ID: 593200
Sample Name: AutoInstall.exe
Cookbook: default.jbs
Time: 13:17:49
Date: 21/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

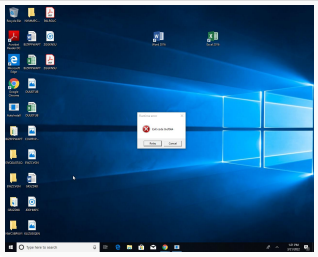
Windows Analysis Report

AutoInstall.exe

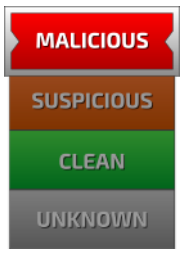
Overview

General Information

Sample Name:	AutoInstall.exe
Analysis ID:	593200
MD5:	7700a0d1b07e63.
SHA1:	6995f2e5f4544b3.
SHA256:	99b4df04fc5236a..
Tags:	exe
Infos:	



Detection

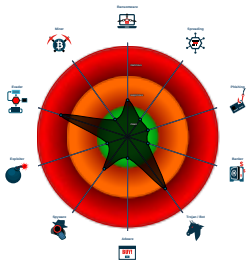


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Queries sensitive video device infor…
- Writes to foreign memory regions
- Allocates memory in foreign process…
- May check the online IP address of…
- PE file contains section with specia…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Creates a DirectInput object (often f…
- Uses 32bit PE files
- Queries the volume information (nam…
- Sigma detected: Suspicious DNS Q…

Classification



Process Tree

- **System is w10x64**
- AutoInstall.exe (PID: 6564 cmdline: "C:\Users\user\Desktop\AutoInstall.exe" MD5: 7700A0D1B07E63F054A730FBF9156EF0)
  - conhost.exe (PID: 4876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AppLaunch.exe (PID: 64 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

There are no malicious signatures, click here to show all signatures.

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

May check the online IP address of the machine

System Summary

PE file contains section with special chars

Data Obfuscation

.NET source code contains potential unpacker

Malware Analysis System Evasion

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

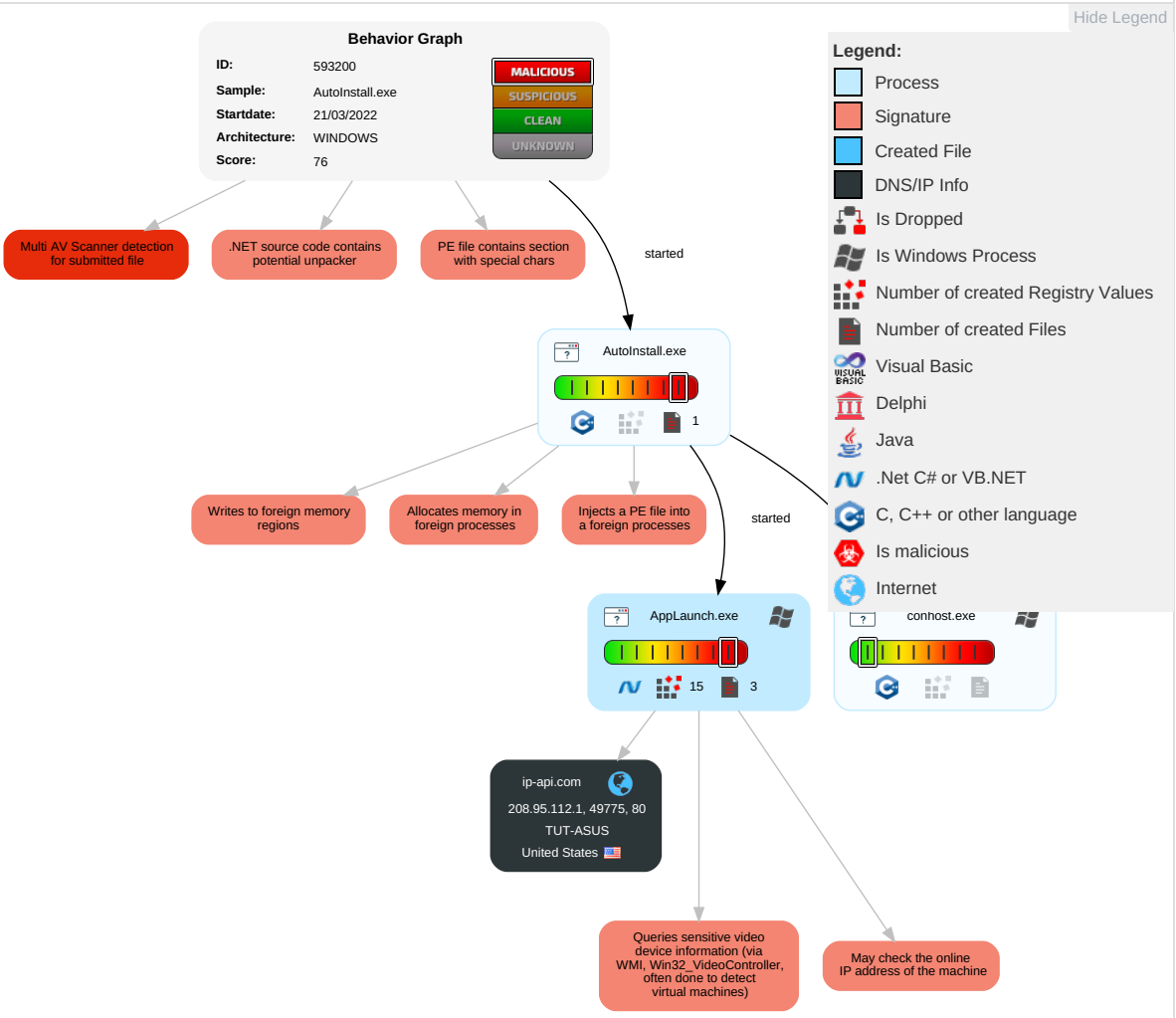
Injects a PE file into a foreign processes

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	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	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	1 1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	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 Query Registry	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 1 Virtualization/Sandbox Evasion	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 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 System Network Configuration Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Software Packing	DCSync	1 4 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
AutoInstall.exe	37%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.3.AutoInstall.exe.24b0000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File
3.2.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net02	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

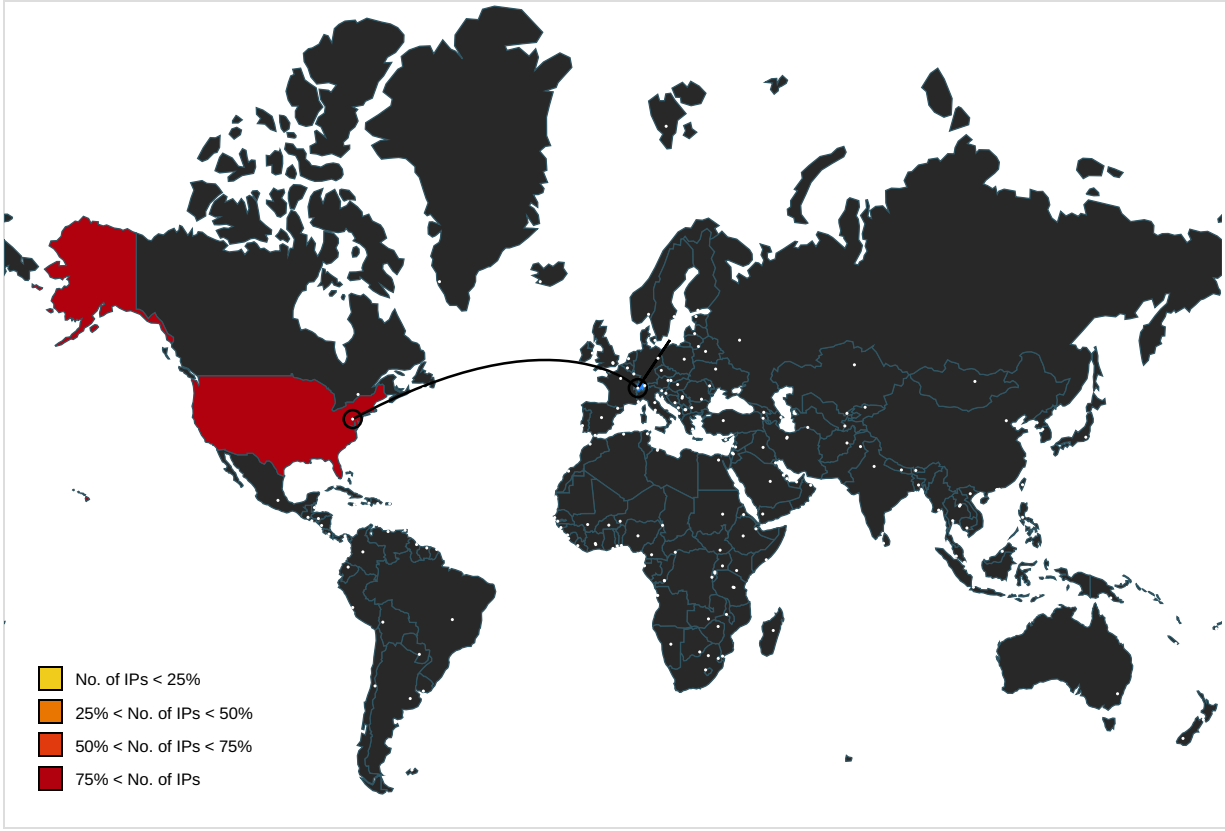
Contacted URLs

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://aia.entrust.net/ts1-chain256.cer01	AutoInstall.exe	false		high
http://www.codeplex.com/DotNetZip	AppLaunch.exe, 00000003.00000002.6402881 32.0000000000402000.00000020.00000400.00 020000.00000000.sdmp	false		high
http://crl.entrust.net/ts1ca.crl0	AutoInstall.exe	false		high
http://ocsp.entrust.net03	AutoInstall.exe	false	• URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/name	AppLaunch.exe, 00000003.00000002.6410341 19.0000000007116000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.entrust.net/rpa0	AutoInstall.exe	false		high
http://ocsp.entrust.net02	AutoInstall.exe	false	• URL Reputation: safe	unknown
http://www.entrust.net/rpa03	AutoInstall.exe	false		high
http://crl.entrust.net/2048ca.crl0	AutoInstall.exe	false		high
http://ip-api.com	AppLaunch.exe, 00000003.00000002.6410341 19.0000000007116000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00003.00000002.641051378.000000000712700 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://ip-api.com4	AppLaunch.exe, 00000003.00000002.6410341 19.0000000007116000.00000004.00000800.00 020000.00000000.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:	593200
Start date and time:	2022-03-21 12:17:49 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AutoInstall.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:	20
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:	mal76.troj.evad.winEXE@4/0@1/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 72% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

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): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, sls.update.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target AutoInstall.exe, PID 6564 because there are no executed function
- 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

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):	5.8762873630378625

TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Win16/32 Executable Delphi generic (2074/23) 0.02% • 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:	AutoInstall.exe
File size:	4344320
MD5:	7700a0d1b07e63f054a730fbf9156ef0
SHA1:	6995f2e5f4544b3e99489364bccc56084198c61d
SHA256:	99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770
SHA512:	9d063f2e37a35e20a322a4ab2be24884a245a40c4924b618a83f69515a62b15a954393717961f79c77945f2b692ea5d26d829153a8ece04c4ff774a48dc8607e
SSDEEP:	98304:IDWrdQJJ6qOobDtlLCSvKBXRAtiX2CVQmYRx6uiNnA9gEEtwPpAK3q2M:D6KPktlvIAtSNn6gFtYrzM
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....b8b.....@.. <.....;.....A...@.....0B.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40953b
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x6238628B [Mon Mar 21 11:33:31 2022 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:	99c2cae0b7316add27de679470515124

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert SHA2 Assured ID Code Signing CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 4/13/2021 5:00:00 PM 4/16/2024 4:59:59 PM
Subject Chain	• CN=Nvidia Corporation, OU=IT-MIS, O=Nvidia Corporation, L=Santa Clara, S=California, C=US
Version:	3
Thumbprint MD5:	991A62097E637843EA62029BF4E829BC
Thumbprint SHA-1:	F518FAD5DEC9E0500DA1C1598C4B0FFC0268B2D0
Thumbprint SHA-256:	A4870BB5FEB7028CCB0E50936E9138F528FF3CCD001D44C7D268A69685455FE8
Serial:	0266ADFA176389D9B4301AC87EFD6A96

Entrypoint Preview

Instruction
call 00007F5E64D0882Eh
jmp 00007F5E64D07F19h
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]

Instruction
push esi
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
movzx eax, word ptr [ecx+14h]
lea edx, dword ptr [ecx+18h]
add edx, eax
movzx eax, word ptr [ecx+06h]
imul esi, eax, 28h
add esi, edx
cmp edx, esi
je 00007F5E64D080BBh
mov ecx, dword ptr [ebp+0Ch]
cmp ecx, dword ptr [edx+0Ch]
jc 00007F5E64D080ACh
mov eax, dword ptr [edx+08h]
add eax, dword ptr [edx+0Ch]
cmp ecx, eax
jc 00007F5E64D080AEh
add edx, 28h
cmp edx, esi
jne 00007F5E64D0808Ch
xor eax, eax
pop esi
pop ebp
ret
mov eax, edx
jmp 00007F5E64D0809Bh
push esi
call 00007F5E64D08B0Bh
test eax, eax
je 00007F5E64D080C2h
mov eax, dword ptr fs:[00000018h]
mov esi, 008211E4h
mov edx, dword ptr [eax+04h]
jmp 00007F5E64D080A6h
cmp edx, eax
je 00007F5E64D080B2h
xor eax, eax
mov ecx, edx
lock cmpxchg dword ptr [esi], ecx
test eax, eax
jne 00007F5E64D08092h
xor al, al
pop esi
ret
mov al, 01h
pop esi
ret
push ebp
mov ebp, esp
cmp dword ptr [ebp+08h], 00000000h
jne 00007F5E64D080A9h
mov byte ptr [008211E8h], 00000001h
call 00007F5E64D08580h
call 00007F5E64D0A8FEh
test al, al
jne 00007F5E64D080A6h
xor al, al

Instruction
pop ebp
ret
call 00007F5E64D1386Eh
test al, al
jne 00007F5E64D080ACh
push 00000000h
call 00007F5E64D0A905h
pop ecx
jmp 00007F5E64D0808Bh
mov al, 01h
pop ebp
ret
push ebp
mov ebp, esp
cmp byte ptr [008211E9h], 00000000h
je 00007F5E64D080A6h
mov al, 01h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x41f12c	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x422800	0x2200	
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	0x41ced8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x410000	0x154	.rdata
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
.text	0x1000	0x23fe5	0x24000	False	0.55852593316	data	6.58598139573	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.iXgHkK	0x25000	0x3eac39	0x3eae00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x410000	0xf8d8	0xfa00	False	0.546984375	data	5.65055331195	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x420000	0x1ce8	0x1000	False	0.18994140625	data	3.03654885505	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pyX$d	0x422000	0x910	0xa00	False	0.881640625	data	7.40228735958	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

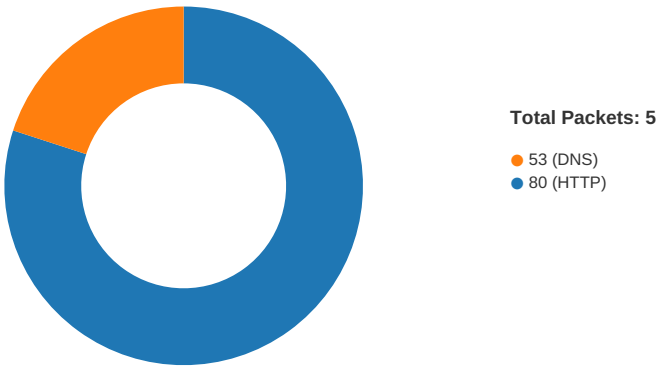
Imports

DLL	Import
USER32.dll	GetSysColorBrush, MessageBeep, MessageBoxA, GetSystemMetrics, SendNotifyMessageA

DLL	Import
KERNEL32.dll	TlsSetValue, CreateFileW, HeapSize, GetProcessHeap, SetStdHandle, SetEnvironmentVariableW, GetLastError, GetCurrentProcessId, GetCurrentThreadId, GetModuleHandleA, GetProcAddress, MultiByteToWideChar, FreeConsole, GetConsoleWindow, WideCharToMultiByte, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionEx, DeleteCriticalSection, EncodePointer, DecodePointer, LCMapStringEx, GetStringTypeW, GetCPInfo, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleW, FreeEnvironmentStringsW, RaiseException, RtlUnwind, SetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, WriteConsoleW, TlsFree, FreeLibrary, LoadLibraryExW, GetStdHandle, WriteFile, GetModuleFileNameW, ExitProcess, GetModuleHandleExW, GetCommandLineA, GetCommandLineW, HeapAlloc, HeapFree, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, GetFileType, CloseHandle, FlushFileBuffers, GetConsoleOutputCP, GetConsoleMode, ReadFile, GetFileSizeEx, SetFilePointerEx, ReadConsoleW, HeapReAlloc, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetEnvironmentStringsW

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2022 13:19:19.080195904 CET	49775	80	192.168.2.6	208.95.112.1
Mar 21, 2022 13:19:19.109673977 CET	80	49775	208.95.112.1	192.168.2.6
Mar 21, 2022 13:19:19.109812975 CET	49775	80	192.168.2.6	208.95.112.1
Mar 21, 2022 13:19:19.119479895 CET	49775	80	192.168.2.6	208.95.112.1
Mar 21, 2022 13:19:19.149487019 CET	80	49775	208.95.112.1	192.168.2.6
Mar 21, 2022 13:19:19.292432070 CET	49775	80	192.168.2.6	208.95.112.1
Mar 21, 2022 13:19:58.370439053 CET	80	49775	208.95.112.1	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2022 13:19:18.970336914 CET	52858	53	192.168.2.6	8.8.8.8
Mar 21, 2022 13:19:18.989157915 CET	53	52858	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 21, 2022 13:19:18.970336914 CET	192.168.2.6	8.8.8.8	0x45cd	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
Mar 21, 2022 13:19:18.989157915 CET	8.8.8.8	192.168.2.6	0x45cd	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ip-api.com

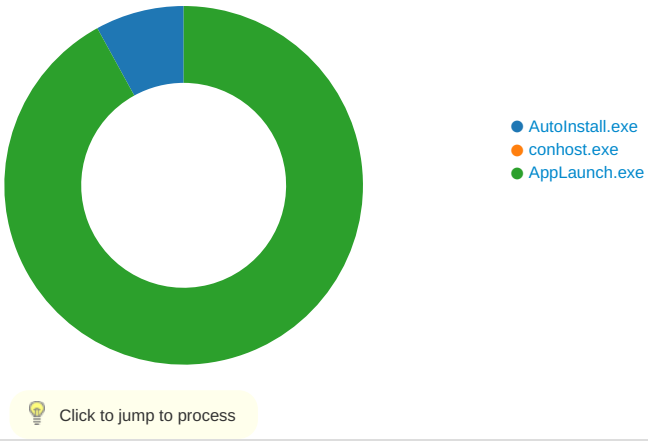
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49775	208.95.112.1	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
Mar 21, 2022 13:19:19.119479895 CET	1097	OUT	GET /line/?fields=hosting HTTP/1.1 Host: ip-api.com Connection: Keep-Alive
Mar 21, 2022 13:19:19.149487019 CET	1097	IN	HTTP/1.1 200 OK Date: Mon, 21 Mar 2022 12:19:18 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: AutoInstall.exe PID: **6564**, Parent PID: **6076**

General

Target ID:	1
Start time:	13:18:59
Start date:	21/03/2022
Path:	C:\Users\user\Desktop\AutoInstall.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\AutoInstall.exe"
Imagebase:	0x400000

File size:	4344320 bytes
MD5 hash:	7700A0D1B07E63F054A730FBF9156EF0
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			invalid handle	43	419080	WriteFile
unknown	unknown	1			invalid handle	5	419080	WriteFile

Analysis Process: conhost.exe PID: **4876**, Parent PID: **6564**

General

Target ID:	2
Start time:	13:19:00
Start date:	21/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: **64**, Parent PID: **6564**

General

Target ID:	3
Start time:	13:19:02
Start date:	21/03/2022
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:	0x1050000
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

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	6D8CCF06	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	6D8CCF06	unknown
C:\Users\user\AppData\Local\8d96007aa6619f065c7ec2509ce5f96d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C71BEFF	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	6D8A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6D8A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D8A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6D8ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6D8ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6D8A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6D8A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D8A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C711B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C711B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	6C711B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	6C711B4F	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