ID: 509563
Sample Name: GHhMZFFEmf
Cookbook: default.jbs
Time: 17:10:46
Date: 26/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

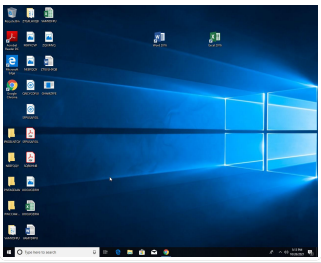
Windows Analysis Report GHhMZFFEmf

Overview

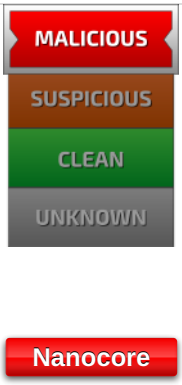
General Information

Sample Name:	GHhMZFFEmf (renamed file extension from none to exe)
Analysis ID:	509563
MD5:	ace96cf7ef24eea..
SHA1:	fa89615f55a87ef…
SHA256:	d4ee80500d9c28..
Tags:	32 exe NanoCore trojan
Infos:	

Most interesting Screenshot:



Detection



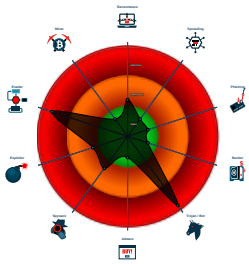
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Sigma detected: Bad Opsec Default…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Allocates memory in foreign process…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- GHhMZFFEmf.exe (PID: 6388 cmdline: 'C:\Users\user\Desktop\GHhMZFFEmf.exe' MD5: ACE96CF7EF24EEAC993B4DA172A5A8F0)
  - schtasks.exe (PID: 6656 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eWoGxZG' /XML 'C:\Users\user\AppData\Local\Temp\tmpBBC.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6680 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - RegSvcs.exe (PID: 6716 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
    - schtasks.exe (PID: 6764 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpA2A2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6836 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpA9E6.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 6852 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 7024 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 7080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 4408 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 5676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

Copyright Joe Security LLC 2021

```
{
  "Version": "1.2.2.0",
  "Mutex": "70bb352e-dceb-4105-9fdd-010e83e2",
  "Group": "NEW LIFE",
  "Domain1": "drrkingsleym001.ddns.net",
  "Domain2": "drrkingsleym001.ddns.net",
  "Port": 1665,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "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
00000007.00000002.629752938.000000000597 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost
00000007.00000002.629752938.000000000597 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x8ba5:$x2: NanoCore.ClientPluginHost • 0x9b74:$s2: FileCommand • 0xe576:$s4: PipeCreated • 0x8bbf:$s5: IClientLoggingHost
00000000.00000002.374588602.000000000462 7000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10155:$x1: NanoCore.ClientPluginHost • 0x10192:$x2: IClientNetworkHost • 0x13cc5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.374588602.000000000462 7000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.374588602.000000000462 7000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfebd:$a: NanoCore • 0xfecd:$a: NanoCore • 0x10101:$a: NanoCore • 0x10115:$a: NanoCore • 0x10155:$a: NanoCore • 0xff1c:$b: ClientPlugin • 0x1011e:$b: ClientPlugin • 0x1015e:$b: ClientPlugin • 0x10043:$c: ProjectData • 0x10a4a:$d: DESCrypto • 0x18416:$e: KeepAlive • 0x16404:$g: LogClientMessage • 0x125ff:$i: get_Connected • 0x10d80:$j: #=q • 0x10db0:$j: #=q • 0x10dcc:$j: #=q • 0x10dfc:$j: #=q • 0x10e18:$j: #=q • 0x10e34:$j: #=q • 0x10e64:$j: #=q • 0x10e80:$j: #=q

Click to see the 42 entries

Copyright Joe Security LLC 2021

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.RegSvcs.exe.5a10000.16.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3d99:$x1: NanoCore.ClientPluginHost • 0x3db3:$x2: IClientNetworkHost
7.2.RegSvcs.exe.5a10000.16.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x3d99:$x2: NanoCore.ClientPluginHost • 0x4dce:$s4: PipeCreated • 0x3d86:$s5: IClientLoggingHost
7.2.RegSvcs.exe.5a30000.17.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
7.2.RegSvcs.exe.5a30000.17.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x350b:$x2: NanoCore.ClientPluginHost • 0x52b6:$s4: PipeCreated • 0x34f8:$s5: IClientLoggingHost
7.2.RegSvcs.exe.5810000.9.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 92 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

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 submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

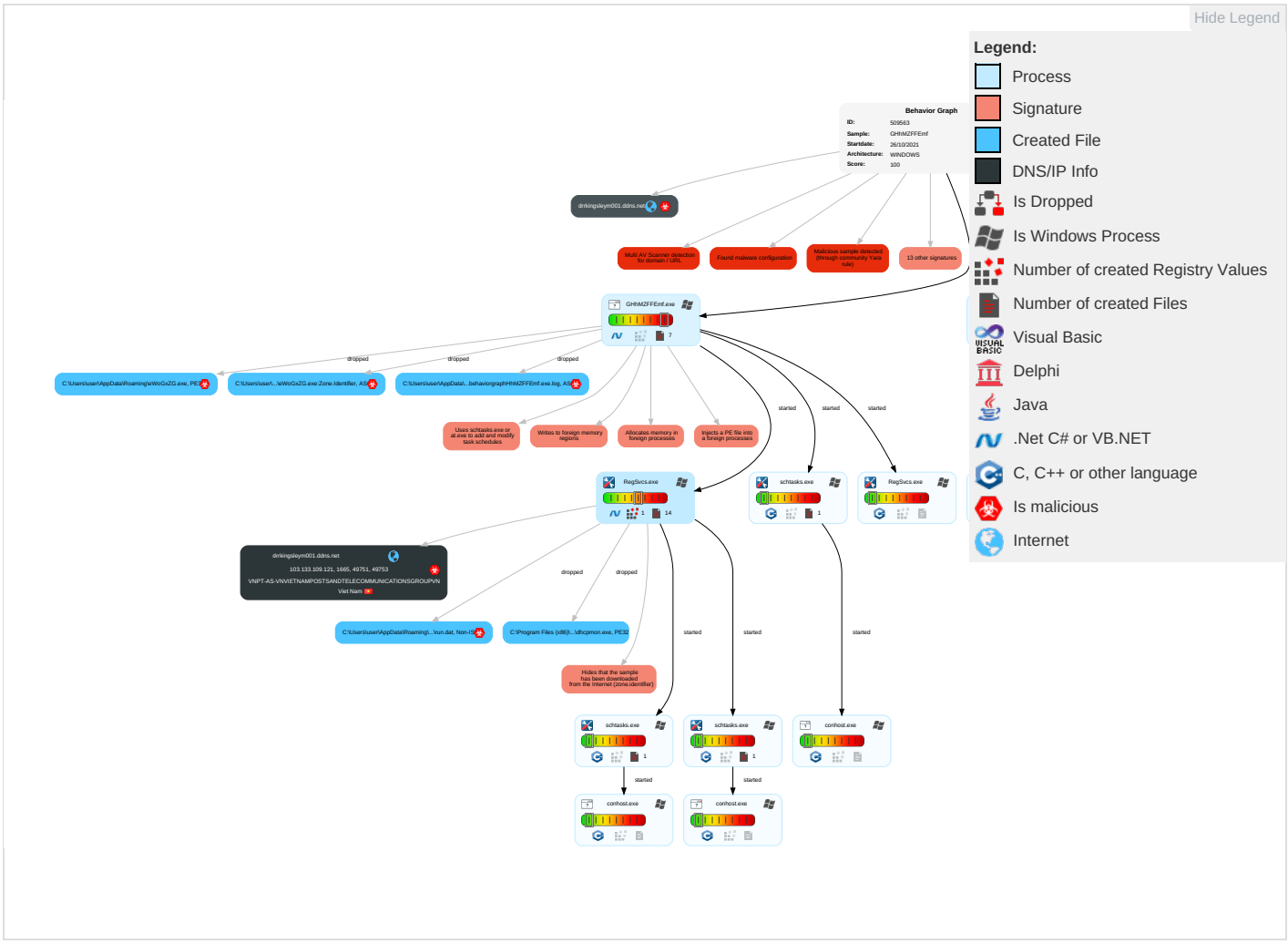
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Valid Accounts	Command and Scripting Interpreter 2	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 1 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transfer
Default Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypte Channel

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 3 1 2	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Star Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 2 1	SSH	Keylogging	Data Transfer Size Limits	Non-Applicati Layer Protocol
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applicati Layer Protocol
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 1	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commor Used Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicati Layer Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tran Protocols

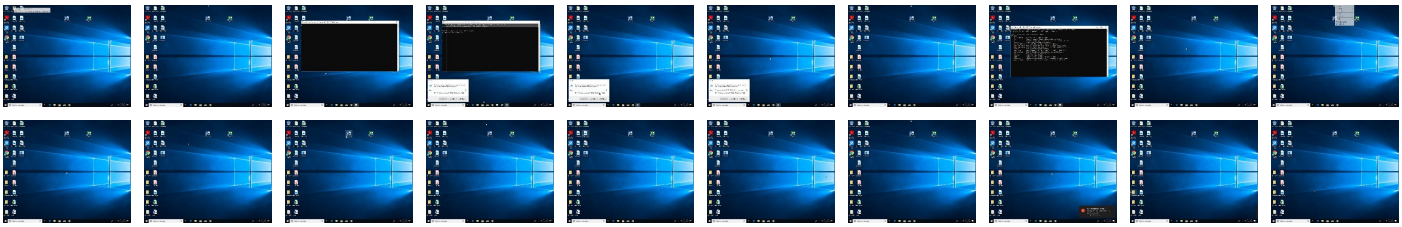
Behavior Graph



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
GHhMZFFEmf.exe	35%	Virustotal		Browse
GHhMZFFEmf.exe	43%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
GHhMZFFEmf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\eWoGxZG.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\eWoGxZG.exe	43%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.RegSvcs.exe.5ab0000.23.unpack	100%	Avira	TR/NanoCore.fadte		Download File
7.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
drrkingsleym001.ddns.net	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn.	0%	Virustotal		Browse
http://www.zhongyicts.com.cn.	0%	Avira URL Cloud	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.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html5	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl	0%	URL Reputation	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	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.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/f	0%	Avira URL Cloud	safe	
http://www.fontbureau.come.comc	0%	Avira URL Cloud	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.typography.netL	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.typography.netved.	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.carterandcone.comRea	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.typography.netze	0%	Avira URL Cloud	safe	
http://www.typography.netes	0%	Avira URL Cloud	safe	
drrkingsleym001.ddns.net	0%	Avira URL Cloud	safe	
http://www.carterandcone.comwdth	0%	URL Reputation	safe	
http://www.founder.com.cn/cn(	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drrkingsleym001.ddns.net	103.133.109.121	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
drrkingsleym001.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.133.109.121	drrkingsleym001.ddns.net	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	509563
Start date:	26.10.2021
Start time:	17:10:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	GHhMZFFEmf (renamed file extension from none to 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@20/14@17/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.7% (good quality ratio 2.2%) • Quality average: 38.2% • Quality standard deviation: 36.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Copyright Joe Security LLC 2021

Simulations

Behavior and APIs

Time	Type	Description
17:11:54	API Interceptor	1x Sleep call for process: GHhMZFFEmf.exe modified
17:12:01	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe" s>$(Arg0)
17:12:02	API Interceptor	868x Sleep call for process: RegSvcs.exe modified
17:12:04	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
17:12:04	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.133.109.121	Purchase order_122.doc	Get hash	malicious	Browse	
	b2ZeLApyX2.exe	Get hash	malicious	Browse	
	Purchase order_122.doc	Get hash	malicious	Browse	
	YKr3m9a7C3.exe	Get hash	malicious	Browse	
	SWIFT COPY.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
drrkingsleym001.ddns.net	Purchase order_122.doc	Get hash	malicious	Browse	• 103.133.109.121
	b2ZeLApyX2.exe	Get hash	malicious	Browse	• 103.133.109.121
	Purchase order_122.doc	Get hash	malicious	Browse	• 103.133.109.121
	YKr3m9a7C3.exe	Get hash	malicious	Browse	• 103.133.109.121
	SWIFT COPY.doc	Get hash	malicious	Browse	• 103.133.109.121

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	Purchase order_122.doc	Get hash	malicious	Browse	• 103.133.109.121
	IMS211323.xlsx	Get hash	malicious	Browse	• 103.149.12.116
	purchase order # 4459.xls	Get hash	malicious	Browse	• 103.141.138.110
	6811A4CEA56365431B3799600303C945593A997E61968.exe	Get hash	malicious	Browse	• 103.114.104.13
	KfvEoN0wlw	Get hash	malicious	Browse	• 103.68.250.127
	INQ_42-4I090.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	PO doc 42782.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	b2ZeLApyX2.exe	Get hash	malicious	Browse	• 103.133.109.121
	Purchase order_122.doc	Get hash	malicious	Browse	• 103.133.109.121
	DMS210949 MV LYDERHORN LOW MIX RATIO.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	payment issue need help.exe	Get hash	malicious	Browse	• 103.133.110.241
	DMS210949 MV LYDERHORN LOW MIX RATIO.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	PO1-424480.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	arm7	Get hash	malicious	Browse	• 14.225.246.61
	PI Alu Circle_Dt. 14.05.2021.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	YKr3m9a7C3.exe	Get hash	malicious	Browse	• 103.133.109.121

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SWIFT COPY.doc	Get hash	malicious	Browse	• 103.133.109.121
	Airway bill# 7899865792021.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	presupuesto.xlsx	Get hash	malicious	Browse	• 103.140.251.116
	Purchase orders with bank details.ppa	Get hash	malicious	Browse	• 103.141.138.110

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	DRAFT BL-DOCS-20211510-VP-KMC022021.exe	Get hash	malicious	Browse	
	b2ZeLApyX2.exe	Get hash	malicious	Browse	
	YKr3m9a7C3.exe	Get hash	malicious	Browse	
	tEdxwnE4lw.exe	Get hash	malicious	Browse	
	87R65JT93I.exe	Get hash	malicious	Browse	
	invo.exe	Get hash	malicious	Browse	
	U5s97oQj9A.exe	Get hash	malicious	Browse	
	hAmgDpjdg5.exe	Get hash	malicious	Browse	
	PO00174Quotations.exe	Get hash	malicious	Browse	
	mNgTZMYBA8.exe	Get hash	malicious	Browse	
	xvE67cxGKh.exe	Get hash	malicious	Browse	
	C9UKyFaVBg.exe	Get hash	malicious	Browse	
	IzopQnj0od.exe	Get hash	malicious	Browse	
	khmU580OCp.exe	Get hash	malicious	Browse	
	eKLFu9iX5X.exe	Get hash	malicious	Browse	
	HXMhjytc4v.exe	Get hash	malicious	Browse	
	ID3xMSKdE5.exe	Get hash	malicious	Browse	
	bzPdZR1ZMh.exe	Get hash	malicious	Browse	
	IyAJkrCCbT.exe	Get hash	malicious	Browse	
	V672IT45op.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7515815714465193
Encrypted:	false
SSDEEP:	384:BOj9Y8/gS7SDriLGKq1MHR5U4Ag6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgWSW72uw:B+gSAdN1MH3HAFRJngW2u
MD5:	71369277D09DA0830C8C59F9E22BB23A
SHA1:	37F9781314F0F6B7E9CB529A573F2B1C8DE9E93F
SHA-256:	D4527B7AD2FC4778CC5BE8709C95AEA44EAC0568B367EE14F7357D72898C3698
SHA-512:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Joe Sandbox View:	• Filename: DRAFT BL-DOCS-20211510-VP-KMC022021.exe, Detection: malicious, Browse • Filename: b2ZeLApyX2.exe, Detection: malicious, Browse • Filename: YKr3m9a7C3.exe, Detection: malicious, Browse • Filename: tEdxwnE4lw.exe, Detection: malicious, Browse • Filename: 87R65JT93I.exe, Detection: malicious, Browse • Filename: invo.exe, Detection: malicious, Browse • Filename: U5s97oQj9A.exe, Detection: malicious, Browse • Filename: hAmgDpjdg5.exe, Detection: malicious, Browse • Filename: PO00174Quotations.exe, Detection: malicious, Browse • Filename: mNgTZMYBA8.exe, Detection: malicious, Browse • Filename: xvE67cxGKh.exe, Detection: malicious, Browse • Filename: C9UKyFaVBg.exe, Detection: malicious, Browse • Filename: IzopQnj0od.exe, Detection: malicious, Browse • Filename: khmU580OCp.exe, Detection: malicious, Browse • Filename: eKLFu9iX5X.exe, Detection: malicious, Browse • Filename: HXMhjytc4v.exe, Detection: malicious, Browse • Filename: ID3xMSKdE5.exe, Detection: malicious, Browse • Filename: bzPdZR1ZMh.exe, Detection: malicious, Browse • Filename: lyAJkrCCbT.exe, Detection: malicious, Browse • Filename: V672IT45op.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....P... .....k... .....@.. .....[.. ..@.....k..K..... k..... .....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\GHhMZFFEmf.exe.log	
Process:	C:\Users\user\Desktop\GHhMZFFEmf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmpA2A2.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135021273392143
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mn4xtn:cbk4oL600QydbQxIYODOLedq3Z4j
MD5:	40B11EF601FB28F9B2E69D36857BF2EC
SHA1:	B6454020AD2CEED193F4792B77001D0BD741B370
SHA-256:	C51E12D18CC664425F6711D8AE2507068884C7057092CFA11884100E1E9D49E1
SHA-512:	E3C5BCC714CBFCA4B8058DDCDDF231DCEFA69C15881CE3F8123E59ED45CFB5DA052B56E1945DCF8DC7F800D62F9A4EECB82BCA69A66A1530787AEFFEB15E 2BD5
Malicious:	false
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\tmpA9E6.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.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
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF385 1
Malicious:	false
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.....[.&

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Jn:Jn
MD5:	E337E0BC57E076912DC359F37771751A
SHA1:	1534E393ADFDB71F571BAA9AC4A25D626A872F64
SHA-256:	CF204C685AADF83087B8C4B93697C2FBAD6CA74813BE93660BA509135296E94C
SHA-512:	C659DC7F17348FA502EA8B04D9C26B2675354733280C294FA5B6221FBF40F3EB37E7334D968F4DCEE17AEF83A07B4D098B4628F36B8BD73DE9F37EB64FA32DB
Malicious:	**true**
Preview:	^.xd..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.795707286467131
Encrypted:	false
SSDEEP:	3:oMty8WbSX/MNn:oMLWus
MD5:	D685103573539B7E9FDBF5F1D7DD96CE
SHA1:	4B2FE6B5C0B37954B314FCAEE1F12237A9B02D07
SHA-256:	D78BC23B0CA3EDDF52D56AB85CDC30A71B3756569CB32AA2F6C28DBC23C76E8E
SHA-512:	17769A5944E8929323A34269ABEEF0861D5C6799B0A27F5545FBFADC80E5AB684A471AD6F6A7FC623002385154EA89DE94013051E09120AB94362E542AB0F1DD
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe

C:\Users\user\AppData\Roaming\eWoGxZG.exe	
Process:	C:\Users\user\Desktop\GHhMZFFEmf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	368128
Entropy (8bit):	7.943323696866316
Encrypted:	false
SSDEEP:	6144:biuHodpZO0/zxllEpjNGLTk+eRSMjf9oHpqUFNsWPAyJt4SKbxF+wkonJx:upZOu7EpjAnkR/9a9rsWPAmyScxFRb
MD5:	ACE96CF7EF24EEAC993B4DA172A5A8F0
SHA1:	FA89615F55A87EF1D9EE9330EC5B0C040F54E8C1
SHA-256:	D4EE80500D9C280E85B290B467592A5910E9D4EE127CFDA17AD40467B2C88942
SHA-512:	E1D5279223D7E82003BAD73E94B1607B043C0B987987E99DC39AB9790558C4C840CD6949A37F87134FBD13B64C4A2492FB572EEBDE870DB709D2A77C419C7EA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 43%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X.wa.....0..... .....@.. ....@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....?...A.....}.....1.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*....0..8.....s....%.Bo.....%.Po .....%.Do.....%.Io.....%.Wo.....+..*.0..8.....s....%.oo.....%.+o.....%.-o.....%.*o.....%.=o.....+..*".(.....*....0.. .....%.r...p.%.r7..p.%....+..*&.(.....*...0..0.....o#....oO...3. .o%....oQ.....+...,....+....+..*.0..0.....o#....o#...3..o%....o%.....+...,....+....

C:\Users\user\AppData\Roaming\eWoGxZG.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\GHhMZFFEmf.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**

C:\Users\user\AppData\Roaming\eWoGxZG.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1145
Entropy (8bit):	4.462201512373672
Encrypted:	false
SSDEEP:	24:zKLXkzPDObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0zPDQntKKH1MqJC
MD5:	46EBEB88876A00A52CC37B1F8E0D0438
SHA1:	5E5DB352F964E5F398301662FF558BD905798A65
SHA-256:	D65BD5A6CC112838AFE8FA70BF61FD13C1313BCE3EE3E76C50E454D7B581238B
SHA-512:	E713E6F304A469FB71235C598BC7E2C6F8458ABC61DAF3D1F364F66579CAFA4A7F3023E585BDA552FB400009E7805A8CA0311A50D5EDC9C2AD2D067772A071BE
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:... /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo Suppress logo output... /quiet Suppress logo output and success output...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.943323696866316
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	GHhMZFFEmf.exe
File size:	368128
MD5:	ace96cf7ef24eeac993b4da172a5a8f0
SHA1:	fa89615f55a87ef1d9ee9330ec5b0c040f54e8c1
SHA256:	d4ee80500d9c280e85b290b467592a5910e9d4ee127cfda17ad40467b2c88942
SHA512:	e1d5279223d7e82003bad73e94b1607b043c0b987987e9dc39ab9790558c4c840cd6949a37f87134fbd13b64c4a2492fb572eebde870db709d2a77c419c7ea1
SSDEEP:	6144:biuHodpZO0/zxllEpjNGLTk+eRSMjf9oHpqUFNsWPAyJt4SKbxF+wkonJx:upZOu7EpjAnkR/9a9rsWPAmyScxFRb
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X.wa.....0..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x45b2f6
Entrypoint Section:	.text

General

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:	0x61778758 [Tue Oct 26 04:43:04 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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	0x592fc	0x59400	False	0.962431066176	data	7.95466244747	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x5c000	0x5dc	0x600	False	0.4296875	data	4.16495497717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5e000	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
10/26/21-17:12:06.400060	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62044	8.8.8.8	192.168.2.6
10/26/21-17:12:13.421862	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63791	8.8.8.8	192.168.2.6
10/26/21-17:12:20.059046	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61346	8.8.8.8	192.168.2.6
10/26/21-17:12:26.416582	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51774	8.8.8.8	192.168.2.6
10/26/21-17:12:32.822515	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58384	8.8.8.8	192.168.2.6
10/26/21-17:12:52.460411	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50339	8.8.8.8	192.168.2.6
10/26/21-17:13:32.283168	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64021	8.8.8.8	192.168.2.6
10/26/21-17:13:39.916980	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58177	8.8.8.8	192.168.2.6
10/26/21-17:13:46.338970	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50700	8.8.8.8	192.168.2.6

Network Port Distribution

Copyright Joe Security LLC 2021

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 26, 2021 17:12:06.380254030 CEST	192.168.2.6	8.8.8.8	0x9b77	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:13.401860952 CEST	192.168.2.6	8.8.8.8	0x5965	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:20.037813902 CEST	192.168.2.6	8.8.8.8	0xcd55	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:26.385204077 CEST	192.168.2.6	8.8.8.8	0x5706	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:32.800523996 CEST	192.168.2.6	8.8.8.8	0xba2f	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:39.173913002 CEST	192.168.2.6	8.8.8.8	0x8beb	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:46.170840979 CEST	192.168.2.6	8.8.8.8	0x5406	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:52.440460920 CEST	192.168.2.6	8.8.8.8	0x61c8	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:58.633362055 CEST	192.168.2.6	8.8.8.8	0xeb75	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:04.940239906 CEST	192.168.2.6	8.8.8.8	0xe4cf	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:11.638370991 CEST	192.168.2.6	8.8.8.8	0xc0e2	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:18.900628090 CEST	192.168.2.6	8.8.8.8	0x5c4d	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:25.865489006 CEST	192.168.2.6	8.8.8.8	0x3e91	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:32.262892962 CEST	192.168.2.6	8.8.8.8	0xea00	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:39.896927118 CEST	192.168.2.6	8.8.8.8	0x3d8c	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:46.314315081 CEST	192.168.2.6	8.8.8.8	0xeb06	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:53.440485954 CEST	192.168.2.6	8.8.8.8	0xa231	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 26, 2021 17:12:06.400059938 CEST	8.8.8.8	192.168.2.6	0x9b77	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:13.421861887 CEST	8.8.8.8	192.168.2.6	0x5965	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:20.059046030 CEST	8.8.8.8	192.168.2.6	0xcd55	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:26.416582108 CEST	8.8.8.8	192.168.2.6	0x5706	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:32.822515011 CEST	8.8.8.8	192.168.2.6	0xba2f	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:39.193416119 CEST	8.8.8.8	192.168.2.6	0x8beb	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:46.190529108 CEST	8.8.8.8	192.168.2.6	0x5406	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:52.460411072 CEST	8.8.8.8	192.168.2.6	0x61c8	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:12:58.651909113 CEST	8.8.8.8	192.168.2.6	0xeb75	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:04.958895922 CEST	8.8.8.8	192.168.2.6	0xe4cf	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 26, 2021 17:13:11.657114983 CEST	8.8.8.8	192.168.2.6	0xc0e2	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:18.918715000 CEST	8.8.8.8	192.168.2.6	0x5c4d	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:25.883599997 CEST	8.8.8.8	192.168.2.6	0x3e91	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:32.283168077 CEST	8.8.8.8	192.168.2.6	0xea00	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:39.916980028 CEST	8.8.8.8	192.168.2.6	0x3d8c	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:46.338969946 CEST	8.8.8.8	192.168.2.6	0xeb06	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 17:13:53.460067987 CEST	8.8.8.8	192.168.2.6	0xa231	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: GHhMZFFEmf.exe PID: 6388 Parent PID: 5900

General

Start time:	17:11:48
Start date:	26/10/2021
Path:	C:\Users\user\Desktop\GHhMZFFEmf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\GHhMZFFEmf.exe'
Imagebase:	0xd80000
File size:	368128 bytes
MD5 hash:	ACE96CF7EF24EEAC993B4DA172A5A8F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.374588602.0000000004627000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.374588602.0000000004627000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.374588602.0000000004627000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.373937130.0000000003581000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.374161297.0000000003630000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.374682357.00000000046A9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.374682357.00000000046A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.374682357.00000000046A9000.00000004.00000001.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: 6656 Parent PID: 6388

General

Start time:	17:11:56
Start date:	26/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eWoGxZG' /XML 'C:\Users\user\AppData\Local\Temp\tmpBBC.tmp'
Imagebase:	0xea0000
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

Analysis Process: conhost.exe PID: 6672 Parent PID: 6656

General

Start time:	17:11:56
Start date:	26/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000

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: RegSvcs.exe PID: 6680 Parent PID: 6388

General

Start time:	17:11:56
Start date:	26/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0x360000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegSvcs.exe PID: 6716 Parent PID: 6388

General

Start time:	17:11:57
Start date:	26/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0x7e0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
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: 00000007.00000002.629752938.0000000005970000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.629752938.0000000005970000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.629950144.00000000059F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.629950144.00000000059F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.630106440.0000000005A70000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.630106440.0000000005A70000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.621893164.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.621893164.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.621893164.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.629869803.00000000059C0000.00000004.00020000.sdmp, Author: Florian Roth

	• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.629869803.00000000059C0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.630029119.0000000005A30000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.630029119.0000000005A30000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.629930642.00000000059E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.629930642.00000000059E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.630174361.0000000005AB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.630174361.0000000005AB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.630174361.0000000005AB0000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.629989793.0000000005A10000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.629989793.0000000005A10000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.629818927.00000000059A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.629818927.00000000059A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.629622545.0000000005790000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.629622545.0000000005790000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.629898256.00000000059D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.629898256.00000000059D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.630057484.0000000005A40000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.630057484.0000000005A40000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.629669654.0000000005810000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.629669654.0000000005810000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.627669995.0000000003D81000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.627669995.0000000003D81000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

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: 6764 Parent PID: 6716

General

Start time:	17:11:59
Start date:	26/10/2021
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\tmpA2A2.tmp'
Imagebase:	0xea0000
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: 6772 Parent PID: 6764

General

Start time:	17:11:59
Start date:	26/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 6836 Parent PID: 6716

General

Start time:	17:12:01
Start date:	26/10/2021
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\tmpA9E6.tmp'
Imagebase:	0xea0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Read

Analysis Process: RegSvcs.exe PID: 6852 Parent PID: 936

General

Start time:	17:12:01
Start date:	26/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0
Imagebase:	0xac0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6876 Parent PID: 6836

General

Start time:	17:12:01
Start date:	26/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6896 Parent PID: 6852

General

Start time:	17:12:02
Start date:	26/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Analysis Process: dhcpmon.exe PID: 7024 Parent PID: 936

General

Start time:	17:12:04
Start date:	26/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x4c0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 7080 Parent PID: 7024

General

Start time:	17:12:05
Start date:	26/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 4408 Parent PID: 3440

General

Start time:	17:12:12
Start date:	26/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x580000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 5676 Parent PID: 4408

General

Start time:	17:12:13
Start date:	26/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021