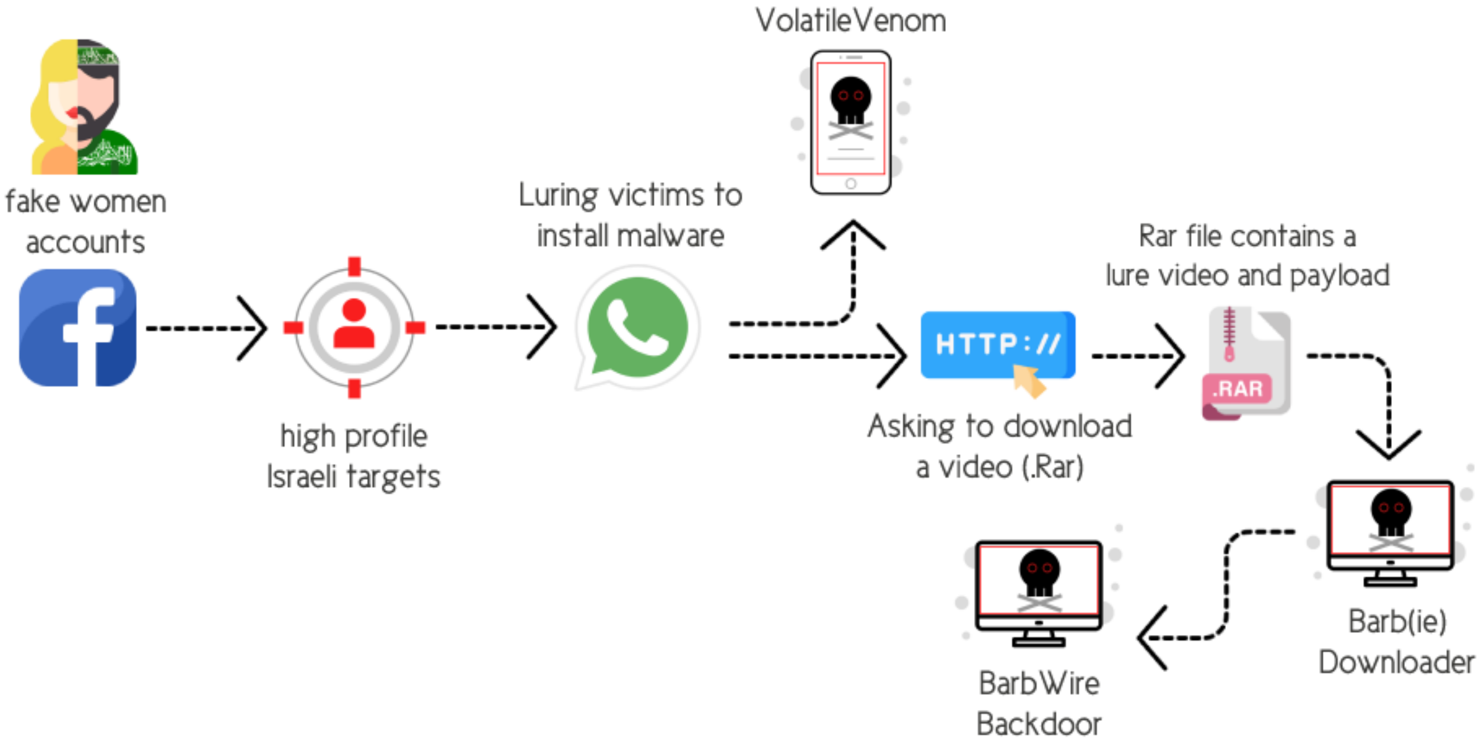
Severity

High

Analysis Summary

APT-C-23 (aka AridViper) is an Arabic-speaking Advanced Persistent Threat group working for Hamas. The threat group has been previously known to target Middle-Eastern countries but has been recently observed targeting Israeli officials and individuals. Their espionage campaign aims to steal credentials and sensitive information from the victim's PC and mobile devices. Their most active targets are Israeli individuals working for the military, emergency services, and any law enforcement agencies. Their primary infection method is social engineering, through which they deliver trojanized messages via facebook or other social media applications. The group has been using an upgraded malware called "Barb(ie) Downloader" and "BarbWire Backdoor" and an android implant named VolatileVenom.


fake women accounts
high profile Israeli targets
Luring victims to install malware
VolatileVenom
HTTP://
Asking to download a video (.Rar)
Rar file contains a lure video and payload
.RAR
Barb(ie) Downloader
BarbWire Backdoor

Impact

- Information Theft and Espionage

Indicators of Compromise

Domain Name

- marina-samuel[.]com

MD5

- b1933dcd56ac861d8e49407d94b2317a

SHA-256

- 7ecf4ac13b237925e9903ae7a1c287c3269315dba8e67c8171cb9dd6f148628e

SHA-1

- 9651e3a3a134385eaadbe5d769c6f9f5602c172a

Remediation

- Block all threat indicators at your respective controls.
- Always be suspicious about emails sent by unknown senders.

- Never click on links/attachments sent by unknown senders.
- Search for IOCs in your environment