CSU Connection August 2023

Serving our community for over 30 years

Our mission is to deliver outstanding IT support to your business in order to improve uptime, productivity. and profitability.

You take care of running your business, we'll take care of your technology.

in this issue...

Pg 1-2 Zero Click Malware
Pg 3 Tech Facts, Birthday Time, Gadget of the Month
Pg 4-5 Building a Remote Workforce, Tech Quiz
Pg 6-7 Tik Tok Safety Warnings
Pg 8 Sweet Times at CSU

> "It is better to fail in originality than to succeed in imitation."
>
> — Herman Melville

What is Zero-Click Malware?

In today's digital landscape, cybersecurity threats continue to evolve. They pose significant risks to individuals and organizations alike. One such threat gaining prominence is zero-click malware. This insidious form of malware requires no user interaction. It can silently compromise devices and networks.

One example of this type of attack happened due to a missed call. That's right, the victim didn't even have to answer. This infamous WhatsApp breach occurred in 2019, and a zero-day exploit enabled it. The missed call triggered a spyware injection into a resource in the device's software.

A more recent threat is a new zero-click hack targeting iOS users. This attack initiates when the user receives a message via iMessage. They don't even need to interact with the message of the malicious code to execute. That code allows a total device takeover.

Below, we will delve into what zero-click malware is. We'll also explore effective strategies to combat this growing menace.

Understanding Zero-Click Malware

Zero-click malware refers to malicious software that can do a specific thing. It can exploit vulnerabilities in an app or system with no interaction from the user. It is unlike traditional malware that requires users to click on a link or download a file.

The Dangers of Zero-Click Malware

Zero-click malware presents a significant threat. This is due to its stealthy nature and ability to bypass security measures. Once it infects a device, it can execute a range of malicious activities.

These include...

-Data theft
-Remote control
-Cryptocurrency mining
-Spyware
-Ransomware
-Turning devices into botnets for launching attacks

This type of malware can affect individuals, businesses, and even critical infrastructure. Attacks can lead to financial losses, data breaches, and reputational damage.

cont. on pg 2

Fighting Zero-Click Malware

To protect against zero-click malware, it is crucial to adopt two things. A proactive and multilayered approach to cybersecurity.

Here are some essential strategies to consider:

• Keep Software Up to Date

Regularly update software, including operating systems, applications, and security patches. This is vital in preventing zero-click malware attacks. Software updates often contain bug fixes and security enhancements.

• Use Network Segmentation

Segment networks into distinct zones. Base these on user roles, device types, or sensitivity levels. This adds an extra layer of protection against zero-click malware.

• Use Behavioral Analytics and AI

Leverage advanced technologies like behavioral analytics and artificial intelligence. These can help identify anomalous activities that may indicate zero-click malware.

• Uninstall Unneeded Applications

The more applications on a device, the more vulnerabilities it has. Many users download apps then rarely use them. Yet they remain on their device, vulnerable to an attack.

• Put in Place Robust Endpoint Protection

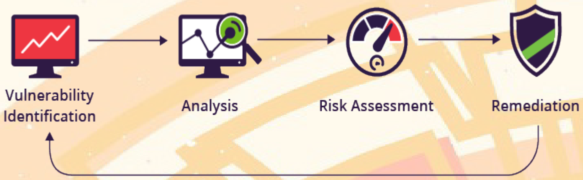
Deploying comprehensive endpoint protection solutions can help detect and block zero-click malware. Use advanced antivirus software, firewalls, and intrusion detection systems.

• Educate Users

Human error remains a significant factor in successful malware attacks. Educate users about the risks of zero-click malware and promote good cybersecurity practices. This is crucial. Encourage strong password management. As well as caution when opening email attachments or clicking on unfamiliar links.

• Conduct Regular Vulnerability Assessments

Perform routine vulnerability assessments and penetration testing. This can help identify weaknesses in systems and applications.



• Only Download Apps from Official App Stores

Be careful where you download apps. You should only download from official app stores.

Tech Facts

Did you know?

1. In the orginal Pac-Man, the red one was programmed to follow behind Pac-Man, the pink one in front, but the cyan ghost was designed to be unpredictable!

2. The most efficent keyboard layout is called Colemak, which is designed to reduce finger movements by half. It uses home row 74% of the time, compared to Qwerty's 34%

3. QR codes were invented in 1994. They were first used to track vehicles on the assembly line.

facts found on consultinnotek.com

Happy Birthday, Mike!

Celebrating another trip around the sun this month is our much loved and valued CSU employee and friend, Mike!

"Say what you mean, and mean what you say."

Some fun facts about Mike that you should really know...

1. His favorite movie is ***Pulp Fiction.***

2. His dream travel destination is ***Hawaii!***

3. If he could go on a game show, he would go on ***Jeopardy.*** **He believes he would likely come in 4th place.** Not too bad!

4. His favorite way to wind down after work is ***dinner and TV with his his wife & high school sweetheart, Jami.*** SO sweet!!

5. One trend Mike is glad is gone is ***the mullet.*** **Although, he is concerned about it recently making a comeback...**

6. If Mike were in the circus, he would like to be a ***clown.***

7. If he had an **extra hour** each day, Mike would spend it ***"sleeping in" (AKA laying in bed, wishing he was actually asleep)***, rather than rising with the early birds.

8. When Mike starts his next career in WWE, his entrance song with be ***"Welcome to the Jungle"***... oh SNAP!

9. If the apocolypse were happening, **Mike wouldn't take any 3 CSU employees on his team without first interviewing them for their skills.** Let's hope zombies look a lot like cyber-criminals.

10. He **doesn't have a favorite color.** But when asked, he says ***red.***

Gadget of the Month:

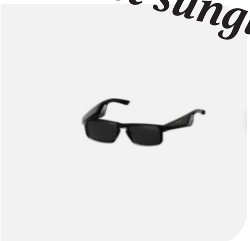
Bose Frames Soprano Audio Sunglasses

Thoughtfully refined and strikingly elegant, Bose Frames Soprano flaunt polarized lenses and premium craftsmanship, while exclusive Bose OpenAudio™ technology produces sound you'd never expect from sunglasses. It's a jaw-dropping experience that leaves you free to engage with the world around you, all while discreetly listening to music.

Get yours today at www.bose.com

"They're just sunglasses!"

Bose Frames Soprano have a rechargeable battery offering up to 5.5 hours of playtime, as well as an advanced microphone system and tap, touch, swipe controls for on the go, hands-free calls.



The Benefits (and Challenges) of Building a Remote Workforce for Your Business

While in the past, employees arrived at their offices in person, working from home has become increasingly popular since 2020. But is building a remote workforce a worthy investment for businesses?

Like other endeavors, it has its challenges and rewards.

Since digital infrastructure allows people to connect globally, businesses could hire top talent and improve flexibility with a remote team. Find out more about pros and cons of remote workforces.

The Rise of Remote Work in the Modern Business Landscape

Remote work has existed for well over a decade. The sharp increase in internet availability and collaboration tools has increased its prevalence even more. Yet, many employers still avoided fully utilizing it, viewing remote work with skepticism.

Only after the Covid-19 pandemic forced a large portion of the commuting workforce to work from home did remote work become a widely accepted option. Many business owners couldn't afford to lose weeks or months of productivity to prevent the spread of illness or comply with shelter-in-place orders. Thus, work-from-home policies became more commonplace.

Businesses Benefit from Remote Work Forces

By building a remote workforce, businesses can reap benefits that often translate to higher rates of productivity from employees.

Time Savings: Working from home eliminates the commute. Workers who don't commute can spend more focus and energy on their daily tasks.

Flexible Hiring: When hiring candidates for a remote workforce, companies don't need to limit the pool of candidates to people nearby. Businesses can choose the best applicants from a much broader pool.

Cost Savings: Depending on a business's needs, renting a big office space may not be necessary. With partially or fully remote workforces, companies save money on real estate. In short, remote work **saves companies money and increases employee satisfaction.**

Challenges of Building a Remote Workforce

All good changes still come with their challenges, and remote work is no different. Once a company hires remote staff, teams may need to develop a different type of infrastructure and evolve with the business's needs. Some business owners are woefully unprepared for the infrastructure differences and constant adaptation. Some challenges of remote workforces include:

-**Strong daily communication** is a must. Finding the best communication methods for a company's operational needs can be a struggle.

-Since employees operate remotely, management might struggle to build a culture or support their needs.

-To ensure that staff continue developing and improving, managers will need to **identify and track metrics that measure their progress**.

-As business-oriented technology advances, so does technology that victimizes businesses. **Implementing strong security measures and data protection strategies** requires research and attention to detail.

Tips to Build and Manage a Remote Workforce

Here are a few ways you can circumvent some common challenges of building a remote workforce:

1. Integrate software solutions that facilitate daily communication, project management, and productivity tracking.

2. Use applications like Slack to encourage company culture through conversation and file sharing on a more casual level.

3. Develop strong internal security measures or outsource security work to another company.

Building a remote workforce offers numerous advantages to businesses across various industries. It can boost productivity, provide access to a wider talent pool, and generate cost savings. While challenges exist, such as effective communication and maintaining company culture, these obstacles can be overcome with the right strategies and tools. By embracing remote work, businesses can unlock new opportunities for growth, innovation, and employee satisfaction. As the business landscape continues to evolve, investing in a remote workforce is increasingly becoming a strategic imperative for long-term success.

Tech Quiz Time!

No cheating!

1) Which search engine almost bought Google in the 90's?

2) What was the world's first widely-used web browser?

3) In computing history, who were the dirty dozen?

4) What are Android releases named after?

5) In old PC's what was the function on the Turbo button?

1) Excite
2) Mosaic
3) Engineers who created the first IBM PC
4) Sweets and desserts
5) Strangely, it made the computer run slower so it could run software designed for slower machines

How To Stay Safe on Social Media: A Series

Part 3: TikTok

The ”Influencers aren’t happy but many governments, including our own think that TikTok is a huge threat to your privacy and security. The FBI and Federal Communications Commission officials have warned that ByteDance could share TikTok user data — such as browsing history, location, and biometric identifiers — with China’s authoritarian government.

Authorities in North America, Europe and Asia-Pacific have banned the TikTok app, mostly on government-issued phones or devices used for official business, citing cybersecurity concerns.

Among the information that they collect:

- Any information you add to your profile, like age, language, phone number, photo, and email address
- Any information it can gain from third-party accounts (like Facebook or Google) you link to your TikTok account
- Any content you upload, like photos and videos
- Information it can find about you from other “publicly available sources”
- Information about what you searched for on TikTok
- Information about your phone, including your IP address, your mobile carrier, time zone, and app and file names found on your phone
- Keystroke patterns or rhythms
- Location data
- Messages you send and receive from other users

TikTok (continued)

Once TikTok has your information, the company uses it. Some of the uses include tailoring what type of TikTok videos show up in your FYP (For You Page) and learning how to target you with ads. Tik Tok also shares your information with third parties.

Concerns around TikTok were heightened in December when ByteDance said it fired four employees who accessed data on journalists from Buzzfeed News and The Financial Times while attempting to track down the source of a leaked report about the company.

SCAMS? Yes, The Federal Trade Commission (FTC) considers TikTok a goldmine for scammers. TikTok has many of the same scams that other social media apps have: **Romance Scams, Investment Sams and Phishing Scams** abound. Follower or like scams are where the messenger promises that, for a low fee, they'll boost your followers or video likes to make you look like a TikTok star. Just block them and report them for spam.

Finally, **beware of TikTok trends**. TikTok is a breeding ground for dangerous trends like the BORG drinking trend. If you have a kiddo or teen on the app, be sure to stay on top of the latest trends and talk to your child about them.

Sources and additional information:

- **Why TikTok's security risks keep raising fears** (https://apnews.com/article/tiktok-ceo-shou-zi-chew-security-risk-cc36f36801d84fc0652112fa461ef140)
- **Why TikTok is being banned on gov't phones in US and beyond** (https://apnews.com/article/why-is-tiktok-being-banned-7d2de01d3ac5ab2b8ec2239dc7f2b20d)
- **Is TikTok Safe?** Here's what you need to know (https://www.safewise.com/is-tiktok-safe/)

Our Services:

-Data Backup & Recovery
-Managed Services
-IT Consulting
-Network Security
-Cloud Computing
-Remote IT Services
-Cyber Security Training
-Mobile Device Management

We believe that experienced, reputable and fast responding IT support should be the standard.

CSU COMPUTER SERVICES UNLIMITED

What's Happening at CSU?

Lots of Sweetness. Literally

In honor of both International Ice Cream and Sour Candy Days, we decided to celebrate. ***It was a rush!***

We decided that Sour Patch Kids extreme are the most sour candy. Although nothing beats Warheads. Beware!

Sour Candy Day July 18th

National Ice Cream Day July 16th

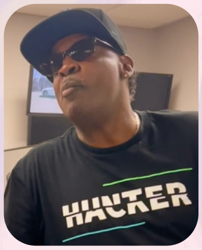
Guess the flavor!

Chuck guessing his favorite flavor!

No one guessed a single flavor correctly... it was still delicious at least.

Will thinking hard

The culprits that stumped us.



Check out everyone's sour faces!!

Vote for your favorite on our Facebook page and stay tuned for the winner!

Get connected with us!

Instagram:
computer_services_unlimited

Facebook:
Computer Services Unlimited Inc.

Phone:
(703) 968-2600

Coffee Break:
www.csuinc.com/coffee

Digital Version of Newsletter:
www.csuinc.com/news