ID: 319596
Sample Name: Prueba de pago.exe
Cookbook: default.jbs
Time: 13:22:12
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Prueba de pago.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Threatname: HawkEye 5
Yara Overview 5
Dropped Files 6
Memory Dumps 6
Unpacked PEs 6
Sigma Overview 7
Signature Overview 7
AV Detection: 7
Networking: 8
Key, Mouse, Clipboard, Microphone and Screen Capturing: 8
System Summary: 8
Data Obfuscation: 8
Hooking and other Techniques for Hiding and Protection: 8
Malware Analysis System Evasion: 8
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 9
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 12
URLs 12
Domains and IPs 14
Contacted Domains 14
Contacted URLs 14
URLs from Memory and Binaries 14
Contacted IPs 19
Public 20
Private 20
General Information 20
Simulations 21
Behavior and APIs 21
Joe Sandbox View / Context 22
IPs 22
Domains 22
ASN 23
JA3 Fingerprints 24
Dropped Files 24
Created / dropped Files 24
Static File Info 30
General 30
File Icon 30

Static PE Info 30
General 30
Entrypoint Preview 31
Data Directories 32
Sections 32
Resources 33
Imports 34
Possible Origin 34
Network Behavior 35
Network Port Distribution 35
TCP Packets 35
UDP Packets 36
DNS Queries 37
DNS Answers 38
HTTP Request Dependency Graph 38
HTTP Packets 38
SMTP Packets 39
Code Manipulations 39
Statistics 40
Behavior 40
System Behavior 40
Analysis Process: Prueba de pago.exe PID: 5080 Parent PID: 5684 40
General 40
Analysis Process: Prueba de pago.exe PID: 2168 Parent PID: 5080 41
General 41
File Activities 42
File Created 42
File Written 43
File Read 44
Analysis Process: Windows Update.exe PID: 5672 Parent PID: 2168 44
General 44
Analysis Process: Windows Update.exe PID: 5388 Parent PID: 5672 45
General 45
File Activities 46
File Created 47
File Deleted 47
File Written 47
File Read 48
Registry Activities 48
Key Value Created 48
Key Value Modified 49
Analysis Process: dw20.exe PID: 2220 Parent PID: 5388 49
General 49
File Activities 49
Registry Activities 49
Analysis Process: vbc.exe PID: 6120 Parent PID: 5388 49
General 49
File Activities 50
File Created 50
Analysis Process: vbc.exe PID: 3484 Parent PID: 5388 50
General 50
File Activities 50
File Created 50
File Written 50
File Read 50
Analysis Process: WerFault.exe PID: 4112 Parent PID: 5388 51
General 51
File Activities 51
File Created 51
File Deleted 51
Analysis Process: WindowsUpdate.exe PID: 6328 Parent PID: 3388 52
General 52
Analysis Process: WindowsUpdate.exe PID: 6392 Parent PID: 6328 52
General 52
Analysis Process: Windows Update.exe PID: 6456 Parent PID: 6392 54
General 54
Analysis Process: Windows Update.exe PID: 6476 Parent PID: 6456 54
General 54
Analysis Process: dw20.exe PID: 7024 Parent PID: 6476 56
General 56

Disassembly 56
Code Analysis 56

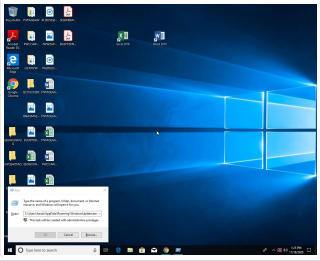
Analysis Report Prueba de pago.exe

Overview

General Information

Sample Name:	Prueba de pago.exe
Analysis ID:	319596
MD5:	b3a244a097904a..
SHA1:	b16032d83c91ee..
SHA256:	286b416351f4ca6.
Tags:	ESP exe geo HawkEye

Most interesting Screenshot:



Detection

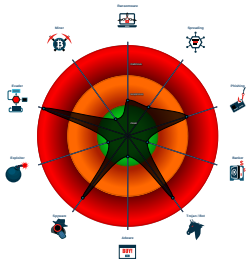
HawkEye
MailPassView

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 dropp…
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code contains potentia…
- .NET source code references suspic…
- Allocates memory in foreign process…
- Changes the view of files in windows…

Classification



Startup

- **System is w10x64**
- Prueba de pago.exe (PID: 5080 cmdline: 'C:\Users\user\Desktop\Prueba de pago.exe' MD5: B3A244A097904A4D6689A582D7EC9985)
  - Prueba de pago.exe (PID: 2168 cmdline: 'C:\Users\user\Desktop\Prueba de pago.exe' MD5: B3A244A097904A4D6689A582D7EC9985)
    - Windows Update.exe (PID: 5672 cmdline: 'C:\Users\user\AppData\Roaming\Windows Update.exe' MD5: B3A244A097904A4D6689A582D7EC9985)
      - Windows Update.exe (PID: 5388 cmdline: 'C:\Users\user\AppData\Roaming\Windows Update.exe' MD5: B3A244A097904A4D6689A582D7EC9985)
        - dw20.exe (PID: 2220 cmdline: dw20.exe -x -s 2384 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
        - vbc.exe (PID: 6120 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: 3484 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
        - WerFault.exe (PID: 4112 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5388 -s 2488 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- WindowsUpdate.exe (PID: 6328 cmdline: 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' MD5: B3A244A097904A4D6689A582D7EC9985)
  - WindowsUpdate.exe (PID: 6392 cmdline: 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' MD5: B3A244A097904A4D6689A582D7EC9985)
    - Windows Update.exe (PID: 6456 cmdline: 'C:\Users\user\AppData\Roaming\Windows Update.exe' MD5: B3A244A097904A4D6689A582D7EC9985)
      - Windows Update.exe (PID: 6476 cmdline: 'C:\Users\user\AppData\Roaming\Windows Update.exe' MD5: B3A244A097904A4D6689A582D7EC9985)
        - dw20.exe (PID: 7024 cmdline: dw20.exe -x -s 2376 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
- **cleanup**

Malware Configuration

Threatname: HawkEye


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


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Windows Update.e_1044ba73b302b1a19e09d2f83986d3c5672f_ffa3413f_105a0017\Report.wer	SUSP_WER_Suspicious_Crash_Directory	Detects a crashed application executed in a suspicious directory	Florian Roth	• 0x11c:$a1: ReportIdentifier= • 0x19e:$a1: ReportIdentifier= • 0x75a:$a2: .Name=Fault Module Name • 0x4ad8:$a3: AppPath= • 0x4ad8:$l4: AppPath=C:\Users\ • 0x4ad8:$s8: AppPath=C:\Users\user\AppData\Roaming\Windows Update.exe
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1FE.tmp.mdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x56e54e:$key: HawkEyeKeylogger • 0x5707b8:$salt: 099u787978786 • 0x56ebab:$string1: HawkEye_Keylogger • 0x56f9ea:$string1: HawkEye_Keylogger • 0x570718:$string1: HawkEye_Keylogger • 0x56ef80:$string2: holdermail.txt • 0x56efa0:$string2: holdermail.txt • 0x56eec2:$string3: wallet.dat • 0x56eeda:$string3: wallet.dat • 0x56eef0:$string3: wallet.dat • 0x5702dc:$string4: Keylog Records • 0x5705f4:$string4: Keylog Records • 0x570810:$string5: do not script --> • 0x56e536:$string6: \pidloc.txt • 0x56e5c4:$string7: BSPLIT • 0x56e5d4:$string7: BSPLIT
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1FE.tmp.mdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1FE.tmp.mdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x56ec03:$hawkstr1: HawkEye Keylogger • 0x56fa30:$hawkstr1: HawkEye Keylogger • 0x56fd5f:$hawkstr1: HawkEye Keylogger • 0x56feba:$hawkstr1: HawkEye Keylogger • 0x57001d:$hawkstr1: HawkEye Keylogger • 0x5702b4:$hawkstr1: HawkEye Keylogger • 0x56e775:$hawkstr2: Dear HawkEye Customers! • 0x56fdb2:$hawkstr2: Dear HawkEye Customers! • 0x56ff09:$hawkstr2: Dear HawkEye Customers! • 0x570070:$hawkstr2: Dear HawkEye Customers! • 0x56e896:$hawkstr3: HawkEye Logger Details:

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.305646126.0000000002E26000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
0000000F.00000002.305646126.0000000002E26000.00000004.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x26a0:$hawkstr1: HawkEye Keylogger • 0x20ec:$hawkstr2: Dear HawkEye Customers! • 0x221e:$hawkstr3: HawkEye Logger Details:
0000000D.00000002.281027497.0000000000402000.00000040.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b6e3:$key: HawkEyeKeylogger • 0x7d94d:$salt: 099u787978786 • 0x7bd40:$string1: HawkEye_Keylogger • 0x7cb7f:$string1: HawkEye_Keylogger • 0x7d8ad:$string1: HawkEye_Keylogger • 0x7c115:$string2: holdermail.txt • 0x7c135:$string2: holdermail.txt • 0x7c057:$string3: wallet.dat • 0x7c06f:$string3: wallet.dat • 0x7c085:$string3: wallet.dat • 0x7d471:$string4: Keylog Records • 0x7d789:$string4: Keylog Records • 0x7d9a5:$string5: do not script --> • 0x7b6cb:$string6: \pidloc.txt • 0x7b759:$string7: BSPLIT • 0x7b769:$string7: BSPLIT
0000000D.00000002.281027497.0000000000402000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
0000000D.00000002.281027497.0000000000402000.00000040.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 200 entries				

Unpacked PEs

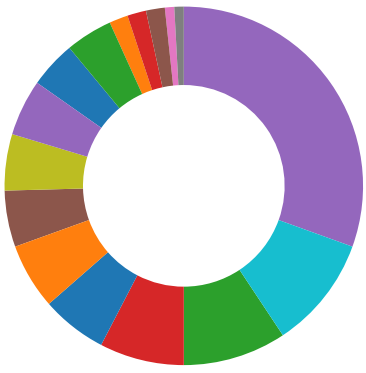
Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
1.2.Prueba de pago.exe.2460000.3.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b8e3:$key: HawkEyeKeylogger • 0x7db4d:$salt: 099u787978786 • 0x7bf40:$string1: HawkEye_Keylogger • 0x7cd7f:$string1: HawkEye_Keylogger • 0x7daad:$string1: HawkEye_Keylogger • 0x7c315:$string2: holdermail.txt • 0x7c335:$string2: holdermail.txt • 0x7c257:$string3: wallet.dat • 0x7c26f:$string3: wallet.dat • 0x7c285:$string3: wallet.dat • 0x7d671:$string4: Keylog Records • 0x7d989:$string4: Keylog Records • 0x7dba5:$string5: do not script --> • 0x7b8cb:$string6: \pidloc.txt • 0x7b959:$string7: BSPLIT • 0x7b969:$string7: BSPLIT
1.2.Prueba de pago.exe.2460000.3.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
1.2.Prueba de pago.exe.2460000.3.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
1.2.Prueba de pago.exe.2460000.3.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
1.2.Prueba de pago.exe.2460000.3.unpack	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x7bf98:$hawkstr1: HawkEye Keylogger • 0x7cdc5:$hawkstr1: HawkEye Keylogger • 0x7d0f4:$hawkstr1: HawkEye Keylogger • 0x7d24f:$hawkstr1: HawkEye Keylogger • 0x7d3b2:$hawkstr1: HawkEye Keylogger • 0x7d649:$hawkstr1: HawkEye Keylogger • 0x7bb0a:$hawkstr2: Dear HawkEye Customers! • 0x7d147:$hawkstr2: Dear HawkEye Customers! • 0x7d29e:$hawkstr2: Dear HawkEye Customers! • 0x7d405:$hawkstr2: Dear HawkEye Customers! • 0x7bc2b:$hawkstr3: HawkEye Logger Details:
Click to see the 153 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

Contains functionality to log keystrokes (.Net Source)

Installs a global keyboard hook

System Summary:

Malicious sample detected (through community Yara rule)

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)

Deletes itself after installation

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)

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

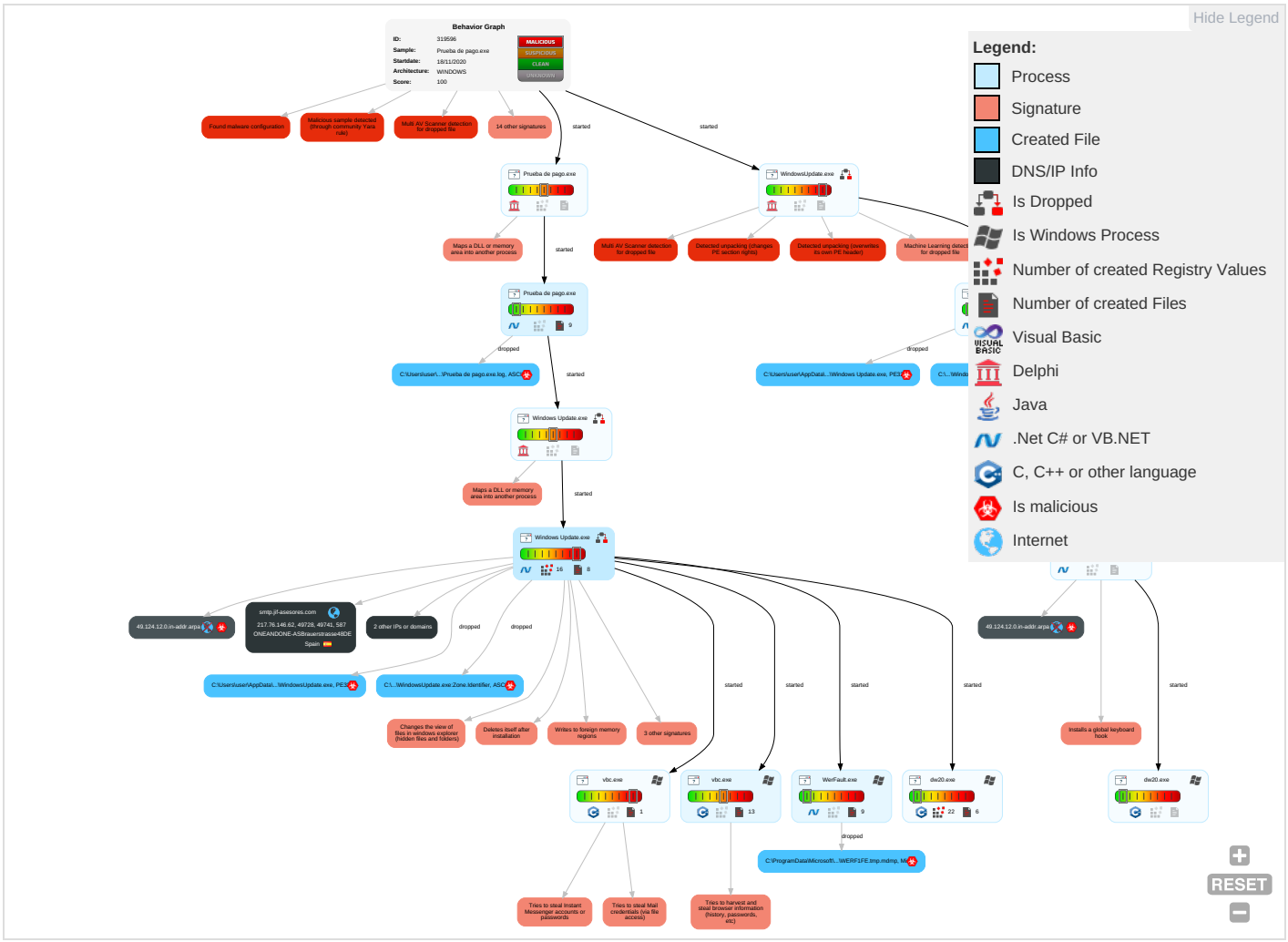
Detected HawkEye Rat

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	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over C Network Medium
Default Accounts	Native API 1 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 2 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Shared Modules 1	Registry Run Keys / Startup Folder 1	Process Injection 5 1 1	Obfuscated Files or Information 2 1	Credentials in Registry 1	File and Directory Discovery 2	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltra
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Software Packing 4 1	Credentials In Files 1	System Information Discovery 3 9	Distributed Component Object Model	Input Capture 2 2 1	Scheduled Transfe
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 2 9 1	SSH	Clipboard Data 3	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 6	VNC	GUI Input Capture	Exfiltration Over C Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protoc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Modify Registry 1	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encryp Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 6	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encry Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 5 1 1	Network Sniffing	System Network Configuration Discovery 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	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

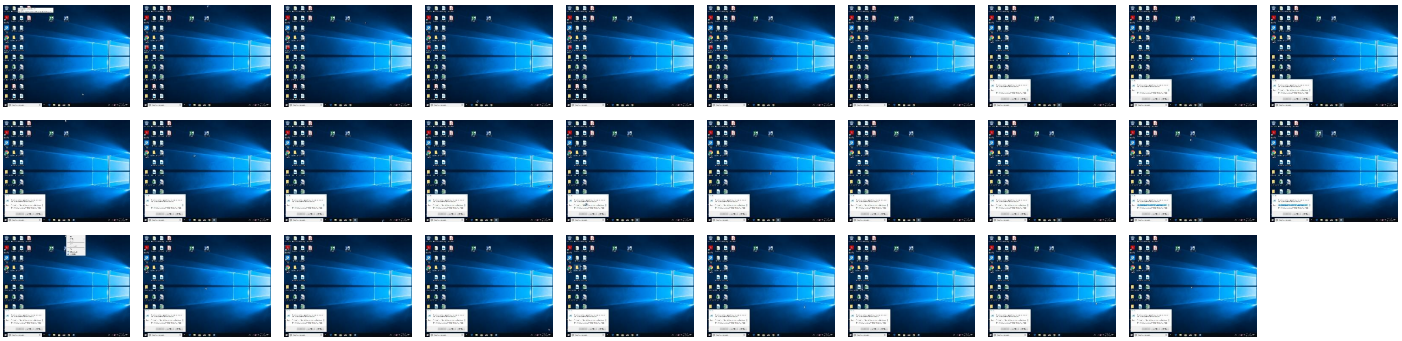
Behavior Graph



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
Prueba de pago.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Windows Update.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Windows Update.exe	44%	ReversingLabs	Win32.Trojan.Wacatac	
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	44%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.WindowsUpdate.exe.2740000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
11.2.WindowsUpdate.exe.2740000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
2.2.Windows Update.exe.27d0000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.1.Windows Update.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.Prueba de pago.exe.2350000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
1.2.Prueba de pago.exe.2350000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.Prueba de pago.exe.26e0000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
0.2.Prueba de pago.exe.26e0000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
13.2.WindowsUpdate.exe.6b0000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
14.2.Windows Update.exe.2700000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
14.2.Windows Update.exe.2700000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
2.2.Windows Update.exe.2820000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
2.2.Windows Update.exe.2820000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
1.2.Prueba de pago.exe.2460000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
1.2.Prueba de pago.exe.2460000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
15.2.Windows Update.exe.2300000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
15.2.Windows Update.exe.2300000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
3.2.Windows Update.exe.2330000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
3.2.Windows Update.exe.2330000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
3.2.Windows Update.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
3.2.Windows Update.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.Prueba de pago.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
14.2.Windows Update.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
15.2.Windows Update.exe.960000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
15.2.Windows Update.exe.960000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
13.1.WindowsUpdate.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
13.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
3.2.Windows Update.exe.22a0000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
3.2.Windows Update.exe.22a0000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.Prueba de pago.exe.2690000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
6.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
1.1.Prueba de pago.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.WindowsUpdate.exe.26f0000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.2.Windows Update.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
13.2.WindowsUpdate.exe.2200000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
13.2.WindowsUpdate.exe.2200000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
15.2.Windows Update.exe.8d0000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
1.2.Prueba de pago.exe.22c0000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
3.2.Windows Update.exe.2210000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
13.2.WindowsUpdate.exe.22b0000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
13.2.WindowsUpdate.exe.22b0000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
15.1.Windows Update.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
15.1.Windows Update.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
15.2.Windows Update.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
15.2.Windows Update.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
1.2.Prueba de pago.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
1.2.Prueba de pago.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
14.2.Windows Update.exe.2310000.2.unpack	100%	Avira	TR/Crypt.ULPM.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.monotype.fyB	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comre	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comes	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnT	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comueno	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.founder.com.cn/cnv	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://whatismyipaddress.comx&	0%	Avira URL Cloud	safe	
http://go.microsoft.	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmQt	0%	Avira URL Cloud	safe	
http://go.microsoft.LinkId=42127	0%	Avira URL Cloud	safe	
http://www.carterandcone.comg	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://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.zhongyicts.com.cnb	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.carterandcone.comues	0%	Avira URL Cloud	safe	
http://www.fontbureau.comB.TTF_g	0%	Avira URL Cloud	safe	
http://www.carterandcone.comsio	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.155.36	true	false		high
smtp.jif-asesores.com	217.76.146.62	true	false		unknown
49.124.12.0.in-addr.arpa	unknown	unknown	true		unknown

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false		high
http://www.monotype.fyB	Prueba de pago.exe, 00000001.00000003.227980976.0000000000B1B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comre	Prueba de pago.exe, 00000001.00000003.219169725.0000000005173000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comes	Prueba de pago.exe, 00000001.00000003.219204649.000000005173000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Prueba de pago.exe, 00000001.00000003.222925322.0000000005171000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnT	Prueba de pago.exe, 00000001.00000003.218253485.000000005172000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersX	Prueba de pago.exe, 00000001.00000003.222383609.000000005172000.00000004.00000001.sdmp	false		high
http://www.tiro.com	Windows Update.exe, 0000000F.00000002.308237547.000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Windows Update.exe, 0000000F.00000002.308237547.000000005100000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	Prueba de pago.exe, 00000001.00000003.219120953.000000005173000.00000004.00000001.sdmp, Prueba de pago.exe, 00000001.00000003.219169725.0000000005173000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comueno	Prueba de pago.exe, 00000001.00000002.232193805.0000000000B10000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.comx&	Windows Update.exe, 0000000F.00000002.305102053.0000000002A33000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.com	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

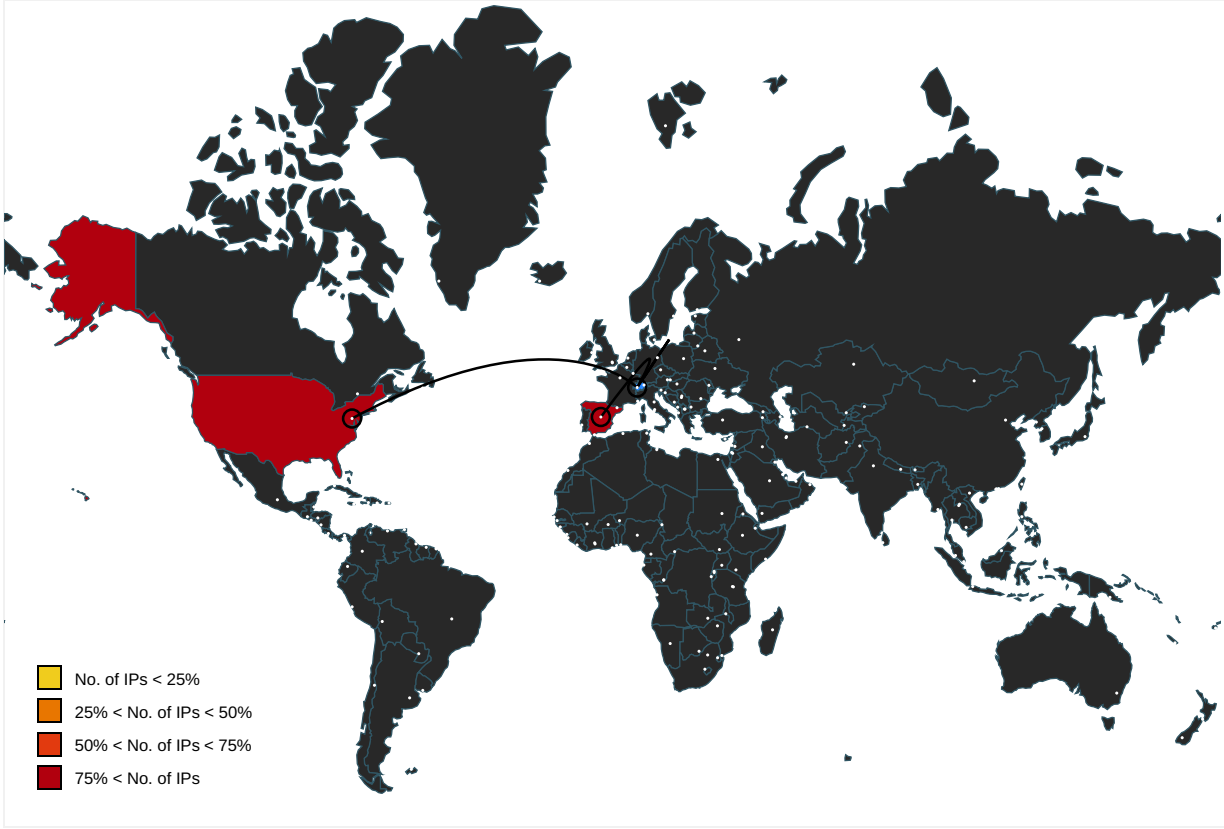
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnv	Prueba de pago.exe, 00000001.00000003.218163414.000000000515A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersd	Prueba de pago.exe, 00000001.00000003.222111568.0000000005172000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersc	Prueba de pago.exe, 00000001.00000003.222480530.0000000005172000.00000004.00000001.sdmp	false		high
http://whatismyipaddress.com/-	Prueba de pago.exe, 00000000.00000002.215547746.00000000026E2000.00000040.00000001.sdmp, Prueba de pago.exe, 00000001.00000002.232284814.0000000002352000.00000004.00000001.sdmp, Windows Update.exe, 00000002.00000002.236281439.00000000028B7000.00000040.00000001.sdmp, Windows Update.exe, 00000003.00000002.266071751.00000000022A2000.00000004.00000001.sdmp, WindowsUpdate.exe, 0000000B.00000002.275686930.00000000027D7000.00000040.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.281027497.0000000000402000.00000040.00000001.sdmp, Windows Update.exe, 0000000E.00000002.292112517.0000000002702000.00000040.00000001.sdmp, Windows Update.exe, 0000000F.00000002.303592164.0000000002302000.00000040.00000001.sdmp, WERF1FE.tmp.mdmp.9.dr	false		high
http://www.galapagosdesign.com/DPlease	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	Prueba de pago.exe, 00000001.00000003.220190167.0000000005171000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.yahoo.com/config/login	Prueba de pago.exe, Windows Update.exe	false		high
http://www.fonts.com	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.site.com/logs.php	Windows Update.exe, 0000000F.00000002.305102053.0000000002A33000.00000004.00000001.sdmp	false		high
http://www.urwpp.deDPlease	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	Windows Update.exe, 0000000F.00000002.303592164.000000002302000.00000040.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersp	Prueba de pago.exe, 00000001.00000003.222071225.000000000517 2000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designerst	Prueba de pago.exe, 00000001.00000003.222925322.000000000517 1000.00000004.00000001.sdmp	false		high
http://https://whatismyipaddress.com/	Windows Update.exe, 0000000F.00000002.305535580.0000000002DF8000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false		high
http://https://whatismyipaddress.com	Windows Update.exe, 0000000F.00000002.305553059.0000000002E01000.00000004.00000001.sdmp	false		high
http://https://whatismyipaddress.comx&	Windows Update.exe, 00000003.00000002.266901685.00000000029E1000.00000004.00000001.sdmp, Windows Update.exe, 0000000F.00000002.305535580.0000000002DF8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://go.microsoft.	Prueba de pago.exe, 00000001.00000002.232076308.00000000006DE000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com	Windows Update.exe, 00000003.00000002.266901685.00000000029E1000.00000004.00000001.sdmp, Windows Update.exe, 0000000F.00000002.305102053.0000000002A33000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htmQt	Prueba de pago.exe, 00000001.00000003.224253184.0000000000B1B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://go.microsoft.LinkId=42127	Prueba de pago.exe, 00000001.00000002.232076308.00000000006DE000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comg	Prueba de pago.exe, 00000001.00000003.219204649.0000000005173000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers)	Prueba de pago.exe, 00000001.00000003.227606996.0000000005172000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	Prueba de pago.exe, 00000001.00000003.218163414.000000000515A000.00000004.00000001.sdmp, Prueba de pago.exe, 00000001.00000003.218282268.0000000005172000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cnb	Prueba de pago.exe, 00000001.00000003.218985995.000000000515 6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	Prueba de pago.exe, 00000001.00000003.221758265.000000000517 6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comt	Prueba de pago.exe, 00000001.00000002.232193805.0000000000B1 0000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Prueba de pago.exe, 00000001.00000002.236537294.00000000063D2000.00000004.00000001.sdmp, Windows Update.exe, 00000003.00000002.270324089.00000000051D0000.00000002.00000001.sdmp, WindowsUpdate.exe, 0000000D.00000002.292639163.00000000051D0000.00000002.00000001.sdmp, Windows Update.exe, 0000000F.00000002.308237547.0000000005100000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comues	Prueba de pago.exe, 00000001.00000003.219120953.000000000517 3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comB.TTF_g	Prueba de pago.exe, 00000001.00000002.232193805.0000000000B1 0000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comsio	Prueba de pago.exe, 00000001.00000003.219204649.000000000517 3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn$	Prueba de pago.exe, 00000001.00000003.218253485.000000000517 2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.155.36	unknown	United States		13335	CLOUDFLARENETUS	false
217.76.146.62	unknown	Spain		8560	ONEANDONE-ASBrauerstrasse48DE	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319596
Start date:	18.11.2020
Start time:	13:22:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Prueba de pago.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:	33
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@23/25@8/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 56.4% (good quality ratio 55.3%) • Quality average: 84.2% • Quality standard deviation: 23.3%
HCA Information:	• Successful, ratio: 80% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.42.151.234, 104.43.193.48, 52.255.188.83, 23.210.248.85, 51.11.168.160, 20.54.26.129, 92.122.213.247, 92.122.213.194, 51.104.144.132 • Excluded domains from analysis (whitelisted): fs.microsoft.com, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/319596/sample/Prueba de pago.exe

Simulations

Behavior and APIs

Time	Type	Description
13:23:18	API Interceptor	47x Sleep call for process: Windows Update.exe modified
13:23:22	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
13:23:23	API Interceptor	2x Sleep call for process: dw20.exe modified
13:23:29	API Interceptor	1x Sleep call for process: WerFault.exe modified

Time	Type	Description
13:23:30	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.155.36	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/
	x2rzwu7CQ3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	LgADCmJ6oQ.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	xV32Do628N.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
whatismyipaddress.com	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• 104.16.155.36
	9vdouqRTh3.exe	Get hash	malicious	Browse	• 104.16.154.36
	5pB35gGfZ5.exe	Get hash	malicious	Browse	• 104.16.155.36
	M9RhKQ1G91.exe	Get hash	malicious	Browse	• 104.16.154.36
	0CyK3Y7XBs.exe	Get hash	malicious	Browse	• 104.16.154.36
	pwYhlZGMa6.exe	Get hash	malicious	Browse	• 104.16.154.36
	fyxC4Hgs3s.exe	Get hash	malicious	Browse	• 104.16.155.36

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEANDONE-ASBrauerstrasse48DE	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 217.160.0.224
	Narud#U017eba 0521360021.xlsx	Get hash	malicious	Browse	• 74.208.22.240
	Quote Request.xlsx	Get hash	malicious	Browse	• 82.165.48.223
	anthony.exe	Get hash	malicious	Browse	• 217.160.0.199
	8miw6WNHCt.exe	Get hash	malicious	Browse	• 74.208.5.21
	WO4jeXWl0L.exe	Get hash	malicious	Browse	• 74.208.45.104
	5YCsNuM4a9.exe	Get hash	malicious	Browse	• 74.208.45.104
	eLaaw7SqMi.exe	Get hash	malicious	Browse	• 74.208.5.22
	vi9qEkXlGm.exe	Get hash	malicious	Browse	• 217.76.150.19
	p8LV1eVFyO.exe	Get hash	malicious	Browse	• 217.160.0.224
	BUd4ZanDeR.exe	Get hash	malicious	Browse	• 198.251.77.47
	0Ia3EzPqrx.exe	Get hash	malicious	Browse	• 74.208.236.235
	mvl9cPORxx.exe	Get hash	malicious	Browse	• 74.208.5.15
	ultimate-mailer (x64).exe	Get hash	malicious	Browse	• 82.165.116.162
	invoice No_SINI0068206497.exe	Get hash	malicious	Browse	• 217.160.23 3.109
	COMMERCIAL INVOICE BILL OF LADING DOC.exe	Get hash	malicious	Browse	• 77.68.64.21
	http://https://moeglobal-my.sharepoint.com/:o:/g/personal/bel_moe-as_no/EhOor6oBqeFEgp-vQYeIFUEB1ye9Et93JElzx8s1IHLnTA?e=3OSEPa	Get hash	malicious	Browse	• 77.68.64.10
	IQtvZjIdhN.exe	Get hash	malicious	Browse	• 217.160.0.224
	f14QUITHh3.exe	Get hash	malicious	Browse	• 74.208.236.51
	Invoice.exe	Get hash	malicious	Browse	• 82.223.120.84
CLOUDFLARENETUS	a66a5257bb6ee2e690450c48a91815d4.exe	Get hash	malicious	Browse	• 104.23.99.190
	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 162.159.13 3.233
	u82lb18JnW.exe	Get hash	malicious	Browse	• 104.31.92.240
	http://https://agrabadconventionhall.com/redirect-outlook.com/server%20configuration/?#info@herbertarchitekten.de	Get hash	malicious	Browse	• 104.16.18.94
	http://https://agrabadconventionhall.com/redirect-outlook.com/server configuration/	Get hash	malicious	Browse	• 104.16.19.94
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 172.67.214.161
	http://cricketventures.com	Get hash	malicious	Browse	• 104.26.13.251
	http://https://www.chm-endurance.com/	Get hash	malicious	Browse	• 104.22.24.131
	http://https://bitly.com/35yFnns	Get hash	malicious	Browse	• 104.16.19.94
	http://https://email.ofificeshareserver1.ml/e/c/eyJlbWFpbF9pZCI6IlJPS0xCZ01BQVhYVjZXVUFLRTFaMUpQWmZrTU1mUT09IiwiaHJlZiI6Imh0dHBzOi8vZmlyZWJhc2VzdG9yYWdlLmdvb2dsZWFwaXMuY29tL3YwL2Ivc2l0ZXMtMDAuYXBwc3BvdC5jb20vby9zaGFyZS1wb2ludCUyRnJlZGlyZWN0Lmh0bWw_YWx0PW1lZGlhXHUwMDI2dG9rZW49NWIwZjItNTE4Ny00YzA3LWExNGUtMDA2OWE0ZWI0ODcxXHUwMDI2ZW1haWw9bWFya3VzLm5pZXRoQGp1bGl1c2JhZXIuY29tIiwibGlua19pZCI6MSwicG9zaXRpb24iOjB9/1b8972b4385f4f0bcb49ca81c6f33c388775dae940b9f44c90bdf57423203612	Get hash	malicious	Browse	• 104.31.71.251
	http://https://j.mp/38NwiZZ	Get hash	malicious	Browse	• 104.27.187.65
	http://https://app.nihaocloud.com/f/06096e5837654796a4d4/	Get hash	malicious	Browse	• 104.16.18.94
	Status____201711.gz.exe	Get hash	malicious	Browse	• 104.23.98.190
	ORDER SPECIFITIONS.exe	Get hash	malicious	Browse	• 23.227.38.64
	Documento relativo al carico e alla spedizione del cliente_italy2020.exe	Get hash	malicious	Browse	• 104.24.127.89
	b095b966805abb7df4ffddf183def880.exe	Get hash	malicious	Browse	• 104.18.48.20
	SIN029088.xls	Get hash	malicious	Browse	• 104.20.139.65
	SIN029088.xls	Get hash	malicious	Browse	• 104.20.138.65
	Request for Quote_PDF.vbs	Get hash	malicious	Browse	• 104.24.127.89

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	01_file.exe	Get hash	malicious	Browse	• 104.24.127.89

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Windows Update.e_1044ba73b302b1a19e09d2f83986d3c5672f_ffa3413f_105a0017\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	19508
Entropy (8bit):	3.763354078456508
Encrypted:	false
SSDEEP:	192:cORZHBUZMXwjV/C9yq5bMvg/LHZ+nNN2l1rzvq5xk0z5xTo/u7sDS274ltCy2:RRJBUZMXwjB7vqsSc/u7sDX4ltCy2
MD5:	7089279C19BDD4172CB67C5E78F95572
SHA1:	4739BDF6E94A6F64C4D118B6AA4D78763E219099
SHA-256:	CBE474CAC4EE630CECAEEB351D97FD9934962F317033A676313246C1EA52DA1C
SHA-512:	A3C977D37F1277390C7619ABB036AB6FCF198E64DE5E9D4C3C10EEB7AC80A1A88A3E9262D4BD714B9668D3B43F1B061FC482FDB54EB7D170D8B8E3B4F2EE44 21
Malicious:	false
Yara Hits:	• Rule: SUSP_WER_Suspicious_Crash_Directory, Description: Detects a crashed application executed in a suspicious directory, Source: C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Windows Update.e_1044ba73b302b1a19e09d2f83986d3c5672f_ffa3413f_105a0017\Report.wer, Author: Florian Roth
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.2.0.8.2.0.5.9.3.8.6.4.4.8.....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.=.1.3.2.5.0.2.0.8.2.0.8.5.9.4.8.8.8.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.5.d.a.8.5.f.b.-.e.e.3.f.-.4.0.9.8.-.a.c.9.2.-.3.f.1.d.1.1.9.5.a.8.c.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.8.a.9.2.f.3.2.-.2.e.7.3.-.4.2.7.5.-.8.2.f.c.-.7.b.3.b.f.3.9.5.9.1.4.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.W.i.n.d.o.w.s. .U.p.d.a.t.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.0.c.-.0.0.0.1.-.0.0.1.7.-.7.b.1.c.-.3.0.0.6.f.1.b.d.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.e.1.f.4.7.9.8.5.d.3.d.4.4.a.1.6.f.b.7.6.b.2.7.3.a.7.6.a.9.7.f.d.0.0.0.0.f.f.f.f.!.0.0.0.0.b.1.6.0.3.2.d.8.3.c.9.1.e.e.3.3.3.2.2.1.f.a.f.a.d.d.5.f.2.3.8.1.c.a.6.5.9.d.7.8.!.W.i.n.d.o.w.s. .U.p.d.a.t.e...e.x.e.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_windows update.e_52f24b01f2038132be328c41fc3923fb83453f_00000000_08e5e905\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):	18680
Entropy (8bit):	3.753140752327928
Encrypted:	false
SSDEEP:	192:WIGbQSVhjV/C9yq5bMvg/LHZ+nNN2l1rzvq5xk0z5xTo/u7sDS274ltf:kbQcjB7vqsSc/u7sDX4ltf
MD5:	4E0405D431FE06C8DB569BB0B90164F7
SHA1:	78A7B21330C5BE49E728871AC8F587736E4FAAF5
SHA-256:	E665909C5DE9CE3B7620FC122A03B76ECE881D6535CDD2C0178135D2E85F31B8
SHA-512:	D542787FE647427B7C9E5581875DB233DEEA077A778191A53A41263745A7C201F074208A86409AE2870C176F0323C90B0B303A4898FC9D9E368587FEF54EDAEA
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.2.0.8.2.0.0.4.8.5.5.3.1.5.....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.=.1.3.2.5.0.2.0.8.2.0.0.8.9.1.7.8.2.4.....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.=.8.4.5.4.2.e.6.a.-.4.3.8.2.-.4.9.a.f.-.8.9.f.e.-.4.6.4.2.8.1.0.e.c.d.2.4.....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.=.0.0.0.0.1.5.0.c.-.0.0.0.1.-.0.0.1.7.-.7.b.1.c.-.3.0.0.6.f.1.b.d.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.e.1.f.4.7.9.8.5.d.3.d.4.4.a.1.6.f.b.7.6.b.2.7.3.a.7.6.a.9.7.f.d.0.0.0.0.f.f.f.f.!.0.0.0.0.b.1.6.0.3.2.d.8.3.c.9.1.e.e.3.3.3.2.2.1.f.a.f.a.d.d.5.f.2.3.8.1.c.a.6.5.9.d.7.8.!.W.i.n.d.o.w.s. .U.p.d.a.t.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.7.:.1.5.:.0.8.:.3.4.!.0.!.W.i.n.d.o.w.s. .U.p.d.a.t.e...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.=.3.4.4.....I.s.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_windows update.e_52f24b01f2038132be328c41fc3923fb83453f_00000000_1b3a43a8\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

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_windows update.e_52f24b01f2038132be328c41fc3923fb83453f_00000000_1b3a43a8\Report.wer	
Size (bytes):	18580
Entropy (8bit):	3.7538345857997233
Encrypted:	false
SSDEEP:	192:OZhQSVhjV/C9yq5bMvg/LHZ+nNN2I1rzvq5xk0z5xT5/u7sDS274It8:2hQcjB7vqsSt/u7sDX4It8
MD5:	8960DF80823EED9590D3BCABCB4A3195
SHA1:	A3F465982AD46B1152E53F64742B9FAB9A1CB5D1
SHA-256:	2D7DEE9873BF1820F0BF4C27776F22D1D60A5DDD5C192ABEC180966B5C02D4A0
SHA-512:	C864E952F30A5CFC0466AEF174CCB475ABDF7C8AEAC68FC46DC183969F6CEE96FB4EB35311EFB4865D2DCE772CEF0513F70CEAC9E917E0E0E31BE71747FE3BA6
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.2.0.8.2.2.5.2.5.1.1.0.2.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.0.2.0.8.2.2.5.7.5.1.0.9.8.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.1.8.4.3.3.7.1.-.6.5.2.f.-.4.5.c.7.-.8.b.2.a.-.a.9.5.6.6.8.f.5.7.7.2.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.=.0.0.0.0.1.9.4.c.-.0.0.0.1.-.0.0.1.7.-.e.4.5.2.-.e.4.1.3.f.1.b.d.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.e.1.f.4.7.9.8.5.d.3.d.4.4.a.1.6.f.b.7.6.b.2.7.3.a.7.6.a.9.7.f.d.0.0.0.0.f.f.f.f.!.0.0.0.0.b.1.6.0.3.2.d.8.3.c.9.1.e.e.3.3.3.2.2.1.f.a.f.a.d.d.5.f.2.3.8.1.c.a.6.5.9.d.7.8.!.W.i.n.d.o.w.s. .U.p.d.a.t.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.7.:.1.5.:.0.8.:.3.4.!.0.!.W.i.n.d.o.w.s. .U.p.d.a.t.e...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.=.3.5.7.....I.s.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D9D.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):	3.724856193004803
Encrypted:	false
SSDEEP:	96:RtIU6o7r3GLt3iEM6UYDYZYQSfZPgTBCaM1Yy1f1tvIm:Rrl7r3GLNiEM6rDYZYQSGCp1Yy1ffIm
MD5:	95F2EBE72FF214D8A8D68A6C166F4DAE
SHA1:	B703C9D6AD7D59A8E86B39D8AAC6457120A97B86
SHA-256:	83AD25F02D92AC80308577ADB0F8E8BE8BBF541CA19CFEAB3CC8B9D281DE5379
SHA-512:	9E87A59ACA83197ACC879DE98631AB9822E35ED8BBFCA24F46A05C9E6D1A127110ABE89F1BE7FBFEDAE26527D9AA1391455D32C0F84EFCB49B07EDDBB89533BE
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.4.7.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3ED7.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):	4.4527618910908435
Encrypted:	false
SSDEEP:	48:cvIwSD8zskJgtWI9i0WSC8BYs8fm8M4JFK82FDQo+q8v//Rvxz4d:uITfihtSNmJFKgoKnRvx4d
MD5:	D97648D73509017640C5A04CF118184F
SHA1:	74D8E8320B6C57A385FB7EF5E1CCDDDA82EEB507
SHA-256:	CD80E6682578C2208BFD215D77294F492F50C0129B729500ACFBF06AD6D9AE72
SHA-512:	AD1E1C3EB7FC757AD4AADCCC19F0CA9CC27CD7869975603A6F80A00E81D3142506D56AA093514E5461321AA3A0E3D016557C25836D1ED621FEBD5AFD5DB242A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="734794" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD1E.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

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD1E.tmp.WERInternalMetadata.xml	
Size (bytes):	5670
Entropy (8bit):	3.719208298799123
Encrypted:	false
SSDEEP:	96:RtlU6o7r3GLt3iQWv6X6BYZYQSfZPgTBCaM1jV1fULBm:Rrl7r3GLNiJv6XiYZYQSGCp1jV1fULBm
MD5:	6F0E93FC5FE862BFE982417D289E9B73
SHA1:	D8DFAAB85670FACC7F829D327EDEFB49EEE794F9
SHA-256:	77A1A290B7BA47BBBA7A66E02FD4026529C19DB6778AA36067DD183D73419755
SHA-512:	C6F405DDA4D5FC0BF12B629B7A7EBBB330A1FB38CEEDF6CB9206BCC7FD4D452C1A0F9AF4C9E4285E48ED12F1D9E91C6153540A39792923F94D44C0084201B0 20
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.3.8.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDDAC.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):	4.450226258139721
Encrypted:	false
SSDEEP:	48:cvIwSD8zsRJgtWI9i0WSC8Bt8fm8M4JFK82FMV+q8v/mRvxzEd:uITfjhtSNYJFKIVK+RvxEd
MD5:	1B03DBE1E2C6F64693C0273C6A3B3A0F
SHA1:	1884CAD7A8024B1FEA071C6D99A3405B888CD11E
SHA-256:	29A1DEE2ECE333022FCDA0FE759627375D5A02C132717F1CC3B3CBE14521924A
SHA-512:	1F65D3F911915B633C1354D95C5EA306220AF642B7A1860B4ABF536F9542B6147292147DD1F871DEB4150365BF11F32244D81C92CF47E2E0266360D1BC9A34AF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" /> .. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="734793" />.. <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\WERF1FE.tmp.mdmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Nov 18 21:23:27 2020, 0x60521 type
Category:	dropped
Size (bytes):	7040228
Entropy (8bit):	4.723675783236964
Encrypted:	false
SSDEEP:	98304:fsqKSRLDPyq9H2bUhr1b1XaE1nU8es2OfBNeQCPoeOVVSTLtTOp:ySR3yq9HcyrL0cCFOV5
MD5:	0FAD6C03DEA3E1B26C0FBF17C4B8C8AB
SHA1:	8130F67C5788401570AE8BA8422940DA7910720B
SHA-256:	7DA5A6E911D169B2B9BA032ED4AB04DC39E53AC17FE49A0FB52AA0BC28AE6984
SHA-512:	77CB0FCDB10012F46467A6BFC5DB7EA0737D35F6A5A7B82B7CE98CC81347BFF708745DB2F1EC274A3304BA88DD1E3369B1F03FABB203DD334043BE3641E365 5
Malicious:	**true**
Yara Hits:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1FE.tmp.mdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1FE.tmp.mdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1FE.tmp.mdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low
Preview:	MDMP..... ....._!.....U.....B.....9.....GenuineIntelW.....T....._.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB36.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB36.tmp.WERInternalMetadata.xml	
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	6350
Entropy (8bit):	3.7261065119655044
Encrypted:	false
SSDEEP:	192:RrI7r3GLNiJU6yIwGYNSxCprq89brtsfCZm:RrlsNia6yIBYNS6rmfV
MD5:	78524C46881C75372A6F8E614683C79F
SHA1:	370969709A50D46B57CF6613B8BB8AF395377971
SHA-256:	EE8A23BA4E379CF7A824D02E64C3D7DACC8FD238DD1B072E3457C8D6CE5F14F8
SHA-512:	FF3F0ABF543461DC416CA12BC7E096F014ABF5C2B926D86D60F5A08386B97B41985DEA5EF5C95957E6019437F92359177246AC214F7C0DB5314AFA6F064C8237
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.3.8.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBC4.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4622
Entropy (8bit):	4.49341035571301
Encrypted:	false
SSDEEP:	48:cvIwSD8zskJgtWI9i0WSC8Bb8fm8M4JwEZFH+q8/UNRvxzXd:uITfihtSNeJJLDNRvxXd
MD5:	75CFD237E67202906AEAA3C9721A7B9F
SHA1:	B89B0224A00DBC6704B2F9B0A022771376BAFBD0
SHA-256:	34AF33BC20E92B2AA31B49596018CCA936AFDE743C660CD38CB3D10A904DEDE6
SHA-512:	0A7B6193EF10AC287A028A420F1AF5AD8E66E0C3146B406CF87C48B1622FFA918F6063E6E26DFEF43F0AF547EA60BF7F976467E9ED898402EAF1D58FBEEB268A
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="734794" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Prueba de pago.exe.log	
Process:	C:\Users\user\Desktop\Prueba de pago.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	916
Entropy (8bit):	5.282390836641403
Encrypted:	false
SSDEEP:	24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2+:MwLLD2Y9h3go2rxxAcAO6ox+g2+
MD5:	5AD8E7ABEADADAC4CE06FF693476581A
SHA1:	81E42A97BBE3D7DE8B1E8B54C2B03C48594D761E
SHA-256:	BAA1A28262BA27D51C3A1FA7FB0811AD1128297ABB2EDCCC785DC52667D2A6FD
SHA-512:	7793E78E84AD36CE65B5B1C015364E340FB9110FAF199BC0234108CE9BCB1AEDACBD25C6A012AC99740E08BEA5E5C373A88E553E47016304D8AE6AEEAB58EEFF
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a9099237864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..

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

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\WindowsUpdate.exe.log	
Entropy (8bit):	5.282390836641403
Encrypted:	false
SSDEEP:	24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2+:MwLLD2Y9h3go2rxxAcAO6ox+g2+
MD5:	5AD8E7ABEADADAC4CE06FF693476581A
SHA1:	81E42A97BBE3D7DE8B1E8B54C2B03C48594D761E
SHA-256:	BAA1A28262BA27D51C3A1FA7FB0811AD1128297ABB2EDCCC785DC52667D2A6FD
SHA-512:	7793E78E84AD36CE65B5B1C015364E340FB9110FAF199BC0234108CE9BCB1AEDACBD25C6A012AC99740E08BEA5E5C373A88E553E47016304D8AE6AEEAB58EE FF
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages _v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a909923 7864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System .Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\SysInfo.txt	
Process:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	48
Entropy (8bit):	4.387380345401073
Encrypted:	false
SSDEEP:	3:oNWXp5cViEaKC59KuCa:oNWXp+NaZ5v
MD5:	95FC50C7E40BB0D5EBD49FCBEE4E890D
SHA1:	E5086A9390CC8D6F512A206AB1AC4309A4CC4326
SHA-256:	DC88107DF527833D0D8B7AC45D31AF0E5343AE36AB9725016B046CDD77E46EC7
SHA-512:	4AC9E01163C00CC874BDBE1E4B5BF2463F8B53B9102705C774C790D8DFD8AEAD662DEDA812CF457022820FFD8174A1CD0275601C4BC6E4CCDB7E5A80CD52F 99
Malicious:	false
Preview:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe

C:\Users\user\AppData\Local\Temp\holderwb.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Windows Update.exe	
Process:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1129472
Entropy (8bit):	6.927370959170246
Encrypted:	false
SSDEEP:	24576:9JCKxWfPNFwyIUlawycDT0+Yrdypzvq3/7j:Zl4s0wbDgt5QW/
MD5:	B3A244A097904A4D6689A582D7EC9985
SHA1:	B16032D83C91EE333221FAFADD5F2381CA659D78
SHA-256:	286B416351F4CA6CC215C58692AF9BE6B9F4EB54C4641160E2A31DFD16C43EC7
SHA-512:	533CBDDF7D78740E2586D58588C5D0AD4407417C835C0407D93D86B3202626F160D664B69AEFB3D32F94416D7558D6BA9377A28F44BE3FF21ACE2FD4E51F074
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 44%

C:\Users\user\AppData\Roaming\Windows Update.exe	
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....@.....p...$...@..dG.....p..... .....CODE..... ..`DATA....\.....@...BSS.....`.....L.....idata...$...p...&...L.....@....tls.....r.....rdata. .....r.....@..P.reloc..p.....t.....@..P.rsrc...dG...@...H.....@..P.....V.....@..P..... .....

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

C:\Users\user\AppData\Roaming\WindowsUpdate.exe	
Process:	C:\Users\user\AppData\Roaming\Windows Update.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1129472
Entropy (8bit):	6.927370959170246
Encrypted:	false
SSDEEP:	24576:9JCKxWfPNFwyIUlawycDT0+Yrdypzvq3/7j:ZI4s0wbDgt5QW/
MD5:	B3A244A097904A4D6689A582D7EC9985
SHA1:	B16032D83C91EE333221FAFADD5F2381CA659D78
SHA-256:	286B416351F4CA6CC215C58692AF9BE6B9F4EB54C4641160E2A31DFD16C43EC7
SHA-512:	533CBDDF7D78740E2586D58588C5D0AD4407417C835C0407D93D86B3202626F160D664B69AEFB3D32F94416D7558D6BA9377A28F44BE3FF21ACE2FD4E51F074
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 44%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....@.....p...$...@..dG.....p..... .....CODE..... ..`DATA....\.....@...BSS.....`.....L.....idata...$...p...&...L.....@....tls.....r.....rdata. .....r.....@..P.reloc..p.....t.....@..P.rsrc...dG...@...H.....@..P.....V.....@..P..... .....

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

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\AppData\Roaming\Windows Update.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false

C:\Users\user\AppData\Roaming\pid.txt	
SSDEEP:	3:G:G
MD5:	AB49EF78E2877BFD2C2BFA738E459BF0
SHA1:	3745C074470E4CC5747DD76743675E1507E59C7A
SHA-256:	1089C7C8B99B159441206D96E5BD6246556F0D8D4D41D3B8A96A9298354BD19F
SHA-512:	100CE65B2EB36A1C04BF6C21D4D54BB510BEDDB5FDD592AD5182001CAA9C7ECF24C9CB5EFC146EB7413D3465F0D72B7BBC3FB9F292DD54D5D51FAB74A316B8F
Malicious:	false
Preview:	6476

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\AppData\Roaming\Windows Update.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	49
Entropy (8bit):	4.441568140944513
Encrypted:	false
SSDEEP:	3:oNWXp5cViEaKC59KYr4a:oNWXp+NaZ534a
MD5:	6078085422A31D60FCEB24D4FA24B6E8
SHA1:	0CD056478F3D877B3D44C7B439485B1ACFD78F5A
SHA-256:	9113E6728CEB1F460E3CEAB19852A31602CD77A92E7B861802FE339FD5CFD837
SHA-512:	22CE5D96BB25519CB14F27BDB44D7FAEDC6D5C8B8F81A1F972EA638BF9731D8793C98359D7C9476D50AF46346E0964E82F5B0B2F8B1B6763B078D2B045FB2EA1
Malicious:	false
Preview:	C:\Users\user\AppData\Roaming\Windows Update.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.927370959170246
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:	Prueba de pago.exe
File size:	1129472
MD5:	b3a244a097904a4d6689a582d7ec9985
SHA1:	b16032d83c91ee333221fafadd5f2381ca659d78
SHA256:	286b416351f4ca6cc215c58692af9be6b9f4eb54c4641160e2a31dfd16c43ec7
SHA512:	533cbddf7d78740e2586d58588c5d0ad4407417c835c0407d93d86b3202626f160d664b69aefb3d32f94416d7558d6ba9377a28f44be3ff21ace2fd4e51f0748
SSDEEP:	24576:9JCKxWfPNFwyIUlawycDT0+Yrdypzvq3/7j:ZI4s0wbDgt5QW/
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	4c567676561e0701

Static PE Info

General

Entrypoint:	0x479884

General

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:	5113dec31b8616dbad783836e7188783

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 00479694h
call 00007FC17CF2F78Dh
mov eax, dword ptr [00495AD0h]
mov eax, dword ptr [eax]
call 00007FC17CF7F54Dh
mov ecx, dword ptr [00495BC8h]
mov eax, dword ptr [00495AD0h]
mov eax, dword ptr [eax]
mov edx, dword ptr [00479188h]
call 00007FC17CF7F54Dh
mov eax, dword ptr [00495AD0h]
mov eax, dword ptr [eax]
call 00007FC17CF7F5C1h
call 00007FC17CF2D284h
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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x97000	0x24c4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa4000	0x74764	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9c000	0x7f70	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x9b000	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	0x788cc	0x78a00	False	0.524172198834	data	6.51448811653	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
DATA	0x7a000	0x1bc5c	0x1be00	False	0.171568455717	data	2.71109267168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x96000	0xcb1	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x97000	0x24c4	0x2600	False	0.352076480263	data	4.94171972073	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x9a000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x9b000	0x18	0x200	False	0.048828125	data	0.20058190744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x9c000	0x7f70	0x8000	False	0.559631347656	data	6.62495186635	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0xa4000	0x74764	0x74800	False	0.814853389887	data	7.42056726509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xa4a08	0x134	data		
RT_CURSOR	0xa4b3c	0x134	data		
RT_CURSOR	0xa4c70	0x134	data		
RT_CURSOR	0xa4da4	0x134	data		
RT_CURSOR	0xa4ed8	0x134	data		
RT_CURSOR	0xa500c	0x134	data		
RT_CURSOR	0xa5140	0x134	data		
RT_BITMAP	0xa5274	0x1d0	data		
RT_BITMAP	0xa5444	0x1e4	data		
RT_BITMAP	0xa5628	0x1d0	data		
RT_BITMAP	0xa57f8	0x1d0	data		
RT_BITMAP	0xa59c8	0x1d0	data		
RT_BITMAP	0xa5b98	0x1d0	data		
RT_BITMAP	0xa5d68	0x1d0	data		
RT_BITMAP	0xa5f38	0x1d0	data		
RT_BITMAP	0xa6108	0x534e1	data	English	United States
RT_BITMAP	0xf95ec	0x1d0	data		
RT_BITMAP	0xf97bc	0xd8	data		
RT_BITMAP	0xf9894	0xd8	data		
RT_BITMAP	0xf996c	0xd8	data		
RT_BITMAP	0xf9a44	0xd8	data		
RT_BITMAP	0xf9b1c	0xd8	data		
RT_BITMAP	0xf9bf4	0xe8	GLS_BINARY_LSB_FIRST		
RT_ICON	0xf9cdc	0x951b	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x1031f8	0x668	data	English	United States
RT_ICON	0x103860	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 16777215, next used block 16777215		
RT_ICON	0x105e08	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 1566797424, next used block 1566797424		
RT_ICON	0x106eb0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x107318	0x10828	data		
RT_DIALOG	0x117b40	0x52	data		
RT_RCDATA	0x117b94	0x10	data		
RT_RCDATA	0x117ba4	0x274	data		
RT_RCDATA	0x117e18	0x7c3	Delphi compiled form 'TForm1'		
RT_GROUP_CURSOR	0x1185dc	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x1185f0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x118604	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x118618	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x11862c	0x14	Lotus unknown worksheet or configuration, revision 0x1		

Name	RVA	Size	Type	Language	Country
RT_GROUP_CURSOR	0x118640	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x118654	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x118668	0x14	data	English	United States
RT_GROUP_ICON	0x11867c	0x4c	data		
RT_HTML	0x1186c8	0x99	data	English	United States

Imports

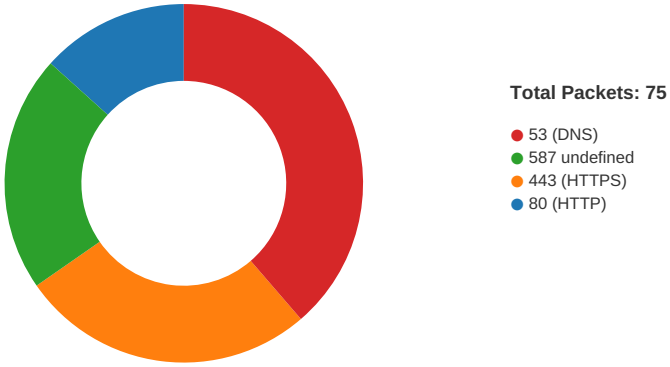
DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, SetCurrentDirectoryA, MultiByteToWideChar, 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, lstrcmpA, 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, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemTime, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, FreeLibrary, FormatMessageA, FindResourceA, FindNextFileA, FindFirstFileA, FindClose, FileTimeToLocalFileTime, FileTimeToDosDateTime, ExitProcess, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWindowExtEx, SetWinMetaFileBits, SetViewportOrgEx, SetViewportExtEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetMapMode, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, 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, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessageTime, GetMessagePos, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardType, 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, ChildWindowFromPoint, 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_Replace, 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

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 13:23:18.156307936 CET	49725	80	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.172880888 CET	80	49725	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:18.172996044 CET	49725	80	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.173736095 CET	49725	80	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.190232992 CET	80	49725	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:18.205449104 CET	80	49725	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:18.255162001 CET	49726	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.256525993 CET	49725	80	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.271610022 CET	443	49726	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:18.271754026 CET	49726	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.326100111 CET	49726	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.342639923 CET	443	49726	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:18.343122005 CET	443	49726	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:18.343375921 CET	443	49726	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:18.343475103 CET	49726	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.372195959 CET	49726	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.373879910 CET	49727	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.388709068 CET	443	49726	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:18.390291929 CET	443	49727	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:18.390434980 CET	49727	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.391196966 CET	49727	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.407581091 CET	443	49727	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:18.408934116 CET	443	49727	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:18.409166098 CET	443	49727	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:18.409308910 CET	49727	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.410748005 CET	49727	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:18.427051067 CET	443	49727	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:19.372533083 CET	49728	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:19.429733992 CET	587	49728	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:19.430356979 CET	49728	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:19.484149933 CET	587	49728	217.76.146.62	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 13:23:19.529613972 CET	49728	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:19.582427979 CET	587	49728	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:19.582458019 CET	587	49728	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:19.632231951 CET	49728	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:19.699366093 CET	49728	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:19.753313065 CET	587	49728	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:19.761369944 CET	49728	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:19.853539944 CET	587	49728	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:22.824961901 CET	587	49728	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:22.826849937 CET	49728	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:22.880068064 CET	587	49728	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:22.881308079 CET	587	49728	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:22.883138895 CET	49728	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:22.937414885 CET	587	49728	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:22.937700033 CET	49728	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:33.304239035 CET	49725	80	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:43.842483044 CET	49738	80	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:43.858910084 CET	80	49738	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:43.859080076 CET	49738	80	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:43.859767914 CET	49738	80	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:43.880752087 CET	80	49738	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:43.888427973 CET	80	49738	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:43.929254055 CET	49739	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:43.945622921 CET	443	49739	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:43.945771933 CET	49739	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:43.997375965 CET	49739	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:44.014508963 CET	443	49739	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:44.019392967 CET	443	49739	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:44.019423962 CET	443	49739	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:44.019490957 CET	49739	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:44.023448944 CET	49739	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:44.025419950 CET	49740	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:44.039880037 CET	443	49739	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:44.039880991 CET	49738	80	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:44.041769028 CET	443	49740	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:44.041887999 CET	49740	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:44.043481112 CET	49740	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:44.059838057 CET	443	49740	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:44.061032057 CET	443	49740	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:44.061183929 CET	443	49740	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:44.061263084 CET	49740	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:44.063715935 CET	49740	443	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:44.081182003 CET	443	49740	104.16.155.36	192.168.2.3
Nov 18, 2020 13:23:45.124259949 CET	49741	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:45.176453114 CET	587	49741	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:45.176635027 CET	49741	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:45.228775024 CET	587	49741	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:45.229201078 CET	49741	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:45.281110048 CET	587	49741	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:45.281131029 CET	587	49741	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:45.281732082 CET	49741	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:45.333138943 CET	587	49741	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:45.333497047 CET	49741	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:45.424472094 CET	587	49741	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:48.434525013 CET	587	49741	217.76.146.62	192.168.2.3
Nov 18, 2020 13:23:48.539719105 CET	49741	587	192.168.2.3	217.76.146.62
Nov 18, 2020 13:23:50.700263977 CET	49738	80	192.168.2.3	104.16.155.36
Nov 18, 2020 13:23:50.700618029 CET	49741	587	192.168.2.3	217.76.146.62

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 13:22:59.856910944 CET	60831	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:22:59.884131908 CET	53	60831	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 13:23:00.483272076 CET	60100	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:00.512110949 CET	53	60100	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:01.471681118 CET	53195	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:01.499043941 CET	53	53195	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:02.286894083 CET	50141	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:02.313980103 CET	53	50141	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:03.059722900 CET	53023	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:03.087019920 CET	53	53023	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:03.804584026 CET	49563	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:03.831875086 CET	53	49563	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:04.833585978 CET	51352	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:04.860826015 CET	53	51352	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:05.954463005 CET	59349	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:05.982014894 CET	53	59349	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:07.099803925 CET	57084	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:07.127032042 CET	53	57084	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:08.202673912 CET	58823	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:08.229778051 CET	53	58823	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:08.892765999 CET	57568	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:08.920062065 CET	53	57568	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:17.814177036 CET	50540	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:17.850110054 CET	53	50540	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:18.107389927 CET	54366	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:18.134546995 CET	53	54366	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:18.217336893 CET	53034	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:18.252717972 CET	53	53034	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:19.293009043 CET	57762	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:19.367795944 CET	53	57762	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:23.021364927 CET	55435	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:23.057523012 CET	53	55435	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:29.014533043 CET	50713	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:29.041577101 CET	53	50713	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:29.716088057 CET	56132	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:29.753537893 CET	53	56132	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:30.325105906 CET	58987	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:30.352339983 CET	53	58987	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:43.442058086 CET	56579	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:43.477823019 CET	53	56579	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:43.787981987 CET	60633	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:43.823657036 CET	53	60633	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:43.896718025 CET	61292	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:43.927705050 CET	53	61292	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:45.081165075 CET	63619	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:45.118835926 CET	53	63619	8.8.8.8	192.168.2.3
Nov 18, 2020 13:23:46.156785011 CET	64938	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:23:46.194552898 CET	53	64938	8.8.8.8	192.168.2.3
Nov 18, 2020 13:24:00.644244909 CET	61946	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:24:00.697611094 CET	53	61946	8.8.8.8	192.168.2.3
Nov 18, 2020 13:24:05.457015038 CET	64910	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:24:05.484110117 CET	53	64910	8.8.8.8	192.168.2.3
Nov 18, 2020 13:24:08.940654993 CET	52123	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:24:08.977572918 CET	53	52123	8.8.8.8	192.168.2.3
Nov 18, 2020 13:24:40.918004990 CET	56130	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:24:40.945200920 CET	53	56130	8.8.8.8	192.168.2.3
Nov 18, 2020 13:24:43.775077105 CET	56338	53	192.168.2.3	8.8.8.8
Nov 18, 2020 13:24:43.802208900 CET	53	56338	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 18, 2020 13:23:17.814177036 CET	192.168.2.3	8.8.8.8	0xc79a	Standard query (0)	49.124.12.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 13:23:18.107389927 CET	192.168.2.3	8.8.8.8	0xf92a	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 18, 2020 13:23:18.217336893 CET	192.168.2.3	8.8.8.8	0xd08c	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 18, 2020 13:23:19.293009043 CET	192.168.2.3	8.8.8.8	0x6512	Standard query (0)	smtp.jif-a sesores.com	A (IP address)	IN (0x0001)
Nov 18, 2020 13:23:43.442058086 CET	192.168.2.3	8.8.8.8	0x6abf	Standard query (0)	49.124.12.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 13:23:43.787981987 CET	192.168.2.3	8.8.8.8	0xc6f8	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 18, 2020 13:23:43.896718025 CET	192.168.2.3	8.8.8.8	0x81b6	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 18, 2020 13:23:45.081165075 CET	192.168.2.3	8.8.8.8	0x6ffd	Standard query (0)	smtp.jif-a sesores.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 18, 2020 13:23:17.850110054 CET	8.8.8.8	192.168.2.3	0xc79a	Name error (3)	49.124.12.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 13:23:18.134546995 CET	8.8.8.8	192.168.2.3	0xf92a	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 13:23:18.134546995 CET	8.8.8.8	192.168.2.3	0xf92a	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2020 13:23:18.252717972 CET	8.8.8.8	192.168.2.3	0xd08c	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 13:23:18.252717972 CET	8.8.8.8	192.168.2.3	0xd08c	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2020 13:23:19.367795944 CET	8.8.8.8	192.168.2.3	0x6512	No error (0)	smtp.jif-a sesores.com		217.76.146.62	A (IP address)	IN (0x0001)
Nov 18, 2020 13:23:43.477823019 CET	8.8.8.8	192.168.2.3	0x6abf	Name error (3)	49.124.12.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 18, 2020 13:23:43.823657036 CET	8.8.8.8	192.168.2.3	0xc6f8	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 13:23:43.823657036 CET	8.8.8.8	192.168.2.3	0xc6f8	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2020 13:23:43.927705050 CET	8.8.8.8	192.168.2.3	0x81b6	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2020 13:23:43.927705050 CET	8.8.8.8	192.168.2.3	0x81b6	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2020 13:23:45.118835926 CET	8.8.8.8	192.168.2.3	0x6ffd	No error (0)	smtp.jif-a sesores.com		217.76.146.62	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	192.168.2.3	49725	104.16.155.36	80	C:\Users\user\AppData\Roaming\Windows Update.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 13:23:18.173736095 CET	155	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 13:23:18.205449104 CET	156	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 18 Nov 2020 12:23:18 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Wed, 18 Nov 2020 13:23:18 GMT Location: https://whatismyipaddress.com/ cf-request-id: 067ce83ba400002bcab53dc000000001 Server: cloudflare CF-RAY: 5f41a9729df12bca-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49738	104.16.155.36	80	C:\Users\user\AppData\Roaming\Windows Update.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 13:23:43.859767914 CET	272	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 18, 2020 13:23:43.888427973 CET	273	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 18 Nov 2020 12:23:43 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Wed, 18 Nov 2020 13:23:43 GMT Location: https://whatismyipaddress.com/ cf-request-id: 067ce89ffc0000c2d6d5989000000001 Server: cloudflare CF-RAY: 5f41aa132d0dc2d6-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

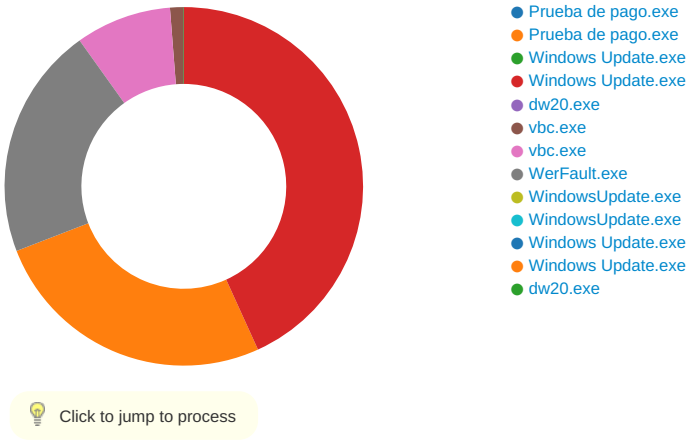
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 18, 2020 13:23:19.484149933 CET	587	49728	217.76.146.62	192.168.2.3	220 smtp-04.servidoresdns.net ESMTP ready
Nov 18, 2020 13:23:19.529613972 CET	49728	587	192.168.2.3	217.76.146.62	EHLO 818225
Nov 18, 2020 13:23:19.582458019 CET	587	49728	217.76.146.62	192.168.2.3	250-smtp-04.servidoresdns.net 250-PIPELINING 250-SIZE 51200000 250-ETRN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-AUTH PLAIN LOGIN CRAM-MD5 250 STARTTLS
Nov 18, 2020 13:23:19.699366093 CET	49728	587	192.168.2.3	217.76.146.62	AUTH login YWRtaW5pc3RyYWNpb25AamlmLWFzZXNvcmVzLmNvbQ==
Nov 18, 2020 13:23:19.753313065 CET	587	49728	217.76.146.62	192.168.2.3	334 UGFzc3dvcmQ6
Nov 18, 2020 13:23:22.824961901 CET	587	49728	217.76.146.62	192.168.2.3	535 5.7.0 Invalid username or password
Nov 18, 2020 13:23:22.826849937 CET	49728	587	192.168.2.3	217.76.146.62	MAIL FROM:<administracion@jif-asesores.com>
Nov 18, 2020 13:23:22.881308079 CET	587	49728	217.76.146.62	192.168.2.3	530 5.7.1 Authentication required
Nov 18, 2020 13:23:45.228775024 CET	587	49741	217.76.146.62	192.168.2.3	220 smtp-04.servidoresdns.net ESMTP ready
Nov 18, 2020 13:23:45.229201078 CET	49741	587	192.168.2.3	217.76.146.62	EHLO 818225
Nov 18, 2020 13:23:45.281131029 CET	587	49741	217.76.146.62	192.168.2.3	250-smtp-04.servidoresdns.net 250-PIPELINING 250-SIZE 51200000 250-ETRN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-AUTH PLAIN LOGIN CRAM-MD5 250 STARTTLS
Nov 18, 2020 13:23:45.281732082 CET	49741	587	192.168.2.3	217.76.146.62	AUTH login YWRtaW5pc3RyYWNpb25AamlmLWFzZXNvcmVzLmNvbQ==
Nov 18, 2020 13:23:45.333138943 CET	587	49741	217.76.146.62	192.168.2.3	334 UGFzc3dvcmQ6
Nov 18, 2020 13:23:48.434525013 CET	587	49741	217.76.146.62	192.168.2.3	535 5.7.0 Invalid username or password

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Prueba de pago.exe PID: 5080 Parent PID: 5684

General

Start time:	13:23:04
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\Prueba de pago.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Prueba de pago.exe'
Imagebase:	0x400000
File size:	1129472 bytes
MD5 hash:	B3A244A097904A4D6689A582D7EC9985
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.215547746.00000000026E2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.215547746.00000000026E2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.215547746.00000000026E2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.215547746.00000000026E2000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.215547746.00000000026E2000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.215631159.0000000002777000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.215631159.0000000002777000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.215631159.0000000002777000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.215631159.0000000002777000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.215631159.0000000002777000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: Prueba de pago.exe PID: 2168 Parent PID: 5080

General

Start time:	13:23:05
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\Prueba de pago.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Prueba de pago.exe'
Imagebase:	0x400000
File size:	1129472 bytes
MD5 hash:	B3A244A097904A4D6689A582D7EC9985
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: 00000001.00000002.232284814.0000000002352000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.232284814.0000000002352000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.232284814.0000000002352000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.232284814.0000000002352000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.232284814.0000000002352000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000001.214625496.00000000004D2000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000001.214625496.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000001.214625496.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000001.214625496.00000000004D2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.232222302.00000000022C0000.00000004.00000001.sdmp, Author:

	Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.232222302.00000000022C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.232222302.00000000022C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.232222302.00000000022C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.232222302.00000000022C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.231765870.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.231765870.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.231765870.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.231765870.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.231765870.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.232402101.0000000002462000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.232402101.0000000002462000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.232402101.0000000002462000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.232402101.0000000002462000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.232402101.0000000002462000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.231841710.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.231841710.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.231841710.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.231841710.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.231841710.0000000000497000.00000040.00000001.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	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Temp\SysInfo.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	244BCAB	CreateFileW
C:\Users\user\AppData\Roaming\Windows Update.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	2BA2D9C	CopyFileW
C:\Users\user\AppData\Roaming\Windows Update.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	2BA2D9C	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Prueba de pago.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\SysInfo.txt	unknown	41	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 50 72 75 65 62 61 20 64 65 20 70 61 67 6f 2e 65 78 65	C:\Users\user\Desktop\Prueba de pago.exe	success or wait	1	2BA0093	WriteFile
C:\Users\user\AppData\Roaming\Windows Update.exe	0	262144	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	5	2BA2D9C	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windows Update.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	2BA2D9C	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Prueba de pago.exe.log	unknown	916	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	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

Analysis Process: Windows Update.exe PID: 5672 Parent PID: 2168

General

Start time:	13:23:13
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Windows Update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Windows Update.exe'
Imagebase:	0x400000
File size:	1129472 bytes
MD5 hash:	B3A244A097904A4D6689A582D7EC9985
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000002.236281439.00000000028B7000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000002.236281439.00000000028B7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.236281439.00000000028B7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.236281439.00000000028B7000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000002.236281439.00000000028B7000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000002.236190946.0000000002822000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000002.236190946.0000000002822000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.236190946.0000000002822000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.236190946.0000000002822000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000002.236190946.0000000002822000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 44%, ReversingLabs
Reputation:	low

Analysis Process: Windows Update.exe PID: 5388 Parent PID: 5672

General

Start time:	13:23:14
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Windows Update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Windows Update.exe'
Imagebase:	0x400000
File size:	1129472 bytes
MD5 hash:	B3A244A097904A4D6689A582D7EC9985
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: 00000003.00000002.266071751.00000000022A2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000003.00000002.266071751.00000000022A2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000003.00000002.266071751.00000000022A2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000002.266071751.00000000022A2000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000003.00000002.266071751.00000000022A2000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000003.00000002.269629299.00000000039E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000002.269629299.00000000039E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000003.00000002.266005625.0000000002210000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000003.00000002.266005625.0000000002210000.00000004.00000001.sdmp, Author: Joe Security

	• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000003.00000002.266005625.0000000002210000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000002.266005625.0000000002210000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000003.00000002.266005625.0000000002210000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000003.00000002.265501034.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000003.00000002.265501034.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000003.00000002.265501034.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000002.265501034.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000003.00000002.265501034.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000003.00000002.266149463.0000000002332000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000003.00000002.266149463.0000000002332000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000003.00000002.266149463.0000000002332000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000002.266149463.0000000002332000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000003.00000002.266149463.0000000002332000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000003.00000002.266901685.00000000029E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000003.00000002.266901685.00000000029E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000003.00000002.266901685.00000000029E1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000003.00000001.234951052.00000000004D2000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000003.00000001.234951052.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000003.00000001.234951052.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000001.234951052.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000003.00000001.234951052.00000000004D2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000003.00000002.265430290.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000003.00000002.265430290.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000003.00000002.265430290.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000002.265430290.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000003.00000002.265430290.0000000000402000.00000040.00000001.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	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\pid.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	21EBCAB	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	21EBCAB	CreateFileW
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	4B757AC	CopyFileW
C:\Users\user\AppData\Roaming\WindowsUpdate.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	4B757AC	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Prueba de pago.exe	success or wait	1	4B72EE6	DeleteFileW
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	4B72EE6	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	4B72EE6	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	35 33 38 38	5388	success or wait	1	4B70093	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	49	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 57 69 6e 64 6f 77 73 20 55 70 64 61 74 65 2e 65 78 65	C:\Users\user\AppData\Roaming\Windows Update.exe	success or wait	1	4B70093	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	0	262144	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	5	4B757AC	CopyFileW
C:\Users\user\AppData\Roaming\WindowsUpdate.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	4B757AC	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	4B70093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4B70093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	4B70093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4B70093	ReadFile
C:\Users\user\AppData\Local\Temp\SysInfo.txt	unknown	4096	success or wait	1	4B70093	ReadFile
C:\Users\user\AppData\Local\Temp\SysInfo.txt	unknown	4096	end of file	1	4B70093	ReadFile
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	4B70093	ReadFile
C:\Users\user\AppData\Roaming\Windows Update.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Users\user\AppData\Roaming\Windows Update.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	4B70093	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	4B70093	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Windows Update	unicode	C:\Users\user\AppData\Roaming\WindowsUpdate.exe	success or wait	1	4B758F2	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	dword	2	1	success or wait	1	4B75492	RegSetValueExW

Analysis Process: dw20.exe PID: 2220 Parent PID: 5388

General

Start time:	13:23:19
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2384
Imagebase:	0x7ff7488e0000
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: 6120 Parent PID: 5388

General

Start time:	13:23:22
Start date:	18/11/2020
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: 00000005.00000002.252405021.0000000000400000.00000040.00000001.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: 3484 Parent PID: 5388

General

Start time:	13:23:22
Start date:	18/11/2020
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: 00000006.00000002.257490095.0000000000400000.00000040.00000001.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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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: WerFault.exe PID: 4112 Parent PID: 5388

General

Start time:	13:23:25
Start date:	18/11/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5388 -s 2488
Imagebase:	0x1330000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA31717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1FE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1FE.tmp.mdmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB36.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB36.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBC4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBC4.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_WindowsUpdate.e_1044ba73b302b1a19e09d2f83986d3c5672f_ffa3413f_105a0017	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DA2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_WindowsUpdate.e_1044ba73b302b1a19e09d2f83986d3c5672f_ffa3413f_105a0017\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA2497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1FE.tmp	success or wait	1	6DA2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB36.tmp	success or wait	1	6DA2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBC4.tmp	success or wait	1	6DA2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1FE.tmp.mdmp	success or wait	1	6DA24BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB36.tmp.WERInternalMetadata.xml	success or wait	1	6DA24BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBC4.tmp.xml	success or wait	1	6DA24BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDDAD.tmp.csv	success or wait	1	6DA24BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDDCD.tmp.txt	success or wait	1	6DA24BEF	unknown

Analysis Process: WindowsUpdate.exe PID: 6328 Parent PID: 3388

General

Start time:	13:23:31
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\WindowsUpdate.exe'
Imagebase:	0x400000
File size:	1129472 bytes
MD5 hash:	B3A244A097904A4D6689A582D7EC9985
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000B.00000002.275686930.00000000027D7000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.275686930.00000000027D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000B.00000002.275686930.00000000027D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.275686930.00000000027D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000B.00000002.275686930.00000000027D7000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000B.00000002.275578797.0000000002742000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.275578797.0000000002742000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000B.00000002.275578797.0000000002742000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.275578797.0000000002742000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000B.00000002.275578797.0000000002742000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 44%, ReversingLabs
Reputation:	low

Analysis Process: WindowsUpdate.exe PID: 6392 Parent PID: 6328

General

Start time:	13:23:32
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\AppData\Roaming\WindowsUpdate.exe'
Imagebase:	0x400000
File size:	1129472 bytes
MD5 hash:	B3A244A097904A4D6689A582D7EC9985
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: 0000000D.00000002.281027497.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000D.00000002.281027497.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000D.00000002.281027497.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000002.281027497.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000D.00000002.281027497.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000D.00000001.274246556.00000000004D2000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000D.00000001.274246556.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000D.00000001.274246556.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000001.274246556.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000D.00000001.274246556.00000000004D2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000D.00000002.281819026.00000000022B2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000D.00000002.281819026.00000000022B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000D.00000002.281819026.00000000022B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000002.281819026.00000000022B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000D.00000002.281819026.00000000022B2000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000D.00000002.281120249.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000D.00000002.281120249.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000D.00000002.281120249.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000002.281120249.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000D.00000002.281120249.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000D.00000002.281367448.00000000006B0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000D.00000002.281367448.00000000006B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000D.00000002.281367448.00000000006B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000002.281367448.00000000006B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000D.00000002.281367448.00000000006B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source:

	0000000D.00000002.281698514.0000000002202000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000D.00000002.281698514.0000000002202000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000D.00000002.281698514.0000000002202000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000002.281698514.0000000002202000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000D.00000002.281698514.0000000002202000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: Windows Update.exe PID: 6456 Parent PID: 6392

General

Start time:	13:23:36
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Windows Update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Windows Update.exe'
Imagebase:	0x400000
File size:	1129472 bytes
MD5 hash:	B3A244A097904A4D6689A582D7EC9985
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000E.00000002.292112517.0000000002702000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000E.00000002.292112517.0000000002702000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000E.00000002.292112517.0000000002702000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000E.00000002.292112517.0000000002702000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000E.00000002.292112517.0000000002702000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000E.00000002.292592274.0000000002797000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000E.00000002.292592274.0000000002797000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000E.00000002.292592274.0000000002797000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000E.00000002.292592274.0000000002797000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000E.00000002.292592274.0000000002797000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: Windows Update.exe PID: 6476 Parent PID: 6456

General

Start time:	13:23:37
Start date:	18/11/2020
Path:	C:\Users\user\AppData\Roaming\Windows Update.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Windows Update.exe'
Imagebase:	0x400000
File size:	1129472 bytes
MD5 hash:	B3A244A097904A4D6689A582D7EC9985
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.305646126.0000000002E26000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000002.305646126.0000000002E26000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000F.00000002.303592164.0000000002302000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.303592164.0000000002302000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.303592164.0000000002302000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000002.303592164.0000000002302000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000002.303592164.0000000002302000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000F.00000002.302581214.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.302581214.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.302581214.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000002.302581214.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000002.302581214.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.305848989.00000000039A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000002.305848989.00000000039A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000F.00000002.303352806.0000000000962000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.303352806.0000000000962000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.303352806.0000000000962000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000002.303352806.0000000000962000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000002.303352806.0000000000962000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000F.00000002.302688394.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.302688394.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.302688394.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000002.302688394.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000002.302688394.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000F.00000001.284532297.0000000000497000.00000040.00020000.sdmp, Author:

	Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000001.284532297.0000000000497000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000001.284532297.0000000000497000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000001.284532297.0000000000497000.00000040.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000001.284532297.0000000000497000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.305679255.0000000002E2C000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000F.00000002.303244261.00000000008D0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.303244261.00000000008D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.303244261.00000000008D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000002.303244261.00000000008D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000002.303244261.00000000008D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: dw20.exe PID: 7024 Parent PID: 6476

General

Start time:	13:23:44
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2376
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

Disassembly

Code Analysis