www.sisainfosec.com

SISA ProACT MDR Solution: Threat Group: Evilnum

Threat Severity: High
Published on: 18th Jan 2023

www.sisainfosec.com

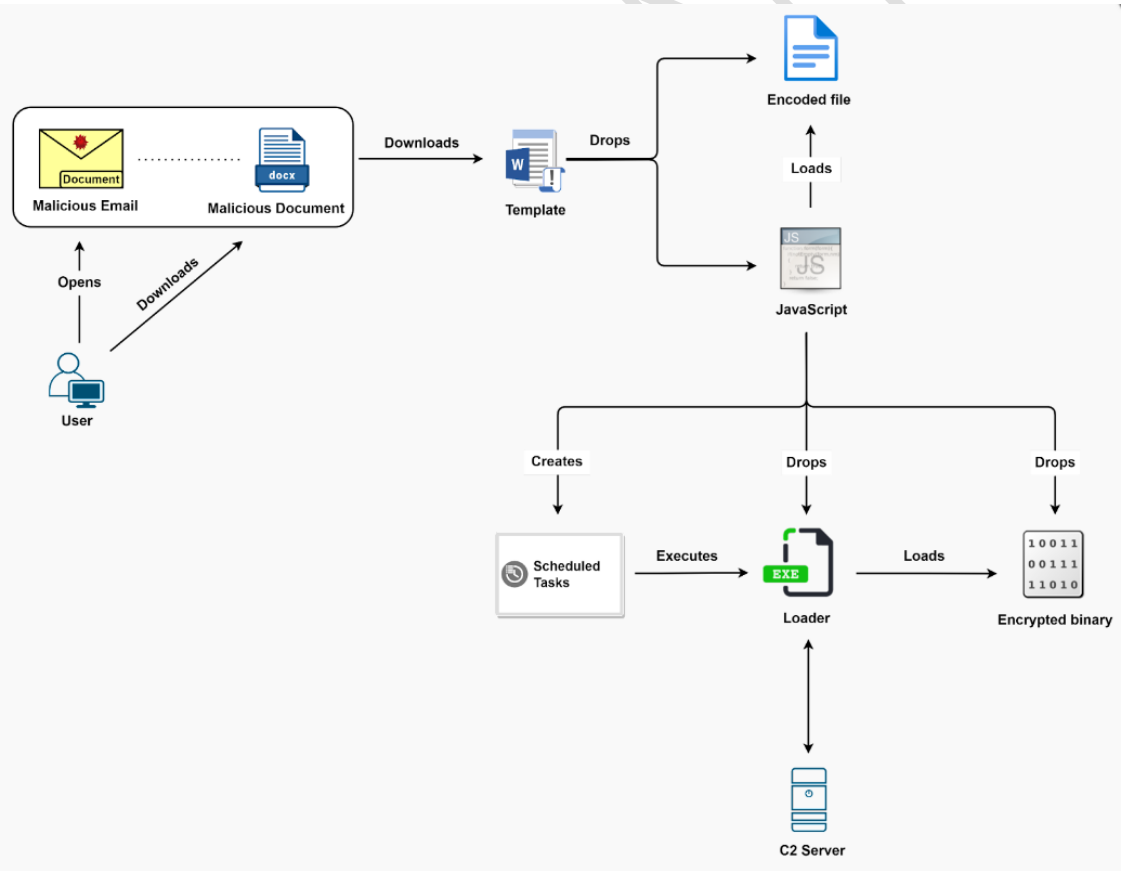
AN IN-DEPTH LOOK AT THE APT, EVILNUM

Overview Of The Group:

The APT TA4563 (also known as Evilnum) is a group that has launched a number of low volume but targeted attack campaigns targeting targets in the UK and Europe. The group initially only targeted the financial sector but has now switched gears and is targeting immigration organizations, according to security experts. The main goal of the group is to spy on its infected targets and steal information such as passwords, documents, browser cookies, email credentials and more.

TACTICS & TECHNIQUES 2022:

The group is using MS Office Word documents, leveraging document template injection – delivering malicious payloads to their target's machines.



SISA Information Security Pvt. Ltd.
No. 79, Road No. 9, KIADB IT PARK, Arebinnamangala Village, Jala Hobli, Bengaluru, Karnataka, India – 562149
India Tel: +91 80 4915 9700 | Email: service@sisainfosec.com

Initial Accces - SpearPhishing [T1192]:

Evilnum starts their attacks by sending a malicious Word document to their victim via spear phishing emails with rogue attachments. Once the victim opens the Word document, a message is displayed claiming that the document was created in a later version of Microsoft Word. This message explains how to enable editing in order to view the content.

Execution - User Execution - Malicious File [T1204.002]:

Once the victim opens the Word document, macro template from the attacker-hosted domain and displays the decoy content.

Defense Evasion - Hide Artifacts: VBA Stomping [T1564.007]:

The template contains the main malicious macro code. It makes use of VBA code stomping technique which is fairly uncommon in the wild.

It destroys the original source code and only a compiled version of the VBA macro code (also known as p-code) is stored in the document. This prevents static analysis tools such as olevba from extracting the decompiled VBA code.

Below are the key functionalities of the macro:

Two text boxes in the document file have their contents encrypted. The VBA macro code will decrypt these textboxes at runtime.

- Textbox 1 - **msform_ct.TextBox1.Text**. This will be decrypted and contents will be written to %appdata%\"**ThirdPartyNotices.txt**"
- Textbox 2 - **msform_ct.TextBox2.Text** - This will be decrypted and contents will be written to **"%appdata%\Redist.txt"**

Defense Evasion - Masquerading: Match Legitimate Name or Location [T1036.005]:

Copies the legitimate Windows binary Wscript.exe to a file with the name "**msdcat.exe**". Such file copy operations are done by malwares as a way to bypass endpoint security products.

The file - Redist.txt contains the obfuscated JavaScript which will be executed with the following command line:

msdcat.exe" /E:jscRipt "%appdata%\Redist.txt" dg ThirdPartyNotices.txt

"**dg**" is a hard coded command line parameter present inside the VBA macro code.

Defense Evasion - Obfuscated Files or Information[T1027]:

After the victim enables editing, an obfuscated JavaScript decrypts and deposits an encrypted binary and a malware loader before creating a scheduled task. To assist in avoiding detection, file system artefacts are created during execution, which are designed to imitate real Windows binary names.

There are two parameters passed to this JavaScript at the time of execution with following command line:

msdcat.exe" /E:jscRipt "C:\Users\user\AppData\Roaming\Redist.txt" dg ThirdPartyNotices.txt

- parameter 1: "**dg**". This string is later used in the string decryption function in JavaScript.
- parameter 2: The file "**ThirdPartyNotices.txt**" contains the encrypted code which will be decrypted and dropped by the JavaScript on the filesystem with binary name - SerenadeDACplApp.exe

Persistence - Scheduled tasks [T1053.005]:

The threat actor uses a scheduled task to maintain persistence. A scheduled task called "**UpdateModel Task**" will be generated during JavaScript execution and used to run the dropped loader binary with the necessary command-line arguments.

Task details:

<Exec>

<Command>

%appdata%\Microsoft\FontCache\CloudFonts\SerenadeDACplApp.exe

</Command>

<Arguments>

"OUM3NjBDNjAtRkNDQi00Q0FDLUE5NEMtNzY0RTc5MDNDN0Mw" "**devZUQVD.tmp**" "NzkzMTA3" "Ni4xLjc2MDE%3D" 0 "E4A6450B" "NTk1NDQxWwpaWhlhdmVbB1tf" Z

</Arguments>

<WorkingDirectory>

%appdata%\Microsoft\FontCache\CloudFonts

</WorkingDirectory>

</Exec>

Command and control - Data Encoding [T1132] :

The JavaScript drops two files:

- An executable file (SerenadeDACplApp.exe) – It turns out to be a loader
- A binary file (devZUQVD.tmp) – This is the file loaded during runtime by the loader

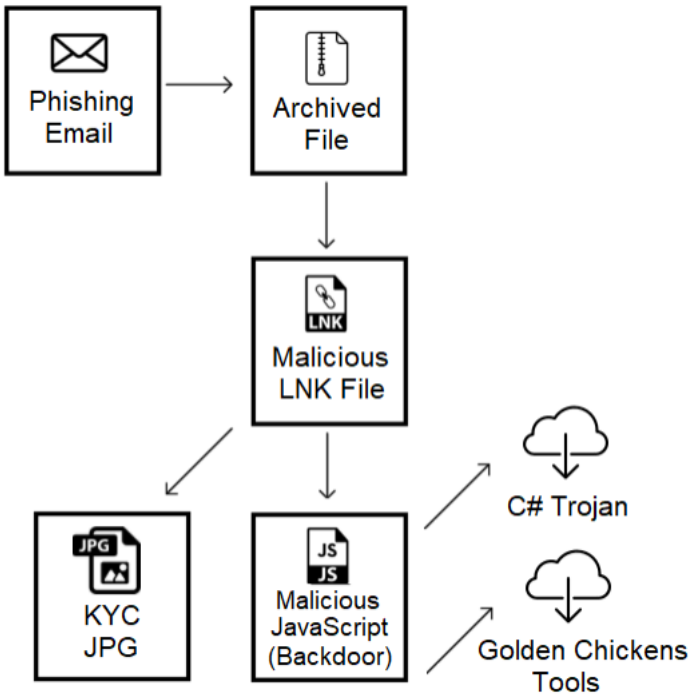
Evilnum's goal is to create a backdoor on infected systems, while machine screen grabs are taken and sent back to the threat actors via POST requests with the exfiltrated data now being in encrypted form.

The backdoor loaded on the infected systems are capable of performing the following tasks:

- Decrypting backdoor configurations
- Resolving API addresses from libraries retrieved from the configuration
- Conducting mutex check
- Creating data exfiltration string to send as a portion of the beacon request
- Encoding and encrypting the string with Base64
- Embedding this string inside the cookie header field

Selecting one of the C2 domains, the backdoor also selects a path string from the configuration and sends the beacon network request. The backdoor will then query the server for available content and downloaded it if the beacon is successful.

TACTICS & TECHNIQUES 2020:



Initial Accces – SpearPhishing [T1192]:

A malicious document is delivered via spear phishing email. Targets are approached with spearphishing emails that contain a link to a ZIP file hosted on Google Drive. That archive contains several LNK (aka shortcut) files that extract and execute a malicious JavaScript component, while displaying a decoy document.

Execution - User Execution: Malicious File[T1204.002]:

These shortcut files have “double extensions” to try to trick the user into opening them, thinking they are benign documents or pictures (in Windows, file extensions for known file types are hidden by default) Once decompress the first zip folders contained the following KYC files.

Filenames observed:

- Driv License front.jpg.lnk
- Driv License back.jpg.lnk
- Credit Card Front.jpg.lnk
- Credit Card Back.jpg.lnk
- Utility Bill.jpg.lnk.

Execution - Windows Management Instrumentation [T1047]:

The file **0.js** is the main agent deployed to the victim’s machine. It’s written in Phantom and this particular script was designed for Windows OS.

Once initiated the agent proceeds to enumerate the infected machine using Windows Management Instrumentation (WMI) to obtain the following information: Computername, Username, AntiVirus Products.

Defense Evasion - System Binary Proxy Execution: Rundll32 [T1218.011]:

For Defense evasion, evilnum is using python 2.7 interpreter to calls through rundll32.

Persistence - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547.001]

To maintain persistence evilnum group adds registry run keys:

- HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\.
- HKEY_CURRENT_USER\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows
- HKEY_CURRENT_USER\\Control Panel\\Cursors
- HKEY_CURRENT_USER\\Software\\Microsoft\\Internet Explorer\\Main
- HKEY_CURRENT_USER\\Software\\Microsoft\\Internet Explorer\\Recovery

- HKEY_CURRENT_USER\\Software\\Microsoft\\Internet Explorer\\PhishingFilter
- HKEY_CURRENT_USER\\Software\\Microsoft\\Internet Explorer\\BrowserEmulation
- HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\ Advanced
- HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings
- HKEY_CURRENT_USER\\Software\\Piriform\\CCleaner
- HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Zones\\3

Boot or Logon Autostart Execution: Shortcut Modification [T1547.009]:

To maintain persistence media.lnk file maps to media.js, which contains a copy of the core agent. and media.lnk is added to registry that is stored in a file named media.reg

C:\\Users\\admin\\AppData\\Roaming\\Microsoft\\Credentials\\MediaPlayer\\MediaManager\\Media.lnk

Command and control - Commonly Used Port [T0885]:

One of the first things the agent does is ping google to check for an internet connection. If the host machine is connected to the internet, the agent proceeds to kill any instances of Internet Explorer which have the command line parameter matching "-Embedding."

If the agent obtains the IP address it will send a GET request to check.php. If the IP address is indeed the correct C2, it returns a message padded with "jifhruhajsdfg444" on each side.

If agent found the correct IP address, POST method is sent on the host based enumeration information. Once received the C2 responded with the agent's unique identifier that will then get saved at **appDataPath + \\Microsoft\\Credentials\\MediaPlayer\\MediaManager\\id.txt.**

Exfiltration - Exfiltration Over Command and Control Channel [T1041]:

For exfiltration the evilnum group will perform following actions:

- Get commands from the C2
- Upload harvested cookies to the C2
- Download file from C2 then place in tmp and appData folders
- Upload file from infected host to C2

HTTP parameters observed during exfiltration:

“cookies.php?id=”+id

“DOWNLOAD_FILE.php”.toLowerCase(), “FILE-URL=”.toLowerCase() + fileURL

“send.php?id=”+id, filePath, “uploaded_file”

“upload.php?id=”+id, sctFile, “uploaded_file”

Software Used:

LaZagne:

LaZagne is a post-exploitation, open-source tool used to recover stored passwords on a system. It has modules for Windows, Linux, and OSX, but is mainly focused on Windows systems. LaZagne is publicly available on GitHub.

More_eggs:

More_eggs is a JScript backdoor used by Cobalt Group and FIN6. Its name was given based on the variable "More_eggs" being present in its code. There are at least two different versions of the backdoor being used, version 2.0 and version 4.4.

Hunting Queries:

Usecase Name	Detection Logic
Evilnum- Defense Evasion System Binary Proxy Execution: Rundll32	parent process: Rundll32.exe new process: python 2.7 interpretor
Evilnum - Persistence - Registry Run Keys	To monitor for modifications in the below registry path: "HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\. HKEY_CURRENT_USER\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows HKEY_CURRENT_USER\\Control Panel\\Cursors HKEY_CURRENT_USER\\Software\\Microsoft\\Internet Explorer\\Main HKEY_CURRENT_USER\\Software\\Microsoft\\Internet Explorer\\Recovery HKEY_CURRENT_USER\\Software\\Microsoft\\Internet Explorer\\PhishingFilter HKEY_CURRENT_USER\\Software\\Microsoft\\Internet Explorer\\BrowserEmulation HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Advanced HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings HKEY_CURRENT_USER\\Software\\Piriform\\CCleaner HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Zones\\3"

Scheduled tasks	Scheduled task with the names **UpdateModel Task** **PropertyDefinitionSync** **Schedule Defrag** **Task details:** **<Exec>** <Command> %appdata%\Microsoft\FontCache\CloudFonts\SerenadeDACplApp.exe </Command> <Arguments> "OUM3NjBDNjAtRkNDQi00Q0FDLUE5NEMtNzY0RTc5MDNDN0Mw" "devZUQVD.tmp" "NzkzMTA3" "Ni4xLjc2MDE%3D" 0 "E4A6450B" "NTk1NDQxWwpaWhlhdmVbB1tf" Z </Arguments> <WorkingDirectory> %appdata%\Microsoft\FontCache\CloudFonts </WorkingDirectory> </Exec>
Evilnum - Boot or Logon Autostart Execution: Shortcut Modification	FIM usecase: to monitor for *.lnk files being modified or if we found **Media.lnk** in windows environment
Evilnum - Hijack Execution Flow: Executable Installer File Permissions Weakness	Evilnum using **SerenadeDACplApp.exe** as a loader
Evilnum - Exfiltration Over Command and Control Channel	HTTP parameters observed during exfiltration: [Network based usecase]
	"cookies.php?id="+id
	"DOWNLOAD_FILE.php".toLowerCase(), "FILE-URL=".toLowerCase() + fileURL
	"send.php?id="+id, filePath, "uploaded_file"
	"upload.php?id="+id, sctFile, "uploaded_file"

MITRE Map:

Initial Access	Execution	Persistence	Defense Evasion	Credential Access	Discovery	Collection	Command and Control	Exfiltration
T1192: Spearphishing Link	T1191: CMSTP	T1060: Registry Run Keys / Startup Folder	T1038: DLL Search Order Hijacking	T1003: Credential Dumping	T1012: Query Registry	T1114: Email Collection	T1043: Commonly Used Port	T1022: Data Encrypted
	T1059: Command Line Interface	T1108: Redundant Access	T1088: Bypass User Access Control	T1503: Credentials from Web Browsers	T1063: Security Software Discovery	T1056: Input Capture	T1132: Data Encoding	T1048: Exfiltration Over Alternative Protocol
	T1129: Execution through Module Load	T1179: Hooking	T1116 Code Signing	T1056: Input Capture	T1518: Software Discovery	T1074: Data Staged	T1008: Fallback Channels	T1041: Exfiltration Over Command and Control Channel
	T1061: Graphical User Interface		T1090: Connection Proxy	T1539: Steal Web Session Cookie	T1082: System Information Discovery	T1005: Data from Local System	T1104: Multi-Stage Channels	
	T1086: PowerShell		T1140: Deobfuscate/ Decode Files or Information			T1113: Screen Capture	T1219: Remote Access Tools	
	T1117: Regsvr32		T1107: File Deletion				T1105: Remote File Copy	
	T1064: Scripting		T1143: Hidden Window				T1071: Standard Application Layer Protocol	
	T1218: Signed Binary Proxy Execution		T1036: Masquerading				T1032: Standard Cryptographic Protocol	
	T1204: User Execution		T1112: Modify Registry				T1102: Web Service	
	T1047: Windows Management Instrumentation		T1027: Obfuscated Files or Information					
	T1220: XSL Script Processing		T1497: Virtualization/ Sandbox Evasion					

Indicators of Compromise (IoCs):

2022:

Hashes:

- 0b4f0ead0482582f7a98362dbf18c219
- 4406d7271b00328218723b0a89fb953b
- 61776b209b01d62565e148585fda1954
- 6d329140fb53a3078666e17c249ce112
- db0866289dfded1174941880af94296f
- f0d3cff26b419aff4acfede637f6d3a2
- 79157a3117b8d64571f60fe62c19bf17
- 63090a9d67ce9534126cfa70716d735f
- f5f9ba063e3fee25e0a298c0e108e2d4
- ea71fcc615025214b2893610cfab19e9
- 51425c9bbb9ff872db45b2c1c3ca0854

Filename:

- proof of ownership.docx
- tradersway compliance.docx
- vantagemarkets documents.docx
- vantagefx compliance.docx
- calliber docs (2).docx
- complaince tfglobaltrading.docx
- complaint europatradecapital.com.docx
- fxtm_compliance.docx
- livetraderfx.docx
- SerenadeDACplApp.exe
- devZUQVD.tmp

C2 Domains:

- travinfor[.]com
- webinfors[.]com
- khnga[.]com
- netwebsoc[.]com
- infcloudnet[.]com
- bgamifieder[.]com
- bunflun[.]com

- refinance-ltd[.]com
- book-advp[.]com
- mailservice-ns[.]com
- advertbart[.]com
- inetp-service[.]com
- yomangaw[.]com
- covdd[.]org
- visitaustriaislands[.]com
- traveladvnow[.]com
- tripadvit[.]com
- moreofestonia[.]com
- moretraveladv[.]com
- estoniaforall[.]com
- bookingitnow[.]org
- travelbooknow[.]org
- bookaustriavisit[.]com
- windnetap[.]com
- roblexmeet[.]com
- netrcmapi[.]com
- meetomoves[.]com
- bingapianalytics[.]com
- azuredcloud[.]com
- appdllsvc[.]com
- udporm[.]com
- pcamanalytics[.]com
- nortonalytics[.]com
- deltacldll[.]com
- mscloudin[.]com
- msdllopt[.]com

URI paths:

- /actions/async.php
- /admin/settings.php
- /admin/user/controller.php
- /admin/loginauth.php
- /administrator/index.php
- /cms/admin/login.php
- /backend/login/ajax_index.php
- /wp-admin/media-new.php

- /get.php
- /auth/login

Scheduled Task Names:

- UpdateModel Task
- PropertyDefinitionSync
- Schedule Defrag

2020:

LNK Hashes:

- 3F71525D531690A6B75CABE113B7221504108B44
- 212FA26C100BF56120C7F2F2D569819E3DABE556
- 46AA42970418010DBD5EFD571BC7056BECBCB2DC
- 7379FD28E0816555D081196F0CA3EB44C8E62911
- 27A75DE6BC73106BF192A38A45740DEE47A1D9D3
- EF2B07B2C6B5B1F25C18FA7546EDC1EEDB3CC055
- EDD1CA115D600E982623A3A2342810855B0DE543
- F113CA2DA0F1E4ECC92000E419DAD2B259A9F839
- DB50FC4EA4F6C13FDBCD28EBE2F1CC44A74A83BF
- EE050A767EAA5227ED40D7A77B7746AEA0554AE5
- 97820A79FD43F664F553C46DCA682BCE135B2CC3
- C7575DCCC6D1A228393E9AC0840A4C10BB4C1FB2
- AA7585DF29E8F1D058FF267B94E8E7084DE4C7C1
- F35961EB47EC4FF1B79300B8115FECD2313C6DFC
- A2DBD75DD079594D36509F5EF84A22F869DF68CF
- EB046DEB4BDF36461BB828967CE15D5123637CEE
- 228FE78F80565BC7C02DA137505196E9EDBA767C
- 45BB89DF5A612F53B119A6111E6AC6DE60E071D5
- AF0A98F04697F836878D76DC402668C42FF1E2CA
- A5F300C880842328B4D0D9C83F8314180520BD5A
- 29EF1FE11A063FBE218DE9BF91A4C2F871592F26
- 513B161299D99F4BE1DFFBB171B7C4040FF83DE7
- BD8D4C93234B01A155128E3FABB61AE1CC81B5F1
- F15C8F755B32A70471639B050B93FDBFB5A4D403
- 438B0C180A7CFF5AEDBFC9FF83668A0DEC0174A4
- 910382E02738661583813D212904742390C5008A
- B6767E63CC8483444540D701F00705B65055C69B

- A5C91E06881E19079B7E8496C6F229A790E8C1EE
- 3AAED43B2B8E36DA80046AF51C33A3ADFB49BD1F
- 854A17550FF473FB4C5AB03FD39ABFD1B3953E9C
- E29011596AFE794BA673906F8F8F35AB71F397ED
- C2739DDC99027AB515C75C352FB532524A082066
- 23DA05A5FAD175F2C035A8C4601E09E30C98B202
- DBB54C9B29AEA16EFA8E3AE663428E6F2BDE4919
- 55D1AEA9BBB49A96A383AA5B604870DF06E7DE09
- 34A72738DC025353EBDC3D5C99B19DAE4D9DE2E6
- A21522A20DB85C24CDC0CF46818E576F19CB0927
- 5A2227A37676564969F4392790FE9E3B995D7782
- 36345044D5E88CC8C002863E3F1F48FDEC8FF4D9
- DE0FF4B04F05482ADE4CF3BA765A453818F6858E
- EE59BC476BB3A7DB1190BEB791A5AA8550FC9541
- 4CDD87F5B9AB8C2AFCD76E4B8127B0CB6E880CF1
- FBCB367EC7DD64B253482B4475CCDE6FF6B10AB0
- F0DB18E0FD8C376A7EF7316C413240857F37CCAA
- 650DEB9BAFF4B7564146222DEB555E77D5CBBE36

Filenames:

- %APPDATA%\Microsoft\Credentials\MediaPlayer\MediaManager\media.js

C&C servers:

- 139.28.39[.]165
- 139.28.37[.]63
- 185.62.190[.]89

URLs parsed for C&C:

- https://gitlab[.]com/jhondeer123/test/raw/master/README.md
- https://gitlab[.]com/bliblobla123/testingtesting/-/raw/master/README.md
- https://www.digitalpoint[.]com/members/johndeer123.923670
- https://www.digitalpoint[.]com/members/bliblobla.943007/
- https://www.reddit[.]com/user/deltadelta2222/comments/gepb1w/hey/
- https://gitlab[.]com/amigo_159753/gold/-/raw/master/README.md
- https://gitlab[.]com/galagroba/myoneandonly-haled/raw/master/README.md
- https://gitlab[.]com/deadpooool/awesome-news/raw/master/README.md

C# component:

MSI installer:

- A6ECD3A818D463155C31977000E6FDE3EB8A2352 - SecuUpdate2021.msi

File copier:

- D6341CD464847C9C2716030111261D5B84A43B2A – ypoc.exe
- AB0C6268C61D9F36996BA7653B3A3E1EDE2AEE51 – ypoc.exe

Loader:

- 4187F714076853B1FFA38A84835DB2623460F537 – Policy.exe
- 04F7FEDF8FDDF8EB5B592A57F67F72B1075C7CC1 – ServiceHud.exe
- B6B9C5EFFDD14E2920183B313C56E5068C57A709 – ServiceHud.exe

Agent:

- B3C8C1C80824278661FBB26B17040B87180D1D34 – system.memmory.dll
- C23F0551C2F7937EA4AD4B970B01CBD4D104EFFE – Policy.exe
- 6E7493BD1EF727FBC6EECD3AE5EC31BB8C1E897D – Policy.exe

Other files:

- %LOCALAPPDATA%\microsoft\windows\explorer\iconcache_2048.db (stores C&C address)

Paths:

- %LOCALAPPDATA%\Microsoft\Mediia
- %LOCALAPPDATA%\Microsoft\policy
- %LOCALAPPDATA%\Microsoft\Windows\Explorer
- %LOCALAPPDATA%\Microsoft\Windows\Explore
- C:\Users\<user>\AppData\Localpolicy

Windows registry:

- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
- HKCU\Control Panel\Cursors\AppStarting = "%SystemRoot%\cursors\aero_arrow.cur"

C&C servers:

- 176.107.176[.]237
- 185.20.186[.]75
- http://176.107.176[.]237/secupdate202222.msi
- http://176.107.176[.]237/67364732647836478231.msi

- http://45.9.239[.]50/secupdate2021.msi

HTTP requests:

- /Validate/getid?action=getSerial&computer_name=<name>&username=<user>&version=4.0&cli=***
- /Validate/getid?action=up&uid=<id>&antivirus=<av_name>
- /Validate/zaqxswcde123456789?action=sendScreenshot&uid=<id>&data=<b64imgdata>
- /Validate/getcommand?action=getCommand&uid=<id>
- /Validate/zaqxswcde1224567891?action=error&uid=<id>&data=<errormsg>

PDB paths:

- C:\work\Marvel\vs\Marvel.LLDTenga\obj\Release\System.Memmory.pdb
- C:\work\Marvel\vs\Marvel.Agent\obj\Release\Policy.pdb
- C:\work\Marvel\vs\MarvelCopyForMSI\obj\Release\ypoc.pdb
- C:\work\Marvel\vs\MarvelCopyForMSI\obj\Release\znn.pdb
- C:\git\VS\out\binaries\x86ret\bin\i386\DPCA.pdb

More_eggs:

Files:

- 976DA2E8BDD698D974D38D01593897CA64946D92 – load.ocx
- 1303EB76FE1F978C6BFB6EA28329E7CDA61126AF – loadsigned.ocx
- 3200E9832CD61828DDF4E82155D66B63D2E6A54E – 32753.ocx
- AF68B3E310BF8446E4CD10EFCF4776196131E785 – 13681.ocx
- D675D3AC1C05DC7AC73674C47FA141D75F537DD3 – 13435.ocx

Paths:

- %APPDATA%\Microsoft

C&C servers:

- https://api.win640[.]com/json
- https://api.adobe.com[.]kz/v1
- https://api.adobe.com[.]kz/update/check
- https://api.adobe.com[.]kz/release/init
- Code-signing certificate SHA-1 thumbprint
- 90C22DB300F44EC79BEAB4662BB77ED1E81843BC

TerraPreter:

Files:

- 1C1D8D0AF6AA728589C5D0D0F46C01B129C75BA0 – msf_64.ocx
- A7F1C2BE87B5EE4392757948FB7C895CAD95520B – msfsigned.ocx
- 7D9037377DC2A2E3FC1985983942D1E9F986AA42 – msfsignednofront.ocx

C&C Servers:

- https://cdn.lvsys[.]com/
- https://d2nz6secq3489l.cloudfront[.]net/
- https://faxing-mon[.]best/
- Code-signing certificate SHA-1 thumbprint
- 90C22DB300F44EC79BEAB4662BB77ED1E81843BC

Other files:

- 9677FCBF6F59BE2A5AB61BE5E6DF91599FB67602 – abc.bat (executes Golden Chickens components)
- 476BB78BCF194523C385E2CEE364D6D097464ECA – hi.txt (remote scriptlet)

TerraStealer:

Files:

- 7C98E37CBA9B9C757E77892F02E1783A80AC450F
- 73C5792AA05C122903C1AEA1E1F965D223C073D8
- C341D18A79057B032DC0A03F4524606205057F62
- E8A95EC590E5786B780D3D6986282273895B4C8A

C&C servers:

- http://json.ama-prime-client[.]com/

TerraTV:

Files:

- E0957B2421A6EF3237A33A37DA8B52A9F29863D6 – 15159.ocx
- 1F287AA922911F72F68B4B0C8645B4C909EB07B9 – ACTIVEDS.dll

Path:

- C:\Users\Public\Public Documents\57494E2D3850535046373333503532\

Other tools and scripts:

Files:

- 401BC3740385A73EF0D3AD93DFCE03C82770072A – rev.py
- 27054C073C10F61452101646DA5AC9AA21DC90DB – runner.py
- C4817D8C8E0B147ED5220229987FC84A43DA16A5 – PythonProxy.py
- 480C6F0C3998009C017051A8D6FFE199BC2A18DF – socks.py
- C17CF1E8B4806A931F5FA0D73AD4BB521C43849A – log.py
- 47A7CD789C90735325EBD2C495A983A9C7E56E6F – l.py
- 2B8522ED748178037BD13FC4D3F564CE8B7BA6D6 – Win.ps1

Servers:

- 185.61.137[.]141
- 185.62.189[.]210

Ending Notes:

Evilnum is an active threat and hence, it is recommended to use the IOCs provided in the report. While we still don't know the origins of this threat actor, its victimology points to a state-backed interest in cyberespionage campaigns.

Reference:

- https://www.prevailion.com/phantom-in-the-command-shell-2/https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/https://attack.mitre.org/
- https://www.avertium.com/resources/threat-reports/an-in-depth-look-at-the-apt-evilnum
- https://github.com/eset/malware-ioc/tree/master/evilnum
- https://www.zscaler.com/blogs/security-research/return-evilnum-apt-updated-ttps-and-new-targets
- https://www.bleepingcomputer.com/news/security/malware-loader-goes-through-heavens-gate-to-avoid-detection/

MITRE ATT&CK techniques:

ID	Name	Description
T1192	Spearphishing Link	Emails contain a link to download a compressed file from an external server.
T1191	CMSTP	cmstp.exe is used to execute a remotely hosted scriptlet that drops a malicious ActiveX file.
T1059	Command-Line Interface	cmd.exe is used to execute commands and scripts.
T1129	Execution through Module Load	The malicious payload for the version 4.0 C# component is loaded from a DLL. TerraTV loads a malicious DLL to enable silent use of TeamViewer.
T1061	Graphical User Interface	TerraTV malware allows remote control using TeamViewer.
T1086	PowerShell	Evilnum group executes LaZagne and other PowerShell scripts after their JS component has compromised a target.
T1117	Regsvr32	Evilnum group uses regsvr32.exe to execute their Golden Chickens tools.
T1064	Scripting	Initial compromise and post-compromise use several JavaScript, Python and PowerShell scripts.
T1218	Signed Binary Proxy Execution	msiexec.exe is used to install the malicious C# component.
T1204	User Execution	Victims are lured to open LNK files that will install a malicious JS component.
T1047	Windows Management Instrumentation	WMI is used by the JS component to obtain information such as which antivirus product is installed.
T1220	XSL Script Processing	More_eggs malware uses msxsl.exe to invoke JS code from an XSL file.
T1060	Registry Run Keys / Startup Folder	Registry Run keys are created in order to persist by the JS and C# components, as well as More_eggs
T1108	Redundant Access	Evilnum components are independent and provide redundancy in case one of them is detected and removed.
T1179	Hooking	TerraTV malware hooks several API calls in TeamViewer.
T1038	DLL Search Order Hijacking	TerraTV malware has TeamViewer load a malicious DLL placed in the TeamViewer directory, instead of the original Windows DLL located in a system folder.
T1088	Bypass User Access Control	A PowerShell script is used to bypass UAC.
T1116	Code Signing	Some of the Golden Chickens components are malicious signed executables. Also, Evilnum group uses legitimate (signed) applications such as cmstp.exe or msxsl.exe as a defense evasion mechanism.
T1090	Connection Proxy	Connection to a proxy server is set up with post-compromise scripts.
T1140	Deobfuscate/Decode Files or Information	Encryption, encoding and obfuscation are used in many Evilnum malware components.
T1107	File Deletion	Both JS and C# components delete temporary files and folders created during the initial compromise.
T1143	Hidden Window	TerraTV runs TeamViewer with its window and tray icon hidden.
T1036	Masquerading	The C# component has its payload in system.memmory.dll , which masquerades as a benign .NET Framework DLL.
T1112	Modify Registry	Evilnum modifies the registry for different purposes, mainly to persist in a compromised system (for example, by using a registry's Run key).
T1027	Obfuscated Files or Information	Encryption, encoding and obfuscation is used in many Evilnum malware components.

T1497	Virtualization/Sandbox Evasion	The Golden Chickens components implement several integrity checks and evasion techniques.
T1003	Credential Dumping	Scripts and tools such as LaZagne are used to retrieve stored credentials.
T1503	Credentials from Web Browsers	The C# component retrieves stored passwords from Chrome.
T1056	Input Capture	Custom Python scripts have been used for keylogging.
T1539	Steal Web Session Cookie	Evilnum malware steals cookies from Chrome.
T1012	Query Registry	More_eggs queries the registry to know if the user has admin privileges.
T1063	Security Software Discovery	Both the JS and C# components search for installed antivirus software.
T1518	Software Discovery	TerraStealer malware looks for specific applications.
T1082	System Information Discovery	Information about the system is sent to the C&C servers.
T1074	Data Staged	Data is stored in a temporary location before it is sent to the C&C.
T1005	Data from Local System	The JS component (v2.1) has code to exfiltrate Excel files from the local system.
T1114	Email Collection	TerraStealer malware targets email applications.
T1056	Input Capture	Keystrokes are logged with a Python script.
T1113	Screen Capture	Screenshots are taken by some Evilnum malware components.
T1043	Commonly Used Port	HTTP and HTTPS are used for C&C communication.
T1132	Data Encoding	Some of the data sent to the C&C is base64-encoded.
T1008	Fallback Channels	The JS and C# components can obtain a new C&C by parsing third-party webpages if the original C&C is down.
T1104	Multi-Stage Channels	Evilnum malware uses independent C&C servers for its various components.
T1219	Remote Access Tools	TerraTV malware uses TeamViewer to give control of the compromised computer to the attackers.
T1105	Remote File Copy	Files are uploaded to/downloaded from a C&C server.
T1071	Standard Application Layer Protocol	HTTP and HTTPS are used for C&C.
T1032	Standard Cryptographic Protocol	More_eggs malware uses RC4 to encrypt data to be sent to the C&C.
T1102	Web Service	GitHub, GitLab, Reddit and other websites are used to store C&C server information.
T1022	Data Encrypted	Some Evilnum components encrypt data before sending it to the C&C.
T1048	Exfiltration Over Alternative Protocol	Scripts are manually deployed by the malware operators to send data to an FTP server.
T1041	Exfiltration Over Command and Control Channel	Data is exfiltrated over the same channel used for C&C.