TLP: Clear - Unlimited disclosure, this information can be shared publicly with everyone.

JANUARY 2023 MONTHLY BULLETIN

The end of the holiday season and the start of the new year bring renewed energy, not only for individuals but also for organizations. This renewed energy can be seen in increased productivity and focus when it comes to cybersecurity, enabling individuals and organizations to detect and address potential security threats more efficiently. Furthermore, this also brings a renewed commitment to maintaining good security practices.

01 Executive Summary

Our collaborative and information sharing efforts have grown stronger, despite the threat landscape remaining consistent. This is beneficial for our organizations as it allows them to access a wider range of expertise and resources, which can enhance their ability to detect and respond to potential cyber incidents, thereby improving their overall security posture.

By staying informed, organizations can stay ahead of the threats and keep their sensitive information and systems secure. In these monthly bulletins, we cover the most prominent security incidents of the past month and provide insights into emerging trends and tactics used by threat actors.

02 Case Study

Rise in Sophisticated HTML Smuggling Phishing Threat

During January, our operations team noticed a rise in a sophisticated form of credential phishing known as HTML smuggling. Traditional phishing attempts typically involve sending an email that prompts the recipient to click a link to a fake website, masquerading as a reputable company, in an attempt to trick them into providing their login information. However, email security scanners have become increasingly adept at identifying and blocking these malicious URLs before the emails reach the user's inbox.

In response to this countermeasure, phishers have begun using HTML attachments in their emails. HTML, or Hypertext Markup Language, is a legitimate and commonly used language to format and structure emails, including the inclusion of images, text styling, and links. Since these types of attachments are not typically blocked by email security scanners, phishers are able to use them to sneak in fake login pages. Once the user opens the HTML attachment, they are taken to the fake login page, which is embedded with JavaScript that captures their login information without their knowledge.

JavaScript is a programming language used to add interactivity and dynamic behavior to websites and applications, such as auto-saving an email draft or triggering automatic file downloads. While JavaScript powers many of today's internet platforms, it presents both significant benefits and potential security risks.

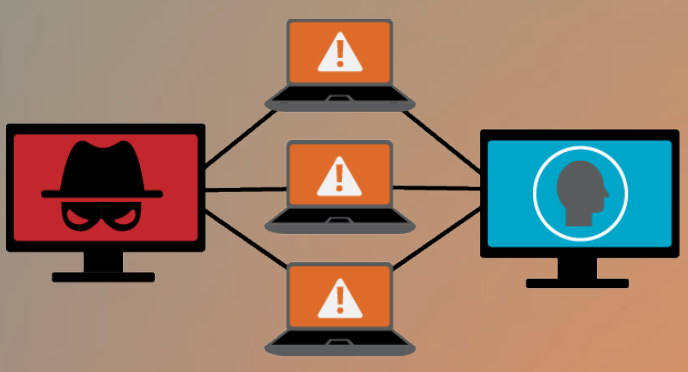
Steps to Mitigate Risk

- Regularly educate employees on how to identify and report suspicious emails, particularly those containing .html file attachments that may ask for login information, and foster a culture where reporting them is encouraged.
- Implement phish-resistant multi-factor authentication (MFA) for all employee login accounts, which can effectively protect against unauthorized access, even if login credentials are compromised.

03 External Trend Spotlight

Healthcare organizations warned of DDoS threat from pro-Russian hacktivist group, KillNet

The Health Sector Cybersecurity Coordination Center (HC3) recently issued a warning regarding KillNet, a pro-Russian hacktivist group posing a threat to U.S. healthcare organizations. The group has been active since January 2022 and is known for Distributed Denial of Service (DDoS) attacks against Ukraine supporters, causing service outages lasting hours to days, according to the HC3.



A DDoS is a type of cyber-attack where multiple compromised computer systems are used to flood a target network with a large amount of traffic, causing it to become overwhelmed and unavailable to its intended users. The goal of a DDoS attack is to overload the target's servers and cause them to crash or become unavailable. This type of attack can cause significant damage to online businesses, governments, and organizations, as well as disrupt communication and internet access for users.

In January, the threat group listed two of our healthcare organizations, along with other well-known healthcare systems in the U.S., U.K., Spain, Germany, Finland, Norway, Poland, and the Netherlands as potential targets on their official Telegram page. The team's proactive actions enabled the timely detection of the potential threat, resulting in prompt information sharing with the impacted organizations. One attempt impacted one organization's third-party hosted domain, but quick identification and readiness prevented significant service disruption.

Given Killnet's capabilities, healthcare organizations should take proactive steps to mitigate the risk of a DDoS attack. Specifically, consider enabling web application firewalls (WAFs) such as Cloudflare Protection on public-facing web servers to help mitigate application-level attacks. These distribute web traffic across a multi-content delivery network (CDN) to balance the load and prevent server overload.

Contact Us for More Info: 248-837-1400 solutions@cyberforceq.com