Indian Cyber Crime Coordination Centre

DAILY DIGEST

26th May 2023

Prepared by
Indian Cyber Crime Coordination Centre
Ministry of Home Affairs

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
सत्यमेव जयते

G20 भारत 2023 INDIA

National

S. No.	News	Source
1.	Surat Cybercrime Police Seize Rs 1.41 Crore in high currency notes used in Cryptocurrency fraud and online investment scam	Times of India
2.	Notebooks will create awareness on cyber safety introduced for students by Dr. Ananth Prabhu G	Times of India
3.	Kolkata Police organizes first Facebook Live session on e-crime	India Times
4.	An accused of cheating on OLX fraud has been arrested by the cyber cell team from Haryana from Bharatpur	ABP Live
5.	A scammer duped a man of over Rs 5 crore using AI face-swapping technology	India Today
6.	Gurugram man loses over 70 lakhs after part-time job scam	India Today
7.	Cyber crooks dupe patients in the name of confirmation of appointment of Aditya Birla Memorial Hospital doctors	Hindustan Times
8.	A cybercrime organization called the Lemon Group has reportedly infected 8.9 million Android devices worldwide with a Guerilla malware	Kalinga TV
9.	4 arrested for cheating Rs 2.8 lakh, four ATM cards seized	The Tribune
10.	Three people have been arrested for duping people of lakhs of rupees on the pretext of investing in cryptocurrencies	The Tribune

International

S. No.	News	Source
1.	South Korean researchers have developed an artificial intelligence (AI) model that has been trained to spot cyber security red flags on the dark web	Mssp Alert
2.	Thieves use new tool to hack into cell phones on public Wi-Fi and access other personal information	Click 2 Houston
3.	AhRat Android RAT was concealed in iRecorder app in Google Play	Security affairs
4.	Chinese hackers breach US critical infrastructure in stealthy attacks	Bleeping Computer

National

Surat Cybercrime Police Seize Rs 1.41 Crore in high currency notes used in Cryptocurrency fraud and online investment scam

The Surat cybercrime police seized a huge haul of currency notes worth Rs 1.41 crore that from a house in the Unn Patiya area of the city on Wednesday. Acting on specific information, the cybercrime sleuths raided the house of Akram Hussain Patel in the Dabarnagar locality and seized the notes. Of these, there were 500 tenders of Rs 2,000 denomination each, amounting to Rs 10 lakh, and 23,100 notes of Rs 500 denomination each total worth Rs 1.15 crore. Other notes included 6,000 of Rs 200 denomination and 3,500 of Rs 100 denomination.

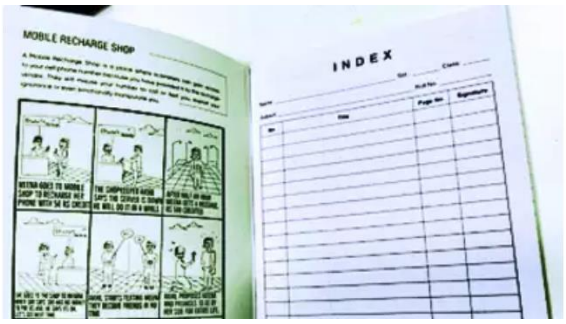
Police suspect that the cash could be used for cryptocurrency fraud or some online investment scam. Investigators said they had information that Patel was involved in cybercrime offences.

However, the source of such large cash is being investigated. Assistant commissioner of police, YA Gohil, said : "We raided the house based on information that a cybercrime was being carried out from the house and that there is a big amount of cash there. We have seized the cash as per section 102 of the criminal procedure code." As the amount is large, the police have also informed the income tax department. "We strongly suspect that the cash was accumulated from cheating or some cyber fraud," Patel said.

Patel, however, was not found at his home and the police have launched a manhunt to trace him. The recovery of Rs 2,000 denomination notes raised eyebrows as the government has decided to withdraw the notes from circulation. They will continue to be legal tenders even after September 30 deadline to exchange or deposit them in the banks.

Notebooks will create awareness on cyber safety introduced for students by Dr. Ananth Prabhu G

With a rise in cybercrime cases and cyber safety still not being taught in several schools and colleges in the state, cyber security



expert Ananth Prabhu G has tied up with School Book Company, Udupi, to print notebooks with pages dedicated to awareness on cyber safety.

Ananth Prabhu said, "I was wondering what could be done to ensure that children browse the internet responsibly and understand the perils of the digital world. I tied up with the School Book Company, Udupi, and requested them to come out with the Cyber Safe India series. The books are not charged anything extra, but every book will have three infotoons from the CyberSafe girl v5.0 book, cyber safety tips for mobile and internet users and the important cyber laws of India. The inner cover (front) has one infotoon and the back bind has two infotoons. One page is exclusively dedicated to mobile and internet safety tips, and at the back are the important cyber laws of India."

Prabhu said that this was an attempt made to ensure that without being a burden on the pockets of students, the much-needed information was incorporated. "I am willing to share details on cyber safety with any publishers across the country wanting to incorporate this in their notebooks. The Cybersafe girl e-book is available online for free, and already five crore downloads have taken place. The fifth version has references to 50 different cyber crimes, and the sixth version to be launched soon will have 65 different crimes, indicating that about 15 crimes have increased in a year, because of AI. These books have been published in

Kannada, Konkani and Gujarati. Soon, Kannada infotoons will be introduced in the ruled and unruled books,".

The next version of the notebooks will have QR code-based videos. School Book Company, Udupi, has a tie-up with many schools in Udupi, and the books are printed in eight different colours, so that students have access to the whole set. So far, 1 lakh books have been printed and distributed in

seven schools, said Prabhu, requesting the state government to ensure mandatory printing of this message in all notebooks distributed to the students of government schools.

Kolkata Police organizes first Facebook Live session on e-crime

If you have any doubts about any transaction, call up Lalbazar helpline number – 8585063104 – and seek their advice. You can also call any divisional cyber cell and seek help before carrying out the transaction, Kolkata Police announced on Wednesday.

Jolted by the multiple cases of fraud across ATMs, social networking sites and e-commerce sites ever since the pandemic, the detective department organized its first Facebook Live in the post pandemic era where the announcement was made.

The cops took questions online and even brought cyber crime victims face-to-face with the virtual audience who described their exper-iences. The one-hour session saw around 300-350 online participants.

Commissioner of police Vineet Goyal said it was important to save yourself from fraud. "At times, even the educated fall prey to such traps. Whether it is a loan scam, social engineering fraud or sextortion, it is important not to feel shy or repentant and inform us. We are there 24X7 for you and ready to guide you at all times," said Goyal.

The cyber cell organized the second part of the programme that detailed new age digital crimes, mainly on popular social media platforms. As many as 623 persons were present for the online programme, one of the most well-attended events in recent awareness drives by Lalbazar.

An accused of cheating on OLX fraud has been arrested by the cyber cell team from Haryana from Bharatpur

Mewat region of Bharatpur district of Rajasthan has become a mini Jamtara in cyber crime cases. Cheating has been happening in Mewat area of Bharatpur for a long time. Meanwhile, a cyber cell team from Gurugram in Haryana reached the Nagar police station area of Bharatpur to nab one of the accused, Zahir. In this way, the police of 15 states of the country keep raiding the Mewat area of Bharatpur to catch cyber criminals.

First of all, the thugs of Mewat area used to cheat people by telling them brass bricks to be gold. After that, the people of Mewat region changed the way of cheating and by advertising on OLX, thugs pretending to be army soldiers or officers and advertising to sell any car, motorcycle, other household items, call people or advance money from them in their account. They used to do fraud by tricking. These thugs vacate people's accounts by posing as officials of the electricity company, by asking OTP or by pretending that their bank accounts are closed.

So many cases have been registered so far

According to the information, in the year 2021, 82 cases were registered in Bharatpur and 23 people were arrested. In the year 2021, 106 cases of cybercrime were registered in Alwar district and 110 people were arrested by the police. In Bharatpur district, in the year 2022, 72 cases were registered in different police stations of Bharatpur and 27 people were arrested. In the year 2022, 137 cases of cybercrime were registered in Alwar district in which 17 people were arrested. From January 2023 to March, Bharatpur police has registered 42 cases of cybercrime and 23 thugs have been arrested. Similarly, 36 cases have been registered by the Alwar police.

what the police have to say

Superintendent of Police Shyam Singh has told that about 125 villages of 8 police station areas of Bharatpur district are affected by

cybercrime. It was revealed in the police survey that

thugs hide their identity by bringing sims from other states. Sims are brought from Assam, Odisha, and West Jungle. Police investigated by taking mobile data of those states, after that about one lakh SIM and one lakh 11 thousand Android phones were blocked. In April, 36 thousand SIMs have been found active in Mewat area. There have been 21 thousand complaints on these 36 SIMs. Police have seized about 800 motorcycles from Mewat area, which were used by these miscreants for crime. Till now 500 accused have also been arrested.

A scammer duped a man of over Rs 5 crore using AI face-swapping technology

The age of Artificial Intelligence (AI) is here and people across the world are finding new ways of using the technology to make their lives simpler. AI is being used to write essays and poems, simplify and explain code, compose poetry and music, and a lot more. Over time, people started realising the possible downsides of the emerging technology as well and creating deepfake images and videos turned out to be one of them. However, a man in Northern China went a step ahead and used deepfake technology to dupe a man of over Rs 5 crore.

For the unversed, deepfakes refer to fake images and videos online that look real and can be used to spread misinformation.

Man dupes victim of over Rs 5 crore using AI

According to a Reuters report, a scammer in Northern China used highly advanced 'deepfake' technology and convinced a man to transfer money into his account. The scammer used AI-powered face-swapping technology and impersonated the victim's close friend.

The police in Baotou city, as per the report, said that the fraudster impersonated the victim's friend while being on video call and asked him to transfer 4.3 million yuan (around Rs 5 crore).

TRENDING TOPICS

The victim, believing that his friend was in dire need of money during a bidding process, transferred the amount. The police also revealed that the victim realised what had transpired only after his friend (whom the scammer impersonated) expressed 'ignorance at the situation'. Also, the police have recovered most of the stolen funds and are working to trace the rest of the amount.

The incident has raised concerns in China over AI being used to carry out financial crimes.

AI voice-related scam

TRENDING TOPICS

This is not the first time that AI has been used to dupe a person of their hard-earned money. Last month, a case left the world shocked in which scammers used AI to clone a teenager's voice and demand ransom from her mother.

A report by WKYT, a US-based news channel affiliated with CBS news, revealed how a woman from Arizona, Jennifer DeStefano, got a call from an unknown number one day that turned her world upside down.

DeStefano told the news channel that her 15-year-old daughter was out on a skiing trip when she received the call. The moment she picked up the phone, the woman heard her daughter's voice saying 'Mom' followed by sobbing. What followed next was a man's voice threatening the woman to not go to the police.

The woman then added that she could hear her daughter's voice in the background, calling for help. The man then demanded USD 1 million to let the teenager go.

"It was never a question of who is this? It was completely her voice. It was her inflection. It was the way she would have cried," the victim told the local news media and added, "I never doubted for one second it was her. That's the freaky part that really got me to my core."

However, her daughter was safe and sound and had not been kidnapped at all.

Gurugram man loses over 70 lakhs after part-time job scam

In the past few months, there has been a rise in cases of online fraud. Many people across the country have fallen victim to online fraud, losing lakhs. Scammers are targeting innocent people through social messaging apps like WhatsApp and Telegram, luring them into part-time job opportunities on the pretext of earning extra money. In a reported case, a man from Gurugram ended up losing Rs 70 lakh after falling for a similar scam.

According to the Indian Express, the victim, a resident of Sector 43 in Gurgaon, fell into the trap of scammers after receiving a message on his mobile. In his complaint, the victim stated that on February 27, he received a message about a part-time job opportunity to earn extra money. The job involved small tasks like rating hotels and liking videos. In return, the scammers promised him a hefty commission. However, after falling for the promise, the victim ended up in debt as he borrowed money from his family and lost Rs 70 lakhs to the scammers.

"I was promised a commission of Rs 2,000-3,000. They opened a new bank account for me, in which they deposited Rs 10,000 as a trial bonus. I was given 30 tasks, and upon

completion of the first level, I had Rs 2,200 credited. After withdrawing the commission, they asked me if I wanted to continue, and when I replied affirmatively, they wiped the account clean and asked me to deposit Rs 10,000 again," said the complainant in the report.

After depositing more money, the victim was able to see his commission reflected in the account created by the scammers. To lure the victim further, the scammers even increased the amount shown on the account to gain his trust and make him deposit more. "They kept me under the impression that I was earning a lot, as many members in their Telegram group were sending screenshots of what they earned working for the fraudsters. But suddenly, a 'premium' task cropped up with an increased commission. Since it was a new task, they asked me to deposit Rs 63,000 to get started. I deposited it, after which they sent some money and commission to me. By the seventh day, I had sent Rs 27 lakh.

The victim further revealed that when he tried to withdraw his earned money, he received a message stating that since the amount he wanted to take out exceeded Rs 2 lakh, he had to give a security deposit worth 50 per cent of the total amount to the fraudsters.

"I did not have enough money, and it took several days before I could send it. When I sent a request for withdrawal, more tasks were shown. I bided my time and did all of them. By this time, I had lost around Rs 70 lakh. When I could not withdraw any further, I went to the police," the victim further revealed.

According to the complaint, the victim ended up in significant debt as he had borrowed loans against his house, his father's property, and his business. "Earlier, I had a business, but in a month, I have lost it all," he revealed.

Notably, the victim stresses that even after being denied withdrawal of the amount, the Telegram account where he was connected with the scammers and the groups where all the part-time tasks were given are still active.

Cyber crooks dupe patients in the name of confirmation of appointment of Aditya Birla Memorial Hospital doctors

In the latest scam to have surfaced, cybercrooks are conning unassuming patients and their kin seeking online appointments with doctors affiliated to the Aditya Birla Memorial Hospital (ABMH). Turns out the patients/relatives are using Google search services to find the contact numbers of ABMH (ABMH doctors) only to come across unauthorised numbers listed by the fraudsters. Upon calling these numbers,

the patients/kin are being cheated of huge sums of money in the name of confirming the doctors' appointments. Interestingly, the scammers seem to be well aware of the names, contact details, timing and availability of the doctors affiliated to ABMH.

So far, two incidents have come to light wherein patients/relatives have been cheated of ₹17,500 and ₹55,555, respectively. In the first such incident reported on April 12, a patient used Google search services to book an online appointment with a doctor at ABMH only to end up losing ₹16,000 and ₹1,500 in two separate transactions.

In the second incident, a complaint regarding which was filed on May 19, one Balasaheb Dhakne from Nigdi lost ₹55,555 while booking an online appointment with a doctor at ABMH. Dhakne complained to the hospital and the police. He said that while looking for ABMH's contact numbers to book an appointment, he came across a number on a non-ABMH website being paraded as a ABMH number. "Upon calling that number, my call got disconnected and a person called me back from another number to tell me that the hospital would get back to me. Later, I received an SMS from another number. Again, someone called me from a new number and told me to send a 'hi' on WhatsApp from my number. He then shared a link with me and asked me to fill in the patient's details and pay ₹ 10. Upon entering the UPI code, the payment failed. However, on May 14 at 1.48 pm, I got an SMS alert that ₹ 55,555 had been deducted from my account.

Saurav Chatterjee, senior general manager, ABMH, said, "We have been receiving various such complaints from our patients in writing and on the phone about this fraud for the last few weeks. We have already lodged complaints with the cybercrime cell for necessary action. Further, we have put up a notice in the interest of the public at large on our official website and on our social media platforms to alert our patients to be careful while making any such unauthorised transactions through unidentified telephone numbers."

In its complaint filed with the cybercrime cell of Wakad police station, ABMH stated that the hospital has realised that fraudsters are displaying unauthorised mobile numbers as belonging to ABMH on Google pages and asking patients for online payments in the name of confirming doctors' appointments.

According to Chatterjee, the numbers reported as used by the fraudsters for such transactions include: 9162124966, 9004676782, 9356153321, 07439279713, 8828824128, 08100085894, 07439303221, 078404005321, 08910218730, and 18002086388. He clarified that ABMH does not solicit payments through unidentified telephone numbers and all payment transactions are processed through authorised channels only. Those who suspect they are being taken for a ride should contact the hospital authorities and not fall prey to the scam, he said.

Sanjay Tungar, senior police inspector attached to the cybercrime cell of Pimpri-Chinchwad police, who is investigating the complaint, asked citizens to be cautious when availing online services and making online payments. "The patients and citizens should crosscheck the credentials of the number, website and links before making any payment. It is better if they contact the official number of the hospital for an appointment. Cybercriminals remain anonymous and one should not trust them to share details like names, numbers or bank details.

"Do not trust an unknown person whom you have never seen. Never click on an unknown link or install any application," Tungar warned.

In 2021, a similar phishing scam was reported in which families of patients in critical care and ICUs at private hospitals and Sassoon General Hospital had been targeted. Several patients and their relatives had been conned on the pretext of selling emergency medicines and injections.

A cybercrime organization called the Lemon Group has reportedly infected 8.9 million Android devices worldwide with a Guerilla malware

In another incident malware attack, a cybercrime organisation called the Lemon Group has reportedly infected 8.9 million Android devices worldwide with a Guerilla malware.

Among the nearly 9 million devices there are smartphones, watches, TVs, and TV boxes.

Japanese multinational cyber security software company, Trend Micro, reported that the malware has risked the accounts and personal data of Android users.

The Guerilla malware allegedly allows cybercriminals to perform various malicious activities such as stealing one-time passwords from SMS, hijacking WhatsApp sessions, loading additional payloads, setting up a reverse proxy from the infected device, and more.

According to cyber security software company, the malware has infected millions of Android devices across the world in over 180 countries.

India is in the top 10 list of countries affected by this malware including US, Mexico, Indonesia, Thailand, Russia, South Africa, Angola, Philippines, and Argentina.

Lemon Group is a large and sophisticated cybercrime organisation, which has been operating for several years. According to the report, the Lemon Group was first noticed by the cyber security firm in February 2022. However, it allegedly changed its name to

"Durian Cloud SMS" later. It still works with the same servers.

The Trend Micro company said in a blog post that they have detected over 490,000 mobile numbers used for OTP requests of Lemon SMS and, later, Durian SMS service. The customers of Lemon SMS PVA generate OTPs from platforms like JingDong, WhatsApp, Facebook, QQ, Line, and Tinder, among other applications.

The report reveals that the Lemon Group has installed Guerilla malware and other types of malware tools to attack victims. Though, there is noclear information on how the device got infected with the Guerilla malware. But, the company revealed that they have found that it is often pre-installed on devices that have been re-flashed with a new ROM.

Notably, the Guerilla malware can load additional plugins that carry out specific tasks, such as:

SMS plugin: It can steal the one-time passwords sent via SMS for WhatsApp, JingDong, and Facebook.

Proxy plugin and proxy seller: Attackers can use this plugin to invade victim's network resources by setting up a backward proxy from the infected phone.

Cookie plugin/WhatsApp plugin/Send plugin and promotion platform: These plugin sends Facebook cookies to a central server. The compromised device can then take control of WhatsApp sessions and send unwanted messages.

Splash plugin: This displays unwanted pop-up ads while users are using official apps.

Silent Plugin: This tool silently installs additional apps or removes existing ones based on instructions from a central server. The process happens in the background without the user noticing.

4 arrested for cheating Rs 2.8 lakh, four ATM cards seized

Anand Singh, a resident of Daria, allege that he had received a WhatsApp call from an unknown person who claimed that the complainant's son, Vipin Rawat, who is serving with the Assam Rifles, has been caught by terrorists. The caller told the complainant that if he wanted to save his son, then he would have to pay for that.

The complainant transferred a total of Rs 2.80 lakh in three instalments to the account number given by the fraudster. He later called his son up and

came to know that he had been duped. He informed the police about the incident. The cybercrime police registered a case.

During investigation, the police conducted a raid at Siwan, Bihar, and nabbed three suspects, identified as Divyanshu Kumar, alias Golu; Akash Kumar Thakur (20) and Rahiv Kumar (23).

During interrogation, the suspects revealed the name of a fourth suspect, Seeptain (23), in whose bank account the money was transferred. He was also arrested.

Four ATM cards and mobile phones have been seized from the suspects.

Three people have been arrested for duping people of lakhs of rupees on the pretext of investing in cryptocurrencies

Three men were arrested for allegedly duping people of lakhs of rupees on the pretext of investing in cryptocurrency, the police said on Wednesday. The accused were identified as Pushkar Jat (22), Vishal Tank (21) and Nitesh Mali (20), they said.

According to the police, the matter came to light in April after a complaint was filed by a resident of Mayur Vihar who alleged that she was cheated on the pretext of investing money in cryptocurrency. She was, instead, duped of Rs 7.80 lakh by a group of cheaters active on Telegram.

Initially, she received a message on WhatsApp regarding work from home and was given a task to post reviews on Google for different hotels and was paid some money to gain her trust. Later, she was asked to join Telegram and invest money in cryptocurrency through an APK android application.

She got suspicious when they blocked her account on Telegram and she was unable to withdraw the invested money, the police said. DCP (East) Amrutha Gugloth said that during the investigation, it was found that the cheated money was transferred into 8-10 different bank accounts in Haryana, Noida, Maharashtra and other parts of the country.

Information was procured regarding the alleged bank accounts in which partial cheated amount of Rs 2.23 lakh was transferred by the complainant. On the basis of technical evidence and surveillance, a raid was conducted in Akola, Chittorgarh, in Rajasthan and the three accused were arrested in the case.

"During the interrogation, it was revealed that these people were also selling bank accounts after activating net-banking and UPIs to foreign nationals from China, Indonesia, Nepal and other countries and receiving huge amount in exchange of these,"

she added. Mobile phones containing bank account details used in cheating, bank account kits and SIM cards were recovered, police said, adding further probe is underway.

International

South Korean researchers have developed an artificial intelligence (AI) model that has been trained to spot cyber security red flags on the dark web

The Korea Advanced Institute of Science and Technology (KAIST), in collaboration with data intelligence organization S2W, are behind DarkBERT, a generative AI language model that has been trained exclusively on datasets sourced from the dark web.

Revealing Cyber Threats from the Dark Web

DarkBERT can uncover cyber threats emanating from the dark web, including data leaks and ransomware. These characteristics are often exploited by cybercriminals, who use it to host underground markets and share illegal content, S2W stated.

DarkBERT is based on the RoBERTa architecture, an AI approach first developed in 2019. So far, it has been fed more than six million pages from the dark web as part of its pretraining on texts in English, according to multiple reports.

DartBERT and the Dark Web

Here's the key features of DarkBERT and facts about the dark web:

- The dark web is a corner of the internet accessible not by conventional web browsers, but by special software, like Tor, which anonymizes a user's IP address making it difficult to track their movements.
- The dark web can be characterized as illicit marketplaces where access to ransomware and other malware are sold, as well serving as a haven to drug traders, confidential information stealers and weapons brokers.
- The researchers crawled the dark web using the Tor software and curated a trove of content used to train DarkBERT.
- The DarkBERT project is dissimilar from ChatGPT or Bard in that it is not intended to act as a back-and-forth chat but rather as a vehicle to probe data sets and address specific queries.
- According to reports, DarkBERT fed two sets of data over 16 days, with some of the material redacted such as the names of

victim organizations, details on leaked data, threat statements, and illegal images. Over 1,000 pages of this data set were categorized as adult entertainment.

Don't count on DarkBERT's availability to the public owing the nature of the material in which it traffics. However, requests for the use of the AI model for academic purposes can be made.

Thieves use new tool to hack into cell phones on public Wi-Fi and access other personal information

Kristen Maurer of Magnolia is the founder of a K9 rescue charity who very recently needed to be rescued herself from an attack she never saw coming.

Maurer says a cyber pirate hacked his way into her cellphone.

"It's really terrifying because you have no idea what they can get into and what they can steal from you," Maurer said.

Maurer is just one of the people who have been victimized by cyber criminals armed with wild-looking devices, like something out of Star Wars, that they use to electronically smash their way into people's cellphones and then steal their most sensitive information.

In Maurer's case, the thieves rang up hundreds of dollars on her credit card and hacked into her email as well.

"What these guys were able to do to me was break into my personal email address, break into my credit card, and utilize it for their benefit. So, just what did she do wrong?

Absolutely nothing, other than use public WIFI systems, just like millions of us do every day.

Cyber thieves have created a brand new scheme that targets public WIFI users and it's called WIFI Jacking.

It's a crime that allows the crooks to actually break into your smartphone and take whatever they want, according to United States Secret Service Agent Michael Alvarez, a specialist in forensic network intrusion.

"This crime has been called the 'man-in-the-middle-attack' or 'WIFI Jacking' and what happens is these guys will set up outside of a public WIFI location, and as long as they're able to access the WIFI signal from that location, they can impersonate that WIFI and they can start setting up the attack," Alvarez said.

Colman Ryan is a forensic cyber detective with Kgriff Investigations in Houston and he shows KPRC 2 Investigates the high-tech equipment these criminals will use to pull off this crime.

"So, this is a very high-powered, directional antenna that these criminals use. It looks like a ray gun out of Star Wars, but it's actually a very powerful tool. What they are going to do is aim this thing in the direction of potential victims at a coffee shop, hotel, wherever there is a public WIFI network and they're going to force your smartphone onto their network. Once they do that, they can grab whatever they want from your phone, passwords, emails, credit card information, banking information.

In fact, these cyber pirates, Ryan says, can hack your phone even after you've left that public WIFI location because your phone remembers that WIFI network and the thieves can connect it to your phone.

To prove that, KPRC 2 asked Kelly Shidler, who also works in I.T., to use the WIFI at a local coffee shop. When she leaves the place, we follow her to her home.

Now, with Shidler's help, we're going to show how Ryan, using his high-powered antenna and the rest of his hacking equipment, can hack into her phone and take total control of it.

Now, parked down the block and across the street, 50 yards away, Ryan simply points his antenna at Shidler's house and the crime begins. Ryan uses that antenna to impersonate the WIFI network that Shidler was on at the coffee shop. He then forces her phone onto his network and boom, he now has control of her cellphone.

"I'm trying to force her phone onto my network. It's coming, and, and I've got her. I am in control now of her phone," Ryan demonstrated.

Now, to prove that Ryan's got the control he is bragging about, we ask Shidler to go to a favorite website of hers, but she never gets there. Instead, Ryan sends her to an inappropriate adult website.

Shidler is both stunned and flabbergasted, not by the website, but by what has just been done to her phone without her permission. I didn't want to go there. I can't believe it.

In Maurer's case, it wasn't just shock and surprise. Those hackers swept hundreds and hundreds of dollars after gaining access to her phone.

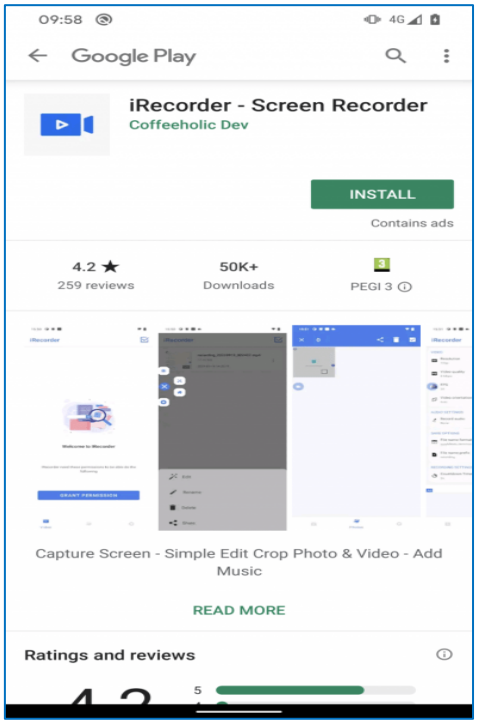
AhRat Android RAT was concealed in iRecorder app in Google Play

ESET researchers have discovered an Android app on Google Play that was hiding a new remote access trojan (RAT) dubbed AhRat.

The app, named iRecorder – Screen Recorder, has more than 50,000 installs. The app was initially uploaded to the Google Play store without malicious features on September 19th, 2021. Threat actors

introduced the support for malicious functionalities in version 1.3.8 which was uploaded on August 2022.

The app was designed to extract microphone recordings and stealing files with specific extensions, a circumstance that suggests it was involved in an espionage campaign. Researchers have not detected the AhRat anywhere else in the wild.



The AhRat is a customization of the open-source AhMyth Android RAT (remote access trojan). The AhMyth RAT supports various malicious functions, including exfiltrating call logs, contacts, and text messages, obtaining a list of files on the device, tracking the device location, sending SMS messages, recording audio, and taking pictures. However, ESET observed only a limited set of malicious features derived from the original AhMyth RAT in both versions of AhRat analyzed by its experts.

ESET immediately notified Google that quickly removed the iRecorder app from its store. The experts pointed out that the app can also be found in alternative and unofficial Android stores.

ESET was not able to link the AhRat malware to any known threat actors. The researchers only reported that previously, the open-source AhMyth was employed by the Pakistan-linked APT group Transparent Tribe (aka APT36).

Chinese hackers breach US critical infrastructure in stealthy attacks

Microsoft says a Chinese cyberespionage group it tracks as Volt Typhoon has been targeting critical infrastructure organizations across the United States, including Guam, an island hosting multiple military bases, since at least mid-2021.

Their targets and breached entities span a wide range of critical sectors, including government, maritime, communications, manufacturing, information technology, utilities, transportation, construction, and education.

"Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications

infrastructure between the United States and Asia region during future crises.

The initial attack vector is the compromise of Internet-exposed Fortinet FortiGuard devices by exploiting an unknown zero-day vulnerability.

After breaching the targets' networks, they launch what Microsoft describes as "living-off-the-land" attacks with hands-on-keyboard activity and living-off-the-land binaries (LOLBins) such as PowerShell, Certutil, Netsh, and the Windows Management Instrumentation Command-line (WMIC).

However, they were also seen using open-source tools like Fast Reverse Proxy (frp), the Mimikatz credential-stealing tool, and the Impacket networking framework, according to a joint advisory published today by the FBI, NSA, CISA, and Five Eyes partners cybersecurity agencies from Australia, New Zealand, the United Kingdom, and Canada.

To ensure that their malicious activity blends with legitimate network traffic to evade detection, Volt Typhoon employs compromised small office and home office (SOHO) network equipment from ASUS, Cisco, D-Link, Netgear, FatPipe, and Zyxel, such as routers, firewalls, and VPN appliances.

Leveraging the privileged access obtained after compromising the Fortinet devices allows the state hackers to dump credentials through the Local Security Authority Subsystem Service (LSASS).

The stolen credentials allow them to deploy Awen-based web shells for data exfiltration and persistence on the hacked systems.

As Mandiant Intelligence Chief Analyst John Hultquist told BleepingComputer, these intrusions into US critical infrastructure orgs are likely part of a concerted effort to provide China with access in the event of a future conflict between the two countries.

"There are a variety of reasons actors target critical infrastructure, but a persistent focus on these sectors may indicate preparation for disruptive or destructive cyberattack.

"States conduct long-term intrusions into critical infrastructure to prepare for possible conflict, because it may simply be too late to gain access when conflict arises. Similar contingency intrusions are regularly conducted by states.

"Over the last decade, Russia has targeted a variety of critical infrastructure sectors in operations that we do not believe were designed for immediate effect. China has done the same in the past, targeting the oil and gas sector. These operations are aggressive and potentially dangerous, but they don't necessarily indicate attacks are looming."

News / Feeds References

National

1. https://timesofindia.indiatimes.com/city/surat/over-1-crore-cash-seized-10l-in-2000-denomination/articleshow/100489110.cms
2. https://timesofindia.indiatimes.com/city/mangaluru/notebooks-will-create-awareness-on-cyber-safety-introduced-for-students/articleshow/100489161.cms?from=mdr
3. https://timesofindia.indiatimes.com/city/kolkata/kolkata-police-holds-first-fb-live-session-on-e-crime/articleshow/100488733.cms
4. https://www.abplive.com/states/rajasthan/bharatpur-police-handed-over-the-accused-of-cyber-fraud-to-the-haryana-police-ann-2415904
5. https://www.indiatoday.in/technology/news/story/man-loses-over-rs-5-crore-after-scammer-pretends-to-be-his-friend-using-ai-face-swapping-technology-2383289-2023-05-23
6. https://www.indiatoday.in/technology/news/story/gurugram-man-loses-over-70-lakh-after-falling-for-part-time-job-scam-here-is-what-exactly-happened-2383792-2023-05-24
7. https://www.hindustantimes.com/cities/pune-news/cybercrooks-conning-patients-and-kin-seeking-appointments-with-aditya-birla-memorial-hospital-doctors-in-latest-pune-scam-101684947335405.html
8. https://kalingatv.com/technology/new-malware-alert-nearly-90-lakh-android-devices-infected-with-guerilla-malware-tips-to-protect-your-device/
9. https://www.tribuneindia.com/news/chandigarh/4-held-for-duping-resident-of-2-8l-four-atm-cards-seized-511010
10. https://www.tribuneindia.com/news/delhi/three-dupe-woman-of-rs-7-8-lakh-on-pretext-of-crypto-investment-held-510980

International

1. https://www.msspalert.com/cybersecurity-news/cybercrime-fighter-researchers-develop-dark-web-trained-ai/
2. https://www.click2houston.com/news/local/2023/05/25/wifi-jacking-thieves-use-new-device-to-hack-into-cell-phones-on-public-wifi-accessing-others-personal-information/
3. https://securityaffairs.com/146593/malware/ahrat-malware-google-play.html
4. https://www.bleepingcomputer.com/news/security/chinese-hackers-breach-us-critical-infrastructure-in-stealthy-attacks/

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

Indian
Cyber
Crime
Coordination
Centre

Are you a victim of Online Financial Fraud

Immediately call Helpline Number 1930

and register your complaint at
www.cybercrime.gov.in