

A Review of the 2023 Cybersecurity Landscape

From 1-Hit Wonders to Unrelenting Threats

In 1976, Thin Lizzy's iconic hit "The Boys Are Back in Town" climbed to the 12th spot on the charts and quickly became their signature tune. However, Thin Lizzy's claim to fame was short-lived, and they would forever remain a 1-hit wonder. While the music world moved on, cybercriminals embarked on a journey that would yield them continuous chart-topping success in the world of cyberattacks. Looking back at 2023, it's evident that cyberthreats never let their guard down, much like a timeless hit that keeps returning to the airwaves, slightly revised.

The Rise of Cyber Incidents

Since the early days of the Creeper virus in 1971, cyber incidents have been on the rise. In 2023, the cybersecurity landscape painted a bleak picture:

- **Phishing Dominance:** Phishing scams continued their reign as the most common form of cyberattack for the third consecutive year.
- **Business Impact:** A staggering 46% of cyberattacks impacted businesses with fewer than 1000 employees, underscoring the vulnerability of smaller enterprises.
- **Slow Response:** On average, it took 277 days to identify and contain a data breach, with an average cost of \$139,000 per claim.
- **Alarming Frequency:** In 2023, there was one successful cyberattack every 1.12 seconds, highlighting the relentless nature of these threats.
- **SMB Vulnerability:** The average financial impact of a breach for small and medium-sized businesses (SMBs) stood at \$98,000.

Preparation and Prevention

Despite the ever-growing threat landscape, not all organizations were adequately prepared to defend against cyberattacks. In fact, only 44% of companies had both a prevention and response plan for IT security incidents. Sadly, the prevailing mindset often treats cybersecurity as a backward-looking function rather than a forward-looking, value-added one.

Promising Developments

Amid these challenges, we see signs of hope. Gartner predicted that organizations that isolated or segmented their Internet of Things (IoT) devices would experience 25% fewer successful cyberattacks by 2023. This marked a significant step toward enhancing cybersecurity.

(Continued on page 3)



Take Note

Our Latest Hit!

Check out our website's fresh new look! It's now so amazing that we're sure it's going to hit the top of the charts. Have fun strumming through our updated design and enhanced features.

www.it-radix.com

February 7

WEBINAR

Tech Talk:

Boost Your Microsoft 365
Security in 2024

www.it-radix.com/webinar

Starts @ 12:10pm sharp

If you would rather receive our newsletter via email, sign up on our website or send an email to resource@it-radix.com



More free tech tips at:
www.it-radix.com/blog

Like a 1-Hit Wonder... One Phishing Scheme Nets Millions

Beware of QuickBooks Update Scams

Many of us remember a hit song called “Gangnam Style” by the artist, Psy. He is a great example of a 1-Hit Wonder. There is something to be learned from his success—you only need to hit it big once to make it big time. That song released in 2012 has given Psy a net worth of \$60 million!

Cyber thieves know well they need just one hit to make it big. That’s why now so many are using a scam about the false need to update software like QuickBooks. With so many relying on QuickBooks for efficient fiscal management, scammers love the “QuickBooks Update Scam.” The swindle features a fraudster posing as a representative of Intuit, QuickBooks’ parent company. They tell you that you must install an update. Other scams use the same tactics but use another software application as the reason for the call or email. This is just a ploy to extract sensitive information or spread malware. You must stay vigilant, understand the scammers tactics, then employ effective defensive strategies to counter these malicious attempts.

Beware of:

1. **Phishing Emails:** Fraudulent scam emails impersonating QuickBooks, Intuit or others claiming an essential software update is available, linking to deceptive websites that harvest credentials.
2. **Pop-Up Messages:** Pop-ups claiming necessary updates, which could install harmful software or grant unauthorized access.

3. **Phone Calls:** Unsolicited calls alerting users to fake security or performance issues, leading them to download malicious files or provide remote computer access.

How to avoid being victimized by a scamming 1-Hit Wonder:

1. **Verify the Source:** Ensure messages claiming to be from QuickBooks or Intuit or any provider are genuine. Validate email addresses, phone numbers, and website domains.
2. **Avoid Suspicious Links:** Refrain from clicking on questionable links in emails, pop-ups, or websites. Confirm updates and alerts directly through official provider channels.
3. **Enable Two-Factor Authentication:** Boost account security by enabling a second form of verification through a unique code sent to your mobile device.
4. **Educate Employees:** Inform staff about threats, emphasizing skepticism towards unexpected messages and the importance of source verification.
5. **Install Endpoint Security Antivirus Software:** Implement Zero Trust and Antivirus software to safeguard your computer systems from malware and attacks from nefarious players.

Avoid the pitfalls of these scams with IT Radix’s advanced security solutions that enhance security and protection against cyberthreats. Call us today to learn more about how you can avoid these and similar ruses.

Is Your Personal Info a “Hit” on the Dark Web Charts?



Just like a 1-Hit Wonder, it only takes one hit for a hacker to get your personal information on the Dark Web, and then it’s out there forever. Now is a good time to review if any of your credentials are found on the Dark Web.

Our 100% FREE and confidential Dark Web Scan is your first line of defense! Hopefully it will be ALL CLEAR and you can breathe easy. Sign up today for a free Dark Web Scan: www.it-radix.com/dark-web-scan

Cybercriminals will stop at NOTHING to steal your credentials. And once they have your password(s), it’s only a matter of time before they destroy your business and scare away your customers.

A Review of the 2023 Cybersecurity Landscape

(Continued from page 1)

Attack Vectors: The Greatest Hits

Cybercriminals continued to adapt and evolve, employing various attack vectors to breach systems and compromise data. Some of the most prominent attack tactics included:

- **Malicious Documents:** Globally, 38% of malicious email attachments were Microsoft Office formats, such as Word, PowerPoint, and Excel.
- **Archive Files:** Archive files like .zip and .jar represented around 37% of all malicious file extensions.
- **RedLine Stealer Trojan:** Cybersecurity experts discovered this Trojan being sold on hacking forums and the Dark Web for as little as \$150, posing a significant threat to personal data security.
- **Ecommerce Exploitation:** Small and medium-sized retailers became victims of formjacking code injection, highlighting the risks associated with online shopping.

Changing Motivations

Cybercriminal motivations underwent a shift, moving from mere financial gain to intelligence gathering. In 2023, 96% of targeted attacks aimed at intelligence gathering.

The Phishing Phenomenon

Phishing attacks reached their highest level in three years, with more than 30% involving keyloggers. Spear phishing was the most frequent targeted attack vector, affecting small organizations at a higher rate. Notably, over 95% of malware-distributing emails required human action.

Spam Stays Relevant

Spam remained a dominant force in email-based cybercrime. Cybercriminals manipulated feedback forms on large companies' websites to bypass spam filters and reach victims.

Cloud Solutions Hit Sour Notes

Cloud-based systems are now being targeted as more organizations shift from in-house, on-premises business applications to cloud-hosted systems. Monitoring,

detection and response solutions are emerging but are playing catch up.

Mobile Takes Center Stage

Mobile platforms became a primary target, with 70% of online fraud occurring through mobile devices. More than 90% of surveyed organizations experienced compromises involving mobile devices.

Cybercrime's Lucrative Earnings

Atlas VPN revealed that cybercrime earned criminals a staggering \$1.5 trillion annually, dwarfing the revenue of major corporations.

Protecting Against the Encore

As cyberthreats continued to evolve, businesses had to adapt. IT Radix recommendations for improving cybersecurity included:

- **Multi-Layered Defense:** Implementing a multi-layered defense strategy across systems, networks, programs, and data.
- **Employee Education:** Educating employees about data security principles, including strong passwords and email security.
- **Cybersecurity Framework:** Establishing a framework for dealing with cyberattacks.
- **Investing in Technology:** Utilizing technology to protect endpoint devices, networks, and the cloud.
- **Regular Updates and Patching:** Keeping all software and systems up-to-date.
- **Access Controls:** Restricting access to essential information.
- **Regular Audits and Testing:** Conducting cybersecurity audits and penetration testing.

In closing, unlike 1-hit wonders, cyberattacks have proven to be an enduring threat that demands constant vigilance and adaptation. As organizations face an ever-evolving cyber landscape, your ability to stay ahead of the curve will determine your resilience in the face of unrelenting cyber adversaries.

IT Radix is here to keep you tuned in to the ever changing "Top 100 Cyberattacks" chart. Let's talk about your cybersecurity landscape in 2024.

2023
YEAR IN REVIEW

Inside This Issue

- A review of the cybersecurity landscape in 2023
- How to stay a step ahead of scammers and avoid being a victim of their tactics
- Ask us how to get a free Dark Web Scan

IT Radix Family and Friends
321 Delighted Clients Drive
Geekville, NJ USA

"The beautiful thing about learning is that nobody can take it away from you."
— B. B. King

off the mark.com by Mark Parisi



From the desk of Cathy Coloff

This issue's cartoon made me laugh at myself. As someone who is constantly trying to be organized, keep a clean desktop, email Inbox and more, I find it extremely difficult to do in practice. With the wealth of information sources, a myriad of demands on my time, and just plain ol' procrastination, I find that my desks at home and at the office are often quite cluttered. Albert Einstein said, "Out of clutter, find simplicity."

While I'm still searching for simplicity, I have started making strong first steps. For example, I've streamlined my email filing system and am only keeping those emails that I truly need. I absolutely love using OneNote and have for years to capture notes, screen shots, and much more. It's "notebook-style" interface works well for helping me to organize information into tabs, topics, use personally customized tagging and much more. I also love the transcription features in many communications platforms such as Teams which help me focus on the conversation at hand and worry less about taking notes. If I do want to take notes, I can link the calendar entry to a page in my OneNote notebook—super cool but also very convenient!

As we enter a new year, I encourage you to look for ways to leverage your technology to simplify your day-to-day life. I wish you and your loved ones all the best in the upcoming year.

