DECIPHER

Security news that informs and inspires

IRANIAN

Mar 31, 2021

By Dennis Fisher

An attack group known as Charming Kitten or Phosphorus that is tied to the Iranian government recently ran a highly targeted credential-theft campaign against senior personnel in medical institutions and research facilities in the United States and Israel, using rigged PDFs as a lure and possibly signaling a change in targeting for the group.

The campaign occurred in December 2020 and researchers discovered that the Phosphorus group targeted a small, quite specific group of people in the medical research field. The attackers used the familiar spear-phishing technique, although the lure itself is a little odd, given that the targets are all in the medical field. The group, which Proofpoint calls TA453, sent emails to the potential victims with the subject line, "Nuclear weapons at a glance: Israel". The body of the email contains some information on Israel's nuclear capabilities and a link to a website controlled by the attackers. If the victim clicks on the link, the site serves a phishing page that asks the victim to enter credentials for Microsoft OneDrive. The campaign is known as BadBlood and researchers said it shared some similarities with other known campaigns by the same group.

"Attempting to use any other hyperlink in the webpage results in the same redirect to the same forged Microsoft login page, except for the "Create one!" link. This tab leads to the legitimate Microsoft Outlook 'Sign Up' page," a report from Proofpoint, which discovered the campaign, says.

“Once an email is entered by the user and ‘Next’ is clicked, the page prompts for a password. Once a user enters their credentials, they are then redirected to Microsoft’s OneDrive where the benign ‘Nuclear weapons at a glance: Israel’ document is hosted.”

This kind of highly targeted campaign is typical of APT groups, and medical professionals and researchers have become prime targets in the last year as the COVID-19 pandemic has stretched on. There have been a number of APT campaigns that targeted COVID-19 vaccine research and manufacturing facilities in recent months, but the new Phosphorus campaign targeted medical professionals in oncology, genetics, and neurology, not epidemiology or infectious disease research.

"TA453's credential phishing campaigns typically target a small number of indiviiduals, which is a departure from other Iranian APTS," said Sherrod DeGrippo, senior director of threat detection and response at Proofpoint.

The attack group is known to have targeting and collection that aligns with Iran’s Islamic Revolutionary Guard Corps.

“TA453 targeted less than 25 senior professionals at a variety of medical research organizations located in the US and Israel. Proofpoint analysis of the targets’ publicly available research efforts and resumes indicate TA453 targeted individuals with a background in either genetics, oncology, or neurology,” the Proofpoint report says.

“These medical professionals appear to be extremely senior personnel at a variety of medical research organizations. Additionally, TA453 targeting Israeli organizations and individuals is consistent with increased geopolitical tensions between Israel and Iran during 2020.”

"While this campaign may represent a shift in TA453 targeting overall, it is also possible it may be an outlier."

The Phosphorus group has been active for several years and has not escaped the notice of law enforcement officials and security and technology companies. In 2019, Microsoft conducted a takedown of a large swath of the Phosphorus infrastructure, taking over 99 separate domains used in the group’s phishing campaigns and later that year the company published details of a campaign in which Phosphorus targeted people associated with the 2020 presidential campaigns, journalists, and government officials. The group has also been known to target defense companies and government agencies.

Proofpoint’s researchers said the recent campaign can’t be seen as definitive proof of a change in the group’s tasking or targeting. It could be an anomaly, or part of a larger effort to establish footholds in a broader set of networks.

“As collaboration for medical research is often conducted informally over email, this campaign may demonstrate that a subset of TA453 operators have an intelligence requirement to collect specific

medical information related to genetic, oncology, or neurology research. Alternatively, this campaign may demonstrate an interest in the patient information of the targeted medical personnel or an aim to use the recipients' accounts in further phishing campaigns. While this campaign may represent a shift in TA453 targeting overall, it is also possible it may be an outlier, reflective of a specific priority intelligence tasking given to TA453," the researchers said.

DeGrippo said that TA453 seems to have left off its phishing efforts since this campaign ended.

"While multiple domains with lure documents are still available as of this report, we have not seen any further credential phishing camapigns since December," she said.