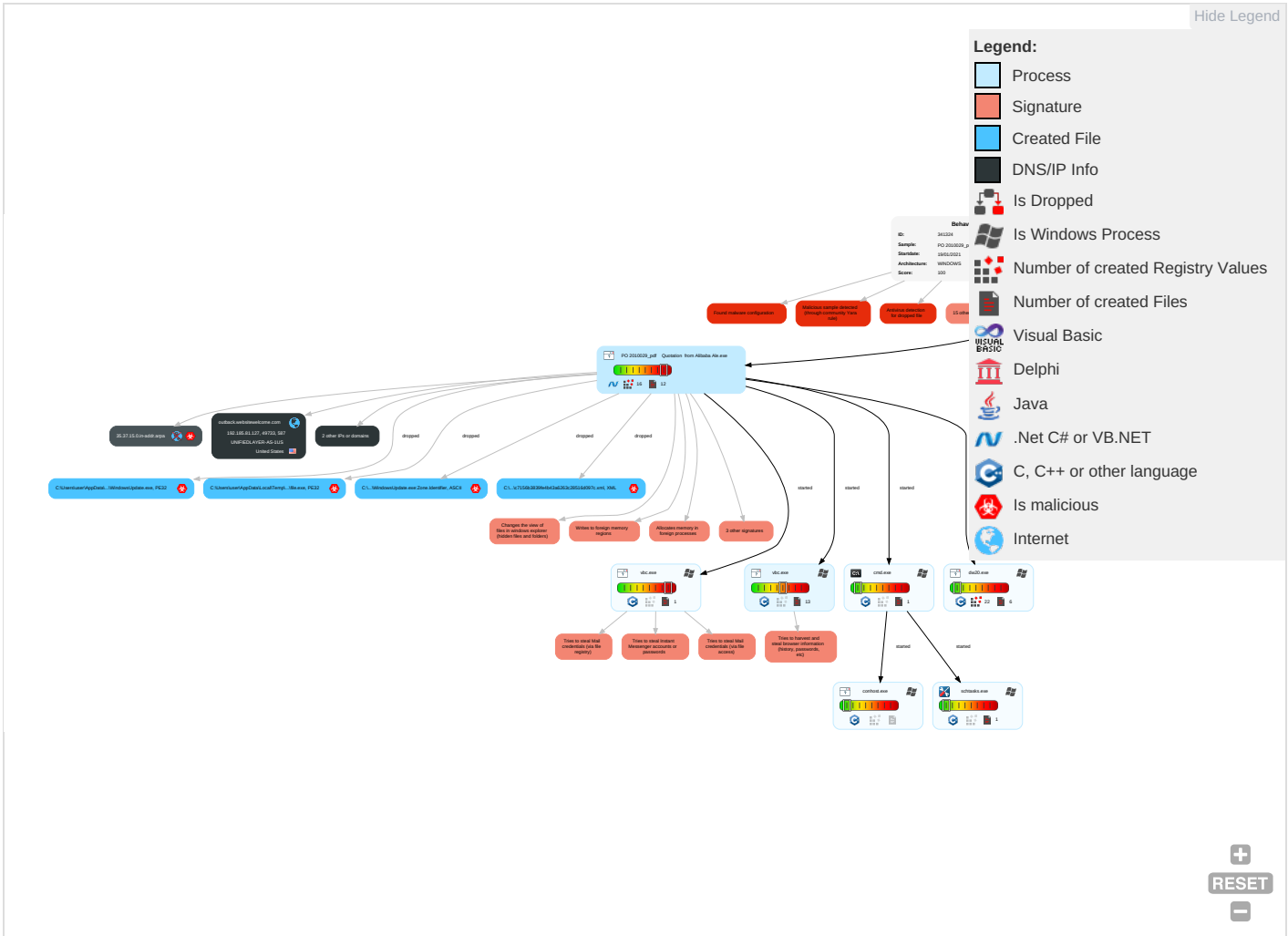
Yara detected HawkEye Keylogger

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 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 2	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Shared Modules 1	Scheduled Task/Job 1	Process Injection 4 1 1	Obfuscated Files or Information 3 1	Credentials in Registry 2	Account Discovery 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Software Packing 1 1	Credentials In Files 1	File and Directory Discovery 2	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 1	DLL Side-Loading 1	LSA Secrets	System Information Discovery 3 9	SSH	Clipboard Data 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 5	DCSync	Security Software Discovery 1 8 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 4 1 1	Proc Filesystem	Virtualization/Sandbox Evasion 5	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	Process Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	System Network Configuration Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB

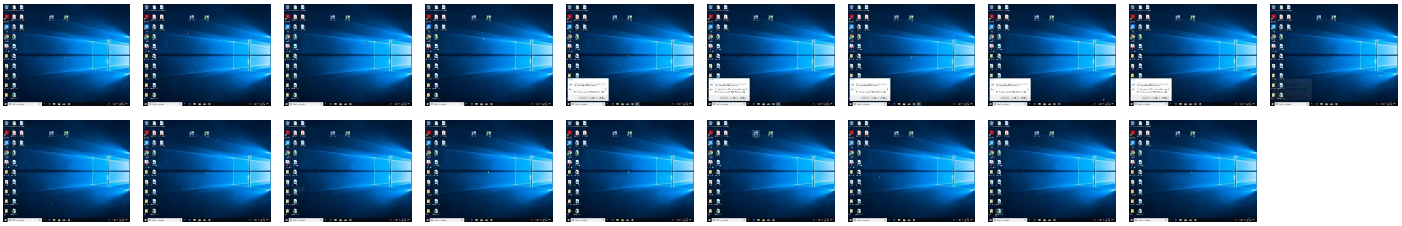
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO 2010029_pdf Quotation from Alibaba Ale.exe	39%	ReversingLabs	Win32.Backdoor.NanoBot	
PO 2010029_pdf Quotation from Alibaba Ale.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\folder\file.exe	100%	Avira	HEUR/AGEN.1138127	
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\folder\file.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\folder\file.exe	39%	ReversingLabs	Win32.Backdoor.NanoBot	
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	39%	ReversingLabs	Win32.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.WindowsUpdate.exe.a00000.1.unpack	100%	Avira	HEUR/AGEN.1138127		Download File
9.0.WindowsUpdate.exe.a00000.0.unpack	100%	Avira	HEUR/AGEN.1138127		Download File
9.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
9.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
14.0.WindowsUpdate.exe.a00000.0.unpack	100%	Avira	HEUR/AGEN.1138127		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
9.2.WindowsUpdate.exe.1ab70000.4.unpack	100%	Avira	TR/Inject.vcoldi		Download File
9.2.WindowsUpdate.exe.1d3a0000.5.unpack	100%	Avira	TR/Inject.vcoldi		Download File
14.2.WindowsUpdate.exe.1620000.2.unpack	100%	Avira	TR/Inject.vcoldi		Download File
9.2.WindowsUpdate.exe.a00000.1.unpack	100%	Avira	HEUR/AGEN.1138127		Download File
14.2.WindowsUpdate.exe.1dd20000.6.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
14.2.WindowsUpdate.exe.1dd20000.6.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
8.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
0.0.PO 2010029_pdf Quotation from Alibaba Ale.exe.be0000.0.unpack	100%	Avira	HEUR/AGEN.1138127		Download File
14.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
14.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
9.2.WindowsUpdate.exe.1d440000.6.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
9.2.WindowsUpdate.exe.1d440000.6.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.1d950000.5.unpack	100%	Avira	TR/Inject.vcoldi		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.1d9e0000.6.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.1d9e0000.6.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.be0000.1.unpack	100%	Avira	HEUR/AGEN.1138127		Download File
14.2.WindowsUpdate.exe.1dc90000.5.unpack	100%	Avira	TR/Inject.vcoldi		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.1b540000.4.unpack	100%	Avira	TR/Inject.vcoldi		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comsig	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/.kL	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/yk?	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://foo.com/fooT	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/el-g	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.com6	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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.jiyu-kobo.co.jp/jp/.kL	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%k	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/%k	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/pk	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://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://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/fk	0%	Avira URL Cloud	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://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://ocsp.sectigo.com03	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ok	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/yk?	0%	Avira URL Cloud	safe	
http://www.fontbureau.comiond	0%	Avira URL Cloud	safe	
http://crl.m	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	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://www.carterandcone.comce	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0/pk	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0/8k~	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
outback.websitewelcome.com	192.185.81.127	true	false		high
whatismyipaddress.com	104.16.155.36	true	false		high
35.37.15.0.in-addr.arpa	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://whatismyipaddress.com/	false		high

URLs from Memory and Binaries

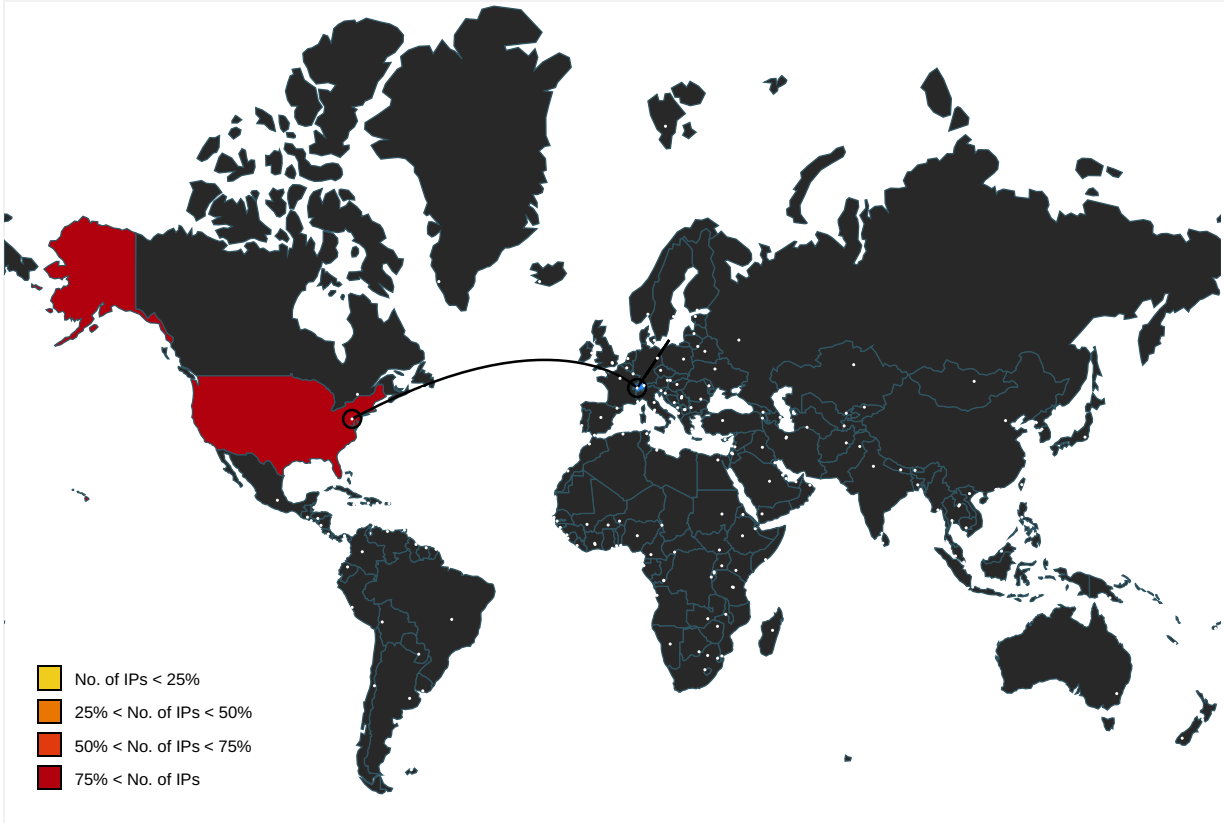
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comsig	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665025745.000000001DF0D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/.kL	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665220746.000000001DF05000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/yk?	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665148269.000000001DF05000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://foo.com/fooT	WindowsUpdate.exe, 00000009.00000002.711861825.000000001B201000.00000004.00000001.sdmp, WindowsUpdate.exe, 0000000E.00000002.727436272.000000001BB0100.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/el-g	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665824786.000000001DF09000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com6	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665025745.000000001DF0D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665025745.000000001DF0D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/.kL	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665824786.000000001DF09000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/%k	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665148269.000000001DF05000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/%k	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665220746.000000001DF05000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com/-	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.756675173.000000001C7C1000.00000004.00000001.sdmp, WindowsUpdate.exe, 00000009.00000002.710741179.000000001AB70000.00000004.00000001.sdmp, WindowsUpdate.exe, 0000000E.00000002.722985777.0000000000400000.00000040.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comgrito	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759400107.000000001DF00000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665880005.000000001DF18000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.yahoo.com/config/login	WindowsUpdate.exe	false		high
http://www.fonts.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/pk	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665824786.000000001DF09000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	WindowsUpdate.exe, 0000000E.000000002.722985777.0000000000400000.00000040.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.760610314.000000001F6D1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.666711909.000000001DF0D000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/fk	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665824786.000000001DF09000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.760610314.000000001F6D1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.agfamonotype.	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.669445042.000000001DF35000.00000004.00000001.sdmp, PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665824786.000000001DF09000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com03	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.760610314.000000001F6D1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/ok	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665824786.000000001DF09000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665824786.000000001DF09000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/yk?	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665333527.000000001DF08000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comiond	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.667302759.000000001DF0D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.m	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.760610314.000000001F6D1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp, PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.663981836.000000001DF15000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.667302759.000000001DF0D000.00000004.00000001.sdmp, PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false		high
http://www.monotype.	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.668830663.000000001DF35000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665824786.000000001DF09000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.759636394.000000001E130000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comce	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665025745.000000001DF0D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0/pk	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665220746.000000001DF05000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0/8k~	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.665824786.000000001DF09000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.81.127	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
104.16.155.36	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	341324
Start date:	19.01.2021
Start time:	08:44:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO 2010029_pdf Quotation from Alibaba Ale.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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winEXE@14/11@3/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.3% (good quality ratio 14.4%) • Quality average: 78.4% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 96% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.64.90.137, 51.104.144.132, 168.61.161.212, 92.122.213.247, 92.122.213.194, 2.20.142.210, 2.20.142.209, 52.254.96.93, 20.54.26.129, 52.147.198.201 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, bn2eap.displaycatalog.md.mp.microsoft.com.akadns.net, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.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 exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:45:06	API Interceptor	36x Sleep call for process: PO 2010029_pdf Quotation from Alibaba Ale.exe modified
08:45:10	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
08:45:19	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
08:45:41	API Interceptor	1x Sleep call for process: dw20.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.155.36	hkaP5RPCGNDVq3Z.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
whatismyipaddress.com	hkaP5RPCGNDVq3Z.exe	Get hash	malicious	Browse	• 104.16.155.36
	B6LNCKjOGt5EmFQ.exe	Get hash	malicious	Browse	• 104.16.154.36
	NDt93WWQwd089H7.exe	Get hash	malicious	Browse	• 104.16.155.36
	JkhR5oeRHA.exe	Get hash	malicious	Browse	• 66.171.248.178
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 104.16.155.36
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• 104.16.154.36
	INQUIRY.exe	Get hash	malicious	Browse	• 104.16.154.36
	Prueba de pago.exe	Get hash	malicious	Browse	• 104.16.155.36
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	http://https://my-alliances.co.uk/	Get hash	malicious	Browse	• 66.171.248.178
	c9o0CtTIYT.exe	Get hash	malicious	Browse	• 104.16.154.36
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• 104.16.155.36
	6JLHKYvboo.exe	Get hash	malicious	Browse	• 104.16.155.36
	jSMd8npgmU.exe	Get hash	malicious	Browse	• 104.16.155.36
	khJdbt0clZ.exe	Get hash	malicious	Browse	• 104.16.154.36
	ZMOKwXqVHO.exe	Get hash	malicious	Browse	• 104.16.154.36
	5Av43Q5IXd.exe	Get hash	malicious	Browse	• 104.16.154.36

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	payment _doc.exe	Get hash	malicious	Browse	• 104.21.89.194
	Statement Of Account.exe	Get hash	malicious	Browse	• 172.67.170.231
	CQcT4Ph03Z.exe	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ucPCgX1NlH.exe	Get hash	malicious	Browse	• 66.235.200.5
	C5XbwziaXz.exe	Get hash	malicious	Browse	• 104.21.64.146
	9gVzvJI8zq.exe	Get hash	malicious	Browse	• 172.67.160.246
	ugGgUEbqio.exe	Get hash	malicious	Browse	• 172.67.160.246
	pY5XEdTwX7.exe	Get hash	malicious	Browse	• 104.21.72.98
	Zz92XfcijKVXcny.exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_53771.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Shipping document.xlsx	Get hash	malicious	Browse	• 172.67.177.177
	FedEx 772584418730.doc	Get hash	malicious	Browse	• 104.21.19.200
	TJyVCvjegT.exe	Get hash	malicious	Browse	• 104.21.19.200
	SHEXD210117S_ShippingDocument_DkD.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	IMG_53771.doc	Get hash	malicious	Browse	• 172.67.188.154
	Pre-order.xlsx	Get hash	malicious	Browse	• 172.67.154.246
	RFQ TK011821.doc	Get hash	malicious	Browse	• 162.159.135.233
	Frq5Dvse34.exe	Get hash	malicious	Browse	• 162.159.133.233
	PC51Jij3Pq.exe	Get hash	malicious	Browse	• 162.159.133.233
	SecuriteInfo.com.Generic.mg.fb5363e0cae04979.exe	Get hash	malicious	Browse	• 172.67.188.154
UNIFIEDLAYER-AS-1US	Statement for T10495.jar	Get hash	malicious	Browse	• 108.167.143.113
	xPkiX7vwNVqQf9I.exe	Get hash	malicious	Browse	• 108.179.230.69
	CQcT4Ph03Z.exe	Get hash	malicious	Browse	• 192.185.4.24
	yxYmHtT7uT.exe	Get hash	malicious	Browse	• 162.241.60.214
	TAg7hqAEaq.exe	Get hash	malicious	Browse	• 108.167.140.161
	9gVzvJI8zq.exe	Get hash	malicious	Browse	• 162.241.217.138
	Y75vU558UfuGbzM.exe	Get hash	malicious	Browse	• 192.185.35.70
	Materials.exe	Get hash	malicious	Browse	• 192.185.34.202
	orden pdf.exe	Get hash	malicious	Browse	• 192.185.5.166
	dg9PJ79P3G.exe	Get hash	malicious	Browse	• 192.185.163.193
	180120211200.exe	Get hash	malicious	Browse	• 50.87.193.205
	5YfNeXk1f0wrxXm.exe	Get hash	malicious	Browse	• 192.185.35.243
	YUAN PAYMENT.exe	Get hash	malicious	Browse	• 162.214.103.133
	TEC20201601.exe	Get hash	malicious	Browse	• 162.214.103.133
	Materials.exe	Get hash	malicious	Browse	• 74.220.199.6
	file_012021_5_2279069.doc	Get hash	malicious	Browse	• 50.116.93.238
	Payment Advice.xlsx	Get hash	malicious	Browse	• 50.87.153.159
	Payment Advice.xlsx	Get hash	malicious	Browse	• 50.87.153.159
	Packing list #U2022 Invoice #U2022 Country of origin.exe	Get hash	malicious	Browse	• 50.87.196.173
	Draft FCR-HBL.exe	Get hash	malicious	Browse	• 192.185.0.218

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_I3UYUDMLOPVYGRAZ_ff5d37c08782585231182226e219de1bf556ec8_00000000_12aa1aeb\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):	18526
Entropy (8bit):	3.7595009509515065

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_I3UYUDMLOPVYGRAZ_ff5d37c08782585231182226e219de1bf556ec8_00000000_12aa1aeb\Report.wer	
Encrypted:	false
SSDEEP:	192:+U+vhLWMBVm03jjy3qhb91t4No8XN1Dzv2Hk0K+Z5JNKU/u7s5S274It0bj:+hLNVjADfv1eKU/u7s5X4ItU
MD5:	E0234DDB8DCD0049C26D45270E302670
SHA1:	8B38E799954AB55705B1C9FA05224A68462D1484
SHA-256:	E38FEDC1A75B6FE1189FA7A986D9D349202208C8AE591BD99C8DFD279095FD34
SHA-512:	82FBAF04F07502D9967F7C3E049E0FD4D3B4476CF5B383BC2F5A5468522C4A5583F5E65757D9FAD230A0CCB71E822E040A8A0194BBC454F81DF2236601DD21D
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.=.1.3.2.5.5.5.1.5.9.0.7.1.9.8.6.3.1.9.....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.=.1.3.2.5.5.5.1.5.9.0.8.7.4.5.5.2.3.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.9.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.1.6.a.a.b.b.3.-.0.0.7.b.-.4.2.6.4.-.a.d.e.3.-.0.a.8.d.f.0.d.d.4.b.4.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.2.8.-.0.0.0.1.-.0.0.1.b.-.c.f.4.4.-.5.0.f.c.3.6.e.e.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.e.c.5.e.b.d.5.8.d.1.9.3.3.b.e.2.9.b.8.8.7.2.0.2.0.b.9.e.c.0.5.8.0.0.0.0.f.f.f.f.!.0.0.0.0.8.3.4.0.7.c.5.d.0.7.5.e.7.a.8.6.6.4.b.d.5.0.b.1.c.f.e.6.d.8.2.e.b.9.3.6.3.4.2.e.!.P.O. .2.0.1.0.0.2.9._.p.d.f. . . . .Q.u.o.t.a.t.i.o.n. . .f.r.o.m. .A.l.i.b.a.b.a. .A.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.1././.1.8.:.2.0.:.1.6.:.5.3.!.0.!.P.O. .2.0.1.0.0.2.9._.p.d.f. . . . .Q.u.o.t.a.t.i.o.n. . .f.r.o.m.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9679.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):	7790
Entropy (8bit):	3.7103725108859273
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiNCG6fnanWojq6YrVSUyFxDWgmfZ4X1Sb+p1nbpE1fpNjm:RrlsNiR6au6YJSUyFkgmfGX1S+nbpufm
MD5:	4663DEC090868E16DA7F5BCA796C9E56
SHA1:	CCD5A6093B43EBECDBBE73CA9846324728F1060F
SHA-256:	161D1F741C110B43374FE458DC88E13DBC776FBF264B8119304EEA6D3A7F364C
SHA-512:	C67FF00C65C6F75B3A5122DC111F0D7BDD4385EE2970F0624A89B0F5042D91017EFB41BD2111896DCDAF82F1390ADCDD4A0FA7589ED47B46A35B2E8FD7C147D
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9745.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):	4727
Entropy (8bit):	4.524625212788249
Encrypted:	false
SSDEEP:	48:cvIwSD8zs3JgtWl9qPkWSC8BIa8fm8M4JFKgxFt+q8v7pxz6z4d:uITfZtP9SNmvJFKCK9J04d
MD5:	09230AF117101F309F1D2A9272EC4DD6
SHA1:	49371E06E109D22646A4A01042B3A6151AE2642E
SHA-256:	B88430E87A0873ED3F7677059408CE9AF0B3543E3186BC9D0E61FE5A64841C04
SHA-512:	5BD3418B89D7F41D7D39DBA4AD76F6B5440A04C8E8C4EFF30695A76007DC4694222B7303DADD1E2B679F3BD3D5A63CE703C80ECDF4E5F9BC7D2F2159020CAD6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="823255" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\WindowsUpdate.exe.log	
Process:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	916
Entropy (8bit):	5.282390836641403
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\WindowsUpdate.exe.log	
SSDEEP:	24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2+:MwLLD2Y9h3go2rxxAcAO6ox+g2+
MD5:	5AD8E7ABEADADAC4CE06FF693476581A
SHA1:	81E42A97BBE3D7DE8B1E8B54C2B03C48594D761E
SHA-256:	BAA1A28262BA27D51C3A1FA7FB0811AD1128297ABB2EDCCC785DC52667D2A6FD
SHA-512:	7793E78E84AD36CE65B5B1C015364E340FB9110FAF199BC0234108CE9BCB1AEDACBD25C6A012AC99740E08BEA5E5C373A88E553E47016304D8AE6AEEAB58EE FF
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages _v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a909923 7864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System .Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\c7156b3839fe4b43a6263c28516d097c.xml	
Process:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1287
Entropy (8bit):	5.212090243419571
Encrypted:	false
SSDEEP:	24:2do4+S8TcqdQrsgFwvpIrovlgU3ODOiIQRvh7hwZgvw43aVdQfL3Tbn:c+XBQYpIrovl33ODOiLdKZgfo6L3/
MD5:	1F2AB60BB7267870886B92CD09BDD40F
SHA1:	B1FEB45A9F57DA9201C09C6BDF68A85F6B3B357C
SHA-256:	954E70C360613EE7521DC580232C08E22897A247F0EE9D8F1F137D5D44DEDAD6
SHA-512:	0C09CC3F8AA004537497320CBCEE4843141955268A797114E668FBB329AD332CAD378C0422048DEB3676CCA04FE4D475644DDB58F0C7193E84C4AD9866EF38E
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version = "1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.<RegistrationInfo>.<Date>2015-09-27 T14:27:44.8929027</Date > .<Author>992547\user</Author>.</RegistrationInfo>.<Triggers>.<LogonTrigger>.<Enabled>true</Enabled>.<UserId>992547\user</UserId>. </LogonTrigger>.<RegistrationTrigger>.<Enabled>false</Enabled>.</RegistrationTrigger>.</Triggers>.<Principals>.<Principal id="Author">.<UserId>992547\user< /UserId>.<LogonType>InteractiveToken</LogonType>.<RunLevel>LeastPrivilege</RunLevel>.</Principal>.</Principals>.<Settings>.<MultipleInstancesPolicy>St opExisting</MultipleInstancesPolicy>.<AllowHardTerminate>false</AllowHardTerminate>.<StartWhenAvailable>true</StartWhenAvailable>.<RunOnlyIfNetworkAva ilable>false</RunOnlyIfNetworkAvailable>.<IdleSettings>.<StopOnIdleEnd>true</StopOnIdleEnd>.<RestartOnIdle>false</RestartOnIdle>.</IdleSettings>.<Allo wStartOnDemand>true</AllowStartOnDemand>.<Enabled>true</Enabled>.<Hidden>fals

C:\Users\user\AppData\Local\Temp\folder\file.exe	
Process:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1086474
Entropy (8bit):	7.578465944506682
Encrypted:	false
SSDEEP:	24576:S8W4T17vgKzzHA3VJTMrxwpO7GAa18Xj:SU7JAlJTUme
MD5:	61854EA00B96528123E9A176BC0377BF
SHA1:	211FAF0D06BC47276DB738914C4D9B03DB1CA0F5
SHA-256:	28615FFA1BD821066848828F83A436587BD4FF8DA5F206B1EFAB09988FDA27C7
SHA-512:	9211791D4911B6619AE2EE69904013902E38E35A6852FDE1D667CD4D941228A289C3AD25A556B4CC78E7CCC65725E9972E8F5682504D9DACB4EA4C579173281F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8...|..|..|....v.....n..._#.....o....a.....n.....m..|.....}.....}....}..Rich|.... .....PE..L.....`.....@.....@.....F..... .....`..<,...6.....06..@.....`..... .....text...:..... ..`.rdata.....@..@.data...4....`.....B.....@....gfids..t.....N.....@..@.rsrc... .....P.....@..@.reloc..<,...`..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\holderwb.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0

C:\Users\user\AppData\Local\Temp\holderwb.txt	
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Roaming\WindowsUpdate.exe	
Process:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1086464
Entropy (8bit):	7.578501414918202
Encrypted:	false
SSDEEP:	24576:S8W4T17vgKzzHA3VJTMrxwpO7GAa18XjX:SU7JAlJTUmej
MD5:	134BF4DDD2A72C5C396647F7037AF0E1
SHA1:	83407C5D075E7A8664BD50B1CFE6D82EB936342E
SHA-256:	76DB811BCA515B8C2F782394E24B4BBCE6269211F6E8971B4897BDFFD554303B
SHA-512:	E010172192C7A0EE2DB793B01D0C90644DF0AEDA6A475598B42C6CE8ABC67195C3A807D529CFA6755905FA1ADCB25FC2EB80B4FCC7DAB0D42380B81D5726C 12
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8...|..|..|....v.....n..._#.....o....a.....n.....m..|.....}.....}....}..Rich|.... .....PE..L.....`.....@.....@.....F..... .....`..<,...6.....06..@.....`..... .....text...:..... ..`.rdata.....@..@.data...4....`.....B.....@....gfids..t.....N.....@..@.rsrc... .....P.....@..@.reloc..<,...`..... .....@..B..... .....

C:\Users\user\AppData\Roaming\WindowsUpdate.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:wRn:wR
MD5:	08425B881BCDE94A383CD258CEA331BE
SHA1:	035190E86082BBA15DAF822EA166639C626F9578
SHA-256:	C89351F5FEE4406D095BB248EDAF8A2C01BD57BC6CB4DCF45EA28EB2B4EF1A51
SHA-512:	8ACA3AF257A30AB72FFFD2FCE1CDAA55B64951E8DF1054BD21A2126FE22D61D073424A6A1F672B56AC2FBEEFBE89F362EE2DF747A19C1E9BE7488B283CBB1 FA2
Malicious:	false
Preview:	6184

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.726683293133492
Encrypted:	false
SSDEEP:	3:oNt+WfW1qOL/kiRMQFLTzxl0C:oNwvgOLHXLvxl0C
MD5:	82A4BD3798C0A5581741E25F32F233E7
SHA1:	73554D6548669CE4F8594A02863C6F4C36607D3B
SHA-256:	095CB76FECF1095B4D4AB724B0E29039E00BA8388CCCA9899D0AB559C7167718
SHA-512:	D578CB85F5DDB495AD0E420E8038E376F696E7556B731479284852549FA1987E8BBF06E10BBCF96C1733FE9E3F2C7C1E179473074B9A91E10F00BE04B80E87F6
Malicious:	false
Preview:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.578501414918202
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	PO 2010029_pdf Quotation from Alibaba Ale.exe
File size:	1086464
MD5:	134bf4ddd2a72c5c396647f7037af0e1
SHA1:	83407c5d075e7a8664bd50b1cfe6d82eb936342e
SHA256:	76db811bca515b8c2f782394e24b4bbce6269211f6e8971b4897bdffd554303b
SHA512:	e010172192c7a0ee2db793b01d0c90644df0aeda6a475598b42c6ce8abc67195c3a807d529cfa6755905fa1adcb25fc2eb80b4fcc7dab0d42380b81d5726c712
SSDEEP:	24576:S8W4T17vgKzzHA3VJTMrxwpO7GAa18XjX:SU7JAlJTUmej
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8...|...|...|.....v.....n...._#.....o.....a.....n.....m...|.....}.....}.....}...Rich|.....

File Icon

Icon Hash:	6eeccccd6d2f2f2

Static PE Info

General

Entrypoint:	0x401308
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6005ECB5 [Mon Jan 18 20:16:53 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0

General

File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	3f85ebb67bac58f72de974a91d40889a

Entrypoint Preview

Instruction
call 00007F8624A94F08h
jmp 00007F8624A949C5h
push 00000014h
push 00453B58h
call 00007F8624A95257h
push 00000001h
call 00007F8624A94CD0h
pop ecx
test al, al
jne 00007F8624A949C9h
push 00000007h
call 00007F8624A94FF7h
xor bl, bl
mov byte ptr [ebp-19h], bl
and dword ptr [ebp-04h], 00000000h
call 00007F8624A94BB9h
mov byte ptr [ebp-24h], al
mov eax, dword ptr [00456A80h]
xor ecx, ecx
inc ecx
cmp eax, ecx
je 00007F8624A9499Eh
test eax, eax
jne 00007F8624A94A0Bh
mov dword ptr [00456A80h], ecx
push 0044B290h
push 0044B270h
call 00007F8624AB5E2Fh
pop ecx
pop ecx
test eax, eax
je 00007F8624A949D3h
mov dword ptr [ebp-04h], FFFFFFFEh
mov eax, 000000FFh
jmp 00007F8624A94ABBh
push 0044B26Ch
push 0044B264h
call 00007F8624AB5DADh
pop ecx
pop ecx
mov dword ptr [00456A80h], 00000002h
jmp 00007F8624A949C7h
mov bl, cl
mov byte ptr [ebp-19h], bl
push dword ptr [ebp-24h]
call 00007F8624A94DA7h
pop ecx
call 00007F8624A94F6Eh
mov esi, eax
xor edi, edi
cmp dword ptr [esi], edi
je 00007F8624A949DCh
push esi
call 00007F8624A94D09h
pop ecx

Instruction
test al, al
je 00007F8624A949D1h
push edi
push 00000002h
push edi
mov esi, dword ptr [esi]
mov ecx, esi
call 00007F8624A95197h
call esi

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x546dc	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x59000	0x1cd20	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x76000	0x2c3c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x53610	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x53630	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x4b000	0x260	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4993a	0x49a00	False	0.472012945671	data	6.61525137664	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x4b000	0xa3aa	0xa400	False	0.45107660061	SysEx File - Mesosha	5.24006298806	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x56000	0x1f34	0xc00	False	0.171549479167	DOS executable (block device driver \277DN)	2.22955442271	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x58000	0x174	0x200	False	0.341796875	data	2.11448669888	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x59000	0x1cd20	0x1ce00	False	0.270706507035	data	5.15178641696	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x76000	0x2c3c	0x2e00	False	0.783797554348	data	6.6314339311	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x591c0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x5b768	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x5c810	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x5cc78	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x60ea0	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_RCDATA	0x71718	0x4605	data	English	United States
RT_GROUP_ICON	0x716c8	0x4c	data	English	United States

Imports

DLL	Import
KERNEL32.dll	Heap32Next, LoadResource, FreeLibrary, GetLongPathNameA, CancelIo, BuildCommDCBAndTimeoutsA, ExitThread, GlobalFindAtomW, GetStdHandle, HeapAlloc, GetProcessHeap, SetConsoleCursorPosition, DecodePointer, EncodePointer, SetEndOfFile, WriteConsoleW, HeapReAlloc, HeapSize, GetTimeZoneInformation, SetConsoleMode, ReadConsoleInputW, ReadConsoleInputA, PeekConsoleInputA, GetNumberOfConsoleInputEvents, CreateFileW, SetConsoleCtrlHandler, GetStringTypeW, SetStdHandle, SetEnvironmentVariableW, SetEnvironmentVariableA, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, GetCommandLineA, GetCPInfo, GetOEMCP, IsValidCodePage, FindNextFileW, FindNextFileA, FindFirstFileExW, FindFirstFileExA, FindClose, MoveFileExW, GetFileAttributesExW, CreateProcessW, CreateProcessA, GetExitCodeProcess, WaitForSingleObject, GetCurrentThread, DeleteFileW, CloseHandle, GetConsoleCP, FlushFileBuffers, EnumSystemLocalesW, GetUserDefaultLCID, IsValidLocale, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, IsProcessorFeaturePresent, GetModuleHandleW, GetCurrentProcess, TerminateProcess, InterlockedPushEntrySList, InterlockedFlushSList, RtlUnwind, GetLastError, SetLastError, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetProcAddress, LoadLibraryExW, ExitProcess, GetModuleHandleExW, ReadFile, QueryPerformanceFrequency, MultiByteToWideChar, WriteFile, GetModuleFileNameW, GetModuleFileNameA, WideCharToMultiByte, GetACP, HeapFree, SetFilePointerEx, GetConsoleMode, ReadConsoleW, GetFileType, OutputDebugStringA, OutputDebugStringW, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, RaiseException
SHELL32.dll	DragQueryFile, Shell_NotifyIconA
MSWSOCK.dll	EnumProtocolsA, GetNameByTypeW, GetServiceA, getnetbyname
mscms.dll	EnumColorProfilesW, UnregisterCMMA, CreateProfileFromLogColorSpaceW, GetPS2ColorRenderingIntent, EnumColorProfilesA
msi.dll	
WS2_32.dll	gethostbyaddr, WSCInstallNameSpace, WSALookupServiceNextA, WSARemoveServiceClass
ODBC32.dll	VRetrieveDriverErrorsRowCol
USER32.dll	GetDC, GrayStringW

Possible Origin

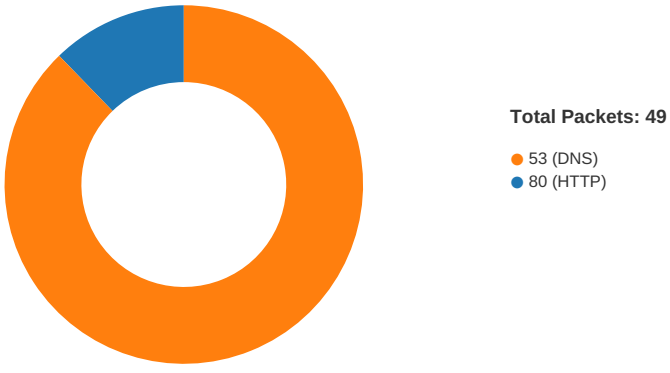
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/19/21-08:45:05.791595	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49728	104.16.155.36	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 08:45:05.703176975 CET	49728	80	192.168.2.4	104.16.155.36
Jan 19, 2021 08:45:05.743170023 CET	80	49728	104.16.155.36	192.168.2.4
Jan 19, 2021 08:45:05.744184017 CET	49728	80	192.168.2.4	104.16.155.36
Jan 19, 2021 08:45:05.745187044 CET	49728	80	192.168.2.4	104.16.155.36
Jan 19, 2021 08:45:05.785067081 CET	80	49728	104.16.155.36	192.168.2.4
Jan 19, 2021 08:45:05.791594982 CET	80	49728	104.16.155.36	192.168.2.4
Jan 19, 2021 08:45:05.842942953 CET	49728	80	192.168.2.4	104.16.155.36
Jan 19, 2021 08:45:21.424724102 CET	49728	80	192.168.2.4	104.16.155.36
Jan 19, 2021 08:45:21.464867115 CET	80	49728	104.16.155.36	192.168.2.4
Jan 19, 2021 08:45:21.464962959 CET	49728	80	192.168.2.4	104.16.155.36
Jan 19, 2021 08:45:21.578411102 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:21.735934973 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:21.736063004 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:22.062592983 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:22.062877893 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:22.220532894 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:22.220808983 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:22.381907940 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:22.422467947 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:22.589298964 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:22.756324053 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:22.756364107 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:22.756386042 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:22.756402016 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:22.756438017 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:22.756489992 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:22.758081913 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:22.795583010 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:22.954921961 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:23.000612974 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:23.545238972 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:23.703063011 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:23.704037905 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:23.862426043 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:23.863172054 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:24.027528048 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:24.028479099 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:24.186069012 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:24.186877966 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:24.350517035 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:24.351160049 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:24.508589983 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:24.509702921 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:24.509939909 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:24.510049105 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:24.510185957 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:24.510272026 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:24.510390043 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:24.667107105 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:24.667150021 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:24.667190075 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:24.667313099 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:24.667359114 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:24.667511940 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:24.667937994 CET	587	49733	192.185.81.127	192.168.2.4
Jan 19, 2021 08:45:24.719496965 CET	49733	587	192.168.2.4	192.185.81.127
Jan 19, 2021 08:45:47.959813118 CET	49733	587	192.168.2.4	192.185.81.127

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 08:44:57.608969927 CET	49714	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:44:57.659780979 CET	53	49714	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:01.339618921 CET	58028	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 08:45:01.387502909 CET	53	58028	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:03.010580063 CET	53097	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:03.058511019 CET	53	53097	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:05.358360052 CET	49257	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:05.417759895 CET	53	49257	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:05.627551079 CET	62389	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:05.678183079 CET	53	62389	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:09.557236910 CET	49910	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:09.605043888 CET	53	49910	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:15.021019936 CET	55854	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:15.069343090 CET	53	55854	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:21.466996908 CET	64549	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:21.535942078 CET	53	64549	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:23.510432005 CET	63153	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:23.558269978 CET	53	63153	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:24.895240068 CET	52991	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:24.952120066 CET	53	52991	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:25.947082996 CET	53700	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:25.994999886 CET	53	53700	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:28.761084080 CET	51726	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:28.805495024 CET	56794	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:28.818804026 CET	53	51726	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:28.861666918 CET	53	56794	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:30.320110083 CET	56534	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:30.367938995 CET	53	56534	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:31.216104031 CET	56627	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:31.274847031 CET	53	56627	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:34.498747110 CET	56621	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:34.549451113 CET	53	56621	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:42.069797993 CET	63116	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:42.127693892 CET	53	63116	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:45.354842901 CET	64078	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:46.393657923 CET	64078	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:47.456290960 CET	64078	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:47.515433073 CET	53	64078	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:48.043181896 CET	64801	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:48.114690065 CET	53	64801	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:48.422040939 CET	61721	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:48.517926931 CET	53	61721	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:50.022212982 CET	51255	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:50.084577084 CET	53	51255	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:51.780360937 CET	61522	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:51.839528084 CET	53	61522	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:52.757272959 CET	52337	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:52.813530922 CET	53	52337	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:53.825488091 CET	55046	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:53.881767988 CET	53	55046	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:54.906923056 CET	49612	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:54.954777956 CET	53	49612	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:56.174213886 CET	49285	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:56.230391979 CET	53	49285	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:57.559679031 CET	50601	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:57.620481014 CET	53	50601	8.8.8.8	192.168.2.4
Jan 19, 2021 08:45:58.419656992 CET	60875	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:45:58.470292091 CET	53	60875	8.8.8.8	192.168.2.4
Jan 19, 2021 08:46:00.960335970 CET	56448	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:46:01.017916918 CET	53	56448	8.8.8.8	192.168.2.4
Jan 19, 2021 08:46:06.678324938 CET	59172	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:46:06.729052067 CET	53	59172	8.8.8.8	192.168.2.4
Jan 19, 2021 08:46:07.489012957 CET	62420	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:46:07.536947012 CET	53	62420	8.8.8.8	192.168.2.4
Jan 19, 2021 08:46:09.761728048 CET	60579	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:46:09.809808016 CET	53	60579	8.8.8.8	192.168.2.4
Jan 19, 2021 08:46:11.707901001 CET	50183	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 08:46:11.756141901 CET	53	50183	8.8.8.8	192.168.2.4
Jan 19, 2021 08:46:13.527553082 CET	61531	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:46:13.586816072 CET	53	61531	8.8.8.8	192.168.2.4
Jan 19, 2021 08:46:17.784444094 CET	49228	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:46:17.835203886 CET	53	49228	8.8.8.8	192.168.2.4
Jan 19, 2021 08:46:18.612889051 CET	59794	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:46:18.660845041 CET	53	59794	8.8.8.8	192.168.2.4
Jan 19, 2021 08:46:19.908061981 CET	55916	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:46:19.964338064 CET	53	55916	8.8.8.8	192.168.2.4
Jan 19, 2021 08:46:23.141788960 CET	52752	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:46:23.192622900 CET	53	52752	8.8.8.8	192.168.2.4
Jan 19, 2021 08:46:24.768100023 CET	60542	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:46:24.818840027 CET	53	60542	8.8.8.8	192.168.2.4
Jan 19, 2021 08:46:32.575464010 CET	60689	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:46:32.623409986 CET	53	60689	8.8.8.8	192.168.2.4
Jan 19, 2021 08:46:33.881192923 CET	64206	53	192.168.2.4	8.8.8.8
Jan 19, 2021 08:46:33.929156065 CET	53	64206	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 08:45:05.358360052 CET	192.168.2.4	8.8.8.8	0xb503	Standard query (0)	35.37.15.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jan 19, 2021 08:45:05.627551079 CET	192.168.2.4	8.8.8.8	0x3a6	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Jan 19, 2021 08:45:21.466996908 CET	192.168.2.4	8.8.8.8	0x15eb	Standard query (0)	outback.we bsitewelco me.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 08:45:05.417759895 CET	8.8.8.8	192.168.2.4	0xb503	Name error (3)	35.37.15.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Jan 19, 2021 08:45:05.678183079 CET	8.8.8.8	192.168.2.4	0x3a6	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Jan 19, 2021 08:45:05.678183079 CET	8.8.8.8	192.168.2.4	0x3a6	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Jan 19, 2021 08:45:21.535942078 CET	8.8.8.8	192.168.2.4	0x15eb	No error (0)	outback.we bsitewelco me.com		192.185.81.127	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- whatismyipaddress.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49728	104.16.155.36	80	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 08:45:05.745187044 CET	555	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 08:45:05.791594982 CET	556	IN	HTTP/1.1 403 Forbidden Date: Tue, 19 Jan 2021 07:45:05 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=de8a777b8e6b7c58309aef25df64241f71611042305; expires=Thu, 18-Feb-21 07:45:05 GMT; path=/; domain=.whatismyipaddress.com; HttpOnly; SameSite=Lax; Secure cf-request-id: 07bb33cef100009748d0248000000001 Server: cloudflare CF-RAY: 613eef2b1e229748-FRA Data Raw: 65 72 72 6f 72 20 63 6f 64 65 3a 20 31 30 32 30 Data Ascii: error code: 1020

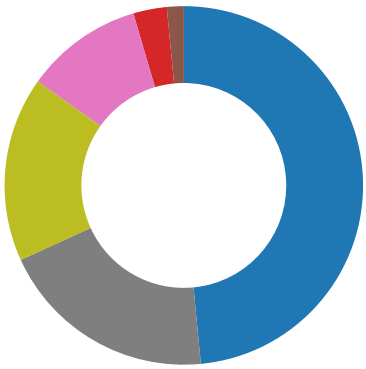
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 19, 2021 08:45:22.062592983 CET	587	49733	192.185.81.127	192.168.2.4	220-outback.websitewelcome.com ESMTP Exim 4.93 #2 Tue, 19 Jan 2021 01:45:21 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 19, 2021 08:45:22.062877893 CET	49733	587	192.168.2.4	192.185.81.127	EHLO 992547
Jan 19, 2021 08:45:22.220532894 CET	587	49733	192.185.81.127	192.168.2.4	250-outback.websitewelcome.com Hello 992547 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 19, 2021 08:45:22.220808983 CET	49733	587	192.168.2.4	192.185.81.127	STARTTLS
Jan 19, 2021 08:45:22.381907940 CET	587	49733	192.185.81.127	192.168.2.4	220 TLS go ahead

Code Manipulations

Statistics

Behavior



- PO 2010029_pdf Quotation from Al...
- cmd.exe
- conhost.exe
- schtasks.exe
- dw20.exe
- vbc.exe
- vbc.exe
- WindowsUpdate.exe
- WindowsUpdate.exe

Click to jump to process

System Behavior

Analysis Process: PO 2010029_pdf Quotation from Alibaba Ale.exe PID: 6184 Parent PID: 5756

General

Start time:	08:44:58
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe'
Imagebase:	0xbe0000
File size:	1086464 bytes
MD5 hash:	134BF4DDD2A72C5C396647F7037AF0E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.758588141.000000001D9E2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.758588141.000000001D9E2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.758588141.000000001D9E2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.758588141.000000001D9E2000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.758588141.000000001D9E2000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.755347738.000000001B540000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.755347738.000000001B540000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.755347738.000000001B540000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.755347738.000000001B540000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.755347738.000000001B540000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.756675173.000000001C7C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.756675173.000000001C7C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.756675173.000000001C7C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.756675173.000000001C7C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.756675173.000000001C7C1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.757447737.000000001D8CB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.757447737.000000001D8CB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.757447737.000000001D8CB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.757447737.000000001D8CB000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.757447737.000000001D8CB000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.758041850.000000001D950000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.758041850.000000001D950000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.758041850.000000001D950000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.758041850.000000001D950000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.758041850.000000001D950000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.755565035.000000001B7C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.755565035.000000001B7C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.755565035.000000001B7C1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.749770349.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.749770349.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.749770349.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.749770349.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.749770349.0000000000400000.00000040.00000001.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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	722760AC	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	722760AC	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	722760AC	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	118BDFF	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	118BDFF	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	1DAE5068	CopyFileW
C:\Users\user\AppData\Roaming\WindowsUpdate.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	1DAE5068	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	1DAE5D22	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	1DAE5D22	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	36 31 38 34	6184	success or wait	1	1DAE0163	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	72	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 50 4f 20 32 30 31 30 30 32 39 5f 70 64 66 20 20 20 20 51 75 6f 74 61 74 69 6f 6e 20 20 66 72 6f 6d 20 41 6c 69 62 61 62 61 20 41 6c 65 2e 65 78 65	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe	success or wait	1	1DAE0163	WriteFile
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 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 38 9e 8a d9 7c ff e4 8a 7c ff e4 8a 7c ff e4 8a 0f 9d e7 8b 76 ff e4 8a 0f 9d e1 8b ce ff e4 8a 0f 9d e0 8b 6e ff e4 8a e2 5f 23 8a 7f ff e4 8a d1 a1 e7 8b 6f ff e4 8a d1 a1 e1 8b 61 ff e4 8a d1 a1 e0 8b 6e ff e4 8a 0f 9d e5 8b 6d ff e4 8a 7c ff e5 8a ec ff e4 8a c9 a1 ec 8b 7d ff e4 8a c9 a1 1b 8a 7d ff e4 8a c9 a1 e6 8b 7d ff e4 8a 52 69 63 68 7c ff e4 8a 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....8...|...|...|.....v. .....n...._#..... o.....a.....n.....m...|. .....}.....}.....}... Rich|.....	success or wait	5	1DAE5068	CopyFileW
C:\Users\user\AppData\Roaming\ WindowsUpdate.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	1DAE5068	CopyFileW

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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	1DAE0163	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1DAE0163	ReadFile
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	1DAE0163	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	1DAE0163	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	1DAE0163	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_MSIL\System.Runtime.Remoting\2.0.0.0 __b77a5c561934e089\System.Runtime.Remoting.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_MSIL\System.Runtime.Remoting\2.0.0.0 __b77a5c561934e089\System.Runtime.Remoting.dll	unknown	512	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7234BF06	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Windows Update	unicode	C:\Users\user\AppData\Roaming\WindowsUpdate.exe	success or wait	1	1DAE5242	RegSetValueExW

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	1DAE4AFE	RegSetValueExW

Analysis Process: cmd.exe PID: 1904 Parent PID: 6184

General

Start time:	08:44:59
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c schtasks /Create /TN file /XML 'C:\Users\user\AppData\Local\Temp\c7156b3839fe4b43a6263c28516d097c.xml'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 6116 Parent PID: 1904

General

Start time:	08:45:00
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: schtasks.exe PID: 1836 Parent PID: 1904

General

Start time:	08:45:00
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /Create /TN file /XML 'C:\Users\user\AppData\Local\Temp\c7156b3839fe4b43a6263c28516d097c.xml'
Imagebase:	0x1180000
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\c7156b3839fe4b43a6263c28516d097c.xml	unknown	2	success or wait	1	118AB22	ReadFile
C:\Users\user\AppData\Local\Temp\c7156b3839fe4b43a6263c28516d097c.xml	unknown	1288	success or wait	1	118ABD9	ReadFile

Analysis Process: dw20.exe PID: 4856 Parent PID: 6184

General

Start time:	08:45:06
Start date:	19/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2532
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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: vbc.exe PID: 5896 Parent PID: 6184

General

Start time:	08:45:09
Start date:	19/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.683246916.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EFC	CreateFileA

Analysis Process: vbc.exe PID: 5556 Parent PID: 6184

General

Start time:	08:45:09

Start date:	19/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.687360804.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holderwb.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	407175	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	2	ff fe	..	success or wait	1	407BCF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	100	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	100	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	2048	success or wait	1	414E52	ReadFile

Analysis Process: WindowsUpdate.exe PID: 6748 Parent PID: 3424

General

Start time:	08:45:19
Start date:	19/01/2021
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\WindowsUpdate.exe'
Imagebase:	0xa00000
File size:	1086464 bytes
MD5 hash:	134BF4DDD2A72C5C396647F7037AF0E1
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: 00000009.00000002.710741179.000000001AB70000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000002.710741179.000000001AB70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000009.00000002.710741179.000000001AB70000.00000004.00000001.sdmp, Author: Joe Security

	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000009.00000002.710741179.000000001AB70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000009.00000002.710741179.000000001AB70000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000009.00000002.706683978.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000002.706683978.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000009.00000002.706683978.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000009.00000002.706683978.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000009.00000002.706683978.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000009.00000002.712471863.000000001D442000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000002.712471863.000000001D442000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000009.00000002.712471863.000000001D442000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000009.00000002.712471863.000000001D442000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000009.00000002.712471863.000000001D442000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000009.00000002.712000579.000000001C201000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000002.712000579.000000001C201000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000009.00000002.712000579.000000001C201000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000009.00000002.712000579.000000001C201000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000009.00000002.712000579.000000001C201000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000009.00000002.712159981.000000001D3A0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000002.712159981.000000001D3A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000009.00000002.712159981.000000001D3A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000009.00000002.712159981.000000001D3A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000009.00000002.712159981.000000001D3A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000009.00000003.706344481.000000001AD20000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000003.706344481.000000001AD20000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000009.00000003.706344481.000000001AD20000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000009.00000003.706344481.000000001AD20000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000009.00000003.706344481.000000001AD20000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 39%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	722760AC	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	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\WindowsUpdate.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722634A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\WindowsUpdate.exe.log	unknown	916	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7254A33A	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	722A5544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	1D560163	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1D560163	ReadFile

Analysis Process: WindowsUpdate.exe PID: 6204 Parent PID: 3424

General

Start time:	08:45:27
Start date:	19/01/2021
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\WindowsUpdate.exe'
Imagebase:	0xa00000
File size:	1086464 bytes
MD5 hash:	134BF4DDD2A72C5C396647F7037AF0E1
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: 0000000E.00000002.722985777.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000E.00000002.722985777.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000E.00000002.722985777.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000E.00000002.722985777.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000E.00000002.722985777.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000E.00000002.728700513.000000001DC90000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000E.00000002.728700513.000000001DC90000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000E.00000002.728700513.000000001DC90000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000E.00000002.728700513.000000001DC90000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000E.00000002.728700513.000000001DC90000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000E.00000002.727723353.000000001CB01000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000E.00000002.727723353.000000001CB01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000E.00000002.727723353.000000001CB01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000E.00000002.727723353.000000001CB01000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000E.00000002.727723353.000000001CB01000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000E.00000002.729263092.000000001DD22000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000E.00000002.729263092.000000001DD22000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000E.00000002.729263092.000000001DD22000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000E.00000002.729263092.000000001DD22000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000E.00000002.729263092.000000001DD22000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000E.00000002.723425868.0000000001620000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000E.00000002.723425868.0000000001620000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000E.00000002.723425868.0000000001620000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000E.00000002.723425868.0000000001620000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000E.00000002.723425868.0000000001620000.00000004.00000001.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	722760AC	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	722760AC	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	722760AC	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	722760AC	unknown

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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	1B7A0163	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1B7A0163	ReadFile

Disassembly

Code Analysis