Monthly Cybersecurity Newsletter

September 2024

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Torry Crass

Cyberattack on U.S. Oilfield Firm, Halliburton, Confirmed

Halliburton, one of the world's largest oilfield services companies has became the latest high-profile victim of cyberattacks that impacted its operations. According to the Houston Press, the attack was first identified on Aug. 21, within the company's North Houston campus. As a result, Halliburton was forced to take several internal systems offline as a precautionary measure to prevent further damage.

The specifics to this attack have not been released, but it bears similarities to several ransomware attacks that we reported in earlier editions of this newsletter. These attacks have increasingly plagued critical infrastructure sectors.

Ransomware typically involves malicious actors encrypting sensitive data and demanding a ransom for its release.

Although Halliburton has not confirmed if this was the exact method used, the company's swift response included working with external cybersecurity experts and law enforcement agencies to investigate and mitigate its effects.

The Houston Business Journal writes that, despite the disruption, Halliburton has assured its stakeholders that it is actively restoring its systems and evaluating the overall impact of the attack.

As of now, it remains unclear whether the cyber incident will have a long-term affect on Halliburton's operations or financial standing.

The energy sector, being critical infrastructure, continues to be a lucrative target for cybercriminals, necessitating the need to have enhanced cybersecurity measures.

Cyberattack Disrupts the City of Columbus

Columbus, Ohio, is reeling from a massive cyberattack that struck the heart of the city's digital infrastructure, throwing city services and local businesses into chaos.

What began as a typical Monday quickly turned into high-stakes drama as hackers unleashed a sophisticated ransomware assault, forcing the city to scramble for solutions. The aftermath has left residents and business owners grappling with a harsh new reality: the cyber battlefield is upon them.

The recent cyberattack has significantly exposed the city's digital vulnerabilities.

According to reports on Reddit, the ransomware group, Rhysida, is taking credit for the attacks. The group was able to infiltrate municipal systems and steal sensitive data, including Social Security numbers and confidential records of domestic violence victims.

Although the city replied with a swift response, the shockwave of this breach ignites a fierce debate about escalating cyberwars.

This ransomware attack not only stole data, but it shattered the illusion of safety. For days, critical city services were disrupted, forcing officials into a race against time to regain control. The breach exposed Columbus to financial and legal repercussions and has raised alarming questions about the adequacy of local government cybersecurity.

For this reason, most municipal governments are seen as soft targets to cybercriminals due to their limited access to cybersecurity resources.

Governments at all levels should take this as a reminder to bolster their defenses or face the devastating consequences.

Surviving the Aftermath: Shielding Yourself from Post-Storm Cyberthreats

So, you've just weathered the storm – literally.

Whether it was a hurricane, a blizzard or a major power outage, you're probably busy dealing with the aftermath: cleaning up debris, checking on neighbor, or, let's be honest, finding out which of your favorite takeout spots are back in action.

But while you are focused on getting life back to normal, there's another storm brewing that you might not see coming – cyberattacks. Hackers love to strike when you are distracted. The key is learning how to stay cyber-savvy and outsmart them.

Phishing for Trouble: Don't Take the Bait

Imagine this: You are strolling through your email and suddenly you see a message from what looks like your insurance company. It keeps asking you to click a link to "speed up your claim" or "get urgent updates." It seems legit, right?

Before you click, remember that cybercriminals are sneaky – they craft emails that look almost identical to real ones, just waiting for you to take the bait.

Instead of falling for it, take a deep breath, channel your inner detective and verify the email first. Look for telltale signs like weird spelling mistakes, suspicious links, or an email address that's a bit off. If you are unsure, contact the company directly. This will prevent you from falling victim to post disaster schemes disguised as urgent messages.

The Dangerous Duo: Passwords and Public Wi-Fi

Let's say the storm knocked out your internet, and you are tempted to hop on the nearest public Wi-Fi to check in with the world. Stop right there!

Public Wi-Fi is like the wild west of the internet – full of dangers lurking in every corner. Without proper protection, your personal information could be up for grabs faster than you can say "password123".

If you must use public Wi-Fi, make sure your devices are updated, use a VPN, do not do any online banking or shopping until you are back on a secure network.

Sharing Your Personal Information

We get it – the storm threw everything into chaos, and you might need to share your personal data to get assistance or file claims. Just be mindful of who is receiving this information. Treat your information like your favorite secret recipe – you wouldn't just hand it to anyone, right?

When surfing the web, stick to secured sites using the "https" protocol in the URL. Keep an eye on your digital accounts, making sure to set up alerts for anything that is out of place. These are just a few ways to safeguard your information in a crisis.

Plan, Prepare, and Protect

Lastly, let's turn this situation into a lesson for the future. Just like you have a plan for boarding up windows and stocking up on canned goods, have a plan to secure your cyberspace. Regularly update your software, use strong passwords, and educate your household on how to spot scams. As a reminder: even during a crisis, we have to remain vigilant. Add these tips to your toolkit, and you should be ready to weather any storm.

Attackers Abuse Google Drawings to Host Phishing Pages

Researchers at Menlo Security warn that a phishing campaign is exploiting Google Drawings to evade security filters.

The phishing emails inform users that their Amazon account has been suspended, instructing them to click on a link to update their information and reactivate their account.

The phishing page is crafted with Google Drawings, which makes it more likely to fool humans while evading detection by security technologies.

"This graphic is actually hosted in Google Drawings, part of the Google Workspace suite, that allows users to collaborate on graphics," the researchers write. "Such a site is not typically blocked by traditional security tools. Another thing that makes Google Drawings appealing in the beginning of the attack is that it allows users (in this case, the attacker) to include links in their graphics. Such links may easily go unnoticed by users, particularly if they feel a sense of urgency around a potential threat to their Amazon account."

The attackers are also abusing link shorteners to further increase the chances that the phishing link will bypass security filters.

"We believe that 'l.wl.co' was chosen because shortened WhatsApp links created with this service do not present any type of warning to the user that they are being redirected to a different site altogether," the researchers note. "As an extra precautionary measure, the link created with the WhatsApp URL shortener is then appended with another URL shortener, "qrco[.]de," which is a URL shortener service for dynamic QR codes. We believe that this second step is designed to obfuscate the original link still further, in an effort to evade security URL scanners."

This article is redistributed with permission from KnowBe4.

[WHOA] - This 'Unpatch Attack' Is A New One To Me!

In a startling revelation at Black Hat 2024, SafeBreach security researcher Alon Leviev demonstrated a critical vulnerability in Windows systems, dubbed the "Windows Downdate" attack.

This exploit allows threat actors to forcibly downgrade fully updated Windows 10, 11 and Windows Server systems to older versions, reintroducing vulnerabilities that had been previously patched.

By exploiting zero-day vulnerabilities (CVE-2024-38202 and CVE-2024-21302), attackers can bypass security features like Credential Guard and Virtualization-Based Security, making a supposedly secure system susceptible to thousands of past exploits.

Despite being reported to Microsoft six months ago, no patch has been released, leaving users vulnerable. Microsoft advises following mitigation strategies until a fix is deployed.

Read the full article at BleepingComputer.

This article is redistributed with permission from KnowBe4.

Employment Scams Continue to Target Job Seekers Via Phony Employment Offers

Threat actors continue to target job seekers with phony employment offers on job search platforms like Indeed, researchers at Bitdefender warn.

These scams are often designed to steal personal information or money. The threat actors exploit the fact that people who are unemployed are often desperate and may overlook the warning signs when they see a good opportunity.

Bitdefender says job seekers should be on the lookout for the following red flags:

- **Too-Good-to-Be-True Offers:** In this scenario, scammers advertise jobs with unusually high pay for minimal work or qualifications. For example, you may stumble upon listings promising $100 an hour for data entry. Needless to say, job listings like this one are likely not legitimate.
- **Vague or Overly Simple Job Descriptions**: Con artists rarely provide detailed job descriptions, as they want potential victims to reach out to them. If the listing lacks basic details, such as job duties, employer expectations or the type of work expected, proceed with caution.
- **Immediate Hiring Without Interview:** Job offers made immediately without formal interviews or background checks are red flags. Remember that scammers usually add a sense of urgency to their made-up scenarios to impede critical thinking and decision-making skills.
- **Requests for Personal or Financial Information:** Any job offer that asks for your financial details, such as your bank account information for “direct deposit setup” before you even meet the employer, is suspicious.
- **Upfront Payment Requests:** No legitimate job would require you to pay for training, application processing, or equipment before starting work.

Job seekers should research a company to see if it has a legitimate online presence and “pair” the company’s name with keywords like “review,” “scam” or “complaint” for more accurate results that may reveal the company’s true nature.

This article is redistributed with permission from KnowBe4.

Training & Continued Learning Resources

- FedVTE: Free Online Training Environment: https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service: https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies: https://niccs.cisa.gov/
- ICS-CERT Training: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

CYBERSECURITY NEWSLETTERS

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. Access the newsletter. ***Note:*** *You must have a valid state employee Microsoft 365 account.*

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch/

Upcoming Training & Events

- **Sept. 9:** SANS Webinar: Justice Denied: How Bad Digital Forensics Threatens and Undermines Justice
- **Sept. 11:** SANS Webinar: SANS 2024 AI Survey: AI and Its Growing Role in Cybersecurity: Lessons Learned and Path Forward
- **Sept. 12:** SANS Webinar: Adversaries are Doing Stranger Things
- **Sept. 19:** SANS Webinar: The Evolution to GenAI: Implications and Mitigations
- **Sept. 24:** SANS Webinar: SCATTERED SPIDER and The Com: Cybercrime Intelligence for Proactive Defense
- **Sep 25** SANS Webinar: Architecting Safety using Cybersecurity Requirements and Assessments

View a list of upcoming SANS webcasts.

Be sure to follow the N.C. Department of Information Technology on X (formerly known as Twitter), Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. Remember … Stop. Think. Connect.
