CYBER THREATS YOU CAN'T SEE

Hidden dangers in the digital world

Educational Community
ALLIANCE CREDIT UNION

EDUCACU.COM | 419-381-2323
3845 Angola Road, Toledo, OH 43615

THIS MONTH'S TOPICS:

Cybercriminals are no longer relying on loud, disruptive attacks to make an impact. Instead, they operate in the shadows, exploiting unseen vulnerabilities and infiltrating systems quietly. From sophisticated zero-day exploits to silent cryptojacking schemes, these invisible threats can cause massive financial and operational damage while remaining undetected for months.

As cybercrime costs continue to rise, organizations must shift their focus from reactive defense to proactive resilience. In this issue, we uncover the hidden dangers lurking in networks and explore strategies needed to strengthen security against unseen threats.

$ The Costs of Cybercrime $

1. **The total cost of damages incurred by cybercrime...**
is expected to reach $10.5 trillion by 2025. This number is up from $3 trillion in 2015.

Forbes

2. **The average cost of a data breach in the U.S...**
is the highest in the world, at $9.36 million.

Forbes

3. **The average cost of a data breach globally in 2024...**
was $4.88 million.

Forbes

4. **The cost of damage caused by cyberattacks globally...**
is around $16.4 billion a day – or $190,000 a second.

Cybersecurity Ventures

5. **The average cost of a healthcare data breach in 2023...**
was $10.93 million, higher than any other industry.

The HIPAA Journal

ZERO-DAY ATTACKS

Vulnerability	A zero-day vulnerability is a newly discovered flaw in software or hardware that remains unpatched, leaving it exposed to potential exploitation.
Exploit	After a vulnerability is discovered, an attacker can then craft a zero-day exploit. An exploit is a method or malicious software designed to take advantage of a security vulnerability.
Attack	With an exploit in hand, a malicious hacker can launch a zero-day attack on a business or organization.

SONY PICTURES ZERO-DAY BREACH

WHAT HAPPENED?

In 2014, Sony Pictures was targeted by a zero-day attack, crippling its network and exposing sensitive data. The attackers, using an unknown vulnerability, leaked confidential corporate information on file-sharing sites, including employee and family details, internal emails, executive salaries, and unreleased films. They also deployed a variant of the Shamoon wiper malware, erasing numerous systems across Sony's corporate network.

HOW WAS IT RESOLVED?

Upon discovering the breach on November 24, 2014, Sony Pictures took swift action by shutting down its network to prevent further damage. The company engaged the Federal Bureau of Investigation (FBI) and cybersecurity firm FireEye to investigate the intrusion and assist in remediation efforts.

SCAM OF THE MONTH: CRYPTOJACKING

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Mark Reynolds, an IT administrator at a financial services firm, noticed unusual slowdowns and overheating across employee workstations. After investigating, he discovered that a seemingly harmless browser extension, "SpeedBrowse Plus," had secretly installed a cryptojacking script. This malware hijacked system resources to mine Monero (XMR) cryptocurrency, operating stealthily to avoid detection. Employees experienced sluggish performance, and the company saw unexpected energy cost spikes, but antivirus scans showed nothing suspicious. A deeper network analysis revealed hidden connections to a remote mining server, confirming the attack.

By the time the cryptojacking was uncovered, the attackers had already mined thousands of dollars' worth of cryptocurrency at the company's expense, also causing hardware failures. To prevent future incidents, Mark's team enforced stricter endpoint detection, real-time monitoring, and banned unauthorized browser extensions.

DID YOU SPOT THE RED FLAGS?

- Unusual system slowdowns and overheating were concerning.
- Unexpected, increased energy costs raised a red flag.

STAY SAFE

HOW TO PROTECT YOURSELF

- Use task manager or activity monitor to spot unusual activity.
- Only install trusted extensions and software from official sources. Enforce company policies that limit downloads to IT-approved applications.
- Regularly update antivirus software and enable real-time threat monitoring to detect cryptojacking attempts before they spread.

Defense Tactics

STRENGTHENING CYBER RESILIENCE AGAINST SILENT BREACHES

Implement Robust Security Measures

Organizations should not blindly trust software vendors, as attackers often exploit legitimate updates and integrations to infiltrate systems. As businesses increasingly rely on interconnected software and services, they create more entry points for cyber threats. Strengthening supply chain security measures is essential to mitigate risks, detect potential breaches early, and prevent widespread damage.

Identify Critical Vendors

To effectively manage third-party risks, organizations must first determine which vendors are critical to their operations and incorporate cybersecurity requirements into their contracts. Continuous monitoring—through vulnerability assessments, penetration testing, and other security measures—helps detect risks in real-time. Rather than just enforcing compliance, businesses should collaborate with vendors to strengthen security, ensuring ongoing risk assessments beyond annual audits.

Clarify Third Party Contracts

Organizations should ensure that third-party contracts explicitly define security obligations, including mandatory patching timelines, multi-factor authentication (MFA), and logging requirements. Adopting a zero-trust approach—assuming any third-party access could be compromised—helps strengthen defenses. Additionally, incorporating privileged access management enforces strict access controls, limiting the impact of potential breaches and enabling a swift response by revoking or modifying access credentials when necessary.