Analysis of APT35 Infrastructure Reveals Interest in Egyptian Shipping Companies

securityscorecard.com/blog/analysis-of-apt35-infrastructure-reveals-interest-in-egyptian-shipping-companies

1. Blog

By Ryan Slaney and Robert Ames, Staff Threat Researchers and Alex Heid, Chief Research Officer

Posted on August 31st, 2022

Executive Summary

- SecurityScorecard has identified domains resolving to Iran-linked Advanced Persistent Threat (APT) infrastructure, likely to be used to support phishing campaigns against Egypt-based shipping and marine services companies.
- In at least three instances, Iran-linked APT actors may have gained unauthorized access to the DNS configuration of legitimate domains to create rogue subdomains.
- CNAME records were used to forward requests to unauthorized third-party mail servers that were under the control of malicious actors.
- SecurityScorecard assesses with high confidence that these subdomains were created to support Iran-linked APT phishing campaigns.

Background

On August 23, Google's Threat Analysis Group (TAG) released a blog about a new data extraction tool used by an Iranian APT. While the tool was designed to be run locally, it still needed to receive a response from one of two Command and Control (C2) servers before proceeding. TAG identified these IPs as 136.243.108[.]14 (Germany) and 173.209.51[.]54 (Canada)

Interesting Subdomains

Pivoting on the information provided by TAG, SecurityScorecard's Threat Research, Intelligence, Knowledge and Engagement (STRIKE) Team got to work. We started by looking at the C2 IP, 136.243.108[.]14, and quickly discovered that it was hosting some interesting mail subdomains. Dig requests for each of these subdomains reveal that they each have CNAME record that points to smtp11.smtplab[.]com. Browsing to smtp11.smptlab[.]com redirects to smtp11.smtplab[.]com/webmail/login, which displays a Kerio Connect Secure Email login interface. According to its website, Kerio Connect is a mail server and all-in-one collaboration tool that is easy to manage and deploy. It is just the right size for small and medium businesses with smaller budgets and limited IT staff.

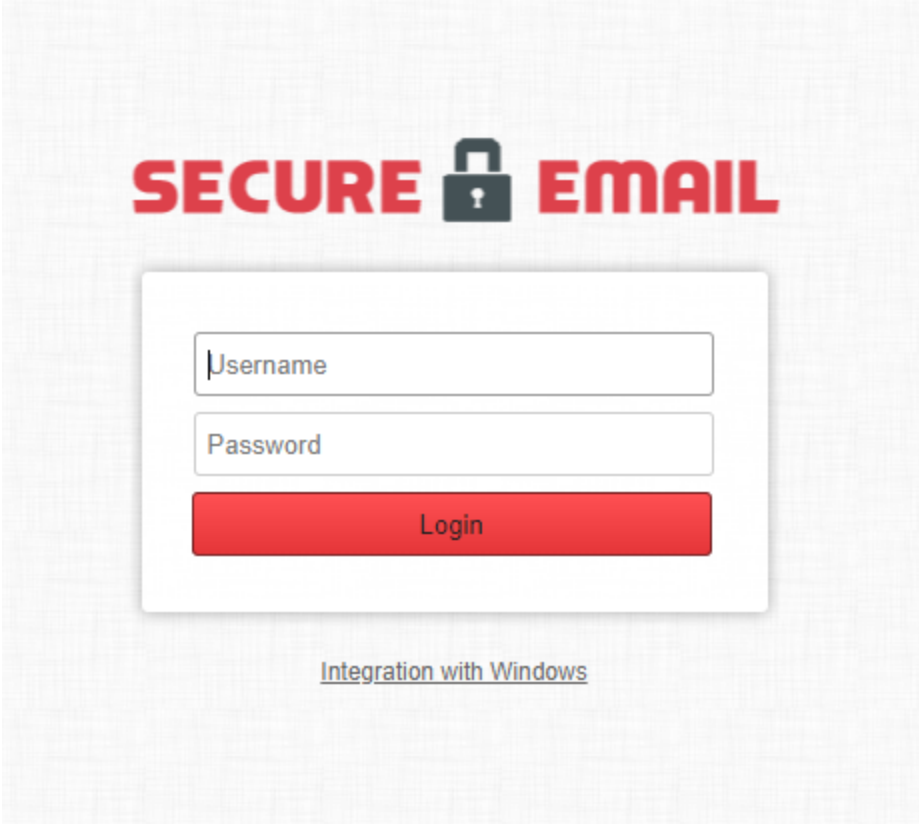

Image 1: Kerio Connect login page found at smtp11.smtplab[.]com/webmail/login

STRIKE analyzed all the mail servers resolving to IP 136.243.108[.]14 and determined that most are typosquatted domains, attempting to pose as mail servers belonging to the targeted entities.

Impostor Domain	Likely Target
mail.friendsgroupco[.]net	Marine Services Company located in Port Said, El Sharq District, Egypt
mail.myegycom[.]com	Arabic-language dating website
mail.atlas-shipsupplier[.]com	Marine Services Company located in Port Said, Egypt
mail.salamcoshipping[.]com	Shipping and Forwarding Company based in Jordan
mail.elcosteelgroup[.]com	Steel manufacturer in Port Said, Egypt
mail.maroceanshipping[.]com	Trading and Shipping company based in Israel
mail.greenway-egy[.]com	Egypt-based organization that provides vocational training opportunities in Germany
mail.ems-shippingserv[.]com	Possible Egyptian postal company
mail.winmarine[.]com	Marine Consultancy Service provider based in India
mail.pts-chemical[.]com	Unknown
mail.friendsgroupmarine[.]com	Marine Services Company located in Port Said, El Sharq District, Egypt
mail.sysegy[.]com	Possible equipment provider for filtration and heat exchange, based in Egypt
mail.elco-steel[.]com	Steel manufacturer in Port Said, Egypt
mail.alainspecial[.]ae	Center for Care and Rehabilitation based in the UAE

Table 1: Imposter mail server domains resolving to IP address 136.243.108[.]14

Likely Targets

Most of these imposter mail subdomains appear to target Egypt-based shipping and marine services companies. Many of the non-shipping services Egyptian firms listed above are also based in Port Said; attempts to impersonate them may, therefore, still reflect the targeting of the shipping service industry. Port Said is a shipping hub, and professional services firms located there likely serve the area's major industries. That being the case, those firms also likely handle data relevant to the shipping and marine services industries and could therefore prove to be of interest to a threat actor looking to access such data.

STRIKE identified a series of domains related to investment in the Eilat region of southern Israel. These domains simply switch an "L" with a "T" (i.e., eilatinvest[.]com/eitatinvest[.]com). Eilat is close to Israel's border with Jordan and home to the Trans-Israel pipeline's southern terminal, originally built as a joint venture between Iran and Israel back in friendlier times. Iran was no longer able to use the pipeline after the overthrow of the Shah in 1979 and pursued a claim for compensation against Israel. The case was decided in Iran's favor in 2016, awarding $1.1 billion. Eilat Ashkelon Pipeline Company is one of Israel's most secretive companies. The current wonder of the pipeline, the Eilat Ashkelon Pipeline Company (EAPC), enjoys a state decree that shrouds its affairs in secrecy for reasons the Israeli government says are related to national security.

Other domains appeared to imitate the legitimate domain of a prominent law firm in the UAE, whose clients include H. H. SH. Saeed Bin Mohammed Hasher Al Maktoum.

All of the typo-squatted top-level domains were registered with the same registration details, indicating that they are Wild West Domains resold by a small Egyptian hosting company called EgWan. EgWan also provides other hosting services, such as email via Office 365.

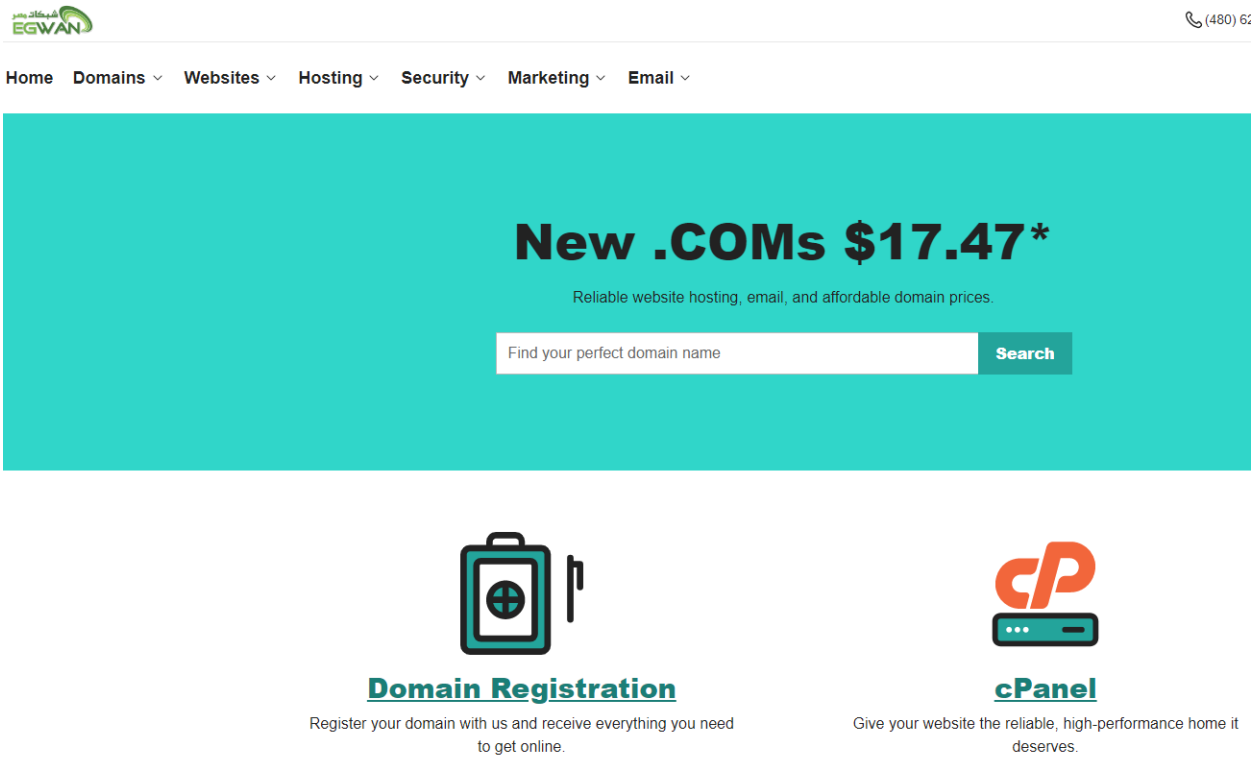

Image 2: Homepage of EgWan Hosting

Rogue Subdomains

STRIKE identified three other mail server subdomains that at first appeared to be typo-squatted, but further investigation revealed that they are more likely rogue subdomains of legitimate domains. For example, elephantmarine[.]com leads to what appears to be a legitimate website that has been around since at least 2011, currently hosted on IP address 207.180.247[.]135. However mail.elephantmarine[.]com is hosted on 136.243.108[.]14, with a CNAME record directing it to smpt11.smtplab[.]com. Two other examples of these rogue subdomains are mail.hhfis[.]com and mail.etisalategypt[.]com.

According to Whois information, these domains were also registered through EgWan. To create a subdomain, one would need to have access to the CPanel, or DNS configuration, for these domains. It is possible that the threat actor managed to gain access to one or both of these via an unknown method. Once they gained access, they were able to create the rogue mail subdomain, and point it to the same infrastructure as the typo-squatted domains, namely IP 136.243.108[.]14 and smpt11.smtplab[.]com.

Attribution

Google does not discuss the apparent use of hijacked subdomains to impersonate various Middle Eastern businesses in its recent report on the HYPERSCRAPE tool it attributed to APT35/Charming Kitten. However, the targeting suggested by these impersonations would be in keeping with Iran-linked APT groups' established patterns. Suchgroups have, in the

past, targeted large industries in the US client states in the region (like Egypt and the UAE,) and such targeting likely still serves Iranian regional interests in the present. Thus, based on this targeting and the links to infrastructure used in activity attributed to APT35, STRIKE assesses with high confidence that these subdomains were created to support Iran-linked APT phishing campaigns.

Recommendations

It is important to be aware of domain names impersonating your own, as these will likely be used to facilitate attacks on your organization. STRIKE recommends using a brand monitoring service, such as SecurityScorecard's Cyber Risk Intelligence (CRI), that detects impostor domains and helps mitigate your exposure to this critical cyber risk.

About STRIKE Team

SecurityScorecard's Threat, Research, Intelligence, Knowledge and Engagement (STRIKE) team now offers Cyber Risk Intelligence (CRI) services in order to provide clients with custom intelligence regarding their risk exposure to issues such as leaked credentials, impostor domains, hacker chatter, adversary counterintelligence, and more. STRIKE-CRI also includes custom investigations into areas of interest for clients, such as active campaigns, specific actors, infrastructure, and TTPs. STRIKE-CRI empowers organizations by augmenting existing investigative resources and leveraging the comprehensive data sets collected by SecurityScorecard in unique, customized ways.

For more custom insights on a regular basis through our team's 100+ years of combined threat research and investigation experience, or more details on these findings and the other keywords that were provided, please visit our website.

About SecurityScorecard

SecurityScorecard offers a 360-degree approach to security prevention and response. For more information, request a demo. SecurityScorecard's threat research and intelligence could be the competitive advantage organizations need to stay ahead of today's fast-moving threat actors.

Return to Blog