University of Central Florida

INFOSEC

Security Awareness Newsletter

Issue 2 | February 14, 2023

UCF Information Security Office

David Zambri

Associate Vice President and Chief Information Security Officer

Top 3: Security News in February 2023

1. ChatGPT Writes Malware

ZDNet.com

Analysis of chatter on dark web forums shows that efforts are already under way to use OpenAI's chatbot to help script malware.

2. NortonLifeLock Breached, Password Manager Accounts

BleepingComputer.com

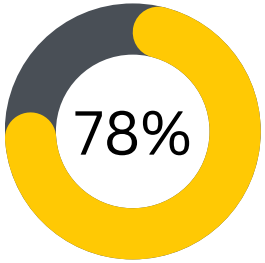
NortonLifeLock underlines that the risk is especially large for those who use similar Norton account passwords and Password Manager master keys, allowing the attackers to pivot more easily.

3. Unknown Hackers Steal 124,000 Patient Files from Texas Care Center

BiteDefender.com

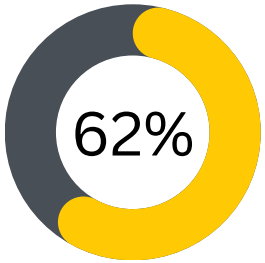
Home Care Providers of Texas (HCPT) has warned patients that hackers may have stolen personal and health information from its servers.

DID YOU KNOW?



According to an audit, 78 percent of UK schools have experienced a cyber incident
National Cyber Security Centre (NCSC) and the National Grid for Learning (LGfL), Click to read more.

GDPR fines surged 168% over the past year.
New data from DLA Piper. Click to read more.



The Russian invasion of Ukraine in early 2022 has led to a 62 percent decrease in stolen payment card records published to the dark web
according to Recorded Future. Click to read more.

February Article of the Month

Vulnerability Management

Vulnerability management is a critical component of an organization's overall security plan. The goal is to identify, assess and prioritize vulnerabilities in order to reduce the risk of a security breach. The first step is to perform a comprehensive audit of all assets, including hardware, software and data. This information will provide insight into the potential impact of a security breach and prioritize which vulnerabilities need to be addressed first.

Regular scans of assets should be conducted using reliable, updated tools to detect vulnerabilities. Automated scanning tools simplify the process and provide consistent and accurate results. Once vulnerabilities are detected, they should be categorized and prioritized based on their potential impact, and a remediation plan should be implemented.

Staying up-to-date with the latest security threats and vulnerabilities is crucial and requires ongoing research and subscriptions to relevant security alerts and bulletins. Regular communication and reporting to stakeholders, including management and key personnel, will ensure that everyone is aware of the organization's security posture and areas that need improvement.

In conclusion, a successful vulnerability management program requires technical expertise and strong communication skills. By proactively managing vulnerabilities, organizations can reduce the risk of a security breach and protect their critical assets and data.

In Other (Security) News...

Ransomware Attack Against University of Duisburg-Essen

The threat actor Vice Society has claimed responsibility for the ransomware attack against the University of Duisburg-Essen, Click to read more.

Azure Services SSRF Vulnerabilities Exposed Internal Endpoints

Orca Security published details on four server-side request forgery (SSRF) vulnerabilities impacting different Azure services. Click to read more.

Security Alerts

Microsoft Exchange Server Elevation of Privilege Vulnerability

Click to read more.

Critical Patches Issued for Microsoft Products

Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution in the context of the logged on user. Click to read more.