Check Point Research uncovers rare techniques used by Iranian-affiliated threat actor, targeting Israeli entities

By etal

Published: 2023-04-25 · Archived: 2026-04-05 16:55:08 UTC

Highlights:

- ***Check Point Research reveals new findings related to Phosphorus APT group, an Iranian APT group operating in the Middle East and North America. CPR dubbed this activity cluster Educated Manticore***
- ***Educated Manticore has substantially enhanced its toolkit by incorporating new techniques, embracing current attack trends, and employing ISO images and other archive files to initiate infection chains.***
- ***The research puts a spotlight on the lures of the attack, which used Hebrew and Arabic languages, suggesting targets were entities in Israel.***

Main findings .

Today, Check Point Research (CPR) reveals new findings of a group closely related to **Phosphorus**. This research presents a new and improved infection chain used by the attackers. By following the attack's trail, CPR was able to establish links to Phosphorus, an Iran-based threat group operating in both North America and the Middle East. Phosphorus has previously been associated with a broad spectrum of activity, ranging from ransomware to spear-phishing of high-profile individuals.

In the attacks detailed in this report, we reveal the threat actor has significantly improved its mechanisms and adopted rarely seen in the wild techniques, such as using .NET binary files created in mixed mode with assembly code. The newly discovered version is likely intended for phishing attacks focused around Iraq, using an ISO file to initiate the infection chain. Other documents inside the ISO file were in Hebrew and Arabic languages, suggesting the lures were aimed at Israeli targets. CPR decided to track this activity cluster as **Educated Manticore**.

Since 2021, a new cluster of activity with clear ties to Iran has caught the attention of the Threat Intelligence community. The aggressive nature of the new threat, in combination with their ties to ransomware deployments, led to a thorough analysis of its activities.

As the activity evolved, the ties between the different clusters became harder to untangle. While the two ends on the spectrum of those activities differ significantly, not once has the threat intelligence community stumbled upon an activity that does not easily fit the known clusters. CPR's previous report described one of those samples and the overlaps between the Log4J exploitation activity to an Android app previously tied to APT35.

The variant described in this report was delivered using ISO files, indicating it is likely meant to be the initial infection vector. Because it is an updated version of previously reported malware, this variant (PowerLess),

associated with some of Phosphorus' Ransomware operations, may only represent the early stages of infection, with significant fractions of post-infection activity yet to be seen in the wild.

Given these new infections are never before seen in the wild techniques, Check Point Software can provide certain defense tips to protect against such attacks :

- **Up-to-Date Patches** : WannaCry, one of the most famous ransomware variants in existence, is an example of a ransomware worm. At the time of the famous WannaCry attack in May 2017, a patch existed for the EternalBlue vulnerability used by WannaCry. This patch was available a month before the attack and labeled as "critical" due to its high potential for exploitation. However, many organizations and individuals did not apply the patch in time, resulting in a ransomware outbreak that infected 200,000 computers within three days. Keeping computers up-to-date and applying security patches, especially those labeled as critical, can help to limit an organization's vulnerability to attacks as such patches are usually overlooked or delayed too long to offer the required protection.
- **Cyber Awareness Training:** Phishing emails are one of the most popular ways to spread malware. By tricking a user into clicking on a link or opening a malicious attachment, cybercriminals can gain access to the employee's computer .With the global gap in cybersecurity talent impacting organisations around the world, frequent cybersecurity awareness training is crucial to protecting the organization against cyberattacks, leveraging their own staff as the first line of defence in ensuring a protected environment. This training should instruct employees to do the following:
    - Not to click on malicious links
    - Never open unexpected or untrusted attachments
    - Avoid revealing personal or sensitive data to phishers
    - Verify software legitimacy before downloading it
    - Never plug an unknown USB into their computer
    - Use a VPN when connecting via untrusted or public Wi-Fi
- **Utilize better threat prevention:** Most attacks can be detected and resolved before it is too late. You need to have automated threat detection and prevention in place in your organization to maximize your chances of protection.
    - **Scan and monitor emails**. Emails are a common choice of cybercriminals executing phishing schemes, so take the time to scan and monitor emails on an ongoing basis and consider deploying an automated email security solution to block malicious emails from ever reaching users.
    - **Scan and monitor file activity**. It is also a good idea to scan and monitor file activity. You should be notified whenever there is a suspicious file in play—before it becomes a threat.
- **Threat intelligence** provides the information required to effectively detect zero-day attacks. Protecting against them requires solutions that can translate this intelligence into actions that prevent the attack from succeeding. Check Point has developed over sixty threat prevention engines that leverage ThreatCloud AI threat intelligence for zero-day prevention.
- **Security Consolidation works:** Many organizations are reliant upon a wide array of standalone and disconnected security solutions. While these solutions may be effective at protecting against a particular threat, they decrease the effectiveness of an organization's security team by overwhelming them with data and forcing them to configure, monitor, and manage many different solutions. As a result, overworked security personnel overlook critical alerts.

A unified security platform is essential to preventing zero-day attacks. A single solution with visibility and control across an organization's entire IT ecosystem has the context and insight required to identify a distributed cyberattack. Additionally, the ability to perform coordinated, automated responses across an organization's entire infrastructure is essential to preventing fast-paced zero-day attack campaigns.

For the full deep dive on Educated Manticore, visit the CPR blog.
