CYBERFORCE | Q

August 16, 2023

JULY 2023 MONTHLY BULLETIN

CyberForce|Q continues to work diligently to detect the latest threats of the cyber landscape. 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.

Key Takeaways

Takeaway 1

Port Filtering reduces the likelihood of unauthorized access and helps ensure that sensitive information remains protected.

Takeaway 2

Universities tend to be frequent targets of employment scams, and similar related activities.

Takeaway 3

Employees and students who are trained on how to recognize and avoid fraudulent messages are less likely to fall prey to advance fee fraud and other scams.

Case Study

Attack Surface Management: Port Filtering

Generally, organizations will place a firewall at the network perimeter to help prevent unauthorized network access. If we imagine the internal network and its public-facing resources as a house and front lawn, the firewall is like the front gate and fence that separates the house from the street. It regulates and monitors traffic entering and leaving the network, blocking unauthorized access attempts while allowing legitimate traffic to pass through. Network ports are like the doors and windows that allow traffic to enter and exit the house. The primary goal of these network monitoring systems is to continuously analyze network traffic flowing between the internal (LAN) and external network (WAN) for the purpose of identifying potential threats or abnormalities.

If unauthorized traffic is detected and accepted, the best initial action is to block any connection attempts to or from the unauthorized source. However, relying solely on these actions puts the organization in a highly reactive state. An additional recommendation to help reduce the risk of the activity occurring in the first place is by auditing firewall rules to restrict the number of open or unfiltered ports to those that serve a legitimate business purpose. This will help reduce the attack surface of the network because attackers will have fewer entry points to exploit.

Port filtering is important because it helps mitigate potential attacks that could exploit network vulnerabilities. By restricting access to only necessary ports, organizations can limit the number of opportunities for attackers to gain access to the network. This reduces the likelihood of unauthorized access and helps ensure that sensitive information remains protected. Additionally, managing the organization's attack surface can save time, resources, and potentially millions of dollars in damages.

External Trend

Job Scams Using Bioscience Lures Target Universities

Proofpoint observed a campaign in late May 2023 targeting university students in North America using job-themed email lures. The emails were purportedly from a variety of organizations, primarily related to biosciences, healthcare, and biotechnology, and contained interview requests for remote data entry jobs. The sender would invite the recipient to conduct a video or chat interview on a third-party platform for additional information and to prepare them for the role. Retrospective analysis identified multiple related and similar campaigns using the same biotech themes leading to advance fee fraud (AFF) activity in Proofpoint threat data and external sources going back to at least March 2023.

Threat actors may target universities for a variety of reasons. Students are likely more open to flexible, remote work opportunities, and rising inflation and cost of education is putting the pinch on students' finances, making the promise of quick cash more attractive. International students may not recognize telltale signs of fraudulent emails as well as native English speakers. Universities tend to be frequent targets of employment scams, and similar related activity following the job fraud model goes back a number of years.

Steps To Mitigate

Educate employees and students on how to recognize and avoid phishing emails and other fraudulent messages.

Establish clear policies and procedures for handling sensitive information and financial transactions to prevent employees and students from falling prey to advance fee fraud and other scams.

How CyberForce|Q Can Help

For over 27 years, CyberForce|Q has been a trusted name in advancing cybersecurity programs. Our expertise lies in designing and executing measurable cybersecurity strategies tailored to organizations of all sizes. With a track record of proven results, we offer services such as customized security assessments, robust security operations centers, and comprehensive strategic guidance. Let us assist your organization in prioritizing its goals, elevating your cybersecurity capabilities, and providing meaningful measurements of progress. Our participants are innovative leaders who share optimal strategies to implement and advance a proven cybersecurity program. CyberForce|Q together with our participants protecting the cyber realm.

Contact Us For More Information

248-837-1400 • solutions@cyberforceq.com

CYBERFORCE | Q