# Q-News

*April 2022*

## A Word from Jack

"The Times They are a-Changin'." This quote by the famous philosopher Bob Dylan is just as relevant today as it was in 1964 when the song was released. Last month there was an unprecedented move by the FBI to remove malware that was created in Russia. The malware affected many business firewalls. The FBI was able to reverse engineer the Russian malware, and use the techniques in the malware, to gain access to affected systems. Using this technique, the FBI was able to remove the malware. What else is changing? Not long ago if you wanted a program like Microsoft Word, Excel, Adobe, QuickBooks, it was simple. You could just purchase the product, install it, and use it. Software vendors, with little to no exception, are all moving to an annual or monthly recurring licensing mode. Microsoft has recently announced a new pricing model that will require customers to make a 12-month commitment on their licensing count. All new clients to Microsoft 365 platform now have to purchase licenses under this new program. Existing Microsoft cloud clients can continue under their current agreement, but they can expect to be forced into the new model within the next 12 to 24 months. The ink is barely dry on the new program, and we are working with our suppliers to fully understand the impact and timeline. The other big challenge is the tremendous amount of consolidation of service suppliers. Cloud backup providers, security service providers, network management providers are being bought up by large private equity companies. These are very interesting times to be in the IT industry and it will be interesting to see how things shake out in the next few years.

## LinkedIn Phishing

Hackers are using LinkedIn business tools to create convincing and legitimate phishing links. LinkedIn has a legitimate tool that allows businesses to create LinkedIn URL links that link to an outside site. These links have been deemed "Slinks" because the URL code used includes the word. The generic format is "https://www.linkedin.com/slink?code=" followed by numbers and letters.

Criminals are setting up new LinkedIn business accounts, or using hacked accounts to send Slink links in a variety of scams. There are examples of Slinks that point to fake IRS pages, Amazon logins, and PayPal phishing pages. Generally, these attacks are phishing for login credentials or personal information and are dispersed through SMS text message, email, and instant messenger.

Slinks are an effective phishing tool because LinkedIn is widely viewed as a trustworthy site, so spam filters are unlikely to block the links. Additionally, with many people working from home, and looking for remote work, the tactic could be used in a variety of attack vectors. Early in the pandemic, we reported on ways LinkedIn was being used to attack employees who were new to a remote job. The attackers posed as the new hire's IT support, and were able to steal business login credentials in the attack.

LinkedIn is also used to scrape personal information from users. The site faces a difficult balance of public information for the benefit of the job seeker, and that same information being used to target an individual for an attack. Click here for our blog on LinkedIn scraping.

Like most phishing attacks, criminals use a sense of urgency to try to get users to click the link. Be on the lookout for emails that look legitimate, and could make it through your spam filter using linkedin.com as the root URL. If the email or text message is threatening a grave consequence if you don't click the link right away, this should be a red flag to stop, consider the source, and check the legitimacy in another way.

Quanexus™
571 Congress Park Dr.
Dayton, OH 45459
937.885.7272
quanexus.com

# The US Removed Russian Malware Worldwide

The United States said it secretly removed malware from computers around the world in an attempt to head off a Russian cyberattack. The malware allowed Russia to create botnets which are typically used in DDoS attacks to overwhelm websites or services. Read our blog post here on DDoS Attacks.

US Attorney General Merrick Garland made the thwarted attack public saying, "It does not matter how well you conceal your assets. It does not matter how cleverly you write your malware or hide your online activity. The Justice Department will use every available tool to find you, disrupt your plots, and hold you accountable."

A Russian-linked hacker group installed malware on networking devices built by WatchGuard Technologies and ASUSTek Computer. The companies were aware of the command-and-control system distributing malware and informed their customers to patch and update the network devices. Instead of relying on the customer to patch the routers and firewalls, the DOJ went to the source and removed the underlying malware and reconfigured the devices that allowed the hacker group to control the botnet.

The FBI said it launched an awareness campaign to inform WatchGuard users to patch and update their systems, but less than half of the devices had been updated to the necessary level to keep hackers out.

The botnet could have been used for surveillance or to attack critical infrastructure. American officials said they were not interested in waiting to find out what Russia was planning to do with the fleet of infected network devices. Weeks ago, the Federal Government warned businesses to fortify cybersecurity practices based on intelligence, apparently at the same time they were taking this botnet offline.

"Through close collaboration with WatchGuard and our law enforcement partners, we identified, disrupted and exposed yet another example of the Russian GRU's hacking of innocent victims in the United States and around the world," U.S. Attorney Cindy Chung said in a statement.

# DDoS Attacks on the Rise

Distributed Denial of Service (DDoS) attacks are getting smarter and increasing in every available vector in 2022. This style of attack was up 434% in 2021 over the previous year. Additionally, targeted smart attacks were up 31% and multi-vector attacks were up 73%. US Banks were targeted the most, but the healthcare industry, remote learning and education, and technology companies also ranked high on the list of targeted demographics. The United States also tops the list of targeted countries at 54% followed by India and Europe.

Microsoft released details over the weekend of a new record-breaking DDoS attack they fended off. The attack peaked at 3.47 Tbps and came from 10,000 sources across 10 countries. DDoS attacks occur when hackers use compromised devices connected to the internet to overload a targeted server, website, or network. IoT devices are one category of devices that can be weaponized. Read our recent blog post on IoT security here.

Criminals are also using compromised servers to amplify attack numbers causing new attacks to still break records. Hackers use open DNS resolvers to filter the data through and increase the size of the attack hundreds of times the original size.

While a DDoS attack is not a data breach, it can act as a diversion for a ransomware attack. The attacks are becoming more targeted, so criminals could use a DDoS attack to divert IT resources to give hackers more time in the network to steal and encrypt data. Typically, DDoS attacks intend to deface company or government websites, create financial hardship, or disrupt web traffic. Lately, hackers have been targeting online gaming servers because a disruption of just a couple of seconds can have a detrimental outcome in an online multi-player game.

No business is too small to be attacked. It's important to understand the threats of a DDoS attack and discuss options with your MSP to keep from becoming an easy target. Some best practices include up-to-date firewalls, understanding your bandwidth need, and monitoring tools to alert you of an attack.

# SIM Swapping on the Rise

The FBI issued an announcement to warn consumers of the increase of complaints of hackers stealing money through SIM swapping. SIM swapping is not a new hacking technique, but the reports of attacks have increased exponentially over the past year. The FBI received 1,611 complaints that resulted in $68 million being stolen in 2021. This is a dramatic increase compared to only 320 complaints in the previous three years combined.

SIM swapping is a technique used by criminals to gain access to a targeted mobile phone. Hackers convince mobile phone carriers to swap service from the target's phone to a SIM card controlled by the criminal. Criminals use phishing techniques to get the personal information needed to impersonate the user to the phone company and authorize the transaction. Once the SIM has been swapped, the criminal has access to the user's phone calls and text messages. Then they can perform a password reset on bank accounts or other high-profile accounts with two-factor authentication. Criminals are primarily targeting user bank accounts and cryptocurrency accounts.

The FBI released some tips on how to protect yourself from SIM swapping including the following:

- *Do not provide your mobile number account information over the phone to representatives that request your account password or pin. Verify the call by dialing the customer service line of your mobile carrier.*

- *Avoid posting personal information online, such as mobile phone number, address, or other personal identifying information.*

- *Use a variation of unique passwords to access online accounts.*

- *Be aware of any changes in SMS-based connectivity.*

- *Use strong multi-factor authentication methods such as biometrics, physical security tokens, or standalone authentication applications to access online accounts.*

SMS-based two-factor authentication is the easiest method for extra security, but it's also the most vulnerable to SIM swapping hacks. The US government recommended companies move away from SMS-based authentication in 2017, but companies have been slow to react. However, any form of two-factor authentication or multi-factor authentication is better than none at all. You should always use MFA/2FA if it is an option, especially on your more important online accounts.

# Kaspersky Antivirus Banned by FCC for Federal Subsidies

The US Federal Communications Commission (FCC) added Russian cybersecurity company and anti-virus provider Kaspersky to the list of companies "deemed to pose an unacceptable risk to the national security of the United States." This was the first time a Russian company had been added to The Secure Networks Act list comprised only of China-based technology and telecom companies before the Kaspersky addition.

The move by the FCC bars Kaspersky from receiving federal subsidies.

This is not the first time the Federal Government has pushed back on Kaspersky. In 2017, the US removed Kaspersky from the approved list of anti-virus manufacturers that could be used on US Government computers or networks. The US Dept. of Homeland Security said, "This action is based on the information security risks presented by the use of Kaspersky products on federal information systems," and issued a directive to remove all Kaspersky products within 90 days. The FCC said its decision to add Kaspersky to the banned list was motivated by the actions and response in 2017.

Kaspersky responded with a statement that reads, in part, "Kaspersky is disappointed with the decision by the Federal Communications Commission. This decision is not based on any technical assessment of Kaspersky products — that the company continuously advocates for — but instead is being made on political grounds."

# Don't Make it Easy for Criminals to Attack You!

## Hacker Reconnaissance 101:

Oversharing information is a huge issue for every organization. The oversharing of information can make your organization an easy target to hack.

Hackers are constantly monitoring all forms of social media as part of their mission. To illustrate this problem, I'll use a "fictitious example".

Suppose you work for a bank, and you are excited about a new software platform that the bank will soon be installing. You post on your Facebook and LinkedIn page all the great features that the bank will now be able to offer, and how it will benefit the bank's clients. This type of information is interesting to your friends and clients, however it is very exciting to a criminal.

A hacker with this knowledge will now start stalking you and others in the company. The criminal now has several goals. First, they want to find out who is working on this project and then learn as much as they can about each person. The second step is to learn as much as they can about the project and the details of the installation and migration process.

Next, the criminal will likely reach out to you and some coworkers using a fictitious identity and attempt to join your LinkedIn network and possibly friend you on Facebook. Creating a fictitious identity that would tempt you to accept a friend request is an easy task. The criminal's goal at this point, is to determine who most likely will fall for a social engineering attack. (Social engineering is getting someone to do something they would not normally do).

With all the acquired information, the criminal is now ready for the attack. The most likely attack vector the criminal will choose, is to call the victim during the installation or data migration phase of the project. They will impersonate a team member of the company performing the project ask for help with getting access to the system. Sometimes to make it appear more legitimate, they may send an email or call ahead of time to schedule an appointment to work on the project.

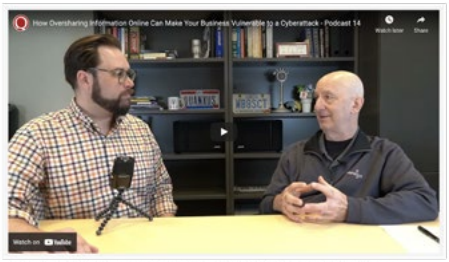
Companies need to be aware of and have polices that limit the amount of company information that employees are allowed to share on their personal social media sites. Employees also need to understand that by oversharing personal information makes them and the company they work for more likely to a potential attack.

## Podcast

**We have two new short Podcasts out this month. Jack and Chuck discuss The CIS 18 Cybersecurity Controls and How Oversharing Information can make your business Vulnerable to an online attack.**

CIS 18 Cybersecurity Controls and Cyber Insurance

[Click Here for Podcast- CIS 18 Cybersecurity Controls]



Oversharing can make your Business Vulnerable

[Click Here for Podcast- Oversharing Information and Cybersecurity Vulnerability]


Quanexus™

571 Congress Park Dr.
Dayton, OH 45459
937.885.7272
quanexus.com


## Follow Quanexus on Social Media!

Find Quanexus on Facebook, Youtube, LinkedIn, and Instagram! Click on the buttons below to access our social media pages. Like, comment and subscribe!

Also, subscribe to our email list to regularly receive tech news, cybersecurity alerts, and information on upcoming events. **Visit Quanexus.com to sign up!**

@Quanexus571 @Quanexus @Quanexus @Quanexus571 @Quanexus571