ID: 458908
Sample Name: iGZtra5EaP.exe
Cookbook: default.jbs
Time: 21:11:20
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

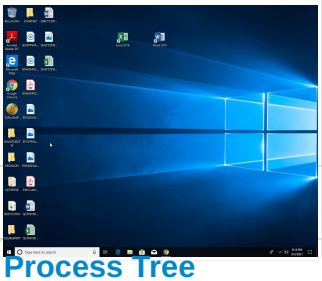
Windows Analysis Report iGZtra5EaP.exe

Overview

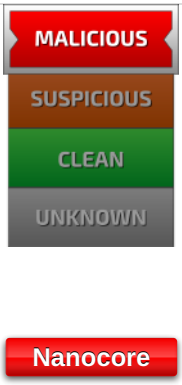
General Information

Sample Name:	iGZtra5EaP.exe
Analysis ID:	458908
MD5:	5abfc84b2a67161.
SHA1:	fb2e5175272b90a.
SHA256:	776e6e841b2a1b..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



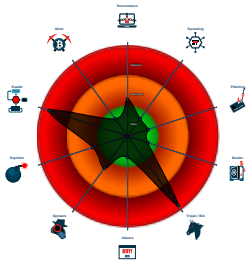
Nanocore

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 doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- iGZtra5EaP.exe (PID: 5832 cmdline: 'C:\Users\user\Desktop\iGZtra5EaP.exe' MD5: 5ABFC84B2A671617A4930A61E218B6C6)
  - schtasks.exe (PID: 6008 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmp3997.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - iGZtra5EaP.exe (PID: 4720 cmdline: {path} MD5: 5ABFC84B2A671617A4930A61E218B6C6)
    - schtasks.exe (PID: 4664 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp489A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 2588 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5556 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp4CC2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- iGZtra5EaP.exe (PID: 1288 cmdline: C:\Users\user\Desktop\iGZtra5EaP.exe 0 MD5: 5ABFC84B2A671617A4930A61E218B6C6)
  - schtasks.exe (PID: 5044 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmpF219.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - iGZtra5EaP.exe (PID: 5016 cmdline: {path} MD5: 5ABFC84B2A671617A4930A61E218B6C6)
- dhcpmon.exe (PID: 496 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 5ABFC84B2A671617A4930A61E218B6C6)
  - schtasks.exe (PID: 5004 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmpF5E2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 3008 cmdline: {path} MD5: 5ABFC84B2A671617A4930A61E218B6C6)
- dhcpmon.exe (PID: 5756 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 5ABFC84B2A671617A4930A61E218B6C6)
  - schtasks.exe (PID: 1036 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmp63D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 5200 cmdline: {path} MD5: 5ABFC84B2A671617A4930A61E218B6C6)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "f0d143be-967c-4293-98d3-3a1e128b",
  "Group": "BotNet",
  "Domain1": "microsoftsecurity.sytes.net",
  "Domain2": "backupnew.duckdns.org",
  "Port": 1177,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Enable",
  "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": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "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
0000001B.00000002.417862891.0000000002A1 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001B.00000002.417862891.0000000002A1 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x6934b:$a: NanoCore • 0x693a4:$a: NanoCore • 0x693e1:$a: NanoCore • 0x6945a:$a: NanoCore • 0x693ad:$b: ClientPlugin • 0x693ea:$b: ClientPlugin • 0x69ce8:$b: ClientPlugin • 0x69cf5:$b: ClientPlugin • 0x5f4d6:$e: KeepAlive • 0x69835:$g: LogClientMessage • 0x697b5:$i: get_Connected • 0x59781:$j: #=q • 0x597b1:$j: #=q • 0x597ed:$j: #=q • 0x59815:$j: #=q • 0x59845:$j: #=q • 0x59875:$j: #=q • 0x598a5:$j: #=q • 0x598d5:$j: #=q • 0x598f1:$j: #=q • 0x59921:$j: #=q
0000000C.00000002.482078580.0000000006E4 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
0000000C.00000002.482078580.0000000006E4 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x350b:$x2: NanoCore.ClientPluginHost • 0x52b6:$s4: PipeCreated • 0x34f8:$s5: IClientLoggingHost
00000021.00000002.428437498.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 96 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.iGZtra5EaP.exe.6de0000.35.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x13a8:$x1: NanoCore.ClientPluginHost
12.2.iGZtra5EaP.exe.6de0000.35.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x13a8:$x2: NanoCore.ClientPluginHost • 0x1486:$s4: PipeCreated • 0x13c2:$s5: IClientLoggingHost
12.2.iGZtra5EaP.exe.6e10000.38.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1deb:$x1: NanoCore.ClientPluginHost • 0x1e24:$x2: IClientNetworkHost
12.2.iGZtra5EaP.exe.6e10000.38.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1deb:$x2: NanoCore.ClientPluginHost • 0x1f36:$s4: PipeCreated • 0x1e05:$s5: IClientLoggingHost
33.2.dhcpmon.exe.3009684.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost

Click to see the 237 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 domain / URL

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

Uses dynamic DNS services

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:

Yara detected AntiVM3

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

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

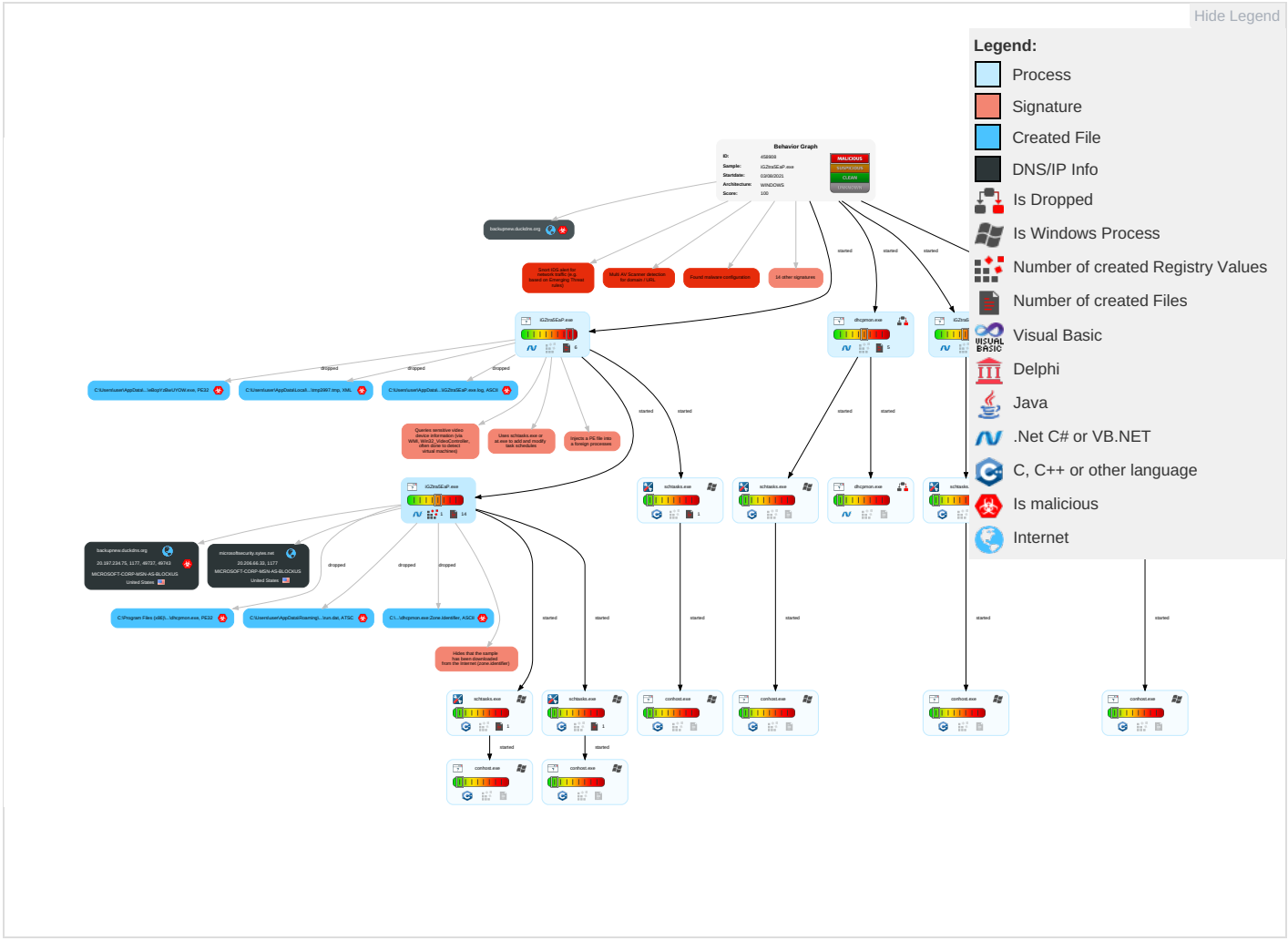
Yara detected Nanocore RAT

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 1 1 2	Masquerading 2	Input Capture 1 1	Security Software Discovery 3 1 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	Process Discovery 2	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 1 3 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 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 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	System Information Discovery 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

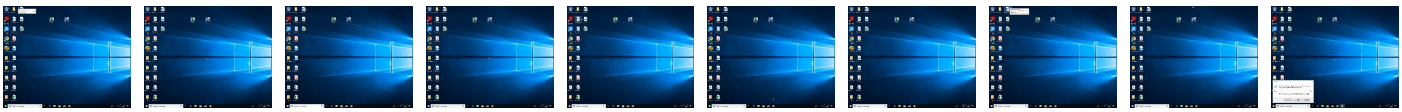
Behavior Graph

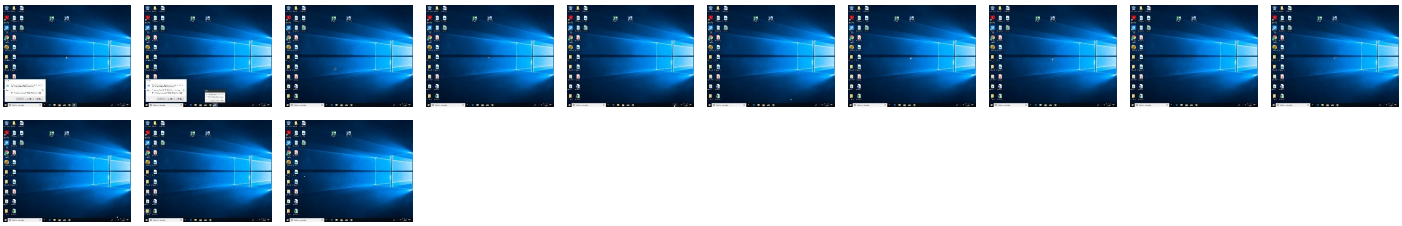


Screenshots

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
iGZtra5EaP.exe	49%	Virustotal		Browse
iGZtra5EaP.exe	64%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
iGZtra5EaP.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\eBopYzBwUYOW.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	64%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\eBopYzBwUYOW.exe	64%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
27.2.iGZtra5EaP.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
30.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.iGZtra5EaP.exe.69d0000.31.unpack	100%	Avira	TR/NanoCore.fadte		Download File
12.2.iGZtra5EaP.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
33.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
backupnew.duckdns.org	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
microsoftsecurity.sytes.net	9%	Virustotal		Browse
microsoftsecurity.sytes.net	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
backupnew.duckdns.org	9%	Virustotal		Browse
backupnew.duckdns.org	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://douglasheriot.com/uno/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
backupnew.duckdns.org	20.197.234.75	true	true	• 9%, Virustotal, Browse	unknown
microsoftsecurity.sytes.net	20.206.66.33	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
microsoftsecurity.sytes.net	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown
backupnew.duckdns.org	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
20.206.66.33	microsoftsecurity.sytes.net	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
20.197.234.75	backupnew.duckdns.org	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458908
Start date:	03.08.2021
Start time:	21:11:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	iGZtra5EaP.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:	43
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@30/15@7/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.8% (good quality ratio 0.5%) • Quality average: 40.1% • Quality standard deviation: 36.9%
HCA Information:	• Successful, ratio: 99% • 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
21:12:54	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
21:12:55	API Interceptor	653x Sleep call for process: iGZtra5EaP.exe modified
21:12:56	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\iGZtra5EaP.exe" s>$(Arg0)
21:12:56	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
backupnew.duckdns.org	y7PKSDpFe0.exe	Get hash	malicious	Browse	• 191.177.183.137

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\iGZtra5EaP.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	788480
Entropy (8bit):	7.405761902599822
Encrypted:	false
SSDEEP:	24576:K+J70cLvBwP+8oUSmntIV+60wST8OQpi:KK70qvFISLZ5I3
MD5:	5ABFC84B2A671617A4930A61E218B6C6
SHA1:	FB2E5175272B90AA204853DD2BA2DC175FF5958F
SHA-256:	776E6E841B2A1B1DACD2BEB12F76949DC9A395A45BD7107475D90B60F09E5F39
SHA-512:	64A5E3C121442007176DE090B4F24FBB7FFE0018BB774431D70B4941EFE9264E23349CF0A83750BEAE6172E05D30C9CBAAFD542F74FA22EDFEE190DD7515DF3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 64%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].`.....x.....^.... .....@.. .....`..... ..@.....O.....@..... ....H.....text...dw... ...x..... ..`.rsrc.....z.....@..@.rel oc.....@.....@..B.....@.....H.....0...._.....0.....*...0.....s....(.....*.0.....(.....*.0.....}.....}.....(.....}..... (...s'...}.....}.....}.....u....,9..o.....(...r...p(....-...o.....(....r...p(....+..+....,...t....s0.....}....*.0..I.....(.... N... !I..a%..^E.....+.... ...Z ..a+....}....*....0..E..... q[0. ..L .a%..^E.....#...+!....$...s#...}..... .(.+Z]r..a+.*....0..

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\iGZtra5EaP.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

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	false
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\Microsoft\CLR_v4.0_32\UsageLogs\iGZtra5EaP.exe.log	
Process:	C:\Users\user\Desktop\iGZtra5EaP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
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\tmp3997.tmp	
Process:	C:\Users\user\Desktop\iGZtra5EaP.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.197051255242617
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBpFtn:cbh47TlNQ//rydbz9I3YODOLNdq3nv
MD5:	F100F4090A302E04A4E5584333049320
SHA1:	69E6D2690B5E7D9BAFD8D69FF8D9ABEA0C34AC01
SHA-256:	A9DFF35D768ED46D311434A85F8BFF2F1B7D02160E6FCE7EFB8A579C90E02BB0
SHA-512:	CF0A3368A7A96FFD4A6DE947120BB61CA61C751DB91458BA4DC77EF2836B1D44E4AD3E464EB21FFD82AE9B1A17196545C09D196DE8D30A1716F383049907743
Malicious:	**true**
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\tmp3997.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp489A.tmp	
Process:	C:\Users\user\Desktop\iGZtra5EaP.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	5.108613782269879
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0zgLrxtn:cbk4oL600QydbQxIYODOLedq3Lvj
MD5:	73882135D094B9C109522AE7A7FB03A0
SHA1:	8455954767A1F42B6393ADCB5CA25E96CA467D7B
SHA-256:	9AD453C7A4F46761E71DC36D48B953E8A8818299E599528545284311EE94C7FF
SHA-512:	9785A28A920F0964EE37087EF8D6C17CC432F982EF88A684CFEA3261BE9CC01B6D89C67E2F631E506154167 86E8D6A36AA8264C9086A0883C90E698B5BCA387E
Malicious:	false
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\Local\Temp\tmp4CC2.tmp	
Process:	C:\Users\user\Desktop\iGZtra5EaP.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
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\Local\Temp\tmp63D.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.197051255242617
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBpFtn:cbh47TlNQ//rydbz9I3YODOLNdq3nv
MD5:	F100F4090A302E04A4E5584333049320
SHA1:	69E6D2690B5E7D9BAFD8D69FF8D9ABEA0C34AC01
SHA-256:	A9DFF35D768ED46D311434A85F8BFF2F1B7D02160E6FCE7EFB8A579C90E02BB0
SHA-512:	CF0A3368A7A96FFD4A6DE947120BB61CA61C751DB91458BA4DC77EF2836B1D44E4AD3E464EB21FFD82AE9B1A17196545C09D196DE8D30A1716F383049907743
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\tmp63D.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpF219.tmp	
Process:	C:\Users\user\Desktop\iGZtra5EaP.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.197051255242617
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBpFtn:cbh47TlNQ//rydbz9I3YODOLNdq3nv
MD5:	F100F4090A302E04A4E5584333049320
SHA1:	69E6D2690B5E7D9BAFD8D69FF8D9ABEA0C34AC01
SHA-256:	A9DFF35D768ED46D311434A85F8BFF2F1B7D02160E6FCE7EFB8A579C90E02BB0
SHA-512:	CF0A3368A7A96FFD4A6DE947120BB61CA61C751DB91458BA4DC77EF2836B1D44E4AD3E464EB21FFD82AE9B1A17196545C09D196DE8D30A1716F383049907743
Malicious:	false
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpF5E2.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.197051255242617
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBpFtn:cbh47TlNQ//rydbz9I3YODOLNdq3nv
MD5:	F100F4090A302E04A4E5584333049320
SHA1:	69E6D2690B5E7D9BAFD8D69FF8D9ABEA0C34AC01
SHA-256:	A9DFF35D768ED46D311434A85F8BFF2F1B7D02160E6FCE7EFB8A579C90E02BB0
SHA-512:	CF0A3368A7A96FFD4A6DE947120BB61CA61C751DB91458BA4DC77EF2836B1D44E4AD3E464EB21FFD82AE9B1A17196545C09D196DE8D30A1716F383049907743
Malicious:	false
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\iGZtra5EaP.exe
File Type:	data
Category:	dropped
Size (bytes):	696
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	12:X4LEnybgCF0uCYKZr+dLEnybgCF0uCYKZr+dLEnybgCF0uCYKZr+K:IQnybgC4jh+dQnybgC4jh+dQnybgC4jp
MD5:	AF6AA7C823112E2342E8D98BE5EDE0A9
SHA1:	D48CA92F4FA11CC9619185563F2D57A6099D21D0
SHA-256:	8D2ACD0CB78A2C690E2DCA1E9C92D273DAF4804DF0B4AC55E14D120C96F7671D
SHA-512:	B822403E85339F4FF2D88608D73DA75A149756FF44454386E1EB2451A6CCCE0F65ECA596F95BBBAD942C963F8C4CA2ADE582D6E50750596DB263BA879FB3ECB1
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\iGZtra5EaP.exe
File Type:	ATSC A/52 aka AC-3 aka Dolby Digital stream, reserved frequency,, emergency (E) 2 front/2 rear,
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:d:d
MD5:	20522AD33E431199BB129A1CA16DC20F
SHA1:	13C39E11506CDFEC1DB5466B527EB0FD330EA995
SHA-256:	C21A5D95DEA000373611071378FFB0EA886D4ED3F351DF8B7F1622B81E159164
SHA-512:	E49AD7E3542762FA4505433CC34A38175C6AD670D25D374104B3D7819F2162ABBA011B9AFD1181717A5FA80143EBEC7412653870F1C63713F2D88D7102BE8468
Malicious:	**true**
Reputation:	unknown
Preview:	.wB!.V.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\iGZtra5EaP.exe
File Type:	data
Category:	modified
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wl8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3A
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..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v."".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_..&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.........Vg.2xC.....O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<._.[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$...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.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\iGZtra5EaP.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.337435460048129
Encrypted:	false
SSDEEP:	3:oNWXp5vMiZXEQgE1J:oNWXpFMgX5Br
MD5:	6C946DFBF2EF9628FED080E3558D6822
SHA1:	B3DF6F9B8483D7F991B1D45AD814E5411CBE9001
SHA-256:	A82D2B0C7E89C7C267181AC684F6319F8EF28CAFD5A4BB4B8792DECB80AD7403
SHA-512:	BF0E078002808DD32BFD4D8757857C64026C091647A79838B49D37F085377569E74D553872D0DB10FF6481958057FFF973EB257AC58F0EC43907004D627CC524
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\iGZtra5EaP.exe

C:\Users\user\AppData\Roaming\eBopYzBwUYOW.exe	
Process:	C:\Users\user\Desktop\iGZtra5EaP.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	788480
Entropy (8bit):	7.405761902599822

C:\Users\user\AppData\Roaming\eBopYzBwUYOW.exe

Encrypted:	false
SSDEEP:	24576:K+J70cLvBwP+8oUSmntlV+60wST8OQpi:KK70qvFISLZ5I3
MD5:	5ABFC84B2A671617A4930A61E218B6C6
SHA1:	FB2E5175272B90AA204853DD2BA2DC175FF5958F
SHA-256:	776E6E841B2A1B1DACD2BEB12F76949DC9A395A45BD7107475D90B60F09E5F39
SHA-512:	64A5E3C121442007176DE090B4F24FBB7FFE0018BB774431D70B4941EFE9264E23349CF0A83750BEAE6172E05D30C9CBAAFD542F74FA22EDFEE190DD7515DF3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 64%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].`.....x.....^.... .....@.. .....`..... ..@.....O.....@..... ....H.....text...dw... ...x..... ..`.rsrc.....z.....@..@.rel oc.....@.....@..B.....@.....H.....0...._.....0.....*....0.....s....(.....*.0.....(.....*.0.....}.....}.....(.....}..... (...s'...}.....}.....}.....u....,9..o.....(....r...p(....-...o.....(....r...p(....+..+....,...t....s0.....}....*.0..I.....(.... N... !l..a%..^E.....+.... ...Z ..a+....}....*....0..E..... q[0. ..L .a%..^E.....#...+!....$...s#...}..... .(.+Z]r..a+.*....0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.405761902599822
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	iGZtra5EaP.exe
File size:	788480
MD5:	5abfc84b2a671617a4930a61e218b6c6
SHA1:	fb2e5175272b90aa204853dd2ba2dc175ff5958f
SHA256:	776e6e841b2a1b1dacd2beb12f76949dc9a395a45bd7107475d90b60f09e5f39
SHA512:	64a5e3c121442007176de090b4f24fbb7ffe0018bb774431d70b4941efe9264e23349cf0a83750beae6172e05d30c9cbaafd542f74fa22edfee190dd7515df36
SSDEEP:	24576:K+J70cLvBwP+8oUSmntlV+60wST8OQpi:KK70qvFISLZ5I3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].`.....x.....^.... .....@.. .....`.....@.....

File Icon

Icon Hash:	f8beee8f9792cc60

Static PE Info

General

Entrypoint:	0x4a975e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60FF5D0A [Tue Jul 27 01:10:34 2021 UTC]
TLS Callbacks:	

General

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	0xa7764	0xa7800	False	0.768110132929	data	7.50200224495	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x18a1c	0x18c00	False	0.646977588384	data	6.18338598117	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc4000	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
08/03/21-21:13:53.952166	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	1177	192.168.2.3	20.197.234.75
08/03/21-21:14:01.197544	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	1177	192.168.2.3	20.197.234.75
08/03/21-21:14:08.027723	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	1177	192.168.2.3	20.197.234.75
08/03/21-21:14:15.852637	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	1177	192.168.2.3	20.197.234.75

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 21:12:57.517040014 CEST	192.168.2.3	8.8.8.8	0x2fa0	Standard query (0)	microsoftsecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:13:16.810172081 CEST	192.168.2.3	8.8.8.8	0xced5	Standard query (0)	microsoftsecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:13:35.243072987 CEST	192.168.2.3	8.8.8.8	0x56c6	Standard query (0)	microsoftsecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:13:53.562072992 CEST	192.168.2.3	8.8.8.8	0x3bf6	Standard query (0)	backupnew.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 21:14:00.827917099 CEST	192.168.2.3	8.8.8.8	0x5378	Standard query (0)	backupnew.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 21:14:07.783363104 CEST	192.168.2.3	8.8.8.8	0xa0b0	Standard query (0)	backupnew.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 21:14:15.611778975 CEST	192.168.2.3	8.8.8.8	0xdf8f	Standard query (0)	backupnew.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 21:12:57.551525116 CEST	8.8.8.8	192.168.2.3	0x2fa0	No error (0)	microsoftsecurity.sytes.net		20.206.66.33	A (IP address)	IN (0x0001)
Aug 3, 2021 21:13:16.852745056 CEST	8.8.8.8	192.168.2.3	0xced5	No error (0)	microsoftsecurity.sytes.net		20.206.66.33	A (IP address)	IN (0x0001)
Aug 3, 2021 21:13:35.278100014 CEST	8.8.8.8	192.168.2.3	0x56c6	No error (0)	microsoftsecurity.sytes.net		20.206.66.33	A (IP address)	IN (0x0001)
Aug 3, 2021 21:13:53.690700054 CEST	8.8.8.8	192.168.2.3	0x3bf6	No error (0)	backupnew.duckdns.org		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 21:14:00.968957901 CEST	8.8.8.8	192.168.2.3	0x5378	No error (0)	backupnew.duckdns.org		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 21:14:07.818789959 CEST	8.8.8.8	192.168.2.3	0xa0b0	No error (0)	backupnew.duckdns.org		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 21:14:15.644599915 CEST	8.8.8.8	192.168.2.3	0xdf8f	No error (0)	backupnew.duckdns.org		20.197.234.75	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iGZtra5EaP.exe PID: 5832 Parent PID: 5496

General

Start time:	21:12:07
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\iGZtra5EaP.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\iGZtra5EaP.exe'
Imagebase:	0x950000
File size:	788480 bytes
MD5 hash:	5ABFC84B2A671617A4930A61E218B6C6
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: 00000000.00000002.294511650.0000000003CC9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.294511650.0000000003CC9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.294511650.0000000003CC9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.293558443.0000000002CC1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6008 Parent PID: 5832

General

Start time:	21:12:49
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmp3997.tmp'
Imagebase:	0xae0000
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: 5896 Parent PID: 6008

General

Start time:	21:12:50
Start date:	03/08/2021
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: iGZtra5EaP.exe PID: 4720 Parent PID: 5832

General

Start time:	21:12:51
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\iGZtra5EaP.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xef0000
File size:	788480 bytes
MD5 hash:	5ABFC84B2A671617A4930A61E218B6C6
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.00000002.482078580.0000000006E40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.482078580.0000000006E40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.476961664.000000000454E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.476961664.000000000454E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.477178193.000000000465D000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.477178193.000000000465D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.482179100.0000000006E90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.482179100.0000000006E90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.471078718.0000000001AD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.471078718.0000000001AD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.475401082.000000000374C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.481910813.0000000006DB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.481910813.0000000006DB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.481995550.0000000006E00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.481995550.0000000006E00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.481497763.00000000069D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.481497763.00000000069D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.481497763.00000000069D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.482020693.0000000006E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.482020693.0000000006E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.481961618.0000000006DE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.481961618.0000000006DE0000.00000004.00000001.sdmp,

	Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.481945946.0000000006DD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.481945946.0000000006DD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.467302367.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.467302367.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.467302367.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.482036750.0000000006E20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.482036750.0000000006E20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.473787584.00000000034F7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.480093816.0000000005EC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.480093816.0000000005EC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.482102080.0000000006E50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.482102080.0000000006E50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.477941629.00000000048DF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.477941629.00000000048DF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.480306697.0000000006760000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.480306697.0000000006760000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.476599395.00000000044C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.476599395.00000000044C9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.476392070.0000000004481000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.476392070.0000000004481000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.481978911.0000000006DF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.481978911.0000000006DF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.472713339.0000000003481000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 4664 Parent PID: 4720

General

Start time:	21:12:53
Start date:	03/08/2021
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\tmp489A.tmp'
Imagebase:	0xae0000
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: 2588 Parent PID: 4664

General

Start time:	21:12:53
Start date:	03/08/2021
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: schtasks.exe PID: 5556 Parent PID: 4720

General

Start time:	21:12:54
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp4CC2.tmp'
Imagebase:	0xae0000
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: 256 Parent PID: 5556

General

Start time:	21:12:54
Start date:	03/08/2021
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: iGZtra5EaP.exe PID: 1288 Parent PID: 528

General

Start time:	21:12:56
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\iGZtra5EaP.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\iGZtra5EaP.exe 0
Imagebase:	0x630000
File size:	788480 bytes
MD5 hash:	5ABFC84B2A671617A4930A61E218B6C6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000011.00000002.398277931.0000000002B51000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.400817271.0000000003B59000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.400817271.0000000003B59000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.400817271.0000000003B59000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: dhcpmon.exe PID: 496 Parent PID: 528

General

Start time:	21:12:57
Start date:	03/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xc60000
File size:	788480 bytes
MD5 hash:	5ABFC84B2A671617A4930A61E218B6C6
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: 00000012.00000002.404628541.0000000004099000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.404628541.0000000004099000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.404628541.0000000004099000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000012.00000002.400511596.0000000003091000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 64%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: dhcpmon.exe PID: 5756 Parent PID: 3388

General

Start time:	21:13:03
Start date:	03/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xc20000
File size:	788480 bytes
MD5 hash:	5ABFC84B2A671617A4930A61E218B6C6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.411142657.0000000003141000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.412689646.0000000004149000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.412689646.0000000004149000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.412689646.0000000004149000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: schtasks.exe PID: 5044 Parent PID: 1288

General

Start time:	21:13:37
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmpF219.tmp'
Imagebase:	0xae0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5096 Parent PID: 5044

General

Start time:	21:13:38
Start date:	03/08/2021
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: iGZtra5EaP.exe PID: 5016 Parent PID: 1288

General

Start time:	21:13:38
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\iGZtra5EaP.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x520000
File size:	788480 bytes
MD5 hash:	5ABFC84B2A671617A4930A61E218B6C6

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.417862891.0000000002A11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.417862891.0000000002A11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000002.415827598.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.415827598.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.415827598.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.418018556.0000000003A19000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.418018556.0000000003A19000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: schtasks.exe PID: 5004 Parent PID: 496

General

Start time:	21:13:38
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmpF5E2.tmp'
Imagebase:	0xae0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1324 Parent PID: 5004

General

Start time:	21:13:39
Start date:	03/08/2021
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

Analysis Process: dhcpmon.exe PID: 3008 Parent PID: 496

General

Start time:	21:13:40

Start date:	03/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb20000
File size:	788480 bytes
MD5 hash:	5ABFC84B2A671617A4930A61E218B6C6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.422052368.0000000003011000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.422052368.0000000003011000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001E.00000002.417477798.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.417477798.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.417477798.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.423536148.0000000004019000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.423536148.0000000004019000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: schtasks.exe PID: 1036 Parent PID: 5756

General

Start time:	21:13:43
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmp63D.tmp'
Imagebase:	0xae0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5072 Parent PID: 1036

General

Start time:	21:13:43
Start date:	03/08/2021
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

Analysis Process: dhcpmon.exe PID: 5200 Parent PID: 5756

General

Start time:	21:13:44
Start date:	03/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb10000
File size:	788480 bytes
MD5 hash:	5ABFC84B2A671617A4930A61E218B6C6
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: 00000021.00000002.428437498.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000002.428437498.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.428437498.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000002.431850871.0000000003FA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.431850871.0000000003FA9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000002.431679291.0000000002FA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.431679291.0000000002FA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis