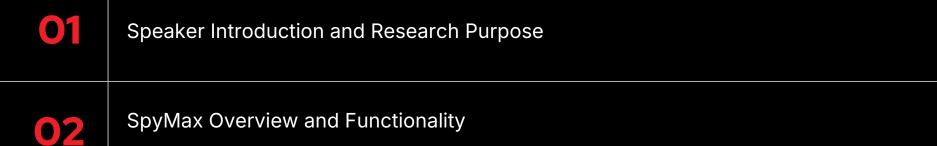


SpyMax - Mobile Malware On The Frontlines of Syria's Civil War



# Agenda



Uncovering Samples & Infrastructure

Attribution, Impact, and Conclusion

### Research Focus

/Reportage Syria | 14 MIN READ

# How a Spyware App Compromised Assad's Army

An investigation reveals how a cyberattack exploited soldiers' vulnerabilities and may have changed the course of the Syrian conflict

Kamal Shahin

Kamal Shahin is a Syrian journalist who worked for decades covering political and

May 26, 2025





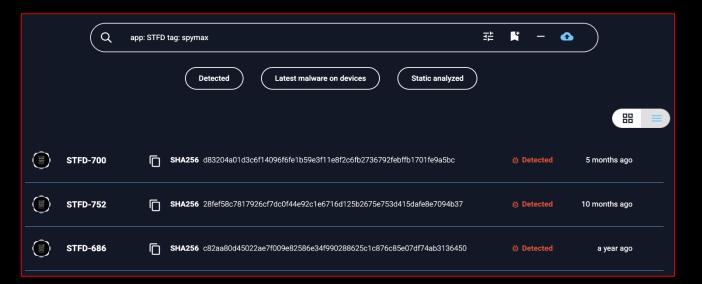
# Research Methodology

n the early summer of 2024, months before the opposition launched
Operation Deterrence of Aggression, a mobile application began circulating among a group of Syrian army officers. It carried an innocuous name: STFD-686, a string of letters standing for Syria Trust for Development.

A review of the domains associated with Syr1.store revealed six linked domains, one of which was registered anonymously. Through SpyMax, whoever was behind the app extracted a devastating range of data from the officers' phones, including their ranks and identities, whether they were responsible for sensitive posts and their geographical locations (possibly in real time). They would have access to troop concentrations, phone conversations, text messages, photos and maps on officers' devices, and be able to monitor military facilities remotely.











# SpyMax Permissions

- READ\_CONTACTS, CALL\_LOG, SMS
- ACCESS\_COARSE\_LOCATION
- RECORD\_AUDIO
- CAMERA
- READ\_EXTERNAL\_STORAGE
- INTERNET
- RECEIVE\_BOOT\_COMPLETED
- SYSTEM\_ALERT\_WINDOW







### Domain: syr1[.]store September 2023







### Domain: syr1[.]store October 2023







### Domain: syr1[.]online January 2024







### Domain: syr1[.]online October 2024







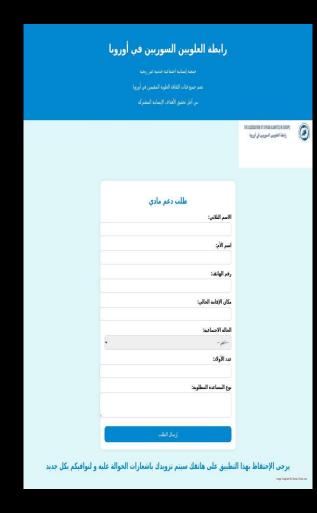
### Domain: syr1[.]online December 2024 (Post War)





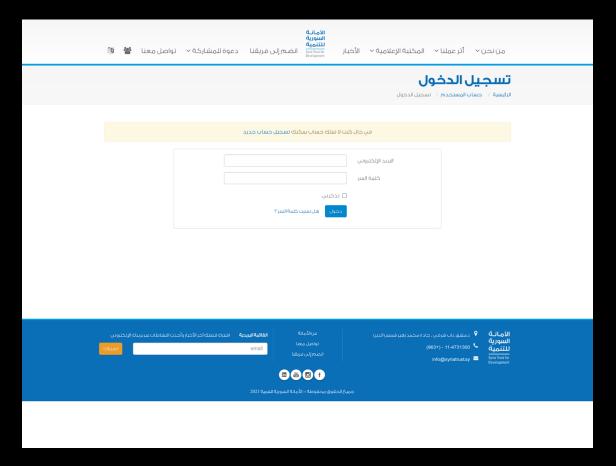


### Domain: syr1[.]online July 2025 (Post War)





# Syriatrust[.]sy







# About SpyMax

#### What it is:

- Derived from SpyNote malware
- Features a highly obfuscated code base

#### How it spreads and communicates:

- Distributed via Telegram channels and phishing sites
- Uses hardcoded servers for command and control

#### How it operates:

- Prompts users to grant multiple app permissions
- Harvests sensitive data through a webview interface once permissions are granted
- Exfiltrated data via direct socket communication





# Spy Family History

#### Origins:

- SpyNote first released in 2016
- SpyNote previously used by Syria-nexus adversary DEADEYE HAWK

#### **Evolution of variants:**

- 2019-2020: **SpyMax** appears in criminal forums
- Additional variants such as CraxsRAT and EagleSpy emerge in 2025

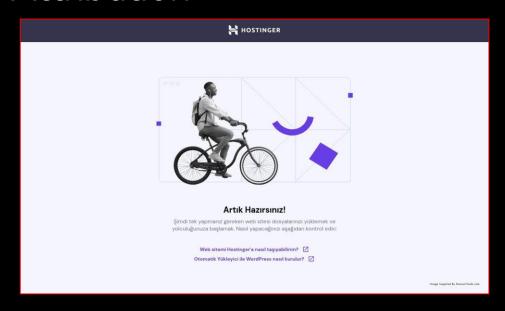
#### **Current landscape:**

- CraxsRAT and EagleSpy are the most active variants across current cyber criminal forums
- Detection rules frequently cross-match variants due to shared code base and functionality





# Attribution



#### **Certificate Subject**

Distinguished Name C:rb, CN:Benim ismim, L:Antan, O:Benim Firmam, ST:SANANE, OU:Benim Firmam, email:sahte@gmail.com

Email sahte@gmail.com

Common Name Benim ismim
Organization Benim Firmam
Organizational Unit Benim Firmam

Country Code rb

State SANANE Locality Antan





# Possible Impacts

- Real-time mapping of deployments
- Location of critical military assets (weapons, comms, facilities)
- Exposed command structure
- Troop movements
- Estimated thousands of affected personnel (according to NewsLine)





# Intelligence Gaps

- Attribution is currently unclear
- The way in which SpyMax first began circulating among Syrian Army Officers is unknown
- Whether the campaign extends past the samples and infrastructure identified is unknown
- How was the information uploaded to the harvesting webview pages used?





### This was not:

- A carefully crafted exploit
- Expensive, stealthy, no-click spyware
- A Zero day

### This was:

 Commodity malware that anyone can buy



## loCs

#### C2 Domains:

- west2.shop
- WebView Domains:
  - syr1[.]store
  - syr1[.]online

#### SHA256 Hashes

- d83204a01d3c6f14096f6fe1b59e3f11e8f2c6fb2736792febffb1701fe9a5bc
- 28fef58c7817926cf7dc0f44e92c1e6716d125b2675e753d415dafe8e7094b3
   7
- c82aa80d45022ae7f009e82586e34f990288625c1c876c85e07df74ab3136
   450
- 60ca970a774c5ff1ada52170857989721158064b932e999714bff7f4bd8b57
   0c
- db041da97c1f30a6fc7765994b556839f8550774af1662ae0ab105e2fc3244
   87
- 2c1aa8139f55b6566ff8fcb88efccd169040b8cff932683e8d4e1401f9c64644





# Thank you!