ID: 452411
Sample Name:
IDeVaZ8ESy.exe
Cookbook: default.jbs
Time: 10:11:18
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

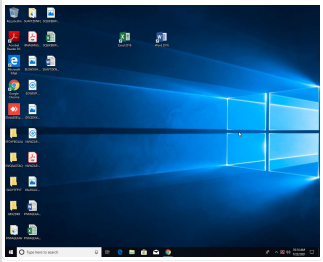
Windows Analysis Report IDeVaZ8ESy.exe

Overview

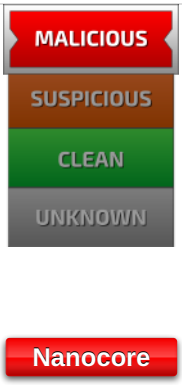
General Information

Sample Name:	IDeVaZ8ESy.exe
Analysis ID:	452411
MD5:	b0876b8da9dcb8..
SHA1:	80e619da78e64b..
SHA256:	d6215a4b16d74d..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



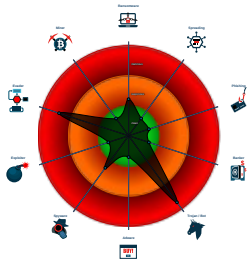
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- IDeVaZ8ESy.exe (PID: 5976 cmdline: 'C:\Users\user\Desktop\IDeVaZ8ESy.exe' MD5: B0876B8DA9DCB8A3B22D2CBF2B6A4711)
  - IDeVaZ8ESy.exe (PID: 1384 cmdline: C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe MD5: B0876B8DA9DCB8A3B22D2CBF2B6A4711)
  - IDeVaZ8ESy.exe (PID: 5056 cmdline: C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe MD5: B0876B8DA9DCB8A3B22D2CBF2B6A4711)
    - schtasks.exe (PID: 6064 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpBB0F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 2476 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- IDeVaZ8ESy.exe (PID: 5972 cmdline: C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe 0 MD5: B0876B8DA9DCB8A3B22D2CBF2B6A4711)
  - IDeVaZ8ESy.exe (PID: 1276 cmdline: C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe MD5: B0876B8DA9DCB8A3B22D2CBF2B6A4711)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "0bb207a5-6f92-4ff1-abb5-35e0dc25",
  "Group": "AUGUST",
  "Domain1": "asweee.jumpingcrab.com",
  "Domain2": "tryweaswweee.ydns.eu",
  "Port": 8234,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "asweee.jumpingcrab.com",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task>"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.298170775.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000002.298170775.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000C.00000002.298170775.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
0000000A.00000002.282656161.00000000026F2000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x57b01:$x1: NanoCore.ClientPluginHost • 0x57b3e:$x2: IClientNetworkHost • 0x5b671:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
0000000A.00000002.282656161.00000000026F2000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x57869:$a: NanoCore • 0x57879:$a: NanoCore • 0x57aad:$a: NanoCore • 0x57ac1:$a: NanoCore • 0x57b01:$a: NanoCore • 0x578c8:$b: ClientPlugin • 0x57aca:$b: ClientPlugin • 0x57b0a:$b: ClientPlugin • 0x579ef:$c: ProjectData • 0x583f6:$d: DESCrypto • 0x59fab:$i: get_Connected • 0x5872c:$j: #=q • 0x5875c:$j: #=q • 0x58778:$j: #=q • 0x587a8:$j: #=q • 0x587c4:$j: #=q • 0x587e0:$j: #=q • 0x58810:$j: #=q • 0x5882c:$j: #=q • 0x58870:$j: #=q • 0x5888c:$j: #=q
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.IDeVaZ8ESy.exe.3df0614.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
12.2.IDeVaZ8ESy.exe.3df0614.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
12.2.IDeVaZ8ESy.exe.3df0614.5.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
12.2.IDeVaZ8ESy.exe.3df0614.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x287b9:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x287e6:$x2: IClientNetworkHost
12.2.IDeVaZ8ESy.exe.3df0614.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x287b9:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0x29894:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost • 0x287d3:$s5: IClientLoggingHost
Click to see the 28 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

- Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

- Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

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

HIPS / PFW / Operating System Protection Evasion:

- Injects a PE file into a foreign processes
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

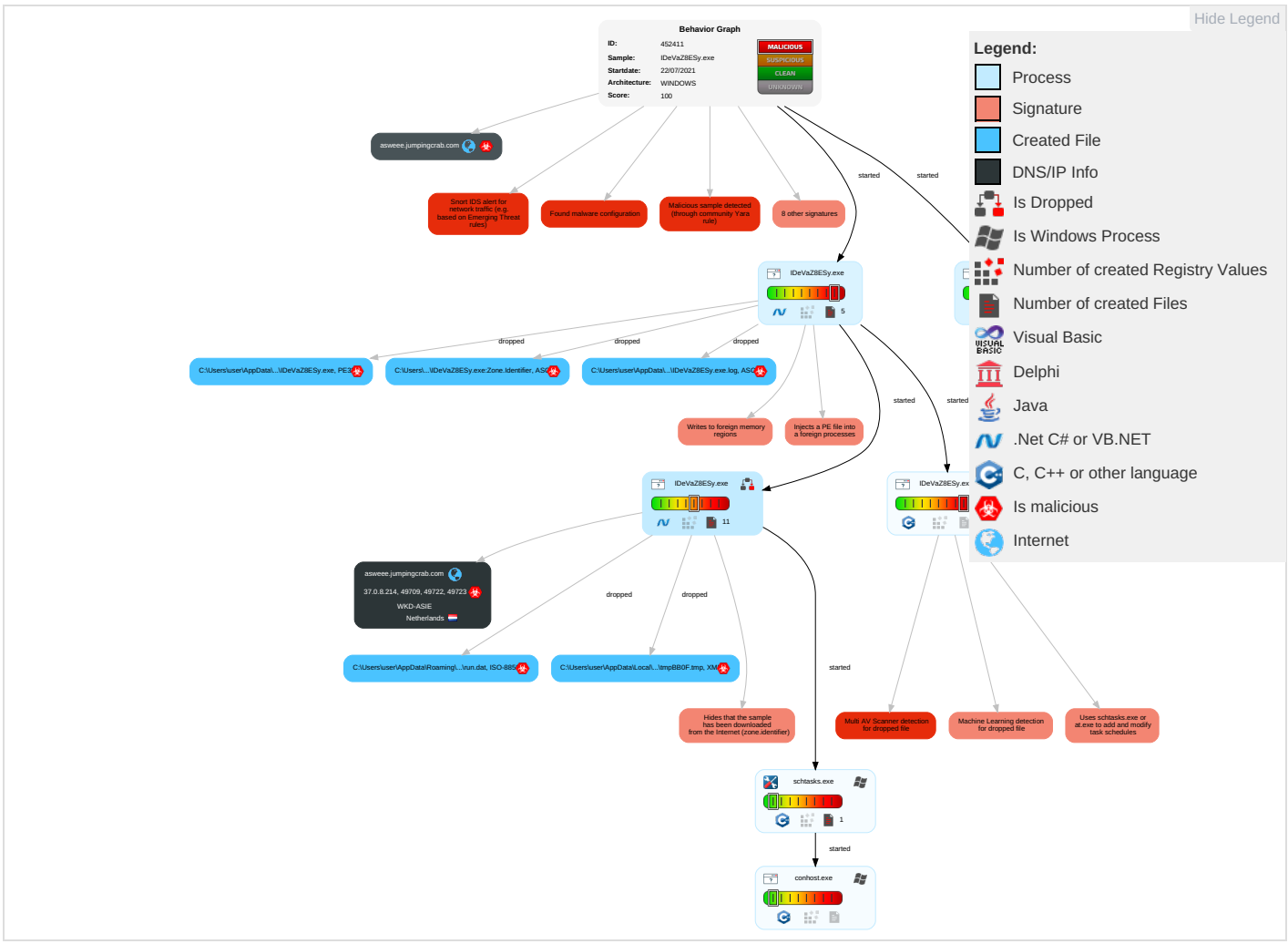
Remote Access Functionality:

- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 2 1 1	Masquerading 1	Input Capture 1 1	Query Registry 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 1	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	Network Sniffing	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	Software Packing 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

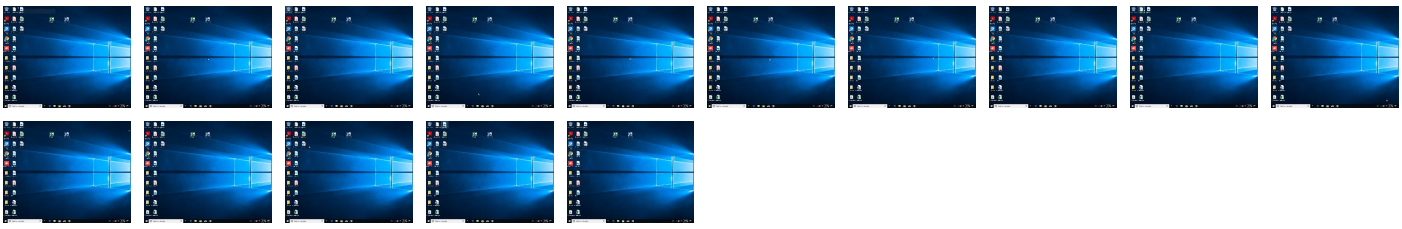
Behavior Graph



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
IDeVaZ8ESy.exe	24%	Virustotal		Browse
IDeVaZ8ESy.exe	23%	Metadefender		Browse
IDeVaZ8ESy.exe	32%	ReversingLabs	ByteCode-MSIL.Coinminer.BitCoinMiner	
IDeVaZ8ESy.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe	24%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe	23%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe	32%	ReversingLabs	ByteCode-MSIL.Coinminer.BitCoinMiner	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.IDeVaZ8ESy.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
asweee.jumpingcrab.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
asweee.jumpingcrab.com	4%	Virustotal		Browse
asweee.jumpingcrab.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
tryweaswweee.ydns.eu	2%	Virustotal		Browse
tryweaswweee.ydns.eu	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
asweee.jumpingcrab.com	37.0.8.214	true	true	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
asweee.jumpingcrab.com	true	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
tryweaswweee.ydns.eu	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.0.8.214	asweee.jumpingcrab.com	Netherlands		198301	WKD-ASIE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452411
Start date:	22.07.2021
Start time:	10:11:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IDeVaZ8ESy.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:	29
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@11/9@16/1
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 • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:12:13	API Interceptor	903x Sleep call for process: IDeVaZ8ESy.exe modified
10:12:32	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\IDeVaZ8ESy.exe.log

Process:	C:\Users\user\Desktop\IDeVaZ8ESy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\IDeVaZ8ESy.exe.log	
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe	
Process:	C:\Users\user\Desktop\IDeVaZ8ESy.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	565248
Entropy (8bit):	6.2839101385440355
Encrypted:	false
SSDEEP:	12288:3FBH6YCzj8MFiAInR2MDDT/lgCc+zElDiUQm:1/Czjli14m8ym
MD5:	B0876B8DA9DCB8A3B22D2CBF2B6A4711
SHA1:	80E619DA78E64BF6845F284C50BFACF17C55A274
SHA-256:	D6215A4B16D74DB6DAFC28A78F15885DE77570347ACFBAC416F18B223BA08E26
SHA-512:	3B52E3ABA69434D0B13E26B359F28493C303593BFDB254D86D3F91F7BFDE8F318BB11FFB3A9EE26547EE389EF181EB61E863E2060F2A950F6EBF0AF94D26A146
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 24%, Browse • Antivirus: Metadefender, Detection: 23%, Browse • Antivirus: ReversingLabs, Detection: 32%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...t .`.....I...2.....2.... ........@.. ..... ..@.....W.....</..... ..... ..H.....text...8j... ...I..... ..`.rsrc...</.....0...n.....@..@.relo c.....@..B.....H.....n..0..... ....1...=.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0..%.....(.....-.&& ...-.&&+.}....+.}....+.*....0..\.....(.... .U...-.&.s.....,.&&(....~....%-/+.(....+.}....+.&~.....s....%.-.&+.....+.o....*.0..).....s.....-.&..(....-.+..+..{.....o.....*.*....0..$.....(.....-.&.,.+..+..{ .....o....&.*.*.0.....-.&{.....-.&o....+.&+.&+.*..0.....-.&{.

C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\IDeVaZ8ESy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\tmpBB0F.tmp	
Process:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1311
Entropy (8bit):	5.12366956692759
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0aLxtn:cbk4oL600QydbQxIYODOLedq3BLj
MD5:	48241E0061B6E8208F2B28FF3896C16B
SHA1:	7A3C99770473C1F92E22D5CF3666E84F23815F10

C:\Users\user\AppData\Local\Temp\tmpBB0F.tmp	
SHA-256:	2C2AF82671F7D1F7835E843CFFD29F4FA334B997649BA0E823A4C532B62DD6CC
SHA-512:	CB9640388D552237FE1BAA52CEC19ABAD2E18FDFB229B43B0B42F5E42E86CA519F496F074F86BE3CD28428EDC8ACC6067099030FC7E3A64430B5500302AD055 1
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCr
MD5:	838CD9DBC78EA45A5406EAE23962086D
SHA1:	C8273AACDEE03AC0CDCDDBAA83F51D04D6A4203C
SHA-256:	6E11A62511C5BBC0413128305069B780C448684B54FAA3E8DD0B4FD3DB8C9867
SHA-512:	F7D25EF1FA6F50667DD6785CC774E0AA6BC52A2231FE96E7C59D14EFDFDDA076F6399288CF6EAC8EFA8A75727893432AA155DA0E392F8CD1F26C5C5871EAC6 B5
Malicious:	false
Reputation:	unknown
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Zt:T
MD5:	B298CDF095904A184461B5CF41DDBFD8
SHA1:	7CD28EFCCF3896A7B1F29BD5FA141BCA4D987155
SHA-256:	EB5E8C19784EECC2DCC1C974116E21E3E45A89331D8BE9F929CEB4F0120A7249
SHA-512:	54C3E4B2E17403899C500FB01D2A2F97273B36A658145314FBE70BED2B8794F8398A39FD90D0C30AAAD4EB46251781A396551BADCE244DFE49D36171A010BE44
Malicious:	**true**
Reputation:	unknown
Preview:	..I.3M.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Reputation:	unknown
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV.,,...0.... ....n.w6PMl.....v."".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[.../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*l..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.Ql..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..l..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....l..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	48
Entropy (8bit):	4.55404701206774
Encrypted:	false
SSDEEP:	3:oNWXp5cViE2J5xAIs6AC:oNWXp+N23fz
MD5:	6A1470C263611221341BBA42E51B85CE
SHA1:	9F136F89C8F6C8D9238AD5BC4BE00662B7C8BDDC
SHA-256:	771EAEEC47531B823EADBCD3E95EA80AA1D634848CA506B23FE3884C0279C7EE
SHA-512:	3BA49F78789234C6BC16E5FD7FF9D693B342AF30B3829A46438A30818DEAC00F71F4FA98538EDA74ABA21CF868ED947E1E3C2A833567D6E71D0BBBE17126BFE 4
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.2839101385440355
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	IDeVaZ8ESy.exe
File size:	565248
MD5:	b0876b8da9dcb8a3b22d2cbf2b6a4711
SHA1:	80e619da78e64bf6845f284c50bfacf17c55a274
SHA256:	d6215a4b16d74db6dafc28a78f15885de77570347acfbac 416f18b223ba08e26
SHA512:	3b52e3aba69434d0b13e26b359f28493c303593bfdb254c 86d3f91f7bfde8f318bb11ffb3a9ee26547ee389ef181eb61 e863e2060f2a950f6ebf0af94d26a146
SSDEEP:	12288:3FBH6YCzj8MFiAInR2MDDT/lgCc+zElDiUQm:1/ Czjli14m8ym

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...t.`.....I...2.....2.... ....@.. .....@.....

File Icon

Icon Hash:	499669d8d82916a8

Static PE Info

General

Entrypoint:	0x488a32
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60F82074 [Wed Jul 21 13:26:12 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x86a38	0x86c00	False	0.746072008349	data	6.20385416645	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x2f3c	0x3000	False	0.69677734375	data	6.71663956615	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-10:12:33.217914	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	8234	192.168.2.3	37.0.8.214

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-10:12:40.509972	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	8234	192.168.2.3	37.0.8.214
07/22/21-10:12:48.555142	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	8234	192.168.2.3	37.0.8.214
07/22/21-10:12:55.373984	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	8234	192.168.2.3	37.0.8.214
07/22/21-10:13:02.137554	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	8234	192.168.2.3	37.0.8.214
07/22/21-10:13:09.462872	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	8234	192.168.2.3	37.0.8.214
07/22/21-10:13:16.164647	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	8234	192.168.2.3	37.0.8.214
07/22/21-10:13:23.046489	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	8234	192.168.2.3	37.0.8.214
07/22/21-10:13:31.366337	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	8234	192.168.2.3	37.0.8.214
07/22/21-10:13:38.273686	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	8234	192.168.2.3	37.0.8.214
07/22/21-10:13:44.446402	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	8234	192.168.2.3	37.0.8.214
07/22/21-10:13:51.623633	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	8234	192.168.2.3	37.0.8.214
07/22/21-10:13:57.692526	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	8234	192.168.2.3	37.0.8.214
07/22/21-10:14:05.154406	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	8234	192.168.2.3	37.0.8.214
07/22/21-10:14:12.712032	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	8234	192.168.2.3	37.0.8.214
07/22/21-10:14:18.043589	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	8234	192.168.2.3	37.0.8.214

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 10:12:32.898813009 CEST	192.168.2.3	8.8.8.8	0x2bc0	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:12:40.395188093 CEST	192.168.2.3	8.8.8.8	0x3636	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:12:48.051269054 CEST	192.168.2.3	8.8.8.8	0xd70c	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:12:55.243602991 CEST	192.168.2.3	8.8.8.8	0xb15c	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:02.021925926 CEST	192.168.2.3	8.8.8.8	0x2265	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:09.345129013 CEST	192.168.2.3	8.8.8.8	0xb607	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:15.940887928 CEST	192.168.2.3	8.8.8.8	0xea1e	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:22.932476044 CEST	192.168.2.3	8.8.8.8	0x5485	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:31.250138044 CEST	192.168.2.3	8.8.8.8	0xf29f	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:38.157721996 CEST	192.168.2.3	8.8.8.8	0x4ef7	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:44.280306101 CEST	192.168.2.3	8.8.8.8	0x6d0a	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:51.347198963 CEST	192.168.2.3	8.8.8.8	0xb158	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:57.575160980 CEST	192.168.2.3	8.8.8.8	0xa0aa	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:14:04.869976997 CEST	192.168.2.3	8.8.8.8	0xf64e	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 10:14:12.535176992 CEST	192.168.2.3	8.8.8.8	0xf46b	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:14:17.928350925 CEST	192.168.2.3	8.8.8.8	0x918f	Standard query (0)	asweee.jum pingcrab.com	A (IP address)	IN (0x0001)

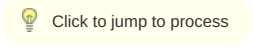
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 10:12:33.077167034 CEST	8.8.8.8	192.168.2.3	0x2bc0	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:12:40.454894066 CEST	8.8.8.8	192.168.2.3	0x3636	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:12:48.132077932 CEST	8.8.8.8	192.168.2.3	0xd70c	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:12:55.300825119 CEST	8.8.8.8	192.168.2.3	0xb15c	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:02.082191944 CEST	8.8.8.8	192.168.2.3	0x2265	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:09.402096987 CEST	8.8.8.8	192.168.2.3	0xb607	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:16.108418941 CEST	8.8.8.8	192.168.2.3	0xea1e	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:22.989346027 CEST	8.8.8.8	192.168.2.3	0x5485	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:31.309767962 CEST	8.8.8.8	192.168.2.3	0xf29f	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:38.214937925 CEST	8.8.8.8	192.168.2.3	0x4ef7	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:44.338745117 CEST	8.8.8.8	192.168.2.3	0x6d0a	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:51.418507099 CEST	8.8.8.8	192.168.2.3	0xb158	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:13:57.634875059 CEST	8.8.8.8	192.168.2.3	0xa0aa	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:14:04.928997993 CEST	8.8.8.8	192.168.2.3	0xf64e	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:14:12.603715897 CEST	8.8.8.8	192.168.2.3	0xf46b	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)
Jul 22, 2021 10:14:17.980721951 CEST	8.8.8.8	192.168.2.3	0x918f	No error (0)	asweee.jum pingcrab.com		37.0.8.214	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: IDeVaZ8ESy.exe PID: 5976 Parent PID: 5624

General

Start time:	10:12:11
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\IDeVaZ8ESy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\IDeVaZ8ESy.exe'
Imagebase:	0xea0000
File size:	565248 bytes
MD5 hash:	B0876B8DA9DCB8A3B22D2CBF2B6A4711
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.253550747.00000000043C7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.253550747.00000000043C7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.253550747.00000000043C7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.253253129.0000000004327000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.253253129.0000000004327000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.253253129.0000000004327000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: IDeVaZ8ESy.exe PID: 1384 Parent PID: 5976

General

Start time:	10:12:25
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe
Imagebase:	0x2a0000
File size:	565248 bytes
MD5 hash:	B0876B8DA9DCB8A3B22D2CBF2B6A4711
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 24%, Virustotal, Browse • Detection: 23%, Metadefender, Browse • Detection: 32%, ReversingLabs

Reputation:	low

Analysis Process: IDeVaZ8ESy.exe PID: 5056 Parent PID: 5976

General

Start time:	10:12:27
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe
Imagebase:	0x8a0000
File size:	565248 bytes
MD5 hash:	B0876B8DA9DCB8A3B22D2CBF2B6A4711
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6064 Parent PID: 5056

General

Start time:	10:12:30
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpBB0F.tmp'
Imagebase:	0x930000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 2476 Parent PID: 6064

General

Start time:	10:12:30
Start date:	22/07/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: IDeVaZ8ESy.exe PID: 5972 Parent PID: 528

General

Start time:	10:12:32
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe 0
Imagebase:	0xf0000
File size:	565248 bytes
MD5 hash:	B0876B8DA9DCB8A3B22D2CBF2B6A4711
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.282656161.00000000026F2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.282656161.00000000026F2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.284916631.0000000003A3A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.284916631.0000000003A3A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.284916631.0000000003A3A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.286367927.0000000003AD9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.286367927.0000000003AD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.286367927.0000000003AD9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: IDeVaZ8ESy.exe PID: 1276 Parent PID: 5972

General

Start time:	10:12:39
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\AppData\Local\Temp\IDeVaZ8ESy.exe
Imagebase:	0x930000
File size:	565248 bytes
MD5 hash:	B0876B8DA9DCB8A3B22D2CBF2B6A4711
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.298170775.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.298170775.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.298170775.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.301106793.0000000003DA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.301106793.0000000003DA9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.300993191.0000000002DA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.300993191.0000000002DA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis