



ID: 511007
Sample Name: NEW PO.exe
Cookbook: default.jbs
Time: 14:42:08
Date: 28/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report NEW PO.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
System Summary: 6
Data Obfuscation: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 12
Contacted IPs 12
Public 12
Private 12
General Information 12
Simulations 12
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 19
General 19
File Icon 19
Static PE Info 20
General 20
Entrypoint Preview 20
Data Directories 20
Sections 20
Resources 20
Imports 20
Version Infos 20
Network Behavior 20
Snort IDS Alerts 20
Network Port Distribution 20
TCP Packets 20
UDP Packets 21
DNS Queries 21
DNS Answers 21
HTTP Request Dependency Graph 21
HTTP Packets 21
SMTP Packets 22
Code Manipulations 22
Statistics 22

Copyright Joe Security LLC 2021

Behavior 22
System Behavior 22
Analysis Process: NEW PO.exe PID: 7156 Parent PID: 4972 22
General 22
File Activities 23
File Created 23
File Written 23
File Read 23
Analysis Process: NEW PO.exe PID: 6044 Parent PID: 7156 23
General 23
File Activities 25
File Created 25
File Deleted 25
File Written 26
File Read 26
Registry Activities 26
Key Value Created 26
Key Value Modified 26
Analysis Process: vbc.exe PID: 6692 Parent PID: 6044 26
General 26
File Activities 26
File Created 26
File Deleted 26
File Written 26
File Read 26
Analysis Process: vbc.exe PID: 6728 Parent PID: 6044 26
General 26
File Activities 27
File Created 27
Analysis Process: WerFault.exe PID: 6724 Parent PID: 6044 27
General 27
File Activities 27
File Created 27
File Deleted 27
File Written 27
Registry Activities 27
Key Created 27
Key Value Created 27
Analysis Process: WindowsUpdate.exe PID: 6976 Parent PID: 3352 28
General 28
File Activities 28
File Created 28
File Written 28
File Read 28
Analysis Process: WindowsUpdate.exe PID: 7120 Parent PID: 6976 28
General 28
File Activities 29
File Created 29
File Read 30
Analysis Process: WindowsUpdate.exe PID: 4816 Parent PID: 3352 30
General 30
Analysis Process: WindowsUpdate.exe PID: 3996 Parent PID: 4816 30
General 30
Analysis Process: vbc.exe PID: 6828 Parent PID: 3996 33
General 33
Analysis Process: vbc.exe PID: 5076 Parent PID: 3996 33
General 33
Analysis Process: WerFault.exe PID: 6008 Parent PID: 3996 34
General 34
Analysis Process: WerFault.exe PID: 5028 Parent PID: 3996 34
General 34
Disassembly 34
Code Analysis 34

Copyright Joe Security LLC 2021

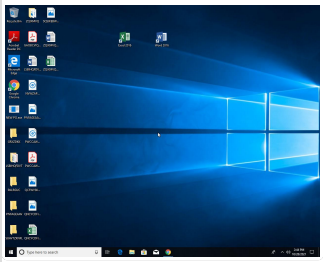
Windows Analysis Report NEW PO.exe

Overview

General Information

Sample Name:	NEW PO.exe
Analysis ID:	511007
MD5:	770f6e88b7bf3fe…
SHA1:	ed96d179403ab3..
SHA256:	08187be5bb78da..
Tags:	exe hawkeye
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

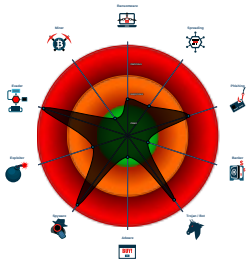
HawkEye
MailPassView

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

Signatures

- Yara detected MailPassView
- Yara detected HawkEye Keylogger
- Yara detected AntiVM3
- Malicious sample detected (through …
- Detected HawkEye Rat
- Tries to detect sandboxes and other…
- Tries to steal Mail credentials (via fil…
- Machine Learning detection for samp…
- May check the online IP address of …
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal browser in…
- Sample uses process hollowing tech…
- Installs a global keyboard hook

Classification



Process Tree

- **System is w10x64**
- NEW PO.exe (PID: 7156 cmdline: 'C:\Users\user\Desktop\NEW PO.exe' MD5: 770F6E88B7BF3FE3AAE144A5AA41DC96)
  - NEW PO.exe (PID: 6044 cmdline: C:\Users\user\Desktop\NEW PO.exe MD5: 770F6E88B7BF3FE3AAE144A5AA41DC96)
    - vbc.exe (PID: 6692 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 6728 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - WerFault.exe (PID: 6724 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6044 -s 2424 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- WindowsUpdate.exe (PID: 6976 cmdline: 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' MD5: 770F6E88B7BF3FE3AAE144A5AA41DC96)
  - WindowsUpdate.exe (PID: 7120 cmdline: C:\Users\user\AppData\Roaming\WindowsUpdate.exe MD5: 770F6E88B7BF3FE3AAE144A5AA41DC96)
- WindowsUpdate.exe (PID: 4816 cmdline: 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' MD5: 770F6E88B7BF3FE3AAE144A5AA41DC96)
  - WindowsUpdate.exe (PID: 3996 cmdline: C:\Users\user\AppData\Roaming\WindowsUpdate.exe MD5: 770F6E88B7BF3FE3AAE144A5AA41DC96)
    - vbc.exe (PID: 6828 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 5076 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - WerFault.exe (PID: 6008 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3996 -s 2412 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 5028 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3996 -s 2412 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000000.391647562.000000000358E000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000012.00000000.391647562.000000000358E000.00000004.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x25f8:$hawkstr1: HawkEye Keylogger • 0x2088:$hawkstr2: Dear HawkEye Customers! • 0x21b6:$hawkstr3: HawkEye Logger Details:
00000007.00000000.320473195.0000000007EE0000.00000004.00020000.sdmp	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
00000012.00000000.400119443.000000000359A000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000012.00000000.400119443.000000000359A000.00000004.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x7230:$hawkstr1: HawkEye Keylogger • 0xc090:$hawkstr1: HawkEye Keylogger • 0xc0f0:$hawkstr2: Dear HawkEye Customers! • 0x126:$hawkstr3: HawkEye Logger Details:
Click to see the 200 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.0.NEW PO.exe.2d9bffc.45.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
7.0.NEW PO.exe.2afd174.43.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
7.0.NEW PO.exe.7ee0000.37.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
7.0.NEW PO.exe.45fa72.29.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
16.0.WindowsUpdate.exe.45fa72.22.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 622 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:



May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected HawkEye Keylogger

Installs a global keyboard hook

Copyright Joe Security LLC 2021

Contains functionality to log keystrokes (.Net Source)

Contains functionality to register a low level keyboard hook

System Summary:



Malicious sample detected (through community Yara rule)

Data Obfuscation:



.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:



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

Malware Analysis System Evasion:



Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:



Injects a PE file into a foreign processes

Sample uses process hollowing technique

Writes to foreign memory regions

.NET source code references suspicious native API functions

Stealing of Sensitive Information:



Yara detected MailPassView

Yara detected HawkEye Keylogger

Tries to steal Mail credentials (via file registry)

Tries to steal Mail credentials (via file access)

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

Yara detected WebBrowserPassView password recovery tool

Tries to steal Instant Messenger accounts or passwords

Remote Access Functionality:



Yara detected HawkEye Keylogger

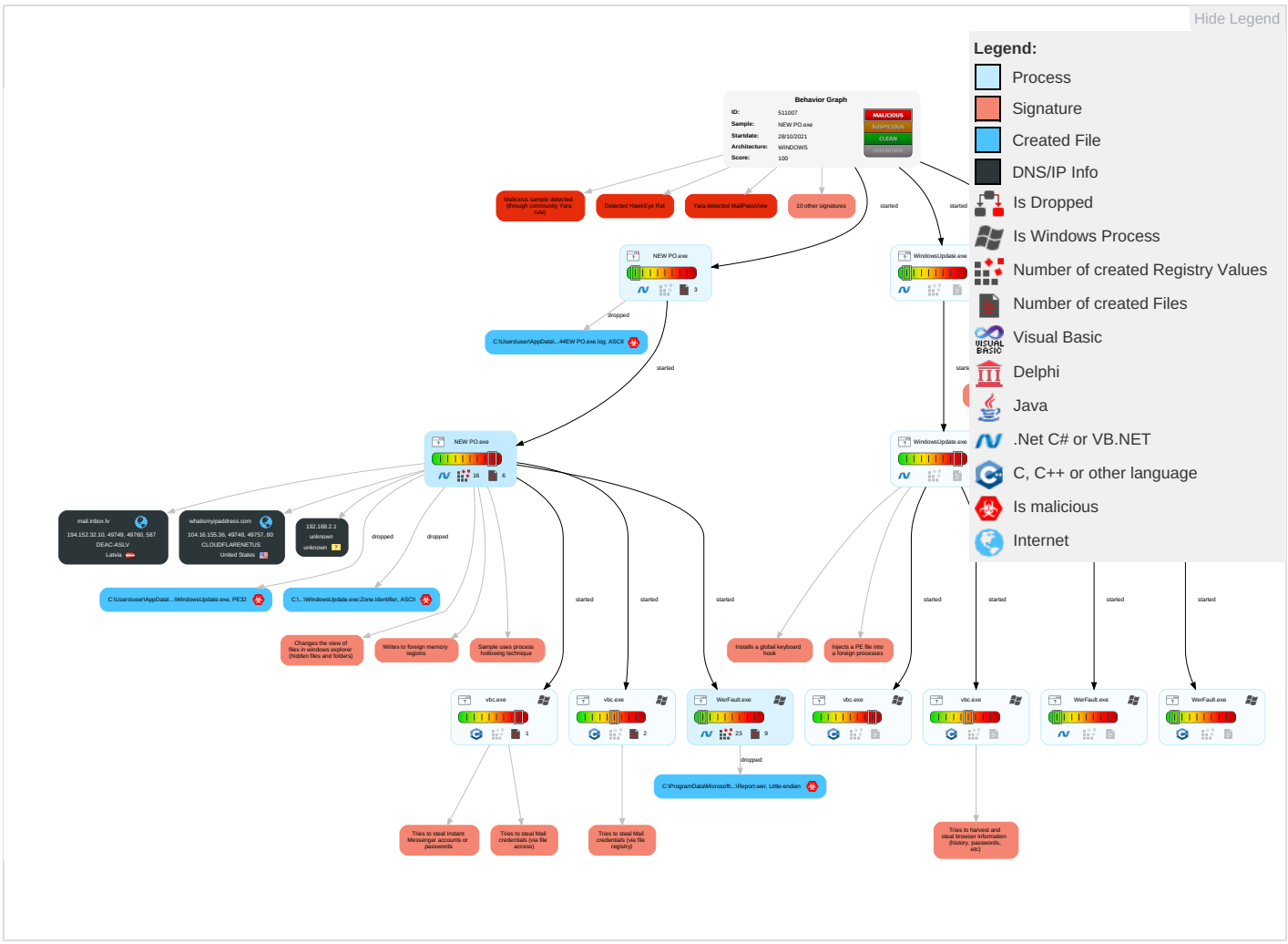
Detected HawkEye Rat

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	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1 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	Registry Run Keys / Startup Folder 1	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1 1	Input Capture 3 1 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth

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

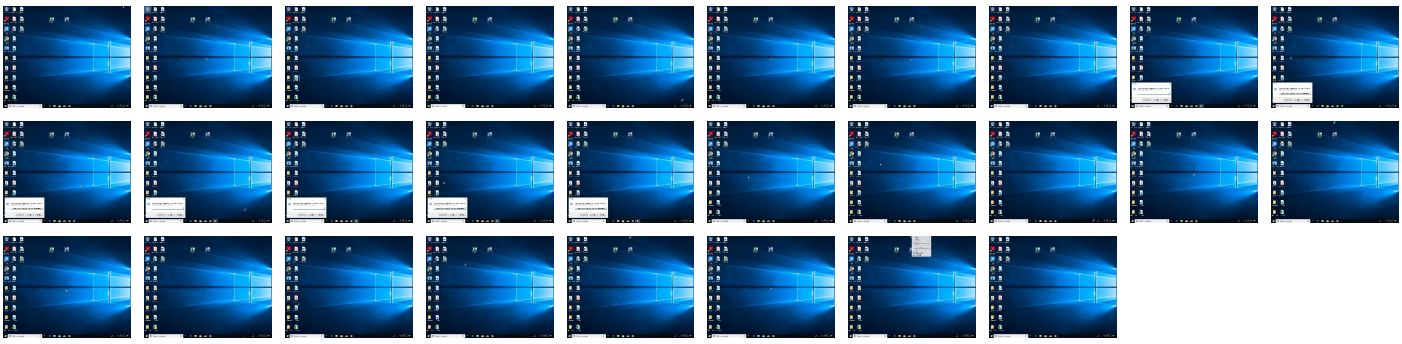
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
NEW PO.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.0.WindowsUpdate.exe.400000.6.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
16.0.WindowsUpdate.exe.400000.6.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
22.0.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
10.0.vbc.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
11.0.vbc.exe.400000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
11.0.vbc.exe.400000.1.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
16.0.WindowsUpdate.exe.400000.21.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
16.0.WindowsUpdate.exe.400000.21.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
18.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
18.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
16.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
16.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
7.0.NEW PO.exe.400000.11.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
7.0.NEW PO.exe.400000.11.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.NEW PO.exe.474fbd0.5.unpack	100%	Avira	TR/Inject.vcoldi		Download File
7.0.NEW PO.exe.400000.6.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
7.0.NEW PO.exe.400000.6.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
18.0.WindowsUpdate.exe.400000.26.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
18.0.WindowsUpdate.exe.400000.26.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
18.0.WindowsUpdate.exe.400000.16.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
18.0.WindowsUpdate.exe.400000.16.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
22.0.vbc.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
23.0.vbc.exe.400000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
23.0.vbc.exe.400000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
11.0.vbc.exe.400000.4.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
23.0.vbc.exe.400000.1.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
22.0.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
7.0.NEW PO.exe.400000.38.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
7.0.NEW PO.exe.400000.38.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
18.0.WindowsUpdate.exe.400000.11.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
18.0.WindowsUpdate.exe.400000.11.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
23.0.vbc.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
18.0.WindowsUpdate.exe.400000.4.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
18.0.WindowsUpdate.exe.400000.4.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
17.2.WindowsUpdate.exe.459fbd0.4.unpack	100%	Avira	TR/Inject.vcoldi		Download File
16.0.WindowsUpdate.exe.400000.4.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
16.0.WindowsUpdate.exe.400000.4.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
11.0.vbc.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
11.0.vbc.exe.400000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
10.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
10.0.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
10.0.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
10.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
22.0.vbc.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
18.0.WindowsUpdate.exe.400000.6.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
18.0.WindowsUpdate.exe.400000.6.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
23.0.vbc.exe.400000.4.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
18.0.WindowsUpdate.exe.400000.37.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
18.0.WindowsUpdate.exe.400000.37.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
7.0.NEW PO.exe.400000.21.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
7.0.NEW PO.exe.400000.21.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
22.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
22.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
7.0.NEW PO.exe.400000.16.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
7.0.NEW PO.exe.400000.16.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
18.0.WindowsUpdate.exe.400000.21.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
18.0.WindowsUpdate.exe.400000.21.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
15.2.WindowsUpdate.exe.402fbd0.5.unpack	100%	Avira	TR/Inject.vcoldi		Download File
16.0.WindowsUpdate.exe.400000.11.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
16.0.WindowsUpdate.exe.400000.11.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
16.0.WindowsUpdate.exe.400000.16.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
16.0.WindowsUpdate.exe.400000.16.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
10.0.vbc.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
7.0.NEW PO.exe.400000.26.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
7.0.NEW PO.exe.400000.26.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
7.0.NEW PO.exe.400000.4.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
7.0.NEW PO.exe.400000.4.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
7.2.NEW PO.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
7.2.NEW PO.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://whatismyipaddress.com4	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=6856811916691;gt	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://foo.com/foo	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.155.36	true	false		high
mail.inbox.lv	194.152.32.10	true	false		high

Contacted URLs

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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.152.32.10	mail.inbox.lv	Latvia		12993	DEAC-ASLV	false
104.16.155.36	whatismyipaddress.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	511007
Start date:	28.10.2021
Start time:	14:42:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW PO.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:	35
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@22/22@4/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.6% (good quality ratio 2.2%) • Quality average: 69% • Quality standard deviation: 36.5%
HCA Information:	• Successful, ratio: 100% • 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

Simulations

Behavior and APIs

Time	Type	Description
14:43:04	API Interceptor	30x Sleep call for process: NEW PO.exe modified
14:43:16	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
14:43:25	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
14:43:27	API Interceptor	25x Sleep call for process: WindowsUpdate.exe modified
14:43:35	API Interceptor	2x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_NEW PO.exe_8055783c936bcb979ba1bb535241e11f1ba84c43_9f8533cf_1bd60d79\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.315991209012618
Encrypted:	false
SSDEEP:	192:8vGZVHBUZMXyaPXUlXK8zlUGrf/u7sjS274ltw9:kGbBUZMXyascf/u7sjX4ltw9
MD5:	4BF5AECA5BB4D456B80A0893C8B0A06F
SHA1:	2A6B42F5FBFE0D2C9B0A9F6197A718071C0787FF
SHA-256:	7600030D4651A32743C99EAF12CD95408762D31B91EEF6CCA2B670C285BD5669
SHA-512:	0FB1526C720E879D40A7C3C94716B9259930D7FB02EBDCB7A6AC27F7AFB5A5D61242243BE2E9996BD457327609EA848F7A9AAC422D35A8A14131AA833A9046E
Malicious:	**true**
Reputation:	unknown
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.=.1.3.2.7.9.9.3.1.0.0.3.0.0.9.3.0.5.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.9.9.3.1.0.1.3.8.0.6.1.5.8.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.b.a.b.a.d.0.0.-.5.f.f.2.-.4.5.5.a.-.9.9.d.6.-.e.8.d.8.0.7.9.5.1.1.3.1.....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.=.d.d.0.6.2.2.4.2.-.7.d.6.5.-.4.7.3.0.-.9.1.9.2.-.f.c.f.a.1.a.1.d.0.d.1.d.....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.=.N.E.W. .P.O...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.C.L.R.S.u.r.r.o.g.a.t.e.E.n.t...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.9.c.-.0.0.0.1.-.0.0.1.c.-.1.b.b.b.-.0.e.c.a.4.4.c.c.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.1.5.a.5.0.3.3.1.0.1.f.6.3.6.c.0.6.3.d.c.0.6.b.9.d.b.8.1.0.7.0.f.0.0.0.0.0.0.0.0.!.0.0.0.0.e.d.9.6.d.1.7.9.4.0.3.a.b.3.1.9.d.a.6.2.c.0.9.2.a.8.1.7.a.5.e.b.e.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_WindowsUpdate.ex_f9725cf91236fb8dfe1d0104b8abc11733cfe3b_2f3b6c15_171ed716\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_WindowsUpdate.ex_f9725cf91236fb8dfe1d0104b8abc11733cfe3b_2f3b6c15_171ed716\Report.wer	
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.317492010859222
Encrypted:	false
SSDEEP:	192:7OPtFZVHBUZMXSaPXUlXK8zIUGrq/u7sjS274ItT:stFbBUZMXSascq/u7sjX4ItT
MD5:	B1FA9A9909F2FC460215410189DAD479
SHA1:	3593C650A86C5CE4F8DC6C624E710C9F78C2A3AB
SHA-256:	B60A4E81770237FFD38D5061B828D2D1D07A1FA7F31EA576473D72A0BFAC0E76
SHA-512:	24863AE1A8EA8411BDBB89ED9EFDD2DD7FDDD7589387A9467D06D8D53EA177EF3656DC2243FD08468204B56D9916F05F509679329A792FCCC1813D97E24B1A(
Malicious:	false
Reputation:	unknown
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.=.1.3.2.7.9.9.3.1.0.4.0.7.0.0.2.6.6.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.9.9.3.1.0.5.0.5.4.4.0.0.4.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.5.3.e.0.c.b.9.-.3.e.6.2.-.4.a.3.4.-.8.6.9.3.-.e.a.8.7.1.d.f.f.6.d.8.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.=.1.7.b.7.3.2.f.2.-.0.3.a.6.-.4.c.3.5.-.a.4.b.4.-.1.d.d.f.7.7.7.a.0.d.f.d.....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.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.C.L.R.S.u.r.r.o.g.a.t.e.E.n.t...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.f.9.c.-.0.0.0.1.-.0.0.1.c.-.f.d.9.d.-.5.4.d.e.4.4.c.c.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.1.5.a.5.0.3.3.1.0.1.f.6.3.6.c.0.6.3.d.c.0.6.b.9.d.b.8.1.0.7.0.f.0.0.0.0.0.0.0.0.!.0.0.0.0.e.d.9.6.d.1.7.9.4.0.3.a.b.3.1.9.d.a.6.2.c.0.9.2.a.8.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6775.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Oct 28 21:43:27 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	449964
Entropy (8bit):	3.6035865303609618
Encrypted:	false
SSDEEP:	3072:DmVJqTllF9gIOgF5wSw10pi9UCgUVlYYFx3oNTwegf0Yr9xjd+pMBlRZwD72p:DuqTllF9RpD2xTjKQceC0YrQp
MD5:	EA0FD51B403912177C2B26EBDD1A5AB1
SHA1:	DD8B91956C56A71A99A95EB18CD8C6BA56C21AB2
SHA-256:	3D5B64107139405029346058857F2F358ADA5C3F8211C4B803594B6E2CBEAA42
SHA-512:	155D054675CF0872A8C98BDF0789506801A99E86C44A00E8656D07510E33BDFF262AE166CCF89500445202D983DDC3D5FE5BAF7CBEA8C40F8A85106AE050A0A
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....{a.....T.....%..h.....<...d1.....=.....`.....8.....T.....]..... 1.....3.....U.....B.....$4... ...GenuineIntelW.....T.....i.{a.....0.....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..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FB2.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8336
Entropy (8bit):	3.689893445241779
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiEG6lo/6Yno6RgmfZPgSRCprx89bXysf69m:RrlsNit6C6Yo6RgmfRgSnXxfZ
MD5:	CFC0F3B85C65720723980E8C1DA197F6
SHA1:	0AE9AC449498FA019FB696E799C5081AEAADF187
SHA-256:	0EDA42A1EB6F0C2030499A5E30895E07DB3C26B92D644E7A5DBCDEB51ACF10DE
SHA-512:	BFAB105DAEEEB2650BA354521C3F46D5D6596C2170EEE3F9A9793869B213F4525FE0DEC6362A1213B22C687B90E070E659E88BF724A3435AC6866FC57FCB08DA
Malicious:	false
Reputation:	unknown
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.>.6.0.4.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER836C.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720

C:\ProgramData\Microsoft\Windows\WER\Temp\WER836C.tmp.xml	
Entropy (8bit):	4.4547449585238095
Encrypted:	false
SSDEEP:	48:cvIwSD8zsSJgtWI9FJWSC8By8fm8M4JpPWlFy+q8v4PWQe7W6Zkd:uITfgK4SNNJZKAe7WUkd
MD5:	E5DBAA3FCC088650C247209B16E6D90D
SHA1:	2E57CEBC70AD7DE1CF396C0C07280EBFBF290FFE
SHA-256:	05E0F0403A6D803BACE005ABE0255FF2D915E79B3CF64C2C84EBBC2673266914
SHA-512:	40238DFE9C4824AE636196FC2381ED06F987B107C7AB3D00F8743B84BD45021EEC4F19EE8EFDD940F2E18C93F8FE009C220A2D65E38817A048F70E244C46945D
Malicious:	false
Reputation:	unknown
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="1230174" />.. <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\WERACBA.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Oct 28 21:44:02 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	439718
Entropy (8bit):	3.7315579748248786
Encrypted:	false
SSDEEP:	3072:xvm3oH9BGjx9gIOgF5zGRyApw0VmUCgUityZdBrvLuWozt/L2Vc0Cjd+peQ7bU/o:xldBG99RpDaPpwhTjZTKR0vpyFe
MD5:	FC30AAB9F9F32DA48F184F0CCA49188B
SHA1:	DC73378F02E183142F72A31583C1C7B40ACE0762
SHA-256:	8155D5002069C5C3C96F62E6581C9411CFBBA02DF8A968831E32A27743FC5233
SHA-512:	DC84C89587A42959806840EF7FECBA1ECB215127F7557E9E63B213D582149408F17913CFDBD8F9774CF8552B3E0566B6353BAFAD114B84F17189F4C7E030CCA0
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....{a.....$.....%..8.....$....0.....;..b~.....`.....8.....T.....\...Y.....0.....2.....U.....B.....p3... ...GenuineIntelW.....T.....{a..... .....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..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE20.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8368
Entropy (8bit):	3.6864794615673935
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiqY6PL6Yx36qFRgmfZYgSRCprg89b+ZsfGWKm:RrlsNi96D6YR6qFRgmfSgSU+yfGy
MD5:	650062C22FF749C2444559315E871C75
SHA1:	944F516F87F3DBC9A309BE538F685AB7B0F8C0E0
SHA-256:	5139AC177A5C63F4F4A0C9CD9CB26BA1A316A7ED4EB7AAFF776AED1B2B545BAD
SHA-512:	BF536FAF04DF0F997590FED0494DF9BD60758406FF6E8BA545B361CC31DE26102093342993DEF3280E39C459974B4649CF8B41BBE921B97DAF9942B2B9782D9D
Malicious:	false
Reputation:	unknown
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.>.3.9.9.6.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC48A.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4755
Entropy (8bit):	4.461257300281675
Encrypted:	false
SSDEEP:	48:cvIwSD8zsSJgtWI9FJWSC8BX8fm8M4JZPWlFw9+q8vnPW3eadoZkd:uITfgK4SNyJZKueadSkd
MD5:	478C37E58C9ED9F7B169C268F097CEF6

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC48A.tmp.xml	
SHA1:	51A1BE08A636F85E1A5F76DE8FF353C069F25986
SHA-256:	4A78098278530B111978CDE087D9AD979591F8CA0D2FB86849FB2AD0307869A6
SHA-512:	3B431CAE51FCD9013985FAC93A971ED0C8DDF9A0B9420EC4E84D43AFFAEFF76E79621197D9E86E58DB1450FA89F2B9493573D632C1AA7F2E9626C9DF07618F37
Malicious:	false
Reputation:	unknown
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="1230174" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW PO.exe.log	
Process:	C:\Users\user\Desktop\NEW PO.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WindowsUpdate.exe.log	
Process:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\bhv94FC.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x0456f320, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	1.0515290357457872
Encrypted:	false
SSDEEP:	24576:dVqA2TaAxucRfDw/ND0Xko5QqbMgSFDb7uBi:uRfD3y
MD5:	5B2767DB09030D6BFA3DECDD780AA574

C:\Users\user\AppData\Local\Temp\bhv94FC.tmp	
SHA1:	5A863841DFF01C3C305CFEB9C652D0E6B6976DB1
SHA-256:	C14996019A48718A5DB499651C737EB902699611C66087EB7B78EEC49FB7F09A
SHA-512:	EFB28E20C19138610139095BDD9A30F9B02459A5DC9ECBDFBCFEF6446C4A732BB19BD75B4800A66ED8DB10A273E42D47322770D209B01ADC2BB7A98E2DB99F 61
Malicious:	false
Reputation:	unknown
Preview:	.V. ... .F1.....te3....wg.....o.....,*...y..,*...y..h.q.....6..43....wl.....Z.....B..... ....7*...y..... .....+...y.y.....+...y..... .....

C:\Users\user\AppData\Local\Temp\bhvF8EB.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x2e45d84b, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	1.0515137857335044
Encrypted:	false
SSDEEP:	24576:F7qA2TaAxucRfDw/ND0Xko5QqbMgSFDb7uBi:URfD3y
MD5:	3042CAAEE52655CA002C2960DBD44156
SHA1:	5294AF930E5AEEE2B024744DF918FFE768CB97C9
SHA-256:	7189E52085B69F651887B9B5DB9E3F9683BE94D5B247F7AE5B1A73B151E24858
SHA-512:	69727D18648F18396E00A8C08CEF2471F803305F62E203DDB155F45E3DD0522DE989E63E264F43874DC2C7A314BB35A4DF61A94E167040D341BF7ABC8A59710D
Malicious:	false
Reputation:	unknown
Preview:	.E.K... .....F1.....te3....wg.....o.....,*...y..,*...y..h.q.....6..43....wl.....Z.....B..... ....7*...y..... .....D>7*...y.y.....).J.*...y?..... .....

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
Reputation:	unknown
Preview:	..

C:\Users\user\AppData\Roaming\WindowsUpdate.exe	
Process:	C:\Users\user\Desktop\NEW PO.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	774144
Entropy (8bit):	7.880107119214288
Encrypted:	false
SSDEEP:	12288:S1xn35Qfx7M5fMcm8FvLS3agsmMIFCnJGzhm0pIy4n8wmnPVMliAyZg5N44:Sz351JrFzeNIJGFBmy48ddMliRZg5N4
MD5:	770F6E88B7BF3FE3AAE144A5AA41DC96
SHA1:	ED96D179403AB319DA62C092A817A5EBEEA8C3DA
SHA-256:	08187BE5BB78DA6C7751C5D870D46E43E6B4204DB6ABF2CC2D80E9830FD136BA
SHA-512:	90D8F872263FBB46BC8E71BC7A370581F39DD1FE740E5972805D45C4BD8FB81E19E12D3154C3E694839F24AAD9A5E73ECBF381FA54DD399BF8E4145589C8DD1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Roaming\WindowsUpdate.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...dnza.....0..... .....@.. .....@..... ..@.....K..... ....H.....text...4.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....G..`.....C...:.....?.....?.....?.....?.... ....

C:\Windows\appcompat\Programs\Amcache.hve	
MD5:	B9FEDE34538A4B64EABC43541461671D
SHA1:	2BE5E4F403EEFB0CD08619280408437F9471C164
SHA-256:	FB09EB2D2149D103F2B612E793913B92A270CD1B9B779C9CF61384686E9FAAB6
SHA-512:	0884950B4CEA35AB2F8D13E925DC9A48A12384497957A44E558042EC5D567EB4F8400C8636843EBADB9FFC66D4B7152C291A1D1DE097DBA95C666F84764DAF4
Malicious:	false
Reputation:	unknown
Preview:	regfZ...Z...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm...D..... ....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	4.217554824061032
Encrypted:	false
SSDEEP:	768:L20kdCQMwqhCrrC2i5ftx1aJ4Xw/FT7ABqXPeq5QMVyi6a54LXsuzxSNWv:LNfCCg38CREhL
MD5:	AD5FEEAF6306262EDDB4ACF5D8D346FB
SHA1:	D4E55BC73AA0CE125C35FA9D87F9D8233E88CEF6
SHA-256:	44232A8F8FB4C8CA684C7941CBEC62163EB822C9F6F53C1671CC3EA38AD89521
SHA-512:	F2AC2C9360957F9DFD458923C6F3AFB963E367E10D039C8E3BBD834D7E5758AB09DB2782CF46EA7903E09F9B1DBB4F97DB514500D3540ADF709DEE3C80CC37A
Malicious:	false
Reputation:	unknown
Preview:	regfY...Y...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm...D..... ....HvLE.....Y.....Oyf.vA.k.L...8..... ....P.....0..... ..hbin.....p.\..,.....nk,.%-..D..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .%-..D..... ....Z.....Root.....lf.....Root....nk .%-..D.....}..... .....*.....DeviceCensus.....vk.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.880107119214288
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	NEW PO.exe
File size:	774144
MD5:	770f6e88b7bf3fe3aae144a5aa41dc96
SHA1:	ed96d179403ab319da62c092a817a5ebeea8c3da
SHA256:	08187be5bb78da6c7751c5d870d46e43e6b4204db6abf2cc2d80e9830fd136ba
SHA512:	90d8f872263fbb46bc8e71bc7a370581f39dd1fe740e5972805d45c4bd8fb81e19e12d3154c3e694839f24aad9a5e73ecbf381fa54dd399bf8e4145589c8dd19
SSDEEP:	12288:S1xn35Qfx7M5fMcm8FvLS3agsmMIFCnJGzhm0ply4n8wmnPVMliAyZg5N44:Sz351JrFzeNIJGFBmy48ddMliRZg5N4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...dnza.....0..... .....@.. .....@.....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4be22e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x617A6E64 [Thu Oct 28 09:33:24 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbc234	0xbc400	False	0.923099269588	data	7.88873846261	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x608	0x800	False	0.328125	data	3.46210381505	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/28/21-14:43:11.069910	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49748	104.16.155.36	192.168.2.3
10/28/21-14:43:47.071824	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49757	104.16.155.36	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 28, 2021 14:43:10.965198040 CEST	192.168.2.3	8.8.8.8	0x9e68	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Oct 28, 2021 14:43:12.834615946 CEST	192.168.2.3	8.8.8.8	0xc9ce	Standard query (0)	mail.inbox.lv	A (IP address)	IN (0x0001)
Oct 28, 2021 14:43:46.966675043 CEST	192.168.2.3	8.8.8.8	0xae52	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Oct 28, 2021 14:43:49.683657885 CEST	192.168.2.3	8.8.8.8	0x1315	Standard query (0)	mail.inbox.lv	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 28, 2021 14:43:10.990313053 CEST	8.8.8.8	192.168.2.3	0x9e68	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Oct 28, 2021 14:43:10.990313053 CEST	8.8.8.8	192.168.2.3	0x9e68	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Oct 28, 2021 14:43:12.853415966 CEST	8.8.8.8	192.168.2.3	0xc9ce	No error (0)	mail.inbox.lv		194.152.32.10	A (IP address)	IN (0x0001)
Oct 28, 2021 14:43:34.242847919 CEST	8.8.8.8	192.168.2.3	0x54e8	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Oct 28, 2021 14:43:46.989118099 CEST	8.8.8.8	192.168.2.3	0xae52	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Oct 28, 2021 14:43:46.989118099 CEST	8.8.8.8	192.168.2.3	0xae52	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Oct 28, 2021 14:43:49.702991962 CEST	8.8.8.8	192.168.2.3	0x1315	No error (0)	mail.inbox.lv		194.152.32.10	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	49748	104.16.155.36	80	C:\Users\user\Desktop\NEW PO.exe

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 14:43:11.043543100 CEST	1091	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Oct 28, 2021 14:43:11.069910049 CEST	1092	IN	HTTP/1.1 403 Forbidden Date: Thu, 28 Oct 2021 12:43:11 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 16 Connection: keep-alive X-Frame-Options: SAMEORIGIN Referrer-Policy: same-origin Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Server: cloudflare CF-RAY: 6a543f9218035b86-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 65 72 72 6f 72 20 63 6f 64 65 3a 20 31 30 32 30 Data Ascii: error code: 1020

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49757	104.16.155.36	80	C:\Users\user\Desktop\NEW PO.exe

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 14:43:47.042749882 CEST	1169	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Oct 28, 2021 14:43:47.071824074 CEST	1169	IN	HTTP/1.1 403 Forbidden Date: Thu, 28 Oct 2021 12:43:47 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 16 Connection: keep-alive X-Frame-Options: SAMEORIGIN Referrer-Policy: same-origin Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Server: cloudflare CF-RAY: 6a5440731a042c52-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 65 72 72 6f 72 20 63 6f 64 65 3a 20 31 30 32 30 Data Ascii: error code: 1020

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Oct 28, 2021 14:43:15.111594915 CEST	587	49749	194.152.32.10	192.168.2.3	220 mail.inbox.lv relay for customers ESMTP ready
Oct 28, 2021 14:43:15.118011951 CEST	49749	587	192.168.2.3	194.152.32.10	EHLO 051829
Oct 28, 2021 14:43:15.160445929 CEST	587	49749	194.152.32.10	192.168.2.3	250-mail.inbox.lv relay for customers 250-SIZE 59900000 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Oct 28, 2021 14:43:15.162899017 CEST	49749	587	192.168.2.3	194.152.32.10	STARTTLS
Oct 28, 2021 14:43:15.209489107 CEST	587	49749	194.152.32.10	192.168.2.3	220 2.0.0 Start TLS
Oct 28, 2021 14:43:51.831136942 CEST	587	49760	194.152.32.10	192.168.2.3	220 mail.inbox.lv relay for customers ESMTP ready
Oct 28, 2021 14:43:51.837745905 CEST	49760	587	192.168.2.3	194.152.32.10	EHLO 051829
Oct 28, 2021 14:43:51.880465031 CEST	587	49760	194.152.32.10	192.168.2.3	250-mail.inbox.lv relay for customers 250-SIZE 59900000 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
Oct 28, 2021 14:43:51.880744934 CEST	49760	587	192.168.2.3	194.152.32.10	STARTTLS
Oct 28, 2021 14:43:51.923423052 CEST	587	49760	194.152.32.10	192.168.2.3	220 2.0.0 Start TLS

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: NEW PO.exe PID: 7156 Parent PID: 4972

General

Start time:	14:42:57
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\NEW PO.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NEW PO.exe'
Imagebase:	0xeb0000
File size:	774144 bytes
MD5 hash:	770F6E88B7BF3FE3AAE144A5AA41DC96
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.296608068.0000000003321000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.297183407.0000000004329000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.297183407.0000000004329000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.297183407.0000000004329000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.297183407.0000000004329000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.297183407.0000000004329000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: NEW PO.exe PID: 6044 Parent PID: 7156

General

Start time:	14:43:05
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\NEW PO.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\NEW PO.exe
Imagebase:	0x600000
File size:	774144 bytes
MD5 hash:	770F6E88B7BF3FE3AAE144A5AA41DC96
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000007.00000000.320473195.0000000007EE0000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000007.00000000.293845303.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000000.293845303.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.293845303.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000000.293845303.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000000.293845303.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source:

00000007.00000000.293293515.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000000.293293515.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.293293515.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000000.293293515.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000000.293293515.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.318319979.0000000002DF6000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000000.313426139.0000000003AA1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000000.313426139.0000000003AA1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000007.00000000.310799543.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000000.310799543.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.310799543.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000000.310799543.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000000.310799543.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.317923125.0000000002D5E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000000.317923125.0000000002D5E000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000007.00000002.366905535.0000000007C60000.00000004.00020000.sdmp, Author: Arnim Rupp
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000007.00000000.292647600.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000000.292647600.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.292647600.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000000.292647600.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000000.292647600.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.317941479.0000000002D6A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000007.00000000.315132026.0000000007C60000.00000004.00020000.sdmp, Author: Arnim Rupp
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000007.00000000.315200782.0000000007EE0000.00000004.00020000.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.313223758.0000000002D6A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.313404967.0000000002DFA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000000.318371710.0000000003AA1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000000.318371710.0000000003AA1000.00000004.00000001.sdmp, Author:

	Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000007.00000000.315913694.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000000.315913694.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.315913694.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000000.315913694.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000000.315913694.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000007.00000000.292021486.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000000.292021486.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.292021486.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000000.292021486.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000000.292021486.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.313199266.0000000002D5E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000000.313199266.0000000002D5E000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000007.00000002.360431975.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.360431975.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.360431975.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.360431975.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000002.360431975.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.362315745.0000000002ADF000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000007.00000002.362315745.0000000002ADF000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000007.00000002.367050092.0000000007EE0000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.364013571.0000000003AA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.364013571.0000000003AA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000007.00000000.320411963.0000000007C60000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.362383688.0000000002B10000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Key Value Modified

Analysis Process: vbc.exe PID: 6692 Parent PID: 6044

General

Start time:	14:43:15
Start date:	28/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000A.00000000.316195444.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000A.00000000.317013131.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000A.00000000.316648058.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000A.00000002.331769902.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 6728 Parent PID: 6044

General

Start time:	14:43:15
Start date:	28/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000000.319742971.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000000.320558066.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000000.320160730.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.321594034.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

Analysis Process: WerFault.exe PID: 6724 Parent PID: 6044

General

Start time:	14:43:20
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6044 -s 2424
Imagebase:	0x20000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
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.00000003.337353333.0000000005780000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000D.00000003.337353333.0000000005780000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000D.00000003.337353333.0000000005780000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: WindowsUpdate.exe PID: 6976 Parent PID: 3352

General

Start time:	14:43:25
Start date:	28/10/2021
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\WindowsUpdate.exe'
Imagebase:	0x780000
File size:	774144 bytes
MD5 hash:	770F6E88B7BF3FE3AAE144A5AA41DC96
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000F.00000002.359519718.0000000003C09000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.359519718.0000000003C09000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.359519718.0000000003C09000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000002.359519718.0000000003C09000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000002.359519718.0000000003C09000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000F.00000002.356792870.0000000002C01000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: WindowsUpdate.exe PID: 7120 Parent PID: 6976

General

Start time:	14:43:28
Start date:	28/10/2021
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Imagebase:	0x710000
File size:	774144 bytes
MD5 hash:	770F6E88B7BF3FE3AAE144A5AA41DC96
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000000.344193172.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000000.344193172.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000000.344193172.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000000.344193172.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000000.344193172.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000000.350144733.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000000.350144733.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000000.350144733.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000000.350144733.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000000.350144733.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000002.357544933.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000002.357544933.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000002.357544933.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000002.357544933.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000002.357544933.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000000.347313096.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000000.347313096.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000000.347313096.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000000.347313096.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000000.347313096.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000000.351819444.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000000.351819444.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000000.351819444.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000000.351819444.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000000.351819444.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: WindowsUpdate.exe PID: 4816 Parent PID: 3352

General

Start time:	14:43:33
Start date:	28/10/2021
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\WindowsUpdate.exe'
Imagebase:	0xc00000
File size:	774144 bytes
MD5 hash:	770F6E88B7BF3FE3AAE144A5AA41DC96
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000011.00000002.373074864.0000000003171000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000011.00000002.373941007.0000000004179000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000011.00000002.373941007.0000000004179000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000011.00000002.373941007.0000000004179000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000002.373941007.0000000004179000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000011.00000002.373941007.0000000004179000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: WindowsUpdate.exe PID: 3996 Parent PID: 4816

General

Start time:	14:43:39
Start date:	28/10/2021
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Imagebase:	0xdd0000
File size:	774144 bytes
MD5 hash:	770F6E88B7BF3FE3AAE144A5AA41DC96
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000000.391647562.000000000358E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000000.391647562.000000000358E000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000000.400119443.000000000359A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000000.400119443.000000000359A000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000012.00000002.439571003.0000000008640000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source:

00000012.00000000.401286482.00000000042D1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000000.401286482.00000000042D1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000012.00000000.368028200.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000000.368028200.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000000.368028200.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000000.368028200.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000000.368028200.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000012.00000000.395440509.0000000008660000.00000004.00020000.sdmp, Author: Arnim Rupp
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000012.00000000.395401347.0000000008640000.00000004.00020000.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000000.399998942.000000000358E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000000.399998942.000000000358E000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000012.00000000.389083600.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000000.389083600.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000000.389083600.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000000.389083600.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000000.389083600.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000000.392059792.00000000035EA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000002.436080566.00000000042D1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000002.436080566.00000000042D1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000002.435142271.000000000330F000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000002.435142271.000000000330F000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000012.00000000.408411000.0000000008640000.00000004.00020000.sdmp, Author: Arnim Rupp
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000012.00000000.370231808.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000000.370231808.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000000.370231808.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000000.370231808.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000000.370231808.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000012.00000000.369064581.0000000000402000.00000040.00000001.sdmp, Author:

Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000000.369064581.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000000.369064581.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000000.369064581.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000000.369064581.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000012.00000000.367380540.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000000.367380540.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000000.367380540.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000000.367380540.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000000.367380540.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000012.00000000.408464737.0000000008660000.00000004.00020000.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000000.391692528.000000000359A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000000.391692528.000000000359A000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000000.392382903.00000000042D1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000000.392382903.00000000042D1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000000.400644306.00000000035EA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000012.00000002.433632203.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000002.433632203.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000002.433632203.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000002.433632203.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000002.433632203.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000012.00000002.439615340.0000000008660000.00000004.00020000.sdmp, Author: Arnim Rupp
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000012.00000000.396224265.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000012.00000000.396224265.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000000.396224265.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000000.396224265.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000012.00000000.396224265.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000012.00000002.435207427.0000000003338000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

Analysis Process: vbc.exe PID: 6828 Parent PID: 3996

General

Start time:	14:43:53
Start date:	28/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000016.00000000.399740135.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000016.00000002.420264771.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000016.00000000.398239322.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000016.00000000.399210452.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 5076 Parent PID: 3996

General

Start time:	14:43:53
Start date:	28/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000017.00000000.402469174.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000017.00000002.404452957.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000017.00000000.402038118.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000017.00000000.401599576.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6008 Parent PID: 3996

General

Start time:	14:43:59
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3996 -s 2412
Imagebase:	0x20000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: WerFault.exe PID: 5028 Parent PID: 3996

General

Start time:	14:44:01
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3996 -s 2412
Imagebase:	0x20000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021