CYBERFORCE|Q

June 14, 2023

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

CYBERFORCE|Q

MAY 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

Protecting VIPs: Why Safeguarding Against Cyber Threats is Crucial for Organizational Success

Protecting the security of an organization's VIPs is crucial for the success of a company. VIPs, which include C-suite executives, presidents, and operations directors, are high-value targets for cybercriminals. These bad actors often try to obtain sensitive information to disrupt the organization's operations by targeting its leaders.

For example, if a cybercriminal gains access to the email account of an institution's president and uses it to send malicious emails to internal employees, the recipients may be more likely to trust the content of the email due to the sender's perceived authority. A VIP may have greater access to confidential data, making them a target for credential theft. While it is crucial to protect the security of all employees, threat actors tend to target those with the highest influence in their organization due to the potential reputational and operational damage that could be caused.

When it comes to safeguarding an organization, it is crucial to stay vigilant against any potential threats. This means that not only should any malicious attempts be dealt with as soon as possible, but also that proactive measures should be taken to prevent such attempts from occurring in the first place.

Steps to Mitigate Risk

- **Implement strong access controls through strict authentication and authorization policies.**
- **Provide ongoing cybersecurity training to VIPs to keep them informed about trending threats.**
- **Conduct regular security assessments.**
- **Establish a well-defined incident response plan.**

03 External Trend Spotlight

Hackers are Actively Using the New .zip TLD for Malicious Attacks

Google has released the .zip top-level domain (TLD) to the public, which allows interested parties to register .zip domains. However, cyber criminals have already taken advantage of this by using .zip domains in phishing campaigns, such as officeupdate.zip or microsoft-office.zip. This is possible because .zip is both a popular file extension and a top-level domain.

Most registered .zip domains are not set up to display web content. While there is currently little reason to access .zip domains, if legitimate companies and software developers announce that their products are availible on a specific .zip domain, this may change. It is recommended to disable access to .zip domains until the risk can be assessed.

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