University of Central Florida

INFOSEC

Security Awareness Newsletter

Volume 2, Issue 5 ⚡ May 14, 2024

UCF Information Security Office

David Zambri
Associate Vice President and Chief Information Security Officer

Top 3: Security News in May 2024

1. **The DOJ Detected the SolarWinds Hack 6 Months Earlier Than First Disclosed**
   [Wired.com]
   The US Department of Justice, Mandiant, and Microsoft stumbled upon the SolarWinds breach six months earlier than previously reported. Suspicions were triggered when the DOJ detected unusual traffic emanating from one of its servers that was running a trial version of the Orion software suite made by SolarWinds.

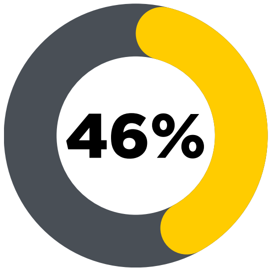
2. **Malware-Free Cyberattacks on the Rise**
   DarkReading.com
   Kurtz and Sentonas returned to the keynote stage to walk the audience through a case study of just how easily a threat actor can not just penetrate a network but also move laterally and persist without making a ripple, illustrating in stark terms the kind of challenge cybersecurity teams face trying to detect, much less mitigate, malwareless compromises.

3. **Google Authenticator Syncing Isn't End-to-End Encrypted**
   Gizmodo.com
   A new two-factor authentication tool from Google isn't end-to-end encrypted, which could expose users to significant security risks, a test by security researchers found.

DID YOU KNOW?

Report Shows Nearly 600% Annual Growth in Vulnerable Cloud Attack Surface

A new report reveals security organizations experienced 133% year-over-year growth in cyber assets, resulting in increased security complexity and mounting pressure for cloud enterprises.
Click to read more.



of Organizations Faced Synthetic Identity Fraud in 2022

New artificial intelligence (AI) technologies have raised a number of security concerns. AI can make it easier to commit fraud, as artificially created audio and video becomes increasingly believable.
Click to read more.

Report Reveals 65% of Cyberattacks Targeted at U.S.

A new report reveals an increase in cyberattacks targeting financial institutions, food retailers and healthcare providers
Click to read more.

May Security Article

Enhancing Security Awareness at UCF with KnowBe4's Phishing Simulation Platform

The UCF Information Security Office is always looking for effective ways to increase security awareness among the UCF Community. Phishing attacks are a constant threat, and we need to ensure that everyone in our organization understands how to recognize and avoid them. That's why we utilize the KnowBe4 platform, a provider of security awareness training and phishing simulation services.

KnowBe4's phishing simulation platform allows us to create realistic phishing campaigns that mimic real-world attacks. By sending these simulated phishing emails to our faculty, staff and students, we can track who falls for the scam and who reports it. The results help us identify areas where additional security training is needed, so we can target our efforts more effectively.

While it may seem counterintuitive to conduct phishing campaigns against our own employees, the reality is that these simulations are an extremely effective way to increase security awareness and identify vulnerabilities that could be exploited by real attackers. By utilizing a platform like KnowBe4, we have been able to establish a culture of security awareness at UCF, where employees are more vigilant and less likely to fall for phishing scams.

Over the past 12 months through education initiatives, we have been able to reduce our phish-prone score from 7.7% to just over 4%, sending over 12,000 simulated emails each month to faculty and staff. While 4% of 12,000 is still a large number, we are consistently below the industry average of 6.5%.

Overall, the use of phishing simulations has helped us to better protect ourselves against phishing attacks and other forms of cyber-attacks. It's just one of many tools and resources available to us, but it has proven to be a particularly powerful one that has had a positive impact at UCF.

In Other (Security) News...

Microsoft Edge is Leaking User Browsing Data to Bing

Reddit users first spotted the privacy issues with Edge last week, noticing that the latest version of Microsoft Edge sends a request to bingapis.com with the full URL of nearly every page you navigate to.
Click to read more.

Trigona Ransomware Targets Microsoft SQL Servers

Threat actors are hacking poorly secured and Interned-exposed Microsoft SQL servers to deploy the Trigona ransomware. Trigona is a malware strain that was discovered in October 2022, and Palo Alto Unit 42 researchers reported similarities between Trigona and the CryLock ransomware. Click to read more.

Google Gets Court Order to Take Down CryptBot That Infected Over 670,000 Computers

CryptBot is estimated to have infected over 670,000 computers in 2022 with the goal of stealing sensitive data such as authentication credentials, social media account logins, and cryptocurrency wallets from users of Google Chrome.
Click to read more.

Security Alerts

Apache Log4j2 Deserialization of Untrusted Data Vulnerability

Click to read more.

Oracle WebLogic Server Unspecified Vulnerability

Click to read more.