SEP 2024

CENTRAL RESERVE POLICE FORCE

CYBER BYTE

New Android Malware NGate

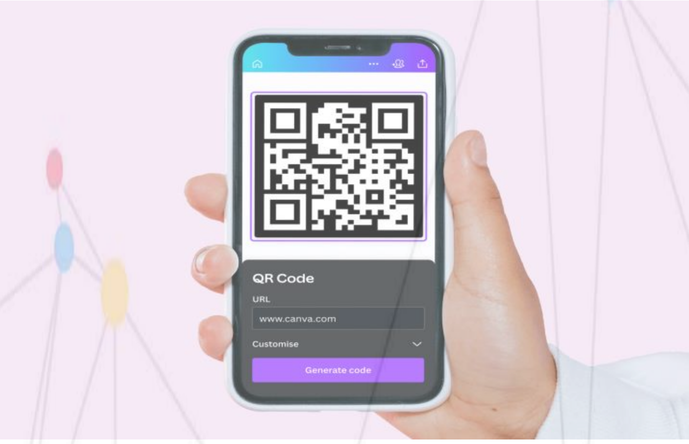
Steals NFC data to Clone contactless payment card.

Biggest Cyber Fraud ever in India

A 75-year-old man has been defrauded of Rs 13 crore.

1.CYBER GEEKS NEWS

A) New QR Code Phishing Campaign Exploits Microsoft Sway to Steal Credentials.



A new QR code phishing campaign uses Microsoft Sway to host fake pages, exploiting its legitimacy to trick victims. Targeting users in Asia and North America, the attacks focus on the technology, manufacturing, and finance sectors.

Suggestions: -

- To protect yourself from QR code phishing attacks, understand how they work and ensure your safety when scanning codes.
- Always verify the source of a code before scanning and watch for typos, misspellings, or suspicious URLs.
- Enroll in QR code security training to learn about risks and how to avoid them.
- Use reliable QR code scanning apps and enable two-factor authentication.
- Ensure your device has up-to-date antivirus software.
- Never share personal information unless you're sure the website is legitimate.

B) Cyber Security Advisory BY National Critical Information Infrastructure Protection Centre.

It has been observed that attackers are targeting government personnel using spoofed / compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

Modus Operandi of the Phishing Attacks: -

Case 1: The spear-phishing email contains a HTML frame with the headline "keep the same password" & "Skip upto 6 months". Upon clicking, it redirects to a URL, which is a phishing email. The Firefox and Chrome browsers detect this URL as a dangerous site.

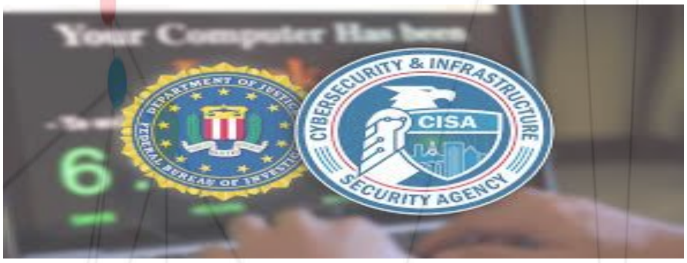
Case 2: The spear-phishing email contains a link that leads to a cloned page mimicking "mod.gov.in" or "ddpdoo.gov.in," with a prompt for NIC mail credentials. The active malicious IP could compromise user credentials or spread malware.

Suggestions: -

- Install and regularly update antivirus software.
- Install Updates and Patched regularly.
- Conduct regular backup practices and keep those backups offline or on a separate network.
- Implement Multi-Factor Authentication (MFA).

- Never click and execute email attachments from unknown sources.
- Never open links shared on social media from unknown sources.
- Never run unknown files with exaggerated titles.

C) The FBI and CISA Issue Joint Advisory on New Threats and How to Stop Ransomware: -



The FBI and CISA issued a joint advisory as part of their ongoing #Stop Ransomware effort to help organizations protect against ransomware. The latest advisory outlines three key actions to mitigate cyber threats from ransomware: installing updates as soon as they are released, requiring phishing-resistant MFA (i.e., non-SMS text-based), and training users. The surge in ransomware and data breaches now demands that cyber defenses keep pace with new attacks and disclosures. This issue stems from rapid advancements in cybercriminal methods and a slow response from many organizations. Generative AI has further transformed cybercrime, requiring urgent updates to defense strategies.

D) New Android Malware N-Gate Steals NFC Data to Clone Contactless Payment Cards.

Cybersecurity researchers have discovered new Android malware that relays contactless payment data from credit and debit cards to an attacker's device for fraudulent use.

The N-Gate malware has the unique ability to relay data from victims' payment cards, via a malicious app installed on their Android devices, to the attacker's rooted Android phone.

The end goal of the attacks is to clone near-field communication (NFC) data from victims' physical payment cards using N-Gate and transmit the information to an attacker device that then emulates the original card to withdraw money from an ATM.

Suggestions: -

- Don't keep your cards in easy-to-reach pockets or bags that might attract pickpockets.
- Line your wallet with tin foil to block scanning devices, or use RFID-blocking products for similar protection.
- Don't let your card out of sight during payment; it could be skimmed for data.
- Don't give your card to friends for payments; be present for all transactions.
- Ask for a receipt to make sure you were charged the correct amount.
- Keep a close eye on bank statements and your credit report to look for any unusual activity.

2.CYBER FRAUDS

Cyber frauds cost India Rs 177 crore in FY24:

The amount of money lost due to cyber fraud in India has more than doubled from Rs 69.68 crore in FY23 to Rs 177.05 crore in FY24.

Rising cyber fraud losses are a troubling trend. If a customer's negligence leads to a loss, they must cover it until reporting the unauthorized transaction to the bank.

The Reserve Bank of India (RBI) has issued guidelines to limit customer losses for unauthorized transactions, which can be avoided if reported within 3 working days and if bank negligence or other system faults are proven.

If a customer reports an unauthorized transaction within 4 to 7 working days, their liability may range from Rs 5,000 to Rs 25,000, depending on the account type. Beyond 7 working days, liability is governed by the bank's policy. The bank must prove customer negligence for unauthorized transactions.

Biggest Cyber Fraud Ever in India: Telangana's Cyber Security Bureau is investigating a major cyber financial scam where a 75-year-old retired manager was defrauded of Rs 13 crore. The victim was tricked by scammers offering an investment opportunity via WhatsApp.

Lured by high returns, the man invested Rs 4 crore. When his balance reached Rs 10 crore, he tried to withdraw but was told he needed to pay additional fees. Believing he could recover his investment and profits, he transferred an extra Rs 9 crore over the next 15 days.

The ED has arrested four people in Bengaluru over a Rs 25 crore cyber investment scam. They were involved in creating companies and bank accounts to launder scam funds.

3. TIP OF THE MONTH

Phishing

In today's fast-paced world, scammers exploit current events for personal gain. They use events in the news to trick us into revealing sensitive information. Understanding these tactics is crucial in safeguarding data and systems.

The recent incidents highlight how quickly scammers can capitalize on a situation. Soon after, scammers sent phishing emails claiming solutions for these issues. They used social engineering tactics to get recipients to click on malicious links.

In addition, others examples of current event scams include:

Natural disasters: Bad actors have impersonated charities to steal donations meant for relief efforts.

Major data breaches: Criminals have posed as affected companies, requesting users to "verify" their account information.

Suggestions: -

Be skeptical of urgent requests.
Scammers use urgency to push quick decisions. If you get an urgent email, pause and verify the sender.

Verify the source.
Check the sender's email and links for typos or suspicious signs before clicking, as they may indicate phishing.

Beware of emotional manipulation.
Scammers use fear, curiosity, or greed to lure clicks. Be cautious of emails with strong emotional appeals or extraordinary promises.

आभार

DIRECTORATE GENERAL
CRPF