ID: 552676
Sample Name: BmFKvDpmPT
Cookbook: default.jbs
Time: 16:15:41
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

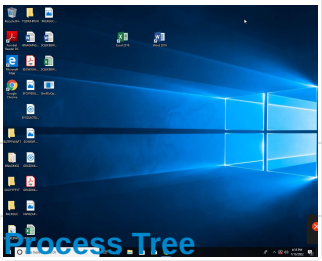
Windows Analysis Report BmFKvDpmPT

Overview

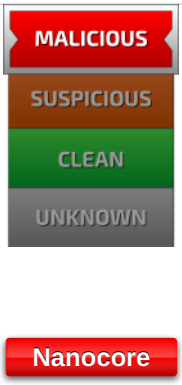
General Information

Sample Name:	BmFKvDpmPT (renamed file extension from none to exe)
Analysis ID:	552676
MD5:	33c0d67befa1150.
SHA1:	843fad90b9becb0.
SHA256:	1fd93f45ddbe623..
Tags:	32 exe NanoCore
Infos:	

Most interesting Screenshot:



Detection

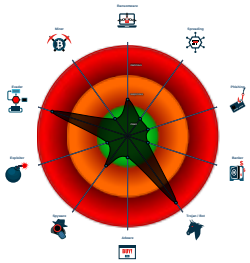


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Sigma detected: Bad Opsec Default…

Classification



- **System is w10x64**
- BmFKvDpmPT.exe (PID: 6756 cmdline: "C:\Users\user\Desktop\BmFKvDpmPT.exe" MD5: 33C0D67BEFA115099A9136F837D11CC9)
  - powershell.exe (PID: 6828 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\RlKeHhAgpZws.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6836 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6844 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\RlKeHhAgpZws" /XML "C:\Users\user\AppData\Local\Temp\tmpD8B7.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6944 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6996 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - schtasks.exe (PID: 3460 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp362C.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5708 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp408E.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6224 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 5832 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 3860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 908 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 4140 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "fea2b910-0578-480b-a4fe-76b7fc47",
  "Group": "Phaddy",
  "Domain1": "obeyice4rm392.bounceme.net",
  "Domain2": "127.0.0.1",
  "Port": 8951,
  "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
00000005.00000002.566000035.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000005.00000002.566000035.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000002.566000035.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000005.00000000.319761146.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000005.00000000.319761146.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 23 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.RegSvcs.exe.29f5df4.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
5.2.RegSvcs.exe.29f5df4.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
5.2.RegSvcs.exe.29a3178.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
5.2.RegSvcs.exe.29a3178.1.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
5.0.RegSvcs.exe.400000.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 46 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: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Possible Applocker Bypass

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

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

Antivirus detection for URL or domain

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:

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

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

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

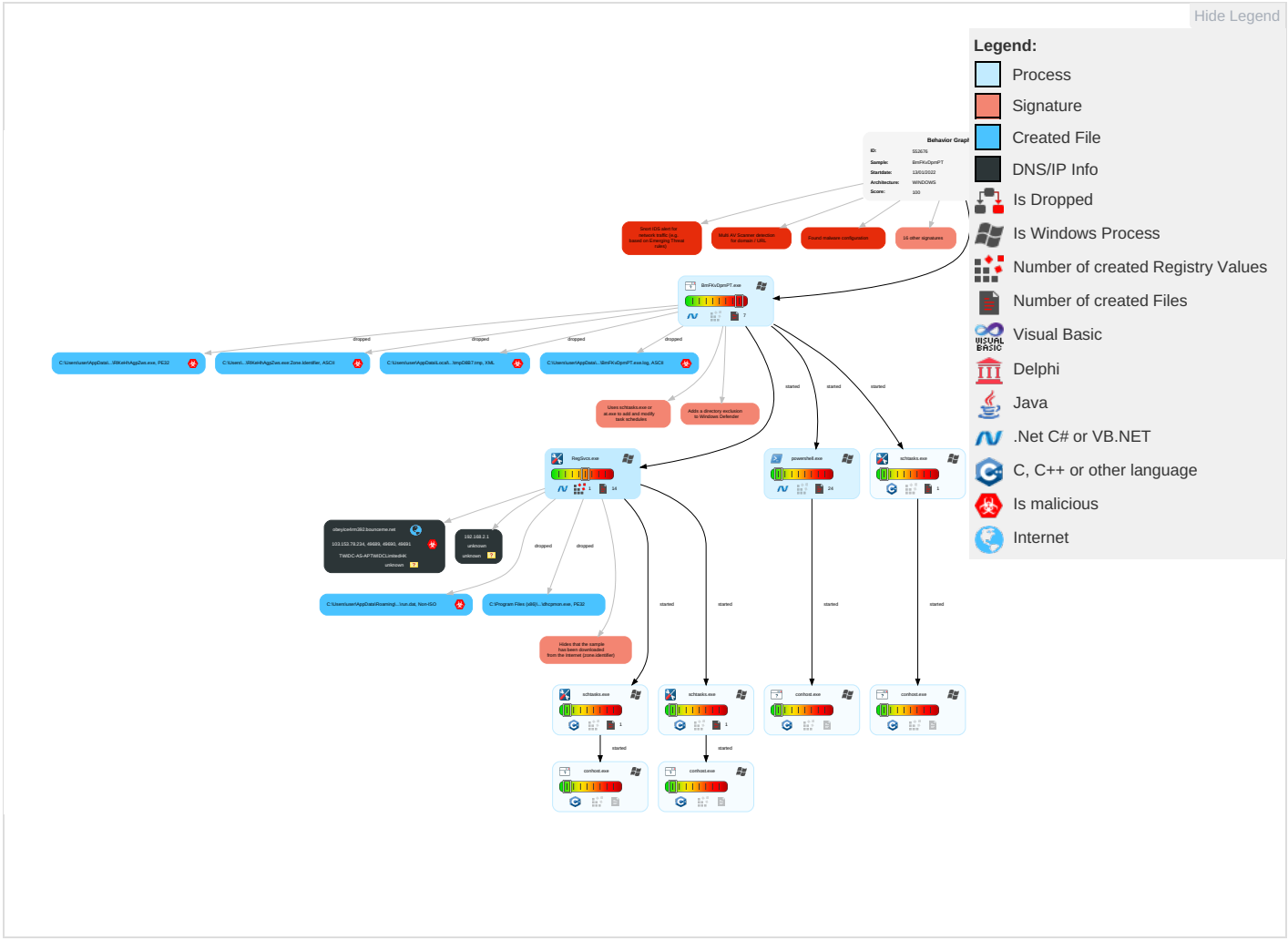
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 2	OS Credential Dumping	Security Software Discovery 2 1 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdı Insecure Networl Commu

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirec Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit S Track D Locatior
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial c Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue \ Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base St

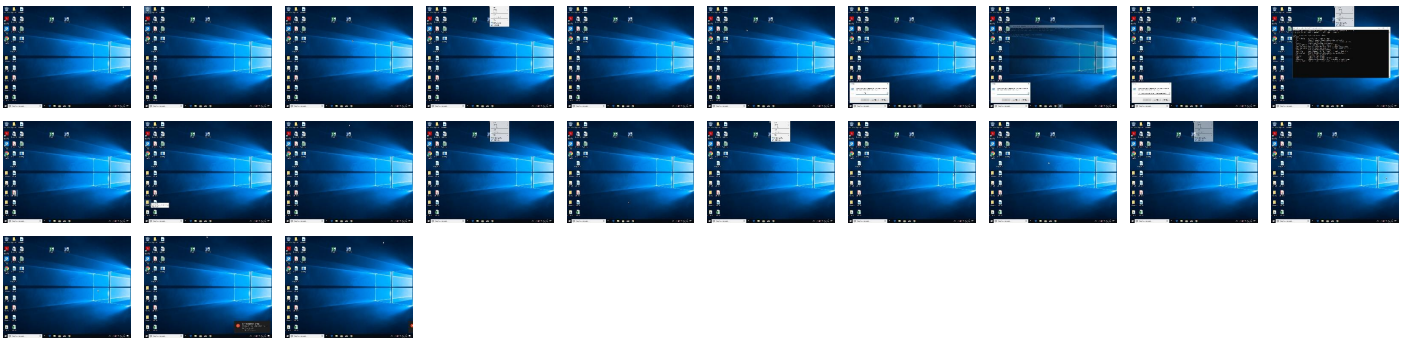
Behavior Graph



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
BmFKvDpmPT.exe	55%	Virustotal		Browse
BmFKvDpmPT.exe	56%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
BmFKvDpmPT.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\RlKeHhAgpZws.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\RlKeHhAgpZws.exe	56%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
5.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
obeyice4rm392.bounceme.net	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.fontbureau.coml:	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0li	0%	Avira URL Cloud	safe	
http://www.fontbureau.comony-u	0%	Avira URL Cloud	safe	
http://www.sakkal.comrm	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//typ	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://crl.microsoft.co	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn-u	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.fontbureau.comueu	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
127.0.0.1	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/T	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn6	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comdF	0%	Avira URL Cloud	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.fontbureau.comM.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/nl	0%	Avira URL Cloud	safe	
obeyice4rm392.bounceme.net	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
obeyice4rm392.bounceme.net	103.153.78.234	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
127.0.0.1	true	• Avira URL Cloud: safe	unknown
obeyice4rm392.bounceme.net	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.153.78.234	obeyice4rm392.bounceme.net	unknown	?	134687	TWIDC-AS-APTWIDCLimitedHK	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552676
Start date:	13.01.2022
Start time:	16:15:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BmFKvDpmPT (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:	21
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@21/21@15/2
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 4% (good quality ratio 1.9%) • Quality average: 28.3% • Quality standard deviation: 35.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:16:45	API Interceptor	1x Sleep call for process: BmFKvDpmPT.exe modified
16:16:50	API Interceptor	41x Sleep call for process: powershell.exe modified
16:17:01	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" s>$(Arg0)
16:17:02	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
16:17:03	API Interceptor	878x Sleep call for process: RegSvcs.exe modified
16:17:04	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(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:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D(B42
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~....,(....~....o....9]...

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

Process:	C:\Users\user\Desktop\BmFKvDpmPT.exe

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BmFKvDpmPT.exe.log	
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	**true**
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\RegSvcs.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22284
Entropy (8bit):	5.6026303008043215
Encrypted:	false
SSDEEP:	384:stCDqC0a+ZtvJ0VswSBKnL4jultI2H7Y9gxSJ3xCT1MabZlbAV7wng7SZBDI+iqY:2XxkR4KsCltJXxcQCqfwEjVQ
MD5:	CA690D76A0FBACD13729411033DE4080
SHA1:	2C544994C7FA4A483B87C7BED0F442CE4610FD7A
SHA-256:	A2E7A4802F7AF8A433032B9D83160D0352184C97637752125C111ADBB6B7D12F
SHA-512:	7687429980BE3673A36D7991E180CF2B04B2C0496C702EFD8758F4BD6C51CD0FB0D6EC7E3328DB59D330321D8C86ED0A12995EF534C71F288B24DFFC26E0754
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Preview:	@...e.....|.....h.N.....G.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1cc2z5ov.cvt.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gtqgws2z.xpb.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp362C.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135668813522653
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mXxtn:cbk4oL600QydbQxIYODOLedq3ZXj
MD5:	8CAD1B41587CED0F1E74396794F31D58
SHA1:	11054BF74FCF5E8E412768035E4DAE43AA7B710F
SHA-256:	3086D914F6B23268F8A12CB1A05516CD5465C2577E1D1E449F1B45C8E5E8F83C
SHA-512:	99C2EF89029DE51A866DF932841684B7FC912DF21E10E2DD0D09E400203BBDC6CBA6319A31780B7BF8B286D2CEA8EA3FC7D084348BF2F002AB4F5A34218CCB F
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>.. <StopIfGoingOnBatterie s>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAv ailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </Idl eSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp408E.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310

C:\Users\user\AppData\Local\Temp\tmp408E.tmp	
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\Local\Temp\tmpD8B7.tmp	
Process:	C:\Users\user\Desktop\BmFKvDpmPT.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1599
Entropy (8bit):	5.150955410410787
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtyxvn:cge4MYrFdOFzOzN33ODOiDdKrsuT2v
MD5:	2A834FE86EAC835920AC846A22C7F27C
SHA1:	1BBABFB4220120CF1CD6420B930684983A961B68
SHA-256:	46D349E79C06781E623586007DB7779AF3190EFF029DB504AB8D26A030E26F2A
SHA-512:	D9965302C5ABFA139638DCEC0961EFE9D09EF5CB77D1C66BC1B6E7A5E1959AE9FF2B7D6C8070B6ABDF44F77F95D49956FBFF40C97B2193E6FFA73396B9091D7
Malicious:	**true**
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</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\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:	3:74n:74n
MD5:	70C2F77424FFC5FE5CC6CE131AB75A1A
SHA1:	5387F558ADF54CE9462C7662E72E10F2FFC5877A
SHA-256:	D986AFDE5DC2CB7F4D2495357F01B6D9DDD4372A87ED53475077A9F768D49E03
SHA-512:	C9E1466694415DE8D940AE3C96EE4B0F1136180C918A631EDF8704D64A1E1E136C4423053153D38AB0129F07FF27649B7FB5AA587744B77D088DB8BC47902D4B

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Malicious:	**true**
Preview:	.9.-...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'..}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,...]t.:.....[.Z.u...3X8.Ql..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC.... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.830795005765378
Encrypted:	false
SSDEEP:	3:oMty8WddSWA1KMNn:oMLW6WA1j
MD5:	08E799E8E9B4FDA648F2500A40A11933
SHA1:	AC76B5E20DED247803448A2F586731ED7D84B9F3
SHA-256:	D46E34924067EB071D1F031C0BC015F4B711EDCE64D8AE00F24F29E73ECB71DB
SHA-512:	5C5701A86156D573BE274E73615FD6236AC89630714863A4CB2639EEC8EC1BE746839EBF8A9AEBA0A9BE326AF6FA02D8F9BD7A93D3FFB139BADE945572DF5FE9
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

C:\Users\user\AppData\Roaming\RlKeHhAgpZws.exe	
Process:	C:\Users\user\Desktop\BmFKvDpmPT.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	459264
Entropy (8bit):	7.786929247209251
Encrypted:	false
SSDEEP:	12288:+K777777777777cP+K8+Zt+9vpb0qOpPx4MQer7Z0mzQmTpvGrUK:+K777777777777c++2x7Ojdr2mzQcvGA
MD5:	33C0D67BEFA115099A9136F837D11CC9

C:\Users\user\AppData\Roaming\RlKeHhAgpZws.exe	
SHA1:	843FAD90B9BECB0457824CBAEABC3899FC055BEA
SHA-256:	1FD93F45DDBE62337F2B72E31E6A82880BC0581430ABEAEBDA88AC1F58272210
SHA-512:	06DE0E772E61AC4755340DA201DE39FCA9086286E6EC620A917847A7DF394E3F8E0D3568760996D0C539ECE99FD57E0911CB0CD11459713C060676A7D3D9FD6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 56%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....%.....0..... ... .@.. .....`..... ..@.....O.... ..8.....@..... ..... ..H.....text..... ..... ..`.rsrc...8.... .....@..@.rel oc.....@.....@..B.....H.....(3.....".....a.....0..(.....(.....,r...ps....z.u....%-.&..*..{....*..{....*.0..'.....(....s.....(.....%..o.....(....s....*..(.....,..(.....(.....Ys....+...s....*..(.....(.....(.....Xs....+...(.....Xs....*..0..E.....YE.....+..(.....+...+..(.....+.r...p.....s....z.*..s*.r...p*...(.....(....+.r#..p..2...(....*.0..b..... (.....,r/..ps....z.....,r9..ps....z..}.....}.....}.

C:\Users\user\AppData\Roaming\RlKeHhAgpZws.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\BmFKvDpmPT.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**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220113\PowerShell_transcript.116938.iUjVe067.20220113161648.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5797
Entropy (8bit):	5.404419164812296
Encrypted:	false
SSDEEP:	96:BZyhSNaqDo1ZKZFhSNaqDo1ZK/lXjZphSNaqDo1Z/V2nn2Zd:4/
MD5:	342ECDAF4F6F13CE7BFB199E9DDD5E1B
SHA1:	207035F852A492CFB34D737A060A93719CE17DA1
SHA-256:	AACC9F126CBE6D338796C036ADDF70031F2FAD9540E459A9784552AF47EC8EF2
SHA-512:	0356BE28BA38E5175B8B900DD5B51AAED6C55623A20B84E0D0C2584F4F17281344FE4AF9068167D3E3033A466CA0A0A3AB9B2683692F6230B2C33EBBCC8958D
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220113161650..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 116938 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\RlKeHhAgpZws.exe..Process ID: 6828..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220113161650..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\RlKeHhAgpZws.exe..**********..Windows PowerShell transcript start..Start time: 20220113162111..Username: computer\user..RunAs User: computer\

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141
Malicious:	false

\Device\ConDrv	
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..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 Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.786929247209251
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:	BmFKvDpmPT.exe
File size:	459264
MD5:	33c0d67befa115099a9136f837d11cc9
SHA1:	843fad90b9becb0457824cbaeabc3899fc055bea
SHA256:	1fd93f45ddbe62337f2b72e31e6a82880bc0581430abeaebda88ac1f58272210
SHA512:	06de0e772e61ac4755340da201de39fca9086286e6ec620a917847a7df394e3f8e0d3568760996d0c539ece99fd57e0911cb0cd11459713c060676a7d3d9fd69
SSDEEP:	12288:+K777777777777cP+K8+Zt+9vpb0qOpPx4MQer7Z0mzQmTpvGrUK:+K777777777777c++2x7Ojdr2mzQcvGA
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....%.....0..... ... .@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47150e
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:	0xCE259BBB [Sun Aug 6 18:13:15 2079 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	0x6f514	0x6f600	False	0.901346362935	SysEx File - PalmTree	7.80319050682	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x72000	0x638	0x800	False	0.33544921875	data	3.48879088224	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x74000	0xc	0x200	False	0.044921875	data	0.0980041756627	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
01/13/22-16:17:05.138307	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54781	8.8.8.8	192.168.2.3
01/13/22-16:17:05.625124	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49689	8951	192.168.2.3	103.153.78.234
01/13/22-16:17:11.821078	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62151	8.8.8.8	192.168.2.3
01/13/22-16:17:12.050770	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49690	8951	192.168.2.3	103.153.78.234
01/13/22-16:17:18.740589	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51209	8.8.8.8	192.168.2.3
01/13/22-16:17:19.038885	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49691	8951	192.168.2.3	103.153.78.234
01/13/22-16:17:26.118051	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49692	8951	192.168.2.3	103.153.78.234
01/13/22-16:17:33.217749	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49694	8951	192.168.2.3	103.153.78.234
01/13/22-16:17:41.616253	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58604	8.8.8.8	192.168.2.3
01/13/22-16:17:41.843070	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49695	8951	192.168.2.3	103.153.78.234
01/13/22-16:17:49.190595	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49696	8951	192.168.2.3	103.153.78.234
01/13/22-16:17:55.871269	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49697	8951	192.168.2.3	103.153.78.234
01/13/22-16:18:02.126321	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49698	8951	192.168.2.3	103.153.78.234
01/13/22-16:18:09.373372	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49699	8951	192.168.2.3	103.153.78.234
01/13/22-16:18:16.668585	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57459	8.8.8.8	192.168.2.3
01/13/22-16:18:16.904489	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49700	8951	192.168.2.3	103.153.78.234
01/13/22-16:18:23.649406	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57875	8.8.8.8	192.168.2.3
01/13/22-16:18:23.890289	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49701	8951	192.168.2.3	103.153.78.234
01/13/22-16:18:30.148710	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49702	8951	192.168.2.3	103.153.78.234
01/13/22-16:18:37.123199	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52806	8.8.8.8	192.168.2.3
01/13/22-16:18:37.430563	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49703	8951	192.168.2.3	103.153.78.234
01/13/22-16:18:45.203552	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53910	8.8.8.8	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/22-16:18:45.468628	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49704	8951	192.168.2.3	103.153.78.234

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 16:17:05.117351055 CET	192.168.2.3	8.8.8.8	0xf55d	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:17:11.801876068 CET	192.168.2.3	8.8.8.8	0xf278	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:17:18.719270945 CET	192.168.2.3	8.8.8.8	0x575	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:17:25.866750956 CET	192.168.2.3	8.8.8.8	0xea94	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:17:32.972183943 CET	192.168.2.3	8.8.8.8	0xcc27	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:17:41.591686010 CET	192.168.2.3	8.8.8.8	0x8203	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:17:48.889053106 CET	192.168.2.3	8.8.8.8	0x197	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:17:55.625232935 CET	192.168.2.3	8.8.8.8	0x4f00	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:01.882651091 CET	192.168.2.3	8.8.8.8	0xb955	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:09.127432108 CET	192.168.2.3	8.8.8.8	0xd49a	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:16.647773981 CET	192.168.2.3	8.8.8.8	0x2e0a	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:23.628566027 CET	192.168.2.3	8.8.8.8	0x7566	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:29.887677908 CET	192.168.2.3	8.8.8.8	0x615c	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:37.102031946 CET	192.168.2.3	8.8.8.8	0x9f61	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:45.182492018 CET	192.168.2.3	8.8.8.8	0x9df0	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 16:17:05.138307095 CET	8.8.8.8	192.168.2.3	0xf55d	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 16:17:11.821078062 CET	8.8.8.8	192.168.2.3	0xf278	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 16:17:18.740588903 CET	8.8.8.8	192.168.2.3	0x575	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 16:17:25.883893013 CET	8.8.8.8	192.168.2.3	0xea94	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 16:17:32.989833117 CET	8.8.8.8	192.168.2.3	0xcc27	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 16:17:41.616252899 CET	8.8.8.8	192.168.2.3	0x8203	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 16:17:48.906569004 CET	8.8.8.8	192.168.2.3	0x197	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 16:17:55.644090891 CET	8.8.8.8	192.168.2.3	0x4f00	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:01.899879932 CET	8.8.8.8	192.168.2.3	0xb955	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:09.146888018 CET	8.8.8.8	192.168.2.3	0xd49a	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:16.668585062 CET	8.8.8.8	192.168.2.3	0x2e0a	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:23.649405956 CET	8.8.8.8	192.168.2.3	0x7566	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:29.907026052 CET	8.8.8.8	192.168.2.3	0x615c	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:37.123198986 CET	8.8.8.8	192.168.2.3	0x9f61	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 16:18:45.203552008 CET	8.8.8.8	192.168.2.3	0x9df0	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: BmFKvDpmPT.exe PID: 6756 Parent PID: 5764

General

Start time:	16:16:39
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\BmFKvDpmPT.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\BmFKvDpmPT.exe"
Imagebase:	0x260000
File size:	459264 bytes
MD5 hash:	33C0D67BEFA115099A9136F837D11CC9
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: 00000000.00000002.325875243.0000000002761000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.333190645.0000000003769000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.333190645.0000000003769000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.333190645.0000000003769000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.329114448.0000000002882000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6828 Parent PID: 6756

General

Start time:	16:16:47
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\RlKeHhAgpZws.exe
Imagebase:	0x960000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6836 Parent PID: 6828

General

Start time:	16:16:47

Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: 6756

General

Start time:	16:16:48
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\RlKeHhAgpZws" /XML "C:\Users\user\AppData\Local\Temp\tmpD8B7.tmp
Imagebase:	0x3f0000
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: 6944 Parent PID: 6844

General

Start time:	16:16:49
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: 6996 Parent PID: 6756

General

Start time:	16:16:50
Start date:	13/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x660000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000005.00000002.566000035.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.566000035.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.566000035.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.319761146.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.319761146.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.319761146.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.319251855.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.319251855.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.319251855.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.320809226.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.320809226.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.320809226.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.320304519.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.320304519.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.320304519.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.567708618.00000000029E3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

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: 3460 Parent PID: 6996

General

Start time:	16:16:59
Start date:	13/01/2022
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\tmp362C.tmp
Imagebase:	0x3f0000
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: 5528 Parent PID: 3460

General

Start time:	16:17:00
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: 5832 Parent PID: 664

General

Start time:	16:17:01
Start date:	13/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe 0
Imagebase:	0xc0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: schtasks.exe PID: 5708 Parent PID: 6996

General

Start time:	16:17:02
Start date:	13/01/2022
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\tmp408E.tmp
Imagebase:	0x3f0000
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: conhost.exe PID: 3860 Parent PID: 5832

General

Start time:	16:17:02
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: 6224 Parent PID: 5708

General

Start time:	16:17:03
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: 908 Parent PID: 664

General

Start time:	16:17:04
Start date:	13/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xb30000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: conhost.exe PID: 6408 Parent PID: 908

General

Start time:	16:17:04
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: 4140 Parent PID: 3352

General

Start time:	16:17:11
Start date:	13/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xb00000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5380 Parent PID: 4140

General

Start time:	16:17:11
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis