Q-News

May 2021

A Word from Jack

Things just keep getting more interesting and the criminals are getting more creative. Last month we saw a LinkedIn scraping incident, where criminals captured 500 million user profiles by scraping the screen data and then selling the data on the Dark Web. This does not represent a breach in the traditional definition, nor did LinkedIn do anything wrong.

The big news this month was the pipeline shutdown. The actual root cause of the attack has not been released because of the on-going investigation. It is believed that the hackers were able to gain access to some Internet facing systems. The company agreed to pay 4.4 million dollars. As a reminder, the basics are your best protection from cyberthreats: keep your systems patched, implement multifactor authentication where possible, use strong passwords, end user training, and have a good backup program. While there are no guarantees, doing the basics will make you less attractive to an attacker.

Current Phishing Threats

Criminals use phishing as an entry point to install malware, gain access to login credentials, or collect personal information. Hackers follow current events and prey on the emotions of their targets to drive up click rates. The Federal Trade Commission is still warning of fraud campaigns related to COVID-19. The scams are being reported in many forms, including phishing emails and texts, robocalls, and fake social media posts. The COVID scams have shifted from cures to requests for money to get to the front of the vaccine wait list. The FBI is also warning of fake COVID antibody test scams that seek to harvest personal information from their victims.

SMS Phishing, or Smishing, continues to grow in popularity among criminals. Smishing events were up over 300% at the end of 2020, and we look for those numbers to continue to increase this year. Criminals are turning to phishing via text message because most consumers trust their text messages. We have become used to receiving two-factor authentication text messages for our banks and access to health care systems. Text messages are not typically questioned before consumers click on a link. Criminals are using this trust to their advantage. Smishing campaigns run the gamut from tax rebates, bank activity, package delivery, and Amazon. Remember, a phishing campaign usually tries to generate fear so the victim will click the link. If the message creates a sense of urgency or it is not something you would normally expect, chances are it is fake.

Tax scams are also on the rise this year. The IRS pushed Tax Day back again this year, and many states are catching up to changing last minute federal laws. The tax scams we are seeing are phone and email phishing based. Be aware of the service you are signing into to file your taxes and use multi-factor authentication if it is an option for your tax service provider. Instead of clicking a link in an email, navigate directly to the site by typing in the site address (URL).

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

Dark Patterns

Dark patterns are design choices that trick users into taking an unintended action or preventing them from taking an action. Examples are, tricking a user to subscribe to a service, and then making it difficult for them to unsubscribe by hiding the unsubscribe button. UX (user experience) designers are trained to think about how people interact with technology. Unfortunately, this knowledge can also be used to deceive users. They are using human psychology to their advantage hoping users will get frustrated and give up or click the wrong option accidentally.

There are many forms of dark patterns. Harry Brignull started the website darkpatterns.org in 2010 to identify and highlight the most egregious offenders. The three most common are the Misdirection, Confirmshaming, and the Roach Motel.

Misdirection is when a website establishes a pattern and then exploits that pattern. An example would be as a user is filling out a form, then clicks a green button to go to the next step, green button, next step, green button, next step. Then at the end of the process, the option to opt into a $10/month service is a green button, and the option to continue without the monthly service fee is black text on a white background. Misdirection also occurs if an option for "yes" is highlighted in red, or an option for "no" is highlighted in green. These design decisions are made to confuse the user and make them click what the business wants them to click.

Confirmshaming is a tactic to guilt users into agreeing to a service or signing up for an email list. These are often found on shopping websites where the language will say, "Sign up for mailing list" and the alternative is "No, I want to pay full price." In some cases, the pop up creates more urgency with added "One time offer" language.

The Roach Motel is familiar to many users. This dark pattern centers around the idea it is easy to get in, but difficult to get out. Have you ever had to Google how to unsubscribe from a service? A Roach Motel purposefully hides the cancel option, and possibly makes users go through multiple confusing confirmations to finally cancel the service. Amazon is famous for how difficult it is to cancel an account. Darkpatterns.org has a great video on all the steps a user has to navigate to cancel an Amazon account, and then at the end of the process the user has to chat with an Amazon specialist because the user actually cannot cancel the membership on their own. Amazon must cancel the membership.

Dark patterns take advantage of psychology and short attention spans. Users get frustrated and give up trying to cancel that monthly membership or email blast. However, with some education and the occasional search engine dive, users can navigate this world of purposefully bad UX design.

Human Operated Ransomware on the Rise

The cost of ransomware attacks in 2021 are projected to reach $20 Billion, almost double the cost impact from 2019. A ransomware attack occurs after a criminal has gained access to a system through a phishing attack or stolen credentials. A typical ransomware attack encrypts data, which stops the company from doing business until the ransom is paid. In a human operated ransomware attack, the criminals gain access to a business network and move around the network to see what they can find.

Microsoft does a good job explaining the difference between the two attack methods:

"Human-operated ransomware attacks are a cut above run-of-the-mill commodity ransomware campaign. Adversaries behind these attacks exhibit extensive knowledge of systems administration and common network security misconfigurations, which are often lower on the list of 'fix now' priorities.

Once attackers have infiltrated a network, they perform thorough reconnaissance and adapt privilege escalation and lateral movement activities based on security weaknesses and vulnerable services they discover in the network."

Hackers can use the business infrastructure to mine bitcoin, run SPAM campaigns, or use company workstations for other criminal activities. Only after they have exploited the private infrastructure do they then execute a typical ransomware attack by encrypting data and asking for money. These criminals can live in a company network for months, using the business infrastructure for their gains.

These 'hands on keyboard' attacks are more time consuming for the criminal, but they can also be much more profitable, which is why we are seeing the increase. While malware attacks are on the decline, ransomware attacks increased 40% last year. Criminals are focusing time and effort on these more elaborate attacks that yield greater gains.

Preventing these targeted attacks starts with education as always. The criminal has to get into the network first. Continued education on phishing campaigns and password management is critical. Additionally, a layered security approach is the best defense along with network monitoring tools. These tools can alarm IT departments to unusual network activity like using workstations to mine bitcoin.

US Pipeline Shutdown by Ransomware Attack

One of the nation's largest pipeline operators was forced to shut down their network following a ransomware attack. In what is being called the worst cyberattack on critical US infrastructure in history, Colonial Pipeline shut down their 5,500 miles of pipeline to contain the breach. The Georgia based company transports more than 100 million gallons of fuel per day including gasoline, diesel, jet fuel, and home heating oil. Oil analysts say the shutdown could affect gas prices if it goes on for more than a few days. The immediate concern is the supply of jet fuel to large airports like Atlanta and Charlotte. Colonial Pipeline moves 45% of the fuel from the Gulf Coast of Texas to customers in the southern and eastern United States.

Ransomware is a type of malware that locks up a victim's files, which the attackers promise to unlock for a payment. More recently, some ransomware groups have also stolen victims' data and threatened to release it unless paid; a kind of double extortion.

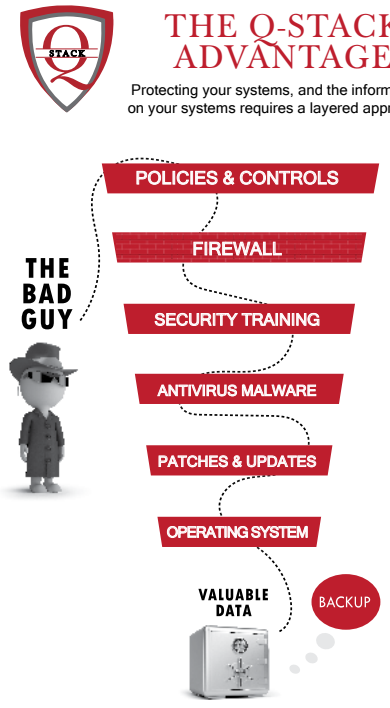
The attack has been confirmed by the FBI to originate from a group of cybercriminals known as DarkSide. They are a new and particularly cruel criminal gang who admit to targeting hospitals, schools, universities, nonprofit organizations, and government infrastructure. The group reportedly stole and encrypted 100 gigabytes of data from Colonial Pipeline they are threatening to leak if the ransom is not paid.

Eric Goldstein, executive assistant director of the cybersecurity division at CISA said,

"This underscores the threat that ransomware poses to organizations regardless of size or sector. We encourage every organization to take action to strengthen their cybersecurity posture to reduce their exposure to these types of threats."

These high profile attacks continue to keep IT security in the news and at the forefront of business owners' minds. The SolarWinds breach was an illustration of the capability and scope of a nation state attack. At the same time we see ransomware attacks on small businesses or city governments who often don't have the budget for IT infrastructure. Ransomware payments peaked in Q3 of last year with an average payout of over $225,000 per incident. Criminals understand many small businesses don't have the resources to defend against these attacks and have no choice but to pay the ransom. Ransomware attacks increased over the prior year by over 300% resulting in victims paying more than $350 million dollars to criminals.

Later reports indicate Colonial Pipeline paid a ransom of nearly $5 million dollars to the Eastern European hacker group on the same day as the attack. The group provided a decryption tool, but apparently it was so slow to work, the pipeline continued to use their backups to restore the missing data. The details from these stories never fail to highlight the security stack we use at Quanexus. **Click below for Q-Stack Video.**



LinkedIn Scraping Attack

LinkedIn is in the spotlight of IT security news again. A hacker claims to have 500 million LinkedIn profiles for sale. The criminal posted four files that contain LinkedIn member IDs, full names, email addresses, phone numbers, genders, job titles, workplace information, and potentially other identifying data.

LinkedIn reviewed the data, confirmed it was real, and released a statement claiming the data was scraped from public profiles, and not a breach.

"This was not a LinkedIn data breach, and no private member account data from LinkedIn was included in what we've been able to review."

For a year now criminals have focused on LinkedIn to acquire information on employees and target them in attacks. LinkedIn is now in the top three companies impersonated in phishing attacks, a year ago it wasn't even in the top 25. Earlier in the pandemic we wrote a blog post about criminals using LinkedIn to attack newly hired employees by impersonating IT support of the company.

The scraped data are forms of publicly identifiable information or PII which can be used along with other public information to give the criminal a more complete picture of a person they are attacking. Even though the information is public, a criminal could use the list to construct a more credible phishing attack. A searchable, sortable, aggregated list of 500 million users could be very useful to a hacker. They could sort the data by business or area code and create more targeted attacks, use the data to pose as LinkedIn, or combine the data with other PII to target individual users in a spear phishing campaign.

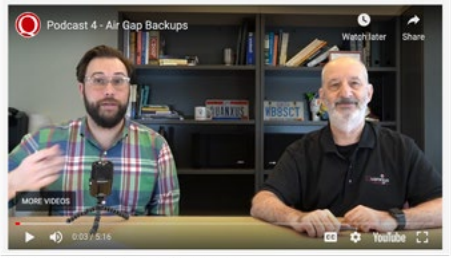
Data scraping is on the rise because we share so much information publicly. LinkedIn has risen in popularity as a business to portray because of so many people looking for new jobs during the pandemic.

With the announcement of this data scraping attack, users should be on the lookout for phishing emails referencing LinkedIn, or the information the user has on LinkedIn. It's always a good idea to understand what information you have publicly available, so if an email or text message doesn't feel right, you can better understand the information the hacker may be working from.

In a couple recent podcasts, Jack talks about oversharing PII, and data aggregation. Find those podcasts here and here.

Podcast

We have two new short Podcasts out this month. Jack and Chuck discuss Insider Security Threats, and Air Gap Backups!



Podcast 4 - Air Gap Backups

Click Here for Podcast 4 - Air Gap Backups

Podcast 5 - Insider Security Threats

Click Here for Podcast 5 - Insider Security Threats

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