Monthly Cybersecurity Newsletter

February 2023
Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the Interim State Chief Risk Officer – Carly Sherrod

Cybercrime Is the World's Third Largest Economy After the U.S. and China

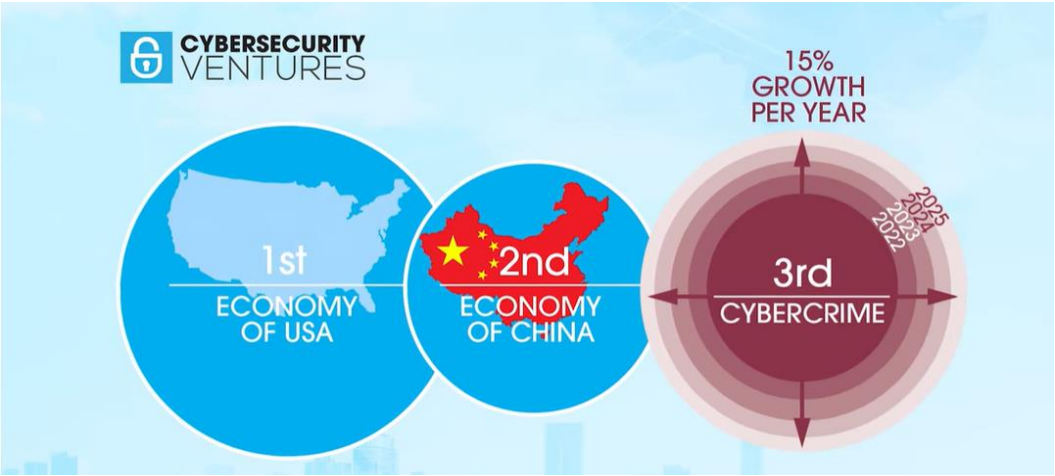
Cybersecurity Ventures released a new report that shows cybercrime will cost the world $8 trillion in 2023. If it were measured as a country, it would be the world's third largest economy after the U.S. and China.

"We expect global cybercrime damage costs to grow by 15% per year over the next three years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015," as stated by Steve Morgan, Editor-in-Chief for Cybercrime Magazine.

"Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm."

The 2022 Official Cybercrime Report published by Cybersecurity Ventures and sponsored by eSentire, provides cyber economic facts, figures, predictions and statistics that convey the magnitude of the cyber threat we are up against, and market data to help understand what can be done about it.

Read more about the report findings here.



This article is redistributed with permission from KnowBe4.

Are QR Codes Really Safe to Use?

In our digital society, QR Codes are everywhere. You see them in restaurants, retail stores, hospitals, hotels, various businesses, and online advertisements – just to name a few.

These codes are commonly used to store and disseminate information of all kinds. They are quick, efficient and easy to use. QR Codes have become a staple in our environment and have started to gain popularity since the rise of the coronavirus pandemic.

Although there are many advantages to using QR Codes, threat actors have found ways to use them as attack vectors to non-vigilant victims. Just as they allow quick and easy access to business information, QR codes also provide a medium for threat actors to have quick and easy access to the victim's information.

How It Works

How is this possible? According to an article by Bob Violino, of CSO Online, threat actors are taking advantage of the increased use of QR codes to steal sensitive information or to conduct sophisticated phishing campaigns better known as "QPhishing." QR codes are being sent via email, text, restaurant menus and various other methods that could lead a victim to what seems to be a legitimate website of a trusted institution. Victims will provide sensitive information such as passwords, personal identifying information and banking credentials without being aware of the pending scam or the website redirect.

In some cases, cybercriminals will enter an establishment and replace the intended QR code with a sticker containing the malicious code, unbeknownst to the victim. Without realizing the danger, the victim will scan the code and will enter their credentials. Scanning QR codes have become second nature to most people, and they never stop to think that the information could be tainted. The risk and dangers of scanning these codes are often overlooked and forgotten.

Real Life Example

The Jester, who is a well-known grey hat hacktivist, exploited vulnerabilities in Safari, Chrome and Android browsers using a QR code that redirected victims to a website with embedded and hidden code. Once the code was scanned, the victim's device would make a TCP shell connection back to his remote server where the data would be exploited. The Jester was responsible for exploits on WikiLeaks and Islamist websites, where he attempted to block communication attempts from anti-American extremist. Read more about the Jester here.

Final Thoughts

Cybercrimes are on the rise. This digitized world has afforded us comfort, but at what risk? Many criminals are experimenting with new ways to exploit victims and the threats are becoming more. It is up to us to ensure our own security and remain vigilant at all times.

How To Avoid Malicious QR Codes

Closely Inspect URLs

Most often, your device will display a clickable link when you scan a QR code. Make sure to closely inspect the link to ensure that it's directing you to a legitimate website. If the URL looks suspicious or doesn't align with what you expected, don't click! QR codes are commonly used to direct victims to malicious websites.

Remain Skeptical

Criminals have been known to replace legitimate QR codes with malicious ones. This allows them to easily defraud people out of money or steal confidential information. As such, it's generally best to avoid QR codes in public areas, and remain especially skeptical of any that you receive at random via email.

Use the Default Scanner

Most modern phones allow you to use the default camera app to scan QR codes, while others have a built-in QR app. Stick with these default options and avoid downloading any third-party QR scanners, which have been known to be malicious and vulnerable to exploits.

Think Before You Scan

If you're unsure if a QR code is safe, don't scan. Use alternative methods to accomplish whatever you need the QR code for, such as typing the web address or website name directly into a browser. Also, remember that QR code phishing can occur both online (such as codes sent via email or social media) and offline (such as the parking lot example). Always think before you scan!

> As a general rule of technology, any time something is made to be quicker and easier, criminals will find a way to leverage it. QR codes are a perfect example of this, and that's why it's important to always prioritize security over convenience.

SAC the security awareness COMPANY

This image is redistributed with permission from KnowBe4.

Unusual Blank-Image Phishing Attacks Impersonate DocuSign

An unusual phishing technique has recently surfaced. Avanan, a Check Point Software company, released a blog detailing a new attack in which hackers hide malicious content inside a blank image within an HTML attachment in phishing emails claiming to be from DocuSign.

The campaign begins with an email appearing to originate from DocuSign, containing a link and an HTML attachment. The phishing email requests the review and signature of a document claiming to be "remittance advice." If clicked, the "View Completed Document" button links to a clean, legitimate webpage, but the attachment, however, is not. If the document is opened, the blank image attack begins. The attachment includes an SVG image encoded with Base64 containing JavaScript that redirects to the malicious link.

Hiding the malware within the empty image attachment hides the true intent of the message, and contains a legitimate link, allowing for the email to bypass link analysis and security scanners. Researchers advise caution around emails containing HTML, suggesting blocking all HTML attachments and treat them like executables.

Jeremy Fuchs, an Avanan cybersecurity researcher/analyst, points out that this amounts to a new variation of existing attack methods. "Hackers can target practically anyone with this technique," he says. "Like most attacks, the idea is to use it to get something from the end-user. Any user with access to credentials or money is a viable target. HTML attachments aren't new, nor are using Base64 trickery. What is new and unique is using an empty image with active content inside – a JavaScript image – which redirects to a malicious URL. It's essentially using a dangerous image, with active content inside that traditional services like VirusTotal don't detect."

The threat actors evolve, and they'll inevitably come up with novel approaches, like this one, that can catch out defenders until the protective tools catch up. An informed, alert user is the best and final line of defense.

This article is redistributed with permission from KnowBe4.

ChatGPT Creates Polymorphic Malware

OpenAI's ChatGPT has reportedly created a new strand of polymorphic malware following text-based interactions with cybersecurity researchers at CyberArk.

According to a technical write-up recently shared by the company with Infosecurity, the malware created using ChatGPT could "easily evade security products and make mitigation cumbersome with very little effort or investment by the adversary."

The report, written by CyberArk security researchers Eran Shimony and Omer Tsarfati, explains that the first step to creating the malware was to bypass the content filters preventing ChatGPT from creating malicious tools.

To do so, the CyberArk researchers simply insisted, posing the same question more authoritatively.

"Interestingly, by asking ChatGPT to do the same thing using multiple constraints and asking it to obey, we received a functional code," Shimony and Tsarfati said.

Further, the researchers noted that when using the API version of ChatGPT (as opposed to the web version), the system reportedly does not seem to utilize its content filter.

"It is unclear why this is the case, but it makes our task much easier as the web version tends to become bogged down with more complex requests," reads the CyberArk report.

Shimony and Tsarfati then used ChatGPT to mutate the original code, thus creating multiple variations of it.

"In other words, we can mutate the output on a whim, making it unique every time. Moreover, adding constraints like changing the use of a specific API call makes security products' lives more difficult."

Thanks to the ability of ChatGPT to create and continually mutate injectors, the cybersecurity researchers were able to create a polymorphic program that is highly elusive and difficult to detect.

"By utilizing ChatGPT's ability to generate various persistence techniques, Anti-VM modules and other malicious payloads, the possibilities for malware development are vast," explained the researchers.

"While we have not delved into the details of communication with the C&C server, there are several ways that this can be done discreetly without raising suspicion."

CyberArk confirmed they will expand and elaborate more on this research and also aim to release some of the source code for learning purposes.

The report comes days after Check Point Research discovered ChatGPT being used to develop new malicious tools, including infostealers, multi-layer encryption tools and dark web marketplace scripts.

This article is redistributed with permission from Infosecurity Magazine.

Training and 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

A Look Back at Mobile Government Cyberattacks Shows Increased Attacks and Weaker Security

A rise in the reliance on unmanaged mobile devices, matched with a lack of patching and increased attacks seeking solely to steal credentials was a perfect storm for government.

You'd think our government has the strongest cybersecurity stance, given the state of modern cyberattacks. But new data from Lookout Software's just-released U.S. Government Threat Report shows that over the last two years, the government hasn't entirely been prepared, despite cybercriminals being more than ready to attack.

The report, spanning all of 2021 and the first half of 2022, paints a picture of a government under attack, with 1 in 8 government employees were exposed to one or more phishing attacks. Part of the problem lies in the devices being used; being just off the heels of COVID when any mobile device that got an employee working remotely was "acceptable," some government entities relied on insecure mobile devices:

- In 2021, 13% of all federal government mobile devices were unmanaged; 38% of all State and local devices were unmanaged.
- The phishing exposure rate was higher on unmanaged devices in 2022 (8.5% of them) than on managed devices (6%).
- One in 11 mobile devices (about 9%) still experience phishing attacks in 2022.

According to the report, about half (46%) of all attacks across all government sectors sought to steal credentials, with 70% of them attempting to install malware. It's this stat about credentials that has me really worried; all it takes is some solid social engineering to trick a user into giving up their credentials.

According to Lookout, 23% of all federal employees clicked on three or more phishing links, despite being notified that they had previously clicked on one.

20 Ways to Block Mobile Attacks

Don't let your guard down just because you're on a mobile device. Be just as careful as you would on a desktop!

WiFi

- Don't allow your device to auto-join unfamiliar networks.
- Always turn off WiFi when you aren't using it or don't need it.
- Never send sensitive information over WiFi unless you're absolutely sure it's a secure network.

Apps

- Only use apps available in your device's official store - NEVER download from a browser.
- Be wary of apps from unknown developers or those with limited/bad reviews.
- Keep them updated to ensure they have the latest security.
- If they're no longer supported by your store, just delete!
- Don't grant administrator, or excessive privileges to apps unless you truly trust them.

Browser

- Watch out for ads, giveaways and contests that seem too good to be true. Often these lead to phishing sites that appear to be legit.
- Pay close attention to URLs. These are harder to verify on mobile screens but it's worth the effort.
- Never save your login information when you're using a web browser.

Bluetooth

- Disable automatic Bluetooth pairing.
- Always turn it off when you don't need it.

Smishing (phishing via SMS)

- Don't trust messages that attempt to get you to reveal any personal information
- Beware of similar tactics in platforms like What's App, Facebook Messenger Instagram, etc.
- Treat messages the same way you would treat email, always think before you click!

Vishing (voice phishing)

- Do not respond to telephone or email requests for personal financial information. If you are concerned, call the financial institution directly, using the phone number that appears on the back of your credit card or on your monthly statement.
- Never click on a link in an unsolicited commercial email.
- Speak only with live people when providing account information, and **only** when you initiate the call.
- Install software that can tell you whether you are on a secure or fake website.

KnowBe4
Human error. Conquered.

This article and the attached graphics are redistributed with permission from KnowBe4.

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/

Feb. 9: SANS Webinar: Starting "OSINT: Open Source Intelligence" from Scratch

Feb. 9: SANS Webinar: What Works in Improving End User Phishing Awareness, Recognition and Resistance

Feb. 15: SANS Webinar: Getting Started with Fuzzing for Bug Discovery

Feb. 16: SANS Webinar: The Secret to Vulnerability Management

Feb. 24: SANS Webinar: SANS 2023 Incident Response Solutions Forum

Feb. 24: SANS Webinar: Rise of the Infostealers

View a list of upcoming SANS webcasts.

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