ID: 354163
Sample Name: Sample_B.exe
Cookbook: default.jbs
Time: 14:15:06
Date: 17/02/2021
Version: 31.0.0 Emerald

Table of Contents

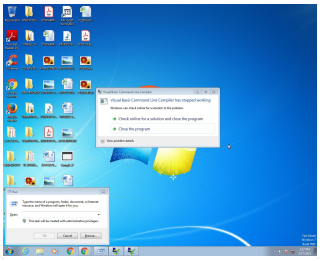
Analysis Report Sample_B.exe

Overview

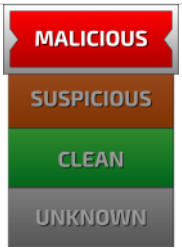
General Information

Sample Name:	Sample_B.exe
Analysis ID:	354163
MD5:	78300bd48d50fa7.
SHA1:	03157f27b0d5141.
SHA256:	424212e76c0e66..

Most interesting Screenshot:



Detection



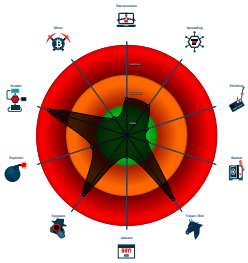
HawkEye
MailPassView

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected HawkEye Rat
- Found malware configuration
- Malicious sample detected (through …
- Yara detected AntiVM_3
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code contains potentia…
- .NET source code references suspic…
- Allocates memory in foreign process…
- Changes the view of files in windows…

Classification



Startup

- **System is w7x64**
- Sample_B.exe (PID: 2368 cmdline: 'C:\Users\user\Desktop\Sample_B.exe' MD5: 78300BD48D50FA7E5F3F6A933CC5F739)
  - Windows Update.exe (PID: 2360 cmdline: 'C:\Users\user\AppData\Roaming\Windows Update.exe' MD5: 78300BD48D50FA7E5F3F6A933CC5F739)
    - dw20.exe (PID: 2932 cmdline: dw20.exe -x -s 1708 MD5: FBA78261A16C65FA44145613E3669E6E)
    - vbc.exe (PID: 2852 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: 1672D0478049ABDAF0197BE64A7F867F)
    - vbc.exe (PID: 2816 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: 1672D0478049ABDAF0197BE64A7F867F)
- **cleanup**

Malware Configuration

Threatname: HawkEye


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


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Sample_B.exe	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x7423:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df

Source	Rule	Description	Author	Strings
Sample_B.exe	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7ba1d:$key: HawkEyeKeylogger • 0x7dd13:$salt: 099u787978786 • 0x7c09a:$string1: HawkEye_Keylogger • 0x7ceed:$string1: HawkEye_Keylogger • 0x7dc73:$string1: HawkEye_Keylogger • 0x7c483:$string2: holdermail.txt • 0x7c4a3:$string2: holdermail.txt • 0x7c3c5:$string3: wallet.dat • 0x7c3dd:$string3: wallet.dat • 0x7c3f3:$string3: wallet.dat • 0x7d837:$string4: Keylog Records • 0x7db4f:$string4: Keylog Records • 0x7dd6b:$string5: do not script --> • 0x7ba05:$string6: \pidloc.txt • 0x7ba93:$string7: BSPLIT • 0x7baa3:$string7: BSPLIT
Sample_B.exe	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Sample_B.exe	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Sample_B.exe	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 1 entries				

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x7423:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7ba1d:$key: HawkEyeKeylogger • 0x7dd13:$salt: 099u787978786 • 0x7c09a:$string1: HawkEye_Keylogger • 0x7ceed:$string1: HawkEye_Keylogger • 0x7dc73:$string1: HawkEye_Keylogger • 0x7c483:$string2: holdermail.txt • 0x7c4a3:$string2: holdermail.txt • 0x7c3c5:$string3: wallet.dat • 0x7c3dd:$string3: wallet.dat • 0x7c3f3:$string3: wallet.dat • 0x7d837:$string4: Keylog Records • 0x7db4f:$string4: Keylog Records • 0x7dd6b:$string5: do not script --> • 0x7ba05:$string6: \pidloc.txt • 0x7ba93:$string7: BSPLIT • 0x7baa3:$string7: BSPLIT
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 7 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.2112965167.00000000036 10000.00000004.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000002.00000002.2112485117.00000000033 71000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.2076206862.0000000000BC2000.00000020.00020000.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b81d:$key: HawkEyeKeylogger • 0x7db13:$salt: 099u787978786 • 0x7be9a:$string1: HawkEye_Keylogger • 0x7cced:$string1: HawkEye_Keylogger • 0x7da73:$string1: HawkEye_Keylogger • 0x7c283:$string2: holdermail.txt • 0x7c2a3:$string2: holdermail.txt • 0x7c1c5:$string3: wallet.dat • 0x7c1dd:$string3: wallet.dat • 0x7c1f3:$string3: wallet.dat • 0x7d637:$string4: Keylog Records • 0x7d94f:$string4: Keylog Records • 0x7db6b:$string5: do not script --> • 0x7b805:$string6: \pidloc.txt • 0x7b893:$string7: BSPLIT • 0x7b8a3:$string7: BSPLIT
00000000.00000002.2076206862.0000000000BC2000.00000020.00020000.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000000.00000002.2076206862.0000000000BC2000.00000020.00020000.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 34 entries				

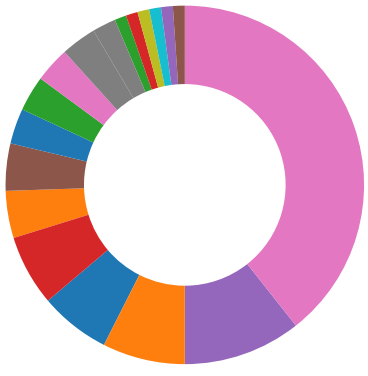
Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.Sample_B.exe.bc9c0d.1.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
0.2.Sample_B.exe.2577280.5.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
2.2.Windows Update.exe.46e0000.9.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
2.2.Windows Update.exe.46f0000.10.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
0.2.Sample_B.exe.c1fa72.2.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 104 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

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

Compliance:

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

Networking:

- May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

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

System Summary:

- Malicious sample detected (through community Yara rule)

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 AntiVM_3

HIPS / PFW / Operating System Protection Evasion:

- .NET source code references suspicious native API functions
- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- Sample uses process hollowing technique
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected HawkEye Keylogger
- Yara detected MailPassView

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

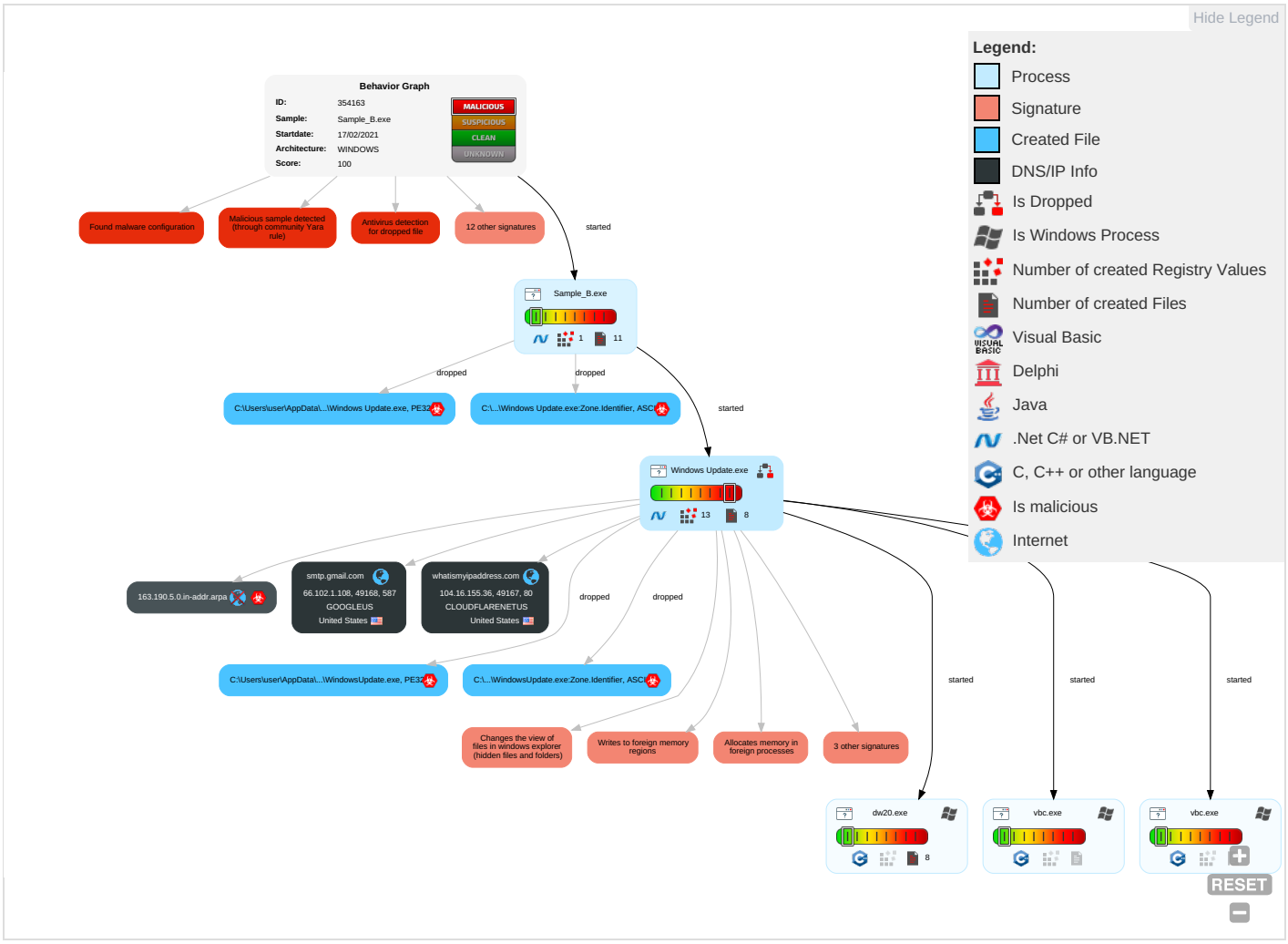
Detected HawkEye Rat

Yara detected HawkEye Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media 1	Windows Management Instrumentation 2 1	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 2 1	Peripheral Device Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 2
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 4 1 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 3 1	Security Account Manager	System Information Discovery 3	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Standard Port 1
Local Accounts	Command and Scripting Interpreter 2	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 4	Cached Domain Credentials	Virtualization/Sandbox Evasion 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1 2
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 4 1 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Configuration Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

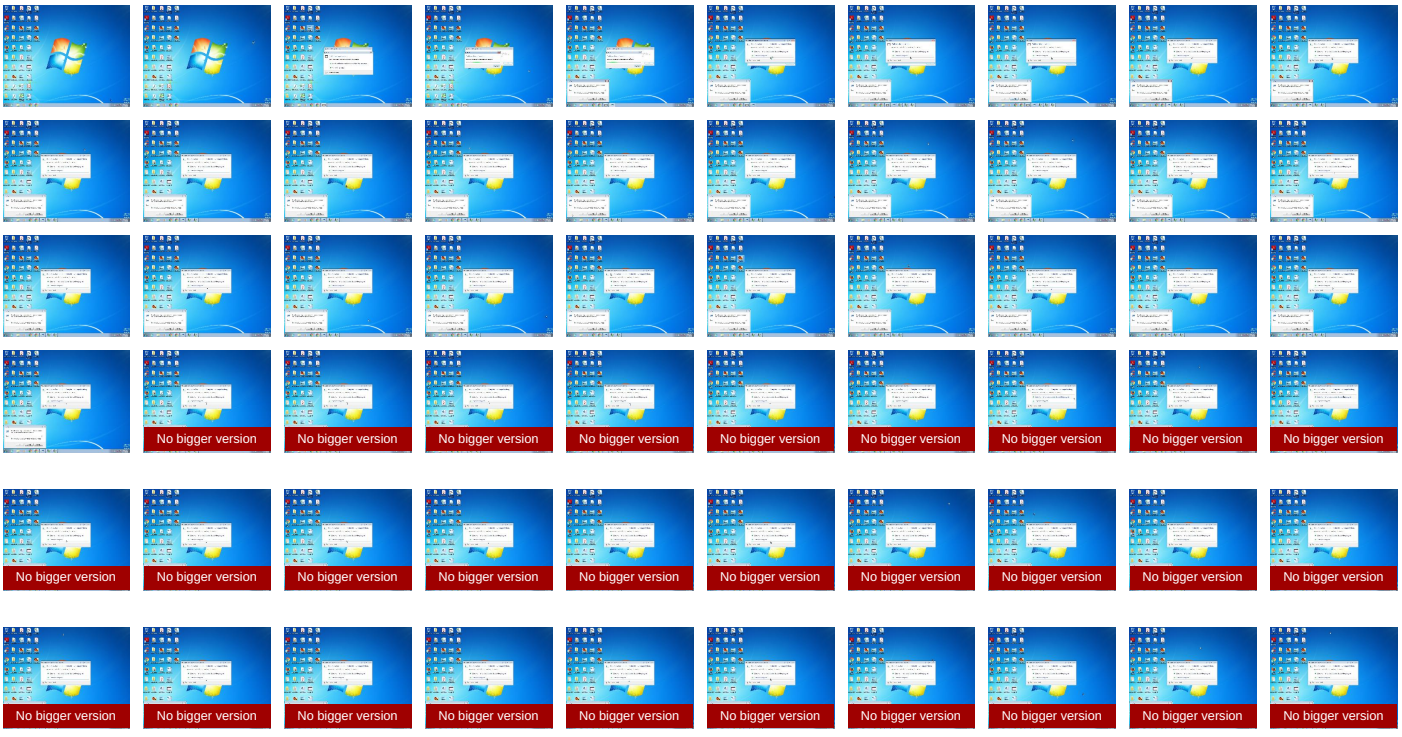
Behavior Graph

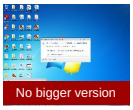


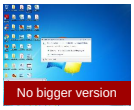
Screenshots

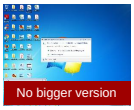
Thumbnails

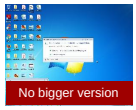
This section contains all screenshots as thumbnails, including those not shown in the slideshow.

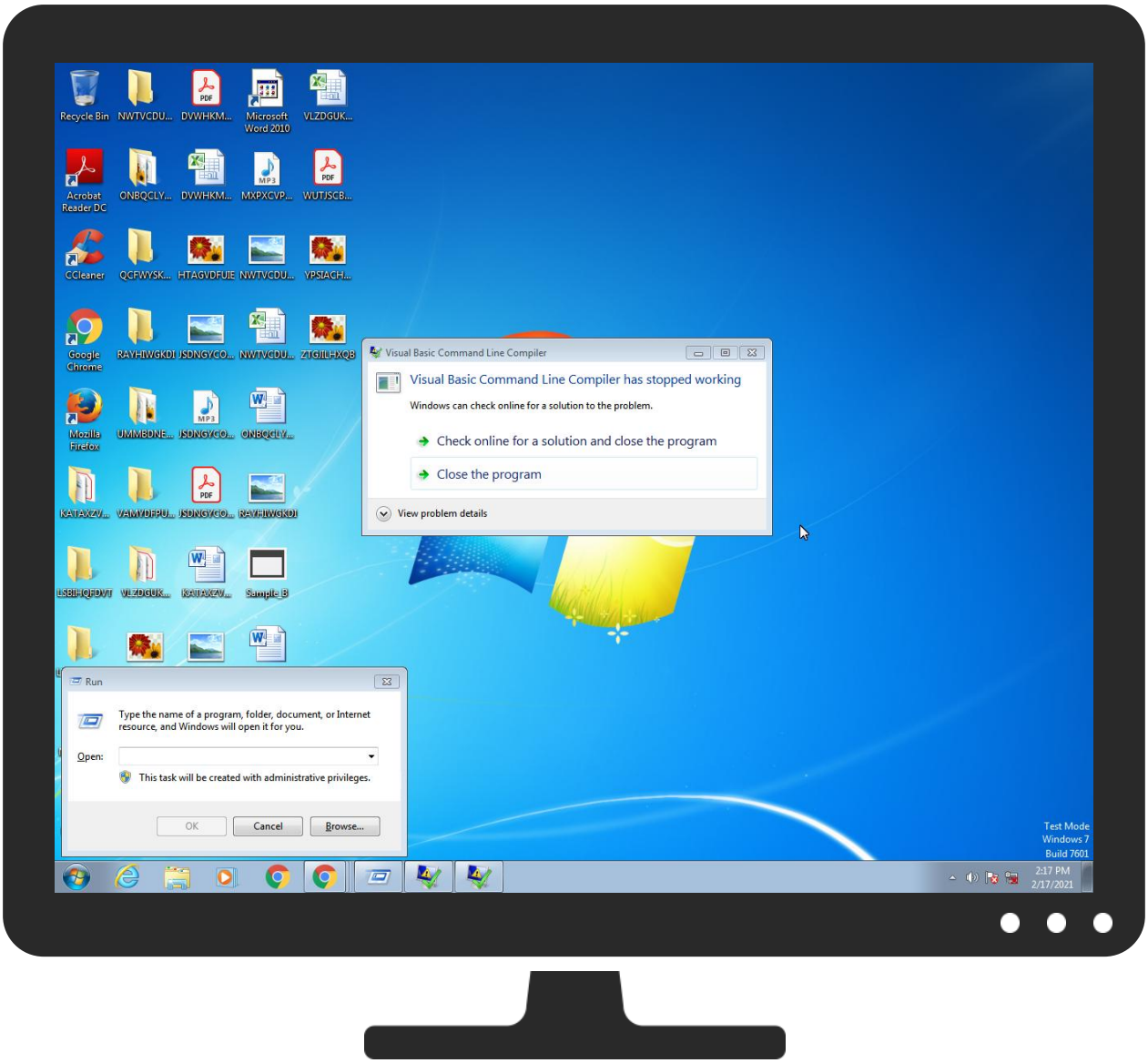












Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Sample_B.exe	100%	Avira	TR/AD.MExecute.lzrac	
Sample_B.exe	100%	Avira	SPR/Tool.MailPassView.473	
Sample_B.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Windows Update.exe	100%	Avira	TR/AD.MExecute.lzrac	
C:\Users\user\AppData\Roaming\Windows Update.exe	100%	Avira	SPR/Tool.MailPassView.473	
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Avira	TR/AD.MExecute.lzrac	
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Avira	SPR/Tool.MailPassView.473	
C:\Users\user\AppData\Roaming\Windows Update.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Sample_B.exe.bc0000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
0.0.Sample_B.exe.bc0000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
2.2.Windows Update.exe.ee0000.1.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
2.2.Windows Update.exe.ee0000.1.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.Sample_B.exe.bc0000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
0.2.Sample_B.exe.bc0000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
2.0.Windows Update.exe.ee0000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
2.0.Windows Update.exe.ee0000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Domains

Source	Detection	Scanner	Label	Link
cdn.digicertcdn.com	0%	Virustotal		Browse
163.190.5.0.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	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
cdn.digicertcdn.com	104.18.10.39	true	false	• 0%, Virustotal, Browse	unknown
smtp.gmail.com	66.102.1.108	true	false		high
163.190.5.0.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

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

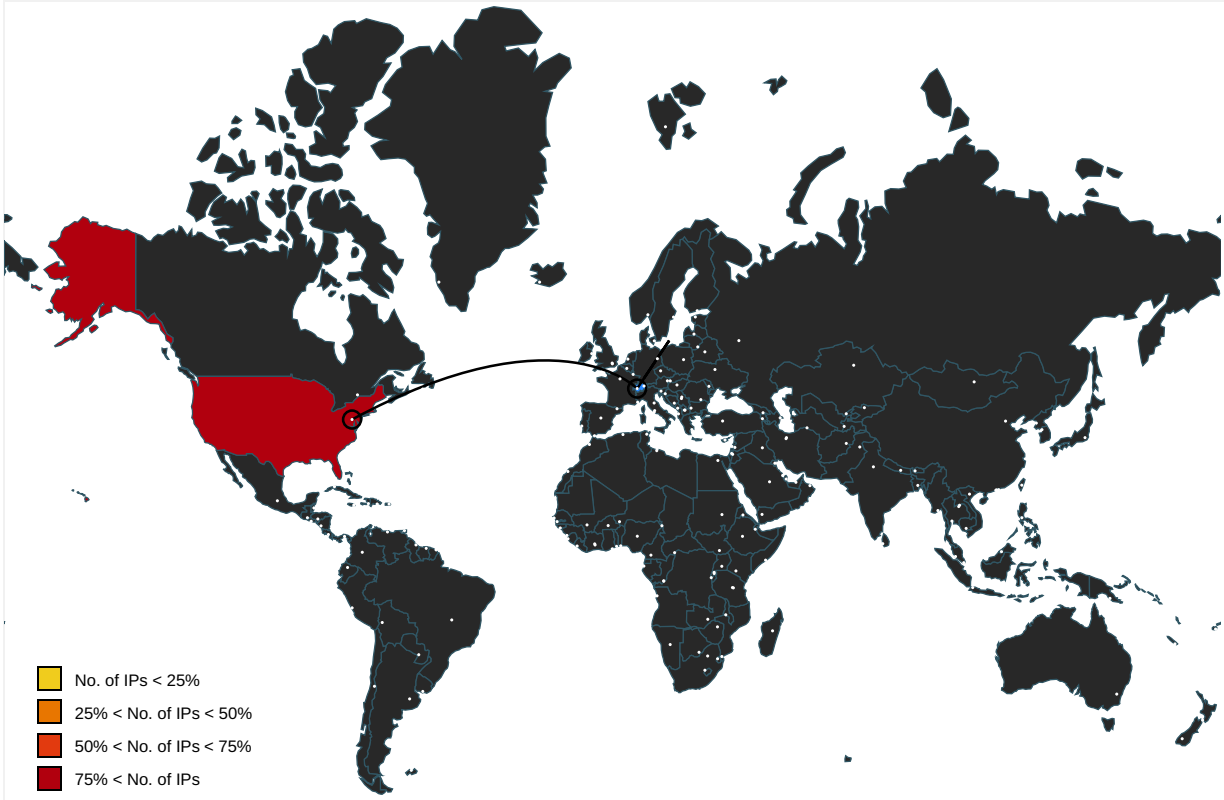
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	Windows Update.exe, 00000002.00000002.2122590766.0000000008DA0000.00000002.00000001.sdmp	false		high
http://investor.msn.com	Sample_B.exe, 00000000.00000002.2078022149.0000000005A30000.00000002.00000001.sdmp, Windows Update.exe, 00000002.00000002.2122590766.0000000008DA0000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	Sample_B.exe, 00000000.00000002.2078022149.0000000005A30000.00000002.00000001.sdmp, Windows Update.exe, 00000002.00000002.2122590766.0000000008DA0000.00000002.00000001.sdmp	false		high
http://crl.entrust.net/server1.crl0	Windows Update.exe, 00000002.00000002.2115217627.000000000548F000.00000004.00000001.sdmp	false		high
http://ocsp.entrust.net03	Windows Update.exe, 00000002.00000002.2115217627.000000000548F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	Windows Update.exe, 00000002.00000002.2115217627.000000000548F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	Windows Update.exe, 00000002.00000002.2111820758.0000000002371000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	Windows Update.exe, 00000002.00000002.2115217627.000000000548F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.pki.goog/gsr202	Windows Update.exe, 00000002.00000002.2115217627.000000000548F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	Sample_B.exe, 00000000.00000002.2078561268.0000000005C17000.00000002.00000001.sdmp, Windows Update.exe, 00000002.00000002.2122804139.0000000008F87000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	Sample_B.exe, 00000000.00000002.2078022149.0000000005A30000.00000002.00000001.sdmp, Windows Update.exe, 00000002.00000002.2122590766.0000000008DA0000.00000002.00000001.sdmp	false		high
http://https://pki.goog/repository/0	Windows Update.exe, 00000002.00000002.2115217627.000000000548F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	Sample_B.exe, 00000000.00000002.2078561268.0000000005C17000.00000002.00000001.sdmp, Windows Update.exe, 00000002.00000002.2122804139.0000000008F87000.00000002.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	Windows Update.exe, 00000002.00000002.2115217627.000000000548F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	Sample_B.exe, 00000000.00000002.2078561268.0000000005C17000.00000002.00000001.sdmp, Windows Update.exe, 00000002.00000002.2122804139.0000000008F87000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	Sample_B.exe, 00000000.00000002.2077174925.00000000049F0000.00000002.00000001.sdmp, Windows Update.exe, 00000002.00000002.2113827446.0000000004A30000.00000002.00000001.sdmp	false		high
http://ocsp.pki.goog/gts1o1core0	Windows Update.exe, 00000002.00000002.2111820758.0000000002371000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	Sample_B.exe, 00000000.00000002.2078022149.0000000005A30000.00000002.00000001.sdmp, Windows Update.exe, 00000002.00000002.2122590766.0000000008DA0000.00000002.00000001.sdmp	false		high
http://crl.pki.goog/GTS1O1core.crl0	Windows Update.exe, 00000002.00000002.2111820758.0000000002371000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://whatismyipaddress.com/-	Sample_B.exe	false		high
http://www.%s.comPA	Sample_B.exe, 00000000.00000002.2077174925.00000000049F0000.00000002.00000001.sdmp, Windows Update.exe, 00000002.00000002.2113827446.0000000004A30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://login.yahoo.com/config/login	Sample_B.exe, Windows Update.exe	false		high
http://www.site.com/logs.php	Windows Update.exe, 00000002.00000002.2111820758.0000000002371000.00000004.00000001.sdmp	false		high
http://crl.pki.goog/gsr2/gsr2.crl0?	Windows Update.exe, 00000002.00000002.2115217627.000000000548F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	Sample_B.exe	false		high
http://ocsp.entrust.net0D	Windows Update.exe, 00000002.00000002.2115241633.000000000054B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	Windows Update.exe, 00000002.00000002.2115217627.000000000548F000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.entrust.net/2048ca.crl0	Windows Update.exe, 00000002.0 0000002.2115241633.00000000054 B2000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.155.36	unknown	United States		13335	CLOUDFLARENETUS	false
66.102.1.108	unknown	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	354163
Start date:	17.02.2021
Start time:	14:15:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Sample_B.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@9/15@6/2
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 11.4% (good quality ratio 8.2%) • Quality average: 48.9% • Quality standard deviation: 36.4%
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 • Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.18.10.39, 2.20.142.210, 2.20.142.209 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, watson.microsoft.com, blobcollector.events.data.trafficmanager.net, cacerts.digicert.com, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:15:33	API Interceptor	24x Sleep call for process: Sample_B.exe modified
14:15:35	API Interceptor	137x Sleep call for process: Windows Update.exe modified
14:15:39	API Interceptor	85x Sleep call for process: dw20.exe modified
14:15:42	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
14:15:51	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.155.36	PO_Invoices_pdf.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Orders.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	nzGUqSK11D.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	hkaP5RPCGNDVq3Z.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NDt93WWQwd089H7.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	INQUIRY.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Prueba de pago.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	6JLHKYvboo.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	jSMd8npgmU.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	9vdouqRTh3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	5pB35gGfZ5.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	fyxC4Hgs3s.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	yk94P18VKp.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	oLHQIQAI3N.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
66.102.1.108	INQ4556 PO.exe	Get hash	malicious	Browse	
	ngx.exe	Get hash	malicious	Browse	
	CBT7797.exe	Get hash	malicious	Browse	
	SCTB 372PO.exe	Get hash	malicious	Browse	
	com.android.secrettalk-1.apk	Get hash	malicious	Browse	
	http://https://drive.google.com/uc?export=download&id=1QwhJnu-bYB73eWYRaGC_EuhkzqVSA20N	Get hash	malicious	Browse	
	http://https://drive.google.com/uc?export=download&id=1BZyO3k5sA4YaOJQDXxp2A3tfsIJBJP_-	Get hash	malicious	Browse	
	PAYMENT 25SW Aug-06-2018.doc	Get hash	malicious	Browse	
	PAYMENT 25SW Aug-06-2018.doc	Get hash	malicious	Browse	
	http://https://protected-documents.solutions/adobe/absa/token.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.digicertcdn.com	index_2021-02-17-11_45.dll	Get hash	malicious	Browse	• 104.18.10.39
	p4lqqCq2c2.exe	Get hash	malicious	Browse	• 104.18.10.39
	n26UEy3elW.exe	Get hash	malicious	Browse	• 104.18.11.39
	eAWqemQlnU.exe	Get hash	malicious	Browse	• 104.18.11.39
	fLPW6kLMgl.exe	Get hash	malicious	Browse	• 104.18.10.39
	a9YPGSem9V.exe	Get hash	malicious	Browse	• 104.18.10.39
	SecuriteInfo.com.Exploit.Siggen3.10048.3748.xls	Get hash	malicious	Browse	• 104.18.10.39
	RFQ.xls	Get hash	malicious	Browse	• 104.18.10.39
	SoftickAudioGatewayInstaller	Get hash	malicious	Browse	• 104.18.11.39
	StrikeSolitaire3	Get hash	malicious	Browse	• 104.18.10.39
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	• 104.18.10.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	• 104.18.10.39
	Farie PO.doc	Get hash	malicious	Browse	• 104.18.11.39
	Cerere de pret NUM003112 09-02-2021.doc	Get hash	malicious	Browse	• 104.18.10.39
	usd2.dll	Get hash	malicious	Browse	• 104.18.10.39
	PeerReviewResults.xls	Get hash	malicious	Browse	• 104.18.10.39
	Walaa-Qasem-resume2.doc	Get hash	malicious	Browse	• 104.18.10.39
	MY CV.doc	Get hash	malicious	Browse	• 104.18.10.39
	INV8222874744_20210111490395.xlsm	Get hash	malicious	Browse	• 104.18.10.39
	Inv0209966048-20210111075675.xls	Get hash	malicious	Browse	• 104.18.11.39
smtp.gmail.com	SecuriteInfo.com.BehavesLike.Win32.Generic.jc.exe	Get hash	malicious	Browse	• 74.125.206.109
	SPECIFICATION.exe	Get hash	malicious	Browse	• 74.125.206.108
	Ransomware Tortoise.exe	Get hash	malicious	Browse	• 172.253.120.109
	Purchase_26012021_003429.exe	Get hash	malicious	Browse	• 173.194.79.109
	Overdue_invoices.exe	Get hash	malicious	Browse	• 108.177.119.109
	SIT-10295.exe	Get hash	malicious	Browse	• 108.177.119.109
	QT21006189.exe	Get hash	malicious	Browse	• 108.177.119.109
	fusion.exe	Get hash	malicious	Browse	• 173.194.69.108
	Revised Invoice.exe	Get hash	malicious	Browse	• 173.194.69.109
	transcach.exe	Get hash	malicious	Browse	• 172.253.120.109
	PCS.exe	Get hash	malicious	Browse	• 172.253.120.109
	transcach.exe	Get hash	malicious	Browse	• 172.253.120.109
	ORDER-02044.exe	Get hash	malicious	Browse	• 66.102.1.109
	EA0Y2020 Outstanding invoice 20190510to 20201214.exe	Get hash	malicious	Browse	• 173.194.69.109
	vygtHoQaI1KaBVp.exe	Get hash	malicious	Browse	• 173.194.69.108
	QCXw2WXDjOalhVZ.exe	Get hash	malicious	Browse	• 108.177.119.109
	yqd2LHZ8y57Bzy4.exe	Get hash	malicious	Browse	• 108.177.119.109
	knitted yarn documents.exe	Get hash	malicious	Browse	• 172.253.120.109
	a9bdc406f87d6072599939a86b766fa4.exe	Get hash	malicious	Browse	• 172.253.120.109
	SecuriteInfo.com.Generic.mg.e1df690a980825ac.exe	Get hash	malicious	Browse	• 173.194.69.108
whatismyipaddress.com	PO_Invoices_pdf.exe	Get hash	malicious	Browse	• 104.16.155.36
	Orders.exe	Get hash	malicious	Browse	• 104.16.155.36
	nzGUqSK11D.exe	Get hash	malicious	Browse	• 104.16.154.36
	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• 104.16.155.36
	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• 104.16.155.36
	hkaP5RPCGNDVq3Z.exe	Get hash	malicious	Browse	• 104.16.155.36
	B6LNCKjOGt5EmFQ.exe	Get hash	malicious	Browse	• 104.16.154.36
	NDt93WWQwd089H7.exe	Get hash	malicious	Browse	• 104.16.155.36
	JkhR5oeRHA.exe	Get hash	malicious	Browse	• 66.171.248.178
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 104.16.155.36
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• 104.16.154.36
	INQUIRY.exe	Get hash	malicious	Browse	• 104.16.154.36
	Prueba de pago.exe	Get hash	malicious	Browse	• 104.16.155.36
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	http://https://my-alliances.co.uk/	Get hash	malicious	Browse	• 66.171.248.178
	c9o0CtTIYT.exe	Get hash	malicious	Browse	• 104.16.154.36
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• 104.16.155.36

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	SecuriteInfo.com.Trojan.Inject4.6572.30773.exe	Get hash	malicious	Browse	• 172.67.188.154
	index_2021-02-17-11_45.dll	Get hash	malicious	Browse	• 104.20.185.68

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	index_2021-02-17-11_45.dll	Get hash	malicious	Browse	• 104.20.184.68
	index_2021-02-17-11_45.dll	Get hash	malicious	Browse	• 104.20.184.68
	f_0008a8.exe	Get hash	malicious	Browse	• 104.16.18.94
	RibermoldOrder 180827.exe	Get hash	malicious	Browse	• 172.67.188.154
	index_2021-02-17-11_45.dll	Get hash	malicious	Browse	• 104.20.185.68
	f6TW7Ob4aY.dll	Get hash	malicious	Browse	• 104.20.185.68
	ew2c3sE5Po.dll	Get hash	malicious	Browse	• 104.20.185.68
	TPYY2n7hzn.dll	Get hash	malicious	Browse	• 104.20.185.68
	ZXKG6rCJwg.dll	Get hash	malicious	Browse	• 104.20.185.68
	YWOro8qqYg.dll	Get hash	malicious	Browse	• 104.20.185.68
	cRoVRprbi1.dll	Get hash	malicious	Browse	• 104.20.185.68
	45tj9pDUII.dll	Get hash	malicious	Browse	• 104.20.185.68
	3I3ECIc9us.dll	Get hash	malicious	Browse	• 104.20.185.68
	VifzEYDt4f.dll	Get hash	malicious	Browse	• 104.20.184.68
	aMvqQZ69tk.dll	Get hash	malicious	Browse	• 104.20.184.68
	BpV9PHuNll.dll	Get hash	malicious	Browse	• 104.20.184.68
	dxjcxlYNoQ.dll	Get hash	malicious	Browse	• 104.20.185.68
	wildix-collaboration-mobile.apk	Get hash	malicious	Browse	• 104.22.10.83
GOOGLEUS	f_0008a8.exe	Get hash	malicious	Browse	• 8.8.4.4
	wildix-collaboration-mobile.apk	Get hash	malicious	Browse	• 142.250.180.131
	mWxzYlRCUi.exe	Get hash	malicious	Browse	• 34.102.136.180
	wildix-collaboration-mobile.apk	Get hash	malicious	Browse	• 142.250.184.42
	Credit Card & Booking details.exe	Get hash	malicious	Browse	• 34.102.136.180
	DnHeI10lQ6.exe	Get hash	malicious	Browse	• 34.102.136.180
	q9xB9DE3RA.exe	Get hash	malicious	Browse	• 34.102.136.180
	Cargo_remitP170201.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	OEVGVSOGAH.dll	Get hash	malicious	Browse	• 216.58.206.65
	LeaveHomeSafe_1.1.4_#U5b89#U5fc3#U72483.apk	Get hash	malicious	Browse	• 142.250.184.42
	plutonium.exe	Get hash	malicious	Browse	• 8.8.8.8
	Quotation.exe	Get hash	malicious	Browse	• 34.102.136.180
	sBt_8xKw.apk	Get hash	malicious	Browse	• 216.58.198.42
	cLMBOaIYSO.exe	Get hash	malicious	Browse	• 35.228.43.35
	51BfqRtUI9.exe	Get hash	malicious	Browse	• 34.102.136.180
	X2Q8MaK1Zm.docx	Get hash	malicious	Browse	• 216.58.208.131
	X2Q8MaK1Zm.docx	Get hash	malicious	Browse	• 172.253.120.155
	dAlyRK9gO7.exe	Get hash	malicious	Browse	• 8.8.8.8
	SU9Gm5Pom3.exe	Get hash	malicious	Browse	• 34.105.243.4
	9j4sD6PmsW.exe	Get hash	malicious	Browse	• 34.102.136.180

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\3C428B1A3E5F57D887EC4B864FAC5DCC	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	data
Category:	dropped
Size (bytes):	914
Entropy (8bit):	7.367371959019618
Encrypted:	false
SSDEEP:	24:c0oGlGm7qGlGd7SK1tcudP5M/C0VQYyL4R3fum:+JnJ17tcudRMq6QsF
MD5:	E4A68AC854AC5242460AFD72481B2A44
SHA1:	DF3C24F9BFD666761B268073FE06D1CC8D4F82A4
SHA-256:	CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\3C428B1A3E5F57D887EC4B864FAC5DCC	
SHA-512:	5622207E1BA285F172756F6019AF92AC808ED63286E24DFECC1E79873FB5D140F1CEB7133F2476E89A5F75F711F9813A9FBB8FD5287F64ADFDCC53B864F9BDC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0...0..v.....:.....(d.....0...*.H.....0a1.0...U....US1.0...U....DigiCert Inc1.0...U....www.digicert.com1 0...U....DigiCert Global Root G20...130801120000Z..380115120000Z0a1.0...U....US1.0...U....DigiCert Inc1.0...U....www.digicert.com1 0...U....DigiCert Global Root G20.."0...*.H.....0.....7.4.{k.h..Ju.F.!.....T.....:..<z...k.-.^.$D.b.~..~.Tu ..P..c.l0.....7...CN.{,.../.:...%.k.`.`.O!I..g..a.....2k..W.].....I.5-..Im.w..IK..U.....#.LmE.....0..LU.'JW.|...s...J...P.....!.....g(.s..=Fv...!4M..E..I.....3.).....B0@0...U.....0....0...U.....0...U.....N"T ....n.....90...*.H.....`g(.o.Hc.1..g..}<.J...+..._sw*2.9.gB.#.Eg5....a.4.. L....5.v..B..D...6t$Z.I..Y5..I....G*=./.\... ._SF..h...0.>1.....>5.._..pPpGA.W.N...../.%.u...o..Aq..*.O. U...E..D..2...SF.,...".K..E....X..}R..YC....&.o....7}.....w_v.<..]V[..fn.57.2.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.l6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....l.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\3C428B1A3E5F57D887EC4B864FAC5DCC	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0734220895273965
Encrypted:	false
SSDEEP:	6:kKbgP4LDKVIbjcalgRAOAUSW0zeEpV1Ew1OXISMlcV/:EQLutWOxSW0zeYrsMlU/
MD5:	DEFF45D6EE453F2E606204F981D12C2A
SHA1:	37196590CCAB4D0DA1ECF8A2C7CD5D3B9057DF9E
SHA-256:	E9D137AC1323596442F223D79DE22A4A34980B7BC84BD51EA5B7EDD07A2994E2
SHA-512:	4F18E2CAA196C0C6910B28C0F74BCDF1ADC35DB1395CA7F3C7F00925EB9454FF76F729E17916B57F845CD06FC49CD25D24F32E57346972DE36BBC9C455DDD83
Malicious:	false
Reputation:	low
Preview:	p..... ....j...5..nz...(..... .....n...u.....h.t.t.p.:././.c.a.c.e.r.t.s...d.i.g.i.c.e.r.t...c.o.m./.D.i.g.i.C.e.r.t.G.l.o.b.a.l.R.o.o.t.G.2...c.r.t..."..5.a.2.8.6.4.1.7.-.3.9.2."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.080958610796429
Encrypted:	false
SSDEEP:	6:kKPbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:+3kPlE99SNxAhUeo+aKt
MD5:	5DE2DFA843897E36DAC2D1F4FCB7F360
SHA1:	717349376361E7175072835A0051A855DBF32BC8
SHA-256:	EB01F1C833C14A267597922655659DE490CBF8548F7C46B305C44896A2E8886C
SHA-512:	F463646650855F0493117ACC769D77DA705C69F7F1880AED8A17689223F5F2839C6340668A9222DCC884C98E64D32EC40C85E356CC62964D3BA77B5DFA6D809D
Malicious:	false
Reputation:	low
Preview:	p..... .....|Lnz...(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\WER\ReportArchive\AppCrash_windows update.e_8def7a6b85a0513a7da3debaf0f7a2c3a14caff_0b1db1a4\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	data
Category:	modified
Size (bytes):	13186
Entropy (8bit):	3.716046470811688
Encrypted:	false
SSDEEP:	192:oTyzzRiyXg9uclA90TfxtdOZC0fFj6IGbQA3ai63yOt7:lzRi4yTOhGmr
MD5:	EF7C318F45EBB3503516CC69659E9F7B
SHA1:	D414EF598B7B337B1132FB28DD4B80C43D479E06
SHA-256:	A74CC73AED01F82B779695EF91898E57CA039EAEF67747838793658E5FFC3AB4
SHA-512:	ED4B52B026CDB3276F93C8349CDEF77F5DCC21D1C6D521D4402C5B29398A6DA748B9836BA74FE0D23F6892FE4882E3A6FD424BBEFEE71582822A0BFEC49B44B
Malicious:	false
Reputation:	low
Preview:	V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.0.7.3.7.3.9.2.8.1.8.3.8.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.8.0.7.3.7.4.0.8.3.7.0.4.3.0.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.a.0.7.6.8.f.3.-.7.1.6.d.-.1.1.e.b.-.a.d.c.f.-.e.c.f.4.b.b.b.5.9.1.5.b.....W.O.W.6.4.=.1.....R.e.s.p.o.n.s.e...B.u.c.k.e.t.I.d.=.4.9.8.8.7.0.9.8.9.....R.e.s.p.o.n.s.e...B.u.c.k.e.t.T.a.b.l.e.=.5.1.2.1.7.6.3.3.1.....R.e.s.p.o.n.s.e...t.y.p.e.=.4.....S.i.g.[.0.]...N.a.m.e.=.P.r.o.b.l.e.m. .S.i.g.n.a.t.u.r.e. .0.1.....S.i.g.[.0.]...V.a.l.u.e.=.w.i.n.d.o.w.s. .u.p.d.a.t.e...e.x.e.....S.i.g.[.1.]...N.a.m.e.=.P.r.o.b.l.e.m. .S.i.g.n.a.t.u.r.e. .0.2.....S.i.g.[.1.]...V.a.l.u.e.=.1...0...0...0.....S.i.g.[.2.]...N.a.m.e.=.P.r.o.b.l.e.m. .S.i.g.n.a.t.u.r.e. .0.3.....S.i.g.[.2.]...V.a.l.u.e.=.6.0.1.6.c.1.0.9.....S.i.g.[.3.]...N.a.m.e.=.P.r.o.b.l.e.m. .S.i.g.n.a.t.u.r.e. .0.4.....S.i.g.[.3.]...V.a.l.u.e.=.P.h.u.l.l.i.....S.i.g.[.4.]...

C:\Users\user\AppData\Local\Temp\CabAB00.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\Local\Temp\SysInfo.txt	
Process:	C:\Users\user\Desktop\Sample_B.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	35
Entropy (8bit):	4.226150431961057
Encrypted:	false
SSDEEP:	3:oNSzORW2EM:oNSzOA2v
MD5:	6A5A5B0A44E4EB0E35D0ED1ED597CB58
SHA1:	1EAE2A59836272E8B62BD8AF9F231E5FF23BC8AB
SHA-256:	A4DB033255E7CEDD4E48A95805F033DD9A3A1AF789440EB627878C1C944C7483
SHA-512:	F21D968FE9400557E881BA3C354073659AA68E0B30D4485D519887ACF62A699730CE59B701D9245056D629C0D25C7F117E64A313B7CE37B6C6737FD9BD6E655F
Malicious:	false
Reputation:	low
Preview:	C:\Users\user\Desktop\Sample_B.exe

C:\Users\user\AppData\Local\Temp\TarAB01.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false

C:\Users\user\AppData\Local\Temp\TarAB01.tmp	
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....R19%..210115004237Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00.+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\WERA42C.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	2626
Entropy (8bit):	3.657382504384408
Encrypted:	false
SSDEEP:	48:yeRipPp6uhzrkG/wU6Gww7VxpAFgYkbkiQG5zepMVOfyi+Sqw+PjsMS+MbPx2xSQ:Shz4tU6o7VxBt33tJ3uE3
MD5:	BB7B91CA690F827AF3B229CB8B174191
SHA1:	6749797C84D4B0B279BD6C887B07CB16ECD9D156
SHA-256:	A7DD4AC1387116D03AC3C70E3074DCAB3E3B8EB864E2304195F86F1B81923575
SHA-512:	ADA582C7A441E85028A09DB2DD2C092D0AD67A0CC69BAE00BAD0ED3A2188DC88A1CCBAC6822AE9BA558CE2B7DAEA7C4666AF907EA2BF2AB7AD0A2B55E1820176
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.6...1.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.7.6.0.1. .S.e.r.v.i.c.e. .P.a.c.k. .1.</./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .7. .P.r.o.f.e.s.s.i.o.n.a.l.</./.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.>.7.6.0.1...2.3.6.7.7...a.m.d.6.4.f.r.e...w.i.n.7.s.p.1._.l.d.r...1.7.0.2.0.9.-.0.6.0.0.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.3.0.<./.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.b.l.e.m.S.i.g.n.a.t.u.

C:\Users\user\AppData\Roaming\Windows Update.exe	
Process:	C:\Users\user\Desktop\Sample_B.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	533504
Entropy (8bit):	6.5061470317531676
Encrypted:	false
SSDEEP:	6144:1ulqe1RKbS/QTjhUqBfxrwEnuNcSsm7IoYGW0VvBXCAt6kihwE+VDpJYWmlwnx9e:MRKQtqB5urTIoYWBQk1E+VF9mOx9Oi
MD5:	78300BD48D50FA7E5F3F6A933CC5F739
SHA1:	03157F27B0D5141465ADEEAF9B3A7B5F3E60F614
SHA-256:	424212E76C0E660538EE49126079980B34F4DD343E002004F67EA71A937AF5E3
SHA-512:	18B015CA0B4DE297195E97BA95872C1485FE55A1D89B7FBDD82769A912E0FBB3825975105E5712356FFED525516D7EF3F482F46CE873E9B4315956F2E2A491E7
Malicious:	**true**
Yara Hits:	• Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....4..... .....@.. ..... ..@.....W.... ...2.....`..... .....H.....text..... ....`.rsrc....2... ...2.....@..@.reloc.....` .....".....@..B.....H.....0}..d.....X.....2s.....*....0.....~.....(.....~....o....~....o.....9.....~....o.....+G~.....o.....o.....). .....~.....~.....o....o.....1.~.....~....o.....o.....~....~....o....o.....~.....(....s....o.....(.....*.....0.. .....(....(.....(....o.....*.....(.....(.....o... ....o.....o.....o.....*.R..(....o....o.....

C:\Users\user\AppData\Roaming\Windows Update.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Sample_B.exe
File Type:	ASCII text, with CRLF line terminators

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

C:\Users\user\AppData\Roaming\WindowsUpdate.exe	
Process:	C:\Users\user\AppData\Roaming\Windows Update.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	533504
Entropy (8bit):	6.5061470317531676
Encrypted:	false
SSDEEP:	6144:1ulqe1RKbS/QTjhUqBfxrwEnuNcSsm7IoYGW0VvBXCAt6kihwE+VDpJYWmlwnx9e:MRKQtqB5urTIoYWBQk1E+VF9mOx9Oi
MD5:	78300BD48D50FA7E5F3F6A933CC5F739
SHA1:	03157F27B0D5141465ADEEAF9B3A7B5F3E60F614
SHA-256:	424212E76C0E660538EE49126079980B34F4DD343E002004F67EA71A937AF5E3
SHA-512:	18B015CA0B4DE297195E97BA95872C1485FE55A1D89B7FBDD82769A912E0FBB3825975105E5712356FFED525516D7EF3F482F46CE873E9B4315956F2E2A491E7
Malicious:	**true**
Yara Hits:	• Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....4..... .....@.. ..... ..@.....W.... ...2.....`..... ....H.....text..... ....`.rsrc....2... ...2.....@..@.reloc.....` .....".....@..B.....H.....0}..d.....X.....2s.....*....0.....~.....(.....~....o....~....o.....9.....~....o.....+G~.....o.....o.....,). .....,.~.....~.....o....o.....1.~.....~....o.....o.....~....~....o....o.....~.....(....s....o.....(.....*.....0.. .....(....(.....(....o.....*.....(.....(.....o... ....o.....o.....o.....*.R..(....o....o.....

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

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\AppData\Roaming\Windows Update.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false

C:\Users\user\AppData\Roaming\pid.txt	
SSDEEP:	3:8:8
MD5:	4EBD440D99504722D80DE606EA8507DA
SHA1:	53127AFA9428C4B39465D8FAFFEA4891967FDD3D
SHA-256:	BA977EDD7884F62CD595D30DC746605253AC8E5700B135AD515AAC7ADAFA512C
SHA-512:	8F474385AB39E7D6E2A314C91E0452F23BFE19F4E79739D8DAA8E6B1187AB289562EBA6795834CA4744C6EF000CEBA41D0448DADFA233AE332BA89EF03E2B9E3
Malicious:	false
Preview:	2360

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\AppData\Roaming\Windows Update.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	49
Entropy (8bit):	4.505229681327448
Encrypted:	false
SSDEEP:	3:oNXp4EaKC59KYr4a:oNPaZ534a
MD5:	08300E5B4297843953DCBA97B84FC23F
SHA1:	0B3D9411DED86F59DAF4BD11A563357DE2BDFB1E
SHA-256:	6903CCA5237DD33175367A846A971979FF15CC5823135182E00A57F69A856C9A
SHA-512:	8C9124CC2258559A2377EB95EC9EB400EE568A133F946FDF7F69BB42A081DA90DFC7F2C544FBDD01AF6A4C235CAF654A0044ACE00835F91FCCDDDAF5F7F579E9
Malicious:	false
Preview:	C:\Users\user\AppData\Roaming\Windows Update.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.5061470317531676
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.69% • Win32 Executable (generic) a (10002005/4) 49.65% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • InstallShield setup (43055/19) 0.21% • Windows Screen Saver (13104/52) 0.07%
File name:	Sample_B.exe
File size:	533504
MD5:	78300bd48d50fa7e5f3f6a933cc5f739
SHA1:	03157f27b0d5141465adeeaf9b3a7b5f3e60f614
SHA256:	424212e76c0e660538ee49126079980b34f4dd343e002004f67ea71a937af5e3
SHA512:	18b015ca0b4de297195e97ba95872c1485fe55a1d89b7fbdd82769a912e0fbb3825975105e5712356ffed525516d7ef3f482f46ce873e9b4315956f2e2a491e7
SSDEEP:	6144:1ulqe1RKbS/QTjhUqBfxrwEnuNcSsm7IoYGW0VvBXCAt6kihwE+VDpJYWmlwnx9e:MRKQtqB5urTIoYWBQk1E+VF9mOx9Oi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....4..... .....@.. .....@.....

File Icon

Icon Hash:	41455554545445a2

Static PE Info

General

Entrypoint:	0x480dee
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:	0x6016C109 [Sun Jan 31 14:39:05 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x80d94	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x82000	0x3200	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x86000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7edf4	0x7ee00	False	0.572546567118	data	6.53992282183	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x3200	0x3200	False	0.105390625	data	3.5876692887	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x86000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x824f0	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2004318071, next used block 4286019447		
RT_ICON	0x827d8	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x82900	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x831a8	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x83710	0x353	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x83a68	0x10a8	data		
RT_ICON	0x84b10	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x84f78	0x68	data		
RT_VERSION	0x82250	0x2a0	data		
RT_MANIFEST	0x84fe0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

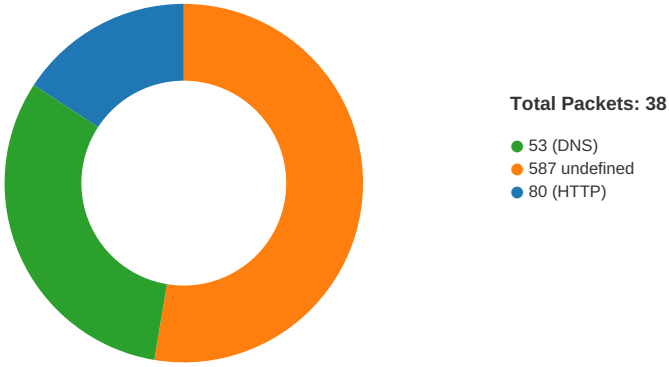
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014
Assembly Version	1.0.0.0
InternalName	Phulli.exe
FileVersion	1.0.0.0
ProductName	Phulli
ProductVersion	1.0.0.0
FileDescription	Phulli
OriginalFilename	Phulli.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/17/21-14:15:57.240377	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	104.16.155.36	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 17, 2021 14:15:57.146359921 CET	49167	80	192.168.2.22	104.16.155.36
Feb 17, 2021 14:15:57.187491894 CET	80	49167	104.16.155.36	192.168.2.22
Feb 17, 2021 14:15:57.187669992 CET	49167	80	192.168.2.22	104.16.155.36
Feb 17, 2021 14:15:57.188503981 CET	49167	80	192.168.2.22	104.16.155.36
Feb 17, 2021 14:15:57.229413033 CET	80	49167	104.16.155.36	192.168.2.22
Feb 17, 2021 14:15:57.240376949 CET	80	49167	104.16.155.36	192.168.2.22
Feb 17, 2021 14:15:57.445694923 CET	49167	80	192.168.2.22	104.16.155.36
Feb 17, 2021 14:15:58.263657093 CET	49167	80	192.168.2.22	104.16.155.36
Feb 17, 2021 14:15:58.304943085 CET	80	49167	104.16.155.36	192.168.2.22
Feb 17, 2021 14:15:58.305743933 CET	49167	80	192.168.2.22	104.16.155.36
Feb 17, 2021 14:15:58.591355085 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:15:58.643999100 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:15:58.644090891 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:15:58.753774881 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:15:58.768049955 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:15:58.820581913 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:15:58.823973894 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:15:58.825731993 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:15:58.878711939 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:15:58.978893995 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:15:59.032215118 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:15:59.032260895 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:15:59.032417059 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:15:59.050864935 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:15:59.103605032 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:15:59.300400972 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:15:59.548762083 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:15:59.601639032 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:15:59.603857994 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:15:59.656851053 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:15:59.658803940 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:15:59.716787100 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:15:59.991312027 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:15:59.991817951 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:16:00.044337034 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:16:00.044538975 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:16:00.044905901 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:16:00.097799063 CET	587	49168	66.102.1.108	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 17, 2021 14:16:00.099353075 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:16:00.157800913 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:16:00.401359081 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:16:00.404243946 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:16:00.404728889 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:16:00.405162096 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:16:00.405478001 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:16:00.457525969 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:16:00.457547903 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:16:00.457556963 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:16:00.457802057 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:16:00.896564007 CET	587	49168	66.102.1.108	192.168.2.22
Feb 17, 2021 14:16:01.110186100 CET	49168	587	192.168.2.22	66.102.1.108
Feb 17, 2021 14:16:17.157942057 CET	49168	587	192.168.2.22	66.102.1.108

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 17, 2021 14:15:56.602780104 CET	52197	53	192.168.2.22	8.8.8.8
Feb 17, 2021 14:15:56.659929991 CET	53	52197	8.8.8.8	192.168.2.22
Feb 17, 2021 14:15:57.036444902 CET	53099	53	192.168.2.22	8.8.8.8
Feb 17, 2021 14:15:57.088181019 CET	53	53099	8.8.8.8	192.168.2.22
Feb 17, 2021 14:15:58.301774025 CET	52838	53	192.168.2.22	8.8.8.8
Feb 17, 2021 14:15:58.366976023 CET	53	52838	8.8.8.8	192.168.2.22
Feb 17, 2021 14:15:58.371413946 CET	52838	53	192.168.2.22	8.8.8.8
Feb 17, 2021 14:15:58.437342882 CET	53	52838	8.8.8.8	192.168.2.22
Feb 17, 2021 14:15:58.455055952 CET	52838	53	192.168.2.22	8.8.8.8
Feb 17, 2021 14:15:58.511831045 CET	53	52838	8.8.8.8	192.168.2.22
Feb 17, 2021 14:15:58.518007994 CET	52838	53	192.168.2.22	8.8.8.8
Feb 17, 2021 14:15:58.580215931 CET	53	52838	8.8.8.8	192.168.2.22
Feb 17, 2021 14:16:00.139292002 CET	61200	53	192.168.2.22	8.8.8.8
Feb 17, 2021 14:16:00.199146986 CET	53	61200	8.8.8.8	192.168.2.22
Feb 17, 2021 14:16:00.212182999 CET	49548	53	192.168.2.22	8.8.8.8
Feb 17, 2021 14:16:00.263868093 CET	53	49548	8.8.8.8	192.168.2.22
Feb 17, 2021 14:16:01.086823940 CET	55627	53	192.168.2.22	8.8.8.8
Feb 17, 2021 14:16:01.135674953 CET	53	55627	8.8.8.8	192.168.2.22
Feb 17, 2021 14:16:01.143835068 CET	56009	53	192.168.2.22	8.8.8.8
Feb 17, 2021 14:16:01.195561886 CET	53	56009	8.8.8.8	192.168.2.22
Feb 17, 2021 14:16:01.475300074 CET	61865	53	192.168.2.22	8.8.8.8
Feb 17, 2021 14:16:01.542368889 CET	53	61865	8.8.8.8	192.168.2.22
Feb 17, 2021 14:16:01.552608967 CET	55171	53	192.168.2.22	8.8.8.8
Feb 17, 2021 14:16:01.611363888 CET	53	55171	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 17, 2021 14:15:56.602780104 CET	192.168.2.22	8.8.8.8	0x26ae	Standard query (0)	163.190.5.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Feb 17, 2021 14:15:57.036444902 CET	192.168.2.22	8.8.8.8	0x80ac	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Feb 17, 2021 14:15:58.301774025 CET	192.168.2.22	8.8.8.8	0xdcd3	Standard query (0)	smtp.gmail.com	A (IP address)	IN (0x0001)
Feb 17, 2021 14:15:58.371413946 CET	192.168.2.22	8.8.8.8	0xdcd3	Standard query (0)	smtp.gmail.com	A (IP address)	IN (0x0001)
Feb 17, 2021 14:15:58.455055952 CET	192.168.2.22	8.8.8.8	0xdcd3	Standard query (0)	smtp.gmail.com	A (IP address)	IN (0x0001)
Feb 17, 2021 14:15:58.518007994 CET	192.168.2.22	8.8.8.8	0xdcd3	Standard query (0)	smtp.gmail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 17, 2021 14:15:56.659929991 CET	8.8.8.8	192.168.2.22	0x26ae	Name error (3)	163.190.5.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 17, 2021 14:15:57.088181019 CET	8.8.8.8	192.168.2.22	0x80ac	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Feb 17, 2021 14:15:57.088181019 CET	8.8.8.8	192.168.2.22	0x80ac	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Feb 17, 2021 14:15:58.366976023 CET	8.8.8.8	192.168.2.22	0xdcd3	No error (0)	smtp.gmail.com		66.102.1.108	A (IP address)	IN (0x0001)
Feb 17, 2021 14:15:58.437342882 CET	8.8.8.8	192.168.2.22	0xdcd3	No error (0)	smtp.gmail.com		66.102.1.108	A (IP address)	IN (0x0001)
Feb 17, 2021 14:15:58.511831045 CET	8.8.8.8	192.168.2.22	0xdcd3	No error (0)	smtp.gmail.com		66.102.1.108	A (IP address)	IN (0x0001)
Feb 17, 2021 14:15:58.580215931 CET	8.8.8.8	192.168.2.22	0xdcd3	No error (0)	smtp.gmail.com		66.102.1.108	A (IP address)	IN (0x0001)
Feb 17, 2021 14:16:01.135674953 CET	8.8.8.8	192.168.2.22	0x92f1	No error (0)	cdn.digice rtcdn.com		104.18.10.39	A (IP address)	IN (0x0001)
Feb 17, 2021 14:16:01.135674953 CET	8.8.8.8	192.168.2.22	0x92f1	No error (0)	cdn.digice rtcdn.com		104.18.11.39	A (IP address)	IN (0x0001)
Feb 17, 2021 14:16:01.195561886 CET	8.8.8.8	192.168.2.22	0x1175	No error (0)	cdn.digice rtcdn.com		104.18.11.39	A (IP address)	IN (0x0001)
Feb 17, 2021 14:16:01.195561886 CET	8.8.8.8	192.168.2.22	0x1175	No error (0)	cdn.digice rtcdn.com		104.18.10.39	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	192.168.2.22	49167	104.16.155.36	80	C:\Users\user\AppData\Roaming\Windows Update.exe

Timestamp	kBytes transferred	Direction	Data
Feb 17, 2021 14:15:57.188503981 CET	0	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Feb 17, 2021 14:15:57.240376949 CET	1	IN	HTTP/1.1 403 Forbidden Date: Wed, 17 Feb 2021 13:15:57 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 16 Connection: keep-alive X-Frame-Options: SAMEORIGIN Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Set-Cookie: __cfduid=df511a3b29767e188cc5ceb9545d8c6061613567757; expires=Fri, 19-Mar-21 13:15:57 GMT; path=/; domain=.whatismyipaddress.com; HttpOnly; SameSite=Lax; Secure cf-request-id: 0851bb23a500004a8588a22000000001 Server: cloudflare CF-RAY: 622fc7b2aa474a85-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":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

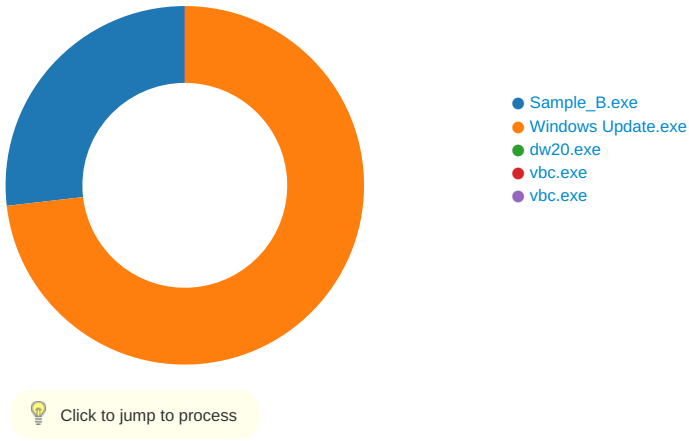
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 17, 2021 14:15:58.753774881 CET	587	49168	66.102.1.108	192.168.2.22	220 smtp.gmail.com ESMTP c3sm3856483wrr.29 - gsmtp
Feb 17, 2021 14:15:58.768049955 CET	49168	587	192.168.2.22	66.102.1.108	EHLO 376483

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 17, 2021 14:15:58.823973894 CET	587	49168	66.102.1.108	192.168.2.22	250-smtp.gmail.com at your service, [84.17.52.38] 250-SIZE 35882577 250-8BITMIME 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-PIPELINING 250-CHUNKING 250 SMTPUTF8
Feb 17, 2021 14:15:58.825731993 CET	49168	587	192.168.2.22	66.102.1.108	STARTTLS
Feb 17, 2021 14:15:58.878711939 CET	587	49168	66.102.1.108	192.168.2.22	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Sample_B.exe PID: 2368 Parent PID: 2956

General

Start time:	14:15:32
Start date:	17/02/2021
Path:	C:\Users\user\Desktop\Sample_B.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Sample_B.exe'
Imagebase:	0xbc0000
File size:	533504 bytes
MD5 hash:	78300BD48D50FA7E5F3F6A933CC5F739
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.2076206862.0000000000BC2000.00000020.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.2076206862.0000000000BC2000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.2076206862.0000000000BC2000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.2076206862.0000000000BC2000.00000020.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.2076206862.0000000000BC2000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000000.2069232329.0000000000BC2000.00000020.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000000.2069232329.0000000000BC2000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000000.2069232329.0000000000BC2000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000000.2069232329.0000000000BC2000.00000020.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000000.2069232329.0000000000BC2000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\SysInfo.txt	read attributes | synchronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	27BCAB	CreateFileW
C:\Users\user\AppData\Roaming\Windows Update.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	5D2CB8	CopyFileW
C:\Users\user\AppData\Roaming\Windows Update.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device | sparse file	sequential only | synchronous io non alert	success or wait	1	5D2CB8	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\SysInfo.txt	unknown	35	43 3a 5c 55 73 65 72 73 5c 41 6c 62 75 73 5c 44 65 73 6b 74 6f 70 5c 53 61 6d 70 6c 65 5f 42 2e 65 78 65	C:\Users\user\Desktop\Sample_B.exe	success or wait	1	27BF33	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windows Update.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 09 c1 16 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 ee 07 00 00 34 00 00 00 00 00 00 ee 0d 08 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....4........... ....@.. ....@................	success or wait	9	5D2CB8	CopyFileW
C:\Users\user\AppData\Roaming\Windows Update.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	5D2CB8	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	27BF33	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	27BF33	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: Windows Update.exe PID: 2360 Parent PID: 2368

General

Start time:	14:15:35
Start date:	17/02/2021
Path:	C:\Users\user\AppData\Roaming\Windows Update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Windows Update.exe'
Imagebase:	0xee0000
File size:	533504 bytes
MD5 hash:	78300BD48D50FA7E5F3F6A933CC5F739
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.2112965167.0000000003610000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000002.2112485117.0000000003371000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000002.2111753690.0000000000EE2000.00000020.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000002.2111753690.0000000000EE2000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.2111753690.0000000000EE2000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.2111753690.0000000000EE2000.00000020.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000002.2111753690.0000000000EE2000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000002.00000002.2113607102.00000000046F0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000000.2075201287.0000000000EE2000.00000020.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000000.2075201287.0000000000EE2000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000000.2075201287.0000000000EE2000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000000.2075201287.0000000000EE2000.00000020.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000000.2075201287.0000000000EE2000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000003.2082749506.00000000054A9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000003.2082749506.00000000054A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000003.2082749506.00000000054A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000003.2082749506.00000000054A9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000002.00000002.2113562918.00000000046E0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000002.2111820758.0000000002371000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.2111820758.0000000002371000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000002.2111820758.0000000002371000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: JPCERT/CC Incident Response Group

Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	read attributes | synchronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	11BCAB	CreateFileW
C:\Users\user\AppData\Roaming\pidloc.txt	read attributes | synchronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	11BCAB	CreateFileW
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	645264	CopyFileW
C:\Users\user\AppData\Roaming\WindowsUpdate.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device | sparse file	sequential only | synchronous io non alert	success or wait	1	645264	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Sample_B.exe	cannot delete	1	642E02	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	32 33 36 30	2360	success or wait	1	11BF33	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	49	43 3a 5c 55 73 65 72 73 5c 41 6c 62 75 73 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 57 69 6e 64 6f 77 73 20 55 70 64 61 74 65 2e 65 78 65	C:\Users\user\AppData\Roaming\Windows Update.exe	success or wait	1	11BF33	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 09 c1 16 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 ee 07 00 00 34 00 00 00 00 00 00 ee 0d 08 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 80 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....4........... ....@.. ....@................	success or wait	9	645264	CopyFileW
C:\Users\user\AppData\Roaming\ WindowsUpdate.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	645264	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	11BF33	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	11BF33	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	11BF33	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	11BF33	ReadFile
C:\Users\user\AppData\Local\Temp\SysInfo.txt	unknown	4096	success or wait	1	11BF33	ReadFile
C:\Users\user\AppData\Local\Temp\SysInfo.txt	unknown	4096	end of file	1	11BF33	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4106	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	73FFA4FC	unknown
C:\Users\user\AppData\Roaming\Windows Update.exe	unknown	4096	success or wait	1	74034496	unknown
C:\Users\user\AppData\Roaming\Windows Update.exe	unknown	512	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	74034496	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Windows Update	unicode	C:\Users\user\AppData\Roaming\WindowsUpdate.exe	success or wait	1	645356	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	dword	2	1	success or wait	1	644B6A	RegSetValueExW

Analysis Process: dw20.exe PID: 2932 Parent PID: 2360

General

Start time:	14:15:38
Start date:	17/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 1708
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	FBA78261A16C65FA44145613E3669E6E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 2852 Parent PID: 2360

General

Start time:	14:15:41
Start date:	17/02/2021
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:	1170056 bytes
MD5 hash:	1672D0478049ABDAF0197BE64A7F867F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: vbc.exe PID: 2816 Parent PID: 2360

General

Start time:	14:15:42
Start date:	17/02/2021
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:	1170056 bytes
MD5 hash:	1672D0478049ABDAF0197BE64A7F867F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis