Q-News

March 2023

A Word from Jack

After 30 wonderful years in this industry, I have decided to take a break. My official retirement date is scheduled for March 31, 2023. As I marvel at how much things have changed in 30 years, the following things come to mind. Coax cable (Thinnet and Thicknet) was used for ethernet connections and ran a speed of just 10 Mbs. The alternative to ethernet was IBM's Token Ring, which gave us speeds of 4 Mbs or 16 Mbs. Typical network speeds today are at least 100 times faster and continue to increase. Email was at its infancy stage and cell phones were only used to make calls, not texting, email, and certainly not videos. Passwords were kept in a rolodex or taped under the keyboard, and cybercrime was not a major concern. There was no spam, or ransomware, and building a network was a complex process versus today. Today, you just buy some cables, a switch and a router and you're done. There are job titles and positions that could never have been imagined 30 years ago. Now, looking into the future, the next big thing on the horizon is artificial intelligence (AI).

It has truly been an awesome experience being in this industry and helping our clients adopt and grow by implementing technologies that have brought value to their organizations. Another wonderful experience from owning a business is getting to help team members learn and grow. There have been many to pass through the ranks of Quanexus, and some have gone on to do great things in the industry. I am very proud to have been a part of their journey.

My advice to young people in our industry is, don't stop learning and keep an eye on future trends. I've often described/compared the value that an individual brings, either to a client or to the company, as that of a fruit in a grocery store. No one buys old rotting fruit; you need to keep your skillsets fresh and relevant in order to be successful. If you are in this industry, you have chosen a career, not a job just eight hours a day, five days a week. Being a part of this industry is a commitment to continual learning.

To all the great clients I've gotten to work with and to all the wonderful team members at Quanexus, past and present, I want to thank you for an awesome 30+ years and wish you all great success!

Jack

Calendar Invitation Phishing

Criminals are using calendar invitations to launch phishing attacks and break through email filtering. Over the summer, we saw a new phishing tactic used against the corporate world to steal employees' login credentials. Criminals used compromised email addresses to send employees meeting invites with malicious links in the body of the invitation disguised as a virtual meeting link. The attack vector has recently worked its way down to individuals at such a rate that Google had to take action last week.

Many phishing attacks use Microsoft documents or PDFs as part of the attack because they will typically make it through email filtering. A calendar invite attack uses a .ICS file for the same reason. Some email clients will even add a calendar invite to a user's calendar before they respond to the invite. The attacks are even more convincing now that virtual meetings are the norm in the workplace, and employees are regularly invited to unusual virtual meetings.

The tactic was used extensively in the first part of the year against personal user accounts to the extent that Google took action and added calendar invitations to their list of automatically filtered spam just last week. Users can also change account settings so only calendar invitations from known contacts automatically appear on their calendar. Calendar invitations from unknown users will still appear in the user's email inbox but will not be added to the calendar without accepting the invitation.

Hive Ransomware Shut Down

The FBI shut down the Hive ransomware hacker's servers and website after working inside the group since July. During that time, they retrieved over 300 decryption keys and passed them on to current victims of Hive ransomware to unlock data and workstations. They also gave more than 1000 decryption keys to previous Hive ransomware victims. The FBI was able to help schools, hospitals, and businesses hacked by Hive ransomware with decryption keys and enable them to unlock their data without paying a ransom.

"We turned the tables on Hive and busted their business model, saving potential victims approximately $130 million in ransomware payments," Deputy Attorney General Lisa Monaco said during a press conference.

Hive used a Ransomware-as-a-Service (RaaS) model utilizing hacker affiliates to hack schools and businesses and then took a percentage of the ransom off the top. The group also had a website where they published stolen data if the victim refused to pay. Hive used multiple attack vectors to infiltrate networks, including email phishing, authentication token vulnerabilities, and VPN access only protected by single-factor authentication. Once inside the network, affiliates shut down security software, delete logs, and encrypt sensitive data. The group used a double extortion model to encrypt data and lock system workstations, so they could not be used. According to the FBI, the Hive ransomware group was categorized as a top-five threat. Click here to read our previous blog post on Hive ransomware.

Through their investigation and discovery of decryption keys, the FBI noted that only about 20% of victims had reported their attack to the FBI. Ransomware groups typically threaten further harm if law enforcement is contacted after an attack. However, the investigation and infiltration were only successful because of victims who reported incidents and worked with law enforcement authorities worldwide.

Healthcare Sector Ransomware

A recent ransomware claim in the healthcare sector is a reminder of ransomware tactics used by criminals. Hackers associated with BlackCat ransomware added NextGen Healthcare Information Systems to their list of compromised businesses last week. The attack is another example of hackers' focus on the healthcare sector, the highest category to experience attacks over the past few years.

A spokesperson from NextGen responded, "NextGen Healthcare is aware of this claim and we have been working with leading cybersecurity experts to investigate and remediate. We immediately contained the threat, secured our network, and have returned to normal operations. Our forensic review is ongoing and, to date, we have not uncovered any evidence of access to or exfiltration of client data. The privacy and security of our client information is of the utmost importance to us." The company did not comment on employee or patent data.

BlackCat is a prolific ransomware that focuses primarily on the healthcare sector. The group uses triple-extortion tactics to convince victims to pay ransoms by threatening to leak the data if they refuse. The group also utilizes DDoS attacks to knock victims' websites offline.

The healthcare sector is a particularly enticing target for hackers because of the personal patient data they store, and the inconsistency of security tools employed by healthcare companies. However, early data shows ransomware payments were down nearly 40% in 2022 across all business sectors. Researchers speculate businesses are investing in security and backup tools and are able to recover from an attack without paying the ransom. Another factor in the decline is that paying a ransom may not be legal in the business's home country. The US government has imposed sanctions on some foreign countries, restricting the export of money and products. If the ransomware group has ties to one of those countries, the company could find itself in legal trouble after recovering its data.

Experts predict the recent decline in payment will prompt ransomware groups may forgo medium-sized businesses with more security measures in place. Instead, they believe hacker groups will get more aggressive with very large and small companies to make up for the difference in revenue loss over the coming year.

Phishing-Resistant MFA

The US Cybersecurity and Infrastructure Security Agency (CISA) published a fact sheet for businesses and industry professionals on phishing-resistant multi-factor authentication (MFA) implementation. MFA is an extra step beyond a password to access an account or information. Traditional MFA notifications via text message are susceptible to SIM swapping or push bombing. Both attack vectors take advantage of people who can be persuaded to hand over credentials through phishing.

"CISA strongly urges all organizations to implement phishing-resistant MFA as part of applying Zero Trust principles. While any form of MFA is better than no MFA and will reduce an organization's attack surface, phishing-resistant MFA is the gold standard and organizations should make migrating to it a high priority effort," CISA notes in its tip sheet.

Phishing, by definition, takes advantage of people, so phishing-resistant MFA seeks to remove the human factor from the authentication process.

The fact sheet highlights two phishing-resistant authentication methods, FIDO and PKI. FIDO is the most widely available method and can utilize physical tokens, embedded mobile or laptop authenticators, or biometric authenticators. PKI-based authentication is less common in public but is the primary form of MFA used by the government, with smart cards used to unlock computers.

The fact sheet highlights how businesses should start thinking about phishing-resistant MFA implementation. High-priority targets like email systems, file servers, and remote access systems are most commonly targeted by hackers and should be protected first. Business owners should also think about protecting high-value users first. Employees with access to customer personal identifiable information (PII), like system administrators, attorneys, and human resources staff, should be at the top of the list of implementations.

Clone Phishing

Clone phishing attacks are a new type of social engineering attack that can be more difficult to detect than typical phishing emails. Clone phishing attacks generally use a clone of a legitimate email to entice users to click a link or enter information. A standard clone phishing tactic would be an email that looks like it's from PayPal on the same day of the month you typically receive your account balance notification. The email would look exactly like the one users receive every month and might even show a high or past-due balance to create urgency and make users more likely to click the link.

Another form of clone phishing can be a follow-up to an initial email. Clone phishing emails can appear to come from a company or colleagues inside your business if a business email compromise (BEC) has occurred. Hackers will resend the previous email and refer to updated links or resources in the new email. Since the attack is based on a previously received email, users are more likely to click on the new email to see what changed. Cloning the original email creates a more trusting environment where users are less likely to check links or email addresses. In the event of a business email compromise, the email could come from a real and trusted email address, increasing the likelihood that users will click the malicious link.

Like other phishing campaigns, the malicious links ask for personal information, login credentials, or credit card information which should be the first red flag for users. Criminals are also using clone phishing tactics to install malware which can be more challenging to detect.

Users should be aware of this new phishing tactic and be reminded to 'think before you click' especially during the holiday season. Like other phishing tactics, criminals try to create urgency with clone phishing to steal data.

Insider Security Threats

A new report reveals that the growing use of cloud data makes insider security threats more difficult to detect and prevent. Insider security threats affect more than 34% of businesses and have increased by 47% over the past two years as many industries move to cloud storage.

Most insider security threats come from negligence. Only about one-third of insider threats come from malicious or disgruntled employees or contractors looking to do damage. The other two-thirds of threats are due to users disobeying security rules for convenience or human error. These users may store confidential data on personal devices or share passwords to make their job easier. Negligent users may also share data with a criminal in a phishing attack.

Malicious insider threats include former employees who steal data during their offboarding process or current employees working with third-party organizations seeking to harm the company.

Storing business data in the cloud introduces new insider security threats that may not have been an issue on physical servers. Many businesses are adding cloud storage without an understanding of segmentation, monitoring, and access controls.

Education is the first line of defense against insider security threats. Businesses should have clear guidelines on personal device use, including USB drives, and those policies should be communicated regularly to employees. A large percentage of insider data breaches occur from an employee trying to make their job easier, so it's essential to communicate how confidential and privileged data should be used.

Next, users should only have access to the data they need to perform their job. The Principle of Least Privilege is still important in cloud data management and is an aspect of security that's being overlooked in the transition online. Businesses can also implement tools that restrict the copying and transferring of data, so users can access assets to do their job but cannot move them.

Lastly, pay attention to third-party vendors. Often vendors are granted access to cloud data, which may not have the same security policies in place as the original organization. Additionally, the data transfer method to the third party is another avenue for a breach.

Podcast

We have two new short Podcasts out this month. Jack talks about EDR/XDR and SIEM Solutions for Small and Medium Sized Businesses

Click Here for Podcast- SIEM Solutions for Small and Medium Sized Businesses

EDR and XDR Cybersecurity - Endpoint Detection and Response and Extended Detection and Response
Watch later
Share
MORE VIDEOS

Click Here for Podcast- EDR and XDR Cybersecurity

Quanexus®

Partner of BLUE ALLIANCE IT

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!**

f	🐦	in	◎	▶
@Quanexus571	@Quanexus	@Quanexus	@Quanexus571	@Quanexus571