ID: 679408
Sample Name: f5OhlYjA9Q.exe
Cookbook: default.jbs
Time: 18:06:11
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report f5OhlYjA9Q.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: LimeRAT 4
Yara Signatures 4
Initial Sample 4
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
Operating System Destruction 6
System Summary 6
Data Obfuscation 6
Boot Survival 6
Malware Analysis System Evasion 6
Lowering of HIPS / PFW / Operating System Security Settings 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 9
Public IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 11
General 11
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 12
Data Directories 14
Sections 14
Imports 14
Network Behavior 15
Snort IDS Alerts 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 15
DNS Queries 16
DNS Answers 16
HTTP Request Dependency Graph 16
HTTPS Proxied Packets 16
Statistics 16
System Behavior 16

Analysis Process: f5OhlYjA9Q.exePID: 5984, Parent PID: 5596 16
General 16
File Activities 17
File Created 17
File Read 17
Registry Activities 17
Key Created 17
Key Value Created 17
Disassembly 18

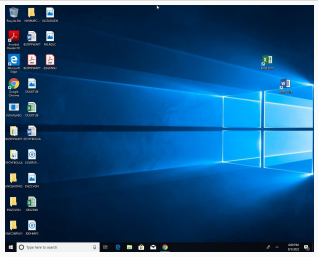
Windows Analysis Report

f5OhlYjA9Q.exe

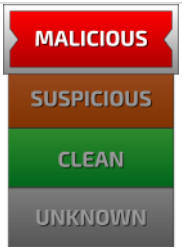
Overview

General Information

Sample Name:	f5OhlYjA9Q.exe
Analysis ID:	679408
MD5:	0c9df96101af0ac..
SHA1:	a43aedc5578add..
SHA256:	9207a09821cbdc..
Tags:	exe LimeRAT RAT
Infos:	



Detection



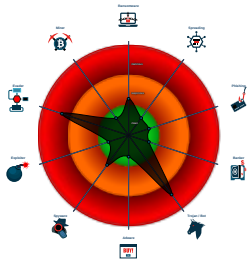
LimeRAT

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Yara detected LimeRAT
- Snort IDS alert for network traffic
- Protects its processes via BreakOn…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Connects to a pastebin service (like…
- Queries sensitive BIOS Information…

Classification



Process Tree

- **System is w10x64**
- f5OhlYjA9Q.exe (PID: 5984 cmdline: "C:\Users\user\Desktop\f5OhlYjA9Q.exe" MD5: 0C9DF96101AF0AC8049408831D42DEDD)
- **cleanup**

Malware Configuration

Threatname: LimeRAT

```
{
  "C2 url": "https://pastebin.com/raw/9uk330hR",
  "AES Key": "O",
  "ENDOF": "|'N'|",
  "Seprator": "|'L'|",
  "Install File": "False",
  "Install Dir": "temp",
  "Version": "v4.0"
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
f5OhlYjA9Q.exe	JoeSecurity_LimeRAT	Yara detected LimeRAT	Joe Security	

Source	Rule	Description	Author	Strings
f5OhlYjA9Q.exe	MALWARE_Win_LimeRAT	LimeRAT payload	ditekSHen	• 0x6892:$s1: schtasks /create /f /sc ONLOGON /RL HIGHEST /tn LimeRAT-Admin /tr • 0x6142:$s2: \vboxhook.dll • 0x6552:$s3: Win32_Processor.deviceid="CPU0" • 0x6474:$s4: select CommandLine from Win32_Process where Name='{0}' • 0x6530:$s5: Minning... • 0x64e2:$s6: Regasm.exe • 0x6815:$s7: Flood! • 0x6374:$s8: Rans-Status
f5OhlYjA9Q.exe	Windows_Trojan_Limerat_24269a79	unknown	unknown	• 0x6892:$a1: schtasks /create /f /sc ONLOGON /RL HIGHEST /tn LimeRAT-Admin /tr "'

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.408797111.00000000001D2000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_LimeRAT	Yara detected LimeRAT	Joe Security	
00000000.00000000.408797111.00000000001D2000.00000002.00000001.01000000.00000003.sdmp	Windows_Trojan_Limerat_24269a79	unknown	unknown	• 0x6692:$a1: schtasks /create /f /sc ONLOGON /RL HIGHEST /tn LimeRAT-Admin /tr "'
Process Memory Space: f5OhlYjA9Q.exe PID: 5984	JoeSecurity_LimeRAT	Yara detected LimeRAT	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.f5OhlYjA9Q.exe.1d0000.0.unpack	JoeSecurity_LimeRAT	Yara detected LimeRAT	Joe Security	
0.0.f5OhlYjA9Q.exe.1d0000.0.unpack	MALWARE_Win_LimeRAT	LimeRAT payload	ditekSHen	• 0x6892:$s1: schtasks /create /f /sc ONLOGON /RL HIGHEST /tn LimeRAT-Admin /tr • 0x6142:$s2: \vboxhook.dll • 0x6552:$s3: Win32_Processor.deviceid="CPU0" • 0x6474:$s4: select CommandLine from Win32_Process where Name='{0}' • 0x6530:$s5: Minning... • 0x64e2:$s6: Regasm.exe • 0x6815:$s7: Flood! • 0x6374:$s8: Rans-Status
0.0.f5OhlYjA9Q.exe.1d0000.0.unpack	Windows_Trojan_Limerat_24269a79	unknown	unknown	• 0x6892:$a1: schtasks /create /f /sc ONLOGON /RL HIGHEST /tn LimeRAT-Admin /tr "'

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN njRAT/Bladabindi/LimeRAT Variant CnC Checkin - Source IP: 192.168.2.5 - Destination IP: 102.133.180.23

Timestamp:	192.168.2.5102.133.180.234976655522832296 08/05/22-18:07:22.413967
SID:	2832296
Source Port:	49766
Destination Port:	5552
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Connects to a pastebin service (likely for C&C)

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected LimeRAT

Operating System Destruction

Protects its processes via BreakOnTermination flag

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Yara detected LimeRAT

Malware Analysis System Evasion

Yara detected LimeRAT

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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

Lowering of HIPS / PFW / Operating System Security Settings

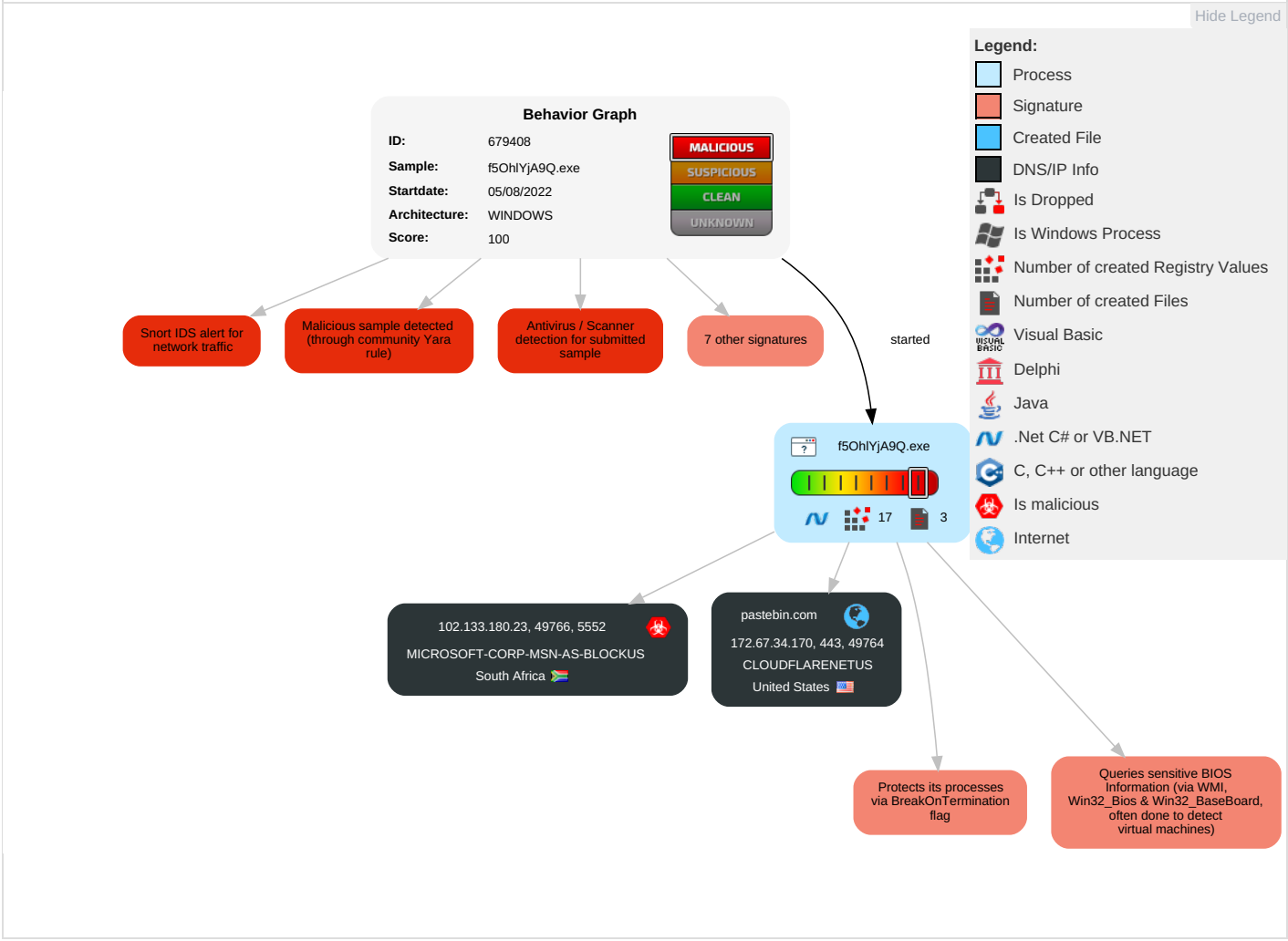
Yara detected LimeRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 1 Windows Management Instrumentation	Path Interception	Path Interception	1 Disable or Modify Tools	OS Credential Dumping	1 Query Registry	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	3 1 Virtualization/Sandbox Evasion	LSASS Memory	1 3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Obfuscated Files or Information	NTDS	3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Software Packing	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	2 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 3 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

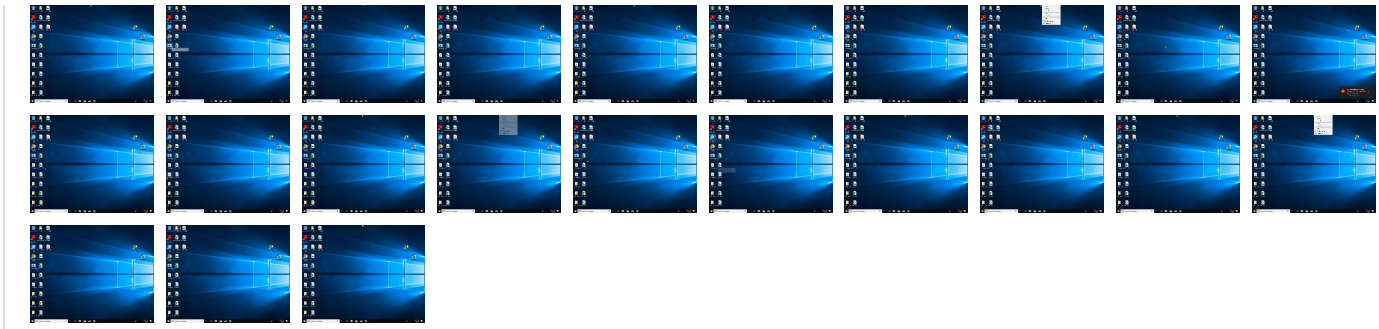
Behavior Graph



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
f5OhlYjA9Q.exe	66%	Virustotal		Browse
f5OhlYjA9Q.exe	66%	Metadefender		Browse
f5OhlYjA9Q.exe	96%	ReversingLabs	ByteCode-MSIL.Backdoor.LimeRAT	
f5OhlYjA9Q.exe	100%	Avira	TR/Spy.Gen8	
f5OhlYjA9Q.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.f5OhlYjA9Q.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1208284		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pastebin.com	172.67.34.170	true	false		high

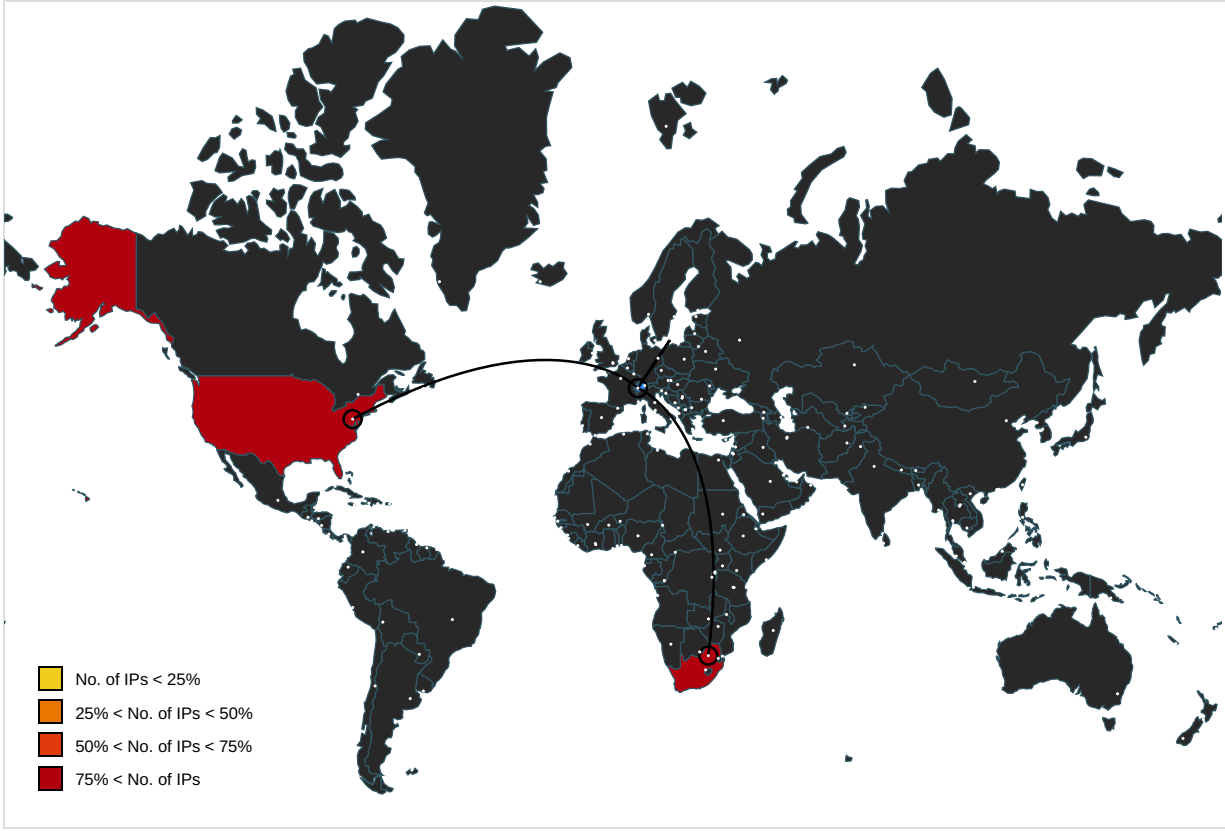
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://pastebin.com/raw/9uk330hR	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	f5OhlYjA9Q.exe, 00000000.00000002.677396151.0000000002511000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.34.170	pastebin.com	United States		13335	CLOUDFLARENETUS	false
102.133.180.23	unknown	South Africa		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679408
Start date and time: 05/08/202218:06:11	2022-08-05 18:06:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	f5OhlYjA9Q.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:	21
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.troj.evad.winEXE@1/0@1/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, licensing.mp.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:07:19	API Interceptor	1x Sleep call for process: f5OhlYjA9Q.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

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 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.933706659390986
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	f5OhlYjA9Q.exe
File size:	29696
MD5:	0c9df96101af0ac8049408831d42dedd
SHA1:	a43aedc5578add2f07269f88b923536b9d239019
SHA256:	9207a09821cbdc73ff5c3909c74914e772a4c356cfcb58eea38f8eeb1ea0c11a
SHA512:	2079380e4b839ba4b46f8f7c9eb34dc85b33a2876faa968efed62c3eb544125395ad6fc0dbf29f627cbf47e4550366485f2e789545a3726dd12df0a7cbb6710b
SSDEEP:	768:rtFHGfbAqYxDeGRey0195mbUjlaMOVUUrjy:ppGTAqYxDeGRe9a+laZj
TLSH:	B0D27D4C77D16368C2DD5AB54BB1606B0DB15A079A3BDB1F0CC864D71B3BACA8741BE0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....p..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x408e8e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62E6C7E4 [Sun Jul 31 18:20:20 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8e38	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6e94	0x7000	False	0.49428013392857145	data	6.048898258700505	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0xa000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

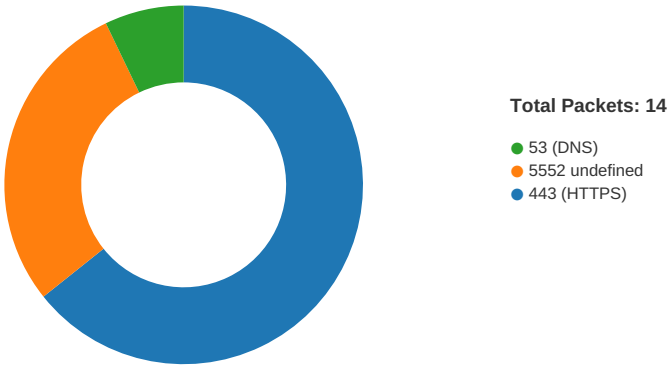
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5102.133.180.23497676555228322960 8/05/22-18:07:22.413967	TCP	2832296	ETPRO TROJAN njRAT/Bladabindi/LimeRAT Variant CnC Checkin	49766	5552	192.168.2.5	102.133.180.23

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 18:07:20.818314075 CEST	49764	443	192.168.2.5	172.67.34.170
Aug 5, 2022 18:07:20.818363905 CEST	443	49764	172.67.34.170	192.168.2.5
Aug 5, 2022 18:07:20.818469048 CEST	49764	443	192.168.2.5	172.67.34.170
Aug 5, 2022 18:07:20.848674059 CEST	49764	443	192.168.2.5	172.67.34.170
Aug 5, 2022 18:07:20.848714113 CEST	443	49764	172.67.34.170	192.168.2.5
Aug 5, 2022 18:07:20.906599045 CEST	443	49764	172.67.34.170	192.168.2.5
Aug 5, 2022 18:07:20.906697035 CEST	49764	443	192.168.2.5	172.67.34.170
Aug 5, 2022 18:07:20.910625935 CEST	49764	443	192.168.2.5	172.67.34.170
Aug 5, 2022 18:07:20.910633087 CEST	443	49764	172.67.34.170	192.168.2.5
Aug 5, 2022 18:07:20.910878897 CEST	443	49764	172.67.34.170	192.168.2.5
Aug 5, 2022 18:07:21.105572939 CEST	49764	443	192.168.2.5	172.67.34.170
Aug 5, 2022 18:07:21.393193960 CEST	49764	443	192.168.2.5	172.67.34.170
Aug 5, 2022 18:07:21.435477972 CEST	443	49764	172.67.34.170	192.168.2.5
Aug 5, 2022 18:07:21.657042980 CEST	443	49764	172.67.34.170	192.168.2.5
Aug 5, 2022 18:07:21.657130957 CEST	443	49764	172.67.34.170	192.168.2.5
Aug 5, 2022 18:07:21.657222986 CEST	49764	443	192.168.2.5	172.67.34.170
Aug 5, 2022 18:07:21.661662102 CEST	49764	443	192.168.2.5	172.67.34.170
Aug 5, 2022 18:07:21.733239889 CEST	49766	5552	192.168.2.5	102.133.180.23
Aug 5, 2022 18:07:21.920842886 CEST	5552	49766	102.133.180.23	192.168.2.5
Aug 5, 2022 18:07:21.920969963 CEST	49766	5552	192.168.2.5	102.133.180.23
Aug 5, 2022 18:07:22.413966894 CEST	49766	5552	192.168.2.5	102.133.180.23
Aug 5, 2022 18:07:22.654601097 CEST	5552	49766	102.133.180.23	192.168.2.5
Aug 5, 2022 18:07:28.179147959 CEST	49766	5552	192.168.2.5	102.133.180.23
Aug 5, 2022 18:07:28.423839092 CEST	5552	49766	102.133.180.23	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 18:07:20.763665915 CEST	59661	53	192.168.2.5	8.8.8.8
Aug 5, 2022 18:07:20.783689976 CEST	53	59661	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 18:07:20.763665915 CEST	192.168.2.5	8.8.8.8	0xa3dd	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 18:07:20.783689976 CEST	8.8.8.8	192.168.2.5	0xa3dd	No error (0)	pastebin.com		172.67.34.170	A (IP address)	IN (0x0001)
Aug 5, 2022 18:07:20.783689976 CEST	8.8.8.8	192.168.2.5	0xa3dd	No error (0)	pastebin.com		104.20.68.143	A (IP address)	IN (0x0001)
Aug 5, 2022 18:07:20.783689976 CEST	8.8.8.8	192.168.2.5	0xa3dd	No error (0)	pastebin.com		104.20.67.143	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- pastebin.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49764	172.67.34.170	443	C:\Users\user\Desktop\f5OhlYjA9Q.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 16:07:21 UTC	0	OUT	GET /raw/9uk330hR HTTP/1.1 Host: pastebin.com Connection: Keep-Alive
2022-08-05 16:07:21 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 16:07:21 GMT Content-Type: text/plain; charset=utf-8 Transfer-Encoding: chunked Connection: close x-frame-options: DENY x-content-type-options: nosniff x-xss-protection: 1;mode=block cache-control: public, max-age=1801 CF-Cache-Status: EXPIRED Last-Modified: Fri, 05 Aug 2022 10:14:18 GMT Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Server: cloudflare CF-RAY: 7360c906be0d909d-FRA
2022-08-05 16:07:21 UTC	0	IN	Data Raw: 31 33 0d 0a 31 30 32 2e 31 33 33 2e 31 38 30 2e 32 33 3a 35 35 35 32 0d 0a Data Ascii: 13102.133.180.23:5552
2022-08-05 16:07:21 UTC	0	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

No statistics

System Behavior

Analysis Process: f5OhlYjA9Q.exe PID: **5984**, Parent PID: **5596**

General

Target ID:	0

Start time:	18:07:14
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\f5OhlYjA9Q.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\f5OhlYjA9Q.exe"
Imagebase:	0x1d0000
File size:	29696 bytes
MD5 hash:	0C9DF96101AF0AC8049408831D42DEDD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 00000000.00000000.408797111.00000000001D2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Windows_Trojan_Limerat_24269a79, Description: unknown, Source: 00000000.00000000.408797111.00000000001D2000.00000002.00000001.01000000.00000003.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp970.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C4D7038	GetTempFileNameW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D68CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D68CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D665705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D66CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4D1B4F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\B1B32F58AD76	success or wait	1	6C4D5F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\B1B32F58AD76	Rans-Status	unicode	Not encrypted	success or wait	1	6C4D646A	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\B1B32F58AD76	Flood	unicode		success or wait	1	6C4D646A	RegSetValueExW

Disassembly

No disassembly