ID: 489483
Sample Name: 9jV2cBN6cQ
Cookbook: default.jbs
Time: 07:36:13
Date: 24/09/2021
Version: 33.0.0 White Diamond

Table of Contents

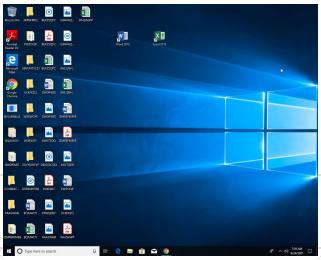
Windows Analysis Report 9jV2cBN6cQ

Overview

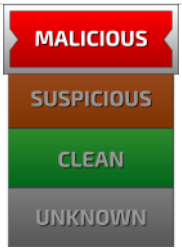
General Information

Sample Name:	9jV2cBN6cQ (renamed file extension from none to exe)
Analysis ID:	489483
MD5:	b105bec27851da..
SHA1:	f822c5a33d94cbe..
SHA256:	ed133e3bc6f781c..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



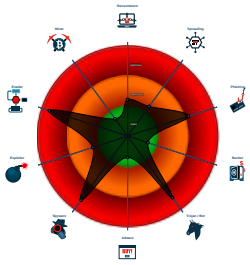
HawkEye
MailPassView

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

Signatures

- 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…
- Writes to foreign memory regions
- .NET source code references suspic…
- Tries to detect sandboxes and other…
- Contains functionality to log keystro…
- Tries to steal Mail credentials (via fil…

Classification



Process Tree

- **System is w10x64**
- 9jV2cBN6cQ.exe (PID: 6968 cmdline: 'C:\Users\user\Desktop\9jV2cBN6cQ.exe' MD5: B105BEC27851DABE21E1CF1C56BFDA0E)
  - 9jV2cBN6cQ.exe (PID: 4240 cmdline: C:\Users\user\Desktop\9jV2cBN6cQ.exe MD5: B105BEC27851DABE21E1CF1C56BFDA0E)
    - vbc.exe (PID: 6444 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: 6436 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

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.664391602.000000000307 9000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000002.915272981.000000000716 0000.00000004.00020000.sdmp	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
00000007.00000002.692945681.000000000040 0000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000005.00000002.915336004.000000000732 0000.00000004.00020000.sdmp	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df

Source	Rule	Description	Author	Strings
00000001.00000002.669409810.0000000004ED7000.00000004.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x1085d0:$key: HawkEyeKeylogger • 0x10a7ce:$salt: 099u787978786 • 0x108be9:$string1: HawkEye_Keylogger • 0x109a3c:$string1: HawkEye_Keylogger • 0x10a72e:$string1: HawkEye_Keylogger • 0x108fd2:$string2: holdermail.txt • 0x108ff2:$string2: holdermail.txt • 0x108f14:$string3: wallet.dat • 0x108f2c:$string3: wallet.dat • 0x108f42:$string3: wallet.dat • 0x10a310:$string4: Keylog Records • 0x10a628:$string4: Keylog Records • 0x10a826:$string5: do not script --> • 0x1085b8:$string6: \pidloc.txt • 0x10861e:$string7: BSPLIT • 0x10862e:$string7: BSPLIT
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.9jV2cBN6cQ.exe.7160000.9.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
5.2.9jV2cBN6cQ.exe.45fa72.2.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
5.2.9jV2cBN6cQ.exe.3b29930.7.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
5.2.9jV2cBN6cQ.exe.7320000.10.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
6.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 74 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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)

.NET source code contains very large strings

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Sample uses process hollowing technique

Writes to foreign memory regions

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

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

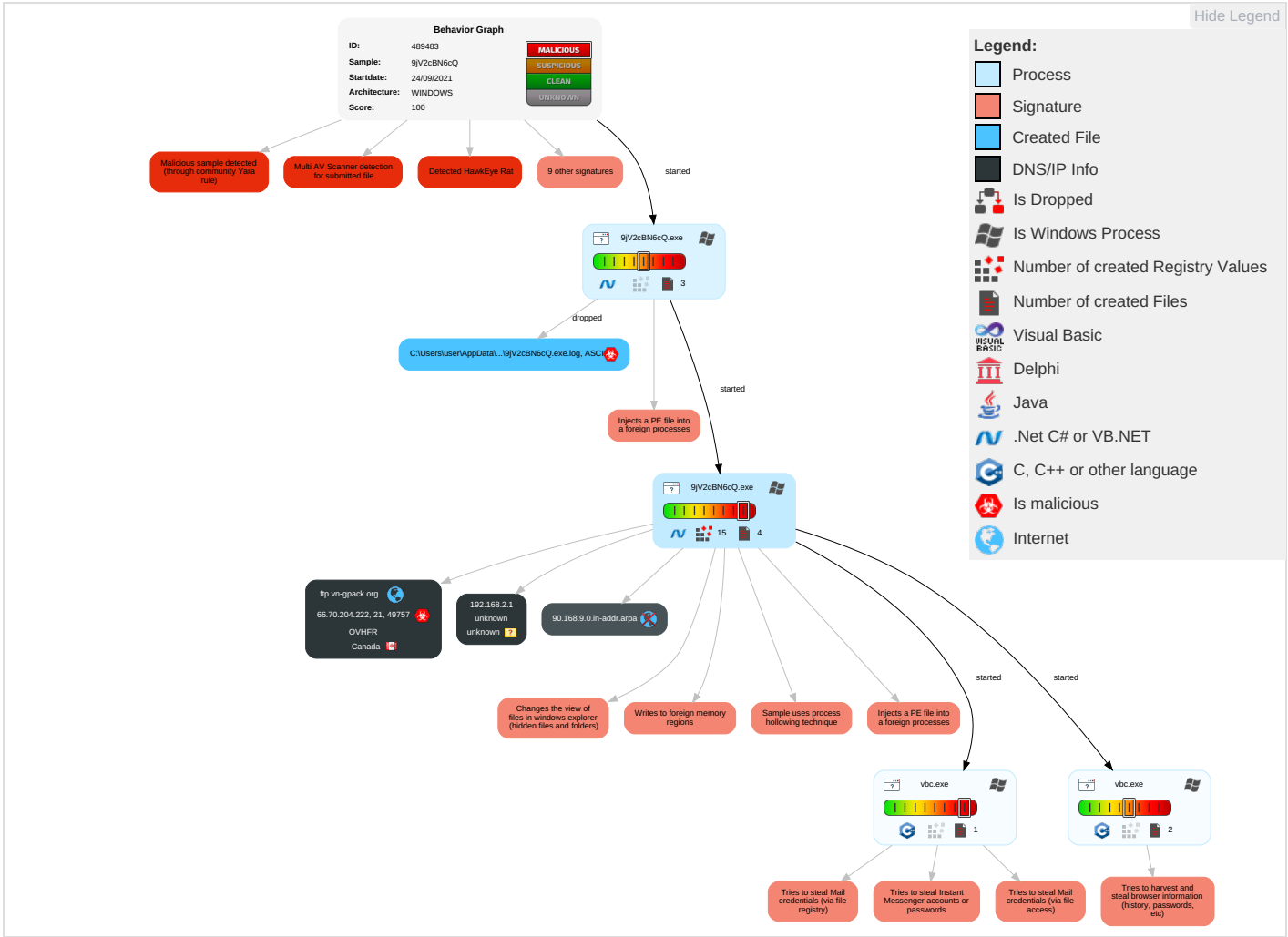
Detected HawkEye Rat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	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 3 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	R S
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 4 1	Credentials in Registry 2	Account Discovery 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	N A L P
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	Credentials In Files 1	File and Directory Discovery 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	A L P
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	System Information Discovery 1 8	SSH	Clipboard Data 1	Data Transfer Size Limits	F C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	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 3 1 2	DCSync	Security Software Discovery 1 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C U

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Virtualization/Sandbox Evasion 2 1	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
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

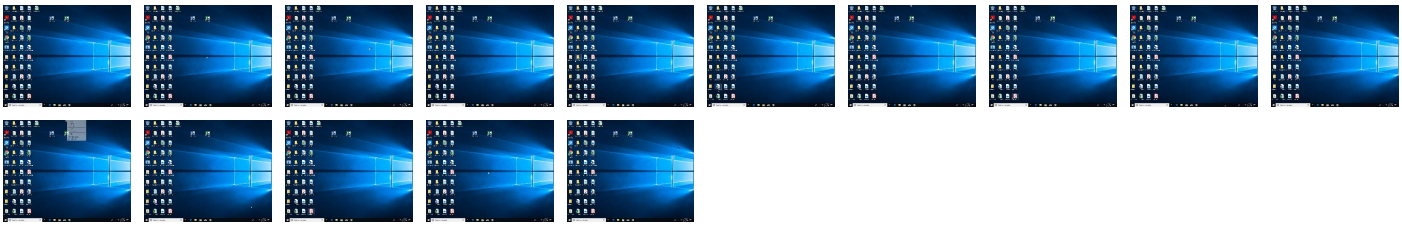
Behavior Graph



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
9jV2cBN6cQ.exe	54%	Virustotal		Browse
9jV2cBN6cQ.exe	43%	Metadefender		Browse
9jV2cBN6cQ.exe	82%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
9jV2cBN6cQ.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.9jV2cBN6cQ.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
5.2.9jV2cBN6cQ.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
7.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
1.2.9jV2cBN6cQ.exe.4f63ce0.5.unpack	100%	Avira	TR/Inject.vcoldi		Download File

Domains

Source	Detection	Scanner	Label	Link
ftp.vn-gpack.org	2%	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	• 2%, Virustotal, Browse	unknown
90.168.9.0.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:	489483
Start date:	24.09.2021
Start time:	07:36:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9jV2cBN6cQ (renamed file extension from none to 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
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:37:08	API Interceptor	6x Sleep call for process: 9jV2cBN6cQ.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ftp.vn-gpack.org	300821.PDF.exe	Get hash	malicious	Browse	• 66.70.204.222

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	HSBC94302,pdf.exe	Get hash	malicious	Browse	• 51.254.53.102
	ZamCfP5Dev.exe	Get hash	malicious	Browse	• 178.32.120.127
	zuyrzhibfm.exe	Get hash	malicious	Browse	• 188.165.222.221
	INV, BL, PL.exe	Get hash	malicious	Browse	• 94.23.48.114
	b3astmode.x86	Get hash	malicious	Browse	• 37.59.48.250
	b3astmode.arm	Get hash	malicious	Browse	• 51.83.43.58
	New Order.doc	Get hash	malicious	Browse	• 164.132.171.176
	2xgbTybbdX	Get hash	malicious	Browse	• 51.222.234.64
	qri9CgHh4M	Get hash	malicious	Browse	• 51.222.234.64
	eerjoaAQC2	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.mpsl	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.mips	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.arm7	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.x86	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.arm5	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.arm4	Get hash	malicious	Browse	• 51.222.234.64
	VwszKgEB99.exe	Get hash	malicious	Browse	• 188.165.222.221
	SYsObQNkC1.exe	Get hash	malicious	Browse	• 51.89.100.136
	New Order Specifications Pdf.exe	Get hash	malicious	Browse	• 51.81.56.51
	ak0joqnVCZ.exe	Get hash	malicious	Browse	• 192.99.131.252

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\9jV2cBN6cQ.exe.log	
Process:	C:\Users\user\Desktop\9jV2cBN6cQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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\bhv6C63.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xe0a9ace6, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	30408704
Entropy (8bit):	1.0887524045390116
Encrypted:	false
SSDEEP:	24576:xpy/YflH6N2gt8HVmyrqw781LfXy7R4aUpPX7Cr6f63rsLOZ:j1flH6N2iyrsrO
MD5:	4F2DD471D3B2E63DED4C30D7B8130155
SHA1:	DDA6F9E1763F27E1419383F1A2C6FE77B7A6FF1F
SHA-256:	8EFF1816D2E0C0DFCA195F2D00C3BA898CE546BD520277455A7625AE56104EDF
SHA-512:	1AE697BEABA27D21089089A7B8F74087E3DF145EDAE7F450EA98327901D0091D9A3FC516D8879DD382240B817CF7E367E11B3B48C1432AD45EF6E5461B4F9BD
Malicious:	false
Reputation:	low
Preview:	....?....._e..*....w.....^.8.....:#...xc.0$...y..h.:.....b...*....w.....{.....B..... ....2$...y..... .....5..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\9jV2cBN6cQ.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false

C:\Users\user\AppData\Roaming\pid.txt	
SSDEEP:	3:F:F
MD5:	FD272FE04B7D4E68EFFD01BDDCC6BB34
SHA1:	403667553498DF159BDD52AF68CCF072F564FCC0
SHA-256:	15811BD57B46D0025F3A839BB785419C90F4F22518025A487979085DA2C6A189
SHA-512:	4329260A721F5A9AC58F608E4A4DAE1B443E5DBC41D6DDF02E37E7F8ABB292490626A6FDE5646D0F67AFB92C2EF295155C279297855BAE82A02A1C15DEA5803E
Malicious:	false
Reputation:	low
Preview:	4240

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\Desktop\9jV2cBN6cQ.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.301084704157686
Encrypted:	false
SSDEEP:	3:oNt+WfWcjwDLNn:oNwvcjULN
MD5:	AB856F9007C1F896B09F99AFE43E4AA9
SHA1:	696D6602810AFF8669396217A56DA37B2AEE5277
SHA-256:	2FA5A88044C2630B0D5C309A5F0CA2A4BBEEC513FF2E77A0648F731C20731DF5
SHA-512:	2739144A2E99DEDA988D45F754175626E4BF3A960FA67BCD1B434F73DCED4441B88B3CBF57ACD963470098B59F105F3F8BD13E561F7575FB04C5C7C875B1B44
Malicious:	false
Reputation:	low
Preview:	C:\Users\user\Desktop\9jV2cBN6cQ.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.493273717830563
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:	9jV2cBN6cQ.exe
File size:	1154560
MD5:	b105bec27851dabe21e1cf1c56bfda0e
SHA1:	f822c5a33d94cbea0f69ce327257420b33b0d552
SHA256:	ed133e3bc6f781c4a981f93c180e38c70572ad80e48c12294585767e583b9d0f
SHA512:	aecaed590d316f3a762b97499bcbd62d0d59f31404a171b9f8daeff2dcc70726886fb652f1d96f257e2ab63c64f9a2b32b69d868836114a526b39e0b9b6c710c
SSDEEP:	12288:6sbxvLuoLXS7P2qGuV3uZlaDVEPWN53QwvJH4vNiCmLJ1GcyQizeVzhst:Vi+qDVeZlaDkWHgwq9uXiQzhst
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....d$a.....~.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x51b37e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x612464B2 [Tue Aug 24 03:17:06 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x119384	0x119400	False	0.811327256944	data	7.49843619507	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x11c000	0x600	0x600	False	0.430989583333	data	4.15453923293	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x11e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 24, 2021 07:37:12.394850016 CEST	192.168.2.4	8.8.8.8	0xc13c	Standard query (0)	90.168.9.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Sep 24, 2021 07:37:29.016794920 CEST	192.168.2.4	8.8.8.8	0x9d65	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
Sep 24, 2021 07:37:12.414520025 CEST	8.8.8.8	192.168.2.4	0xc13c	Name error (3)	90.168.9.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Sep 24, 2021 07:37:29.079749107 CEST	8.8.8.8	192.168.2.4	0x9d65	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
Sep 24, 2021 07:37:29.309921980 CEST	21	49757	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 1 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 09:37. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 09:37. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 09:37. 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 1 of 50 allowed.220-Local time is now 09:37. 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.
Sep 24, 2021 07:37:29.310753107 CEST	49757	21	192.168.2.4	66.70.204.222	USER Lloggoss123@vn-gpack.org
Sep 24, 2021 07:37:29.417004108 CEST	21	49757	66.70.204.222	192.168.2.4	331 User Lloggoss123@vn-gpack.org OK. Password required
Sep 24, 2021 07:37:29.417340040 CEST	49757	21	192.168.2.4	66.70.204.222	PASS Xpen2000
Sep 24, 2021 07:37:29.543555975 CEST	21	49757	66.70.204.222	192.168.2.4	421 Home directory not available - aborting

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 9jV2cBN6cQ.exe PID: 6968 Parent PID: 6488

General

Start time:	07:37:00
Start date:	24/09/2021
Path:	C:\Users\user\Desktop\9jV2cBN6cQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\9jV2cBN6cQ.exe'
Imagebase:	0xb10000
File size:	1154560 bytes
MD5 hash:	B105BEC27851DABE21E1CF1C56BFDA0E
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: 00000001.00000002.664391602.0000000003079000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.669409810.0000000004ED7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.669409810.0000000004ED7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.669409810.0000000004ED7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.669409810.0000000004ED7000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.669409810.0000000004ED7000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.672553798.0000000009A31000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.672553798.0000000009A31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.672553798.0000000009A31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.672553798.0000000009A31000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.672553798.0000000009A31000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 9jV2cBN6cQ.exe PID: 4240 Parent PID: 6968

General

Start time:	07:37:09
Start date:	24/09/2021
Path:	C:\Users\user\Desktop\9jV2cBN6cQ.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\9jV2cBN6cQ.exe
Imagebase:	0x710000
File size:	1154560 bytes
MD5 hash:	B105BEC27851DABE21E1CF1C56BFDA0E
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: 00000005.00000002.915272981.0000000007160000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000005.00000002.915336004.0000000007320000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.914204338.0000000003B21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.914204338.0000000003B21000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000002.912588772.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.912588772.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.912588772.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.912588772.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.912588772.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.913535799.0000000002B21000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.913535799.0000000002B21000.00000004.00000001.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: 6444 Parent PID: 4240

General

Start time:	07:37:18
Start date:	24/09/2021
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: 00000006.00000002.684007490.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Reputation:	high

File Activities Show Windows behavior

File Created

Analysis Process: vbc.exe PID: 6436 Parent PID: 4240

General

Start time:	07:37:18
Start date:	24/09/2021
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: 00000007.00000002.692945681.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis

