ID: 321194
Sample Name: PURCHASE ORDER.exe
Cookbook: default.jbs
Time: 15:34:22
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

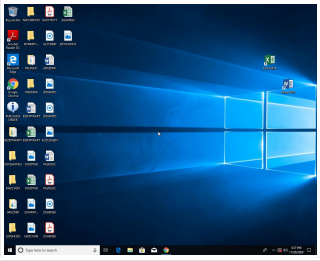
Analysis Report PURCHASE ORDER.exe

Overview

General Information

Sample Name:	PURCHASE ORDER.exe
Analysis ID:	321194
MD5:	8e2337f7cdd4bcd..
SHA1:	457de2e6917947..
SHA256:	d30629a1a9aad3..
Tags:	exe HawkEye

Most interesting Screenshot:



Detection

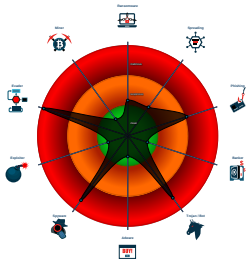
HawkEye
MailPassView

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

Signatures

- Detected HawkEye Rat
- Detected unpacking (changes PE se…
- Detected unpacking (creates a PE fi…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code contains potentia…
- .NET source code references suspic…
- Allocates memory in foreign process

Classification



Startup

- **System is w10x64**
- PURCHASE ORDER.exe (PID: 6508 cmdline: 'C:\Users\user\Desktop\PURCHASE ORDER.exe' MD5: 8E2337F7CDD4BCD18E862B7A73734D49)
  - PURCHASE ORDER.exe (PID: 6524 cmdline: 'C:\Users\user\Desktop\PURCHASE ORDER.exe' MD5: 8E2337F7CDD4BCD18E862B7A73734D49)
    - dw20.exe (PID: 6732 cmdline: dw20.exe -x -s 2104 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
    - vbc.exe (PID: 6928 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: 6940 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
  - PURCHASE ORDER.exe (PID: 6532 cmdline: 'C:\Users\user\Desktop\PURCHASE ORDER.exe' 2 6524 7175453 MD5: 8E2337F7CDD4BCD18E862B7A73734D49)
    - PURCHASE ORDER.exe (PID: 764 cmdline: C:\Users\user\Desktop\PURCHASE ORDER.exe MD5: 8E2337F7CDD4BCD18E862B7A73734D49)
      - PURCHASE ORDER.exe (PID: 6952 cmdline: C:\Users\user\Desktop\PURCHASE ORDER.exe MD5: 8E2337F7CDD4BCD18E862B7A73734D49)
        - dw20.exe (PID: 1112 cmdline: dw20.exe -x -s 2112 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
        - vbc.exe (PID: 1236 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: 3720 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
      - PURCHASE ORDER.exe (PID: 5552 cmdline: 'C:\Users\user\Desktop\PURCHASE ORDER.exe' 2 6952 7204953 MD5: 8E2337F7CDD4BCD18E862B7A73734D49)
        - PURCHASE ORDER.exe (PID: 1396 cmdline: C:\Users\user\Desktop\PURCHASE ORDER.exe MD5: 8E2337F7CDD4BCD18E862B7A73734D49)
          - PURCHASE ORDER.exe (PID: 5140 cmdline: C:\Users\user\Desktop\PURCHASE ORDER.exe MD5: 8E2337F7CDD4BCD18E862B7A73734D49)
            - dw20.exe (PID: 5468 cmdline: dw20.exe -x -s 2304 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
          - PURCHASE ORDER.exe (PID: 3100 cmdline: 'C:\Users\user\Desktop\PURCHASE ORDER.exe' 2 5140 7233203 MD5: 8E2337F7CDD4BCD18E862B7A73734D49)
            - PURCHASE ORDER.exe (PID: 5772 cmdline: C:\Users\user\Desktop\PURCHASE ORDER.exe MD5: 8E2337F7CDD4BCD18E862B7A73734D49)
              - PURCHASE ORDER.exe (PID: 5076 cmdline: C:\Users\user\Desktop\PURCHASE ORDER.exe MD5: 8E2337F7CDD4BCD18E862B7A73734D49)
                - dw20.exe (PID: 4684 cmdline: dw20.exe -x -s 2272 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
                - vbc.exe (PID: 6536 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: 6312 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
              - PURCHASE ORDER.exe (PID: 6660 cmdline: 'C:\Users\user\Desktop\PURCHASE ORDER.exe' 2 5076 7248218 MD5: 8E2337F7CDD4BCD18E862B7A73734D49)
- **cleanup**

Malware Configuration

Threatname: HawkEye

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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000022.00000002.444523132.000000000239 2000.00000040.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net >	• 0x7b69c:$key: HawkEyeKeylogger • 0x7d8cc:$salt: 099u787978786 • 0x7bcdd:$string1: HawkEye_Keylogger • 0x7cb1c:$string1: HawkEye_Keylogger • 0x7d82c:$string1: HawkEye_Keylogger • 0x7c0b2:$string2: holdermail.txt • 0x7c0d2:$string2: holdermail.txt • 0x7bff4:$string3: wallet.dat • 0x7c00c:$string3: wallet.dat • 0x7c022:$string3: wallet.dat • 0x7d3f0:$string4: Keylog Records • 0x7d708:$string4: Keylog Records • 0x7d924:$string5: do not script --> • 0x7b684:$string6: \pidloc.txt • 0x7b712:$string7: BSPLIT • 0x7b722:$string7: BSPLIT
00000022.00000002.444523132.000000000239 2000.00000040.00000001.sdmp	JoeSecurity_MailPassVie w	Yara detected MailPassView	Joe Security	
00000022.00000002.444523132.000000000239 2000.00000040.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000022.00000002.444523132.000000000239 2000.00000040.00000001.sdmp	JoeSecurity_WebBrowser PassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000022.00000002.444523132.000000000239 2000.00000040.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x7bd35:$hawkstr1: HawkEye Keylogger • 0x7cb62:$hawkstr1: HawkEye Keylogger • 0x7ce91:$hawkstr1: HawkEye Keylogger • 0x7cfec:$hawkstr1: HawkEye Keylogger • 0x7d14f:$hawkstr1: HawkEye Keylogger • 0x7d3c8:$hawkstr1: HawkEye Keylogger • 0x7b8c3:$hawkstr2: Dear HawkEye Customers! • 0x7cee4:$hawkstr2: Dear HawkEye Customers! • 0x7d03b:$hawkstr2: Dear HawkEye Customers! • 0x7d1a2:$hawkstr2: Dear HawkEye Customers! • 0x7b9e4:$hawkstr3: HawkEye Logger Details:
Click to see the 198 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_WebBrowser PassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
38.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_MailPassVie w	Yara detected MailPassView	Joe Security	
39.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_WebBrowser PassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
7.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassVie w	Yara detected MailPassView	Joe Security	

Source	Rule	Description	Author	Strings
34.2.PURCHASE ORDER.exe.2390000.3.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b89c:$key: HawkEyeKeylogger • 0x7dacc:$salt: 099u787978786 • 0x7bedd:$string1: HawkEye_Keylogger • 0x7cd1c:$string1: HawkEye_Keylogger • 0x7da2c:$string1: HawkEye_Keylogger • 0x7c2b2:$string2: holdermail.txt • 0x7c2d2:$string2: holdermail.txt • 0x7c1f4:$string3: wallet.dat • 0x7c20c:$string3: wallet.dat • 0x7c222:$string3: wallet.dat • 0x7d5f0:$string4: Keylog Records • 0x7d908:$string4: Keylog Records • 0x7db24:$string5: do not script --> • 0x7b884:$string6: \pidloc.txt • 0x7b912:$string7: BSPLIT • 0x7b922:$string7: BSPLIT
Click to see the 142 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

- AV Detection
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- 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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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:

Detected unpacking (changes PE section rights)

Detected unpacking (creates a PE file in dynamic memory)

Detected unpacking (overwrites its own PE header)

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

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

Maps a DLL or memory area into another process

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

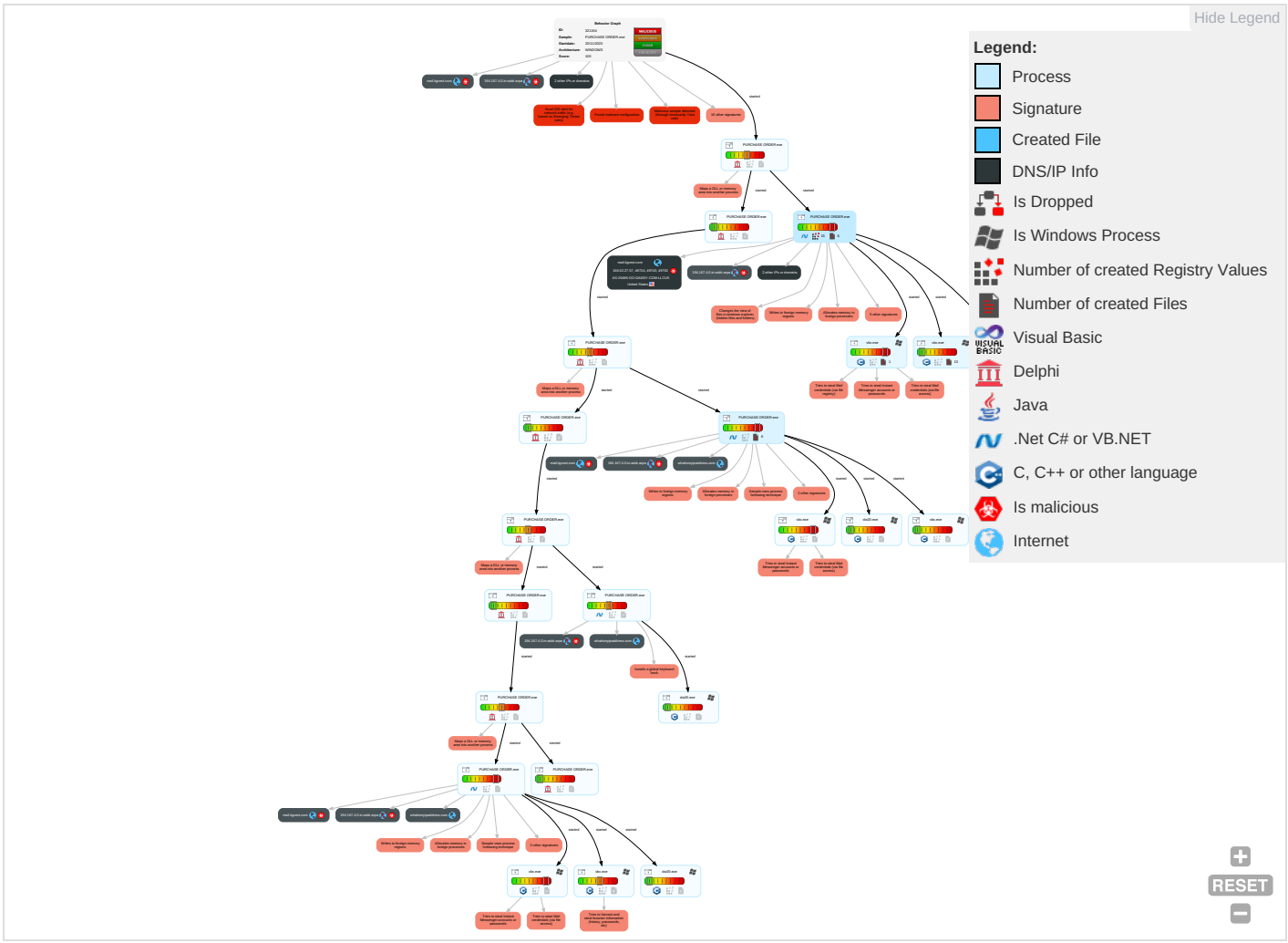
Yara detected HawkEye Keylogger

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 1 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over C Network Medium

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Default Accounts	Native API 1 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 1 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Process Injection 5 1 1	Obfuscated Files or Information 2 1	Credentials in Registry 2	Account Discovery 1	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltra
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 4 1	Credentials In Files 1	File and Directory Discovery 1	Distributed Component Object Model	Email Collection 1	Scheduled Transfe
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	System Information Discovery 3 9	SSH	Input Capture 2 1 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Query Registry 1	VNC	Clipboard Data 3	Exfiltration Over C Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Modify Registry 1	DCSync	Security Software Discovery 1 10 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protoc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 6	Proc Filesystem	Virtualization/Sandbox Evasion 6	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encryp Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 5 1 1	/etc/passwd and /etc/shadow	Process Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encry Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Application Window Discovery 1 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfu Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Owner/User 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	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over U
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Masquerade Task or Service	GUI Input Capture	System Network Configuration Discovery 1	Exploitation of Remote Services	Email Collection	Commonly Used F

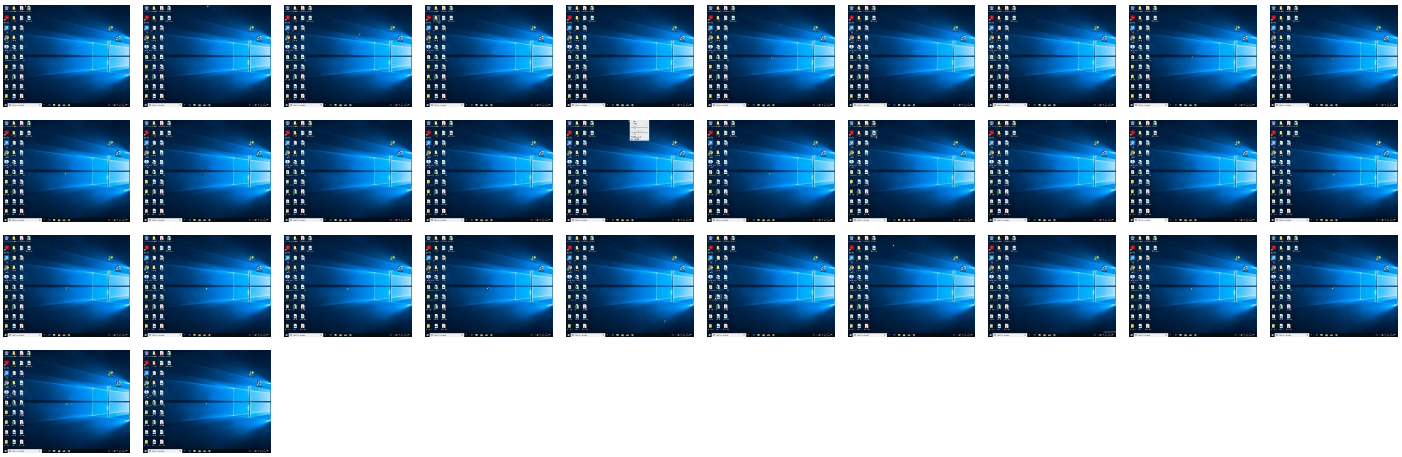
Behavior Graph



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
PURCHASE ORDER.exe	53%	Virustotal		Browse
PURCHASE ORDER.exe	54%	ReversingLabs	Win32.Trojan.LokiBot	
PURCHASE ORDER.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.PURCHASE ORDER.exe.2680000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
1.2.PURCHASE ORDER.exe.2680000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
18.1.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
18.2.PURCHASE ORDER.exe.21b0000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
33.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
16.2.PURCHASE ORDER.exe.2720000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
34.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File

Source	Detection	Scanner	Label	Link	Download
34.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
18.2.PURCHASE ORDER.exe.2240000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
18.2.PURCHASE ORDER.exe.2240000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
33.2.PURCHASE ORDER.exe.2780000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
33.2.PURCHASE ORDER.exe.2780000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
34.1.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.2.PURCHASE ORDER.exe.2320000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
29.2.PURCHASE ORDER.exe.2320000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
35.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
34.2.PURCHASE ORDER.exe.2390000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
34.2.PURCHASE ORDER.exe.2390000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
29.1.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.2.PURCHASE ORDER.exe.2280000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
34.2.PURCHASE ORDER.exe.2280000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
2.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
2.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
18.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
18.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
39.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
28.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
18.2.PURCHASE ORDER.exe.22f0000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
18.2.PURCHASE ORDER.exe.22f0000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
29.2.PURCHASE ORDER.exe.23b0000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
29.2.PURCHASE ORDER.exe.23b0000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
29.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
29.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
2.2.PURCHASE ORDER.exe.ae0000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
16.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
19.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
34.2.PURCHASE ORDER.exe.680000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
16.2.PURCHASE ORDER.exe.2780000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
16.2.PURCHASE ORDER.exe.2780000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
8.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
3.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
2.2.PURCHASE ORDER.exe.b90000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
2.2.PURCHASE ORDER.exe.b90000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
22.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
28.2.PURCHASE ORDER.exe.2780000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
28.2.PURCHASE ORDER.exe.2780000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
2.1.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.PURCHASE ORDER.exe.2630000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
2.2.PURCHASE ORDER.exe.2410000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
2.2.PURCHASE ORDER.exe.2410000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
33.2.PURCHASE ORDER.exe.2720000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
29.2.PURCHASE ORDER.exe.2290000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.iigcest.com	0%	Virustotal		Browse
194.167.4.0.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/L	0%	Avira URL Cloud	safe	
http://www.monotype.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.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	0%	Avira URL Cloud	safe	
http://whatismyipaddress.comx&	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://fontfabrik.comu	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Norm	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.jiyu-kobo.co.jp/Y0J(	0%	Avira URL Cloud	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.founder.com.cn/cnayob	0%	Avira URL Cloud	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://www.fontbureau.comasc	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/icro	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.founder.com.cn/cnLog	0%	Avira URL Cloud	safe	
http://www.fontbureau.comueta	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/L	0%	Avira URL Cloud	safe	
http://https://whatismyipaddress.comx&	0%	Avira URL Cloud	safe	
http://www.fontbureau.comli	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/E	0%	Avira URL Cloud	safe	
http://en.wikipedia	0%	URL Reputation	safe	
http://en.wikipedia	0%	URL Reputation	safe	
http://en.wikipedia	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.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	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.fontbureau.comaE	0%	Avira URL Cloud	safe	
http://www.tiro.	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/al	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn-	0%	Avira URL Cloud	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/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.155.36	true	false		high
mail.iigcest.com	166.62.27.57	true	true	• 0%, Virustotal, Browse	unknown
g.msn.com	unknown	unknown	false		high
194.167.4.0.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.0000000005240000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.0000000005240000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.0000000005240000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.0000000005240000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/L	PURCHASE ORDER.exe, 00000002.00000003.247612292.0000000005099000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.g	PURCHASE ORDER.exe, 00000002.00000003.248147520.00000000050A4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comessed	PURCHASE ORDER.exe, 00000002.00000003.248731713.00000000050A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.0000000005240000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/~	PURCHASE ORDER.exe, 00000002.00000003.247116127.0000000005094000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.comx&	PURCHASE ORDER.exe, 0000001D.00000002.384934808.0000000002FC2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100 000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.0000000005240000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100 000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.0000000005240000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100 000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.0000000005240000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100 000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.0000000005240000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100 000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.0000000005240000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/8	PURCHASE ORDER.exe, 00000002.00000003.247612292.0000000005099000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	vbc.exe, 00000008.00000003.267880542.000000000219C000.000000004.00000001.sdmp, vbc.exe, 00000016.00000003.332376227.000000000219C000.00000004.00000001.sdmp, vbc.exe, 00000027.00000003.416901672.00000000021DC000.00000004.00000001.sdmp	false		high
http://fontfabrik.comu	PURCHASE ORDER.exe, 00000002.00000003.243348763.00000000050C5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	vbc.exe, 00000008.00000003.267880542.000000000219C000.000000004.00000001.sdmp, vbc.exe, 00000008.00000002.269515866.000000000007EC000.00000004.00000020.sdmp, vbc.exe, 00000016.00000003.332376227.000000000219C000.00000004.00000001.sdmp, vbc.exe, 00000027.00000003.416901672.00000000021DC000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comcom	PURCHASE ORDER.exe, 00000002.00000003.248367150.00000000050A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://whatismyipaddress.com/-	PURCHASE ORDER.exe, 00000001.00000002.243036472.000000000271 7000.00000040.00000001.sdmp, PURCHASE ORDER.exe, 00000002.00 000002.292566171.0000000000B92 000.00000004.00000001.sdmp, PU RCHASE ORDER.exe, 00000010.000 00002.306410027.00000000027820 00.00000040.00000001.sdmp, PUR CHASE ORDER.exe, 00000012.0000 0002.354079025.00000000022F200 0.00000040.00000001.sdmp, PURC HASE ORDER.exe, 0000001C.00000 002.368097670.0000000002817000 .00000040.00000001.sdmp, PURCH ASE ORDER.exe, 0000001D.000000 02.382207742.0000000000497000. 00000040.00000001.sdmp, PURCHASE ORDER.exe, 00000021.0000000 2.399940578.0000000002782000.0 0000040.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002 .444523132.0000000002392000.00 000040.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00 000002.358229310.0000000005100 000.00000002.00000001.sdmp, PU RCHASE ORDER.exe, 0000001D.000 00002.386166114.0000000052400 00.00000002.00000001.sdmp, PUR CHASE ORDER.exe, 00000022.0000 0002.448051007.000000000510000 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	PURCHASE ORDER.exe, 00000002.00000003.247612292.000000000509 9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.yahoo.com/config/login	PURCHASE ORDER.exe, vbc.exe	false		high
http://www.fonts.com	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000002.00 000003.243270063.00000000050C5 000.00000004.00000001.sdmp, PU RCHASE ORDER.exe, 00000012.000 00002.358229310.0000000005100 00.00000002.00000001.sdmp, PUR CHASE ORDER.exe, 0000001D.0000 0002.386166114.000000000524000 0.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000 002.448051007.0000000005100000 .00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Norm	PURCHASE ORDER.exe, 00000002.00000003.247344395.000000000509 B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00 000002.358229310.0000000005100 000.00000002.00000001.sdmp, PU RCHASE ORDER.exe, 0000001D.000 00002.386166114.0000000052400 00.00000002.00000001.sdmp, PUR CHASE ORDER.exe, 00000022.0000 0002.448051007.000000000510000 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.site.com/logs.php	PURCHASE ORDER.exe, 0000001D.00000002.384284162.0000000002BF E000.00000004.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00 000002.445346649.0000000002A41 000.00000004.00000001.sdmp	false		high

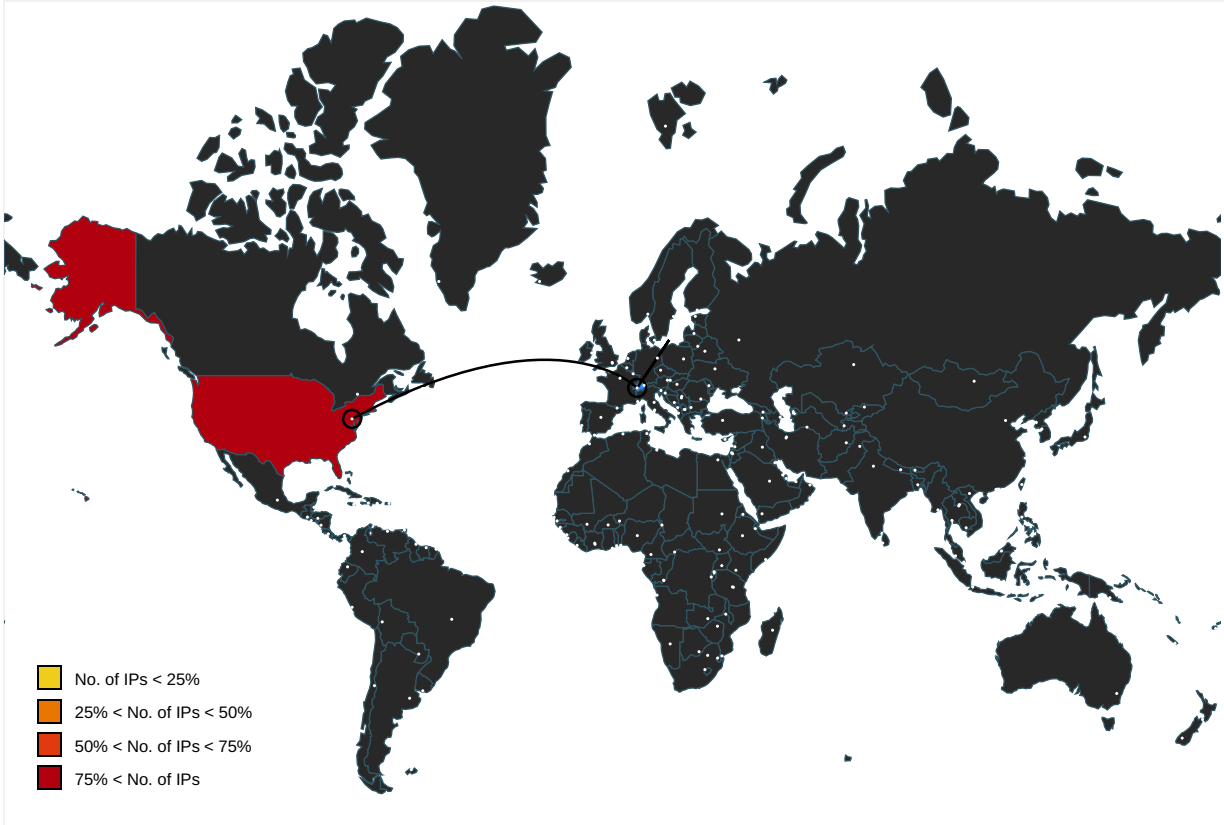
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1https://c	vbc.exe, 00000008.00000003.267880542.000000000219C000.00000004.00000001.sdmp, vbc.exe, 00000016.00000003.332376227.00000000219C000.00000004.00000001.sdmp, vbc.exe, 00000027.00000003.416901672.00000000021DC000.00000004.00000001.sdmp	false		high
http://www.urwpp.deDPlease	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.000000000510000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.000000000524000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.000000000510000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0J(	PURCHASE ORDER.exe, 00000002.00000003.247612292.000000000509000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nirsoft.net/	vbc.exe, 00000026.00000002.413012282.0000000000400000.00000040.00000001.sdmp, vbc.exe, 00000027.00000002.417706986.00000000400000.00000040.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.000000000510000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.000000000524000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.000000000510000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnayob	PURCHASE ORDER.exe, 00000002.00000003.244906268.00000000050A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/checksync.phphttps://contextual.media.net/checksync.php?&vsSync=1&cs=1&	vbc.exe, 00000008.00000003.267880542.000000000219C000.00000004.00000001.sdmp, vbc.exe, 00000016.00000003.332376227.00000000219C000.00000004.00000001.sdmp, vbc.exe, 00000027.00000003.416901672.00000000021DC000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.000000000510000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.000000000524000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.000000000510000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comasc	PURCHASE ORDER.exe, 00000002.00000002.296461553.000000000509000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/icro	PURCHASE ORDER.exe, 00000002.00000003.247344395.000000000509B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://whatismyipaddress.com/	PURCHASE ORDER.exe, 00000022.00000002.445346649.0000000002A41000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.0000000005240000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.0000000005240000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000.00000002.00000001.sdmp	false		high
http://https://whatismyipaddress.com	PURCHASE ORDER.exe, 00000002.00000002.293899335.0000000002BC1000.00000004.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.355012308.0000000002AB1000.00000004.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.384957063.0000000002FD7000.00000004.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.445346649.0000000002A4100.00000004.00000001.sdmp	false		high
http://www.fontbureau.comF	PURCHASE ORDER.exe, 00000002.00000003.248731713.00000000050A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnLog	PURCHASE ORDER.exe, 00000002.00000003.244906268.00000000050A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comueta	PURCHASE ORDER.exe, 00000002.00000002.296461553.000000000509 0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/L	PURCHASE ORDER.exe, 00000002.00000003.247452033.000000000509 5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://whatismyipaddress.comx&	PURCHASE ORDER.exe, 0000001D.00000002.384934808.0000000002FC2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://whatismyipaddress.com	PURCHASE ORDER.exe, 00000002.00000002.293899335.0000000002BC1000.00000004.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.355012308.0000000002AB1000.00000004.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.384934808.0000000002FC2000.00000004.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.445346649.0000000002A4100.00000004.00000001.sdmp	false		high
http://www.fontbureau.comli	PURCHASE ORDER.exe, 00000002.00000003.248367150.00000000050A2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/E	PURCHASE ORDER.exe, 00000002.00000003.247452033.000000000509 5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.wikipedia	PURCHASE ORDER.exe, 00000002.00000003.243158322.000000000509D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	PURCHASE ORDER.exe, 00000002.00000003.247612292.000000000509 9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comd	PURCHASE ORDER.exe, 00000002.00000003.248731713.00000000050A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100 000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.00000000052400 00.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.000000000510000 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comaE	PURCHASE ORDER.exe, 00000002.00000002.296461553.000000000509 0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.	PURCHASE ORDER.exe, 00000002.00000003.245788944.000000000509 D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100 000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.00000000052400 00.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.000000000510000 0.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000002.00000003.245859149.000000000509E 000.00000004.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100 00.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.000000000524000 0.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.0000000005100000 .00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524 0000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.0000000005100 000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.00000000052400 00.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.000000000510000 0.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/al	PURCHASE ORDER.exe, 00000002.00000003.247344395.000000000509 B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn-	PURCHASE ORDER.exe, 00000002.00000003.245859149.000000000509 E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	PURCHASE ORDER.exe, 00000002.00000003.250146188.00000000050C D000.00000004.00000001.sdmp, PURCHASE ORDER.exe, 00000002.00000003.249323990.00000000050CC 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/p	PURCHASE ORDER.exe, 00000002.00000003.247612292.000000000509 9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comm	PURCHASE ORDER.exe, 00000002.00000002.296461553.000000000509 0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	PURCHASE ORDER.exe, 00000002.00000003.247344395.000000000509B000.00000004.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.000000000510000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.000000000524000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.000000000510000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/i	PURCHASE ORDER.exe, 00000002.00000003.247344395.000000000509B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/ogra	PURCHASE ORDER.exe, 00000002.00000003.247116127.000000000509000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	PURCHASE ORDER.exe, 00000002.00000002.296611311.000000000524000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000012.00000002.358229310.000000000510000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 0000001D.00000002.386166114.000000000524000.00000002.00000001.sdmp, PURCHASE ORDER.exe, 00000022.00000002.448051007.000000000510000.00000002.00000001.sdmp	false		high
http://fontfabrik.com(	PURCHASE ORDER.exe, 00000002.00000003.243348763.00000000050C5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/b	PURCHASE ORDER.exe, 00000002.00000003.247344395.000000000509B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.155.36	unknown	United States		13335	CLOUDFLARENETUS	false
166.62.27.57	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321194
Start date:	20.11.2020
Start time:	15:34:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PURCHASE ORDER.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winEXE@44/23@20/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 83.2% (good quality ratio 81.1%) • Quality average: 84.8% • Quality standard deviation: 24.2%
HCA Information:	• Successful, ratio: 87% • 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, SgrmBroker.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 40.88.32.150, 23.210.248.85, 51.104.139.180, 52.255.188.83, 51.103.5.186, 52.155.217.156, 20.54.26.129, 52.142.114.176, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size 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 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
15:35:26	API Interceptor	91x Sleep call for process: PURCHASE ORDER.exe modified
15:35:42	API Interceptor	4x 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	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/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	6JLHKYvboo.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	jSMd8npgmU.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	9vdouqRTh3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	5pB35gGfZ5.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	fyxC4Hgs3s.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	yk94P18VKp.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	oLHQIQAI3N.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	WuGzF7ZJ7P.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NXmokFkh3R.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	qiGQsdRM57.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NSSPH41vE5.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	2v7Vtqfo81.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	355OckuTD3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	i7osF3yJYR.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	D71G6Z9M0O.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
166.62.27.57	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	
	INQUIRY.exe	Get hash	malicious	Browse	
	X62RG9z7kY.exe	Get hash	malicious	Browse	
	SWIFT100892220-PDF.exe	Get hash	malicious	Browse	
	SWIFT0079111-pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.iigcest.com	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• 166.62.27.57
	INQUIRY.exe	Get hash	malicious	Browse	• 166.62.27.57
	Vll6ZcOkEQ.exe	Get hash	malicious	Browse	• 166.62.27.57
	x2rzwu7CQ3.exe	Get hash	malicious	Browse	• 166.62.27.57
	X62RG9z7kY.exe	Get hash	malicious	Browse	• 166.62.27.57
	SWIFT100892220-PDF.exe	Get hash	malicious	Browse	• 166.62.27.57
	SWIFT0079111-pdf.exe	Get hash	malicious	Browse	• 166.62.27.57
	AD1-2001328L_pdf.exe	Get hash	malicious	Browse	• 166.62.27.57
whatismyipaddress.com	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
	8oaZfXDstn.exe	Get hash	malicious	Browse	• 104.16.154.36
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• 104.16.155.36
	9vdouqRTh3.exe	Get hash	malicious	Browse	• 104.16.154.36

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5pB35gGfZ5.exe	Get hash	malicious	Browse	• 104.16.155.36
	M9RhKQ1G91.exe	Get hash	malicious	Browse	• 104.16.154.36

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	http://https://eagleeyeproduce-my.sharepoint.com/:o:/p/mckrayp/EtopxtQDn3pOqhvY4g_gG3ABKX9ornSoGNhGOLlXyaU89Q?e=Ee0wW2	Get hash	malicious	Browse	• 104.16.19.94
	http://https://certified1.box.com/s/2ta9r7cyn5g09fblryd9xqqpnfxbjqej	Get hash	malicious	Browse	• 104.16.19.94
	Report.464129889.doc	Get hash	malicious	Browse	• 104.28.21.160
	SecuriteInfo.com.Trojan.PWS.StealerNET.67.29498.exe	Get hash	malicious	Browse	• 104.28.29.208
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 104.18.27.190
	http://https://ubereats.app.link/cwmLFZfMz5?%243p=a_custom_354088&%24deeplink_path=promo%2Fapply%3FpromoCode%3DRECONFORT7&%24desktop_url=tracking.spectrumemp.com/el?aid=8feeb968-bdd0-11e8-b27f-22000be0a14e&rid=50048635&pid=285843&cid=513&dest=overlordscan.com/cmV0by5tZXR6bGVyQGlzb2x1dGlvbnMuY2g=%23#kkowfocjoyuynaip#	Get hash	malicious	Browse	• 104.24.97.83
	http://https://hastebin.com/raw/xatuvoxixa	Get hash	malicious	Browse	• 104.24.126.89
	http://https://bit.ly/35MTO80	Get hash	malicious	Browse	• 104.31.69.156
	Order List.xlsx	Get hash	malicious	Browse	• 104.24.122.89
	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	• 162.159.133.233
	Request for quotation.xlsx	Get hash	malicious	Browse	• 172.67.181.41
	MV TBN.exe	Get hash	malicious	Browse	• 104.28.5.151
	PO 20-11-2020.pps	Get hash	malicious	Browse	• 172.67.22.135
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 1.1.1.1
	23prRlqeGr.exe	Get hash	malicious	Browse	• 104.23.98.190
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.23.46
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.22.46
	iG9YiwEMru.exe	Get hash	malicious	Browse	• 104.27.132.115
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 104.22.54.159
	SUSPENSION LETTER ON SIM SWAP.pdf.exe	Get hash	malicious	Browse	• 172.67.131.55
AS-26496-GO-DADDY-COM-LLCUS	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	• 192.186.237.168
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• 166.62.27.57
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 198.71.232.3
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 184.168.131.241
	MV.KMTC JEBEL ALI_pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
	PO0119-1620 LQSB 0320 Siemens.exe	Get hash	malicious	Browse	• 184.168.131.241
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 192.186.237.168
	http://homeschoolingteen.com	Get hash	malicious	Browse	• 107.180.51.106
	http://p3nlhclust404.shr.prod.phx3.secureserver.net	Get hash	malicious	Browse	• 72.167.191.65
	INQUIRY.exe	Get hash	malicious	Browse	• 166.62.27.57
	moses.exe	Get hash	malicious	Browse	• 148.66.138.196
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 184.168.131.241
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 184.168.131.241
	http://https://j.mp/38NwiZZ	Get hash	malicious	Browse	• 107.180.26.71
	POSH XANADU Order-SP-20-V241e.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	http://https://tg325.infusion-links.com/api/v1/click/5985883831533568/6575528038498304	Get hash	malicious	Browse	• 198.71.233.138
	http://https://tg325.infusion-links.com/api/v1/click/5985883831533568/6575528038498304	Get hash	malicious	Browse	• 198.71.233.138
	anthony.exe	Get hash	malicious	Browse	• 107.180.4.22
	http://https://sailingfloridakeys.com/Guarantee/	Get hash	malicious	Browse	• 104.238.92.18
	oX3qPEgl5x.exe	Get hash	malicious	Browse	• 198.71.232.3

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_purchase order.e_92d8e08de16268aa8cb7e98cbe71d84aa9135eb_00000000_043644b2\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):	18538
Entropy (8bit):	3.7612741860684284
Encrypted:	false
SSDEEP:	192:M37TMi+VZjV/C9yq5bMvg/LHZ+nNN2I1rzvq5xk0z5xT5/u7sKS274It1:87T2jB7vqsSt/u7sKX4It1
MD5:	E155DAA9C56194B0A9A588D55B99532C
SHA1:	2FAE2B15FB320A1A01A8DBDBBD8A41C5E95553E7
SHA-256:	C77BA4C260975AE297BC00277CF33D2B1884E67A4FCB48B7DE159A7B3C44D9DD
SHA-512:	6D471E389082EEEC988344D1556821240D516F3EB75D2127935093F19A612F11AC68F6B622B5DFE8F5B41E93E9AF95EB714BE75EBF1EE02EAD3804463C5F06E1
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.3.8.8.9.5.5.4.0.5.5.7.9.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.0.3.8.8.9.5.6.6.0.8.6.9.8.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.1.0.a.0.b.e.2.-.0.6.4.a.-.4.9.0.b.-.a.b.3.7.-.2.5.d.e.f.a.4.9.c.9.a.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.2.8.-.0.0.0.1.-.0.0.1.6.-.9.5.6.f.-.e.d.d.f.9.5.b.f.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.5.a.e.6.4.8.2.1.0.a.4.d.f.6.5.b.9.3.a.5.b.a.a.b.5.f.f.f.e.b.a.a.0.0.0.0.f.f.f.f.!.0.0.0.0.4.5.7.d.e.2.e.6.9.1.7.9.4.7.1.1.d.2.5.7.a.b.9.c.6.3.1.5.d.6.f.2.6.4.6.5.c.e.1.a.!.P.U.R.C.H.A.S.E. .O.R.D.E.R...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.8.:.0.7.:.4.5.:.1.7.!.0.!.P.U.R.C.H.A.S.E. .O.R.D.E.R...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.I.d.=.3.5.5.....I.s.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_purchase order.e_92d8e08de16268aa8cb7e98cbe71d84aa9135eb_00000000_1222ed66\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):	18536
Entropy (8bit):	3.761301220538883
Encrypted:	false
SSDEEP:	192:Qe7VMi+VZjV/C9yq5bMvg/LHZ+nNN2I1rzvq5xk0z5xT5/u7slS274ItT:l7V2jB7vqsSt/u7slX4ItT
MD5:	32F3FF00FA2CC344B1A388D72493F31B
SHA1:	A819FE301ED92583003E18631159B233FB1EA8A3
SHA-256:	ADA582DE12F13C70A83C82C21A1D1A95A2D0259C20C3F25854201684E56F23A2
SHA-512:	F60F0A005D9A5E26A11B06BB1896F36C7990D7A6D1BAFE6364FB5036653E9AA9A9B35B4A3DEF1EE433338303FAB967EFFC35772A43FE9A62CA477A65058A997F
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.3.8.8.9.9.6.0.9.3.0.3.6.1.....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.=.1.3.2.5.0.3.8.8.9.9.7.2.4.9.2.8.2.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.4.b.8.0.7.2.5.-.a.e.c.a.-.4.c.5.8.-.b.0.b.6.-.e.5.6.f.0.a.6.8.6.6.4.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.d.4.-.0.0.0.1.-.0.0.1.6.-.4.7.c.0.-.7.5.f.9.9.5.b.f.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.5.a.e.6.4.8.2.1.0.a.4.d.f.6.5.b.9.3.a.5.b.a.a.b.5.f.f.f.e.b.a.a.0.0.0.0.f.f.f.f.!.0.0.0.0.4.5.7.d.e.2.e.6.9.1.7.9.4.7.1.1.d.2.5.7.a.b.9.c.6.3.1.5.d.6.f.2.6.4.6.5.c.e.1.a.!.P.U.R.C.H.A.S.E. .O.R.D.E.R...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.8.:.0.7.:.4.5.:.1.7.!.0.!.P.U.R.C.H.A.S.E. .O.R.D.E.R...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.I.d.=.3.7.1.....I.s.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_purchase order.e_92d8e08de16268aa8cb7e98cbe71d84aa9135eb_00000000_15327d85\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):	18538
Entropy (8bit):	3.7609687340074123
Encrypted:	false
SSDEEP:	192:gc3O7rMi+VZjV/C9yq5bMvg/LHZ+nNN2I1rzvq5xk0z5xT5/u7slS274ItB:pe7r2jB7vqsSt/u7slX4ItB
MD5:	92D85D669290DB026D73199633BD7961
SHA1:	963AAE602E439518BEA07147D50CAC8A40417583
SHA-256:	37ABE930977B082023DD22B6CDD8E2AC129F53C7B1E4E12011736CD540170A92

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_purchase order.e_92d8e08de16268aa8cb7e98cbe71d84aa9135eb_00000000_15327d85\Report.wer	
SHA-512:	F6A83ABCAF757F9FE7C7252E43F1CDD16A8BC9949EBB7EA35DA8BACB1C17BD0AC627A3DDCC48A6AB033DEC78E59B8EB640D3EB6A0C2378081670A1002F9FE858
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.3.8.8.9.8.2.9.5.2.4.2.3.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.0.3.8.8.9.8.4.0.4.6.1.7.0.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.d.d.e.0.5.9.b.-.c.6.e.7.-.4.d.7.4.-.8.6.1.4.-.4.b.8.6.a.1.a.f.7.6.b.c.....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.=.0.0.0.0.1.4.1.4.-.0.0.0.1.-.0.0.1.6.-.1.7.a.d.-.a.7.f.0.9.5.b.f.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.5.a.e.6.4.8.2.1.0.a.4.d.f.6.5.b.9.3.a.5.b.a.a.b.5.f.f.f.e.b.a.a.0.0.0.0.f.f.f.f.!.0.0.0.0.4.5.7.d.e.2.e.6.9.1.7.9.4.7.1.1.d.2.5.7.a.b.9.c.6.3.1.5.d.6.f.2.6.4.6.5.c.e.1.a.!.P.U.R.C.H.A.S.E. .O.R.D.E.R...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.8.:.0.7.:.4.5.:.1.7.!.0.!.P.U.R.C.H.A.S.E. .O.R.D.E.R...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.I.d.=.3.6.6.....I.s.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_purchase order.e_92d8e08de16268aa8cb7e98cbe71d84aa9135eb_00000000_1a21d946\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):	18538
Entropy (8bit):	3.761230444421508
Encrypted:	false
SSDEEP:	192:nUrR75Mi+VZjV/C9yq5bMvg/LHZ+nNN2I1rzvq5xk0z5xT5/u7sKS274ItZ:niR752jB7vqsSt/u7sKX4ItZ
MD5:	553002124FDAD004DAEE206882E6183D
SHA1:	EF5FEB462E2BDB237CF5C68AB03BF33F71AE7F2E
SHA-256:	4EC2699B59D4B60EE73DCEC1CD1C3274456F30D410ABC8B87E2D4DB6BCDDF9DF
SHA-512:	22EF2C8B1B504AB1AC8C152BFE5760DBDC0D97A8533EC1F23588D3F98B8F2348BEC0091B868872B1E096637EAC7DA10EC3B42698324D4C8E285997AF55A22A72
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.3.8.8.9.2.6.9.0.5.6.0.3.9.....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.=.1.3.2.5.0.3.8.8.9.2.8.2.0.2.4.7.5.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.6.5.5.f.2.8.b.-.c.b.e.9.-.4.f.5.d.-.9.3.6.b.-.f.c.5.4.e.b.c.c.8.8.8.6.....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.=.0.0.0.0.1.9.7.c.-.0.0.0.1.-.0.0.1.6.-.c.f.d.3.-.5.c.c.e.9.5.b.f.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.5.a.e.6.4.8.2.1.0.a.4.d.f.6.5.b.9.3.a.5.b.a.a.b.5.f.f.f.e.b.a.a.0.0.0.0.f.f.f.f.!.0.0.0.0.4.5.7.d.e.2.e.6.9.1.7.9.4.7.1.1.d.2.5.7.a.b.9.c.6.3.1.5.d.6.f.2.6.4.6.5.c.e.1.a.!.P.U.R.C.H.A.S.E. .O.R.D.E.R...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.8.:.0.7.:.4.5.:.1.7.!.0.!.P.U.R.C.H.A.S.E. .O.R.D.E.R...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.I.d.=.3.3.9.....I.s.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER75B5.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):	5670
Entropy (8bit):	3.725613373922266
Encrypted:	false
SSDEEP:	96:RtIU6o7r3GLt3i9+c6UURmYXtYZRuvUubSfyIgDyyBCaM11G01fYHHm:Rrl7r3GLNi0c6rmoYZRuvUubSeCp117l
MD5:	66A95A99203A9BEB19706F064BB3DC13
SHA1:	847E3E21815F44DD562403298741AD8D89C466B0
SHA-256:	ABF2579673D7F259C68ADF574CCB6340F0D3324EF8CA1743C5B5F6A9AF93A5DD
SHA-512:	0641DB62BFEF36A5531EDDB2A333FDD2FA0CCB9792C459611DE4BF7A854DC6FE98668294EE7DA7660A38DAA3AE8677C4944880B03E6BCFB5F4C321BAB61CA58
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.1.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7681.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):	4637
Entropy (8bit):	4.466098112221119
Encrypted:	false
SSDEEP:	48:cvIwSD8zsSJgtWI9zjvWSC8Bv8fm8M4JFK87Fo+q8v3rBY/v4zMd:uITfgE+SNOJFKdK7BY/veMd
MD5:	DC70FB9A306A1644A1EB1F8DA23045B0
SHA1:	90005CBC2F21E7029A8F1CC07D3D80D8EBB16C1F
SHA-256:	54F810B4968CBF0822246005C182AE42F6B83A8392B5A04BE07D5FBFEBA78E4A
SHA-512:	D4B09E4EBB5AA5256104619AE7804C84BEEA22C39BF5E98464D7F4A5CF0D01CFD08129BECBDF8391C2D60CE0C0E86665ACA516FAFC6B39D8264BCEE702356CA
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7681.tmp.xml	
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="737807" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A98.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):	7634
Entropy (8bit):	3.6961497902166736
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNixl62k6YZN6ZgmfZRuvUubSeCp1bnk1fzJm:RrlsNiT616YT6ZgmfWvvbSHbnOfA
MD5:	CA2B30B7EA2277725407992554175 45E
SHA1:	8E0C4B5C82194EEF078B159D6A7E98D48269EB37
SHA-256:	9A090539965E65A028FFA43C2E37ACD331AC627EE374F5723D71DEDF56C96315
SHA-512:	26364668BE2C0B864B6B6B5D30812F48A84903432BBB44FBC41BDF921690BA9D44627C441CC5B1C2002AA64CE630609490DB6457416B3883680B41E0C69A4BE4
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.5.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B35.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):	4637
Entropy (8bit):	4.468657512838299
Encrypted:	false
SSDEEP:	48:cvIwSD8zsZJgtWI9zjvWSC8BF8fm8M4JFK87Ft+q8v3SjY/v4zsd:uITfrE+SNMJFK4KIY/vesd
MD5:	5D07C996276098B247DC50666D46E784
SHA1:	D9285F7FEBF09F8EEB7CC216C9AFAD2085C447C4
SHA-256:	0DC16259F4435AF5927F7362859B1EAD065BE6BB08FEC755F8E94D9FB5D7C962
SHA-512:	62269688E80BEAB0EBD09B09FE0FD2D99CDFDB99AD8E9404C003C2DCAD12AC9FE91E154A44658C29E8A6E0E84D477D31B4D0C164C87D96B3ED22DFCD8374 2CEF
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="737806" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA49.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):	5670
Entropy (8bit):	3.728857484284284
Encrypted:	false
SSDEEP:	96:RtIU6o7r3GLt3il+f6C6rYZRuvUubSfyIgDyyBCaM1nz1feWtm:Rrl7r3GLNicf6frYZRuvUubSeCp1nz1i
MD5:	7C44EF98856EAF72430447C00DE7EFB8
SHA1:	511DD1C5AB91F35B5F9FE3B29420421D01851634
SHA-256:	C0A929C728D7F663C7D7112E6C7CB71D377407A52C79F1C2523879C75F1E34E8
SHA-512:	7F076795F77976B16035E4D3F2AC946131EFA8B3BA156CA222091973705D0C6AF9878E7E8F7F08B641CCEB4FBF764D128B2A4070098CF523BEB13187B270DCCE
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.9.5.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA968.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):	5670
Entropy (8bit):	3.7286695574052597
Encrypted:	false
SSDEEP:	96:RtIU6o7r3GLt3ih+m6E/rYZRuvUubSfyIgDyyBCaM15B1f3zm:Rrl7r3GLNiYm6KrYZRuvUubSeCp15B1i
MD5:	B7841460606C8E356254549E96EA26C6
SHA1:	B99721423941373D53910731A608944DDDAEA6FF
SHA-256:	0FCB07A62695F96C266583A67291FAA27EE71820FC7FE255A11CEF250568E3EC
SHA-512:	CE29827049F3CA4504738155E94F402763633B4CE62E6769286D26A3BAA1BFF8CDC45BE08B87D72FEB77E27F3EFBAB87D5029932D2AC57ED14703F83AC072E6
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.0.7.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA05.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):	4637
Entropy (8bit):	4.466997292433701
Encrypted:	false
SSDEEP:	48:cvIwSD8zsSJgtWI9zjvWSC8B28fm8M4JFK87FgY+q8v3EIY/v4zgd:uITfgE+SNpJFKvYKHY/vegd
MD5:	462D0CF1592ACF65F115D8F452325A51
SHA1:	90AF2EA36190B1A8294314BB64B1718299ADB1E8
SHA-256:	6BC87AEB273F0E6DF4CC2068AEF86CAF0F5D90A7791C45FD7DC373836BCAE818
SHA-512:	476A0E70A1F8899B41129857AFD053BDAF49EE677E09A9FEC6EFF2B8A858148E1912FC44F290067300ABA909B6673C6403905C26B2ECA332674E950803DF6A9A
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="737807" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB83.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):	4637
Entropy (8bit):	4.466102726687347
Encrypted:	false
SSDEEP:	48:cvIwSD8zsZJgtWI9zjvWSC8BnL8fm8M4JFK87Fj+q8v30Y/v4z2d:uITfrE+SNyJFKuKkY/ve2d
MD5:	EDD1DDE8D91F253E3171462003970850
SHA1:	F45BCBD24F14E6A5A1BA66CBDA602C1933234726
SHA-256:	2358DD0EE4F13F747AABCF5B0936EB6588B81EC7B76F0282AC7520C2FF8B09E8
SHA-512:	3473AC6A4CF4A494903019E22AD8E90541D6152B55A1ADDAFACA125CADD017DA3B782F488AEED4BBD6BFD1B8D445ADF99163C0593AF124E5C8083B0918281E6C
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="737806" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

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

C:\Users\user\AppData\Local\Temp\holderwb.txt	
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\Desktop\PURCHASE ORDER.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:Ag:Ag
MD5:	4A64D913220FCA4C33C140C6952688A8
SHA1:	6E17D48D70083E4BCB0E1B2335AD62C94F2204AF
SHA-256:	71181F5D23343D7DB98F90AED3499D8C2A23131B3151CC66C4591918DFC09ACC
SHA-512:	E29AF08FD7C5AD519F2DE2137DF95B77FF41306E3B5DDABA2ADD8C75AC54AB6FEE3E05C2792429D66BB72B2620EF5097A7DBC3C69459907543B81704BDFB60 69
Malicious:	false
Preview:	5076

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\Desktop\PURCHASE ORDER.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.469582006060583
Encrypted:	false
SSDEEP:	3:oNUWJRW1wNgg3Jn:oNNJA6Ngg3J
MD5:	6D2242307451E9E440AF62BB1BA24799
SHA1:	CF6B565F218D3DE0086724128957C2C384190C9A
SHA-256:	9166215B6AA36EFDABC32D2F4CE66B0084973FF3E2F77FE2477FA5A5BD73F852
SHA-512:	93E4D51B3DA65057380F97039583D112A18A347B782DA4AF6D4F5C1839F00C8D0633C8E1470794B0B12D58FD579A33CE098C189AE732B49F616D270344DAE994
Malicious:	false
Preview:	C:\Users\user\Desktop\PURCHASE ORDER.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.987045896881915
TrID:	• Win32 Executable (generic) a (10002005/4) 99.66% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	PURCHASE ORDER.exe
File size:	973824
MD5:	8e2337f7cdd4bcd18e862b7a73734d49
SHA1:	457de2e691794711d257ab9c6315d6f26465ce1a
SHA256:	d30629a1a9aad3b8bc1e3827ab767473089214fd801b55 6f9ed3430f39bacbdd
SHA512:	7cf93e3fb60f69895a23fd8537e36394779a7a830709169 1006e56ec3465d57ecfcb854327acfcf0b184e126a1bf8e 6994234155e5ce020caa4bd66fe01c597b
SSDEEP:	24576:Vwz1Kx2k3T0jZGOL7JLBiWgpLW0obEI2PUSuo ebNh2bK39:VwKxz3ewuPgFW0eE7Uu/bw9

General

File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	ecccacacccec70a2

Static PE Info

General

Entrypoint:	0x470d00
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	429b4d8f1079c5bb87cad5efdb4eabf0

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 00470B08h
call 00007F48F0D44C5Dh
mov eax, dword ptr [00489FACh]
mov eax, dword ptr [eax]
call 00007F48F0D99C85h
mov ecx, dword ptr [0048A0A4h]
mov eax, dword ptr [00489FACh]
mov eax, dword ptr [eax]
mov edx, dword ptr [004705ACh]
call 00007F48F0D99C85h
mov eax, dword ptr [00489FACh]
mov eax, dword ptr [eax]
call 00007F48F0D99CF9h
call 00007F48F0D42754h
lea eax, dword ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8c000	0x2496	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x99000	0x5a2ac	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x91000	0x7b70	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x90000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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
CODE	0x1000	0x6fd48	0x6fe00	False	0.517266061453	data	6.51621253086	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x71000	0x19130	0x19200	False	0.189841806592	data	2.85009273727	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x8b000	0xcb1	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x8c000	0x2496	0x2600	False	0.352796052632	data	4.9419643729	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x8f000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x90000	0x18	0x200	False	0.048828125	data	0.186582516435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x91000	0x7b70	0x7c00	False	0.575321320565	data	6.64623366609	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x99000	0x5a2ac	0x5a400	False	0.904878484245	data	7.5640335424	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x99e90	0x134	data		
RT_CURSOR	0x99fc4	0x134	data		
RT_CURSOR	0x9a0f8	0x134	data		
RT_CURSOR	0x9a22c	0x134	data		
RT_CURSOR	0x9a360	0x134	data		
RT_CURSOR	0x9a494	0x134	data		
RT_CURSOR	0x9a5c8	0x134	data		
RT_BITMAP	0x9a6fc	0x1d0	data		
RT_BITMAP	0x9a8cc	0x1e4	data		
RT_BITMAP	0x9aab0	0x1d0	data		
RT_BITMAP	0x9ac80	0x1d0	data		
RT_BITMAP	0x9ae50	0x1d0	data		
RT_BITMAP	0x9b020	0x1d0	data		
RT_BITMAP	0x9b1f0	0x1d0	data		
RT_BITMAP	0x9b3c0	0x1d0	data		
RT_BITMAP	0x9b590	0x53511	data	English	United States
RT_BITMAP	0xeeaa4	0x1d0	data		
RT_BITMAP	0xeec74	0xc0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xeed34	0xd8	data		
RT_BITMAP	0xeee0c	0xe0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xeeeec	0xe0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xeefcc	0xe0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xef0ac	0xc0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xef16c	0xc0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xef22c	0xe0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xef30c	0xd8	data		
RT_BITMAP	0xef3e4	0xd8	data		
RT_BITMAP	0xef4bc	0xc0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xef57c	0xd8	data		
RT_BITMAP	0xef654	0xe0	GLS_BINARY_LSB_FIRST		

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0xef734	0xd8	data		
RT_BITMAP	0xef80c	0xe8	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xef8f4	0xc0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xef9b4	0xe0	GLS_BINARY_LSB_FIRST		
RT_ICON	0xefa94	0x8a8	data	English	United States
RT_DIALOG	0xf033c	0x52	data		
RT_STRING	0xf0390	0x194	data		
RT_STRING	0xf0524	0x2b0	data		
RT_STRING	0xf07d4	0xdc	data		
RT_STRING	0xf08b0	0x17c	data		
RT_STRING	0xf0a2c	0x1f0	data		
RT_STRING	0xf0c1c	0x4ac	data		
RT_STRING	0xf10c8	0x39c	data		
RT_STRING	0xf1464	0x378	data		
RT_STRING	0xf17dc	0x418	data		
RT_STRING	0xf1bf4	0xf4	data		
RT_STRING	0xf1ce8	0xc4	data		
RT_STRING	0xf1dac	0x2e0	data		
RT_STRING	0xf208c	0x35c	data		
RT_STRING	0xf23e8	0x2b4	data		
RT_RCDATA	0xf269c	0x10	data		
RT_RCDATA	0xf26ac	0x280	data		
RT_RCDATA	0xf292c	0x841	Delphi compiled form 'TForm1'		
RT_GROUP_CURSOR	0xf3170	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf3184	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf3198	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf31ac	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf31c0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf31d4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf31e8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0xf31fc	0x14	data	English	United States
RT_HTML	0xf3210	0x99	data	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, SetCurrentDirectoryA, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetCurrentDirectoryA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile, RaiseException, GetStdHandle, GetFileSize, GetFileType, CreateFileA, CloseHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtectEx, VirtualProtect, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVolumeInformationA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemTime, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLogicalDrives, GetLocaleInfoA, GetLastError, GetFullPathNameA, GetFileAttributesA, GetDriveTypeA, GetDiskFreeSpaceA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, FreeLibrary, FormatMessageA, FindResourceA, FindNextFileA, FindFirstFileA, FindClose, FileTimeToLocalFileTime, FileTimeToDosDateTime, ExitProcess, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
mpr.dll	WNetGetConnectionA

DLL	Import
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWindowExtEx, SetWinMetaFileBits, SetViewportOrgEx, SetViewportExtEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetMapMode, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, RectVisible, RealizePalette, Polyline, PolyPolyline, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, ExtTextOutA, ExtCreatePen, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
user32.dll	WindowFromPoint, WinHelpA, WaitMessage, ValidateRect, UpdateWindow, UnregisterClassA, UnionRect, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetMenuItemInfoA, SetMenu, SetKeyboardState, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindowEx, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OpenClipboard, OffsetRect, OemToCharA, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, IsCharAlphaNumericA, IsCharAlphaA, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongW, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessageTime, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDoubleClickTime, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCaretPos, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumClipboardFormats, EndPaint, EndDeferWindowPos, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DeferWindowPos, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreateWindowExA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, BeginDeferWindowPos, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayRedim, SafeArrayCreate, VariantChangeTypeEx, VariantCopyInd, VariantCopy, VariantClear, VariantInit
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create, InitCommonControls
kernel32.dll	MulDiv

Possible Origin

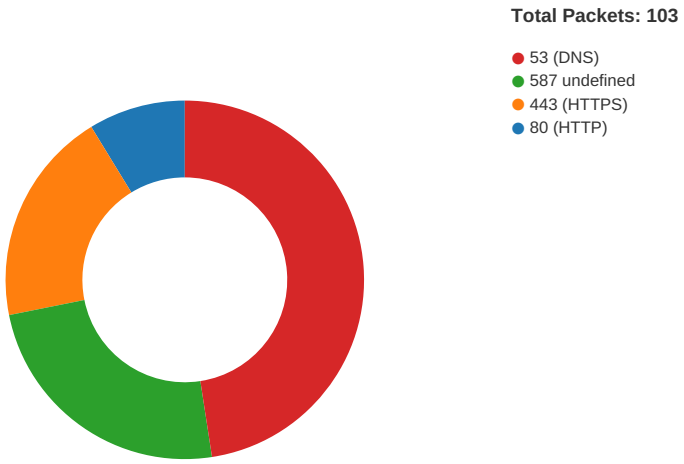
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-15:35:41.173626	TCP	2019926	ET TROJAN HawkEye Keylogger Report SMTP	49724	587	192.168.2.5	166.62.27.57
11/20/20-15:36:11.928255	TCP	2019926	ET TROJAN HawkEye Keylogger Report SMTP	49740	587	192.168.2.5	166.62.27.57
11/20/20-15:36:51.085077	TCP	2019926	ET TROJAN HawkEye Keylogger Report SMTP	49762	587	192.168.2.5	166.62.27.57
11/20/20-15:37:20.113019	TCP	2019926	ET TROJAN HawkEye Keylogger Report SMTP	49767	587	192.168.2.5	166.62.27.57

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:35:26.493499041 CET	49713	80	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.509938955 CET	80	49713	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:26.510598898 CET	49713	80	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.510627031 CET	49713	80	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.526922941 CET	80	49713	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:26.551008940 CET	80	49713	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:26.592200041 CET	49713	80	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.602325916 CET	49714	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.618752956 CET	443	49714	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:26.618880987 CET	49714	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.662209034 CET	49714	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.678555965 CET	443	49714	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:26.678955078 CET	443	49714	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:26.679054976 CET	443	49714	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:26.679136038 CET	49714	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.689137936 CET	49714	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.693531036 CET	49715	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.705611944 CET	443	49714	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:26.709882975 CET	443	49715	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:26.710000992 CET	49715	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.711369038 CET	49715	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.727734089 CET	443	49715	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:26.730894089 CET	443	49715	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:26.731041908 CET	443	49715	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:26.731106043 CET	49715	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.731822968 CET	49715	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:26.748169899 CET	443	49715	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:38.636918068 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:38.917947054 CET	587	49724	166.62.27.57	192.168.2.5
Nov 20, 2020 15:35:38.918087006 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:39.467190027 CET	587	49724	166.62.27.57	192.168.2.5
Nov 20, 2020 15:35:39.467962980 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:39.749670982 CET	587	49724	166.62.27.57	192.168.2.5
Nov 20, 2020 15:35:39.750130892 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:40.031795025 CET	587	49724	166.62.27.57	192.168.2.5
Nov 20, 2020 15:35:40.032147884 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:40.325931072 CET	587	49724	166.62.27.57	192.168.2.5
Nov 20, 2020 15:35:40.326431990 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:40.608051062 CET	587	49724	166.62.27.57	192.168.2.5
Nov 20, 2020 15:35:40.608349085 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:40.891452074 CET	587	49724	166.62.27.57	192.168.2.5
Nov 20, 2020 15:35:40.891730070 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:41.172852993 CET	587	49724	166.62.27.57	192.168.2.5
Nov 20, 2020 15:35:41.172899008 CET	587	49724	166.62.27.57	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:35:41.173625946 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:41.173666000 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:41.173741102 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:41.173904896 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:41.173923969 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:41.174180984 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:41.455326080 CET	587	49724	166.62.27.57	192.168.2.5
Nov 20, 2020 15:35:41.455355883 CET	587	49724	166.62.27.57	192.168.2.5
Nov 20, 2020 15:35:41.472999096 CET	587	49724	166.62.27.57	192.168.2.5
Nov 20, 2020 15:35:41.484783888 CET	587	49724	166.62.27.57	192.168.2.5
Nov 20, 2020 15:35:41.531816006 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:48.427588940 CET	49713	80	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:48.427895069 CET	49724	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:35:54.901406050 CET	49728	80	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:54.918010950 CET	80	49728	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:54.918107986 CET	49728	80	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:54.918652058 CET	49728	80	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:54.935045004 CET	80	49728	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:54.954479933 CET	80	49728	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:55.000778913 CET	49728	80	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:55.062410116 CET	49729	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:55.078886986 CET	443	49729	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:55.079018116 CET	49729	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:55.129223108 CET	49729	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:55.145587921 CET	443	49729	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:55.145808935 CET	443	49729	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:55.145884991 CET	443	49729	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:55.145937920 CET	49729	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:55.155306101 CET	49729	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:55.156743050 CET	49730	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:55.171847105 CET	443	49729	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:55.173038006 CET	443	49730	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:55.173186064 CET	49730	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:55.174810886 CET	49730	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:55.191153049 CET	443	49730	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:55.192327976 CET	443	49730	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:55.192462921 CET	443	49730	104.16.155.36	192.168.2.5
Nov 20, 2020 15:35:55.192893028 CET	49730	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:55.194118977 CET	49730	443	192.168.2.5	104.16.155.36
Nov 20, 2020 15:35:55.210383892 CET	443	49730	104.16.155.36	192.168.2.5
Nov 20, 2020 15:36:09.311714888 CET	49740	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:36:09.583421946 CET	587	49740	166.62.27.57	192.168.2.5
Nov 20, 2020 15:36:09.583595991 CET	49740	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:36:10.120619059 CET	587	49740	166.62.27.57	192.168.2.5
Nov 20, 2020 15:36:10.121017933 CET	49740	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:36:10.392924070 CET	587	49740	166.62.27.57	192.168.2.5
Nov 20, 2020 15:36:10.439893007 CET	49740	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:36:10.448016882 CET	49740	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:36:10.720060110 CET	587	49740	166.62.27.57	192.168.2.5
Nov 20, 2020 15:36:10.723824978 CET	49740	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:36:11.006926060 CET	587	49740	166.62.27.57	192.168.2.5
Nov 20, 2020 15:36:11.008655071 CET	49740	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:36:11.280472040 CET	587	49740	166.62.27.57	192.168.2.5
Nov 20, 2020 15:36:11.280853987 CET	49740	587	192.168.2.5	166.62.27.57
Nov 20, 2020 15:36:11.553639889 CET	587	49740	166.62.27.57	192.168.2.5
Nov 20, 2020 15:36:11.596276045 CET	49740	587	192.168.2.5	166.62.27.57

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:35:22.485043049 CET	52441	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:22.512227058 CET	53	52441	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:23.208142042 CET	62176	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:23.235186100 CET	53	62176	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:35:23.995783091 CET	59596	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:24.023004055 CET	53	59596	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:24.719803095 CET	65296	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:24.746911049 CET	53	65296	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:25.369910955 CET	63183	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:25.397202015 CET	53	63183	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:26.177361012 CET	60151	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:26.223524094 CET	53	60151	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:26.435781002 CET	56969	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:26.473666906 CET	53	56969	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:26.560717106 CET	55161	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:26.600693941 CET	53	55161	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:29.742211103 CET	54757	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:29.777884960 CET	53	54757	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:30.927819014 CET	49992	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:30.954982996 CET	53	49992	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:31.373215914 CET	60075	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:31.409970999 CET	53	60075	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:34.082715034 CET	55016	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:34.109980106 CET	53	55016	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:35.164407015 CET	64345	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:35.191513062 CET	53	64345	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:37.027270079 CET	57128	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:37.084184885 CET	53	57128	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:38.597119093 CET	54791	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:38.635288000 CET	53	54791	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:38.655385971 CET	50463	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:38.682647943 CET	53	50463	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:53.465348005 CET	50394	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:53.511528969 CET	53	50394	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:53.852731943 CET	58530	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:53.888447046 CET	53	58530	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:55.023741007 CET	53813	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:55.059571981 CET	53	53813	8.8.8.8	192.168.2.5
Nov 20, 2020 15:35:58.005474091 CET	63732	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:35:58.032727957 CET	53	63732	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:03.671190977 CET	57344	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:03.717258930 CET	53	57344	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:04.601073027 CET	54450	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:04.636589050 CET	53	54450	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:05.352711916 CET	59261	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:05.388645887 CET	53	59261	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:05.818730116 CET	57151	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:05.854357958 CET	53	57151	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:06.149993896 CET	59413	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:06.185600042 CET	53	59413	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:08.338323116 CET	60516	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:08.365674973 CET	53	60516	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:08.549774885 CET	51649	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:08.587776899 CET	53	51649	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:09.024678946 CET	65086	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:09.060378075 CET	53	65086	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:09.269169092 CET	56432	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:09.304965973 CET	53	56432	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:09.714523077 CET	52929	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:09.741713047 CET	53	52929	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:10.749423981 CET	64317	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:10.785088062 CET	53	64317	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:12.220356941 CET	61004	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:12.264134884 CET	53	61004	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:13.368071079 CET	56895	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:13.405908108 CET	53	56895	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:13.877084970 CET	62372	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:13.904150009 CET	53	62372	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:36:15.087770939 CET	61515	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:15.124664068 CET	53	61515	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:21.511286974 CET	56675	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:21.546901941 CET	53	56675	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:21.999161005 CET	57172	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:22.034761906 CET	53	57172	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:22.141558886 CET	55267	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:22.179312944 CET	53	55267	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:25.500250101 CET	50969	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:25.527271032 CET	53	50969	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:35.422328949 CET	64362	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:35.457957983 CET	53	64362	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:35.715254068 CET	54766	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:35.750921011 CET	53	54766	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:35.838325024 CET	61446	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:35.874130964 CET	53	61446	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:38.651498079 CET	57515	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:38.697566986 CET	53	57515	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:41.010653019 CET	58199	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:41.037905931 CET	53	58199	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:48.295718908 CET	65221	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:48.331558943 CET	53	65221	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:59.161374092 CET	61573	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:59.199176073 CET	53	61573	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:59.228987932 CET	56562	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:59.257011890 CET	53	56562	8.8.8.8	192.168.2.5
Nov 20, 2020 15:36:59.310436010 CET	53591	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:36:59.346191883 CET	53	53591	8.8.8.8	192.168.2.5
Nov 20, 2020 15:37:17.825516939 CET	59688	53	192.168.2.5	8.8.8.8
Nov 20, 2020 15:37:17.869319916 CET	53	59688	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 15:35:26.177361012 CET	192.168.2.5	8.8.8.8	0x2a1c	Standard query (0)	194.167.4.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 20, 2020 15:35:26.435781002 CET	192.168.2.5	8.8.8.8	0xfe21	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:35:26.560717106 CET	192.168.2.5	8.8.8.8	0x5f15	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:35:38.597119093 CET	192.168.2.5	8.8.8.8	0xd370	Standard query (0)	mail.iigcest.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:35:53.465348005 CET	192.168.2.5	8.8.8.8	0xa285	Standard query (0)	194.167.4.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 20, 2020 15:35:53.852731943 CET	192.168.2.5	8.8.8.8	0x4211	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:35:55.023741007 CET	192.168.2.5	8.8.8.8	0x20d1	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:09.269169092 CET	192.168.2.5	8.8.8.8	0x5551	Standard query (0)	mail.iigcest.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:12.220356941 CET	192.168.2.5	8.8.8.8	0x40ef	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:21.511286974 CET	192.168.2.5	8.8.8.8	0x4b0e	Standard query (0)	194.167.4.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 20, 2020 15:36:21.999161005 CET	192.168.2.5	8.8.8.8	0x99e4	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:22.141558886 CET	192.168.2.5	8.8.8.8	0x7ed8	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:35.422328949 CET	192.168.2.5	8.8.8.8	0xb6a7	Standard query (0)	194.167.4.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 20, 2020 15:36:35.715254068 CET	192.168.2.5	8.8.8.8	0x5be9	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:35.838325024 CET	192.168.2.5	8.8.8.8	0x87be	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:48.295718908 CET	192.168.2.5	8.8.8.8	0xbe2c	Standard query (0)	mail.iigcest.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:59.161374092 CET	192.168.2.5	8.8.8.8	0x2abe	Standard query (0)	194.167.4.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 15:36:59.228987932 CET	192.168.2.5	8.8.8.8	0xa2ff	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:59.310436010 CET	192.168.2.5	8.8.8.8	0x2337	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:17.825516939 CET	192.168.2.5	8.8.8.8	0x951a	Standard query (0)	mail.iigcest.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 15:35:26.223524094 CET	8.8.8.8	192.168.2.5	0x2a1c	Name error (3)	194.167.4.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 20, 2020 15:35:26.473666906 CET	8.8.8.8	192.168.2.5	0xfe21	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:35:26.473666906 CET	8.8.8.8	192.168.2.5	0xfe21	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:35:26.600693941 CET	8.8.8.8	192.168.2.5	0x5f15	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:35:26.600693941 CET	8.8.8.8	192.168.2.5	0x5f15	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:35:38.635288000 CET	8.8.8.8	192.168.2.5	0xd370	No error (0)	mail.iigcest.com		166.62.27.57	A (IP address)	IN (0x0001)
Nov 20, 2020 15:35:53.511528969 CET	8.8.8.8	192.168.2.5	0xa285	Name error (3)	194.167.4.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 20, 2020 15:35:53.888447046 CET	8.8.8.8	192.168.2.5	0x4211	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:35:53.888447046 CET	8.8.8.8	192.168.2.5	0x4211	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:35:55.059571981 CET	8.8.8.8	192.168.2.5	0x20d1	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:35:55.059571981 CET	8.8.8.8	192.168.2.5	0x20d1	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:09.304965973 CET	8.8.8.8	192.168.2.5	0x5551	No error (0)	mail.iigcest.com		166.62.27.57	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:12.264134884 CET	8.8.8.8	192.168.2.5	0x40ef	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:36:21.546901941 CET	8.8.8.8	192.168.2.5	0x4b0e	Name error (3)	194.167.4.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 20, 2020 15:36:22.034761906 CET	8.8.8.8	192.168.2.5	0x99e4	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:22.034761906 CET	8.8.8.8	192.168.2.5	0x99e4	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:22.179312944 CET	8.8.8.8	192.168.2.5	0x7ed8	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:22.179312944 CET	8.8.8.8	192.168.2.5	0x7ed8	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:35.457957983 CET	8.8.8.8	192.168.2.5	0xb6a7	Name error (3)	194.167.4.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 20, 2020 15:36:35.750921011 CET	8.8.8.8	192.168.2.5	0x5be9	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:35.750921011 CET	8.8.8.8	192.168.2.5	0x5be9	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:35.874130964 CET	8.8.8.8	192.168.2.5	0x87be	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 15:36:35.874130964 CET	8.8.8.8	192.168.2.5	0x87be	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:48.331558943 CET	8.8.8.8	192.168.2.5	0xbe2c	No error (0)	mail.iigcest.com		166.62.27.57	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:59.199176073 CET	8.8.8.8	192.168.2.5	0x2abe	Name error (3)	194.167.4.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 20, 2020 15:36:59.257011890 CET	8.8.8.8	192.168.2.5	0xa2ff	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:59.257011890 CET	8.8.8.8	192.168.2.5	0xa2ff	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:59.346191883 CET	8.8.8.8	192.168.2.5	0x2337	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:59.346191883 CET	8.8.8.8	192.168.2.5	0x2337	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:17.869319916 CET	8.8.8.8	192.168.2.5	0x951a	No error (0)	mail.iigcest.com		166.62.27.57	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	192.168.2.5	49713	104.16.155.36	80	C:\Users\user\Desktop\PURCHASE ORDER.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 15:35:26.510627031 CET	65	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 20, 2020 15:35:26.551008940 CET	65	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 20 Nov 2020 14:35:26 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Fri, 20 Nov 2020 15:35:26 GMT Location: https://whatismyipaddress.com/ cf-request-id: 0687adedb90000178272bcf000000001 Server: cloudflare CF-RAY: 5f52e5c2caab1782-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49728	104.16.155.36	80	C:\Users\user\Desktop\PURCHASE ORDER.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 15:35:54.918652058 CET	193	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 20, 2020 15:35:54.954479933 CET	193	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 20 Nov 2020 14:35:54 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Fri, 20 Nov 2020 15:35:54 GMT Location: https://whatismyipaddress.com/ cf-request-id: 0687ae5cb1000005c44690f000000001 Server: cloudflare CF-RAY: 5f52e6744e3a05c4-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49752	104.16.155.36	80	C:\Users\user\Desktop\PURCHASE ORDER.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 15:36:22.089561939 CET	5819	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 20, 2020 15:36:22.114939928 CET	5819	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 20 Nov 2020 14:36:22 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Fri, 20 Nov 2020 15:36:22 GMT Location: https://whatismyipaddress.com/ cf-request-id: 0687aec6d4000005bb99ada000000001 Server: cloudflare CF-RAY: 5f52e71e1fb005bb-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49757	104.16.155.36	80	C:\Users\user\Desktop\PURCHASE ORDER.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 15:36:35.808811903 CET	5858	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 20, 2020 15:36:35.830921888 CET	5858	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 20 Nov 2020 14:36:35 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Fri, 20 Nov 2020 15:36:35 GMT Location: https://whatismyipaddress.com/ cf-request-id: 0687aefc6b0000d6d59004c000000001 Server: cloudflare CF-RAY: 5f52e773db84d6d5-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49764	104.16.155.36	80	C:\Users\user\Desktop\PURCHASE ORDER.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 15:36:59.282638073 CET	5888	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 20, 2020 15:36:59.305939913 CET	5888	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 20 Nov 2020 14:36:59 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Fri, 20 Nov 2020 15:36:59 GMT Location: https://whatismyipaddress.com/ cf-request-id: 0687af581d00002bd6a0220000000001 Server: cloudflare CF-RAY: 5f52e8069d332bd6-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 15:35:39.467190027 CET	587	49724	166.62.27.57	192.168.2.5	220-sg2plcpnl0157.prod.sin2.secureserver.net ESMTP Exim 4.93 #2 Fri, 20 Nov 2020 07:35:39 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 20, 2020 15:35:39.467962980 CET	49724	587	192.168.2.5	166.62.27.57	EHLO 305090

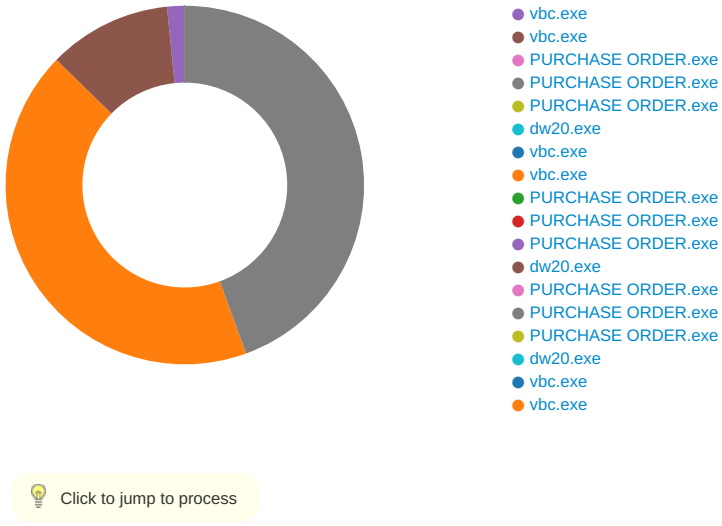
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 15:35:39.749670982 CET	587	49724	166.62.27.57	192.168.2.5	250-sg2plcpnl0157.prod.sin2.secureserver.net Hello 305090 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP
Nov 20, 2020 15:35:39.750130892 CET	49724	587	192.168.2.5	166.62.27.57	AUTH login YW5zYWZAaWlnY2VzdC5jb20=
Nov 20, 2020 15:35:40.031795025 CET	587	49724	166.62.27.57	192.168.2.5	334 UGFzc3dvcmQ6
Nov 20, 2020 15:35:40.325931072 CET	587	49724	166.62.27.57	192.168.2.5	235 Authentication succeeded
Nov 20, 2020 15:35:40.326431990 CET	49724	587	192.168.2.5	166.62.27.57	MAIL FROM:<ansaf@iigcest.com>
Nov 20, 2020 15:35:40.608051062 CET	587	49724	166.62.27.57	192.168.2.5	250 OK
Nov 20, 2020 15:35:40.608349085 CET	49724	587	192.168.2.5	166.62.27.57	RCPT TO:<ansaf@iigcest.com>
Nov 20, 2020 15:35:40.891452074 CET	587	49724	166.62.27.57	192.168.2.5	250 Accepted
Nov 20, 2020 15:35:40.891730070 CET	49724	587	192.168.2.5	166.62.27.57	DATA
Nov 20, 2020 15:35:41.172899008 CET	587	49724	166.62.27.57	192.168.2.5	354 Enter message, ending with "." on a line by itself
Nov 20, 2020 15:35:41.174180984 CET	49724	587	192.168.2.5	166.62.27.57	.
Nov 20, 2020 15:35:41.484783888 CET	587	49724	166.62.27.57	192.168.2.5	250 OK id=1kg7Vk-004UTj-W8
Nov 20, 2020 15:36:10.120619059 CET	587	49740	166.62.27.57	192.168.2.5	220-sg2plcpnl0157.prod.sin2.secureserver.net ESMTP Exim 4.93 #2 Fri, 20 Nov 2020 07:36:09 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 20, 2020 15:36:10.121017933 CET	49740	587	192.168.2.5	166.62.27.57	EHLO 305090
Nov 20, 2020 15:36:10.392924070 CET	587	49740	166.62.27.57	192.168.2.5	250-sg2plcpnl0157.prod.sin2.secureserver.net Hello 305090 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP
Nov 20, 2020 15:36:10.448016882 CET	49740	587	192.168.2.5	166.62.27.57	AUTH login YW5zYWZAaWlnY2VzdC5jb20=
Nov 20, 2020 15:36:10.720060110 CET	587	49740	166.62.27.57	192.168.2.5	334 UGFzc3dvcmQ6
Nov 20, 2020 15:36:11.006926060 CET	587	49740	166.62.27.57	192.168.2.5	235 Authentication succeeded
Nov 20, 2020 15:36:11.008655071 CET	49740	587	192.168.2.5	166.62.27.57	MAIL FROM:<ansaf@iigcest.com>
Nov 20, 2020 15:36:11.280472040 CET	587	49740	166.62.27.57	192.168.2.5	250 OK
Nov 20, 2020 15:36:11.280853987 CET	49740	587	192.168.2.5	166.62.27.57	RCPT TO:<ansaf@iigcest.com>
Nov 20, 2020 15:36:11.553639889 CET	587	49740	166.62.27.57	192.168.2.5	250 Accepted
Nov 20, 2020 15:36:11.655267000 CET	49740	587	192.168.2.5	166.62.27.57	DATA
Nov 20, 2020 15:36:11.927423954 CET	587	49740	166.62.27.57	192.168.2.5	354 Enter message, ending with "." on a line by itself
Nov 20, 2020 15:36:11.928617954 CET	49740	587	192.168.2.5	166.62.27.57	.
Nov 20, 2020 15:36:12.212925911 CET	587	49740	166.62.27.57	192.168.2.5	250 OK id=1kg7WF-004V9z-OV
Nov 20, 2020 15:36:48.885966063 CET	587	49762	166.62.27.57	192.168.2.5	220-sg2plcpnl0157.prod.sin2.secureserver.net ESMTP Exim 4.93 #2 Fri, 20 Nov 2020 07:36:48 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 20, 2020 15:36:49.445619106 CET	49762	587	192.168.2.5	166.62.27.57	EHLO 305090
Nov 20, 2020 15:36:49.717065096 CET	587	49762	166.62.27.57	192.168.2.5	250-sg2plcpnl0157.prod.sin2.secureserver.net Hello 305090 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP
Nov 20, 2020 15:36:49.717490911 CET	49762	587	192.168.2.5	166.62.27.57	AUTH login YW5zYWZAaWlnY2VzdC5jb20=
Nov 20, 2020 15:36:49.988996029 CET	587	49762	166.62.27.57	192.168.2.5	334 UGFzc3dvcmQ6
Nov 20, 2020 15:36:50.267446995 CET	587	49762	166.62.27.57	192.168.2.5	235 Authentication succeeded
Nov 20, 2020 15:36:50.267868042 CET	49762	587	192.168.2.5	166.62.27.57	MAIL FROM:<ansaf@iigcest.com>
Nov 20, 2020 15:36:50.539273024 CET	587	49762	166.62.27.57	192.168.2.5	250 OK
Nov 20, 2020 15:36:50.539747000 CET	49762	587	192.168.2.5	166.62.27.57	RCPT TO:<ansaf@iigcest.com>
Nov 20, 2020 15:36:50.811964035 CET	587	49762	166.62.27.57	192.168.2.5	250 Accepted
Nov 20, 2020 15:36:50.812480927 CET	49762	587	192.168.2.5	166.62.27.57	DATA
Nov 20, 2020 15:36:51.083787918 CET	587	49762	166.62.27.57	192.168.2.5	354 Enter message, ending with "." on a line by itself
Nov 20, 2020 15:36:51.086323023 CET	49762	587	192.168.2.5	166.62.27.57	.
Nov 20, 2020 15:36:51.389682055 CET	587	49762	166.62.27.57	192.168.2.5	250 OK id=1kg7Ws-004VvN-TF

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 15:37:18.426717043 CET	587	49767	166.62.27.57	192.168.2.5	220-sg2plcpnl0157.prod.sin2.secureserver.net ESMTP Exim 4.93 #2 Fri, 20 Nov 2020 07:37:18 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 20, 2020 15:37:18.427113056 CET	49767	587	192.168.2.5	166.62.27.57	EHLO 305090
Nov 20, 2020 15:37:18.702619076 CET	587	49767	166.62.27.57	192.168.2.5	250-sg2plcpnl0157.prod.sin2.secureserver.net Hello 305090 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP
Nov 20, 2020 15:37:18.703283072 CET	49767	587	192.168.2.5	166.62.27.57	AUTH login YW5zYWZAaWlnY2VzdC5jb20=
Nov 20, 2020 15:37:18.978506088 CET	587	49767	166.62.27.57	192.168.2.5	334 UGFzc3dvcmQ6
Nov 20, 2020 15:37:19.284562111 CET	587	49767	166.62.27.57	192.168.2.5	235 Authentication succeeded
Nov 20, 2020 15:37:19.284941912 CET	49767	587	192.168.2.5	166.62.27.57	MAIL FROM:<ansaf@iigcest.com>
Nov 20, 2020 15:37:19.559722900 CET	587	49767	166.62.27.57	192.168.2.5	250 OK
Nov 20, 2020 15:37:19.560230970 CET	49767	587	192.168.2.5	166.62.27.57	RCPT TO:<ansaf@iigcest.com>
Nov 20, 2020 15:37:19.836273909 CET	587	49767	166.62.27.57	192.168.2.5	250 Accepted
Nov 20, 2020 15:37:19.836848021 CET	49767	587	192.168.2.5	166.62.27.57	DATA
Nov 20, 2020 15:37:20.111982107 CET	587	49767	166.62.27.57	192.168.2.5	354 Enter message, ending with "." on a line by itself
Nov 20, 2020 15:37:20.113253117 CET	49767	587	192.168.2.5	166.62.27.57	.
Nov 20, 2020 15:37:20.414644957 CET	587	49767	166.62.27.57	192.168.2.5	250 OK id=1kg7XL-004WZO-UM

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: PURCHASE ORDER.exe PID: 6508 Parent PID: 5720

General

Start time:	15:35:18
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PURCHASE ORDER.exe'
Imagebase:	0x400000
File size:	973824 bytes
MD5 hash:	8E2337F7CDD4BCD18E862B7A73734D49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.243036472.0000000002717000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.243036472.0000000002717000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.243036472.0000000002717000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.243036472.0000000002717000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.243036472.0000000002717000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.242972972.0000000002682000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.242972972.0000000002682000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.242972972.0000000002682000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.242972972.0000000002682000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.242972972.0000000002682000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: PURCHASE ORDER.exe PID: 6524 Parent PID: 6508

General

Start time:	15:35:18
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PURCHASE ORDER.exe'
Imagebase:	0x400000
File size:	973824 bytes
MD5 hash:	8E2337F7CDD4BCD18E862B7A73734D49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000002.296134787.0000000003BC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.296134787.0000000003BC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000002.292566171.0000000000B92000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000002.292566171.0000000000B92000.00000004.00000001.sdmp, Author: Joe Security

	• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.292566171.0000000000B92000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.292566171.0000000000B92000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000002.292566171.0000000000B92000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000002.292013464.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000002.292013464.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.292013464.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.292013464.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000002.292013464.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000002.293899335.0000000002BC1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.293899335.0000000002BC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000002.293899335.0000000002BC1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000002.292462185.0000000000AE0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000002.292462185.0000000000AE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.292462185.0000000000AE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.292462185.0000000000AE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000002.292462185.0000000000AE0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000002.291882316.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000002.291882316.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.291882316.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.291882316.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000002.291882316.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000002.292688488.0000000002412000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000002.292688488.0000000002412000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.292688488.0000000002412000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.292688488.0000000002412000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000002.292688488.0000000002412000.00000040.00000001.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	72B860AC	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	72B860AC	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	72B860AC	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	72B860AC	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	24DBCAB	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	24DBCAB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	2BA5E86	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	2BA5E86	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	36 35 32 34	6524	success or wait	1	2BA0093	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	42	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 50 55 52 43 48 41 53 45 20 4f 52 44 45 52 2e 65 78 65	C:\Users\user\Desktop\PURCHASE ORDER.exe	success or wait	1	2BA0093	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	2BA0093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2BA0093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	2BA0093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2BA0093	ReadFile
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	2BA0093	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	2BA0093	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	2BA0093	ReadFile
C:\Users\user\Desktop\PURCHASE ORDER.exe	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Users\user\Desktop\PURCHASE ORDER.exe	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72C5BF06	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72C5BF06	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	dword	2	1	success or wait	1	2BA5326	RegSetValueExW

Analysis Process: PURCHASE ORDER.exe PID: 6532 Parent PID: 6508

General

Start time:	15:35:19
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PURCHASE ORDER.exe' 2 6524 7175453
Imagebase:	0x400000
File size:	973824 bytes
MD5 hash:	8E2337F7CDD4BCD18E862B7A73734D49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: dw20.exe PID: 6732 Parent PID: 6524

General

Start time:	15:35:26
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2104
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: 6928 Parent PID: 6524

General

Start time:	15:35:29
Start date:	20/11/2020
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: 00000007.00000002.264672646.0000000000400000.00000040.00000001.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: 6940 Parent PID: 6524

General

Start time:	15:35:29
Start date:	20/11/2020
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:	0x7ff797770000
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: 00000008.00000002.268465330.0000000000400000.00000040.00000001.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: PURCHASE ORDER.exe PID: 764 Parent PID: 6532

General

Start time:	15:35:47
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Imagebase:	0x400000
File size:	973824 bytes
MD5 hash:	8E2337F7CDD4BCD18E862B7A73734D49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000002.306410027.0000000002782000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000002.306410027.0000000002782000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000002.306410027.0000000002782000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000002.306410027.0000000002782000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000002.306410027.0000000002782000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000002.306634331.0000000002817000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000002.306634331.0000000002817000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000002.306634331.0000000002817000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000002.306634331.0000000002817000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000002.306634331.0000000002817000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: PURCHASE ORDER.exe PID: 6952 Parent PID: 764

General

Start time:	15:35:48
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Imagebase:	0x400000
File size:	973824 bytes
MD5 hash:	8E2337F7CDD4BCD18E862B7A73734D49
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: 00000012.00000002.354079025.00000000022F2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000002.354079025.00000000022F2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000002.354079025.00000000022F2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000002.354079025.00000000022F2000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000002.354079025.00000000022F2000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000012.00000002.353139620.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000002.353139620.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000002.353139620.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000002.353139620.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000002.353139620.0000000000497000.00000040.00000001.sdmp, Author:

	JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000002.356703266.0000000003AB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000002.356703266.0000000003AB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000012.00000002.353893754.00000000021B0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000002.353893754.00000000021B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000002.353893754.00000000021B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000002.353893754.00000000021B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000002.353893754.00000000021B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000012.00000002.353046935.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000002.353046935.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000002.353046935.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000002.353046935.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000002.353046935.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000012.00000002.353958056.0000000002242000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000002.353958056.0000000002242000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000002.353958056.0000000002242000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000002.353958056.0000000002242000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000002.353958056.0000000002242000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000012.00000002.355012308.0000000002AB1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000002.355012308.0000000002AB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000002.355012308.0000000002AB1000.00000004.00000001.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	72B860AC	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	72B860AC	unknown

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	72B860AC	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	72B860AC	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	239BCAB	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	239BCAB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	success or wait	1	2512D8E	DeleteFileW
C:\Users\user\AppData\Roaming\pidloc.txt	success or wait	1	2512D8E	DeleteFileW
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	2512D8E	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	2512D8E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	36 39 35 32	6952	success or wait	1	2510093	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	42	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 50 55 52 43 48 41 53 45 20 4f 52 44 45 52 2e 65 78 65	C:\Users\user\Desktop\PURCHASE ORDER.exe	success or wait	1	2510093	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	2510093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2510093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	2510093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2510093	ReadFile
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	2510093	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	2510093	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	2510093	ReadFile
C:\Users\user\Desktop\PURCHASE ORDER.exe	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Users\user\Desktop\PURCHASE ORDER.exe	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72C5BF06	unknown

Analysis Process: PURCHASE ORDER.exe PID: 5552 Parent PID: 764

General

Start time:	15:35:49
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PURCHASE ORDER.exe' 2 6952 7204953
Imagebase:	0x400000
File size:	973824 bytes
MD5 hash:	8E2337F7CDD4BCD18E862B7A73734D49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: dw20.exe PID: 1112 Parent PID: 6952

General

Start time:	15:35:55
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2112
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: 1236 Parent PID: 6952

General

Start time:	15:35:58
Start date:	20/11/2020
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:	0x7ff797770000
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: 00000015.00000002.325960552.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 3720 Parent PID: 6952

General

Start time:	15:35:58
Start date:	20/11/2020
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: 00000016.00000002.335094690.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: PURCHASE ORDER.exe PID: 1396 Parent PID: 5552

General

Start time:	15:36:15
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Imagebase:	0x400000
File size:	973824 bytes
MD5 hash:	8E2337F7CDD4BCD18E862B7A73734D49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001C.00000002.368097670.0000000002817000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001C.00000002.368097670.0000000002817000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000002.368097670.0000000002817000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000002.368097670.0000000002817000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001C.00000002.368097670.0000000002817000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001C.00000002.367864416.0000000002782000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001C.00000002.367864416.0000000002782000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000002.367864416.0000000002782000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000002.367864416.0000000002782000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001C.00000002.367864416.0000000002782000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: PURCHASE ORDER.exe PID: 5140 Parent PID: 1396

General

Start time:	15:36:16
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Imagebase:	0x400000
File size:	973824 bytes
MD5 hash:	8E2337F7CDD4BCD18E862B7A73734D49
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: 0000001D.00000002.382207742.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001D.00000002.382207742.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.382207742.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000002.382207742.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001D.00000002.382207742.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001D.00000002.383019570.00000000023B2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001D.00000002.383019570.00000000023B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.383019570.00000000023B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000002.383019570.00000000023B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001D.00000002.383019570.00000000023B2000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.384995181.0000000002FF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001D.00000002.384995181.0000000002FF0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001D.00000002.382905012.0000000002322000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001D.00000002.382905012.0000000002322000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.382905012.0000000002322000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000002.382905012.0000000002322000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001D.00000002.382905012.0000000002322000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001D.00000002.382096293.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001D.00000002.382096293.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.382096293.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000002.382096293.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001D.00000002.382096293.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.385013929.0000000002FF6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001D.00000002.385265608.0000000003B71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000002.385265608.0000000003B71000.00000004.00000001.sdmp, Author:

	Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001D.00000002.382801146.0000000002290000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001D.00000002.382801146.0000000002290000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.382801146.0000000002290000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000002.382801146.0000000002290000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001D.00000002.382801146.0000000002290000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: PURCHASE ORDER.exe PID: 3100 Parent PID: 1396

General

Start time:	15:36:17
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PURCHASE ORDER.exe' 2 5140 7233203
Imagebase:	0x400000
File size:	973824 bytes
MD5 hash:	8E2337F7CDD4BCD18E862B7A73734D49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: dw20.exe PID: 5468 Parent PID: 5140

General

Start time:	15:36:22
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2304
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PURCHASE ORDER.exe PID: 5772 Parent PID: 3100

General

Start time:	15:36:30
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PURCHASE ORDER.exe

Imagebase:	0x400000
File size:	973824 bytes
MD5 hash:	8E2337F7CDD4BCD18E862B7A73734D49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000021.00000002.399940578.0000000002782000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000021.00000002.399940578.0000000002782000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000021.00000002.399940578.0000000002782000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000021.00000002.399940578.0000000002782000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000021.00000002.399940578.0000000002782000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000021.00000002.400160823.0000000002817000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000021.00000002.400160823.0000000002817000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000021.00000002.400160823.0000000002817000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000021.00000002.400160823.0000000002817000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000021.00000002.400160823.0000000002817000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: PURCHASE ORDER.exe PID: 5076 Parent PID: 5772

General

Start time:	15:36:31
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Imagebase:	0x400000
File size:	973824 bytes
MD5 hash:	8E2337F7CDD4BCD18E862B7A73734D49
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: 00000022.00000002.444523132.0000000002392000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000002.444523132.0000000002392000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000002.444523132.0000000002392000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000022.00000002.444523132.0000000002392000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000002.444523132.0000000002392000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000022.00000002.443510229.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000002.443510229.0000000000497000.00000040.00000001.sdmp, Author: Joe Security

	• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000002.443510229.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000022.00000002.443510229.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000002.443510229.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000022.00000002.445346649.0000000002A41000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000002.445346649.0000000002A41000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000002.445346649.0000000002A41000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000022.00000002.444206771.0000000002282000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000002.444206771.0000000002282000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000002.444206771.0000000002282000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000022.00000002.444206771.0000000002282000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000002.444206771.0000000002282000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000022.00000002.443391424.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000002.443391424.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000002.443391424.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000022.00000002.443391424.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000002.443391424.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000022.00000002.443761363.0000000000680000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000002.443761363.0000000000680000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000002.443761363.0000000000680000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000022.00000002.443761363.0000000000680000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000002.443761363.0000000000680000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000002.446960963.0000000003A41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000022.00000002.446960963.0000000003A41000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: PURCHASE ORDER.exe PID: 6660 Parent PID: 5772

General

Start time:	15:36:32
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PURCHASE ORDER.exe' 2 5076 7248218
Imagebase:	0x400000
File size:	973824 bytes
MD5 hash:	8E2337F7CDD4BCD18E862B7A73734D49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: dw20.exe PID: 4684 Parent PID: 5076

General

Start time:	15:36:35
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2272
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: 6536 Parent PID: 5076

General

Start time:	15:36:38
Start date:	20/11/2020
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: 00000026.00000002.413012282.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 6312 Parent PID: 5076

General

Start time:	15:36:38
Start date:	20/11/2020
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: 00000027.00000002.417706986.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis