ID: 473673
Sample Name: 300821.PDF.exe
Cookbook: default.jbs
Time: 06:54:09
Date: 30/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 300821.PDF.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: HawkEye 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
System Summary: 5
Data Obfuscation: 5
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
Private 10
General Information 10
Simulations 10
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 13
General 13
File Icon 13
Network Behavior 14
Snort IDS Alerts 14
Network Port Distribution 14
TCP Packets 14
UDP Packets 14
DNS Queries 14
DNS Answers 14
FTP Packets 14
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: 300821.PDF.exe PID: 4816 Parent PID: 6592 15
General 15
File Activities 16
File Created 16
File Written 16
File Read 16
Analysis Process: 300821.PDF.exe PID: 2848 Parent PID: 4816 16

General 16
File Activities 17
File Created 17
File Deleted 17
File Written 17
File Read 17
Registry Activities 17
Key Value Modified 17
Analysis Process: vbc.exe PID: 1668 Parent PID: 2848 17
General 17
File Activities 17
File Created 17
File Deleted 18
File Written 18
File Read 18
Analysis Process: vbc.exe PID: 5604 Parent PID: 2848 18
General 18
File Activities 18
File Created 18
Disassembly 18
Code Analysis 18

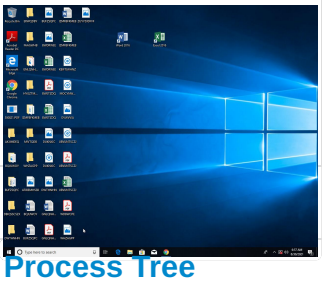
Windows Analysis Report 300821.PDF.exe

Overview

General Information

Sample Name:	300821.PDF.exe
Analysis ID:	473673
MD5:	ddfc57b8fd3e5e0..
SHA1:	ca35000ed1844f3.
SHA256:	c1cd0692836798..
Tags:	exe hawkeye
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

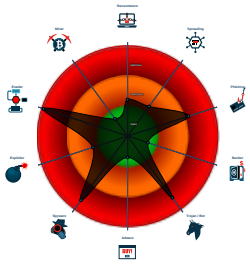
HawkEye
MailPassView

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

Signatures

- Found malware configuration
- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e.…
- Yara detected MailPassView
- Multi AV Scanner detection for subm…
- Yara detected HawkEye Keylogger
- Malicious sample detected (through …
- Yara detected AntiVM3
- Detected HawkEye Rat
- Sample uses process hollowing tech…
- Initial sample is a PE file and has a …
- .NET source code references suspic…

Classification



Process Tree

- **System is w10x64**
- 300821.PDF.exe (PID: 4816 cmdline: 'C:\Users\user\Desktop\300821.PDF.exe' MD5: DDFC57B8FD3E5E0F81DEE8EAD0E38518)
  - 300821.PDF.exe (PID: 2848 cmdline: C:\Users\user\Desktop\300821.PDF.exe MD5: DDFC57B8FD3E5E0F81DEE8EAD0E38518)
    - vbc.exe (PID: 1668 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 5604 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

Threatname: HawkEye

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.665567909.0000000002FA5000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000009.00000002.684649797.0000000000400000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000008.00000002.693074434.0000000000400000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.916254009.0000000003B61000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000005.00000002.916254009.0000000003B61000.00000004.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.300821.PDF.exe.45fa72.1.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
9.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
5.2.300821.PDF.exe.3b69930.8.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
5.2.300821.PDF.exe.409c0d.3.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
9.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 73 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

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:

.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 AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Sample uses process hollowing technique

.NET source code references suspicious native API functions

Stealing of Sensitive Information:

Yara detected MailPassView

Yara detected HawkEye Keylogger

Tries to steal Mail credentials (via file registry)

Yara detected WebBrowserPassView password recovery tool

Tries to steal Mail credentials (via file access)

Tries to steal Instant Messenger accounts or passwords

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

Remote Access Functionality:

Yara detected HawkEye Keylogger

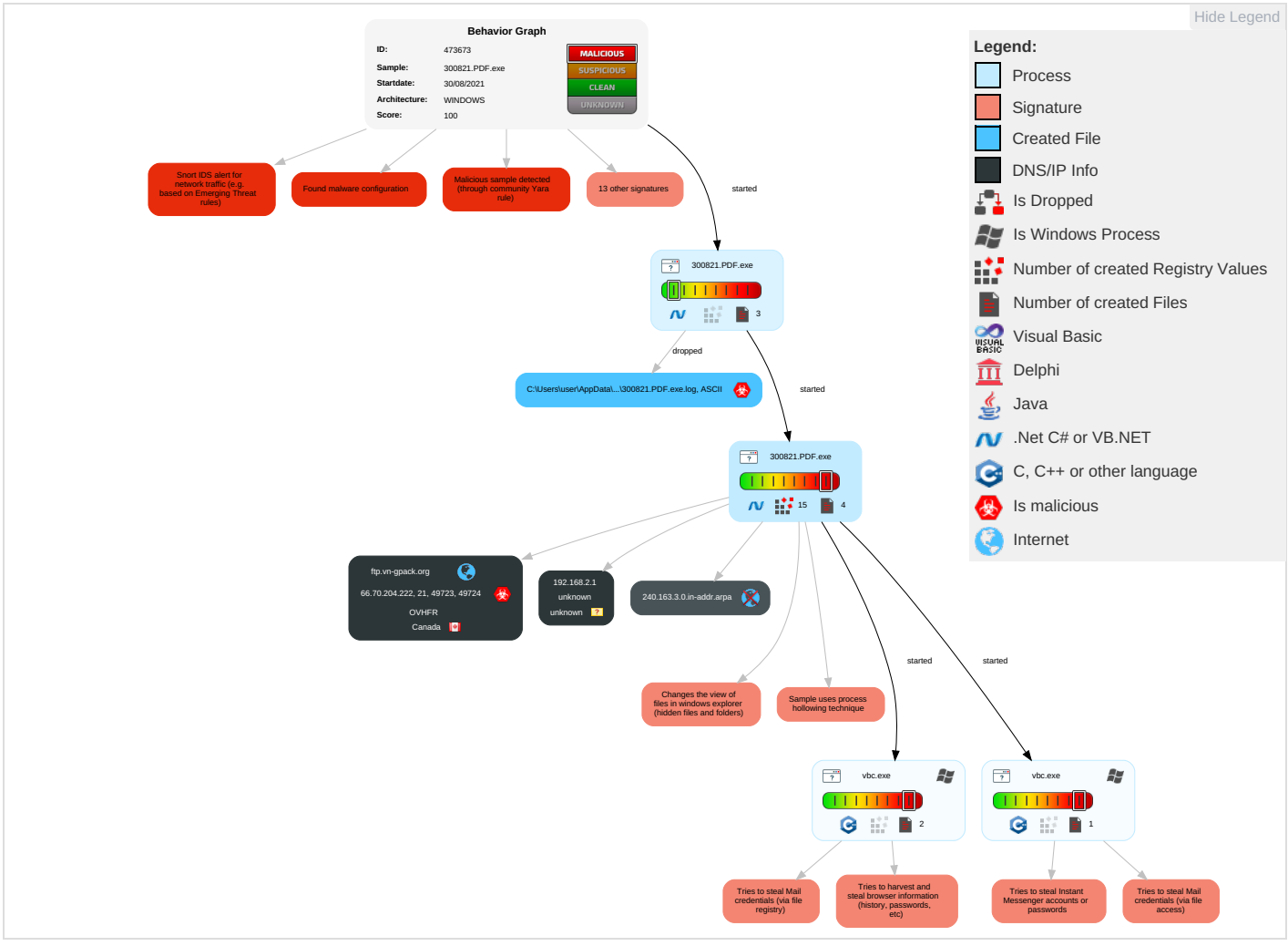
Detected HawkEye Rat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
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	Encr Char
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 1 1 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Non-Port
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	Rem Softw
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	Credentials In Files 1	File and Directory Discovery 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Non-Appl Laye Prot
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	Appl Laye Prot
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 4 1	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Com

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 1	DCSync	Security Software Discovery 1 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Virtualization/Sandbox Evasion 4 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appl Laye
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Process Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
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	File Prot
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	Mail
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	DNS

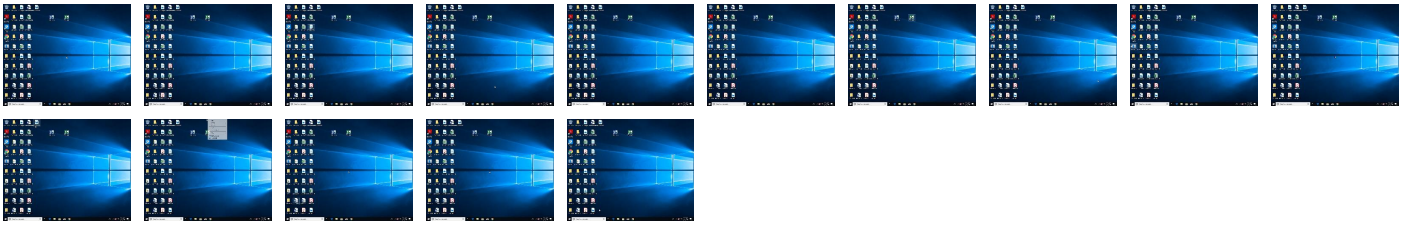
Behavior Graph



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
300821.PDF.exe	22%	ReversingLabs	ByteCode-MSIL.Infostealer.Heye	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.300821.PDF.exe.4d2ad28.6.unpack	100%	Avira	TR/Inject.vcoldi		Download File
5.2.300821.PDF.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
5.2.300821.PDF.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Domains

Source	Detection	Scanner	Label	Link
ftp.vn-gpack.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6Ijk4OGQ1ZDgwMWE2ODQ2NDNkM2ZkMmYyMGEwOTgwMWQ3MDE2Z	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000/Converged_v21033_-0mnSwu67knBd7qR7YN9GQ2.css	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b5	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e	0%	Avira URL Cloud	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://https://172.217.23.78/	0%	Avira URL Cloud	safe	
http://https://aefd.nelreports.net/api/report?cat=bingrms	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImYxODk5OTBhOWZjYjFmZjNjNmMxNDhmYjkzM2M3NzY1Mzk3Z	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://adservice.google.co.uk/adsid/google/ui?gadsid=AORoGNQXg7AHkvg6J6S0TqGFa_0HynGV3_XxYfs4fLINJG	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjJkYTFhZDAwNDEyNzQ2M2E3MGUyMWVkZmIxNmUyZjQ2MjBkM	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000/content/js/ConvergedLoginPaginatedStrings.en_5QoHC_ilFOmb96M0pIeJ	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000/content/js/OldConvergedLogin_PCore_xqcDwEKeDux9oCNjuqEZ-A2.js	0%	URL Reputation	safe	
http://cookies.onetrust.mgr.consensu.org/onetrust-logo.svg	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28230.00/images/microsoft_logo.svg?x=ee5c8d9fb6248c938fd0dc19370e	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.28230.00/ConvergedLogin_PCore.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ftp.vn-gpack.org	66.70.204.222	true	true	• 1%, Virustotal, Browse	unknown
240.163.3.0.in-addr.arpa	unknown	unknown	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.70.204.222	ftp.vn-gpack.org	Canada		16276	OVHFR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	473673
Start date:	30.08.2021
Start time:	06:54:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	300821.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:	20
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@7/5@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 98.9% (good quality ratio 95.9%) • Quality average: 85.6% • Quality standard deviation: 23.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
06:55:04	API Interceptor	6x Sleep call for process: 300821.PDF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.70.204.222	Dolmas.xlsm.exe	Get hash	malicious	Browse	• tesla-com .tk/Awele/ SINOPHIL@LOKIRAW_HGiTKz109.bin
	eurobank.pdf.exe	Get hash	malicious	Browse	• tesla-com .tk/ford/SINOPHIL@LOKIRAW_GCLYOSF135.bin

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	sx5Yixa5GO.exe	Get hash	malicious	Browse	• 158.69.65.151
	fzUNUBx4wC.exe	Get hash	malicious	Browse	• 158.69.65.151
	DpO9nEw19q.exe	Get hash	malicious	Browse	• 158.69.65.151
	d6Q0sXQjkY.exe	Get hash	malicious	Browse	• 158.69.65.151
	VoFsQd7jwx.exe	Get hash	malicious	Browse	• 158.69.65.151
	waKnA3vFb3	Get hash	malicious	Browse	• 79.137.66.196
	xQDLIutCAU.exe	Get hash	malicious	Browse	• 158.69.65.151
	io9rjV248Z.exe	Get hash	malicious	Browse	• 158.69.65.151
	LeSA7F7a96.exe	Get hash	malicious	Browse	• 158.69.65.151
	loligang.arm	Get hash	malicious	Browse	• 92.246.246.95
	sG41vsm1Pe.exe	Get hash	malicious	Browse	• 158.69.65.151
	0tLYXVrJOe.exe	Get hash	malicious	Browse	• 158.69.65.151
	RyGaFxV75v.exe	Get hash	malicious	Browse	• 158.69.65.151
	uvVLne3r48.exe	Get hash	malicious	Browse	• 158.69.65.151
	gMWaIDKK37.exe	Get hash	malicious	Browse	• 158.69.65.151
	hsRrR2KPY7.exe	Get hash	malicious	Browse	• 158.69.65.151
	pCSou0ozZy.exe	Get hash	malicious	Browse	• 158.69.65.151
	ZUd8KSXXVD.exe	Get hash	malicious	Browse	• 158.69.65.151
	FWXckJ56fn.exe	Get hash	malicious	Browse	• 158.69.65.151
	k2vbB70cV7.exe	Get hash	malicious	Browse	• 158.69.65.151

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\300821.PDF.exe.log	
Process:	C:\Users\user\Desktop\300821.PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\bhvE2B1.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x6c81e4e3, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	29884416
Entropy (8bit):	1.0563745804808284
Encrypted:	false
SSDEEP:	24576:GjbVPt8HVmyvYw781dfXy7R4aUpPX7Cr6f63rsLOZgv:8NyvArO0v
MD5:	AB607EDB401FC1704B6A7FA5E5208D71
SHA1:	747438185721FADCD454E338D8F5B45E47D56336
SHA-256:	D4786F79983EDE99BE61190781F57AF3A290175F890D3CB09CB2F963A20BACFF
SHA-512:	7B7490EDD7BFD6E3B86BCCFB463EF67D072DABBE894678337A5F047316A0FBD542CC215B30A61915F383F102CF5E8AE69A992A7296D2EDE536A78CD7C29CF90
Malicious:	false
Reputation:	low
Preview:	l..... .....?....._e..*....w.....^.8.....;#...xE.-6...yQ.h.:.....b...*....w.....{.....B..... ....36...y..... .....AI.7...y.....7...y..... .....

C:\Users\user\AppData\Local\Temp\holderwb.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\Desktop\300821.PDF.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5

C:\Users\user\AppData\Roaming\pid.txt	
Encrypted:	false
SSDEEP:	3:Dd:B
MD5:	5A2756A3CB9CDE852CAD3C97E120B656
SHA1:	1BA65BC81EE7D284E60782ECD3308EC517B73B82
SHA-256:	95F180E417E425F00E97C5A95BFE534C0B1C90D9D8115C9ACAD2C04C8D6CB246
SHA-512:	06BFD8C0391AB013E57F0B422A2AFDF73C810ABC0AFFE45717EAAA5FD68F0BCDA8D26D42F6B064D693951C9C481E466393DA2020D2F82F898EF84BB343516F74
Malicious:	false
Reputation:	low
Preview:	2848

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\Desktop\300821.PDF.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.247030650103631
Encrypted:	false
SSDEEP:	3:oNt+WfWWVEXoA:oNwvWVmoA
MD5:	132D6BAEE131E302BCF347807AA06DE3
SHA1:	0CC45AF10E562B4D26A27A5B6731FCFCC7DC6F01
SHA-256:	9DE550232E6E9D639391A3D4A1E7A8B3F745B822D43856C562F5DD7439F5EB93
SHA-512:	C32670ADCB6E052B3909B9837E7BDD72E89BBEA23B806B16E44C49486EF92A795DED85880D15E836088D1EF80F1D5556B03E5A7CC0B0ACE80844677CFF7E2DE
Malicious:	false
Reputation:	low
Preview:	C:\Users\user\Desktop\300821.PDF.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.076704069722482
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:	300821.PDF.exe
File size:	987136
MD5:	ddfc57b8fd3e5e0f81dee8ead0e38518
SHA1:	ca35000ed1844f30e932d8903633e4beb519967f
SHA256:	c1cd0692836798f5cb7e9335f4547a2650b77cf456193cbe7e384906a20c0603
SHA512:	083bc3c27ddefbf541b91ef71728a2e3831563be171f4d7ca63dea9e04357533d2bf345c7ccdced551cc8220826d79f894b43f1de2ae8d3fd17a39c1bf838fcc
SSDEEP:	12288:MeTvtJpA3OXv2BFokZRhXQ5TZaRPlPO0E09wrp:MeDtJSO/2ffxA5TZaP20Eh9
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....",a.....0.....$.. .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/30/21-06:55:26.317879	TCP	2020410	ET TROJAN HawkEye Keylogger FTP	49723	21	192.168.2.4	66.70.204.222

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 30, 2021 06:55:09.080276966 CEST	192.168.2.4	8.8.8.8	0x9257	Standard query (0)	240.163.3.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 30, 2021 06:55:25.124269009 CEST	192.168.2.4	8.8.8.8	0xc7d5	Standard query (0)	ftp.vn-gpack.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 30, 2021 06:55:09.113172054 CEST	8.8.8.8	192.168.2.4	0x9257	Name error (3)	240.163.3.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Aug 30, 2021 06:55:17.953084946 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 30, 2021 06:55:25.328469038 CEST	8.8.8.8	192.168.2.4	0xc7d5	No error (0)	ftp.vn-gpack.org		66.70.204.222	A (IP address)	IN (0x0001)

FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 30, 2021 06:55:25.554527044 CEST	21	49723	66.70.204.222	192.168.2.4	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 5 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 5 of 50 allowed.220-Local time is now 08:55. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 5 of 50 allowed.220-Local time is now 08:55. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 5 of 50 allowed.220-Local time is now 08:55. 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 5 of 50 allowed.220-Local time is now 08:55. 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.
Aug 30, 2021 06:55:25.555402994 CEST	49723	21	192.168.2.4	66.70.204.222	USER Nwwwlooggs@vn-gpack.org
Aug 30, 2021 06:55:25.661725044 CEST	21	49723	66.70.204.222	192.168.2.4	331 User Nwwwlooggs@vn-gpack.org OK. Password required
Aug 30, 2021 06:55:25.661969900 CEST	49723	21	192.168.2.4	66.70.204.222	PASS @!V8[3L!PsE1
Aug 30, 2021 06:55:25.780798912 CEST	21	49723	66.70.204.222	192.168.2.4	230 OK. Current restricted directory is /
Aug 30, 2021 06:55:25.887681007 CEST	21	49723	66.70.204.222	192.168.2.4	504 Unknown command
Aug 30, 2021 06:55:25.888890028 CEST	49723	21	192.168.2.4	66.70.204.222	PWD
Aug 30, 2021 06:55:25.995340109 CEST	21	49723	66.70.204.222	192.168.2.4	257 "/" is your current location
Aug 30, 2021 06:55:25.995663881 CEST	49723	21	192.168.2.4	66.70.204.222	TYPE I
Aug 30, 2021 06:55:26.102369070 CEST	21	49723	66.70.204.222	192.168.2.4	200 TYPE is now 8-bit binary
Aug 30, 2021 06:55:26.102632046 CEST	49723	21	192.168.2.4	66.70.204.222	PASV

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 30, 2021 06:55:26.209256887 CEST	21	49723	66.70.204.222	192.168.2.4	227 Entering Passive Mode (66,70,204,222,202,233)
Aug 30, 2021 06:55:26.317878962 CEST	49723	21	192.168.2.4	66.70.204.222	STOR HawkEye_Keylogger_Stealer_Records_238576 8.30.2021 7:03:04 AM.txt
Aug 30, 2021 06:55:26.427908897 CEST	21	49723	66.70.204.222	192.168.2.4	150 Accepted data connection
Aug 30, 2021 06:55:26.541986942 CEST	21	49723	66.70.204.222	192.168.2.4	226-File successfully transferred 226-File successfully transferred226 0.114 seconds (measured here), 13.08 Kbytes per second

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 300821.PDF.exe PID: 4816 Parent PID: 6592

General

Start time:	06:54:57
Start date:	30/08/2021
Path:	C:\Users\user\Desktop\300821.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\300821.PDF.exe'
Imagebase:	0xa60000
File size:	987136 bytes
MD5 hash:	DDFC57B8FD3E5E0F81DEE8EAD0E38518
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: 00000000.00000002.665567909.0000000002FA5000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.667948277.0000000004BA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.667948277.0000000004BA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.667948277.0000000004BA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.667948277.0000000004BA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.667948277.0000000004BA1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.666209862.000000000400E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.666209862.000000000400E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.666209862.000000000400E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.666209862.000000000400E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.666209862.000000000400E000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 300821.PDF.exe PID: 2848 Parent PID: 4816

General

Start time:	06:55:05
Start date:	30/08/2021
Path:	C:\Users\user\Desktop\300821.PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\300821.PDF.exe
Imagebase:	0x6f0000
File size:	987136 bytes
MD5 hash:	DDFC57B8FD3E5E0F81DEE8EAD0E38518
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.916254009.0000000003B61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.916254009.0000000003B61000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000002.914785913.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.914785913.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.914785913.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.914785913.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.914785913.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.915489413.0000000002B61000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.915489413.0000000002B61000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: vbc.exe PID: 1668 Parent PID: 2848

General

Start time:	06:55:15
Start date:	30/08/2021
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: 00000008.00000002.693074434.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 5604 Parent PID: 2848

General

Start time:	06:55:15
Start date:	30/08/2021
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: 00000009.00000002.684649797.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

Disassembly

Code Analysis