Q-News

November 2022

A Word from Jack

A Season to be Grateful

As we enter the holiday season, I take time to reflect on the previous year. Things that went well and things that could have gone better. But at the end of the day, I am grateful for all the positive and negative experiences that I have encountered. Being grateful for the positive experiences is easy, but taking the lessons learned from the other experiences can also be positive. Afterall, it is a mix of all our experiences that make us who we are and any change in our past experiences might have put us in a different place in life. One of the things that I am truly grateful for is the wonderful team that I get to work with every day. Their dedication to taking care of our clients is top notch and it is an honor to work with the team.

I am also grateful for all our clients who trust us to assist them with managing their network environments. While at times being a service provider can be more than a little challenging, the satisfaction of keeping our clients operational and safe during these challenging times is very rewarding.

Wishing everyone a happy, healthy, and safe holiday season!

Jack Gerbs, Founder/Advisor

IoT Federal Rating

The Federal Government is taking steps to assign Internet of Things (IoT) devices a security rating similar to how they give Energy Star Ratings to energy-efficient products. IoT devices are any "smart" devices that can connect to the internet and interact with apps or other devices. Read our blog post on IoT devices here. These types of devices in the home are increasing rapidly. Everything from refrigerators to thermostats and door locks can be connected to the internet and are subject to security compromises.

The security of IoT devices is particularly timely now because of the rise of DDoS attacks we have seen over the past few weeks. Compromised IoT devices are commonly used to create botnets that can be weaponized and pointed at websites or businesses to disrupt traffic and take down services temporarily, like we saw fifteen airports deal with. Securing IoT devices is the first step in making the devices unavailable to criminals looking to weaponize devices.

Many devices are sold with a default password to help users with setup. The instructions typically tell consumers to change the password, but few follow the steps needed to secure the device. Leaving the default password opens the device up to multiple compromises. In the case of a camera, the criminal could view or control the device. In the case of a router, the compromised device could serve as a jumping-off point for criminals to explore the network looking for personal or financial information. Lastly, as cited above, the compromised device could be added to a botnet and used to attack other businesses or websites.

The Federal rating would help consumers choose more secure devices that have passed the credentials needed for approval. The Federal label would seek to secure IoT home cameras and routers first to secure the most critical and at-risk devices.

Quanexus™

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

Ransomware as a Service

Ransomware as a Service (RaaS) is a hacking business model built on the framework created by Software as a Service (SaaS). Users do not need to be skilled in hacking or dispatching ransomware in order to use the tools and attack businesses. Many RaaS kits are built like professional tools with 24/7 support, user reviews, and forums like one would expect from professional SaaS tools.

The hacking portals may also offer a live view of the ransomware attack including total encrypted files, and total payout. The popular tools are growing in popularity on the dark web, and have some large attacks attributed to them. The ransomware group attributed with the Colonial Pipeline attack, that caused gas shortages on the east coast last year, has a RaaS branch. A different ransomware group attributed with the JBS meat processing plant attack last year, also has a RaaS service they offer on the dark web.

As large ransoms are paid, and the attack vector continues to grow, RaaS is also growing in popularity. Some RaaS tools charge a monthly fee, while others take a percentage of the ransom as a cost for using the hacking tool.

Ransomware typically starts as a phishing attack to steal business credentials. Once inside the network, the malware will disable defenses like antivirus and firewalls and look for vulnerable endpoints in order to access other parts of the network. After the entire network is mapped, the malware begins to encrypt or steal business data. RaaS opens up new vulnerabilities to business competitors or disgruntled employees.

Preventing RaaS attacks follows the same process as our Q-Stack. A serious backup practice including offline backups, processes to patch and update systems regularly, and user awareness training are all important steps in a larger security program.

Phishing as a Service with MFA

A hacking group is getting attention for combining two of the recent attack vectors we have covered on the blog. EvilProxy is in the news for offering Ransomware-as-a-Service (Phaas) along with the ability to bypass Multi-Factor Authentication (MFA). We explored Adversary in the Middle (AiTM) attacks just a couple of weeks ago; now, the method is being used for a fee to compromise accounts associated with Apple, Facebook, Google, Microsoft, Twitter, and Instagram.

EvilProxy uses a similar process as other adversary in the middle attacks. The attack starts with a phishing campaign. When the user clicks the link, they are directed to a page that looks like the Microsoft or Google login page being spoofed. The fake phishing page forwards the credentials to the actual site like Microsoft and Google.

This is the first place the attack vector differs from a typical phishing attack. By passing the credentials on to the actual site, the phishing page will determine if the username and password are correct and if the user has MFA enabled for the account. If the username and password check out, the MFA request is transferred back to the user, who answers the security question as they normally would.

The second place these new tactics are different from a typical phishing attack is the capture of cookie data when the MFA request is sent back to the user. This method allows hackers to continue logging into the account without authentication because they captured the login session. This means they can continue to access the email, Facebook page, or Twitter account without triggering an MFA request.

EvilProxy is monetizing the technique for as little as $400 per month. Research also suggests they are targeting software developers and IT engineers to gain access to more services to expand the list of companies they can attack.

What is AiTM Phishing - Back to Basics

Adversary in the Middle (AiTM) attacks are advanced phishing attacks where user credentials cookies are compromised. The result of these next-generation attacks is MFA, or 2FA can be compromised. Multi-factor Authentication (MFA) and Two-factor Authentication (2FA) require an additional authentication source other than a password. Often the second authentication factor is a text message or an authentication app on the user's cellphone. An AiTM attack can circumvent the MFA/2FA by caching the session and returning to the compromise through the session cookies. This method has recently become a popular attack vector for Microsoft 365's email services.

"Note that this is not a vulnerability in MFA," says Microsoft. "Since AiTM phishing steals the session cookie, the attacker gets authenticated to a session on the user's behalf, regardless of the sign-in method the latter uses."

The phishing campaign begins in a typical way with an email asking users to log into a fake website that looks like a Microsoft 365 login page. The difference in these sites is they are proxies and pass the login on to Microsoft and relay the response back to the user. The use of a proxy is the first differentiation between a typical phishing attack and an AiTM attack. Usually, the attacker is trying to steal the login credentials. Instead, the proxy site steals the credentials and the session cookie, resulting in a compromise to the MFA session. The criminal can then continue to log into the user's email multiple times through the session cookie without needing to provide MFA authentication.

Once hackers gain access to a business email, they use the accounts to ask clients for money or launch other attacks. Criminals have remained in email accounts for weeks and launched multiple attacks on the same cookie session. To avoid raising suspicion, attackers create inbox rules to archive response emails and automatically mark them as read.

Apple Passkey

With the release of iOS 16, Apple took a significant step forward in killing the password as we know it. The new technology will be known as passkeys and will allow users to log into apps and websites without a password. In the future, supported platforms will allow account creation without creating a username and password. Passkeys will sync across the iCloud Keychain for backup in the event of a lost or broken device.

Passkeys are not proprietary to Apple; they are a part of open standards from the FIDO Alliance that Google, Microsoft, and Apple are using to eliminate the need for traditional passwords.

"Now is the time to adopt them," Garrett Davidson, an authentication technology engineer at Apple, said in a WWDC talk about passkeys. "With passkeys, not only is the user experience better than with passwords, but entire categories of security — like weak and reused credentials, credential leaks, and phishing — are just not possible anymore."

The open standard works on the premise of a pair of mathematically related keys. One key is stored on a public server and is not secret. The second key is stored on the user's device and is confidential. When the website or app gets a request to unlock the user, they send a request to the smartphone or device on file. The smartphone authenticates through face-ID or fingerprint and sends the authentication back to the site without sharing the private key.

Traditional usernames and passwords make the website or app responsible for the lock. Passkeys put the lock in the hands of the user. The result is a technology that's much more difficult to phish and does not rely on user-created passwords, which are notoriously terrible.

Apple is the first to add the technology to smartphones, but Microsoft uses passwordless login with their authenticator app and Windows Hello. Android announced passkey technology would be available to developers by the end of the year. Read more on our blog post A Future Without Passwords.

Why Do Employees Break Cybersecurity Rules?

Ransomware is the number one cybersecurity threat to businesses of all sizes, and the metrics show that ransomware attacks continue to increase quarter after quarter. Cybersecurity has received mainstream headline attention with the Colonial Pipeline ransomware attack last year along with a number of other high-profile attacks on everything from city governments to the world's largest meat producer. Business leaders are focusing and spending more on cybersecurity, and with the war in Ukraine, the US government is communicating directly with industries that control American infrastructure about cybersecurity.

With all of this new focus on cybersecurity, why do employees continue to break the rules, and open businesses up to attack? A new study by the National Science Foundation digs into this question.

The study followed 330 remote employees in a wide variety of industries and focused on adherence to cybersecurity policies, and stress levels of the employee. The study found that over a two-week work period 67% of employees reported they violated company cybersecurity policies at least once. The percentage averages about once in every 20 job tasks.

When asked why the employee did not follow cybersecurity policies the overwhelming three responses were, "to better accomplish tasks for my job," "to get something I needed," and "to help others get their work done." Only 3% of responses reported malicious or retaliatory intent.

The employees reported they were more likely to knowingly violate cybersecurity protocols when they were stressed. The stresses cited were family, job security, and the stress of the cybersecurity protocol itself.

Cybersecurity training normally assumes the employee is either not aware of a protocol or is not following the protocol because of malicious intent. The study shows there is in fact a middle ground between these assumptions. Employees are more likely to understand the protocol, but purposefully do not follow it for productivity reasons or to help another employee.

Podcast

We have two new short Podcasts out this month. Jack talks about Three Types of UPS and SD WAN and Redundant Internet Access for Business.

Three Types of UPS (Uninterruptible Power Supply)

Click Here for Podcast- Three Types of UPS (Uninterruptible Power Supply)

SD WAN and Redundant Internet Access for Business

Click Here for Podcast- SD WAN and Redundant Internet Access for Business

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!**

@Quanexus571 **@Quanexus** **@Quanexus** **@Quanexus571** **@Quanexus571**