University of Central Florida

INFOSEC

Security Awareness Newsletter

Issue 7 July 11, 2023

UCF Information Security Office

David Zambri

Associate Vice President and Chief Information Security Officer

Top 3: Security News in July 2023

1. Japan's Largest Port Hit with a Ransomware Attack

BleepingComputer.com

The Port of Nagoya, the largest and busiest port in Japan, has been targeted in a ransomware attack that currently impacts the operation of container terminals. The port accounts for roughly 10 percent of Japan's total trade volume. It operates 21 piers and 290 berths. It handles over two million containers and cargo tonnage of 165 million every year.

2. CISA Issues Warning for Cardiac Device System Vulnerability

TheRecord.media

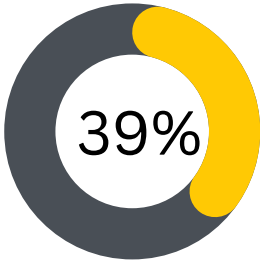
Medtronic said in an advisory that if exploited, the vulnerability allows hackers to delete, steal or modify data from a cardiac device. Hackers can also use the device's issues to penetrate into a healthcare organization's network.

3. Microsoft Denies Major 30 Million Customer-Breach

InfoSecurity-Magazine.com

Anonymous Sudan claimed to have successfully hacked Microsoft to sell the database, however, Microsoft denied those claims with this brief statement, "At this time, our analysis of the data shows that this is not a legitimate claim and an aggregation of data. We have seen no evidence that our customer data has been accessed or compromised."

DID YOU KNOW?

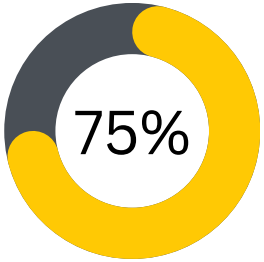


of businesses faced a cloud environment data breach last year

The study found that 39 percent of businesses experienced a data breach in their cloud environment last year, an increase from the 35 percent reported in 2022, Click to read more.

40% increase in global ransomware attacks

The report tracks the ongoing increase in complex ransomware attacks and spotlights recent ransomware trends, including the targeting of public entities and organizations with cyber insurance, growth of ransomware-as-a-service (RaaS) and encryption-less extortion, Click to read more.



of businesses report security as an increasing priority

The PSA Certified 2023 Security Report analyzes the relationship between security investments and legislation, Click to read more.

July Security Article

The Evolution of Phishing Attacks and Detection Best Practices

Phishing attacks have evolved into sophisticated and prevalent threats in the digital landscape. This article explores their evolution and provides essential practices for effectively detecting and combating phishing attempts.

Phishing attacks have advanced significantly over time. Initially characterized by obvious red flags, such as misspellings, they now employ sophisticated techniques. Attackers create convincing emails and messages, often impersonating trusted entities and use social engineering to trick individuals into divulging sensitive information or clicking on malicious links. Phishing attacks have expanded beyond email to include social media, SMS and voice calls, leveraging psychological manipulation and urgency.

To counter evolving phishing threats, it's crucial to adopt effective detection practices:

1. Be safe rather than sorry: Take a skeptical approach to unfamiliar communications. If there's a slight doubt about the legitimacy, trust your gut.

2. Verify the source: Independently verify the sender's identity before interacting with emails, messages or links.

3. Exercise caution with personal information: Refrain from sharing sensitive information through insecure channels and be cautious of requests for such data.

4. Implement security measures: Utilize spam filters, anti-malware software and firewalls to identify and block phishing attempts. Keep security systems updated.

5. Know the procedures for reporting suspected phishing attempts: Facilitate prompt action and prevention.

By staying informed and adopting robust detection practices, we can combat evolving phishing attacks and protect our sensitive information.

In Other (Security) News...

New Tools Capable of Sending External Malware to Microsoft Teams

A member of U.S. Navy's red team has published a tool called TeamsPhisher that leverages an unresolved security issue in Microsoft Teams to bypass restrictions for incoming files from users outside of a targeted organization, Click to read more.

Threat Actors are Exploiting WordPress Zero-Day to Create Secret Admin Accounts

Researchers at the WordPress security firm WPScan noticed rogue new administrator accounts kept appearing on the websites targeted by the threat actors, Click to read more.

UK's Law Could Allow for Real-Time Internet Logs

Britain's cyber and signals intelligence agency GCHQ could monitor logs of domestic internet traffic in the United Kingdom in real-time to identify online fraud and interrupt criminals during the act, under a new law being considered by the government, Click to read more.

Security Alerts

Google Chromium V8 Type Confusion Vulnerability

Click to read more.

Samsung Mobile Devices Improper Input Validation Vulnerability

Click to read more.