Monthly Cybersecurity Newsletter

April 2023 Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

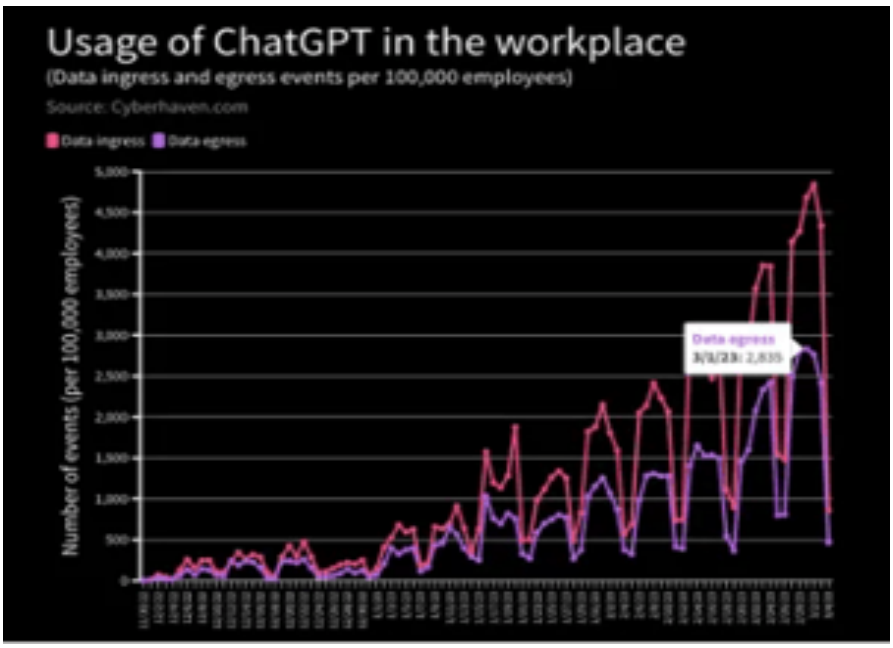
Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the Interim State Chief Risk Officer – Keith Briggs

---

Employees Are Feeding Sensitive Biz Data to ChatGPT, Raising Security Fears

The title said it all, and the news is that more than 4% of employees have put sensitive corporate data into the large language model, raising concerns that its popularity may result in massive leaks of proprietary information. Yikes.



Employees are submitting sensitive business data and privacy-protected information to large language models (LLMs) such as ChatGPT, raising concerns that artificial intelligence (AI) services could be incorporating the data into their models, and that information could be retrieved at a later date if proper data security isn't in place for the service.

In a recent report, data security service Cyberhaven detected and blocked requests to input data into ChatGPT from 4.2% of the 1.6 million workers at its client companies because of the risk of leaking confidential information, client data, source code, or regulated information to the LLM.

In one case, an executive cut and pasted the firm's 2023 strategy document into ChatGPT and asked it to create a PowerPoint deck. In another case, a doctor input his patient's name and their medical condition and asked ChatGPT to craft a letter to the patient's insurance company.

And as more employees use ChatGPT and other AI-based services as productivity tools, the risk will grow, says Howard Ting, CEO of Cyberhaven.

“There was this big migration of data from on-prem to cloud, and the next big shift is going to be the migration of data into these generative apps," he says. "And how that plays out [remains to be seen] — I think, we're in pregame; we're not even in the first inning.”

This article is redistributed with permission from KnowBe4.

Ring Device Phishing Campaign Uncovered

A recent phishing campaign leveraging the popular Ring security device has been uncovered. Attackers are targeting Ring customers with malicious emails containing links to phishing websites that look like official Ring support pages. These websites appear to provide support services and troubleshooting assistance, but instead attempt to steal passwords and other personal information from users.

The emails sent from the attackers typically contain broken English and use the Ring logo. The emails instruct the recipients to “verify” their accounts by clicking a link, which leads to a fake service page. This page then requests the user to enter their Ring username and password, which the attackers then harvest and use to gain access to the user’s account.

To protect yourself from this type of phishing attack, it is important to be aware of the red flags that may indicate a malicious email. These include typos, grammatical errors, and URLs that do not match the official Ring support website. Additionally, if an email requests a password, it is likely that it is not from the legitimate Ring account.

In response to this attack, Ring has issued a warning to its customers, urging users to remain vigilant and only click on links from official websites. It is also advised to use two-factor authentication when logging into Ring accounts, as this provides an extra layer of security that can help protect users from malicious actors.

Overall, phishing campaigns are an ongoing threat to customers of online services. Ring users should be aware of the risks posed by such campaigns and take precautions to protect themselves, such as changing passwords regularly and enabling two-factor authentication when available.

Shoulder Surfing in Public Places

Shoulder surfing is a type of social engineering attack that involves someone looking over the shoulder of another person in a public place as they enter usernames, passwords, credit card information, and other personal, confidential, or financial information into their device. It is a simple, yet effective way for an attacker to gain access to someone's personal data. The goal of shoulder surfing is for an attacker to collect enough of the victims' personal information such as usernames, passwords, Social Security numbers, and credit card numbers to conduct fraudulent activities

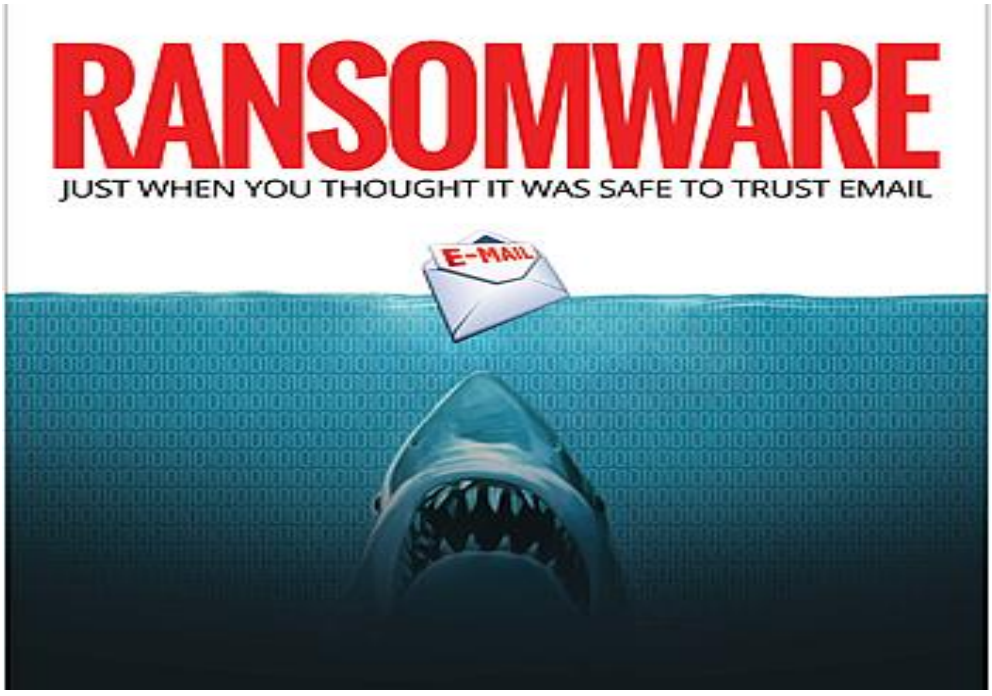
This problem can occur in a variety of places, but one of the most common places where it might happen is in a bar or other social gatherings. It's important for people to be aware of the potential risks of shoulder surfing and to take precautionary steps to protect themselves should they find themselves in a situation where they are susceptible to this type of attack. Some precautions include: covering your hand as you enter your info, using a physical barrier such as a book as a shield to block the view of any shoulder-surfers, and using a distraction to distract potential shoulder-surfers. It is also important to make sure that your device is password protected, and that you choose strong passwords and never share them with anyone. Furthermore, it's essential to regularly change your passwords and enable two-factor authentication where available. Taking these precautions can help protect people from the various dangers of shoulder surfing.

This image is redistributed with permission from KnowBe4.

To defend yourself against shoulder surfing, you should be aware of your surroundings when using a device in public places. Try to keep an eye out for people that may be standing or sitting too close or lingering around longer than expected. You should also be mindful to shield your device's screen when entering in passwords or personal information or take steps to use two-factor authentication to protect your accounts.

If you feel like you're being targeted by someone attempting to engage in shoulder surfing, the best thing to do is remove yourself from the situation and contact the authorities. Shoulder surfing is a form of identity theft that often results in financial theft and fraud. It is important to take all necessary precautions to protect your personal information, both personal and online.

The Emerging Threat of LockBit 3.0 Ransomware



This image is redistributed with permission from KnowBe4.

The emergence of LockBit 3.0 is a cause of serious concern for individuals, businesses, and organizations alike. It's a sophisticated ransomware variant that has already caused significant damage worldwide. The virus is designed to encrypt files on the system and hold them for ransom payment from victims. In this blog post, we will take a closer look at the LockBit 3.0 and what you need to know to protect your systems.

What is LockBit 3.0?

LockBit 3.0 is a ransomware virus that uses sophisticated encryption methods to encrypt files on the infected system or network. Once the virus encrypts files, it demands a ransom payment in return for the decryption key. The virus can infect computers and networks through various means, including

email, software vulnerabilities, and phishing. This ransomware variant is considered to be one of the most dangerous due to its complexity and ability to evade anti-virus programs.

Here's how it typically works:

1. The attacker delivers the LockBit 3.0 ransomware to the victim's computer through a malicious email attachment or by exploiting a vulnerability in the victim's system.

2. Once installed, LockBit 3.0 searches the victim's computer for files to encrypt, such as documents, spreadsheets, images, and videos.

3. LockBit 3.0 uses strong encryption algorithms to lock the victim's files, making them unreadable and inaccessible. The attacker then displays a message on the victim's screen, demanding payment in exchange for the decryption key.

4. The attacker typically demands payment in Bitcoin or another cryptocurrency, as they are difficult to trace.

5. If the victim pays the ransom, the attacker sends the decryption key to unlock the files. However, there is no guarantee.

This image is redistributed with permission from KnowBe4.

How can you protect yourself from a Lockbit 3.0 Ransomware Attack?

LockBit 3.0 is a type of ransomware that can infect your computer system and encrypt all of your files, making them inaccessible unless a ransom is paid. Here are some ways to protect yourself:

1. Update your software and operating system regularly to ensure that the latest security patches are installed.

2. Install updated antivirus software and keep it up to date.

3. Be vigilant about suspicious emails and phishing attempts. Do not click on any links or attachments from unknown sources.

4. Backup your data regularly and store it in a secure, off-site location. This way, if you are hit by ransomware, you can restore your data quickly without paying the ransom.

5. Use strong passwords and two-factor authentication to secure your accounts.

6. Limit access to sensitive files and data only to authorized personnel.

7. Always follow your organization security policies.

8. Also, follow your organization's incident response procedures if you suspect or become a victim of ransomware at work.

By following these steps, you can reduce the risk of a LockBit 3.0 infection and protect your data from being held ransom.

What is CoP and Why Should Companies Implement it

A Community of Practice (CoP) is a group of people who share a common interest, profession or domain of knowledge and come together to share information, experiences, and insights related to their field of expertise. CoPs can be found in various settings, including organizations, universities, and online networks. Members of a CoP learn from one another, collaborate on projects and help each other to solve problems. It's a way to connect with like-minded individuals and develop expertise through collective learning.

The State of North Carolina uses a consolidated method of CoP which allows several different agencies and professionals to come together on a monthly basis to brainstorm ways to improve state processes. This online platform for state government employees promotes collaboration, knowledge sharing and professional development across agencies throughout the state.

There are several reasons why companies should incorporate a CoP within their organization:

Firstly, COP helps to establish and maintain high standards of conduct within the company. By outlining what is expected of employees and management in terms of ethical behavior, legal compliance, and overall best practices, COP can prevent unethical or illegal actions that could harm the company's reputation or bottom line.

Secondly, COP can improve communication and collaboration within the company. By providing clear guidelines for decision-making and behavior, employees are more likely to work together effectively, avoiding misunderstandings and conflicts.

Thirdly, COP can help companies attract and retain top talent. Companies that are known for their strong ethical and professional standards are more appealing to job seekers who value these qualities in a workplace.

Overall, implementing a COP can help a company ensure their success by fostering a culture of accountability, transparency, and ethical behavior.

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

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/

Apr. 3: SANS Webinar: SANS 2023 - Featured Keynote: ChatGPT, GANs, and Deep Learning: Pulling Back the Curtain

Apr. 5: SANS Webinar: Managed Detection and Response: Optimizing External Expertise

Apr. 13: SANS Webinar: Cloud Security: Does the Endpoint Still Matter?

Apr. 13: SANS Webinar: A SANS First Look at Zero Trust-based Access Management and Remote Access for OT-IT-Cloud

Apr. 19: SANS Webinar: 2023 Survey Event | Threat Hunting: Focusing on the Hunters and How Best to Support Them

Apr. 20: SANS Webinar: Managing Apps on BYO and Managed Devices: How to Enforce Policies to Protect Your Data

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.*