ID: 528195
Sample Name: ERIG_0983763673-093876536783.exe
Cookbook: default.jbs
Time: 20:49:36
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report ERIG_0983763673-093876536783.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
AV Detection: 6
E-Banking Fraud: 6
System Summary: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Jbx Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
Private 11
General Information 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 13
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 19
Data Directories 19
Sections 19
Resources 19
Imports 19
Version Infos 19
Network Behavior 19
Snort IDS Alerts 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 19

DNS Queries 19
DNS Answers 20
Code Manipulations 20
Statistics 20
Behavior 20
System Behavior 21
Analysis Process: ERIG_0983763673-093876536783.exe PID: 640 Parent PID: 5712 21
General 21
File Activities 21
File Created 21
File Deleted 21
File Written 21
File Read 21
Analysis Process: powershell.exe PID: 488 Parent PID: 640 21
General 21
File Activities 22
File Created 22
File Deleted 22
File Written 22
File Read 22
Analysis Process: conhost.exe PID: 4392 Parent PID: 488 22
General 22
Analysis Process: schtasks.exe PID: 340 Parent PID: 640 22
General 22
File Activities 22
File Read 22
Analysis Process: conhost.exe PID: 5988 Parent PID: 340 22
General 22
Analysis Process: RegSvcs.exe PID: 3668 Parent PID: 640 23
General 23
File Activities 24
File Created 24
File Deleted 24
File Written 24
File Read 24
Registry Activities 24
Key Value Created 24
Analysis Process: schtasks.exe PID: 6368 Parent PID: 3668 25
General 25
File Activities 25
File Read 25
Analysis Process: conhost.exe PID: 6376 Parent PID: 6368 25
General 25
Analysis Process: schtasks.exe PID: 6424 Parent PID: 3668 25
General 25
File Activities 25
File Read 26
Analysis Process: RegSvcs.exe PID: 6432 Parent PID: 904 26
General 26
File Activities 26
File Created 26
File Written 26
File Read 26
Analysis Process: conhost.exe PID: 6464 Parent PID: 6432 26
General 26
Analysis Process: conhost.exe PID: 6516 Parent PID: 6424 26
General 26
Analysis Process: dhcpmon.exe PID: 6696 Parent PID: 904 27
General 27
Analysis Process: conhost.exe PID: 6716 Parent PID: 6696 27
General 27
Analysis Process: dhcpmon.exe PID: 6868 Parent PID: 3472 27
General 27
Analysis Process: conhost.exe PID: 6876 Parent PID: 6868 27
General 28
Disassembly 28
Code Analysis 28

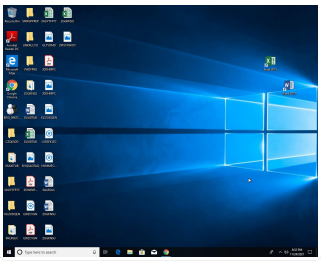
Windows Analysis Report ERIG_0983763673-093876536…

Overview

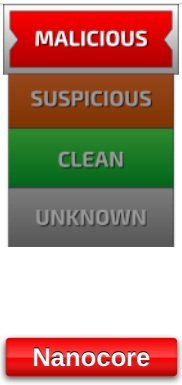
General Information

Sample Name:	ERIG_0983763673-093876536783.exe
Analysis ID:	528195
MD5:	6a4599e499c357..
SHA1:	da9fab687ce9b7c..
SHA256:	02d517033bd02f9.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

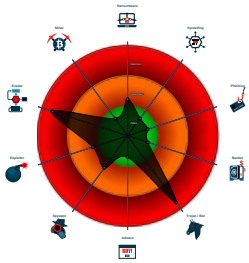


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- .NET source code contains potentia…
- Sigma detected: Powershell Defende…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- ERIG_0983763673-093876536783.exe (PID: 640 cmdline: "C:\Users\user\Desktop\ERIG_0983763673-093876536783.exe" MD5: 6A4599E499C357E47EBDF9021CF4613B)
  - powershell.exe (PID: 488 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\sFSDBgPwTyWm.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4392 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 340 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\sFSDBgPwTyWm" /XML "C:\Users\user\AppData\Local\Temp\tmp2122.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 3668 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - schtasks.exe (PID: 6368 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp6138.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6376 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6424 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp6909.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6516 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 6432 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6464 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6696 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6868 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "7b578534-8b04-4a5d-9eb5-d375830c",
  "Group": "6262",
  "Domain1": "6262.hopto.org",
  "Domain2": "185.140.53.131",
  "Port": 6262,
  "KeyboardLogging": "Enable",
  "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
0000000A.00000002.521737598.00000000051F0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0000000A.00000002.521737598.00000000051F0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
0000000A.00000002.521737598.00000000051F0000.00000004.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000A.00000002.514316239.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000A.00000002.514316239.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 28 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.RegSvcs.exe.51f0000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
10.2.RegSvcs.exe.51f0000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
10.2.RegSvcs.exe.51f0000.6.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
10.0.RegSvcs.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
10.0.RegSvcs.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
Click to see the 58 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

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Networking:

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

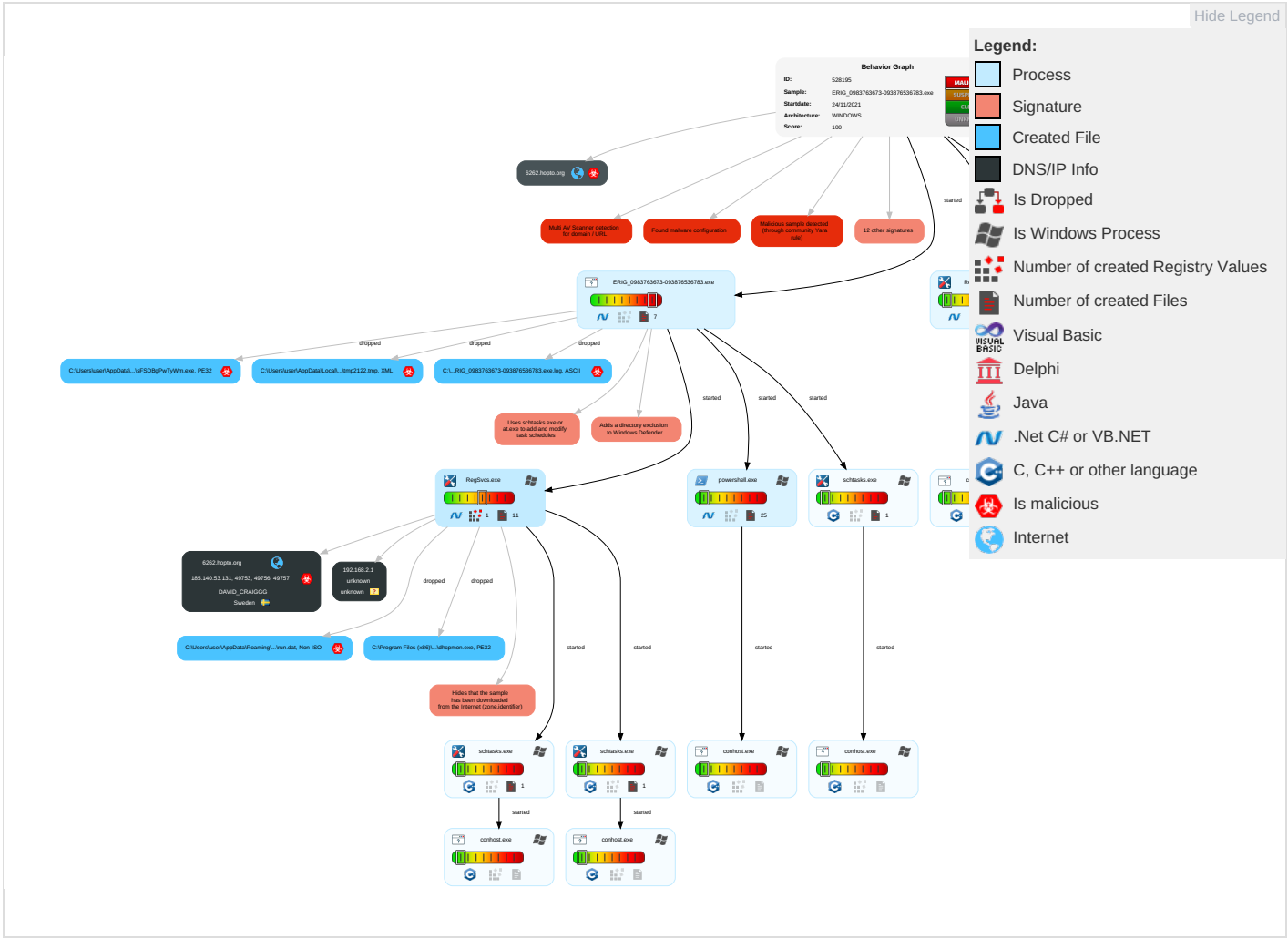
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 2	Input Capture 1 1	Security Software Discovery 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdro Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect 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 De Location
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 Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
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	Manipula Device Commun
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	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P
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	Downgra Insecure Protocols

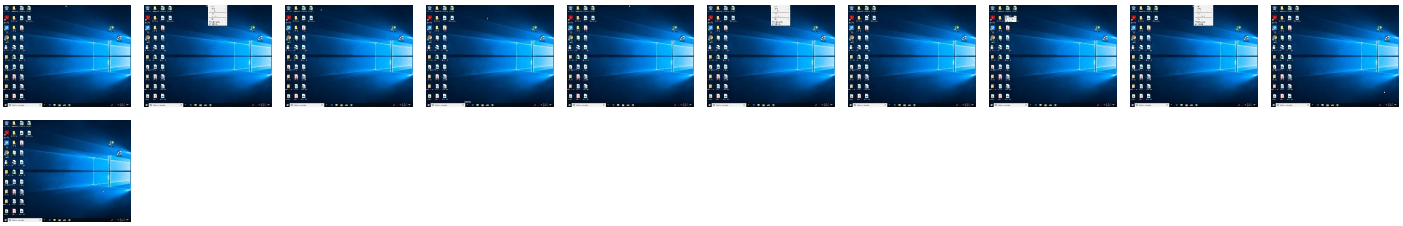
Behavior Graph



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
ERIG_0983763673-093876536783.exe	40%	Virustotal		Browse
ERIG_0983763673-093876536783.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
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\sFSDBgPwTyWm.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.2.RegSvcs.exe.51f0000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
10.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
6262.hopto.org	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
6262.hopto.org	2%	Virustotal		Browse
6262.hopto.org	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.chinhdo.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
185.140.53.131	6%	Virustotal		Browse
185.140.53.131	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
6262.hopto.org	185.140.53.131	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
6262.hopto.org	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
185.140.53.131	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.131	6262.hopto.org	Sweden		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528195
Start date:	24.11.2021
Start time:	20:49:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ERIG_0983763673-093876536783.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:	38
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@21/18@12/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1% (good quality ratio 0.8%) • Quality average: 46.7% • Quality standard deviation: 34.2%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:50:45	API Interceptor	2x Sleep call for process: ERIG_0983763673-093876536783.exe modified
20:50:50	API Interceptor	27x Sleep call for process: powershell.exe modified
20:51:01	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" s>$(Arg0)
20:51:02	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
20:51:03	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
20:51:03	API Interceptor	844x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.131	tj9KzQvUFy.exe	Get hash	malicious	Browse	
	TR0398734893 50601251.exe	Get hash	malicious	Browse	
	UTYHFG03983765367839837653.exe	Get hash	malicious	Browse	
	XPDL_0938763673-3987356378998736563.exe	Get hash	malicious	Browse	
	HVX_098765434567-5456799876.exe	Get hash	malicious	Browse	
	DFTE98765464-4987465546784.exe	Get hash	malicious	Browse	
	MB#U007e1234567876-098767.exe	Get hash	malicious	Browse	
	IMG#U007e0398763536783.exe	Get hash	malicious	Browse	
	remitcopy.jar	Get hash	malicious	Browse	
	remittance copy.jar	Get hash	malicious	Browse	
	remittance copy.jar	Get hash	malicious	Browse	
	MRC20201030XMY,pdf.exe	Get hash	malicious	Browse	
	SP AIR B00,pdf.exe	Get hash	malicious	Browse	
	FACA000400007998.pdf.exe	Get hash	malicious	Browse	
	MS210201,pdf.exe	Get hash	malicious	Browse	
	20082020141903,pdf.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	Urgent order 1812021-672 Q30721,pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
6262.hopto.org	tj9KzQvUFy.exe	Get hash	malicious	Browse	• 185.140.53.131

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	copy_tt_inv_10192ne.exe	Get hash	malicious	Browse	• 91.193.75.149
	DHL Tracking.exe	Get hash	malicious	Browse	• 185.140.53.33
	tj9KzQvUFy.exe	Get hash	malicious	Browse	• 185.140.53.131
	Purchase Order.exe	Get hash	malicious	Browse	• 185.140.53.160
	Orden de Compra -SA765443,pdf.exe	Get hash	malicious	Browse	• 185.140.53.12
	purchase order 0112.exe	Get hash	malicious	Browse	• 185.140.53.137
	9mMANDmw9O.exe	Get hash	malicious	Browse	• 91.193.75.190
	TR0398734893 50601251.exe	Get hash	malicious	Browse	• 185.140.53.131
	swift.xls	Get hash	malicious	Browse	• 91.193.75.212
	SOA_0009877890.exe	Get hash	malicious	Browse	• 185.244.30.58
	8UYr1od7iW.exe	Get hash	malicious	Browse	• 91.193.75.148
	928272_Payment_Receipt.vbs	Get hash	malicious	Browse	• 185.140.53.3
	N2K18_Payment_Copy.vbs	Get hash	malicious	Browse	• 185.140.53.3
	U2M19O_Payment_Copy.vbs	Get hash	malicious	Browse	• 185.140.53.3
	J3m1a_Payment_Copy.vbs	Get hash	malicious	Browse	• 185.140.53.3
	18-11-21 Statement.xlsx	Get hash	malicious	Browse	• 91.193.75.148
	bWKXCwatmt.exe	Get hash	malicious	Browse	• 91.193.75.148
	17-11-21 STATEMENT.xlsx	Get hash	malicious	Browse	• 91.193.75.148
	Copy of Complaint report-1st Nov21 to 16th Nov21.xlsx	Get hash	malicious	Browse	• 91.193.75.148
	UTYHFG03983765367839837653.exe	Get hash	malicious	Browse	• 185.140.53.131

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Euro invoice.exe	Get hash	malicious	Browse	
	Shipping Document BL Draft.exe	Get hash	malicious	Browse	
	incorrect payment information.exe	Get hash	malicious	Browse	
	TransactionSummary_22-11-2021.exe	Get hash	malicious	Browse	
	SWIFT COPY.exe	Get hash	malicious	Browse	
	TT COPY.exe	Get hash	malicious	Browse	
	Payment Advice 50053945.exe	Get hash	malicious	Browse	
	750845PaymentReceipt.exe	Get hash	malicious	Browse	
	Copy BL and Debit Note.exe	Get hash	malicious	Browse	
	QUOTATION.exe	Get hash	malicious	Browse	
	PO_SBK4128332S.exe	Get hash	malicious	Browse	
	New order - C.S.I No. 0987.exe	Get hash	malicious	Browse	
	Bank payment swift message.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	HSBC Payment Advice.exe	Get hash	malicious	Browse	
	UTYHFG03983765367839837653.exe	Get hash	malicious	Browse	
	qaNcOX8rVf.exe	Get hash	malicious	Browse	
	XPDL_0938763673-3987356378998736563.exe	Get hash	malicious	Browse	
	HVX_098765434567-5456799876.exe	Get hash	malicious	Browse	

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%
Joe Sandbox View:	• Filename: Euro invoice.exe, Detection: malicious, Browse • Filename: Shipping Document BL Draft.exe, Detection: malicious, Browse • Filename: incorrect payment information.exe, Detection: malicious, Browse • Filename: TransactionSummary_22-11-2021.exe, Detection: malicious, Browse • Filename: SWIFT COPY.exe, Detection: malicious, Browse • Filename: TT COPY.exe, Detection: malicious, Browse • Filename: Payment Advice 50053945.exe, Detection: malicious, Browse • Filename: 750845PaymentReceipt.exe, Detection: malicious, Browse • Filename: Copy BL and Debit Note.exe, Detection: malicious, Browse • Filename: QUOTATION.exe, Detection: malicious, Browse • Filename: PO_SBK4128332S.exe, Detection: malicious, Browse • Filename: New order - C.S.I No. 0987.exe, Detection: malicious, Browse • Filename: Bank payment swift message.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: HSBC Payment Advice.exe, Detection: malicious, Browse • Filename: UTYHFG03983765367839837653.exe, Detection: malicious, Browse • Filename: qaNcOX8rVf.exe, Detection: malicious, Browse • Filename: XPDL_0938763673-3987356378998736563.exe, Detection: malicious, Browse • Filename: HVX_098765434567-5456799876.exe, Detection: malicious, Browse
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\ERIG_0983763673-093876536783.exe.log	
Process:	C:\Users\user\Desktop\ERIG_0983763673-093876536783.exe

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ERIG_0983763673-093876536783.exe.log	
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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):	22400
Entropy (8bit):	5.6028098013746375
Encrypted:	false
SSDEEP:	384:itqDZn6QtKh8ni8kiDASBKnIjuItIC3t9gZSJ3xOT1MajZlbAV7nJ6ZBDI+lzYB:KhmBkis4KIClt9cZc8CSfwUV0
MD5:	5EBBCF70F00AC7894C76773CF91FC0AE
SHA1:	6A6AC13C75D5BEAC63CE36FE680183B9806ACBB9
SHA-256:	1E599D081E3DC1B71A2BB8505ED9F5B8969593F63CFDD6BF1ADF76C15A7D2A34
SHA-512:	7A9B1AF84B44DAA6531215A8DBE3F7588853A41607365EAEB4925667DFCD66E3598356756A62118C33372E04000EAD17660FC1E312C3D540EF076EBFDC28B9EC
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Preview:	@...e.....h.....l.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.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.DirectoryServices4.....].D.E.....#.....System.Data.<.....H..QN.Y.f.....System.Management...H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.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_rf111wi3.3i2.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__PSScriptPolicyTest_ygu3wsr5.a4g.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\tmp2122.tmp	
Process:	C:\Users\user\Desktop\ERIG_0983763673-093876536783.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1603
Entropy (8bit):	5.1327121199519
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNt5xvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTvv
MD5:	9353CDC2E49582B361ADE986EB7F7FA2
SHA1:	8ED47F2FA24F1856C7645C4796A8428C2006601F
SHA-256:	B3CC22FC1BAFA1224C29C528A277B7E9C62F4C70959CE400F4D20E4465CE6BD1
SHA-512:	E16C4F05B409439944BA5E2CF468A3DCD1F83D2C60FEC3A665616F1E1D5AE4FEE2993F7104E0489E65B02B8EC7D2EC41E1B68C4762EEB9C02BCF61E5277BD37
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\Local\Temp\tmp6138.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

C:\Users\user\AppData\Local\Temp\tmp6138.tmp	
Entropy (8bit):	5.135668813522653
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mXxtn:cbk4oL600QydbQxIYODOLedq3ZXj
MD5:	8CAD1B41587CED0F1E74396794F31D58
SHA1:	11054BF74FCF5E8E412768035E4DAE43AA7B710F
SHA-256:	3086D914F6B23268F8A12CB1A05516CD5465C2577E1D1E449F1B45C8E5E8F83C
SHA-512:	99C2EF89029DE51A866DF932841684B7FC912DF21E10E2DD0D09E400203BBDC6CBA6319A31780B7BF8B286D2CEA8EA3FC7D084348BF2F002AB4F5A34218CCBF
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\tmp6909.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
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\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):	2.75
Encrypted:	false
SSDEEP:	3:mqw8:mP8
MD5:	E5C787E8E2247EDE48E0885667F86F80
SHA1:	0C6F3E57F673652469F9165CBAEBFB14C84B41FD
SHA-256:	CD9202646D461DC2C9DE4DDE02493C43A2E63108CEF57858A9E1A3FE7FFC24AF
SHA-512:	0501EC01C4967090A0167A32B85081A8395E46F894C010422112F175B6C44EB7C63E856F734DFAA06346BE49F192B57E880E0EE2EB7767BA368232EF3BE3D41C
Malicious:	**true**
Preview:	v..+..H

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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

C:\Users\user\AppData\Roaming\sFSDBgPwTyWm.exe	
Process:	C:\Users\user\Desktop\ERIG_0983763673-093876536783.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	749568
Entropy (8bit):	7.516863503906013
Encrypted:	false
SSDEEP:	12288:EGvWeGt5S4UqJetrrgdYWZTAd+7eu9ECUgC6pC6B:bWR5DlJKPgYBOeCJCw
MD5:	6A4599E499C357E47EBDF9021CF4613B
SHA1:	DA9FAB687CE9B7C1E06FD6A5AF0AD85ABE8D0E29
SHA-256:	02D517033BD02F92877D038127BBDA62DFA81CB34A6C0B98B3AB47C9EF614E8D
SHA-512:	ADA93A39D271DC5A23A0CFC6CA0FD4614E72B3193FF45B8B2666A7C70C0765D17222A55C51965F7D2D810CB16FC1A55C7D81E92E7382F8E953599F864D03D1F
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 32%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a..... .....@.. ..... .@.....X...W..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....n.....@..B.....H.....e..D>.....t...\.....(....*..*..z.(.....}.....(....o....}....*..0.....{.....3.....(....*.....0.....{.....,....f... .....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}.....{....ou...:q....(....+..(.....}.....(.....*..... .....n..}.....{.....,..{....oq...*

C:\Users\user\AppData\Roaming\sFSDBgPwTyWm.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\ERIG_0983763673-093876536783.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:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20211124\PowerShell_transcript.932923.K9jPxFRy.20211124205049.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):	5804
Entropy (8bit):	5.397254634548774
Encrypted:	false
SSDEEP:	96:BZ7/oN/qDo1ZaZe/oN/qDo1Z0fvlvHvjZ9/oN/qDo1ZruvXvXvnZ8:itffPPG
MD5:	7703BE8C1C9D8D16011F2BD3D4A9E5CF
SHA1:	9E97E55FD248D77C8ECDAA9C6409EBAB4F83F73C
SHA-256:	BA34D19AA42E6CF817575916B9CAAEF12C3F5DE5DDE9C22D325C52F25A274676
SHA-512:	7DAFD1EB2825CC9A69CDB0CFBA3EAFE1F58C3A9C128FE7576D5C4EE61518ADAE142832AA060DB81056E179B6B0A52803E65EE5ED2D2CD94F2EE4BE3BF960B5EE
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211124205050..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 932923 (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\sFSDBgPwTyWm.exe..Process ID: 488..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: 20211124205050..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\sFSDBgPwTyWm.exe..**********..Windows PowerShell transcript start..Start time: 20211124205408..Username: computer\user..RunAs User: DESKTOP-716T

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141

\Device\ConDrv	
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141
Malicious:	false
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):	7.516863503906013
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:	ERIG_0983763673-093876536783.exe
File size:	749568
MD5:	6a4599e499c357e47ebdf9021cf4613b
SHA1:	da9fab687ce9b7c1e06fd6a5af0ad85abe8d0e29
SHA256:	02d517033bd02f92877d038127bbda62dfa81cb34a6c0b9 8b3ab47c9ef614e8d
SHA512:	ada93a39d271dc5a23a0cfc6ca0fd4614e72b3193ff45b8 b2666a7c70c0765d17222a55c51965f7d2d810cb16fc1a5 5c7d81e92e7382f8e953599f864d03d1f7
SSDEEP:	12288:EGvWeGt5S4UqJetrrgdYWZTAd+7eu9ECUgC6p C6B:bWR5DlJKPgYBOeCJCw
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... .a..... .....@.. ..... @.....

File Icon

Icon Hash:	5cf8fcfeb6b6bc1c

Static PE Info

General

Entrypoint:	0x48a3b2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619DE7E7 [Wed Nov 24 07:21:11 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General

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	0x883b8	0x88400	False	0.924410478784	data	7.90674170611	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8c000	0x2e704	0x2e800	False	0.35587827621	data	5.63155022722	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbc000	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
11/24/21-20:51:04.148208	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61805	8.8.8.8	192.168.2.5
11/24/21-20:51:09.759206	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49557	8.8.8.8	192.168.2.5
11/24/21-20:51:14.943239	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61733	8.8.8.8	192.168.2.5
11/24/21-20:51:35.496614	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	65296	8.8.8.8	192.168.2.5
11/24/21-20:51:40.723678	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60151	8.8.8.8	192.168.2.5
11/24/21-20:52:11.885441	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64345	8.8.8.8	192.168.2.5
11/24/21-20:52:17.043248	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54791	8.8.8.8	192.168.2.5
11/24/21-20:52:37.493031	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50394	8.8.8.8	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2021 20:51:04.118192911 CET	192.168.2.5	8.8.8.8	0x5773	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2021 20:51:09.735202074 CET	192.168.2.5	8.8.8.8	0xd392	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:51:14.923880100 CET	192.168.2.5	8.8.8.8	0x70dd	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:51:35.473900080 CET	192.168.2.5	8.8.8.8	0x8d8f	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:51:40.701515913 CET	192.168.2.5	8.8.8.8	0x7c5	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:51:45.871690989 CET	192.168.2.5	8.8.8.8	0x1333	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:52:06.576910019 CET	192.168.2.5	8.8.8.8	0x7987	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:52:11.864196062 CET	192.168.2.5	8.8.8.8	0x4ee0	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:52:17.021116972 CET	192.168.2.5	8.8.8.8	0x4ee7	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:52:37.471781015 CET	192.168.2.5	8.8.8.8	0xbc62	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:52:42.590425014 CET	192.168.2.5	8.8.8.8	0xe6a4	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:52:47.715754986 CET	192.168.2.5	8.8.8.8	0x22ba	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2021 20:51:04.148207903 CET	8.8.8.8	192.168.2.5	0x5773	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:51:09.759206057 CET	8.8.8.8	192.168.2.5	0xd392	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:51:14.943238974 CET	8.8.8.8	192.168.2.5	0x70dd	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:51:35.496613979 CET	8.8.8.8	192.168.2.5	0x8d8f	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:51:40.723678112 CET	8.8.8.8	192.168.2.5	0x7c5	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:51:45.891486883 CET	8.8.8.8	192.168.2.5	0x1333	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:52:06.596586943 CET	8.8.8.8	192.168.2.5	0x7987	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:52:11.885441065 CET	8.8.8.8	192.168.2.5	0x4ee0	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:52:17.043247938 CET	8.8.8.8	192.168.2.5	0x4ee7	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:52:37.493031025 CET	8.8.8.8	192.168.2.5	0xbc62	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:52:42.611143112 CET	8.8.8.8	192.168.2.5	0xe6a4	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:52:47.735311031 CET	8.8.8.8	192.168.2.5	0x22ba	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ERIG_0983763673-093876536783.exe PID: 640 Parent PID: 5712

General

Start time:	20:50:36
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\ERIG_0983763673-093876536783.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ERIG_0983763673-093876536783.exe"
Imagebase:	0x530000
File size:	749568 bytes
MD5 hash:	6A4599E499C357E47EBDF9021CF4613B
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: 00000000.00000002.289525747.0000000002951000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.291241140.0000000003959000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.291241140.0000000003959000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.291241140.0000000003959000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 488 Parent PID: 640

General

Start time:	20:50:48
Start date:	24/11/2021
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\sFSDBgPwTyWm.exe
Imagebase:	0x1110000
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: 4392 Parent PID: 488

General

Start time:	20:50:48
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 340 Parent PID: 640

General

Start time:	20:50:48
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\sFSDBgPwTyWm" /XML "C:\Users\user\AppData\Local\Temp\tmp2122.tmp
Imagebase:	0x3b0000
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: 5988 Parent PID: 340

General

Start time:	20:50:49
Start date:	24/11/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff797770000
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: 3668 Parent PID: 640

General

Start time:	20:50:52
Start date:	24/11/2021
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:	0x540000
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: 0000000A.00000002.521737598.00000000051F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.521737598.00000000051F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.521737598.00000000051F0000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.514316239.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.514316239.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.514316239.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.521617557.00000000050B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.521617557.00000000050B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.285274859.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.285274859.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.285274859.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.285716690.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.285716690.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.285716690.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.284158874.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.284158874.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.284158874.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.520165197.0000000003859000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.520165197.0000000003859000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.284907194.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.284907194.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.284907194.0000000000402000.00000040.00000001.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: 6368 Parent PID: 3668

General

Start time:	20:50:59
Start date:	24/11/2021
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\tmp6138.tmp
Imagebase:	0x3b0000
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: 6376 Parent PID: 6368

General

Start time:	20:51:00
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6424 Parent PID: 3668

General

Start time:	20:51:01
Start date:	24/11/2021
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\tmp6909.tmp
Imagebase:	0x3b0000
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: RegSvcs.exe PID: 6432 Parent PID: 904

General

Start time:	20:51:01
Start date:	24/11/2021
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:	0x6f0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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 Written

File Read

Analysis Process: conhost.exe PID: 6464 Parent PID: 6432

General

Start time:	20:51:02
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: conhost.exe PID: 6516 Parent PID: 6424

General

Start time:	20:51:02
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6696 Parent PID: 904

General

Start time:	20:51:04
Start date:	24/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x390000
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: 6716 Parent PID: 6696

General

Start time:	20:51:04
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6868 Parent PID: 3472

General

Start time:	20:51:11
Start date:	24/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xc40000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6876 Parent PID: 6868

General

Start time:	20:51:11
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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