Monthly Cybersecurity Newsletter

November 2023

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

What's at Risk When Using QR Codes?

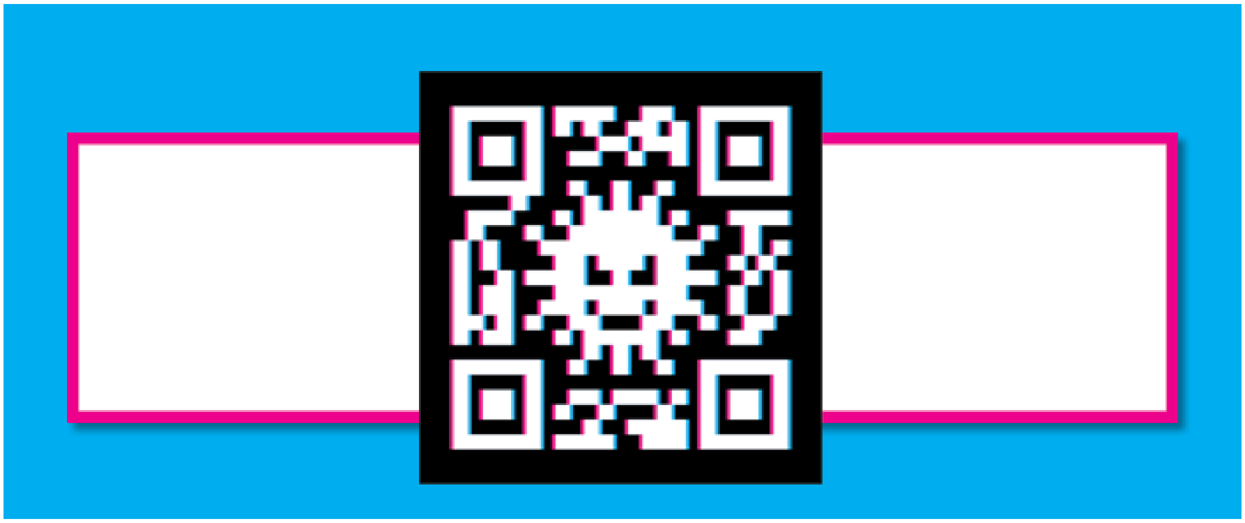
The Triangle InfoSeCon Conference is one of the largest cybersecurity conferences in the Southeast. Hosted annually by the Information Systems Security Association (ISSA), this conference took place on Friday, Oct. 20, 2023, in Raleigh, drawing hundreds of cybersecurity professionals from across the state and beyond.

The use of QR codes to disseminate information quickly was one of the conference's most well-received and used attributes. Many of the vendors presenting at this event chose to use QR codes instead of printing fliers.

It truly is a money-saver for the companies, but what risk does it pose for the attendee? Is this the safest method to use?

No matter where you are, you should always be vigilant of possible fraudulent events, especially when it involves the exchange of information.

Cybersecurity specialists, along with those interested in joining the industry, were the primary attendees of last month's conference. With all these experts under one roof, how many do you think took the time to consider the risks associated with scanning a QR code at an event of this magnitude while moving at



such a fast pace? The vendors at this event were pre-screened and vetted by the hosting organization, giving the attendees a sense of security and ease when dealing with them.

QR codes made it easier for attendees to move from one vendor to another while gathering as much information as possible. So, was security a forethought in such a quick exchange environment?

While QR codes have become increasingly popular and widely used for their convenience and efficiency, it is essential to be aware of the potential risks associated with their usage.

So, how do you recognize QR code flaws and why should you remain alert while using them, especially in large, fast-paced environments? Let's look at a possible scenario that could occur during a conference.

As you walk up to a vendor's exhibit, the vendor directs you to a QR code sitting on their event table. By the time you have entered this space, hundreds of people have already visited that very table.

How easy would it be for a threat actor to replace the vendor's QR code with a fake code that would direct information seekers to a malicious site without the vendor's knowledge? It could be as simple as adding a QR sticker over the legitimate code and walking away without being noticed, especially if the vendor is engaged in conversation with other people.

Some QR codes, when scanned, require individuals to grant certain access to personal data or specific device functionalities, triggering privacy concerns. QR codes often redirect users to websites or apps that can collect user data. Companies can track and store this information for marketing purposes, leading to potential privacy breaches. Users should be very cautious about sharing personal or sensitive data through QR code scans. Please be mindful that these concerns exist even if the intent is not malicious.

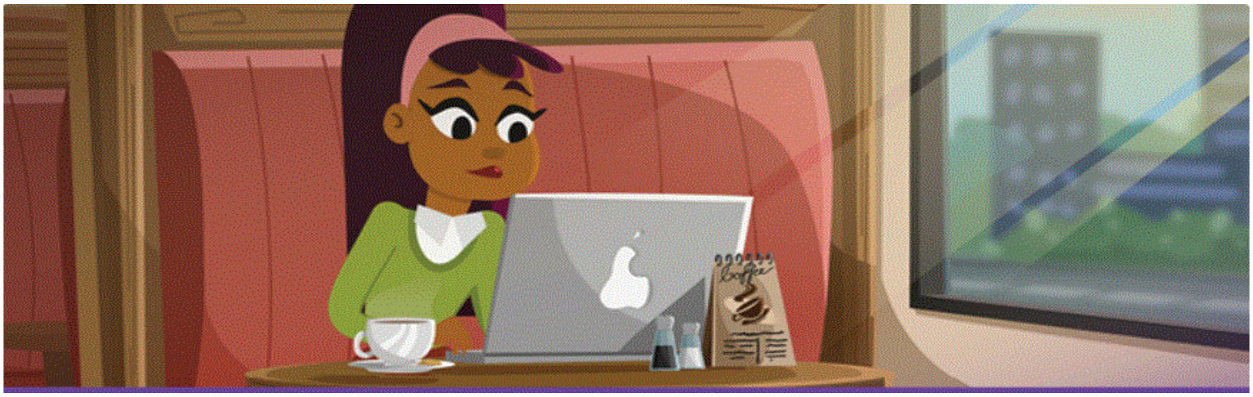
Content spoofing is another potential danger when dealing with QR codes. Spoofing is an attack in which a person and/or a program impersonate a legitimate person and/or program to gain unauthorized access to services or devices. In the case of QR codes, the data can be manipulated within the code to present fake or spoofed content, resulting in users unintentionally revealing personal information or engaging in fraudulent transactions.

To prevent QR code scams at large events:

- Examine the code for evidence of tampering before you scan it.
- Verify the source of the code, and only scan codes from reputable sources like conference organizers or official event material.
- Never scan codes shared by unknown individuals.
- Double-check the actual URL for misspellings, odd characters or discrepancies that might indicate a fraudulent site before adding your information to it.
- Avoid scanning codes that ask for excessive personal information, such as Social Security numbers, credit card details and/or passwords.
- Understand the purpose of the QR code, and if the data presented does not correlate, do not continue.

Always think twice before scanning and entering personal data. Remember, you are the first line of defense against information theft.

Beware of Bogus Roborock Retailers: The Perils of Misleading URLs in E-Commerce



The online storefronts of robot vacuum brand Roborock have been used for cybercrime schemes in the past, and it seems attackers are continuing to create fake online shops.

Distinguishing between authentic and counterfeit online stores can be challenging, especially when the counterfeit ones appear as polished as the one a friend of mine recently got duped by. There were no obvious signs of a fake shop. The corporate design was immaculate, and all imagery seemed appropriate. The website looked complete and legitimate.

He was on the hunt for a new Roborock vacuum cleaner, a device known for both its vacuuming and mopping capabilities. Even though Roborock does not maintain a direct sales page in Germany, directing customers to Amazon, Media Markt and Saturn, my friend could not find the model he wanted on these platforms.

A few weeks later, he discovered a website by chance advertising discounted Roborock products for the IFA event in Berlin. The site seemed legitimate, boasting professional graphics and animations. During checkout, he was given the option to pay via Visa or PayPal, and he completed the verification steps. After placing his order, he promptly received a confirmation email. The payment was processed through Visa, and everything appeared to be in order. Yet, the product did not show up as promised, and even after two weeks, there was no sign of it. The tracking link from a Chinese courier hinted at a customs holdup.

Growing wary after unsuccessful attempts to reach the customer service mentioned in the confirmation email, he began to suspect that it was a scam. He approached Visa with his concerns. Subsequent research on scam detection platforms confirmed his suspicions – the website was fraudulent. Not long after, the site vanished.

He had overlooked a crucial detail – the URL directed to a "de.com" subdomain, not the expected "Roborock.de" domain. That was the initial warning sign. The second was the antiquated typewriter font used in the confirmation email, which seemed out of place for a leading tech manufacturer from China.

This article is redistributed with permission from KnowBe4.

Exposed: Scam Artists Mimicking PepsiCo in Phishing Schemes

Researchers at INKY warn that a phishing campaign is attempting to distribute malware by impersonating PepsiCo.

“As usual, it all starts with a phishing email,” the researchers write. “In this case, the phishers are impersonating the PepsiCo brand, pretending to be potential clients. They are claiming to need what the recipient sells, and they’re asking them to submit a quote for PepsiCo to review. What the would-be victim doesn’t know is that attached to the email is a malicious disk image disguised as an RFQ (Request for Quote). One click will infect the victim’s computer.”

INKY explains that the emails are convincing and detailed in terms of business jargon:

- “As mentioned, the sender’s email address was spoofed. What shows is me@pepsico[.]com, and the sender’s display name uses that of an actual PepsiCo employee who is responsible for procurement management."

- “It is becoming common practice for cybercriminals to create phishing emails with a good amount of detail, so they seem more convincing. You’ll notice this email comes with a lot of information, as well as a threat that their RFQ could be rejected if they don’t follow the specific instructions outlined in the email."

- “A common phishing technique is to create urgency. The phisher does that by imposing a deadline for the RFQ.”

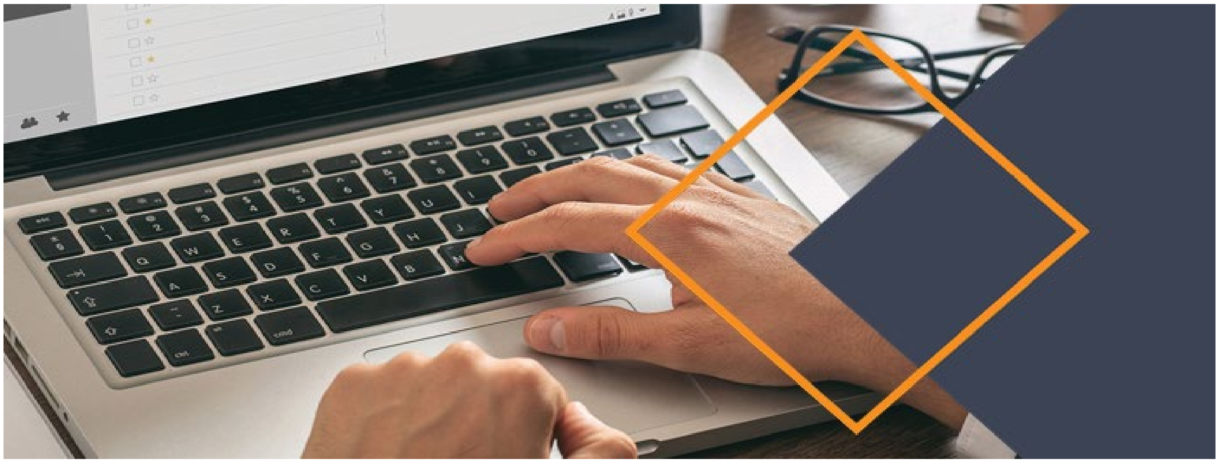
INKY notes that the attackers chose to impersonate PepsiCo to cast a wide net for potential targets.

“With phishing emails, it’s important to choose a brand that prompts readers to act,” the researchers write. “PepsiCo’s product portfolio boasts more than 500 different brands ... With 291,000 employees located all over the world, PepsiCo is a global powerhouse.”

“The way in which this phishing email was deployed also aids in its success. To evade geographical filters, these emails were sent from several U.S.-based virtual private servers controlled by bad actors. Also, the phishers used a 'spray and pray’ technique – meaning they sent out large quantities of the email in hopes that a percentage of recipients would fall for the scam and click on the malicious link.”

This article is redistributed with permission from KnowBe4.

‘Human-Operated’ Ransomware Attacks Double



As attackers leave little-to-no traces of their attack patterns, more ransomware groups are shifting from automated attacks to manual attacks.

According to the newly released Microsoft Digital Defense Report 2023, about 40% of the ransomware attacks detected were human-driven and tracked back to over 120 ransomware-as-a-service (RWaaS) affiliates.

This spike in human-operated ransomware attacks likely goes back to attackers wanting to minimize their footprint within an organization. Think of it this way: All it takes is one detection of something unusual on a single system to alert IT of the attacker’s presence.

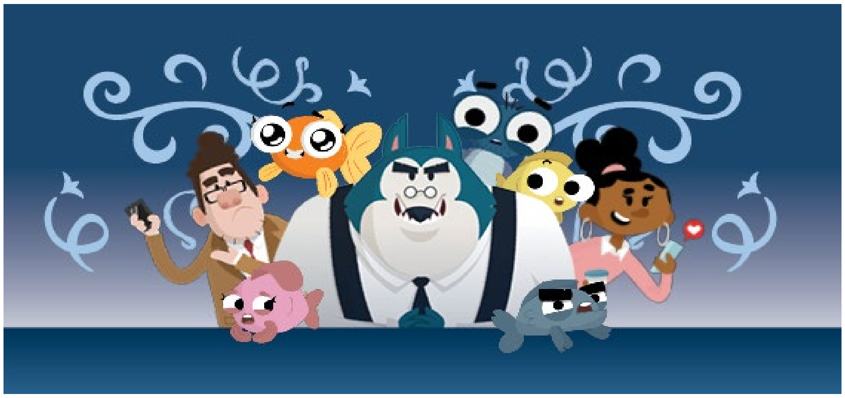
One tactic found in these types of attacks is remote encryption. Attackers can choose to encrypt data from multiple systems on a single compromised machine and copy it back to their appropriate repositories. This is much simpler for cybercriminals to do than to deploy malware on each system and risk process-based detection.

One of the most concerning details around the use of human-operated ransomware is its growth. According to Microsoft, this model of attack has grown over 200% in the last year, and the number of RWaaS affiliates tied to these attacks has grown by 12% in the last year. This signals that 2024 will likely see significant increases in human-operated attacks.

This shift in attack models means more emphasis on initial detection before a threat actor can take control of an endpoint as their foothold in your network. With phishing still being used as the primary method for initial attacks, having a vigilant user base that is continually educated through training will reduce the likelihood that attackers can gain the needed foothold to begin a ransomware attack.

This article is redistributed with permission from KnowBe4.

Harvested Credentials Are Put up for Sale Monthly on the Dark Web at a Rate of 10,000 a Month



Credential harvesting has become a business in and of itself within the cybercrime economy. New insight from Microsoft details the types of attacks your organization should watch out for.

I've attempted to cover every Microsoft 365 credential harvesting attack since the platform is so popular and is an easy target for cybercriminals. But the news coming from their newly released Microsoft Digital Defense Report 2023 puts this type of attack into perspective.

Not only should the 10,000 credentials per month data point make you realize that these types of attacks are prevalent, but there is a black market buying at an equally blistering pace.

In the report, Microsoft points out five specific examples of credential-harvesting attacks:

- **Emails sent from a trusted third party** – compromise one account and then send a malicious email to everyone in their contact list, intent on stealing each recipient's credentials.

- **Using legitimate URLs** – I've covered plenty of stories where threat actors used legitimate web platforms to host landing pages (that usually redirect to malicious sites) to bypass security scanners.

- **Using OneNote attachments** – The use of this file type in attacks is in response to Microsoft disabling macros and attackers needing a relatively commodity filetype supported by the largest number of potential victims possible.

- **OAuth** – The attacker exploits the device authorization grant process within M365 to trick a user into granting them access to their account using a phishing link.

- **Targeted Attacks** – attackers do their diligence on a potential victim and create tailored attacks with appropriate look-alike domains.

In all these cases, the onus may end up solely on the recipient user, with security solutions potentially none-the-wiser. So, your users need to be as up to date as possible on the latest attack methods through continual training.

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*.

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/insights/newsletter

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

Upcoming Events

Nov. 10: SANS Webinar: Zero Trust Solutions Forum 2023: Use Cases, Adoption Trends and Prioritization

Nov. 13: SANS Webinar: Exploring the Link Between Corruption and Cybercrime

Nov. 14: SANS Webinar: Safeguard Your Business-Critical Web Apps and APIs with a WAF

Nov. 15: SANS Webinar: Software Supply Chain Security: Hunting Hidden Threats Before They Strike

Nov. 20: SANS Webinar: Tips & Tricks for Digital Dumpster Diving

Nov. 28: SANS Webinar: Configuring the Future: Addressing Network and Configuration Risks in Modern Cloud Security

View a list of upcoming SANS webcasts.

Be sure to follow the N.C. Department of Information Technology on X (formerly 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.*

***Disclaimer**: Vendors, references and links in this newsletter are for informational purposes only, and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.*