ID: 620828
Sample Name: Q9FAsn6SG6
Cookbook: default.jbs
Time: 09:34:27
Date: 05/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

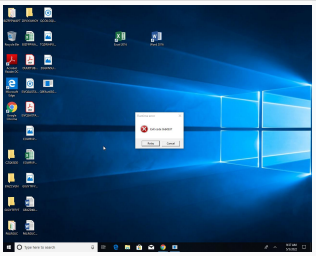
Windows Analysis Report

Q9FAsn6SG6

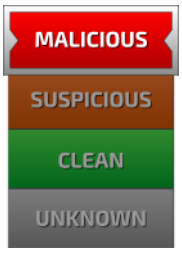
Overview

General Information

Sample Name:	Q9FAsn6SG6 (renamed file extension from none to exe)
Analysis ID:	620828
MD5:	c61f9a9059f8b8b..
SHA1:	70fffde0debf455…
SHA256:	84a5a26f1748c3..
Tags:	32 exe trojan
Infos:	



Detection

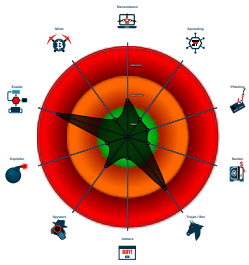


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Queries sensitive video device infor…
- Writes to foreign memory regions
- Query firmware table information (lik…
- Tries to detect sandboxes / dynamic…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- May check the online IP address of…
- Injects a PE file into a foreign proce…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- Q9FAsn6SG6.exe (PID: 6712 cmdline: "C:\Users\user\Desktop\Q9FAsn6SG6.exe" MD5: C61F9A9059F8B8BD0E69F7DF4CB09786)
  - conhost.exe (PID: 6728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AppLaunch.exe (PID: 6780 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

May check the online IP address of the machine

Malware Analysis System Evasion

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Query firmware table information (likely to detect VMs)

Tries to detect sandboxes / dynamic malware analysis system (registry check)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

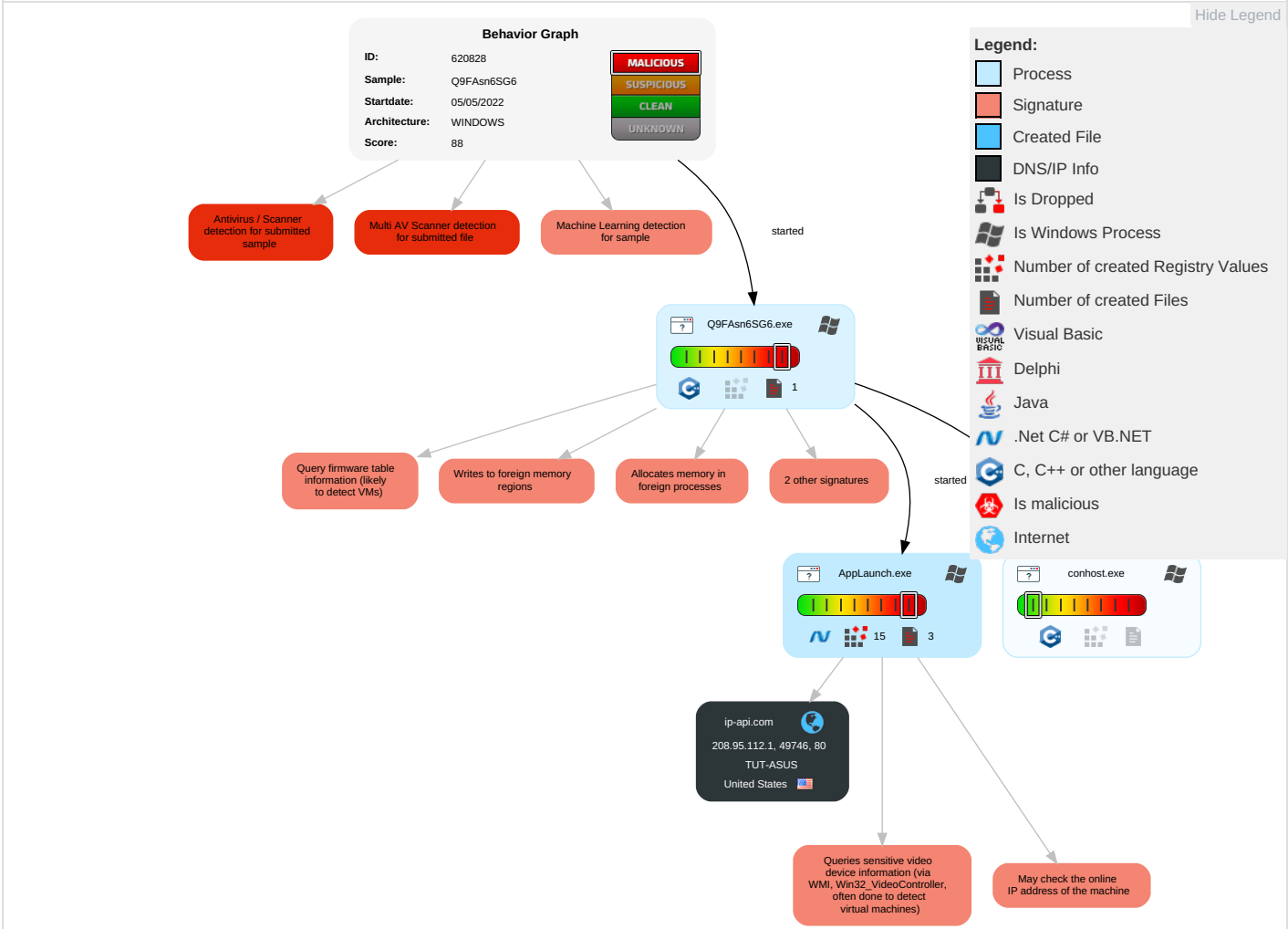
Allocates memory in foreign processes

Injects a PE file into a foreign processes

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 1 1 Windows Management Instrumentation	Path Interception	3 1 1 Process Injection	1 Masquerading	OS Credential Dumping	3 2 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	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	2 2 Virtualization/Sandbox Evasion	LSASS Memory	2 2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	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 Disable or Modify Tools	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 1 Process Injection	NTDS	1 System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

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
Q9FAsn6SG6.exe	69%	Virustotal		Browse
Q9FAsn6SG6.exe	31%	Metadefender		Browse
Q9FAsn6SG6.exe	69%	ReversingLabs	Win32.Trojan.FormBook	
Q9FAsn6SG6.exe	100%	Avira	TR/AD.GenStealjziki	
Q9FAsn6SG6.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File
0.3.Q9FAsn6SG6.exe.3130000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://https://pidgin.im0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://ip-api.com4	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ip-api.com	208.95.112.1	true	false		high

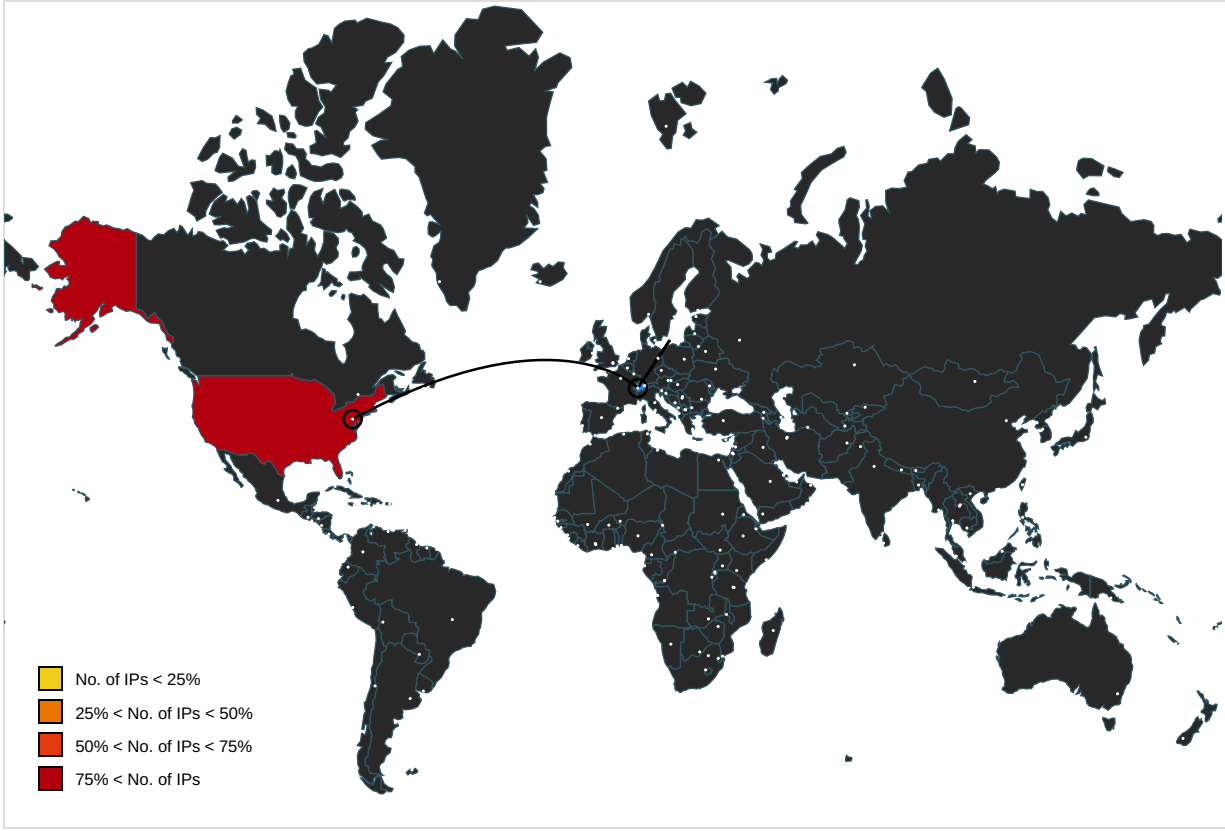
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ip-api.com/line/?fields=hosting	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sectigo.com/CPS0	Q9FAsn6SG6.exe	false	• URL Reputation: safe	unknown
http://www.vmware.com/0	Q9FAsn6SG6.exe	false		high
http://ocsp.sectigo.com0	Q9FAsn6SG6.exe	false	• URL Reputation: safe	unknown
http://www.symauth.com/rpa00	Q9FAsn6SG6.exe	false		high
http://ip-api.com	AppLaunch.exe, 00000002.00000002.532195437.0000000006B47000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.532225269.0000000006B5A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.vmware.com/0/	Q9FAsn6SG6.exe	false		high
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	Q9FAsn6SG6.exe	false	• URL Reputation: safe	unknown
http://https://pidgin.im0	Q9FAsn6SG6.exe	false	• URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	Q9FAsn6SG6.exe	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	AppLaunch.exe, 00000002.00000002.532195437.0000000006B47000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.symauth.com/cps0(	Q9FAsn6SG6.exe	false		high
http://ip-api.com4	AppLaunch.exe, 00000002.00000002.532195437.0000000006B47000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.95.112.1	ip-api.com	United States		53334	TUT-ASUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620828
Start date and time: 05/05/202209:34:27	2022-05-05 09:34:27 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Q9FAsn6SG6 (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:	26
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:	mal88.troj.evad.winEXE@4/0@1/1
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:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 104.208.16.94
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, arc.msn.com, onedsblobprdcus16.centralus.cloudapp.azure.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

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 (console) Intel 80386, for MS Windows
Entropy (8bit):	6.364458086173346
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:	Q9FAsn6SG6.exe
File size:	3677592
MD5:	c61f9a9059f8b8bd0e69f7df4cb09786
SHA1:	70fffde0debf4559859617d49dc48c54df3c156d
SHA256:	84a5a26f1748c3ad1f0b98c438908e8dc842eacc6390484527ee1fe7e56264f5
SHA512:	6a838d9663517e1f89bf47f9ba85b72cd431f0d61c4db97e69516ffa313d8bdfc9f619eb51ead5215786e523b43cde3186300cf3bfab7408d580c66cd7d00453
SSDEEP:	98304:xjFJEyX5ZYpLKwYXA8NMLgJ0CYkL1N5qV0O8:ZFSyJZ8LYEgCCYkDxO8
TLSH:	61067DB32B45629FC1313039FC92CA0E66101275931F7623EBD83978E59F9D12AC9F96
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k\8./=V./=V./=V.;VU.!=V.;VS..=V.;VR.9=V.}HR.>=V.}HU.;=V.}HS.e=V.;VW.*=V./=W.r=V..HS..=V..HT..=V.Rich/=V.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x6230b1
Entrypoint Section:	gTx1qw
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE
Time Stamp:	0x129 [Thu Jan 1 00:04:57 1970 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:	25a9be81ed1ff039b036d3155dd64335

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 3/21/2021 5:00:00 PM 3/21/2024 4:59:59 PM
Subject Chain	• CN=Gary Kramlich, O=Gary Kramlich, STREET=2653 N 54TH ST, L=MILWAUKEE, S=Wisconsin, PostalCode=53210, C=US
Version:	3
Thumbprint MD5:	394B591BC2CE78B7CF207BF4082E62F4
Thumbprint SHA-1:	ADFA744AA074FB5DC57EE6445A3E18D606C7BF96
Thumbprint SHA-256:	AE7DB8B64E8ABD9D36876F049B9770D90C0868D7FE1A2D37CF327DF69FA2DBFE
Serial:	00F6AD45188E5566AA317BE23B4B8B2C2F

Entrypoint Preview

Instruction
push ebp
call 00007F9C6CD76B0Ch
pop ebp
sub ebp, 000CC0B7h
call 00007F9C6CD76B54h
pop eax
sub eax, 002230C3h

Instruction
jmp 00007F9C6CD76C40h
jmp 00007F9C6CD76B0Dh
jmp 00007F9C6CD76ADEh
jmp 00007F9C6CD76B28h
jmp 00007F9C6CD76B67h
mov eax, eax
jmp 00007F9C6CD81F88h
jmp 00007F9C6CD8307Ah
add byte ptr [eax], al
or byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [ecx], al
or byte ptr [eax], al
add byte ptr [eax], al
insb
add ah, cl
add byte ptr [ecx+eax+00000006h], dh
or al, byte ptr [eax]
add byte ptr [eax], al
hlt
xlatb
inc ebx
add edx, edx
in al, B1h
outsd
push es
add byte ptr [eax], al
add byte ptr [ecx], al
loope 00007F9C6CD82012h
xlatb
or al, 00h
add byte ptr [eax], al
rcr byte ptr [ecx], 1
rcr dword ptr [ecx], 1
adc byte ptr [eax], 0000000Ah
add byte ptr [eax], al
add byte ptr [esi-38h], dl
pushfd
dec dword ptr [edx]
add byte ptr [eax], al
add byte ptr [edx-7Ah], ch
inc edi
enter 6484h, 78h
add dword ptr [eax-29h], edx
or al, 00h
add byte ptr [eax], al
pop es
xchg eax, edx
or dword ptr [edx+ecx+00000A7Fh], eax
add dh, bl
jp 00007F9C6CD81FD9h
jno 00007F9C6CD81FCCh
add byte ptr [eax], al
add byte ptr [esi], bl
cmc
iretd
pop ecx
loopne 00007F9C6CD81F95h
fcomp3 st(0)

Instruction
push eax
xlatb
or al, 00h
add byte ptr [eax], al
imul edx, dword ptr [ebx], 09h
test byte ptr [esi-62h], cl
or al, byte ptr [eax]
add byte ptr [eax], al
mov byte ptr [0A71F35Bh], al
add byte ptr [eax], al
add byte ptr [esi], bh
adc al, 33h
cmp al, byte ptr [eax+50017476h]
xlatb

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x156039	0x50	PKmYta
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x37d000	0x8db	9YRtc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x37d468	0x4930	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
JICeboQ	0x1000	0x105e35	0x106000	False	0.412188580928	data	5.62380807968	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
zcPlt	0x107000	0x25075	0x25200	False	0.550301188973	data	6.5843436682	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
rrF5ta	0x12d000	0x1f3a0	0x1f400	False	0.363	data	6.07842695634	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
IKbga	0x14d000	0x1cf0	0x1000	False	0.188720703125	data	3.05371407432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
03AAoc	0x14f000	0x2ddc	0x2e00	False	0.790336277174	data	6.70270981078	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
6maTqw	0x152000	0x4000	0x4000	False	0.0673828125	data	1.21393364646	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
PKmYta	0x156000	0x1000	0x200	False	0.16015625	data	1.14259413026	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
gTx1qw	0x157000	0x226000	0x226000	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
9YRtc	0x37d000	0x8db	0xa00	False	0.29296875	data	5.06332684426	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x37d058	0x883	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators	English	United States

Imports

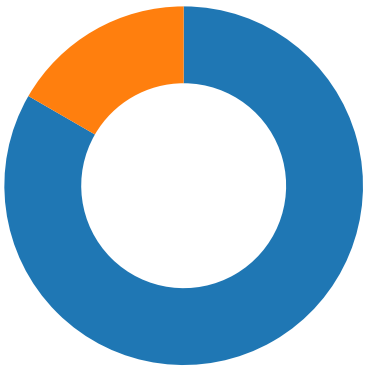
DLL	Import
kernel32.dll	GetModuleHandleA
USER32.dll	FindWindowA

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 6

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 09:35:45.140758038 CEST	49746	80	192.168.2.3	208.95.112.1
May 5, 2022 09:35:45.170057058 CEST	80	49746	208.95.112.1	192.168.2.3
May 5, 2022 09:35:45.170218945 CEST	49746	80	192.168.2.3	208.95.112.1
May 5, 2022 09:35:45.171499968 CEST	49746	80	192.168.2.3	208.95.112.1
May 5, 2022 09:35:45.209554911 CEST	80	49746	208.95.112.1	192.168.2.3
May 5, 2022 09:35:45.315737009 CEST	49746	80	192.168.2.3	208.95.112.1
May 5, 2022 09:36:50.641114950 CEST	80	49746	208.95.112.1	192.168.2.3
May 5, 2022 09:36:50.641221046 CEST	49746	80	192.168.2.3	208.95.112.1
May 5, 2022 09:37:02.769387960 CEST	80	49746	208.95.112.1	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 09:35:45.085983992 CEST	57421	53	192.168.2.3	8.8.8.8
May 5, 2022 09:35:45.104326963 CEST	53	57421	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 5, 2022 09:35:45.085983992 CEST	192.168.2.3	8.8.8.8	0x277f	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 5, 2022 09:35:45.104326963 CEST	8.8.8.8	192.168.2.3	0x277f	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ip-api.com

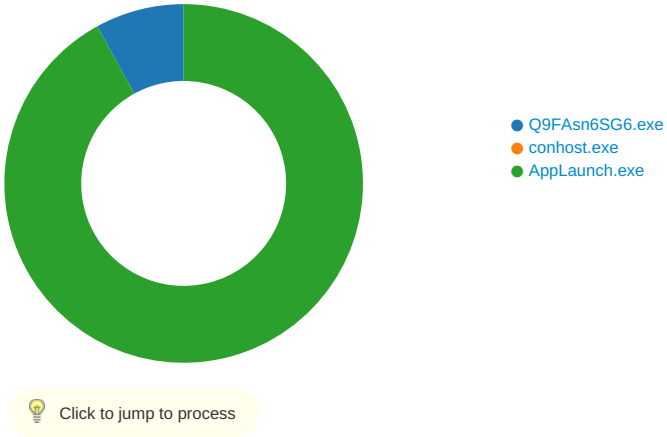
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49746	208.95.112.1	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 09:35:45.171499968 CEST	1141	OUT	GET /line/?fields=hosting HTTP/1.1 Host: ip-api.com Connection: Keep-Alive
May 5, 2022 09:35:45.209554911 CEST	1141	IN	HTTP/1.1 200 OK Date: Thu, 05 May 2022 07:35:44 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 5 Access-Control-Allow-Origin: * X-Ttl: 60 X-Rl: 44 Data Raw: 74 72 75 65 0a Data Ascii: true

Statistics

Behavior



System Behavior

Analysis Process: Q9FAsn6SG6.exe PID: 6712, Parent PID: 5956

General

Target ID:	0
Start time:	09:35:38
Start date:	05/05/2022
Path:	C:\Users\user\Desktop\Q9FAsn6SG6.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Q9FAsn6SG6.exe"
Imagebase:	0xe60000
File size:	3677592 bytes
MD5 hash:	C61F9A9059F8B8BD0E69F7DF4CB09786
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	90			object type mismatch	43	F80115	WriteFile
unknown	unknown	1			object type mismatch	5	F80115	WriteFile

Analysis Process: conhost.exe PID: 6728, Parent PID: 6712

General

Target ID:	1
Start time:	09:35:39
Start date:	05/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AppLaunch.exe PID: 6780, Parent PID: 6712

General

Target ID:	2
Start time:	09:35:40
Start date:	05/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0xdd0000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6DA5CF06	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	6DA5CF06	unknown
C:\Users\user\AppData\Local\86fddf902dc7d50e1674857833db815d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C8ABEFF	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DA3CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DA3CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	6C8A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	6C8A1B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly