Desert Falcons Ransomware

Date: 17th June 2024 | Severity: Medium

Summary

- The Desert Falcons APT group (AKA Arid Viper, APT-C-23, Two-tailed Scorpion) was formed in early 2011 and started operating in 2013. It is considered to be the first Arabic-speaking APT group. The group comprises dozens of attackers, some who are known by name, that operate from various Arab-speaking locations, such as the Palestinian territories, Egypt, and Turkey.
- Desert Falcons targets mostly entities in the Middle East, specifically Israel, but has also been observed operating against other countries, such as the United States and South Korea.
- The group is primarily interested in obtaining sensitive intelligence information and its victims are companies and individuals from various sectors, such as government, military, education, finance, energy, media, trade and commerce, and religion. It is unclear whether Desert Falcons is state-sponsored.
- Desert Falcons' first major operation was in 2015, dubbed "Operation Arid Viper," in which spear phishing email messages were sent to one Kuwaiti organization and to five Israeli-based organizations in the government, transport, infrastructure, military, and academic sectors.

Attack Vectors

- Each message contained a RAR archive file that automatically extracted a SCR file. Once executed, the SCR file dropped two other files, one containing a malicious payload and the other containing pornographic content, possibly in order to distract the victim.
- The dropped malware communicated with the command and control (C2) server and was used to steal documents from the infected systems.
- Cybersecurity researchers reported that the group used Windows malware dubbed Kasperagent and Micropsia, in attacks aimed mainly at targets in the United States, Israel, the Palestinian Territories, and Egypt. The malware was spread through spear phishing email messages and social media instant messages that contain malicious links.
- The group also set up various fake news websites with lures leading to a malware download. The malware can steal web browser passwords, take screenshots, record keystrokes, exfiltrate files, and more. In addition, the threat actors used malicious apps, loaded with SecureUpdate and Vamp Android malware. Those apps were used to steal user credentials, record calls, and steal messages and documents stored on Android devices.

- Researchers discovered that the group started using a new variant of the MICROPSIA malware, dubbed PyMICROPSIA, as it was built with Python. The improved malware was able to upload and delete files, record keystrokes, collect system information, exfiltrate files, and download and execute additional malicious payloads.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 16c8725362d1ebc8443c97c5ab79a1b6428ff87d • e71f1484b1e3acb4c8e8525ba1f5f8822ab7238b • 0dc47d791ad9ecbab3aedd914cb22a81 • e58267f9ff31408d0bb1b84948e1fd3c02231cfd0628797cc2a6045354e0b065 • 46f5df76f723e67a42ef49cce8d84a0f9af869b170f730df01d29138b36d3f24 • d2ccf6fa361ceaf8cebada53bb1f9458b016ad85b74a7dc1bf4ba18774d92645 • 4a56b4968f2559459d98ab35a01a6b7b946d6ab8 • 6279030f7e5eaeacd28232de35382c38614fefc90ef753f2492300c1150e54f0 • 1dcf5da15cceb97198d10bcf44d55e6a • 46b0f586a646e800ab63d1404a08864fb09aca73a13fd22542a9fce038643219 • 5f71a8a50964dae688404ce8b3fbd83d6e36e5cd • e850650e6982469529768988dfabadfdaa53b25abe1e0c0f0b3894b31a83b061 • 75a708bf42ac01d857ecb3bff18c633e334329d4b89ae4201a989f564a2410b6 • 93a21428286602cfe02380a33411cb9d25004f627c685b4363e9ffb3baa5f201 • c9ffb81a97a9458f1fc96f35cd187b1d7311479e77d031586abdc3d426da0859 • 8cf8d06d2935153d3c8d570ecd5990432bb4933ca89845bc2cd763b40ba7edb4 • c999ace5325b7735255d9ee2dd782179ae21a673 • accf87a349b0cfe6403e827089d7a97a8a9bf94dc4535d9ce2e54ecf9bc699fa
URL	• http://firas2019[.]ddns[.]net • http://agentra3[.]dvrcam[.]info • https://linda-gaytan[.]website • https://elizabeth-steiner[.]tech/download/HwIFlqt • https://sites[.]google[.]com/view/janx/about
IP ADDRESS	• 213[.]244.123.150 • 162[.]0.224.52 • 199[.]192.25.241 • 68[.]65.121.120 • 23[.][1]06.223.54 • 23[.]106.223.135 • 198[.]187.31.161 • 64[.]44.102.198 • 173[.]236.89.19 • 66[.]29.141.173

Recommendation

- Block all threat indicators at your respective controls.
- Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Never trust or open links and attachments received from unknown sources/senders.
- Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://dashboard[.]ti[.]insight[.]rapid7[.]com/#/tip/cyber-term/57b9738c0e6731530078d333
- https://www[.]jpost[.]com/middle-east/desert-falcons-cyber-operatives-plunder-middle-easts-cyber-treasures-391694