CYBERFORCE|Q

March 15, 2023

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

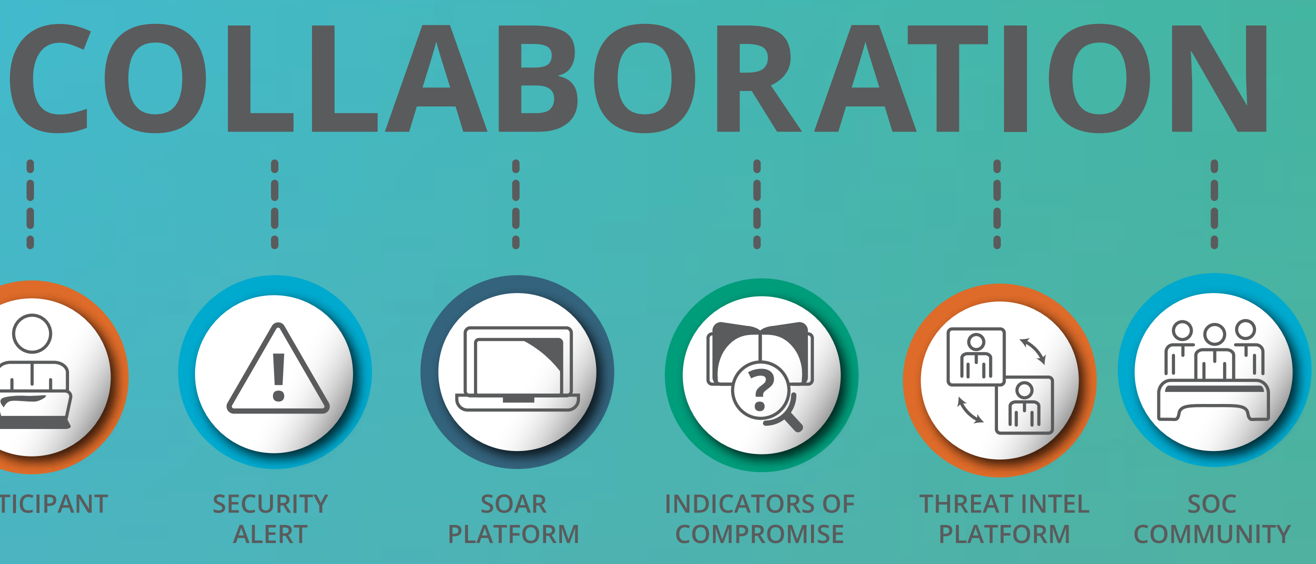
FEBRUARY 2023 MONTHLY BULLETIN

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 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

Post-Macro World Sees Rise in Microsoft OneNote Documents Delivering Malware

Last year, Microsoft disabled macros in Office applications downloaded from the internet, prompting threat actors to explore uncommon file types. This has caused an increase in malicious OneNote file attachments appearing in phishing emails.

Our team observed numerous user-reported emails with suspicious OneNote file attachments from multiple client environments. Upon further investigation, it was found that these files had embedded and encoded scripts that would execute Qakbot malware if the user opened the file. Qakbot, also known as QBot, is a Banking Trojan first observed in 2007 that has become one of the most pervasive threats globally. It is designed to steal banking data, but also has capabilities to spread itself, evade detection, and install additional malware.

These internal developments occurred shortly after we shared intelligence about this malware trend with our organizations, highlighting the importance of timely and accurate information sharing. Globally, OneNote phishing emails have been on the rise, though they don't currently appear to be targeting critical infrastructure entities specifically. However, with any emerging trend, actionable knowledge and insight on threat actors and their malicious activities can enable our clients to reduce harm through proactive security decision-making.

N OneNote

DID YOU KNOW?

*A **Macro** is a set of instructions or code that can be used to perform a series of actions in an Office application such as Microsoft Word, Excel, or Powerpoint. Macros can be used to automate repetitive tasks or create complex functionality that would otherwise be difficult to program. While macros can be useful, they can also pose a security risk. Malicious macros can be used to download malicious code, exploit vulnerabilities, or steal information.*

Steps to Mitigate Risk

- Ensure users are educated on the risks associated with opening files from untrusted sources, and train users to report suspicious emails.
- Implement security controls that prevent users from executing untrusted programs and scripts.
- If possible, block attachments with the file extensions .one and .onepkg from OneNote.

03 External Trend Spotlight

Healthcare Sector Warned About Increase in GootLoader Malware Infections

Security researchers have raised concerns following a surge in cyber-attacks distributing a malware variant known as GootLoader, which is used by a threat actor known as UNC2565. This malware was first identified in 2014 and is now one of the most dangerous malware threats. The threat group behind the campaign is highly sophisticated and has been continuously refining its tactics and developing the malware to avoid detection by security systems.

The malware is spread via search engine optimization (SEO) poisoning campaigns, targeting employees searching for business-related documents. SEO involves using certain keywords and phrases in web content to make it more likely to appear in search engine results. Keywords and phrases are chosen based on what users are likely to search for, so that when they search for related terms, the website or content will appear higher in the search results. This increases the visibility of the website and helps it to rank higher in the search engine results.

An SEO poisoning attack is a malicious technique used by cybercriminals to manipulate search engine rankings and redirect users to malicious websites. This type of attack usually involves injecting malicious code into vulnerable websites or creating malicious websites that appear in search engine results. They can be used to distribute malware, steal user data, or redirect users to phishing websites.

In addition to the legal sector, which has been targeted using the keyword "agreement" in SEO poisoning attacks, the current operation has now shifted to the healthcare industry, using the words "hospital," "health," and "medical."

Steps to Mitigate Risk

- Educate users on the potential implications of visiting and obtaining files from unverified, unreliable sources.
- Ensure that scripts cannot be executed on user workstations without authorization from a system administrator.
- Track and prevent PowerShell activity attempting to establish a connection with an outside host.

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