ID: 458901
Sample Name:
gcsEBQO3BV.exe
Cookbook: default.jbs
Time: 21:01:16
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report gcsEBQO3BV.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 6
AV Detection: 6
E-Banking Fraud: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Jbx Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
Private 11
General Information 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 17
General 17
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18
Data Directories 18
Sections 18
Resources 18
Imports 18
Version Infos 18
Network Behavior 18
Snort IDS Alerts 18
Network Port Distribution 19
TCP Packets 19
UDP Packets 19
DNS Queries 19

DNS Answers 19
Code Manipulations 20
Statistics 20
Behavior 20
System Behavior 20
Analysis Process: gcsEBQO3BV.exe PID: 6300 Parent PID: 6084 20
General 20
File Activities 20
File Created 20
File Deleted 20
File Written 21
File Read 21
Analysis Process: schtasks.exe PID: 4240 Parent PID: 6300 21
General 21
File Activities 21
File Read 21
Analysis Process: conhost.exe PID: 4972 Parent PID: 4240 21
General 21
Analysis Process: gcsEBQO3BV.exe PID: 3484 Parent PID: 6300 21
General 21
Analysis Process: gcsEBQO3BV.exe PID: 6100 Parent PID: 6300 22
General 22
File Activities 23
File Created 23
File Deleted 23
File Written 23
File Read 23
Registry Activities 23
Key Value Created 23
Analysis Process: schtasks.exe PID: 6416 Parent PID: 6100 23
General 23
File Activities 24
File Read 24
Analysis Process: conhost.exe PID: 6380 Parent PID: 6416 24
General 24
Analysis Process: schtasks.exe PID: 6792 Parent PID: 6100 24
General 24
File Activities 24
File Read 24
Analysis Process: conhost.exe PID: 4088 Parent PID: 6792 24
General 24
Analysis Process: gcsEBQO3BV.exe PID: 6664 Parent PID: 968 25
General 25
File Activities 25
File Created 25
File Deleted 25
File Written 25
File Read 25
Analysis Process: dhcpmon.exe PID: 2456 Parent PID: 968 25
General 25
File Activities 26
File Created 26
File Deleted 26
File Written 26
File Read 26
Analysis Process: dhcpmon.exe PID: 2212 Parent PID: 3424 26
General 26
Analysis Process: schtasks.exe PID: 6024 Parent PID: 6664 26
General 26
Analysis Process: conhost.exe PID: 6404 Parent PID: 6024 27
General 27
Analysis Process: schtasks.exe PID: 6844 Parent PID: 2456 27
General 27
Analysis Process: conhost.exe PID: 64 Parent PID: 6844 27
General 27
Analysis Process: gcsEBQO3BV.exe PID: 1444 Parent PID: 6664 28
General 28
Analysis Process: dhcpmon.exe PID: 6408 Parent PID: 2456 28
General 28
Analysis Process: schtasks.exe PID: 6528 Parent PID: 2212 29
General 29
Analysis Process: conhost.exe PID: 4588 Parent PID: 6528 29
General 29
Analysis Process: dhcpmon.exe PID: 7120 Parent PID: 2212 29
General 29
Disassembly 30
Code Analysis 30

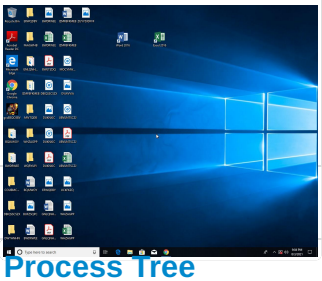
Windows Analysis Report gcsEBQO3BV.exe

Overview

General Information

Sample Name:	gcsEBQO3BV.exe
Analysis ID:	458901
MD5:	008a85f2c1cf538..
SHA1:	b7f9e6b4177b88a.
SHA256:	4ee50840eec3ef8.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

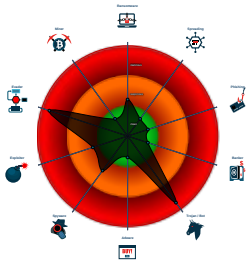
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w10x64**
- gcsEBQO3BV.exe (PID: 6300 cmdline: 'C:\Users\user\Desktop\gcsEBQO3BV.exe' MD5: 008A85F2C1CF538F42F94A7E88CA88C7)
  - schtasks.exe (PID: 4240 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmp1EA2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4972 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - gcsEBQO3BV.exe (PID: 3484 cmdline: {path} MD5: 008A85F2C1CF538F42F94A7E88CA88C7)
  - gcsEBQO3BV.exe (PID: 6100 cmdline: {path} MD5: 008A85F2C1CF538F42F94A7E88CA88C7)
    - schtasks.exe (PID: 6416 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp3A48.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6792 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp3E8F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- gcsEBQO3BV.exe (PID: 6664 cmdline: C:\Users\user\Desktop\gcsEBQO3BV.exe 0 MD5: 008A85F2C1CF538F42F94A7E88CA88C7)
  - schtasks.exe (PID: 6024 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmpE955.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - gcsEBQO3BV.exe (PID: 1444 cmdline: {path} MD5: 008A85F2C1CF538F42F94A7E88CA88C7)
- dhcpmon.exe (PID: 2456 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 008A85F2C1CF538F42F94A7E88CA88C7)
  - schtasks.exe (PID: 6844 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmpEBE5.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 64 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6408 cmdline: {path} MD5: 008A85F2C1CF538F42F94A7E88CA88C7)
- dhcpmon.exe (PID: 2212 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 008A85F2C1CF538F42F94A7E88CA88C7)
  - schtasks.exe (PID: 6528 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eBopYzBwUYOW' /XML 'C:\Users\user\AppData\Local\Temp\tmpFD8.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4588 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 7120 cmdline: {path} MD5: 008A85F2C1CF538F42F94A7E88CA88C7)
- **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
0000001F.00000002.884398030.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001F.00000002.884398030.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001F.00000002.884398030.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
0000000C.00000002.918302480.000000000431000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000C.00000002.923339846.000000000790000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5fee:$x1: NanoCore.ClientPluginHost • 0x602b:$x2: IClientNetworkHost

Click to see the 87 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
31.2.dhcpmon.exe.2fd9684.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
31.2.dhcpmon.exe.2fd9684.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
12.2.gcsEBQO3BV.exe.78a0000.26.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3deb:$x1: NanoCore.ClientPluginHost • 0x3f48:$x2: IClientNetworkHost
12.2.gcsEBQO3BV.exe.78a0000.26.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x3deb:$x2: NanoCore.ClientPluginHost • 0x4d41:$s3: PipeExists • 0x3fe1:$s4: PipeCreated • 0x3e05:$s5: IClientLoggingHost
12.2.gcsEBQO3BV.exe.7880000.24.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x13a8:$x1: NanoCore.ClientPluginHost
Click to see the 186 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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

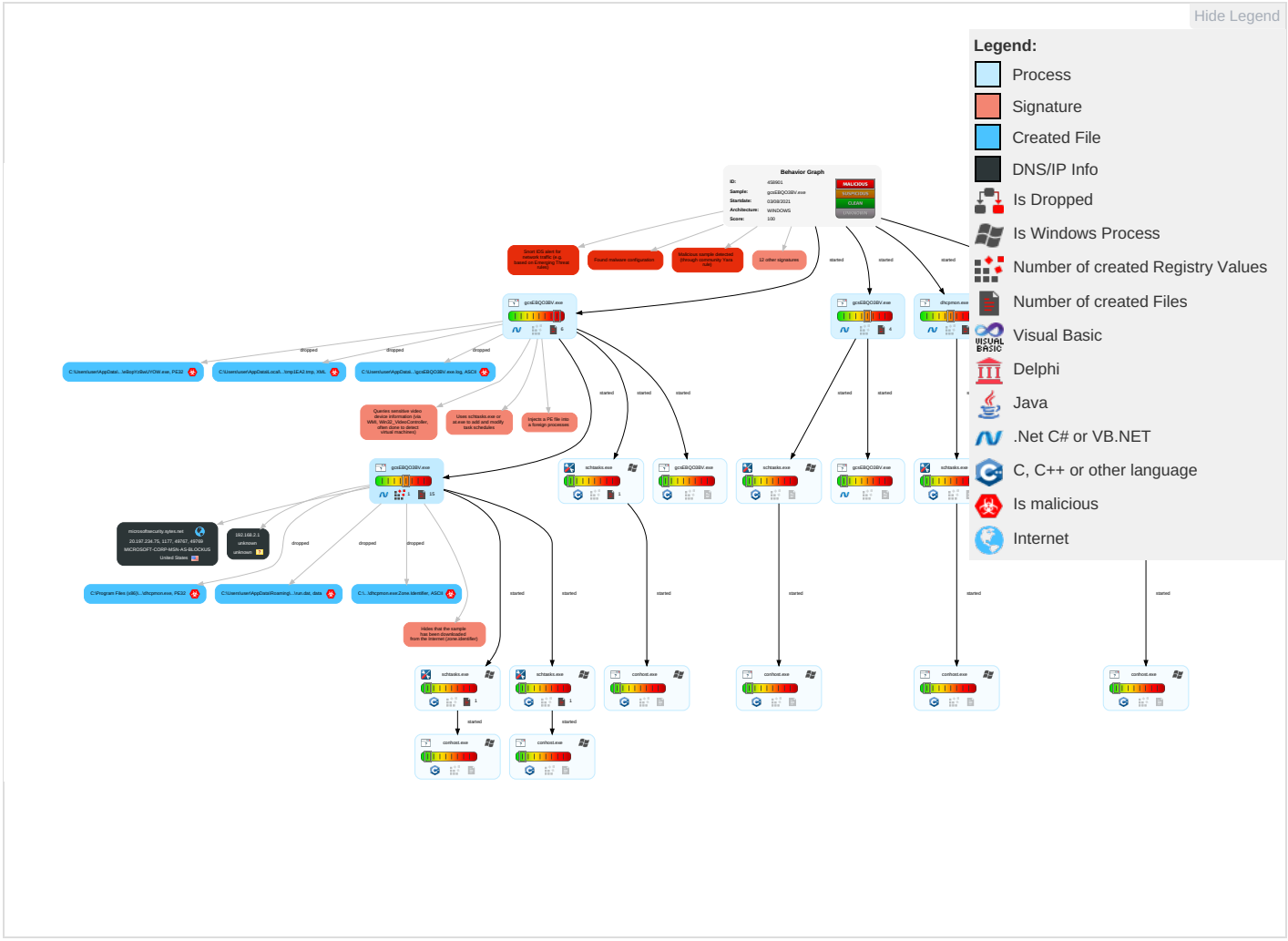
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	System Information Discovery 1 3	Distributed Component Object Model	Input Capture	Scheduled Transfer

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Security Software Discovery 3 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Virtualization/Sandbox Evasion 1 3 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 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
gcsEBQO3BV.exe	51%	Virustotal		Browse
gcsEBQO3BV.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
gcsEBQO3BV.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\eBopYzBwUYOW.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\eBopYzBwUYOW.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.gcsEBQO3BV.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
30.2.gcsEBQO3BV.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
34.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.gcsEBQO3BV.exe.6930000.18.unpack	100%	Avira	TR/NanoCore.fadte		Download File
31.2.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	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.K	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
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	• Avira URL Cloud: safe	unknown
backupnew.duckdns.org	true	• 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:	458901
Start date:	03.08.2021
Start time:	21:01:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gcsEBQO3BV.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:	35
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@32/16@11/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.5% (good quality ratio 0.9%) • Quality average: 40.1% • Quality standard deviation: 36.9%
HCA Information:	• Successful, ratio: 98% • 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
21:02:59	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\gcsEBQO3BV.exe" s>$(Arg0)
21:02:59	API Interceptor	606x Sleep call for process: gcsEBQO3BV.exe modified
21:02:59	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
21:03:00	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(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\gcsEBQO3BV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	703488
Entropy (8bit):	7.478742406317566
Encrypted:	false
SSDEEP:	12288:n+J70shAUfvBweg+wToULrNMmnjx05WqV+60RiVycWTQLbOQDFi14Bp/j+PIH3mq:n+J70cLvBwP+8oUSmntIV+60wST8OQp9
MD5:	008A85F2C1CF538F42F94A7E88CA88C7
SHA1:	B7F9E6B4177B88AE459D5AEE069F06F1B7AD5485
SHA-256:	4EE50840EEC3EF82A73866BD6F2E00B42789A76F348BEF3C01F98124EDCEF8B8
SHA-512:	444BB1A3A5083DA55963429649E079742E212690D1AC18AEEDAB4F2ECBB5F1A68641F19A9533E7F428130D225F35BEF70A59D44D9B05744963A5C5CE147C6860
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].`.....x...B.....^.... .....@.. ..... ..@.....O.....P?..... ..... ..H.....text...dw... ...x..... ..`.rsrc...P?.....@...z.....@..@.rel oc.....@..B.....@.....H.....0...._.....0.....*....0.....s....(.....*.0.....(.....*.0.....}.....}.....(.....}.....(...s'... }.....}.....}.....u...,9..o.....(....r...p(....-...o.....(....r...p(....+..+...,...t....s0.....}....*.0..I.....(.... N... !l..a%..^E.....+.... ...Z ..a+....}....*....0..E..... q[0. ..L.a%..^E... .....#...+!....$...s#...}..... .(.+Z]r..a+.*....0..

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\gcsEBQO3BV.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\gcsEBQO3BV.exe.log	
Process:	C:\Users\user\Desktop\gcsEBQO3BV.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\tmp1EA2.tmp	
Process:	C:\Users\user\Desktop\gcsEBQO3BV.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.189102630149273
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGsFtn:cbhK79lNQR/rydbz9I3YODOLNdq39v
MD5:	74CF069D4425306450AF9C459BBCE9F7
SHA1:	6A1FA39E22803D57BAA3695F3F4581C2DFF68556
SHA-256:	9C0B7CE4B179D72EA019469E600307BF2B5A048804941BFEFD12FEBCFCA1709B
SHA-512:	230E79DA950F63BEAFF52D674070954466E9B677D1987372A53B2C953BF80B9F30BBE24D3A981656C8081F76816A153726B1FAE9823C2EAB7327D25813F206B7
Malicious:	**true**
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\tmp1EA2.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\tmp3A48.tmp	
Process:	C:\Users\user\Desktop\gcsEBQO3BV.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	5.115086565855345
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Yixtn:cbk4oL600QydbQxIYODOLedq3uj
MD5:	ECD2C93B3D28A0B0E2F428E0264D7B6B
SHA1:	09DEA2B0683368E8F8BCEA7B5C6EBE439AEE0133
SHA-256:	6DA36228CAC1E211B86A10B0C6A9031C1D5FEABF3E7D796776376BCBC11088B8
SHA-512:	E1EF65805F0F0BEEE893C5DEE5A087CF84612A61C2451BFC1125F7F0E455F4B14F0303FBD467FCFE3A67AD883E3FAA1548DB760D674F3F2F64E7CEE6D419AD/1
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\tmp3E8F.tmp	
Process:	C:\Users\user\Desktop\gcsEBQO3BV.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\tmpE955.tmp	
Process:	C:\Users\user\Desktop\gcsEBQO3BV.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.189102630149273
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGsFtn:cbhK79lNQR/rydbz9I3YODOLNdq39v
MD5:	74CF069D4425306450AF9C459BBCE9F7
SHA1:	6A1FA39E22803D57BAA3695F3F4581C2DFF68556
SHA-256:	9C0B7CE4B179D72EA019469E600307BF2B5A048804941BFEFD12FEBCFCA1709B
SHA-512:	230E79DA950F63BEAFF52D674070954466E9B677D1987372A53B2C953BF80B9F30BBE24D3A981656C8081F76816A153726B1FAE9823C2EAB7327D25813F206B7
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\tmpE955.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\tmpEBE5.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):	5.189102630149273
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGsFtn:cbhK79lNQR/rydbz9l3YODOLNdq39v
MD5:	74CF069D4425306450AF9C459BBCE9F7
SHA1:	6A1FA39E22803D57BAA3695F3F4581C2DFF68556
SHA-256:	9C0B7CE4B179D72EA019469E600307BF2B5A048804941BFEFD12FEBCFCA1709B
SHA-512:	230E79DA950F63BEAFF52D674070954466E9B677D1987372A53B2C953BF80B9F30BBE24D3A981656C8081F76816A153726B1FAE9823C2EAB7327D25813F206B7
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\tmpFD8.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):	5.189102630149273
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGsFtn:cbhK79lNQR/rydbz9l3YODOLNdq39v
MD5:	74CF069D4425306450AF9C459BBCE9F7
SHA1:	6A1FA39E22803D57BAA3695F3F4581C2DFF68556
SHA-256:	9C0B7CE4B179D72EA019469E600307BF2B5A048804941BFEFD12FEBCFCA1709B
SHA-512:	230E79DA950F63BEAFF52D674070954466E9B677D1987372A53B2C953BF80B9F30BBE24D3A981656C8081F76816A153726B1FAE9823C2EAB7327D25813F206B7
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\gcsEBQO3BV.exe
File Type:	data
Category:	dropped
Size (bytes):	1160
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	24:IQnybgC4jh+dQnybgC4jh+dQnybgC4jh+dQnybgC4jh+dQnybgC4jh+K:IknjhUknjhUknjhUknjhUknjhL
MD5:	7BEBBE1F1511163A3243CD8E0C75CC69
SHA1:	216B3AB5D802FA037A6EC5348B189398D8980B3C
SHA-256:	79A130865E9EFFFAA6C2E453942CE87F652681BCD76AAF987318300CAF5E3778
SHA-512:	4DCCB32411DEF72C938022B8675DA50B2DC4CD2C051B1C0377F63D6AAC42FC3D128B0ED580FB88954AB04A9E9EC8D272EBCCF74EB3F136BEF41ADBB845A1A530
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......[.&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\gcsEBQO3BV.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:fot:o
MD5:	5D50F3D2AC1305B0B1D14FF65E96BFC7
SHA1:	0815E076D2FF28BE4A8EDE8ED7242ADCD14472C8
SHA-256:	6968FFB9754308FBCA0DEE1158F38AAE070055DE1E93FB716E8B1AF1048EF2DE
SHA-512:	E376A82EE3278D9D1FD05CEEF1B6938BCE2A156F7F77E07DFDE9BF5238342EDEC7A99C185147DC35C29AA41FBE5722EEF7A72A2EC1A548AF7175A87C5594CF 49
Malicious:	**true**
Reputation:	unknown
Preview:	...M.V.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin

Process:	C:\Users\user\Desktop\gcsEBQO3BV.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f.~a........~.~.......3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat

Process:	C:\Users\user\Desktop\gcsEBQO3BV.exe
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wl8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3 A
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\gcsEBQO3BV.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):	4.257580907551286
Encrypted:	false
SSDEEP:	3:oNt+WfWCGnnT20C:oNwvCWSJ
MD5:	DC939810D8F43EB38ADAEFB85AD0CEDA
SHA1:	2BB19FE8337D3C2CAF8EE02D1BDEC8D38B918E7B
SHA-256:	C2D5CEEEE6CC36CB0E1B8D95AFC3BCDF5D6147ECF29A5D463C5BC713DD3FAF3F
SHA-512:	4D254397E0259D87C7DA4715BF0224FD0E9282BE96A5F84A00ACFBA384AEA5D990F47D122E4A4AD75AA28313634AFFF27661D43D97154C42F70980801408B8F5
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\gcsEBQO3BV.exe

C:\Users\user\AppData\Roaming\eBopYzBwUYOW.exe	
Process:	C:\Users\user\Desktop\gcsEBQO3BV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	703488
Entropy (8bit):	7.478742406317566
Encrypted:	false
SSDEEP:	12288:n+J70shAUfvBweg+wToULrNMmnjx05WqV+60RiVycWTQLbOQDFi14Bp/j+PIH3mq:n+J70cLvBwP+8oUSmntIV+60wST8OQp9
MD5:	008A85F2C1CF538F42F94A7E88CA88C7
SHA1:	B7F9E6B4177B88AE459D5AEE069F06F1B7AD5485
SHA-256:	4EE50840EEC3EF82A73866BD6F2E00B42789A76F348BEF3C01F98124EDCEF8B8
SHA-512:	444BB1A3A5083DA55963429649E079742E212690D1AC18AEEDAB4F2ECBB5F1A68641F19A9533E7F428130D225F35BEF70A59D44D9B05744963A5C5CE147C6860
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].`.....x...B.....^.... .....@.. ..... ..@.....O.....P?..... ..... ..H.....text...dw... ...x..... ..`.rsrc...P?.....@...z.....@..@.rel oc.....@..B.....@.....H.....0...._.....0.....*...0.....s....(.....*.0.....(.....*.0.....}.....}.....(.....}.....(...s'... }.....}.....}.....u....,9..o.....(....r...p(....-...o.....(....r...p(....+..+....,..t....s0.....}....*.0..I.....(.... N... !l..a%..^E.....+.... ...Z ..a+....}....*....0..E..... q[0. ..L.a%..^E... .....#...+!....$...s#...}..... .(.+Z]r..a+.*....0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.478742406317566
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:	gcsEBQO3BV.exe
File size:	703488
MD5:	008a85f2c1cf538f42f94a7e88ca88c7
SHA1:	b7f9e6b4177b88ae459d5aee069f06f1b7ad5485
SHA256:	4ee50840eec3ef82a73866bd6f2e00b42789a76f348bef3c01f98124edcef8b8
SHA512:	444bb1a3a5083da55963429649e079742e212690d1ac18aeedab4f2ecbb5f1a68641f19a9533e7f428130d225f35bef70a59d44d9b05744963a5c5ce147c6860
SSDEEP:	12288:n+J70shAUfvBweg+wToULrNMmnjx05WqV+60RiVycWTQLbOQDFi14Bp/j+PIH3mq:n+J70cLvBwP+8oUSmntIV+60wST8OQp9
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].`.....x...B.....^.... .....@.. ....@.....

File Icon

Icon Hash:	8099b8acdce4e1e5

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	0x3f50	0x4000	False	0.627807617188	data	5.5633177152	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	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
08/03/21-21:03:03.070861	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49767	1177	192.168.2.4	20.197.234.75
08/03/21-21:03:10.961626	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	1177	192.168.2.4	20.197.234.75
08/03/21-21:03:18.292169	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	1177	192.168.2.4	20.197.234.75
08/03/21-21:03:25.266257	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	1177	192.168.2.4	20.197.234.75
08/03/21-21:03:32.318494	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49772	1177	192.168.2.4	20.197.234.75

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-21:03:39.569786	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	1177	192.168.2.4	20.197.234.75
08/03/21-21:03:44.455750	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	1177	192.168.2.4	20.197.234.75
08/03/21-21:03:49.468825	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	1177	192.168.2.4	20.197.234.75
08/03/21-21:03:56.009783	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	1177	192.168.2.4	20.197.234.75
08/03/21-21:04:03.242027	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	1177	192.168.2.4	20.197.234.75
08/03/21-21:04:09.616586	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	1177	192.168.2.4	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 21:03:02.669002056 CEST	192.168.2.4	8.8.8.8	0x96ad	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:10.531178951 CEST	192.168.2.4	8.8.8.8	0x8d7b	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:17.960906029 CEST	192.168.2.4	8.8.8.8	0x9de4	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:25.024315119 CEST	192.168.2.4	8.8.8.8	0xc473	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:32.071710110 CEST	192.168.2.4	8.8.8.8	0xd17e	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:39.324357033 CEST	192.168.2.4	8.8.8.8	0xc6e4	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:44.149097919 CEST	192.168.2.4	8.8.8.8	0x25a2	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:49.132050037 CEST	192.168.2.4	8.8.8.8	0x4f92	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:55.735852957 CEST	192.168.2.4	8.8.8.8	0x1981	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:02.992939949 CEST	192.168.2.4	8.8.8.8	0xef0	Standard query (0)	microsofts ecurity.sytes.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:09.355088949 CEST	192.168.2.4	8.8.8.8	0x766e	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 21:03:02.703749895 CEST	8.8.8.8	192.168.2.4	0x96ad	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:10.568053961 CEST	8.8.8.8	192.168.2.4	0x8d7b	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:17.996409893 CEST	8.8.8.8	192.168.2.4	0x9de4	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:25.057940006 CEST	8.8.8.8	192.168.2.4	0xc473	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:32.109904051 CEST	8.8.8.8	192.168.2.4	0xd17e	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:39.359462023 CEST	8.8.8.8	192.168.2.4	0xc6e4	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:44.181466103 CEST	8.8.8.8	192.168.2.4	0x25a2	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 21:03:49.165702105 CEST	8.8.8.8	192.168.2.4	0x4f92	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 21:03:55.768687010 CEST	8.8.8.8	192.168.2.4	0x1981	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:03.026909113 CEST	8.8.8.8	192.168.2.4	0xef0	No error (0)	microsofts ecurity.sytes.net		20.197.234.75	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:09.391959906 CEST	8.8.8.8	192.168.2.4	0x766e	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: gcsEBQO3BV.exe PID: 6300 Parent PID: 6084

General

Start time:	21:02:04
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\gcsEBQO3BV.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\gcsEBQO3BV.exe'
Imagebase:	0x960000
File size:	703488 bytes
MD5 hash:	008A85F2C1CF538F42F94A7E88CA88C7
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: 00000001.00000002.755783143.0000000002D11000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.758869447.0000000003D19000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.758869447.0000000003D19000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.758869447.0000000003D19000.00000004.00000001.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: 4240 Parent PID: 6300

General

Start time:	21:02:50
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\tmp1EA2.tmp'
Imagebase:	0x160000
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: 4972 Parent PID: 4240

General

Start time:	21:02:51
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: gcsEBQO3BV.exe PID: 3484 Parent PID: 6300

General

Start time:	21:02:51
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\gcsEBQO3BV.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x3c0000
File size:	703488 bytes
MD5 hash:	008A85F2C1CF538F42F94A7E88CA88C7
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: gcsEBQO3BV.exe PID: 6100 Parent PID: 6300

General

Start time:	21:02:52
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\gcsEBQO3BV.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xfa0000
File size:	703488 bytes
MD5 hash:	008A85F2C1CF538F42F94A7E88CA88C7
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: 0000000C.00000002.918302480.0000000004391000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.923339846.0000000007930000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.923339846.0000000007930000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.921215035.0000000005CE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.921215035.0000000005CE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.923227921.00000000078F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.923227921.00000000078F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.923077412.00000000078A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.923077412.00000000078A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.921626812.0000000006930000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.921626812.0000000006930000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.921626812.0000000006930000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.923194691.00000000078E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.923194691.00000000078E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.923044394.0000000007890000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.923044394.0000000007890000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.921911415.0000000006E30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.921911415.0000000006E30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.923105492.00000000078B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.923105492.00000000078B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.913770641.0000000000402000.00000040.00000001.sdmp, Author:

	Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.913770641.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.913770641.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.923133784.00000000078C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.923133784.00000000078C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.922985944.0000000007870000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.922985944.0000000007870000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.916355133.0000000003341000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.916355133.0000000003341000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.922828441.00000000076F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.922828441.00000000076F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.922966847.0000000007860000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.922966847.0000000007860000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.918972409.000000000462F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.923013512.0000000007880000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.923013512.0000000007880000.00000004.00000001.sdmp, Author: Florian Roth
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: 6416 Parent PID: 6100

General

Start time:	21:02:57
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\tmp3A48.tmp'
Imagebase:	0x160000

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: 6380 Parent PID: 6416

General

Start time:	21:02:57
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6792 Parent PID: 6100

General

Start time:	21:02:58
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\tmp3E8F.tmp'
Imagebase:	0x160000
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: 4088 Parent PID: 6792

General

Start time:	21:02:58
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: gcsEBQO3BV.exe PID: 6664 Parent PID: 968

General

Start time:	21:03:00
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\gcsEBQO3BV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\gcsEBQO3BV.exe 0
Imagebase:	0x9f0000
File size:	703488 bytes
MD5 hash:	008A85F2C1CF538F42F94A7E88CA88C7
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: 00000011.00000002.869500198.0000000003071000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.875420533.0000000004079000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.875420533.0000000004079000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.875420533.0000000004079000.00000004.00000001.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: 2456 Parent PID: 968

General

Start time:	21:03:01
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:	0x9e0000
File size:	703488 bytes
MD5 hash:	008A85F2C1CF538F42F94A7E88CA88C7
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: 00000012.00000002.875421468.0000000003D79000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.875421468.0000000003D79000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.875421468.0000000003D79000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000012.00000002.869398192.0000000002D71000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 63%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: dhcpmon.exe PID: 2212 Parent PID: 3424

General

Start time:	21:03:08
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:	0x8a0000
File size:	703488 bytes
MD5 hash:	008A85F2C1CF538F42F94A7E88CA88C7
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: 00000014.00000002.898848134.0000000003CA9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.898848134.0000000003CA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.898848134.0000000003CA9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.887889351.0000000002CA1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: schtasks.exe PID: 6024 Parent PID: 6664

General

Start time:	21:03:42
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\tmpE955.tmp'
Imagebase:	0x160000
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: 6404 Parent PID: 6024

General

Start time:	21:03:43
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6844 Parent PID: 2456

General

Start time:	21:03:43
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\tmpEBE5.tmp'
Imagebase:	0x160000
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: 64 Parent PID: 6844

General

Start time:	21:03:43
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: gcsEBQO3BV.exe PID: 1444 Parent PID: 6664

General

Start time:	21:03:43
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\gcsEBQO3BV.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb10000
File size:	703488 bytes
MD5 hash:	008A85F2C1CF538F42F94A7E88CA88C7
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.00000002.888954904.0000000003F89000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.888954904.0000000003F89000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.888483621.0000000002F81000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.888483621.0000000002F81000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001E.00000002.882125201.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.882125201.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.882125201.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: dhcpmon.exe PID: 6408 Parent PID: 2456

General

Start time:	21:03:44
Start date:	03/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc00000
File size:	703488 bytes
MD5 hash:	008A85F2C1CF538F42F94A7E88CA88C7
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: 0000001F.00000002.884398030.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001F.00000002.884398030.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001F.00000002.884398030.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001F.00000002.890669255.0000000002F71000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001F.00000002.890669255.0000000002F71000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001F.00000002.891289633.0000000003F79000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001F.00000002.891289633.0000000003F79000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: schtasks.exe PID: 6528 Parent PID: 2212

General

Start time:	21:03:52
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\tmpFD8.tmp'
Imagebase:	0x160000
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: 4588 Parent PID: 6528

General

Start time:	21:03:53
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 7120 Parent PID: 2212

General

Start time:	21:03:54
Start date:	03/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}

Imagebase:	0xa90000
File size:	703488 bytes
MD5 hash:	008A85F2C1CF538F42F94A7E88CA88C7
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: 00000022.00000002.908292630.0000000003F99000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000022.00000002.908292630.0000000003F99000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000022.00000002.908102746.0000000002F91000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000022.00000002.908102746.0000000002F91000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.905512607.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000022.00000002.905512607.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000022.00000002.905512607.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis