ID: 367711
Sample Name:
Y88576645635_03112021.PDF.exe
Cookbook: default.jbs
Time: 02:10:40
Date: 12/03/2021
Version: 31.0.0 Emerald

Table of Contents

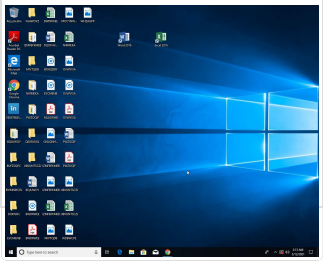
Analysis Report Y88576645635_03112021.PDF.exe

Overview

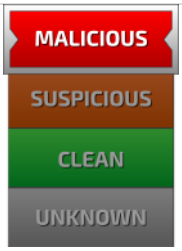
General Information

Sample Name:	Y88576645635_03112021.PDF.exe
Analysis ID:	367711
MD5:	4f0fdcac715b3d9..
SHA1:	1079108984d058..
SHA256:	047d3bebe34018..
Infos:	

Most interesting Screenshot:



Detection



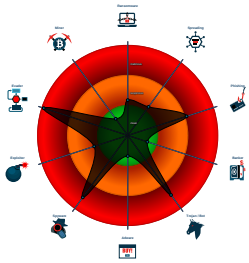
HawkEye
MailPassView

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

Signatures

- Antivirus / Scanner detection for sub…
- Detected HawkEye Rat
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e…
- Yara detected AntiVM_3
- Yara detected HawkEye Keylogger
- Yara detected MailPassView

Classification



Startup

- **System is w10x64**
- Y88576645635_03112021.PDF.exe (PID: 7100 cmdline: 'C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe' MD5: 4F0FDCAC715B3D952FFAB9E7D3EE86AC)
  - Y88576645635_03112021.PDF.exe (PID: 244 cmdline: C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe MD5: 4F0FDCAC715B3D952FFAB9E7D3EE86AC)
  - Y88576645635_03112021.PDF.exe (PID: 3436 cmdline: C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe MD5: 4F0FDCAC715B3D952FFAB9E7D3EE86AC)
  - Y88576645635_03112021.PDF.exe (PID: 6596 cmdline: C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe MD5: 4F0FDCAC715B3D952FFAB9E7D3EE86AC)
    - Y88576645635_03112021.PDF.exe (PID: 5912 cmdline: C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe MD5: 4F0FDCAC715B3D952FFAB9E7D3EE86AC)
    - Y88576645635_03112021.PDF.exe (PID: 6316 cmdline: C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe MD5: 4F0FDCAC715B3D952FFAB9E7D3EE86AC)
      - vbc.exe (PID: 6896 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: 6880 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
00000004.00000002.659715727.0000000002F91000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.908387169.000000000809 0000.00000004.00000001.sdmp	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
00000006.00000002.902253239.000000000040 2000.00000040.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b719:$key: HawkEyeKeylogger • 0x7d917:$salt: 099u787978786 • 0x7bd32:$string1: HawkEye_Keylogger • 0x7cb85:$string1: HawkEye_Keylogger • 0x7d877:$string1: HawkEye_Keylogger • 0x7c11b:$string2: holdermail.txt • 0x7c13b:$string2: holdermail.txt • 0x7c05d:$string3: wallet.dat • 0x7c075:$string3: wallet.dat • 0x7c08b:$string3: wallet.dat • 0x7d459:$string4: Keylog Records • 0x7d771:$string4: Keylog Records • 0x7d96f:$string5: do not script --> • 0x7b701:$string6: \pidloc.txt • 0x7b767:$string7: BSPLIT • 0x7b777:$string7: BSPLIT
00000006.00000002.902253239.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000006.00000002.902253239.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.Y88576645635_03112021.PDF.exe.39b1b5 0.8.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
6.2.Y88576645635_03112021.PDF.exe.809000 0.11.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
6.2.Y88576645635_03112021.PDF.exe.81f0000.12.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
10.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
11.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 59 entries				

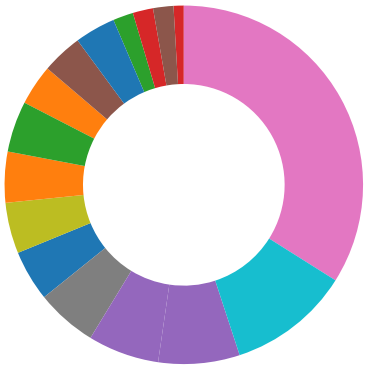
Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Signature Overview

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



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

Contains functionality to log keystrokes (.Net Source)

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Uses an obfuscated file name to hide its real file extension (double extension)

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

Injects a PE file into a foreign processes

Sample uses process hollowing technique

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

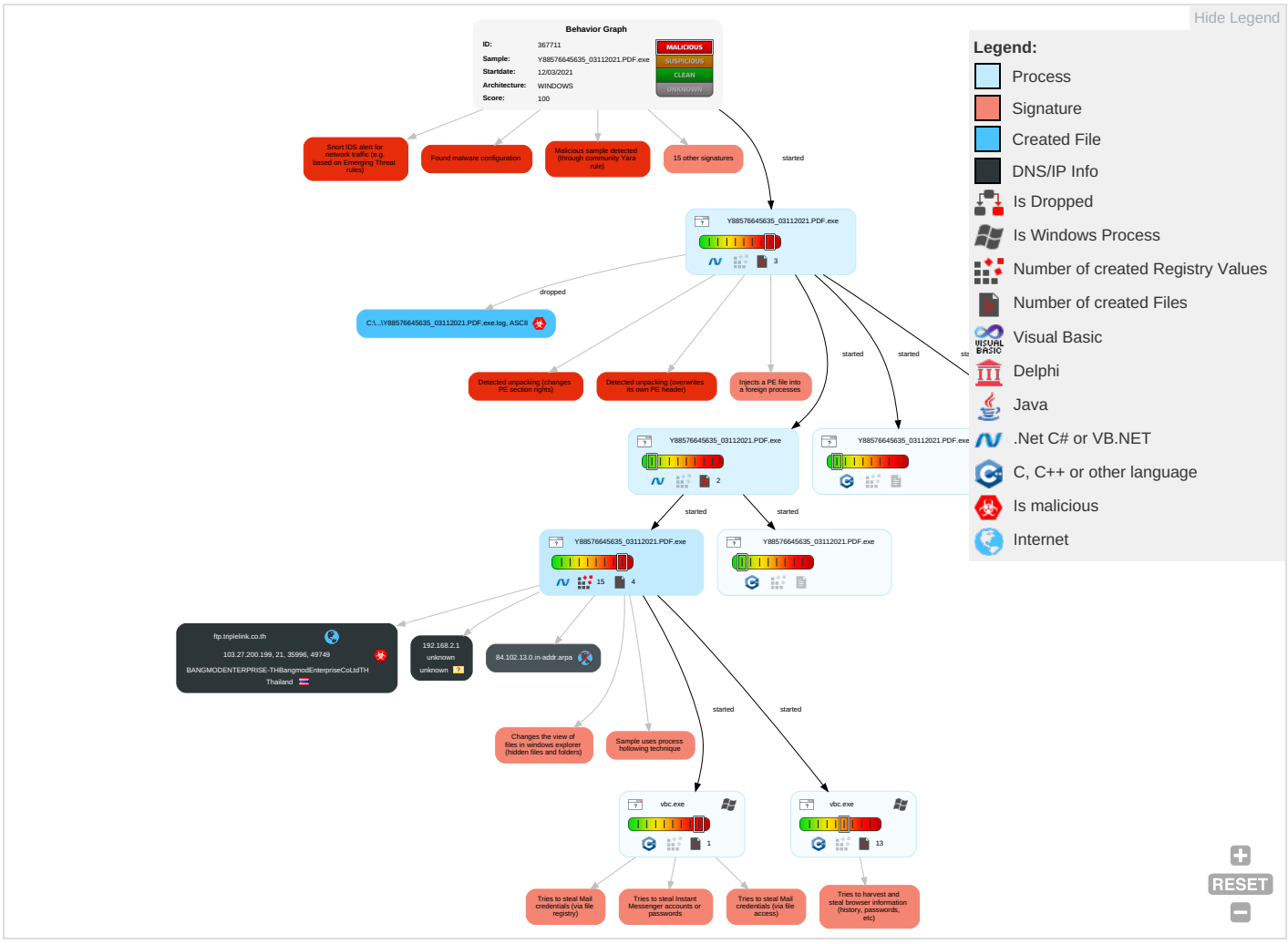
Yara detected HawkEye Keylogger

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 Alternative Protocol 1	E C
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 2 1 2	Deobfuscate/Decode Files or Information 1 1	Input Capture 1 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	N P
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1 4 1	Credentials in Registry 2	Account Discovery 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	R S
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3 3	Credentials In Files 1	File and Directory Discovery 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	N A L P
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	System Information Discovery 1 8	SSH	Clipboard Data 1	Data Transfer Size Limits	A L P
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M C
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2 1 2	DCSync	Security Software Discovery 1 3 1	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	Hidden Files and Directories 1	Proc Filesystem	Virtualization/Sandbox Evasion 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A L
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Process Discovery 4	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Application Window Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	F P

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Owner/User Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	M
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	D

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
Y88576645635_03112021.PDF.exe	21%	ReversingLabs	Win32.Trojan.Pwsx	
Y88576645635_03112021.PDF.exe	100%	Avira	HEUR/AGEN.1137139	
Y88576645635_03112021.PDF.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Y88576645635_03112021.PDF.exe.610000.0.unpack	100%	Avira	HEUR/AGEN.1137139		Download File
11.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
2.2.Y88576645635_03112021.PDF.exe.220000.0.unpack	100%	Avira	HEUR/AGEN.1137139		Download File
6.0.Y88576645635_03112021.PDF.exe.540000.0.unpack	100%	Avira	HEUR/AGEN.1137139		Download File
0.2.Y88576645635_03112021.PDF.exe.610000.0.unpack	100%	Avira	HEUR/AGEN.1109526		Download File
4.0.Y88576645635_03112021.PDF.exe.a40000.0.unpack	100%	Avira	HEUR/AGEN.1137139		Download File
3.0.Y88576645635_03112021.PDF.exe.4f0000.0.unpack	100%	Avira	HEUR/AGEN.1137139		Download File
2.0.Y88576645635_03112021.PDF.exe.220000.0.unpack	100%	Avira	HEUR/AGEN.1137139		Download File
4.2.Y88576645635_03112021.PDF.exe.a40000.1.unpack	100%	Avira	HEUR/AGEN.1137139		Download File
5.2.Y88576645635_03112021.PDF.exe.300000.0.unpack	100%	Avira	HEUR/AGEN.1137139		Download File

Source	Detection	Scanner	Label	Link	Download
5.0.Y88576645635_03112021.PDF.exe.300000.0.unpack	100%	Avira	HEUR/AGEN.1137139		Download File
6.2.Y88576645635_03112021.PDF.exe.540000.4.unpack	100%	Avira	HEUR/AGEN.1137139		Download File
3.2.Y88576645635_03112021.PDF.exe.4f0000.0.unpack	100%	Avira	HEUR/AGEN.1137139		Download File
6.2.Y88576645635_03112021.PDF.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
6.2.Y88576645635_03112021.PDF.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
4.2.Y88576645635_03112021.PDF.exe.4455010.6.unpack	100%	Avira	TR/Inject.vcoldi		Download File

Domains

Source	Detection	Scanner	Label	Link
ftp.triplelink.co.th	2%	Virustotal		Browse
84.102.13.0.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.com#	0%	Virustotal		Browse
http://www.carterandcone.com#	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cne-d0	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.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr-u	0%	Avira URL Cloud	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.urwpp.de6	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.founder.com.cn/cnp	0%	Avira URL Cloud	safe	
http://www.fontbureau.com2	0%	Avira URL Cloud	safe	
http://www.founder.cg	0%	Avira URL Cloud	safe	
http://www.urwpp.deasu	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.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	

Source	Detection	Scanner	Label	Link
http://tempuri.org/XXXXXXXXXXXXXXXXXXXXXX.xsd	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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.sandoll.co.krt	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr-es_	0%	Avira URL Cloud	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.sandoll.co.krnotm	0%	Avira URL Cloud	safe	
http://www.urwpp.deF	0%	Avira URL Cloud	safe	
http://www.agfamonotype.L	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.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.urwpp.deic	0%	Avira URL Cloud	safe	
http://www.fontbureau.comionm	0%	Avira URL Cloud	safe	
http://ftp.triplelink.co.th	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.founder.com.cn/cn4	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/%	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnK	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ftp.triplelink.co.th	103.27.200.199	true	true	• 2%, Virustotal, Browse	unknown
84.102.13.0.in-addr.arpa	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.0000000005C90000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.0000000005C90000.00000002.00000001.sdmp	false		high

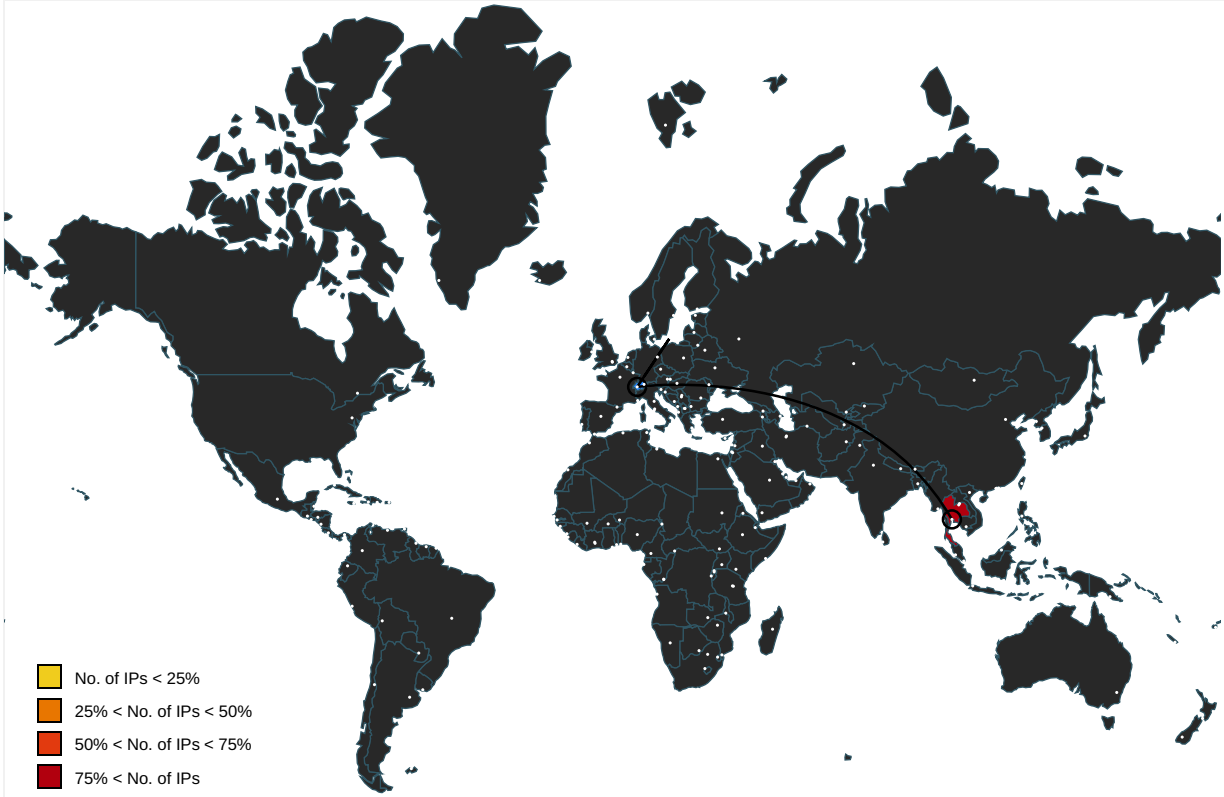
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.0 000000005C90000.00000002.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com#	Y88576645635_03112021.PDF.exe, 00000006.00000003.663058162.0 000000005B48000.00000004.00000 001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.0 000000005C90000.00000002.00000 001.sdmp	false		high
http://www.founder.com.cn/cne-d0	Y88576645635_03112021.PDF.exe, 00000006.00000003.662444137.0 000000005B4E000.00000004.00000 001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.0 000000005C90000.00000002.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.0 000000005C90000.00000002.00000 001.sdmp	false		high
http://www.goodfont.co.kr	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.0 000000005C90000.00000002.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr-u	Y88576645635_03112021.PDF.exe, 00000006.00000003.662151861.0 000000005B4E000.00000004.00000 001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com	Y88576645635_03112021.PDF.exe, 00000006.00000003.663167419.0 000000005B45000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Y88576645635_03112021.PDF.exe, 00000000.00000002.650605072.0 000000002B31000.00000004.00000 001.sdmp, Y88576645635_03112021.PDF.exe, 00000004.00000002.6 59715727.0000000002F91000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.0 000000005C90000.00000002.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.0 000000005C90000.00000002.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.0 000000005C90000.00000002.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.0 000000005C90000.00000002.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de6	Y88576645635_03112021.PDF.exe, 00000006.00000003.666196255.0 000000005B45000.00000004.00000 001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.0 000000005C90000.00000002.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comgrita	Y88576645635_03112021.PDF.exe, 00000006.00000002.903096798.0 000000001177000.00000004.00000 040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnp	Y88576645635_03112021.PDF.exe, 00000006.00000003.662444137.0 000000005B4E000.00000004.00000 001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com2	Y88576645635_03112021.PDF.exe, 00000006.00000002.903096798.0 000000001177000.00000004.00000 040.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.cg	Y88576645635_03112021.PDF.exe, 00000006.00000003.662492268.000000005B4E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deasu	Y88576645635_03112021.PDF.exe, 00000006.00000003.666502735.000000005B45000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com/-	Y88576645635_03112021.PDF.exe, 00000006.00000002.902253239.000000000402000.00000040.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.000000005C90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.yahoo.com/config/login	vbc.exe	false		high
http://www.fonts.com	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.000000005C90000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Y88576645635_03112021.PDF.exe, 00000006.00000003.662151861.000000005B4E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.site.com/logs.php	Y88576645635_03112021.PDF.exe, 00000006.00000002.903358748.000000002991000.00000004.00000001.sdmp	false		high
http://tempuri.org/XXXXXXXXXXXXXXXXXXXXXX.xsd	Y88576645635_03112021.PDF.exe, 00000004.00000002.658406658.000000000402000.00000040.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.000000005C90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	vbc.exe, vbc.exe, 0000000B.00000002.699152607.0000000004000000.00000040.00000001.sdmp	false		high
http://www.urwpp.de	Y88576645635_03112021.PDF.exe, 00000006.00000003.669939773.000000005B48000.00000004.00000001.sdmp, Y88576645635_03112021.PDF.exe, 00000006.00000003.669797236.0000000005B48000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.000000005C90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Y88576645635_03112021.PDF.exe, 00000000.00000002.650605072.000000002B31000.00000004.00000001.sdmp, Y88576645635_03112021.PDF.exe, 00000004.00000002.659715727.0000000002F91000.00000004.00000001.sdmp, Y88576645635_03112021.PDF.exe, 00000006.00000002.903358748.0000000002991000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.000000005C90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.000000005C90000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.000000005C90000.00000002.00000001.sdmp, Y88576645635_03112021.PDF.exe, 00000006.00000002.903096798.0000000001177000.00000004.00000040.sdmp	false		high
http://www.galapagosdesign.com/	Y88576645635_03112021.PDF.exe, 00000006.00000003.675783220.000000005B48000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.krt	Y88576645635_03112021.PDF.exe, 00000006.00000003.662151861.000000005B4E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr-es_	Y88576645635_03112021.PDF.exe, 00000006.00000003.662151861.000000005B4E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.c	Y88576645635_03112021.PDF.exe, 00000006.00000003.662492268.000000005B4E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krnotm	Y88576645635_03112021.PDF.exe, 00000006.00000003.662151861.000000005B4E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlx	Y88576645635_03112021.PDF.exe, 00000006.00000003.668835911.000000005B48000.00000004.00000001.sdmp	false		high
http://www.urwpp.deF	Y88576645635_03112021.PDF.exe, 00000006.00000003.669858103.000000005B48000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.agfamonotype.L	Y88576645635_03112021.PDF.exe, 00000006.00000003.678715082.000000005B48000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.000000005C90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	Y88576645635_03112021.PDF.exe, 00000006.00000003.662579211.000000005B45000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.000000005C90000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	Y88576645635_03112021.PDF.exe, 00000006.00000003.662444137.000000005B4E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Y88576645635_03112021.PDF.exe, 00000006.00000003.667638331.000000005B47000.00000004.00000001.sdmp, Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.0000000005C90000.00000002.00000001.sdmp	false		high
http://www.urwpp.deic	Y88576645635_03112021.PDF.exe, 00000006.00000003.666257144.000000005B45000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	Y88576645635_03112021.PDF.exe, 00000006.00000003.669031244.000000005B48000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comionm	Y88576645635_03112021.PDF.exe, 00000006.00000002.903096798.000000001177000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://ftp.triplelink.co.th	Y88576645635_03112021.PDF.exe, 00000006.00000002.903800843.000000002BBE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.000000005C90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn4	Y88576645635_03112021.PDF.exe, 00000006.00000003.662444137.000000005B4E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	Y88576645635_03112021.PDF.exe, 00000006.00000002.906936323.000000005C90000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/%	Y88576645635_03112021.PDF.exe, 00000006.00000003.675783220.000000005B48000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	Y88576645635_03112021.PDF.exe, 00000006.00000003.666502735.000000005B45000.00000004.00000001.sdmp	false		high
http://www.zhongyicts.com.cnK	Y88576645635_03112021.PDF.exe, 00000006.00000003.662850878.000000005B48000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.27.200.199	ftp.triplelink.co.th	Thailand		58955	BANGMODENTERPRISE-THBangmodEnterpriseCoLtdTH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	367711
Start date:	12.03.2021
Start time:	02:10:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 34s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	Y88576645635_03112021.PDF.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:	23
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@15/4@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.4% (good quality ratio 5.5%) • Quality average: 66.6% • Quality standard deviation: 35.2%
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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 52.255.188.83, 51.104.139.180, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, au.download.windowsupdate.com.edgesuite.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
02:11:25	API Interceptor	7x Sleep call for process: Y88576645635_03112021.PDF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.27.200.199	K409476485-03032021000.pdf.exe	Get hash	malicious	Browse	
	Vkdr225E85.exe	Get hash	malicious	Browse	
	071020207659825.PDF.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	103002994-05102020.PDF.exe	Get hash	malicious	Browse	
	1110975-0080620.PDF.exe	Get hash	malicious	Browse	
	l0185766832020805.PDF.exe	Get hash	malicious	Browse	
	008042020786544141.PDF.exe	Get hash	malicious	Browse	
	dHXjzn9Z5w.exe	Get hash	malicious	Browse	
	O7292020987725545.PDF.exe	Get hash	malicious	Browse	
	98764737722.PDF.exe	Get hash	malicious	Browse	
	gunzipped.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ftp.triplelink.co.th	K409476485-03032021000.pdf.exe	Get hash	malicious	Browse	• 103.27.200.199
	Vkdr225E85.exe	Get hash	malicious	Browse	• 103.27.200.199
	071020207659825.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	file.exe	Get hash	malicious	Browse	• 103.27.200.199
	103002994-05102020.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	1110975-0080620.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	l0185766832020805.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	008042020786544141.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	dHXjzn9Z5w.exe	Get hash	malicious	Browse	• 103.27.200.199
	O7292020987725545.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	98764737722.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	gunzipped.exe	Get hash	malicious	Browse	• 103.27.200.199

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BANGMODENTERPRISE-THBangmodEnterpriseCoLtdTH	CHANG 290386.exe	Get hash	malicious	Browse	• 103.27.200.68
	K409476485-03032021000.pdf.exe	Get hash	malicious	Browse	• 103.27.200.199
	Vkdr225E85.exe	Get hash	malicious	Browse	• 103.27.200.199
	WfSx9pJXxf.exe	Get hash	malicious	Browse	• 103.86.49.11
	l9ZtB4c9Gj.exe	Get hash	malicious	Browse	• 103.86.49.11
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 45.64.187.182
	071020207659825.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	file.exe	Get hash	malicious	Browse	• 103.27.200.199
	103002994-05102020.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	BAL_0MX2NTOGM6VL9.doc	Get hash	malicious	Browse	• 45.64.185.141
	1110975-0080620.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	l0185766832020805.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	008042020786544141.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	dHXjzn9Z5w.exe	Get hash	malicious	Browse	• 103.27.200.199
	O7292020987725545.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	98764737722.PDF.exe	Get hash	malicious	Browse	• 103.27.200.199
	gunzipped.exe	Get hash	malicious	Browse	• 103.27.200.199
	Christmas Greeting eCard.doc	Get hash	malicious	Browse	• 103.27.201.8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Christmas Greeting eCard.doc	Get hash	malicious	Browse	• 103.27.201.8
	Christmas Greeting eCard.doc	Get hash	malicious	Browse	• 103.27.201.8

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Y88576645635_03112021.PDF.exe.log	
Process:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:fT:7
MD5:	6107D91FC9A0B04BC044AA7D8C1443BD
SHA1:	5908618DF3DA243BDBA2C6C2C586222C32A017E0

C:\Users\user\AppData\Roaming\pid.txt	
SHA-256:	B0BAE7AAE64B82780025D6B79916D0D75D708C5B232EB03813DA7FED7AEC54C6
SHA-512:	7B143D6442BDB99690F6A23AAAF9F6270944725FE21E7E55DBC880E2DF40E53E32C8790664F623DAC79EA74EC0BCB46B153A6F10D37683D17F4613AEB1BD81B7
Malicious:	false
Reputation:	low
Preview:	6316

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	52
Entropy (8bit):	4.6259338915848
Encrypted:	false
SSDEEP:	3:oNt+WfW8fHf1TOVUkA:oNwv8f/16VxA
MD5:	5D5E400AE0E8075A1EB45B1A77B8B764
SHA1:	97E120B26B294250BEC1DD7F3843310C0D452CFF
SHA-256:	E192947818C79EDD5D3A95E02D70065C2C3307353E3E408F4FF11BB69F9FED4C
SHA-512:	6125C4F6D7E18035C7732763C6587AFE484FB2B4FC63D77EB6397442978F7D004E378D9A2FD370701F4366CBC7F22D433BB08DDF558108D42FC4521970FEC48D
Malicious:	false
Reputation:	low
Preview:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.939398616269563
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Y88576645635_03112021.PDF.exe
File size:	1821696
MD5:	4f0fdcac715b3d952ffab9e7d3ee86ac
SHA1:	1079108984d0587302e2576c6e72c18a1021154b
SHA256:	047d3bebe340180add07832e734233f7aa762de34f1eca2b5059d48a2daca6bc
SHA512:	bd12f34e1ea80e2d9959c1d549cf0ee872b4327c7704d135e9be619fe392636c6462086a1e2876bd5346e0b6b4e14b51020a3b088687d6b4586d443a2c37e09c
SSDEEP:	49152:0cyb8nxp8HA+bY+hHUsP3DOl7ZUzsajRaWOegWb:BLxp8HrDHUsPJznjDOegW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....I`.....P..8.....V... ...`....@.. ....@.....

File Icon

Icon Hash:	83ccb4ecec878dd1

Static PE Info

General

Entrypoint:	0x5b562e
Entrypoint Section:	.text

General

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:	0x6049BA19 [Thu Mar 11 06:35:05 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1b55dc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1b6000	0x8e20	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1c0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	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	0x1b3634	0x1b3800	False	0.940840045565	data	7.94979367637	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x1b6000	0x8e20	0x9000	False	0.293104383681	data	6.32293632445	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1c0000	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	0x1b61f0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 50331648		
RT_ICON	0x1ba418	0x25a8	data		
RT_ICON	0x1bc9c0	0x10a8	data		
RT_ICON	0x1bda68	0x988	data		
RT_ICON	0x1be3f0	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1be858	0x4c	data		
RT_VERSION	0x1be8a4	0x38a	data		
RT_MANIFEST	0x1bec30	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

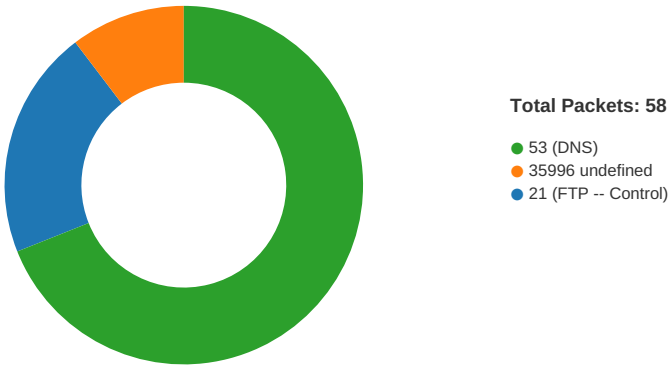
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	2016 TypeLoadException
Assembly Version	16.8.11.18
InternalName	ApplicationIdentity.exe
FileVersion	16.8.11.18
CompanyName	TypeLoadException
LegalTrademarks	NavBar
Comments	
ProductName	NavBar
ProductVersion	16.8.11.18
FileDescription	NavBar
OriginalFilename	ApplicationIdentity.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
03/12/21-02:12:02.718886	TCP	2020410	ET TROJAN HawkEye Keylogger FTP	49749	21	192.168.2.4	103.27.200.199

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 12, 2021 02:11:59.800307035 CET	49749	21	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:00.093427896 CET	21	49749	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:00.093564034 CET	49749	21	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:00.391424894 CET	21	49749	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:00.392848015 CET	49749	21	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:00.703134060 CET	21	49749	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:00.703203917 CET	21	49749	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:00.707108021 CET	49749	21	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:01.048357010 CET	21	49749	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:01.048722982 CET	49749	21	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:01.397772074 CET	21	49749	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:01.398664951 CET	49749	21	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:01.755841970 CET	21	49749	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:01.756288052 CET	49749	21	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:02.095961094 CET	21	49749	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:02.096210957 CET	49749	21	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:02.420974016 CET	21	49749	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:02.421894073 CET	49750	35996	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:02.466784954 CET	49749	21	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:02.718539953 CET	35996	49750	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:02.718642950 CET	49750	35996	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:02.718885899 CET	49749	21	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:02.997607946 CET	21	49749	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:02.998687983 CET	49750	35996	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:03.004828930 CET	49750	35996	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:03.006773949 CET	49750	35996	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:03.044985056 CET	49749	21	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:03.271217108 CET	35996	49750	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:03.277204990 CET	35996	49750	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:03.277251959 CET	35996	49750	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:03.280333042 CET	35996	49750	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:03.280426979 CET	49750	35996	192.168.2.4	103.27.200.199
Mar 12, 2021 02:12:03.284754992 CET	21	49749	103.27.200.199	192.168.2.4
Mar 12, 2021 02:12:03.326284885 CET	49749	21	192.168.2.4	103.27.200.199

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 12, 2021 02:11:18.834980965 CET	59123	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:18.886647940 CET	53	59123	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:20.039439917 CET	54531	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:20.091913939 CET	53	54531	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:21.360070944 CET	49714	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:21.408811092 CET	53	49714	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:22.880412102 CET	58028	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:22.931607962 CET	53	58028	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:24.165766001 CET	53097	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:24.215930939 CET	53	53097	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:25.439687967 CET	49257	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:25.491215944 CET	53	49257	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:26.707967043 CET	62389	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:26.760355949 CET	53	62389	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:27.875890017 CET	49910	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:27.928554058 CET	53	49910	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:29.201910019 CET	55854	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:29.259557962 CET	53	55854	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:30.479374886 CET	64549	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:30.536385059 CET	53	64549	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:31.840060949 CET	63153	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:31.889512062 CET	53	63153	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:33.145288944 CET	52991	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:33.194298029 CET	53	52991	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:34.508697033 CET	53700	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:34.560038090 CET	53	53700	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:35.409905910 CET	51726	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:35.462054014 CET	53	51726	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:36.570456982 CET	56794	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:36.632522106 CET	53	56794	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:37.395400047 CET	56534	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:37.455295086 CET	53	56534	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:38.729446888 CET	56627	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:38.781176090 CET	53	56627	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:39.959359884 CET	56621	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:40.008114100 CET	53	56621	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:42.637505054 CET	63116	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:42.691395998 CET	53	63116	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:44.538364887 CET	64078	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:44.595468998 CET	53	64078	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:47.273685932 CET	64801	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:47.322510958 CET	53	64801	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:53.226907015 CET	61721	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:53.290183067 CET	53	61721	8.8.8.8	192.168.2.4
Mar 12, 2021 02:11:58.387563944 CET	51255	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:11:58.786683083 CET	53	51255	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:08.398677111 CET	61522	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:08.484458923 CET	53	61522	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:09.071412086 CET	52337	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:09.131874084 CET	53	52337	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:09.525918007 CET	55046	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:09.595689058 CET	49612	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:09.616827965 CET	53	55046	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:09.655728102 CET	53	49612	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:10.136986971 CET	49285	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:10.196722984 CET	53	49285	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:10.818593025 CET	50601	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:11.004805088 CET	53	50601	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:11.619841099 CET	60875	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:11.676985025 CET	53	60875	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:12.180793047 CET	56448	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:12.232453108 CET	53	56448	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:12.521667004 CET	59172	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:12.571964025 CET	53	59172	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 12, 2021 02:12:13.062041998 CET	62420	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:13.123425007 CET	53	62420	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:14.159763098 CET	60579	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:14.217411041 CET	53	60579	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:14.742012978 CET	50183	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:14.802248955 CET	53	50183	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:22.957071066 CET	61531	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:22.982532978 CET	49228	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:23.006947994 CET	53	61531	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:23.040098906 CET	53	49228	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:25.751055002 CET	59794	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:25.811125040 CET	53	59794	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:57.370394945 CET	55916	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:57.420788050 CET	53	55916	8.8.8.8	192.168.2.4
Mar 12, 2021 02:12:59.168704987 CET	52752	53	192.168.2.4	8.8.8.8
Mar 12, 2021 02:12:59.236057043 CET	53	52752	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 12, 2021 02:11:44.538364887 CET	192.168.2.4	8.8.8.8	0x58bb	Standard query (0)	84.102.13.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Mar 12, 2021 02:11:58.387563944 CET	192.168.2.4	8.8.8.8	0x23b6	Standard query (0)	ftp.triplelink.co.th	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 12, 2021 02:11:44.595468998 CET	8.8.8.8	192.168.2.4	0x58bb	Name error (3)	84.102.13.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Mar 12, 2021 02:11:58.786683083 CET	8.8.8.8	192.168.2.4	0x23b6	No error (0)	ftp.triplelink.co.th		103.27.200.199	A (IP address)	IN (0x0001)

FTP Packets

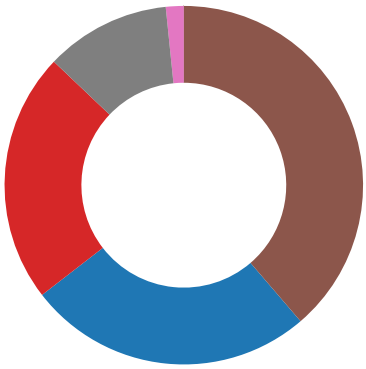
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Mar 12, 2021 02:12:00.391424894 CET	21	49749	103.27.200.199	192.168.2.4	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 2 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 2 of 50 allowed.220-Local time is now 08:08. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 2 of 50 allowed.220-Local time is now 08:08. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 2 of 50 allowed.220-Local time is now 08:08. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 2 of 50 allowed.220-Local time is now 08:08. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
Mar 12, 2021 02:12:00.392848015 CET	49749	21	192.168.2.4	103.27.200.199	USER Loggsszzzxxx@triplelink.co.th
Mar 12, 2021 02:12:00.703203917 CET	21	49749	103.27.200.199	192.168.2.4	331 User Loggsszzzxxx@triplelink.co.th OK. Password required
Mar 12, 2021 02:12:00.707108021 CET	49749	21	192.168.2.4	103.27.200.199	PASS xpen2000
Mar 12, 2021 02:12:01.048357010 CET	21	49749	103.27.200.199	192.168.2.4	230-This server supports FXP transfers 230-This server supports FXP transfers230 OK. Current restricted directory is /
Mar 12, 2021 02:12:01.397772074 CET	21	49749	103.27.200.199	192.168.2.4	504 Unknown command
Mar 12, 2021 02:12:01.398664951 CET	49749	21	192.168.2.4	103.27.200.199	PWD
Mar 12, 2021 02:12:01.755841970 CET	21	49749	103.27.200.199	192.168.2.4	257 "/" is your current location
Mar 12, 2021 02:12:01.756288052 CET	49749	21	192.168.2.4	103.27.200.199	TYPE I
Mar 12, 2021 02:12:02.095961094 CET	21	49749	103.27.200.199	192.168.2.4	200 TYPE is now 8-bit binary
Mar 12, 2021 02:12:02.096210957 CET	49749	21	192.168.2.4	103.27.200.199	PASV
Mar 12, 2021 02:12:02.420974016 CET	21	49749	103.27.200.199	192.168.2.4	227 Entering Passive Mode (103,27,200,199,140,156)
Mar 12, 2021 02:12:02.718885899 CET	49749	21	192.168.2.4	103.27.200.199	STOR HawkEye_Keylogger_Stealer_Records_878164 3.12.2021 2:19:37 AM.txt
Mar 12, 2021 02:12:02.997607946 CET	21	49749	103.27.200.199	192.168.2.4	150 Accepted data connection

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Mar 12, 2021 02:12:03.284754992 CET	21	49749	103.27.200.199	192.168.2.4	226-File successfully transferred 226-File successfully transferred226 0.288 seconds (measured here), 5.18 Kbytes per second

Code Manipulations

Statistics

Behavior



- Y88576645635_03112021.PDF.exe
- Y88576645635_03112021.PDF.exe
- Y88576645635_03112021.PDF.exe
- Y88576645635_03112021.PDF.exe
- Y88576645635_03112021.PDF.exe
- Y88576645635_03112021.PDF.exe
- vbc.exe
- vbc.exe

Click to jump to process

System Behavior

Analysis Process: Y88576645635_03112021.PDF.exe PID: 7100 Parent PID: 5976

General

Start time:	02:11:23
Start date:	12/03/2021
Path:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe'
Imagebase:	0x610000
File size:	1821696 bytes
MD5 hash:	4F0FDCAC715B3D952FFAB9E7D3EE86AC
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: 00000000.00000002.650605072.0000000002B31000.00000004.00000001.sdmp, Author: Joe Security
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	6D3DCF06	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	6D3DCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Y88576645635_03112021.PDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Y88576645635_03112021.PDF.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D6EC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: Y88576645635_03112021.PDF.exe PID: 244 Parent PID: 7100

General

Start time:	02:11:26
Start date:	12/03/2021
Path:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
Imagebase:	0x220000
File size:	1821696 bytes
MD5 hash:	4F0FDCAC715B3D952FFAB9E7D3EE86AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Y88576645635_03112021.PDF.exe PID: 3436 Parent PID: 7100

General

Start time:	02:11:27
Start date:	12/03/2021
Path:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
Imagebase:	0x4f0000
File size:	1821696 bytes
MD5 hash:	4F0FDCAC715B3D952FFAB9E7D3EE86AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Y88576645635_03112021.PDF.exe PID: 6596 Parent PID: 7100

General

Start time:	02:11:28
Start date:	12/03/2021
Path:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
Imagebase:	0xa40000
File size:	1821696 bytes
MD5 hash:	4F0FDCAC715B3D952FFAB9E7D3EE86AC
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: 00000004.00000002.659715727.0000000002F91000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000004.00000002.661841679.0000000003F99000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000002.661841679.0000000003F99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000002.661841679.0000000003F99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000002.661841679.0000000003F99000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000002.661841679.0000000003F99000.00000004.00000001.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	6D3DCF06	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	6D3DCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: Y88576645635_03112021.PDF.exe PID: 5912 Parent PID: 6596

General

Start time:	02:11:31
Start date:	12/03/2021
Path:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
Imagebase:	0x300000

File size:	1821696 bytes
MD5 hash:	4F0FDCAC715B3D952FFAB9E7D3EE86AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Y88576645635_03112021.PDF.exe PID: 6316 Parent PID: 6596

General

Start time:	02:11:32
Start date:	12/03/2021
Path:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Y88576645635_03112021.PDF.exe
Imagebase:	0x540000
File size:	1821696 bytes
MD5 hash:	4F0FDCAC715B3D952FFAB9E7D3EE86AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000006.00000002.908387169.0000000008090000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000006.00000002.902253239.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000002.902253239.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000006.00000002.902253239.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000002.902253239.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000006.00000002.902253239.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000002.904321418.0000000003991000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000002.904321418.0000000003991000.00000004.00000001.sdmp, Author: Joe Security • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000006.00000002.908411308.00000000081F0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000006.00000002.903358748.0000000002991000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000006.00000002.903358748.0000000002991000.00000004.00000001.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	6D3DCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D3DCF06	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	6C221E60	CreateFileW
C:\Users\user\AppData\Roaming\pidloc.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	6C226A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	6C226A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	36 33 31 36	6316	success or wait	1	6C221B4F	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	52	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 59 38 38 35 37 36 36 34 35 36 33 35 5f 30 33 31 31 32 30 32 31 2e 50 44 46 2e 65 78 65	C:\Users\user\Desktop\Y8857664 5635_03112021.PDF.exe	success or wait	1	6C221B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	6C221B4F	ReadFile

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	6C22C075	RegSetValueExW

Analysis Process: vbc.exe PID: 6896 Parent PID: 6316

General

Start time:	02:11:49
Start date:	12/03/2021
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: 0000000A.00000002.696473559.0000000000400000.00000040.00000001.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: 6880 Parent PID: 6316

General

Start time:	02:11:49
Start date:	12/03/2021
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: 0000000B.00000002.699152607.0000000000400000.00000040.00000001.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