CYBERFORCE

July 12, 2023

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

JUNE 2023 MONTHLY BULLETIN

CyberForce|Q continues to work diligently to detect the latest threats of the cyber landscape. Cyber criminals work around the clock to steal your personal information. At CyberForce|Q we work to stay ahead of the cyber criminals. Our monthly bulletin covers the most prominent security incidents of the past month and provides insights into emerging trends and tactics used by threat actors, so you can stay informed.

01 Executive Summary

Our collaborative and information sharing efforts have grown stronger, despite the threat landscape remaining consistent. This is beneficial for our participants 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, we help our participants stay ahead of 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

QR Code Phishing

Our team has observed multiple credential phishing emails that contain malicious QR codes through what appears to be a new phishing technique.

QR codes are two-dimensional barcodes that can be scanned by a smartphone camera to quickly and easily access information or a website. They are commonly used in advertising, on business cards, and for contactless payments. However, threat actors may alter the original QR code and link it to a credential harvesting login portal, or to malware that automatically installs on the user's device as soon as they open the link via a QR code scan.

This poses a significantly higher risk because users may not have a way of knowing where the QR code will take them until they scan it and may not be able to verify the authenticity of the link. This makes it easier for threat actors to trick users into unknowingly downloading malware or giving away their login credentials.

Steps to Mitigate Risk

- **Educate end users on how to spot and report phishing attempts. Additionally, be cautious of business authentication-related emails containing a QR code.**
- **Establish policies and procedures for handling emails requesting personal or sensitive information.**
- **Implement phish-resistant MFA for all user accounts and systems to prevent unauthorized access through stolen credentials.**
- **Users can verify the contents of the QR code by taking a screenshot of the code and uploading it to https://scanqr.org/ to have it quickly analyzed by a free, third party service.**

03 External Trend Spotlight

15% of Employees Regularly Post Sensitive Company Data into ChatGPT, Study Finds

In a report by LayerX titled "Revealing the True genAI Data Exposure Risk", a new study found that 15% of employees regularly post company data into ChatGPT, with over a quarter of that data being considered sensitive information, putting their employers at risk of a security breach. The report analyzed the behavior of over 10,000 employees, examining how they used ChatGPT and other generative AI apps in the workplace. Workers were found inputting data into GenAI tools an average of 36 times per day, with many employees pasting sensitive data on a weekly or even daily basis.

The top categories of confidential information being input into the GenAI tools include internal business data at 43%, source code at 31%, and personally identifiable information at 12%. Unfortunately, since GenAI platforms operate in the browser, existing security solutions cannot address risks like pasting of sensitive data. The study found that 4% of employees paste sensitive data into GenAI on a weekly basis, increasing the chances of sensitive data exfiltration. This exposes sensitive company data into GenAI, even though it is most likely done innocently to save time.

- **Implement employee training to raise awareness about the risks associated with using GenAI tools.**

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