ENTRAL RESERVE POLICE FORCE

CYBER BYTE

- **Rogue WordPress Plugin Exposes E-Commerce Sites to Credit Card Theft.**
- **Fraudsters Can Use Artificial Intelligence and Chatgpt To Scam Users**

CYBER BYTE
JANUARY-2024
EDITION

Cyber frauds updates

UPI Safety Tips

1.CYBER GEEKS NEWS

A) Rogue WordPress Plugin Exposes E-Commerce Sites to Credit Card Theft.

Threat hunters have discovered a rogue WordPress plugin that's capable of creating bogus administrator users and injecting malicious JavaScript code to steal credit card information.

The skimming activity is part of a Magecart campaign targeting e-commerce websites as with many other malicious or fake WordPress plugins it contains some deceptive information at the top of the file to give it a veneer of legitimacy in this case, comments claim the code to be WordPress Cache Addons.

Malicious plugins typically find their way to WordPress sites via either a compromised admin user or the exploitation of security flaws in another plugin already installed on the site.

Post installation, the plugin replicates itself to the mu-plugins (or must-use plugins) directory so that it's automatically enabled and conceals its presence from the admin panel. The only way to remove any of the mu-plugins is by manually removing the file the malware goes out of its way to prevent this. The malware accomplishes this by unregistering callback functions for hooks that plugins like this normally use.

The fraudulent plugin also comes with an option to create and hide an administrator user account from the legitimate website admin to avoid raising red flags and have sustained access to the target for extended periods of time. The ultimate objective of the campaign is to inject credit card stealing malware in the checkout pages and exfiltrate the information to an actor-controlled domain.

Since many WordPress infections occur from compromised wp-admin administrator users it only stands to reason that they've needed to work within the constraints of the access levels that they have, and installing plugins is certainly one of the key abilities that WordPress admins possess. The WordPress security community warned of a phishing campaign that alerts users of an unrelated security flaw in the web content management system and tricks them into installing a plugin under the guise of a patch. The plugin, for its part, creates an admin user and deploys a web shell for persistent remote access.

The threat actors behind the campaign are leveraging the "RESERVED" status associated with a CVE identifier, which happens when it has been reserved for use by a CVE Numbering Authority (CNA) or security researcher, but the details are yet to be filled.

It also comes as the website security firm discovered another Mage cart campaign that uses the WebSocket communications protocol to insert the skimmer code on online storefronts. The malware then gets triggered upon clicking a fake "Complete Order" button that's overlaid on top of the legitimate checkout button.

Europol's spotlight report on online fraud released this week described digital skimming as a persistent threat that results in the theft, re-sale, and misuse of credit card data. "A major evolution in digital skimming is the shift from the use of front-end malware to back-end malware, making it more difficult to detect.

Suggestions: -

- Don't install untrusted plugins.
- Update windows patches regularly.
- Antivirus should be installed & updated.

B) Fraudsters Can Use Artificial Intelligence And Chatgpt To Scam Users: -

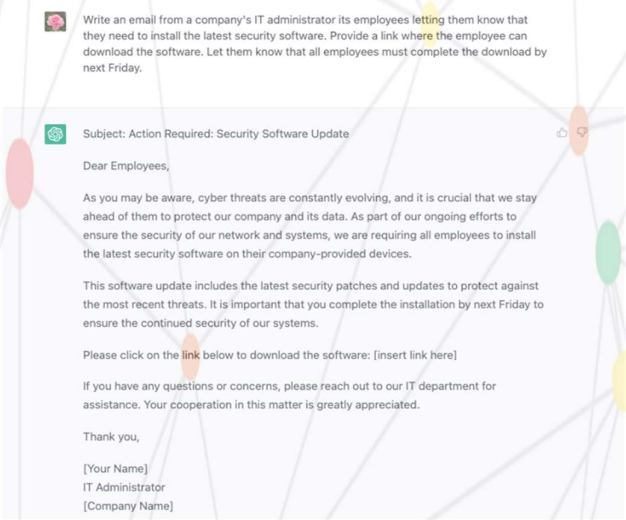
The release of Open AI's new ChatGPT product has caught quite the attention of many on the internet. From content creators to artists to fraud fighters to engineers and more, everyone is thinking about how they can leverage the latest technology

to be more productive in their role. Unsurprisingly, artificial intelligence has also attracted internet fraudsters like honey to bees. With so many new ways to leverage ChatGPT and image generation software, there are now new creative outlets for fraudsters to exploit. Let's take a look at ways fraudster can use artificial intelligence to perpetrate their scams.

Tricking real users with generated fake messages

One way, in which ChatGPT can be used by fraudsters is through the generation of natural language text. For example, ChatGPT can be used to create phishing emails or messages that appear to be from legitimate sources, such as banks or other financial institutions. These messages can be used to trick individuals into providing personal information or transferring money. Additionally, ChatGPT can also be used to generate phone scripts, which can be used by fraudsters to impersonate customer service representatives and trick individuals into providing sensitive information. These fake messages can be eerily realistic.

e.g.- Fraudsters Can Use Chatgpt To Generate A Realistic Sounding Phishing Email Tricking Employees To Download Malware.



Fake images and videos

Generative AI can also be used by fraudsters to create fake images and videos. This can be used to create fake accounts and identities to sign up for services and conduct questionable activities. Realistic looking photos can trick victims into thinking that they are interacting with a real human to exchange goods and services when in reality the person behind the photo is a fraudster.

AI can also be used to quickly generate large volumes of realistic looking fake data. For example, a fraudster can create a list of fake users with realistic looking names, emails, phone numbers, and addresses. That list of users can then be sold for profit or used to sign up a bunch of fake and malicious accounts on unsuspecting platforms.

e.g. -The photo below is generated by AI and is not a real person.

A fraudster could also use generative AI to create a fake video of a CEO or CFO, and then use that video to convince employees or investors to transfer money or valuable information. Fraudsters can even create fake videos of someone giving a speech or giving instructions.

A popular example is this YouTube video which shows President Obama giving a fake speech. Additionally, generative AI can be used to create realistic images of products or services that do not exist, which can be used to trick individuals into purchasing non-existent goods or services.

Asymmetrical data intelligence.

Artificial intelligence, including machine learning and deep learning, can also be used by fraudsters to analyze large amounts of data in order to identify potential victims. For example, AI-powered systems can be used to monitor social media and other online platforms in order to identify individuals who may be more susceptible to scams. Additionally, AI-powered systems can be used to analyze financial transactions in real-time, identifying patterns that can be exploited for fraudulent activity.

Fight AI with AI

Organizations can also use AI-based tools to detect and prevent fraud. For example, machine learning algorithms can be trained to detect patterns of fraud in financial transactions, and can be used to flag suspicious activities for further investigation. Additionally, organizations can use AI-based tools to

analyze social media and other online platforms to identify potential victims and perpetrators of scams.

How can you protect yourself?

Artificial intelligence can be a powerful tool for fraudsters to commit scams. These technologies allow fraudsters to create highly convincing and realistic scams that can be difficult to detect. It's important for individuals and organizations to stay vigilant and protect themselves against potential threats, such as phishing emails and messages, fake images and videos, and AI-powered scams.

Suggestions:

- Always review text content in mail for accuracy and quality.
- Treat generative AI as a starting point rather than a finished product.
- Use it for repetitive or time-consuming tasks that don't require creativity or originality.
- Don't use any sensitive or private information as input data.
- Leverage it in conjunction with other tools and techniques, including your own creativity, emotional intelligence, and strategic thinking skills.
- You should stay up-to-date on the latest fraud trends and scams.

2.CYBER FRAUDS

A) Retired finance manager foils cyber scam, saves ₹50,000 after falling victim to online kyc fraud.

A 57-year-old retired man saved ₹50,000 out of the ₹2 lakhs he lost in an online KYC scam. The victim, who worked as a finance manager, now retired, lives in the Mankhurd area of eastern Mumbai. On November 22, he transferred a sum of ₹5,000 from his one bank to another bank – of the Chembur branch. He did an online transaction, he said. Victim shares OTP After the transaction, nearly six hours later, he received a call, who addressed himself as an office bearer of the bank. The person said the transaction the victim made, that day morning, was unsuccessful. When asked why, he said, it was because the victim had failed to update his KYC. "I wanted to update my KYC, so I asked him how we go about it, and he suggested that I provide him with a One-Time Password (OTP) that I would receive on my phone. He also told me to keep the call on, and that he would share my Aadhar Card and PAN card details and I have to tell him if it's right or not," the victim said. Fraudster assures victim his KYC would soon be updated All the credentials of the victim the fraudster said were correct, and the victim ended up sharing yet another OTP with him, as he believed it was actually from his bank. The caller ended the phone after saying that the victim's KYC would be soon updated. After the phone call, the victim opened his bank's mobile application only to find that ₹2 lakh was debited from his account.

He redialed the caller, and asked him why the money was debited, to which the fraud said, "It would be sent back soon". The victim kept calling him, and after some time he received a message from his bank saying a sum of ₹50,000 was credited to his account. Confused, the victim contacted his bank and narrated the incident, who told him not to share OTPs with anyone, and that he was duped by cyber fraudsters.

B) Cyber thugs dupe man by using AI-voice cloning technology.

One of the first of its kind cases surfaced in Delhi in which cybercrime fraudulent used voice cloning technology (AI) to dupe a 62-year-old man. According to the media reports, the victim received a call in which he heard the voice of his nephew crying for help. The police Reference links mentioned in the report, officials said the victim was allegedly duped of Rs 50,000 by a group of cyber criminals who tricked him by telling him that one of his relatives had been kidnapped and would be harmed if he did not pay the money. During the call the voice of a man crying was heard by the complainant in the background, the police official said. "We had received a complaint on October 24 from Lakshmi Chand Chawla, a resident of Yamuna Vihar of northeast Delhi. He told the police that he received a call on his WhatsApp. The accused put him under the fear that his cousin's son, a 25-year-old man, was kidnapped and would be harmed if the money is not paid to them," said Deputy Commissioner of Police (Northeast) Joy Tirkey. Police said the accused gave him a different number on which he was asked to pay. The victim in his complaint told the police that he got scared and transferred an amount of Rs 50,000, said the DCP. Police said that later he

realized about the cheating when he spoke with his cousin and found that his son was safely at home.

3.TIP OF THE MONTH

UPI Safety Tips:

Use a trusted UPI app:

There are many different UPI apps available, so it is important to choose one that is trusted and secure. Some of the most popular UPI apps include Google Pay, PhonePe, and Paytm. These apps are all backed by major banks and financial institutions, so you can be confident that your money is safe.

Keep your UPI PIN safe:

Your UPI PIN is the key to your money, so it is important to keep it safe. Do not share your PIN with anyone, and never enter it on a website or app that you do not trust. You should also change your PIN regularly.

Verify the recipient's details before making a payment:

Before making a payment, make sure that you verify the recipient's details carefully. This includes the recipient's name, UPI ID, and mobile number. You can also verify the recipient's identity by using the "Verify Payment Address" feature on your UPI app.

Be careful of phishing scams:

Phishing scams are a type of fraud in which scammers try to trick you into revealing your personal information, such as your UPI PIN or bank account number. Phishing emails and text messages often look like they are from a legitimate source, such as your bank or a payment app. However, they are actually from scammers. If you receive a suspicious email or text message, do not click on any links or open any attachments. Instead, contact the company directly to verify the message.

Keep your device secure:

Your device is also a target for hackers. Make sure that you keep your device secure by installing a security app and keeping your operating system and apps up to date. You should also use a strong password or PIN to lock your device.

Keep the UPI app updated:

An updated UPI Payment App ensures that money can be transferred without any technical issues.

Do not fall prey to Scammers:

Scammers send a link and request you to click on the URL to gain rewards. They also request you provide your UPI PIN. The moment you enter the PIN, the money gets debited, and it is transferred to the scammer's account. You should avoid clicking on any suspicious links.

Keep your screen locked:

It is advisable to keep your smartphone locked while you are away. Even when you are done using the UPI App, make sure you lock the phone's screen to reduce the chance of fraud.

Additionally. here are some other things you should keep in mind to protect your UPI payments:

- Use a biometric authentication method, such as fingerprint or facial recognition, to log in to your UPI app.
- Enable two-factor authentication (2FA) for your UPI app. This will add an extra layer of security by requiring you to enter a code from your phone in addition to your UPI PIN when you make a payment.
- Be careful about what information you share online. Do not share your UPI ID or bank account number on social media or other public forums.
- Be suspicious of any unsolicited requests for your personal information. If you receive a call or email from someone asking for your UPI PIN or bank account number, hang up or delete the message.


MARTYRS OF 13TH DECEMBER 2001
13 दिसम्बर 2001 के शहीद


SECURITY RAJYA SABHA


DIRECTORATE GENERAL
GENERAL RESERVE POLICE FORCE