ID: 458234
Sample Name:
oGZg708edu.exe
Cookbook: default.jbs
Time: 04:17:10
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

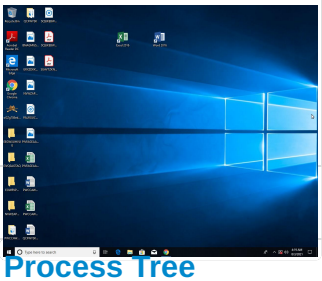
Windows Analysis Report oGZg708edu.exe

Overview

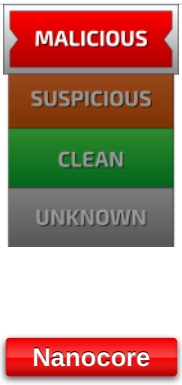
General Information

Sample Name:	oGZg708edu.exe
Analysis ID:	458234
MD5:	a12a9c428510a3..
SHA1:	ff6c453d63faf3d6..
SHA256:	639d614a07d341..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

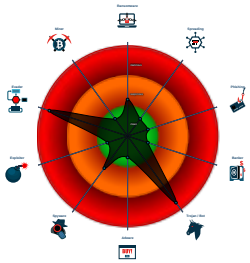


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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**
- oGZg708edu.exe (PID: 3152 cmdline: 'C:\Users\user\Desktop\oGZg708edu.exe' MD5: A12A9C428510A3EE87C68078C3633F69)
  - schtasks.exe (PID: 4948 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmpCB9C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - oGZg708edu.exe (PID: 2000 cmdline: {path} MD5: A12A9C428510A3EE87C68078C3633F69)
  - oGZg708edu.exe (PID: 5424 cmdline: {path} MD5: A12A9C428510A3EE87C68078C3633F69)
  - oGZg708edu.exe (PID: 4404 cmdline: {path} MD5: A12A9C428510A3EE87C68078C3633F69)
    - schtasks.exe (PID: 3156 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpDEB6.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4276 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 3596 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpE241.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 3292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- oGZg708edu.exe (PID: 492 cmdline: C:\Users\user\Desktop\oGZg708edu.exe 0 MD5: A12A9C428510A3EE87C68078C3633F69)
  - schtasks.exe (PID: 5640 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmp7633.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3032 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - oGZg708edu.exe (PID: 5280 cmdline: {path} MD5: A12A9C428510A3EE87C68078C3633F69)
  - oGZg708edu.exe (PID: 5252 cmdline: {path} MD5: A12A9C428510A3EE87C68078C3633F69)
- dhcpmon.exe (PID: 3440 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: A12A9C428510A3EE87C68078C3633F69)
  - schtasks.exe (PID: 5324 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmp8650.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5304 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 5348 cmdline: {path} MD5: A12A9C428510A3EE87C68078C3633F69)
- dhcpmon.exe (PID: 4744 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: A12A9C428510A3EE87C68078C3633F69)
  - schtasks.exe (PID: 3260 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmp990D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2024 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6100 cmdline: {path} MD5: A12A9C428510A3EE87C68078C3633F69)
- **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
00000011.00000002.469053932.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000011.00000002.469053932.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000011.00000002.469053932.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000024.00000002.419402447.000000000409000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000024.00000002.419402447.000000000408 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x435bd:$a: NanoCore • 0x43616:$a: NanoCore • 0x43653:$a: NanoCore • 0x436cc:$a: NanoCore • 0x56d77:$a: NanoCore • 0x56d8c:$a: NanoCore • 0x56dc1:$a: NanoCore • 0x6fd73:$a: NanoCore • 0x6fd88:$a: NanoCore • 0x6fdbd:$a: NanoCore • 0x4361f:$b: ClientPlugin • 0x4365c:$b: ClientPlugin • 0x43f5a:$b: ClientPlugin • 0x43f67:$b: ClientPlugin • 0x56b33:$b: ClientPlugin • 0x56b4e:$b: ClientPlugin • 0x56b7e:$b: ClientPlugin • 0x56d95:$b: ClientPlugin • 0x56dca:$b: ClientPlugin • 0x6fb2f:$b: ClientPlugin • 0x6fb4a:$b: ClientPlugin
Click to see the 65 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
36.2.dhcpmon.exe.40d0614.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
36.2.dhcpmon.exe.40d0614.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
36.2.dhcpmon.exe.40d0614.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
36.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
36.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
Click to see the 134 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

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

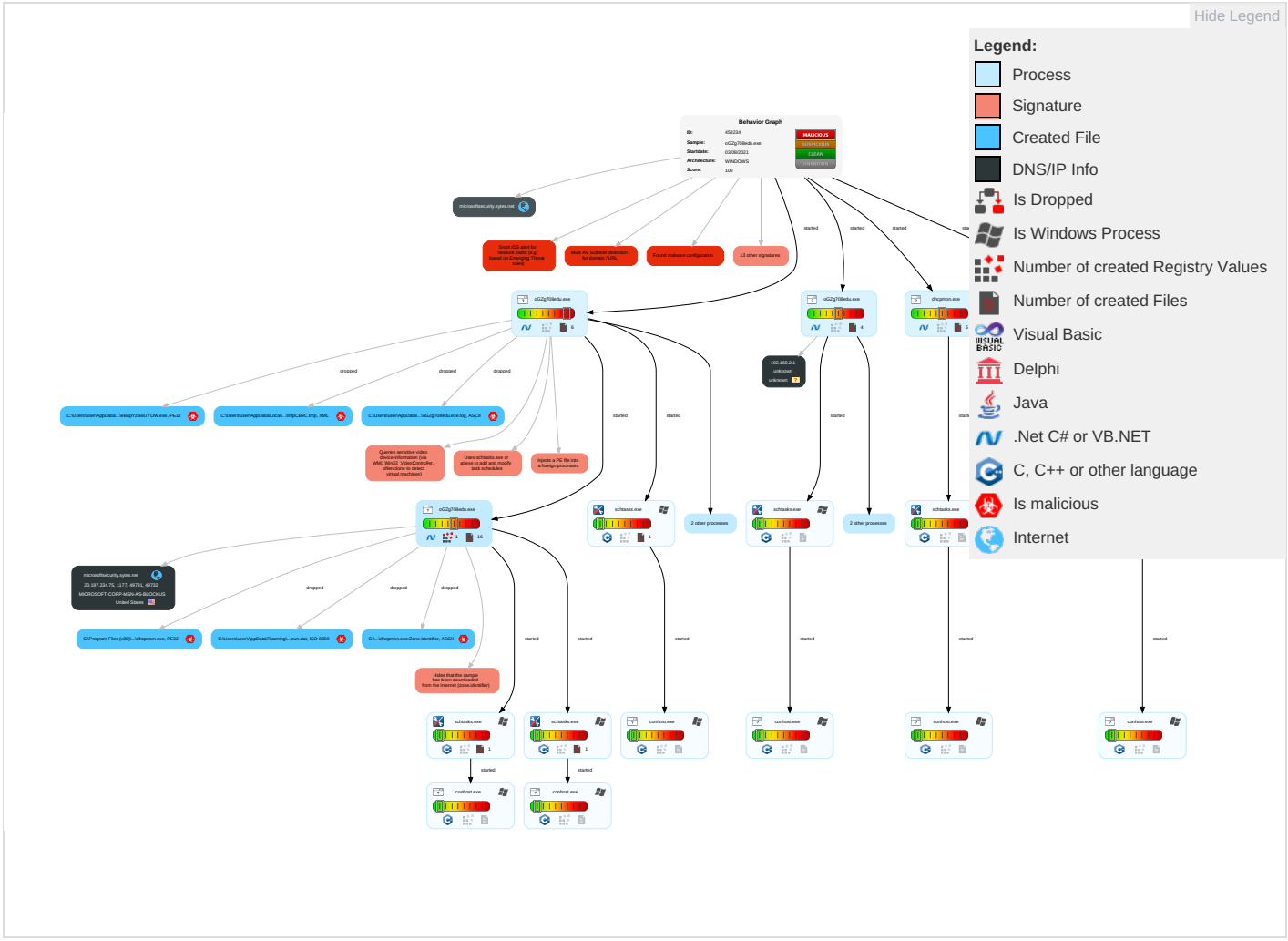
Remote Access Functionality:

- 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 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 2	Input Capture 1 1	Security Software Discovery 3 2 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 Acce 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
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 1 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 Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	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 Protocc

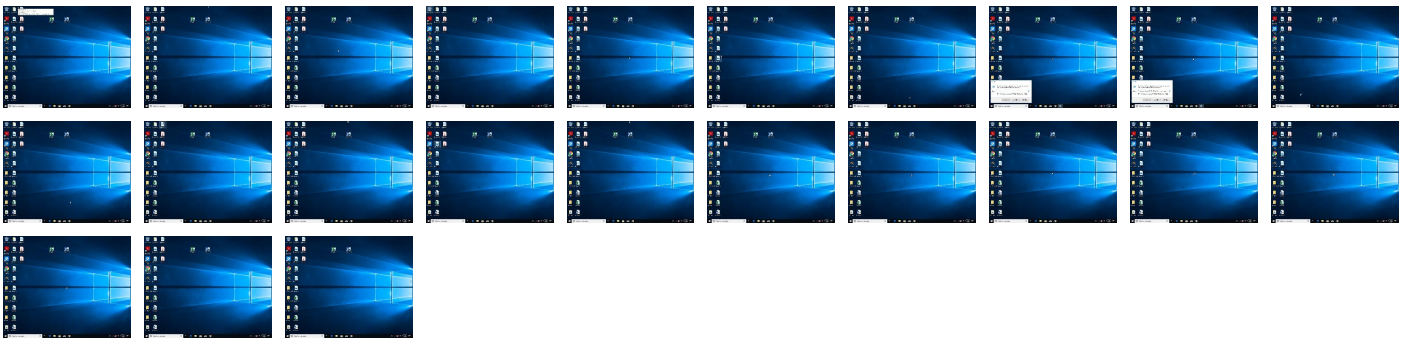
Behavior Graph



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
oGZg708edu.exe	53%	Virustotal		Browse
oGZg708edu.exe	81%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
oGZg708edu.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	53%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	81%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\eBopYzBwUYOW.exe	81%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
36.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.2.oGZg708edu.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
33.2.oGZg708edu.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
40.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

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
microsoftsecurity.sytes.net	20.197.234.75	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
20.197.234.75	microsoftsecurity.sytes.net	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458234
Start date:	03.08.2021
Start time:	04:17:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	oGZg708edu.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@36/17@12/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.2% (good quality ratio 0.8%) • Quality average: 40.2% • Quality standard deviation: 36.8%
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
04:18:44	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\oGZg708edu.exe" s>$(Arg0)
04:18:44	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
04:18:45	API Interceptor	673x Sleep call for process: oGZg708edu.exe modified
04:18:47	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

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\oGZg708edu.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	840192
Entropy (8bit):	7.166906857781212
Encrypted:	false
SSDEEP:	24576:x+J70cLvBwP+8oUSmntIV+60wST8OQpiy:xK70qvFISLZ5I3
MD5:	A12A9C428510A3EE87C68078C3633F69
SHA1:	FF6C453D63FAF3D63ECD17E172E9E8601478911B
SHA-256:	639D614A07D34139806093F8C24190E1DE1E463620B4C852AB0F5A089029F6A6
SHA-512:	3791BD990B51F6B511597F02A95E0D1459BCE7E9835171071132D9C48F4390F2C2AD354BD780D97D947DF288B1E2FC2AFA815BB89CA83B31B68D4A710D8A2C1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 53%, Browse • Antivirus: ReversingLabs, Detection: 81%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].`.....x...X.....^.... .....@.. ..... ..... ..@.....O.....T..... ..... ..H.....text...dw... ...x..... ..`.rsrc....T.....V...z.....@..@.rel oc.....@..B.....@.....H.....0...._.....0.....*....0.....s....(.....*.0.....(.....*.0.....}.....}.....(.....}.....(...s'... }.....}.....}.....u....,9..o.....(....r...p(....-...o.....(....r...p(....+..+....,...t....s0.....}....*.0..I.....(.... N... !l..a%..^E.....+.... ...Z ..a+....}....*....0..E..... q[0. ..L.a%..^E... .....#...+!....$...s#...}..... .(.+Z]r..a+.*....0..

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\oGZg708edu.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\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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
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\oGZg708edu.exe.log	
Process:	C:\Users\user\Desktop\oGZg708edu.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\tmp7633.tmp	
Process:	C:\Users\user\Desktop\oGZg708edu.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\tmp8650.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

C:\Users\user\AppData\Local\Temp\tmp8650.tmp	
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\tmp990D.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\Local\Temp\tmpCB9C.tmp	
Process:	C:\Users\user\Desktop\oGZg708edu.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
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\tmpDEB6.tmp	
Process:	C:\Users\user\Desktop\oGZg708edu.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	5.116011525193795
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Sxtn:cbk4oL600QydbQxIYODOLedq39j
MD5:	A4616A9969F52416137AF93B0850A147

C:\Users\user\AppData\Local\Temp\tmpDEB6.tmp	
SHA1:	87249D767458390015CEAE9F0E15282C9E7D1552
SHA-256:	6EF2344883ECD186A5F7AFC53284B605FC0BD9E01D5A7F149ED3C50BEB03AC78
SHA-512:	3716BF79E3D160E1140A345F72A81E935F5284C83C33F2E114D01F97F53E4EC8DCC6E96E93796FBFE8828F1AF05CF9E13D2FABF1E96F77862D2F6A198EF976F9
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>.. <StopIfGoingOnBatterie s>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAv ailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </Idl eSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpE241.tmp	
Process:	C:\Users\user\Desktop\oGZg708edu.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>.. <StopIfGoingOnBatterie s>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAv ailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </Idl eSettings>.. <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\Desktop\oGZg708edu.exe
File Type:	data
Category:	dropped
Size (bytes):	1624
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhL
MD5:	74AACAE24C76D8BE7578A460BAE23521
SHA1:	523B694F22C1E962B7234BE9637DA09060CFB0C1
SHA-256:	2EFF42A56A82D1EB8E689FE73F5471B111FA17F1ECF72B90A731B59AFF691BFB
SHA-512:	5D715F8D14841552E280A9A5A5F749B23EEEBE713F7E95B288D921982800F2AB1FAAFDA67E420F28D882BF5904799E6BE62D4CAE451507FFB5EC3631B5D11FF6
Malicious:	false
Reputation:	unknown
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......[.&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.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\oGZg708edu.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:nV4:nu
MD5:	D15DECD1081B46827663AF9CF4EACEE8
SHA1:	90EAA0C7BF0E4A3DAF1162DA6E6D4AA40F36D7E5
SHA-256:	01E59B5DB6B8A084D8E868E1B1A3BDC02930E3A4D1F4CA6BA6B92D5D8F19E262

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA-512:	2462E2F3F8EF9AF4A7F828E3E3D94C93BCA6D9E809979B7A24EBFDCC9749C4E4488ECF09EE290BD3ABD05AA6E1EE687DDCB098582ABAB8ED098CCB7B609BD663
Malicious:	**true**
Reputation:	unknown
Preview:	B..spV.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\oGZg708edu.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F97
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\oGZg708edu.exe
File Type:	data
Category:	modified
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYVsRLY6oRDT6P2bfVn1:RzWDlfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A6
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\oGZg708edu.exe
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wI8lkWmtjJ/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..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV.,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.Ql..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC.....O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$...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\oGZg708edu.exe
File Type:	ASCII text, with no line terminators

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.3887904473424575
Encrypted:	false
SSDEEP:	3:oNWXp5vKcx1Nn:oNWXpFKUn
MD5:	EC481BDB5F700B5C4C9976C193C5C9D0
SHA1:	4B244ECDB1AE925A6B5D61AE68F5069F6438D03B
SHA-256:	0923133BA507F2D574D794913F1BBC700DDECFA6C5F834853B39B52DF8B8C223
SHA-512:	E7AB69E5A1C843A6EF3B878394A9E5198A61851761095F64F89ABC2FFF5852B5745262ECD6FA5C263F112643111FF08AC7EC9BE296DE5C7C2BCA4C3F1A8ABF9D
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\oGZg708edu.exe

C:\Users\user\AppData\Roaming\eBopYzBwUYOW.exe	
Process:	C:\Users\user\Desktop\oGZg708edu.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	840192
Entropy (8bit):	7.166906857781212
Encrypted:	false
SSDEEP:	24576:x+J70cLvBwP+8oUSmntIV+60wST8OQpiy:xK70qvFISLZ5I3
MD5:	A12A9C428510A3EE87C68078C3633F69
SHA1:	FF6C453D63FAF3D63ECD17E172E9E8601478911B
SHA-256:	639D614A07D34139806093F8C24190E1DE1E463620B4C852AB0F5A089029F6A6
SHA-512:	3791BD990B51F6B511597F02A95E0D1459BCE7E9835171071132D9C48F4390F2C2AD354BD780D97D947DF288B1E2FC2AFA815BB89CA83B31B68D4A710D8A2C1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 81%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].`.....x...X.....^.... .....@.. ..... ..... ..@.....O.....T..... ..... ..H.....text...dw... ...x..... ..`.rsrc....T.....V...z.....@..@.rel oc.....@..B.....@.....H.....0...._.....0.....*....0.....s....(.....*.0.....(.....*.0.....}.....}.....(.....}.....(...s'... }.....}.....}.....u....,9..o.....(....r...p(....-...o.....(....r...p(....+..+.....t....s0.....}....*.0..I.....(.... N... !l..a%..^E.....+.... ...Z ..a+....}....*....0..E..... q[0. ..L.a%..^E... .....#...+!....$...s#...}..... .(.+Z]r..a+.*....0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.166906857781212
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:	oGZg708edu.exe
File size:	840192
MD5:	a12a9c428510a3ee87c68078c3633f69
SHA1:	ff6c453d63faf3d63ecd17e172e9e8601478911b
SHA256:	639d614a07d34139806093f8c24190e1de1e463620b4c852ab0f5a089029f6a6
SHA512:	3791bd990b51f6b511597f02a95e0d1459bce7e9835171071132d9c48f4390f2c2ad354bd780d97d947df288b1e2fc2afa815bb89ca83b31b68d4a710d8a2c11
SSDEEP:	24576:x+J70cLvBwP+8oUSmntIV+60wST8OQpiy:xK70qvFISLZ5I3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].`.....x...X.....^.... .....@.. ....@.....

File Icon

Icon Hash:	00e87160ec8e11c4

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:	
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	0x25480	0x25600	False	0.499973871237	data	5.05166248803	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	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
08/03/21-04:18:47.741441	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	1177	192.168.2.3	20.197.234.75
08/03/21-04:18:54.505511	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	1177	192.168.2.3	20.197.234.75
08/03/21-04:18:59.595151	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	1177	192.168.2.3	20.197.234.75
08/03/21-04:19:07.000289	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	1177	192.168.2.3	20.197.234.75
08/03/21-04:19:14.314203	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	1177	192.168.2.3	20.197.234.75

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-04:19:21.157290	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	1177	192.168.2.3	20.197.234.75
08/03/21-04:19:28.704182	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	1177	192.168.2.3	20.197.234.75
08/03/21-04:19:35.693482	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	1177	192.168.2.3	20.197.234.75
08/03/21-04:19:43.223929	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	1177	192.168.2.3	20.197.234.75
08/03/21-04:19:50.131484	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	1177	192.168.2.3	20.197.234.75
08/03/21-04:19:57.336641	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	1177	192.168.2.3	20.197.234.75
08/03/21-04:20:04.126786	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	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 04:18:47.383886099 CEST	192.168.2.3	8.8.8.8	0x461d	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 04:18:54.262795925 CEST	192.168.2.3	8.8.8.8	0xec25	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 04:18:59.348112106 CEST	192.168.2.3	8.8.8.8	0x32bf	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:06.734199047 CEST	192.168.2.3	8.8.8.8	0x176d	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:14.065514088 CEST	192.168.2.3	8.8.8.8	0x778	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:20.914865017 CEST	192.168.2.3	8.8.8.8	0x5041	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:28.460050106 CEST	192.168.2.3	8.8.8.8	0x756	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:35.175431013 CEST	192.168.2.3	8.8.8.8	0xcfdb	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:42.992228985 CEST	192.168.2.3	8.8.8.8	0xe000	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:49.874043941 CEST	192.168.2.3	8.8.8.8	0xcaa1	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:57.053425074 CEST	192.168.2.3	8.8.8.8	0xcc57	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 04:20:03.876873016 CEST	192.168.2.3	8.8.8.8	0xbdbc	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 04:18:47.418164968 CEST	8.8.8.8	192.168.2.3	0x461d	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 04:18:54.295703888 CEST	8.8.8.8	192.168.2.3	0xec25	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 04:18:59.383363962 CEST	8.8.8.8	192.168.2.3	0x32bf	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:06.769438028 CEST	8.8.8.8	192.168.2.3	0x176d	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:14.101072073 CEST	8.8.8.8	192.168.2.3	0x778	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 04:19:20.949115038 CEST	8.8.8.8	192.168.2.3	0x5041	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:28.492324114 CEST	8.8.8.8	192.168.2.3	0x756	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:35.210721970 CEST	8.8.8.8	192.168.2.3	0xcfdb	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:43.016822100 CEST	8.8.8.8	192.168.2.3	0xe000	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:49.908018112 CEST	8.8.8.8	192.168.2.3	0xcaa1	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 04:19:57.086298943 CEST	8.8.8.8	192.168.2.3	0xcc57	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 04:20:03.915702105 CEST	8.8.8.8	192.168.2.3	0xbdbc	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: oGZg708edu.exe PID: 3152 Parent PID: 5680

General

Start time:	04:17:58
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\oGZg708edu.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\oGZg708edu.exe'
Imagebase:	0xd00000
File size:	840192 bytes
MD5 hash:	A12A9C428510A3EE87C68078C3633F69
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: 00000001.00000002.296057400.0000000003161000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.297604330.0000000004260000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.297604330.0000000004260000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.297604330.0000000004260000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.297034302.0000000004169000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.297034302.0000000004169000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.297034302.0000000004169000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 4948 Parent PID: 3152

General

Start time:	04:18:39
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\tmpCB9C.tmp'
Imagebase:	0xa30000
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: 1968 Parent PID: 4948

General

Start time:	04:18:39
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
Reputation:	high

Analysis Process: oGZg708edu.exe PID: 2000 Parent PID: 3152

General

Start time:	04:18:40
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\oGZg708edu.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x170000
File size:	840192 bytes
MD5 hash:	A12A9C428510A3EE87C68078C3633F69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: oGZg708edu.exe PID: 5424 Parent PID: 3152

General

Start time:	04:18:40
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\oGZg708edu.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x110000
File size:	840192 bytes
MD5 hash:	A12A9C428510A3EE87C68078C3633F69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: oGZg708edu.exe PID: 4404 Parent PID: 3152

General

Start time:	04:18:41
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\oGZg708edu.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xe10000
File size:	840192 bytes
MD5 hash:	A12A9C428510A3EE87C68078C3633F69
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: 00000011.00000002.469053932.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.469053932.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.469053932.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.474117189.000000000321E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.479023933.0000000004CE8000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.479023933.0000000004CE8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.473767841.00000000031B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.478473398.00000000041B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.478473398.00000000041B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.478830783.0000000004B18000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.478830783.0000000004B18000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
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: 3156 Parent PID: 4404

General

Start time:	04:18:43
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\tmpDEB6.tmp'
Imagebase:	0xa30000
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: 4276 Parent PID: 3156

General

Start time:	04:18:43
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
Reputation:	high

Analysis Process: schtasks.exe PID: 3596 Parent PID: 4404

General

Start time:	04:18:44
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\tmpE241.tmp'
Imagebase:	0xa30000
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: oGZg708edu.exe PID: 492 Parent PID: 528

General

Start time:	04:18:44
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\oGZg708edu.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\oGZg708edu.exe 0
Imagebase:	0xab0000
File size:	840192 bytes
MD5 hash:	A12A9C428510A3EE87C68078C3633F69
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: 00000015.00000002.395101501.0000000003E99000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.395101501.0000000003E99000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.395101501.0000000003E99000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000015.00000002.393602382.0000000002E91000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 3292 Parent PID: 3596

General

Start time:	04:18:44
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: dhcpmon.exe PID: 3440 Parent PID: 528

General

Start time:	04:18:47
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:	0xcd0000
File size:	840192 bytes
MD5 hash:	A12A9C428510A3EE87C68078C3633F69
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: 00000017.00000002.401094970.00000000030F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000002.404321195.00000000040F9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.404321195.00000000040F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.404321195.00000000040F9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 53%, Virustotal, Browse • Detection: 81%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: dhcpmon.exe PID: 4744 Parent PID: 3388

General

Start time:	04:18:52
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:	0xdf0000
File size:	840192 bytes
MD5 hash:	A12A9C428510A3EE87C68078C3633F69
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: 00000018.00000002.410009096.00000000032F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.412621241.00000000042F9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.412621241.00000000042F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.412621241.00000000042F9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: schtasks.exe PID: 5640 Parent PID: 492

General

Start time:	04:19:24
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\tmp7633.tmp'

Imagebase:	0xa30000
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: 3032 Parent PID: 5640

General

Start time:	04:19:24
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: oGZg708edu.exe PID: 5280 Parent PID: 492

General

Start time:	04:19:25
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\oGZg708edu.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x100000
File size:	840192 bytes
MD5 hash:	A12A9C428510A3EE87C68078C3633F69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: oGZg708edu.exe PID: 5252 Parent PID: 492

General

Start time:	04:19:26
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\oGZg708edu.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa80000
File size:	840192 bytes
MD5 hash:	A12A9C428510A3EE87C68078C3633F69
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: 00000021.00000002.411088159.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000002.411088159.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.411088159.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000002.412991615.0000000003E49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.412991615.0000000003E49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000002.412767434.0000000002E41000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.412767434.0000000002E41000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: schtasks.exe PID: 5324 Parent PID: 3440

General

Start time:	04:19:27
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\tmp8650.tmp'
Imagebase:	0xa30000
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: 5304 Parent PID: 5324

General

Start time:	04:19:28
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: dhcpmon.exe PID: 5348 Parent PID: 3440

General

Start time:	04:19:29
Start date:	03/08/2021

Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xcf0000
File size:	840192 bytes
MD5 hash:	A12A9C428510A3EE87C68078C3633F69
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: 00000024.00000002.419402447.0000000004089000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000024.00000002.419402447.0000000004089000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000024.00000002.419130064.0000000003081000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000024.00000002.419130064.0000000003081000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000024.00000002.416229254.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000024.00000002.416229254.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000024.00000002.416229254.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: schtasks.exe PID: 3260 Parent PID: 4744

General

Start time:	04:19:32
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\tmp990D.tmp'
Imagebase:	0xa30000
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: 2024 Parent PID: 3260

General

Start time:	04:19:32
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: 6100 Parent PID: 4744

General

Start time:	04:19:33
Start date:	03/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x670000
File size:	840192 bytes
MD5 hash:	A12A9C428510A3EE87C68078C3633F69
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: 00000028.00000002.428759376.0000000002AF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000028.00000002.428759376.0000000002AF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000028.00000002.428863955.0000000003AF9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000028.00000002.428863955.0000000003AF9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.427422564.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000028.00000002.427422564.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000028.00000002.427422564.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis