ID: 338401
Sample Name:
NDt93WWQwd089H7.exe
Cookbook: default.jbs
Time: 08:29:34
Date: 12/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

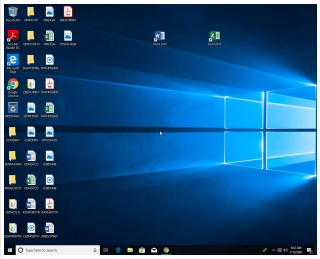
Analysis Report NDt93WWQwd089H7.exe

Overview

General Information

Sample Name:	NDt93WWQwd089H7.exe
Analysis ID:	338401
MD5:	0f330f518f4f71f0…
SHA1:	f34909417588543.
SHA256:	702554b4a0770d..
Tags:	exe HawkEye

Most interesting Screenshot:



Detection

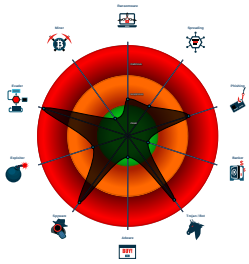
HawkEye
MailPassView

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

Signatures

- Detected HawkEye Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- 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 w10x64**
- NDt93WWQwd089H7.exe (PID: 6980 cmdline: 'C:\Users\user\Desktop\NDt93WWQwd089H7.exe' MD5: 0F330F518F4F71F0735CCE4EAF1612D7)
  - schtasks.exe (PID: 7124 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\etUpjEKgKK' /XML 'C:\Users\user\AppData\Local\Temp\tmp7AE9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - NDt93WWQwd089H7.exe (PID: 3548 cmdline: {path} MD5: 0F330F518F4F71F0735CCE4EAF1612D7)
    - dw20.exe (PID: 2244 cmdline: dw20.exe -x -s 2136 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
    - vbc.exe (PID: 6524 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 6248 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

Threatname: HawkEye


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000003.00000002.398869541.000000000402000.00000040.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b6f7:$key: HawkEyeKeylogger • 0x7d93b:$salt: 099u787978786 • 0x7bd38:$string1: HawkEye_Keylogger • 0x7cb8b:$string1: HawkEye_Keylogger • 0x7d89b:$string1: HawkEye_Keylogger • 0x7c121:$string2: holdermail.txt • 0x7c141:$string2: holdermail.txt • 0x7c063:$string3: wallet.dat • 0x7c07b:$string3: wallet.dat • 0x7c091:$string3: wallet.dat • 0x7d45f:$string4: Keylog Records • 0x7d777:$string4: Keylog Records • 0x7d993:$string5: do not script --> • 0x7b6df:$string6: \pidloc.txt • 0x7b76d:$string7: BSPLIT • 0x7b77d:$string7: BSPLIT
00000003.00000002.398869541.000000000402000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000003.00000002.398869541.000000000402000.00000040.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000003.00000002.398869541.000000000402000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000003.00000002.398869541.000000000402000.00000040.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x7bd90:$hawkstr1: HawkEye Keylogger • 0x7cbd1:$hawkstr1: HawkEye Keylogger • 0x7cf00:$hawkstr1: HawkEye Keylogger • 0x7d05b:$hawkstr1: HawkEye Keylogger • 0x7d1be:$hawkstr1: HawkEye Keylogger • 0x7d437:$hawkstr1: HawkEye Keylogger • 0x7b91e:$hawkstr2: Dear HawkEye Customers! • 0x7cf53:$hawkstr2: Dear HawkEye Customers! • 0x7d0aa:$hawkstr2: Dear HawkEye Customers! • 0x7d211:$hawkstr2: Dear HawkEye Customers! • 0x7ba3f:$hawkstr3: HawkEye Logger Details:
Click to see the 22 entries				

Unpacked PEs

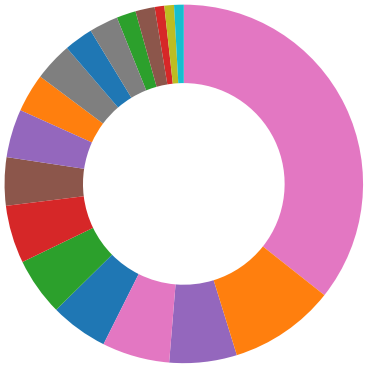
Source	Rule	Description	Author	Strings
7.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
7.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
8.2.vbc.exe.400000.0.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
8.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
3.2.NDt93WWQwd089H7.exe.400000.0.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b8f7:$key: HawkEyeKeylogger • 0x7db3b:$salt: 099u787978786 • 0x7bf38:$string1: HawkEye_Keylogger • 0x7cd8b:$string1: HawkEye_Keylogger • 0x7da9b:$string1: HawkEye_Keylogger • 0x7c321:$string2: holdermail.txt • 0x7c341:$string2: holdermail.txt • 0x7c263:$string3: wallet.dat • 0x7c27b:$string3: wallet.dat • 0x7c291:$string3: wallet.dat • 0x7d65f:$string4: Keylog Records • 0x7d977:$string4: Keylog Records • 0x7db93:$string5: do not script --> • 0x7b8df:$string6: \pidloc.txt • 0x7b96d:$string7: BSPLIT • 0x7b97d:$string7: BSPLIT
Click to see the 4 entries				

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

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:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

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

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

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

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected HawkEye Keylogger

Yara detected MailPassView

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

Tries to steal Instant Messenger accounts or passwords

Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Detected HawkEye Rat

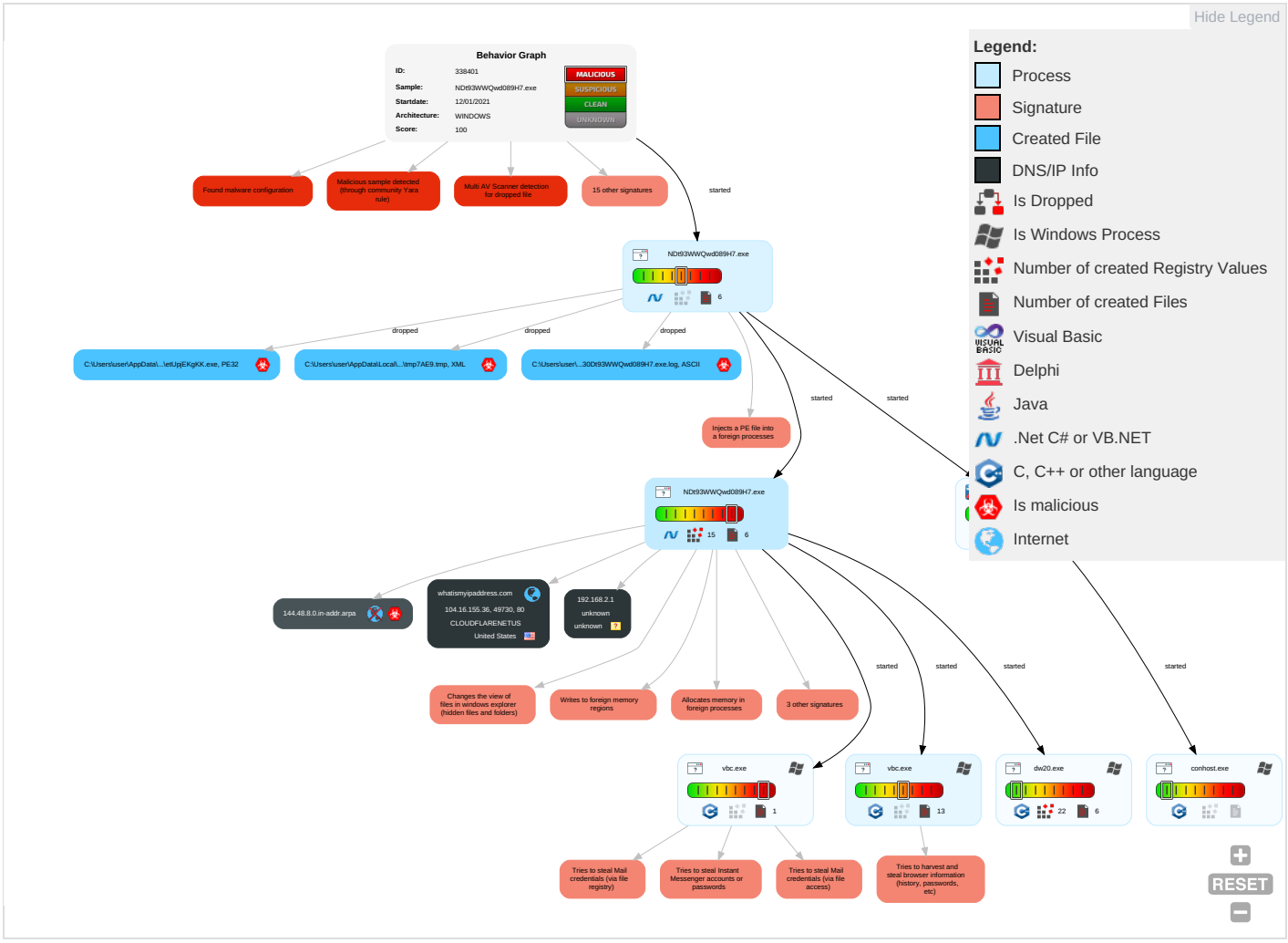
Yara detected HawkEye Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Replication Through Removable Media 1	Windows Management Instrumentation 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	In T
Default Accounts	Native API 1 1	Scheduled Task/Job 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	E C
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Process Injection 4 1 1	Obfuscated Files or Information 4 1	Credentials in Registry 2	Account Discovery 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	R S
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1 3	Credentials In Files 1	File and Directory Discovery 2	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	N A L P
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	System Information Discovery 1 8	SSH	Clipboard Data 2	Data Transfer Size Limits	A L P
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 4	Cached Domain Credentials	Security Software Discovery 2 5 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M C
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C U
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 4 1 1	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A L

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	F P
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Network Configuration Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	M

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
NDt93WWQwd089H7.exe	42%	Virustotal		Browse
NDt93WWQwd089H7.exe	22%	ReversingLabs	Win32.Trojan.Generic	
NDt93WWQwd089H7.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\etUpjEKgKK.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\etUpjEKgKK.exe	22%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
3.2.NDt93WWQwd089H7.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
3.2.NDt93WWQwd089H7.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Domains

Source	Detection	Scanner	Label	Link
144.48.8.0.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comionF	0%	Avira URL Cloud	safe	
http://www.urwpp.dett	0%	Avira URL Cloud	safe	
http://www.tiro.comnt	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fonts.com(	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdsedc	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnv-s	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cna-d	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comcommN	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnC	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.fontbureau.com)	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.urwpp.de:	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/4	0%	Avira URL Cloud	safe	
http://www.urwpp.de4	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	Avira URL Cloud	safe	
http://www.fonts.comp	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cna	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fonts.coms	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/&	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnegu=	0%	Avira URL Cloud	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnse	0%	Avira URL Cloud	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/?	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/x	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.fontbureau.comdik&	0%	Avira URL Cloud	safe	
http://www.urwpp.deo	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/adnl	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnicr	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/j	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd?	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.155.36	true	false		high
144.48.8.0.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.fontbureau.comionF	NDt93WWQwd089H7.exe, 00000000.00000002.382162931.00000000571000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.dett	NDt93WWQwd089H7.exe, 00000000.00000003.345602390.00000000572E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.00000000055500000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false		high
http://www.tiro.comnt	NDt93WWQwd089H7.exe, 00000000.00000003.342561437.0000000005728000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false		high
http://www.fonts.com(	NDt93WWQwd089H7.exe, 00000000.00000003.338297156.0000000005744D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comdsedc	NDt93WWQwd089H7.exe, 00000000.00000003.347562951.0000000005716000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnv-s	NDt93WWQwd089H7.exe, 00000000.00000003.340452276.0000000005713000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cna-d	NDt93WWQwd089H7.exe, 00000000.00000003.340571238.0000000005713000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comcommN	NDt93WWQwd089H7.exe, 00000000.00000003.347562951.0000000005716000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnC	NDt93WWQwd089H7.exe, 00000000.00000003.340769553.0000000005721000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	NDt93WWQwd089H7.exe, 00000000.00000003.337989572.0000000001711D000.00000004.00000001.sdmp, NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com)	NDt93WWQwd089H7.exe, 00000000.00000002.382162931.0000000005710000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cn/cThe	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de:	NDt93WWQwd089H7.exe, 00000000.00000003.347700147.0000000005722000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/4	NDt93WWQwd089H7.exe, 00000000.00000003.343555634.0000000005716000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de4	NDt93WWQwd089H7.exe, 00000000.00000003.345819766.000000000572E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com/-	NDt93WWQwd089H7.exe, 00000000.00000002.381513647.00000000047E8000.00000004.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.398869541.0000000000402000.00000040.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/)	NDt93WWQwd089H7.exe, 00000000.00000003.342884989.0000000005716000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comp	NDt93WWQwd089H7.exe, 00000000.00000003.338202585.000000000574D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cna	NDt93WWQwd089H7.exe, 00000000.00000003.340810224.0000000005721000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersv	NDt93WWQwd089H7.exe, 00000000.00000003.347562951.0000000005716000.00000004.00000001.sdmp	false		high
http://https://login.yahoo.com/config/login	vbc.exe	false		high
http://www.fonts.com	NDt93WWQwd089H7.exe, 00000000.00000003.338177028.000000000574D000.00000004.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.site.com/logs.php	NDt93WWQwd089H7.exe, 00000003.00000002.400292236.0000000002D61000.00000004.00000001.sdmp	false		high
http://www.fonts.coms	NDt93WWQwd089H7.exe, 00000000.00000003.338238361.000000000574D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/&	NDt93WWQwd089H7.exe, 00000000.00000003.343232435.0000000005716000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	vbc.exe, vbc.exe, 00000008.00000002.391162652.0000000000400000.00000040.00000001.sdmp	false		high
http://www.urwpp.de	NDt93WWQwd089H7.exe, 00000000.00000003.347700147.0000000005722000.00000004.00000001.sdmp, NDt93WWQwd089H7.exe, 00000000.00000003.345535992.000000000572E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	NDt93WWQwd089H7.exe, 00000000.00000003.341937780.000000005571E000.00000004.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.come	NDt93WWQwd089H7.exe, 00000000.00000003.337989572.000000000171D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.000000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnegu=	NDt93WWQwd089H7.exe, 00000000.00000003.340571238.000000000571300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com=	NDt93WWQwd089H7.exe, 00000000.00000003.347562951.000000000571600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://2542116.fls.doubleclick.net/activi	vbc.exe, 00000008.00000003.390845966.000000000212C000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.000000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	NDt93WWQwd089H7.exe, 00000000.00000003.347562951.000000000571600.00000004.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cnse	NDt93WWQwd089H7.exe, 00000000.00000003.341937780.000000005571E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comslnt	NDt93WWQwd089H7.exe, 00000000.00000003.342633757.000000005572B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/q	NDt93WWQwd089H7.exe, 00000000.00000003.346033185.000000005572E000.00000004.00000001.sdmp	false		high
http://whatismyipaddress.com	NDt93WWQwd089H7.exe, 00000003.00000002.400292236.0000000002D61000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/	NDt93WWQwd089H7.exe, 00000000.00000003.343555634.000000000571600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/?	NDt93WWQwd089H7.exe, 00000000.00000003.343555634.000000000571600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/x	NDt93WWQwd089H7.exe, 00000000.00000003.343232435.000000000571600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.000000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.000000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.000000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/x	NDt93WWQwd089H7.exe, 00000000.00000003.342884989.000000000571600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comdik&	NDt93WWQwd089H7.exe, 00000000.00000003.347562951.0000000005716000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.deo	NDt93WWQwd089H7.exe, 00000000.00000003.345535992.0000000005702E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	NDt93WWQwd089H7.exe, 00000000.00000003.342884989.0000000005716000.00000004.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/adnl	NDt93WWQwd089H7.exe, 00000000.00000003.343555634.0000000005716000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	NDt93WWQwd089H7.exe, 00000000.00000002.382306744.00000000058A0000.00000002.00000001.sdmp, NDt93WWQwd089H7.exe, 00000003.00000002.403713675.0000000005550000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnicr	NDt93WWQwd089H7.exe, 00000000.00000003.340769553.0000000005721000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/j	NDt93WWQwd089H7.exe, 00000000.00000003.343232435.0000000005716000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd?	NDt93WWQwd089H7.exe, 00000000.00000003.347562951.0000000005716000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338401
Start date:	12.01.2021
Start time:	08:29:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NDt93WWQwd089H7.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winEXE@12/9@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 99.1% (good quality ratio 96.1%) • Quality average: 85.6% • Quality standard deviation: 23.2%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.42.151.234, 51.11.168.160, 2.20.142.210, 2.20.142.209, 51.103.5.186, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 104.79.90.110 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:30:35	API Interceptor	7x Sleep call for process: NDt93WWQwd089H7.exe modified
08:30:56	API Interceptor	1x Sleep call for process: dw20.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.155.36	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/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Prueba de pago.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	6JLHKYvboo.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	jSMd8npgmU.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	9vdouqRTh3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	5pB35gGfZ5.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	fyxC4Hgs3s.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	yk94P18VKp.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	oLHQIQAI3N.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	WuGzF7ZJ7P.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NXmokFkh3R.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	qiGQsdRM57.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NSSPH41vE5.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	2v7Vtqfo81.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	355OckuTD3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	i7osF3yJYR.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
whatismyipaddress.com	JkhR5oeRHA.exe	Get hash	malicious	Browse	• 66.171.248.178
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 104.16.155.36
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• 104.16.154.36
	INQUIRY.exe	Get hash	malicious	Browse	• 104.16.154.36
	Prueba de pago.exe	Get hash	malicious	Browse	• 104.16.155.36
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	http://https://my-alliances.co.uk/	Get hash	malicious	Browse	• 66.171.248.178
	c9o0CtTIYT.exe	Get hash	malicious	Browse	• 104.16.154.36
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• 104.16.155.36
	6JLHKYvboo.exe	Get hash	malicious	Browse	• 104.16.155.36
	jSMd8npgmU.exe	Get hash	malicious	Browse	• 104.16.155.36
	khJdbt0clZ.exe	Get hash	malicious	Browse	• 104.16.154.36
	ZMOKwXqVHO.exe	Get hash	malicious	Browse	• 104.16.154.36
	5Av43Q5lXd.exe	Get hash	malicious	Browse	• 104.16.154.36
	8oaZfXDstn.exe	Get hash	malicious	Browse	• 104.16.154.36
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• 104.16.155.36
	9vdouqRTh3.exe	Get hash	malicious	Browse	• 104.16.154.36

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	zz4osC4FRa.exe	Get hash	malicious	Browse	• 104.18.34.213
	yKFlKg9R6m.exe	Get hash	malicious	Browse	• 66.235.200.147
	DTwcHU5qyI.exe	Get hash	malicious	Browse	• 23.227.38.74
	btVnDhh5K7.exe	Get hash	malicious	Browse	• 104.27.156.22
	T0pH7Bimeq.exe	Get hash	malicious	Browse	• 104.31.64.148
	lKCnywe5rE.exe	Get hash	malicious	Browse	• 23.227.38.74
	Payment Advice.xlsx	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Arrival notice.xlsx	Get hash	malicious	Browse	• 104.24.96.84
	Inv0209966048-20210111075675.xls	Get hash	malicious	Browse	• 104.27.153.52
	ku7PCBVgfP.exe	Get hash	malicious	Browse	• 172.67.188.154
	00000000000900SA.exe	Get hash	malicious	Browse	• 104.28.4.151
	QT55.vbs	Get hash	malicious	Browse	• 172.67.131.130
	VN55.vbs	Get hash	malicious	Browse	• 172.67.131.130
	VP57.vbs	Get hash	malicious	Browse	• 172.67.131.130
	wCRnCAMZ3yT8BQ2.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO_RFQ_2021_12_01.exe	Get hash	malicious	Browse	• 172.67.188.154
	BxiS9KHIxj.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO_RFQ_2021_12_01 - s.doc	Get hash	malicious	Browse	• 172.67.188.154
	UbisoftInstaller.exe	Get hash	malicious	Browse	• 104.27.128.28
	al9LrOC8eM.exe	Get hash	malicious	Browse	• 104.28.5.151

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_ndt93wwqwd089h7._f33cd8375d2498bf766815ce1165fc13564c2_00000000_08f8413b\Report.wer

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16836
Entropy (8bit):	3.7591049213167884
Encrypted:	false
SSDEEP:	192:DTC43NV3aPLk9Mg5N3gFm1pzvnuk1+K1QtKVzz/u7s9S274ItW:XC43PayRv1jzz/u7s9X4ItW
MD5:	D45D05768338987FADF5F584AA5DE670
SHA1:	DFD01FDCC2EEE689BE8B5807D1D3C9A9D61A35CE
SHA-256:	BB55D09A3FAD477BEA8C4D771C3CC31FFB42EA8B0077308D0DF0419B41CB6194
SHA-512:	35A22A5418C27BFB8C7625CF65F2E051A8775D578B9A6BA54F596ED9F7E6A15CFE74464CDE87D363773D9B223D9B95D480AACED4953DC8109922E7967CF2010
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.=.1.3.2.5.4.9.4.2.6.4.8.2.2.5.3.1.7.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.4.9.4.2.6.5.0.2.7.2.1.8.1.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.a.9.9.1.6.e.b.-.3.9.8.f.-.4.2.7.f.-.8.7.1.7.-.b.c.6.0.a.0.4.9.2.6.e.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.d.c.-.0.0.0.1.-.0.0.1.7.-.3.2.2.0.-.d.5.4.4.0.0.e.9.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.6.a.b.3.a.4.1.7.e.3.3.6.e.4.4.9.1.4.5.c.8.9.0.7.b.2.c.6.e.c.1.0.0.0.0.0.0.0.0.!.0.0.0.0.f.3.4.9.0.9.4.1.7.5.8.8.5.4.3.1.1.2.9.7.4.e.b.b.c.0.f.a.8.2.3.6.a.8.a.6.0.4.c.1.!.N.D.t.9.3.W.W.Q.w.d.0.8.9.H.7...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.1././.1.1.:.2.1.:.0.5.:.1.9.!.0.!.N.D.t.9.3.W.W.Q.w.d.0.8.9.H.7...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.l.d.=.3.5.1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F3C.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):	7698
Entropy (8bit):	3.7061102895611078
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi7h6uBgS6Y++66gmfZz1S1Cp1R91f0SB7m:RrlsNi96uT6Yf66gmfd1S8R/ffg
MD5:	3E97BD38E1589EFB5BB6CC9BA303B87F
SHA1:	46EAA58DABFAFA259950D01ECB98D4CC49763A79
SHA-256:	D6C8E1C6059E0F66A3CC067A29B5C1753DFBD0CBB5055F3CC3C19F1A5AC18DDA
SHA-512:	C8CCE21BB922D7B41F5297DE651F4426B6E17168EE269063C235E2C1D984BB0258C395ADDBD98786D0BD8CE3B0F19F88FE6395D484ED46718EBFEC7CE6C7D85
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F3C.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.5.4.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2037.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4645
Entropy (8bit):	4.470302479664142
Encrypted:	false
SSDEEP:	48:cvIwSD8zsoJgtWI9htWSC8BV8fm8M4JFKXF5Fk6+q8veF63nSZSCd:uITfumcSNEJFKXO6KeYCkCd
MD5:	B3E4E32F415240BB43DBD960E8CF563E
SHA1:	44F6E16E88A28700C141DE4F3A42A6C1F7D55A9B
SHA-256:	A40575B4966DC436B2197DC2360B5128E44B2642E2B9B0BE775E8F70D211505F
SHA-512:	56F94DD293C2B4D7AAD3DF3513DACC46B49D76BCC038DFDF46476A80E4E0BD1C9A3880B98C8AB2675DFB8A83ADF2D43B0B1FF1B4F117ACEEDAB4AC0FC5E 9CC9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="813701" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\NDt93WWQwd089H7.exe.log	
Process:	C:\Users\user\Desktop\NDt93WWQwd089H7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

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

C:\Users\user\AppData\Local\Temp\tmp7AE9.tmp	
Process:	C:\Users\user\Desktop\NDt93WWQwd089H7.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1655
Entropy (8bit):	5.15984889759781
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3WaYtn:cbha7JlNQV/rydbz9I3YODOLNdq3UF
MD5:	7A61294EA6F437E114F829A5548F7E73
SHA1:	64F62BB02AA77F5307134C73FACBE241300A3A43
SHA-256:	D92E50D30E97CFC79485FB8A9F3731BCDD737A7B9E4230CC70B2604566DEF63A
SHA-512:	493CDE3EEC80934A56A1EDF610197E1BFEAF768DEF279192B6D51AB319EB58B6D228ABC43493C510E2FBC69F0365303A558C3C13F9FB8CF84027E37400E0CF49
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\etUpjEKgKK.exe	
Process:	C:\Users\user\Desktop\NDt93WWQwd089H7.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1321984
Entropy (8bit):	7.820004783808826
Encrypted:	false
SSDEEP:	24576:ff8nPjsruA/V8HYmqbtRCy6TOVKLrscPGKo8XCktUN4Sjzb8lRm:fUnPjrAqYmkCyUhLftqjzIlRm
MD5:	0F330F518F4F71F0735CCE4EAF1612D7
SHA1:	F34909417588543112974EBBC0FA8236A8A604C1
SHA-256:	702554B4A0770D70BD5972318D2294EF2B26001595B574D122264B8C1793457C
SHA-512:	EE5EC83814A64C56BDFDAEC885396C86364CCF5BD7EAA25B3BDD2C43C6A8C7427BDF2A7514A7C0043294CDF7C9B89699A818CA65D5E4EF6F5D04C0DE94597DB3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 22%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....L..... .....@.. ....@.....\...O.....I.....`..... ..... ..H.....text..... ..... ..`.rsrc....I.....J.....@..@.reloc.....` .....*.....@..B.....H.....<$.. .....t{.....0.....o.... ...._ .....,....8.....o....t..... . &.....o.....o....(.....o.....o.....o....o....Z. Z.....(.....+E.....X.Y.....,.+*.....X.....X.....X.....X.....X.I.Z.....X.....i.....-.....(.....o.....+...*^..}.....(.....(.....*.0.....s.....o.....(....*.".(....*....0.....s.....o..... (....*..0..+.....,..{.....+...,...{....o

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\Desktop\NDt93WWQwd089H7.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:X7n:rn
MD5:	50CF0763D8EB871776D4F28B39DEB564
SHA1:	A1805C1D24E78F77B61181D0D64561EE1EFE6638
SHA-256:	245D17B28D73E10C5C842B53AF64338F46FB04A99773F82622A02198804E6DBA
SHA-512:	727B4B3251D28D0F2E560AEF1082F9AA362FB1703D4DA66A28B84CB5B5DE33CBC0DEC831E2B09D71EA02657BA1EA0C1838A96F8BA4D83F6DB1ED12447446D50A
Malicious:	false
Reputation:	low
Preview:	3548

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\Desktop\NDt93WWQwd089H7.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	45

C:\Users\user\AppData\Roaming\pidloc.txt	
Entropy (8bit):	4.505044830628194
Encrypted:	false
SSDEEP:	3:oNN2+WrHhJLN:oNN2R1JJ
MD5:	35484D514FB8402A3F706EC192EC94AF
SHA1:	9829A7D498C242FB2524BA550B0E0CF826490A5D
SHA-256:	67C1AA10ED8D4385083CEE7E78A63735F2E01DECE93B1D60335813038091AF1B
SHA-512:	3F09256AB3902C7AC040FE204D4610A8A4A6641AEF4FF58389B03C6D8E43D63A2E6F757ADD22156BAC2B31039C8F6177807BF5E7AD385F36024E4412C59FDB1E
Malicious:	false
Preview:	C:\Users\user\Desktop\NDt93WWQwd089H7.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.820004783808826
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	NDt93WWQwd089H7.exe
File size:	1321984
MD5:	0f330f518f4f71f0735cce4eaf1612d7
SHA1:	f34909417588543112974ebbc0fa8236a8a604c1
SHA256:	702554b4a0770d70bd5972318d2294ef2b26001595b574d122264b8c1793457c
SHA512:	ee5ec83814a64c56bdfdaec885396c86364ccf5bd7eaa25b3bdd2c43c6a8c7427bdf2a7514a7c0043294cdf7c9b89699a818ca65d5e4ef6f5d04c0de94597db3
SSDEEP:	24576:ff8nPjsruA/V8HYmqbtRCy6TOVKLrscPGKo8XCktUN4Sjzb8lRm:fUnPjrAqYmkCyUhLftqjzlIRm
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....L..... .....@.. .....@.....

File Icon

Icon Hash:	b2aab6b2e8e8bad2

Static PE Info

General

Entrypoint:	0x53fcae
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:	0x5FFCBD8F [Mon Jan 11 21:05:19 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

General

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x13fc5c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x140000	0x4990	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x146000	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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x13dcb4	0x13de00	False	0.876285698486	data	7.82936221614	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x140000	0x4990	0x4a00	False	0.295713682432	data	5.82925970334	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x146000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x140130	0x4228	data		
RT_GROUP_ICON	0x144358	0x14	data		
RT_VERSION	0x14436c	0x438	data	English	United States
RT_MANIFEST	0x1447a4	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
LegalCopyright	72ab0bc5 e98b 4896 923f 6b415c01b9d8
FileVersion	20.12.0.0
CompanyName	599f2f64 d5c8 4d24 b34b 256dd3f00d2a
LegalTrademarks	b5af90e4 fe79 4a45 a582 3d5efc5a804e
Comments	10667c87 d5a1 44f2 ab7b 9669c914c1a3
ProductName	1baad9cd 9d47 4071 bded 1375b25d7418
ProductVersion	20.12.0.0
FileDescription	f9ca2b02 d6f7 4b2f 8826 598b055ae346
Guid	26367ab8-23b4-4870-b4c7-2f303fc01747
Translation	0x0000 0x04e4

Possible Origin

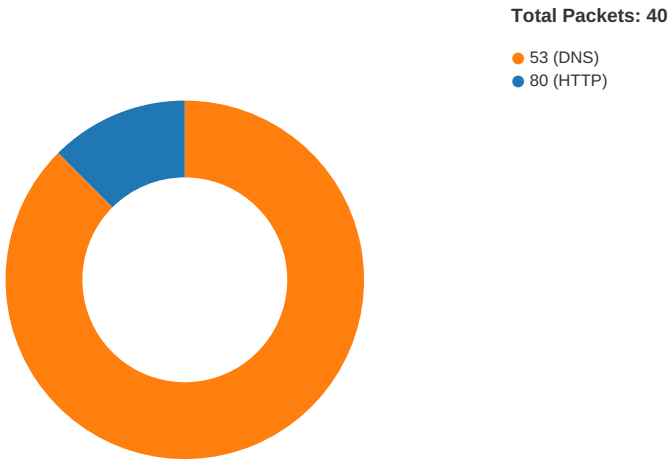
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/21-08:30:46.820573	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49730	104.16.155.36	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 08:30:46.727550983 CET	49730	80	192.168.2.6	104.16.155.36
Jan 12, 2021 08:30:46.767819881 CET	80	49730	104.16.155.36	192.168.2.6
Jan 12, 2021 08:30:46.768065929 CET	49730	80	192.168.2.6	104.16.155.36
Jan 12, 2021 08:30:46.769025087 CET	49730	80	192.168.2.6	104.16.155.36
Jan 12, 2021 08:30:46.809201956 CET	80	49730	104.16.155.36	192.168.2.6
Jan 12, 2021 08:30:46.820573092 CET	80	49730	104.16.155.36	192.168.2.6
Jan 12, 2021 08:30:46.897602081 CET	49730	80	192.168.2.6	104.16.155.36
Jan 12, 2021 08:31:01.298902988 CET	49730	80	192.168.2.6	104.16.155.36

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 08:30:19.951621056 CET	53	56023	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:20.685022116 CET	58384	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:20.732856989 CET	53	58384	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:21.614845991 CET	60261	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:21.663522005 CET	53	60261	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:22.960685968 CET	56061	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:23.008923054 CET	53	56061	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:26.831720114 CET	58336	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:26.890636921 CET	53	58336	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:28.374205112 CET	53781	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:28.422446012 CET	53	53781	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:29.276691914 CET	54064	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:29.327435970 CET	53	54064	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:30.869076014 CET	52811	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:30.920586109 CET	53	52811	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:32.118745089 CET	55299	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:32.175179005 CET	53	55299	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:33.425901890 CET	63745	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:33.487299919 CET	53	63745	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:34.244273901 CET	50055	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:34.293999910 CET	53	50055	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:37.519741058 CET	61374	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:37.570499897 CET	53	61374	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:46.346276045 CET	50339	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:46.404792070 CET	53	50339	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:46.644718885 CET	63307	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:46.701044083 CET	53	63307	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:51.230866909 CET	49694	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:51.281569958 CET	53	49694	8.8.8.8	192.168.2.6
Jan 12, 2021 08:30:51.669358969 CET	54982	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:30:51.717308998 CET	53	54982	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:09.392643929 CET	50010	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:09.450731993 CET	53	50010	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 08:31:11.387994051 CET	63718	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:11.446997881 CET	53	63718	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:12.695867062 CET	62116	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:12.799546003 CET	53	62116	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:13.464844942 CET	63816	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:13.524024963 CET	53	63816	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:14.089591980 CET	55014	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:14.208554029 CET	53	55014	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:14.673410892 CET	62208	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:14.732940912 CET	53	62208	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:15.143646002 CET	57574	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:15.199717045 CET	53	57574	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:15.622399092 CET	51818	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:15.682066917 CET	53	51818	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:16.242536068 CET	56628	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:16.301024914 CET	53	56628	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:16.905329943 CET	60778	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:16.961869955 CET	53	60778	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:17.764086962 CET	53799	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:17.823160887 CET	53	53799	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:18.046360016 CET	54683	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:18.104255915 CET	53	54683	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:18.892868042 CET	59329	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:18.949007988 CET	53	59329	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:19.553423882 CET	64021	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:20.604033947 CET	64021	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:20.651890039 CET	53	64021	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:50.180362940 CET	56129	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:50.228300095 CET	53	56129	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:50.624979973 CET	58177	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:51.637994051 CET	58177	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:51.694196939 CET	53	58177	8.8.8.8	192.168.2.6
Jan 12, 2021 08:31:54.727160931 CET	50700	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:31:54.785674095 CET	53	50700	8.8.8.8	192.168.2.6
Jan 12, 2021 08:32:12.586863041 CET	54069	53	192.168.2.6	8.8.8.8
Jan 12, 2021 08:32:12.637756109 CET	53	54069	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 12, 2021 08:30:46.346276045 CET	192.168.2.6	8.8.8.8	0xbd60	Standard query (0)	144.48.8.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jan 12, 2021 08:30:46.644718885 CET	192.168.2.6	8.8.8.8	0x77b2	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2021 08:30:46.404792070 CET	8.8.8.8	192.168.2.6	0xbd60	Name error (3)	144.48.8.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Jan 12, 2021 08:30:46.701044083 CET	8.8.8.8	192.168.2.6	0x77b2	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Jan 12, 2021 08:30:46.701044083 CET	8.8.8.8	192.168.2.6	0x77b2	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- whatismyipaddress.com

HTTP Packets

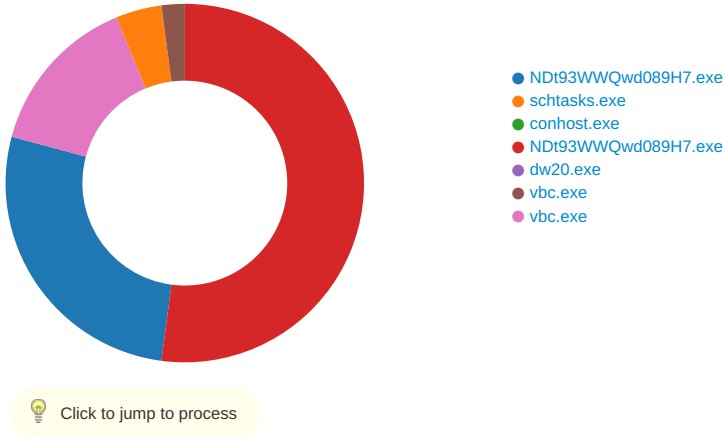
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49730	104.16.155.36	80	C:\Users\user\Desktop\NDt93WWQwd089H7.exe

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2021 08:30:46.769025087 CET	154	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Jan 12, 2021 08:30:46.820573092 CET	155	IN	HTTP/1.1 403 Forbidden Date: Tue, 12 Jan 2021 07:30:46 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=d51b0959e24551d23cc3f7a758162f2e91610436646; expires=Thu, 11-Feb-21 07:30:46 GMT; path=/; domain=.whatismyipaddress.com; HttpOnly; SameSite=Lax; Secure cf-request-id: 07971a2f9200002be90ebcc000000001 Server: cloudflare CF-RAY: 61052c928bd02be9-FRA Data Raw: 65 72 72 6f 72 20 63 6f 64 65 3a 20 31 30 32 30 Data Ascii: error code: 1020

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: NDt93WWQwd089H7.exe PID: 6980 Parent PID: 5924

General

Start time:	08:30:27
Start date:	12/01/2021
Path:	C:\Users\user\Desktop\NDt93WWQwd089H7.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NDt93WWQwd089H7.exe'
Imagebase:	0xb60000
File size:	1321984 bytes
MD5 hash:	0F330F518F4F71F0735CCE4EAF1612D7

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.377690697.000000000346D000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.381513647.00000000047E8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.381513647.00000000047E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.381513647.00000000047E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.381513647.00000000047E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.381513647.00000000047E8000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\etUpjEKgKK.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	693073B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp7AE9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	138B668	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\NDt93WWQwd089H7.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7AE9.tmp	success or wait	1	693145E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\etUpjEKgKK.exe	unknown	1321984	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 8f bd fc 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 de 13 00 00 4c 00 00 00 00 00 00 ae fc 13 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 14 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......_.......... ....L........... ....@.. ....@.................	success or wait	1	6930A6F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp7AE9.tmp	unknown	1655	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </Registratio	success or wait	1	6930A6F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\NDt93WWQwd089H7.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Users\user\Desktop\NDt93WWQwd089H7.exe	unknown	1321984	success or wait	1	6930A6F	ReadFile

Analysis Process: schtasks.exe PID: 7124 Parent PID: 6980

General

Start time:	08:30:40
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\etUpjEKgKK' /XML 'C:\Users\user\AppData\Local\Temp\tmp7AE9.tmp'
Imagebase:	0x13d0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7AE9.tmp	unknown	2	success or wait	1	13DAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7AE9.tmp	unknown	1656	success or wait	1	13DABD9	ReadFile

Analysis Process: conhost.exe PID: 7132 Parent PID: 7124

General

Start time:	08:30:41
Start date:	12/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: NDt93WWQwd089H7.exe PID: 3548 Parent PID: 6980

General

Start time:	08:30:42
Start date:	12/01/2021
Path:	C:\Users\user\Desktop\NDt93WWQwd089H7.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x5d0000
File size:	1321984 bytes
MD5 hash:	0F330F518F4F71F0735CCE4EAF1612D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000003.00000002.398869541.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000003.00000002.398869541.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000003.00000002.398869541.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000002.398869541.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000003.00000002.398869541.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000003.00000002.402872645.0000000003D61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000003.00000002.402872645.0000000003D61000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000003.00000002.400292236.0000000002D61000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000003.00000002.400292236.0000000002D61000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000003.00000002.400292236.0000000002D61000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\pid.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	725CB31E	unknown
C:\Users\user\AppData\Roaming\pidloc.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	725CB31E	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	4F55A62	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	4F55A62	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	33 35 34 38	3548	success or wait	1	4F50093	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	45	43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 44 65 73 6b 74 6f 70 5c 4e 44 74 39 33 57 57 51 77 64 30 38 39 48 37 2e 65 78 65	C:\Users\user\Desktop\NDt93WWQwd089H7.exe	success or wait	1	4F50093	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	4F50093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4F50093	ReadFile
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	4F50093	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	4F50093	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	4F50093	ReadFile
C:\Users\user\Desktop\NDt93WWQwd089H7.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Users\user\Desktop\NDt93WWQwd089H7.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	dword	2	1	success or wait	1	4F54A02	RegSetValueExW

Analysis Process: dw20.exe PID: 2244 Parent PID: 3548

General

Start time:	08:30:47
Start date:	12/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2136
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: vbc.exe PID: 6524 Parent PID: 3548

General

Start time:	08:30:50
Start date:	12/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.386590531.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

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

Analysis Process: vbc.exe PID: 6248 Parent PID: 3548

General

Start time:	08:30:50
Start date:	12/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.391162652.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

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

File Written

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

File Read

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

Disassembly

Code Analysis