

INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet



NEWS FROM THE INDUSTRY CHINA'S EFFORTS TO IMPROVE IT'S HACKING CAPABILITIES

Xi Jinping's efforts to improve China's hacking capabilities. Since the early 2000s, China has been known for its hacking teams that have caused significant damage to private companies and governments around the world, including the United States and its allies. These hackers have stolen valuable information from government databases, weapon system designs, and corporate intellectual property. Some notable examples include the Office of Personnel Management breach, the Marriott and Equifax breaches, and many others. However, Chinese President Xi Jinping has plans to increase China's digital capabilities even further. Since coming to power in 2013, he has made cybersecurity a top priority for the government, focusing on cultivating talent and funding cybersecurity research through universities and security services. The Chinese state has also put a focus on cybersecurity education, providing students with hands-on experience and organizing hacking competitions. They have also been known to collect vulnerabilities for use in network operations against other

IN THIS NEWSLETTER

1. News from the Industry.....01
2. Consultations in the month.....12
3. IFF in the Media.....13

NEWS FROM THE INDUSTRY

countries defense. As such, the onus is on defenders to be prepared to defend against well-trained, well-resourced, and more professional cyber attackers.

As a result of strategic investments made in recent years, China's cyber capabilities have grown significantly. Their hacking teams, which have been honed over the past decade, are now well-equipped and highly skilled, presenting a potential risk for companies. It is crucial for the US and its allies to enhance their defence systems in order to protect government networks from potential compromise.

HACKER BOOTCAMPS IN CHINA

In the early 2000s, China faced challenges in identifying and recruiting talented hackers for government cyber operations. To address this issue, Chinese policymakers sought to standardize and promote cybersecurity education in the country. In 2014, President Xi Jinping formed the Cybersecurity and Informatization Leading Small Group, which aimed to evaluate and standardize the content of China's cybersecurity college degrees. By 2015, the Ministry of Education had implemented these standards nationwide, and universities adjusted their curriculums accordingly.

In 2016, President Xi elevated the Leading Small Group to the Cybersecurity and Informatization Committee of the CCP Central Committee, and also established the Cyberspace Administration of China (CAC) as a formal government agency that could represent the CIC's work to other governments and businesses. The CAC subsequently published a National Cybersecurity Strategy for China, which outlined nine "strategic tasks" for policymakers, including increasing cybersecurity awareness and improving talent cultivation. These efforts by the Chinese government to improve its cybersecurity education, talent cultivation, and its agencies such as CAC, indicate a serious commitment to enhance the country's cyber capabilities.

In an effort to improve its cybersecurity capabilities, the Chinese government has invested in various initiatives to standardize and promote cybersecurity education, and develop physical and educational training infrastructure. After the National Cybersecurity Strategy was published, two provincial projects caught the attention of central government officials, the National Cybersecurity Talent and Innovation Base in Wuhan and the Guiyang's Big Data Cyber Range. Both of these were adopted as national efforts by the central government and the Cyberspace Administration of China (CAC).



NEWS FROM THE INDUSTRY

In addition to physical infrastructure, the Chinese government also introduced a new education initiative in 2017, designating some schools as World-Class Cybersecurity Schools (WCCS), similar to the U.S.'s Centers for Academic Excellence in Cybersecurity. The programme aims to signal to other universities the qualities and content that should be replicated and also enables employers to quickly assess a graduate's competencies.

To attract students and fill these programmes, China has also been hosting thousands of capture-the-flag hacking competitions every year and by 2017, The Ministry of Public Security established a policy that Software vulnerability researchers could only travel abroad for foreign competitions with the express approval of the ministry. This way of encouraging domestic competitions provides a steady stream of vulnerabilities to be used in hacking operations, as software vulnerabilities are perceived as a "national resource" in China.

In addition to promoting and standardizing cybersecurity education, the Chinese government has also implemented policies and created programmes to attract and retain the country's best hackers. These include partnering with the China Information Technology Security Evaluation Center to launch the Information Security Ironman competition, which spans every province in China, and encouraging domestic competitions like the Tianfu Cup to capture the magic of international software security competitions.

To further improve the success of China's hacking teams, the government has also implemented policies requiring software vulnerability researchers to disclose vulnerabilities they find to the Ministry of Industry and Information Technology within 48 hours of discovery, as well as investments in technologies for automatic software vulnerability discovery.

A recent report authored by World-Class Cybersecurity Schools in partnership with the Chinese Academy of Sciences, the Ministry of Education and a cybersecurity firm, predicts that China's deficit of cybersecurity experts will fall to 370,000 by 2027 and the education system is producing more, better-prepared cybersecurity experts.



NEWS FROM THE INDUSTRY

The report also lays out a new approach called the "4+3 Method" of cyber confrontation skills and development, which aims to harmonize the preceding seven years of public policy in China.

As a result of these efforts, it's likely that China's hacking teams will be composed of masses of nameless civil servants, each specializing in a particular skill set and managed by a bureaucracy that has matured over the last decade. This may lead to fewer clusters of activities and incidents of cyberattacks clustered into APTs, Pandas, or elements of the perimeter

AIIMS HIT BY RANSOMWARE

The All India Institute of Medical Sciences (AIIMS), New Delhi server was hit by a ransomware attack, which disrupted the premier medical institutions' digital services and forced them to run manually. Due to the ransomware attack, services that ran on a manual mode at the premier medical institution included services such as OPD registrations, blood sample reports, the smart lab, billing, report generation, and the appointment system.

It appears that the ransomware attack on the server of AIIMS, New Delhi server disrupted various digital hospital services, such as the ability to generate barcodes for samples, access imaging and patient reports, and more.

The hospital and the National Informatics Centre (NIC) are working to restore these services and have sought support from the Indian Computer Emergency Response Team (CERT-In) and the NIC. They are also taking precautions to prevent future attacks. In the meantime, the hospital has been running in manual mode to continue providing necessary services to patients.



RUSSIAN HACKERS SUSPECTED IN UKRAINE RANSOMWARE ATTACKS

Researchers at ESET, a Slovak software company specializing in cybersecurity, have discovered that ransomware called RansomBoggs targets several Ukrainian organizations and is believed to be connected to the Russian military threat group Sandworm.

Researchers have linked the RansomBoggs attacks to the Sandworm Advanced Persistent Threat (APT) actors due to similarities with previous attacks carried out by the group. The POWERGAP Powershell script, which was used in the RansomBoggs attack, is identical to the script used in previous attacks by Sandworm, including the Industroyer2 attacks on the energy sector, in April 2022 and the delivery of the destructive CaddyWiper malware in attacks against Ukrainian organizations in March 2022.

How it works: RansomBoggs is a .NET malware that is distributed using a PowerShell script called POWERGAP. It encrypts files using AES-256 in CBC mode and adds a .chsch extension. It also leaves ransom notes written in the character of James P. Sullivan from Monsters Inc, asking for financial assistance and providing an email address for contact.

It seems that the Sandworm group has been linked to the new RansomBoggs malware, indicating that they are continuously improving their tactics to make their attacks more effective. The development of RansomBoggs and Prestige suggests that the group is financially motivated. Ukrainian organizations were advised to follow best practices and take appropriate security measures to protect themselves from such attacks.



LACK OF PROPER DOMAIN SECURITY LEAVES GLOBAL 2000 COMPANIES VULNERABLE TO THREATS

Corporation Service Company CSC's third annual Domain Security Report found that three out of four Forbes Global 2000 companies have not implemented enough domain security measures, leaving them vulnerable to security threats. These companies have only implemented half of the recommended domain security measures. In addition, 75% of homoglyph domains (which are fake domains that look similar to the targeted brand's domain) are registered to unrelated third parties, with the intent of using the trust placed in the targeted brand to launch phishing attacks or other forms of digital brand abuse or IP infringement.

This can lead to revenue loss, traffic diversion, and damage to the brand's reputation. Homoglyph domains are just one of the many tactics that phishers and malicious third parties can use to spoof domains. Below mentioned are some of the findings of the study.

- One hundred thirty-seven companies (6.8% of the Forbes Global 2000) have not implemented any of the recommended domain security measures, making them vulnerable to attacks such as domain and DNS hijacking, phishing, ransomware, and Business Email Compromise (BEC).

- 45% of companies using enterprise-class domain registrars have implemented registry lock, a cost-effective measure to protect against accidental or unauthorized domain modifications or deletions. Only 5% of companies using consumer-grade registrars have registry locks deployed, and only six organizations within the Global 2000 had the highest overall domain security score, which correlated with their use of enterprise-class registrars.

- DMARC adoption has increased by 12 percentage points in the past year due to increased awareness of phishing attacks. However, the adoption of other domain security measures such as registry lock, DNS redundancy, DNSSEC, and CAA records has seen limited increases.



NEWS FROM THE INDUSTRY

Many Forbes Global 2000 companies are not implementing necessary domain security measures, leaving them vulnerable to attacks. DMARC adoption has increased, but the adoption of other measures has seen limited increases. Many third parties registering homoglyph domains are hiding their identity and have MX records, which can be used for phishing or email interception. Companies need to prioritize securing legitimate domains and monitoring for malicious domains to protect against cyber risks and maintain a zero-trust model, or risk impacting their cyber security posture, data protection, intellectual property, supply chains, consumer safety, revenue, and reputation.

MASSIVE DATA BREACH EXPOSES NEARLY HALF A BILLION WHATSAPP USERS' PHONE NUMBERS ON HACKING FORUM

A hacker is selling a database containing phone numbers of nearly 500 million WhatsApp users on a hacking forum. The data is claimed to be from 2022 and includes users from across the world. WhatsApp has an estimated user base of over two billion people in 180 countries.

The source of the data and the method of collection has not yet been disclosed. Cybersecurity researchers have requested a sample of the data to verify its authenticity, and the seller provided a sample containing valid user numbers from India, the UK, and the US.

In the past, Meta has faced criticism for allowing third parties to scrape or collect user data and has experienced a data leak of 533 million user records. There are concerns that the phone numbers of 487 million WhatsApp users could be used for malicious purposes such as phishing, impersonation, or fraud. Cybersecurity researchers believe that Meta and other tech companies should prioritize protection of their users' data to prevent such risks.

We are updating verified , validated and up to date whatsapp numbers for all countries on daily bas these numbers in MS Excel in two formats

1. Name / Whatsapp Number - Country Wise

2. Only Verified Whatsapp Numbers - Country Wise (This is to cover all the mobile subscribers ex allocated for the telecom operators in each countries and then verify / validate those numbers with

Let us know which country Whatsapp Sample you want , we shall share the sample accordingly .

COUNTS AVAILABLE (Name / Whastapp Number)

Country (Counts)
Africa (3725302)
Albania (338340)
Australia (2987486)
Austria (1033558)
Bahrain (642631)
Bangladesh (2176360)
Belgium (2283925)
Brazil (2105926)
Bulgaria (292525)
Canada (2804782)
Chile (4445212)

Name	Phone	Country
Chavdaanil Chavdaanil	+918200856619	India
Krish Patel	+918200856618	India
Darbar Raj	+918200856614	India
Manoj Gadhiya	+918200856611	India
Swatantra Singh	+918200856577	India
Babar Sayyed	+918200856575	India
Patel Hitanshi	+918200856570	India
Rohit Solanki	+918200856540	India
Shashi Dantani	+918200856530	India
Padhiyar Janaksinh	+918200856505	India
Poonam Patel	+918200858100	India
Rockie Singh	+918200858241	India
Rohit Dabhi	+918200858531	India
Cacs Umang Ratani II	+918200858674	India
Radhe Bala	+918200858708	India
Ahirauro Ahirauro	+918200858722	India
Prem Vaghela	+918200859120	India
Fitpowergirl Chakote	+918200859445	India
Minaxi Jain	+918200859487	India
Kaushal Patel	+918200859484	India
Sajjad Sajjad Belim	+918200859448	India
AJ Gajan	+918200859420	India
Ankita Jain	+918200859407	India
Manisha Mishra	+918200859395	India
Surandar Sahu	+918200859390	India
Patel Meghal	+918200859381	India

DATA OF 5.4 MILLION TWITTER USERS LEAKED ONLINE

A security vulnerability in Twitter's API was exploited to steal over 5.4 million user records, including private phone numbers and email addresses. The data has been shared on a hacker forum and a separate, potentially larger, data dump has also been disclosed. The data includes both public and private information.

A threat actor exploited a Twitter API vulnerability to steal over 5.4 million user records, which were then sold on a hacking forum for USD 30,000. The data included both public information, such as Twitter IDs and names, and private information, such as phone numbers and email addresses.

The vulnerability, which was disclosed in the HackerOne bug bounty programme, allowed people to submit phone numbers and email addresses to the API to retrieve associated Twitter IDs, which were then used to scrape public information about the accounts.


In September and November 2022, the 5.4 million Twitter user records that had been stolen using an API vulnerability were shared for free on a hacking forum. The data included private email addresses, phone numbers, and public scraped information such as the user's Twitter ID, name, and follower count. The data was previously offered for sale in August 2022.

Twitter (Partial) Database - Leaked, Download!

by FazyMalone - Wednesday November 23, 2022 at 06:08 PM

November 23, 2022, 06:08 PM (This post was last modified: November 25, 2022, 12:57 AM by pompompin. Edit Reason: Moved to official)

Hello BreachForums Community,
Today I have uploaded the Twitter (Partial) Database for you to download, thanks for reading and enjoy!



In January 2022, a vulnerability in Twitter's platform allowed an attacker to build a database of the email addresses and phone numbers of millions of users of the social platform. In a disclosure notice later shared in August 2022, Twitter advised that the vulnerability was related to a bug introduced in June 2021 and that they are directly notifying impacted customers. The impacted data included either email address or phone number alongside other public information including the username, display name, bio, location and profile photo. The data included 6.7M unique email addresses across both active and suspended accounts, the latter appearing in a separate list of 1.4M addresses.

This only contains 5.4 Million users, and is missing the 1.4 Million suspended accounts mentioned in the description.

Compromised data: Usernames, Display names, Bios, Locations, Email addresses, Phone numbers

Contents


The download for this Thread is free. You just need to be logged in and it will download once you visit the link below.
<https://cdn.breached.vc/files/down.php?tid=44096>

Database Index <-> How To Get Credits

(AKA Post Malone)
Thank you @TheKreator for MVP! <3
Thank You @LeakBase for GOD! 🙏

~UWU~
Your request for the Transgender award was denied by [Breach Wiki](#)

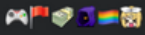
FazyMalone



Trapped In Darkness

GOD

Posts: 190
Threads: 41
Joined: Aug 2022
Reputation: 5%



FIFA WORLD CUP CYBER SCAMS, FAKE HAYYA CARDS FOR MATCHES

Football fans were targeted with APT campaigns, phishing, DDoS attacks, identity theft, and crypto fraud. A Hayya card is a mandatory, personal document required to attend the FIFA World Cup matches in Qatar.

These documents are important, so threat actors have begun to copy them and sell them to unwary targets. According to researchers, ninety Hayya accounts may have been affected. They discovered several Telegram channels that offered Hayya cards for sale for USD50 to USD150. The scammers also had access to the buyers' passports and other forms of identification. Additionally, only Bitcoins were accepted as payment.

The world cup has been sponsored by Crypto.com. Binance, another crypto currency agency has partnered with Cristiano Ronaldo for the promotion of football-related NFTs. This has facilitated the scammers to sell fake world cup themed crypto currency and tokens.

Further, phishing attacks against victims in the Middle East spiked 100% last month. Scammers have set up fake streaming sites and lottery schemes to harvest personal information and steal money from people looking to buy merchandise or tickets online. A sophisticated third-party ad fraud campaign was found using the official website of FC Barcelona to direct traffic to a possibly fraudulent iGaming website.

BAN ON CHINESE TELECOM IMPORTS IN USA

Due to national security concerns, the Federal Communications Commission (FCC) of the United States of America has forbidden itself from approving the import or sale of Chinese telecom and video surveillance products made by Huawei, ZTE, Hytera Communications, Hikvision and Dahua. It is a manifestation of The Secure Device Act, a statute signed by President Biden mandating that the FCC modernise its equipment authorization processes.

According to the new agreements, the FCC will be prohibited from reviewing white label items made by the five Chinese vendors mentioned above. Additionally, networking hardware and CCTV devices, sale of phones, cameras, Wi-Fi routers and other smart home accessories in the USA is not permitted. The use of Chinese CCTV products has been prohibited by the US government entities. Further, the FCC modified its authorisation guidelines to mandate that applicants have a US-based agent.

CYBERCRIMINALS RAMP UP PHISHING CAMPAIGNS AND FAKE WEBSITES DURING HOLIDAY SHOPPING SEASON

Cybercriminals were taking advantage of the holiday shopping season by launching phishing campaigns and fake websites to trick online shoppers. One tactic they used is impersonating popular brands and delivery companies to lure users into clicking on malicious links.

For example, researchers at Check Point Software Technologies, an American-Israeli multinational provider of software and combined hardware and software products for IT security, observed a phishing email campaign that pretended to be from luxury brand Louis Vuitton, with the subject line "Black Friday Sale" and a promise of discounted prices. The recipients were then directed to fake websites selling counterfeit items.

Another tactic observed was cybercriminals mimicking delivery companies, such as DHL and sending emails with a malicious URL designed to steal victims' credentials by claiming that they need to pay a fee to complete the delivery. Within the first 10 days of November, 17% of all malicious emails tracked were related to fake orders/deliveries and shipping.

Some security researchers uncovered a large phishing campaign that targeted users in North America during the holiday shopping season. The campaign used a sophisticated phishing kit that combined social engineering tactics and evasion detection techniques to trick users. The adversaries behind the campaign impersonated well-known brands, hosting companies, user profiles, and testimonials in order to lure victims.



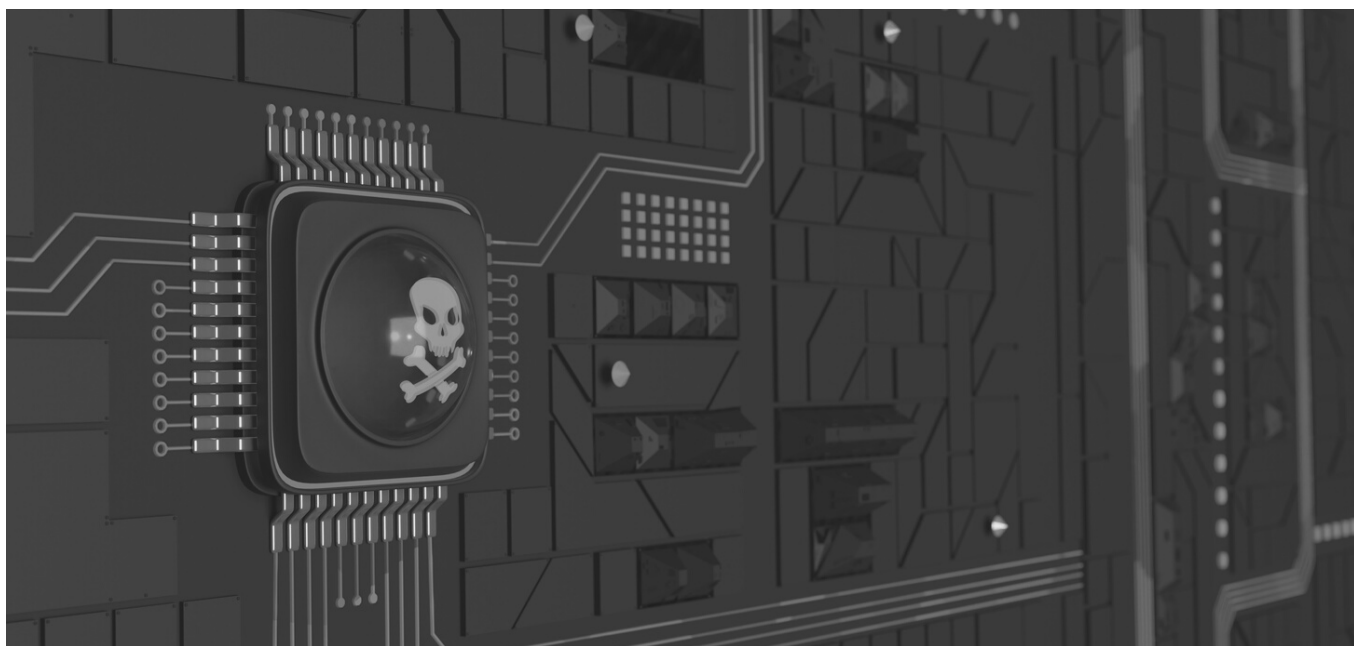
CITRIX SYSTEMS ISSUES SECURITY BULLETIN FOR CRITICAL VULNERABILITIES IMPACTING ADC AND GATEWAY PRODUCTS

Citrix Systems, Inc., an American multinational cloud computing and virtualization technology company, released a security bulletin detailing three vulnerabilities affecting their Application Delivery Controller (ADC) and Gateway products. The most severe vulnerability is an authentication bypass (CVE-2022-27510) which could allow an attacker to gain initial access to a network.

Another vulnerability (CVE-2022-27513) could allow for remote desktop takeover via phishing, if the appliances are operating through a VPN. The third vulnerability (CVE-2022-27516) is a failure in the brute force protection mechanism for user logins, which can be exploited when the appliances are operating through a VPN or with certain enabled settings.

Citrix ADC and Gateway products have been frequently targeted by threat actors in the past by exploiting a vulnerability called CVE-2019-19781. This vulnerability, which was first disclosed in December 2019, has been exploited by state-sponsored actors with links to China and Iran in ransomware attacks against various entities, including those in the healthcare sector. Recently, it has been included in an updated list of the top vulnerabilities exploited by Chinese state-sponsored actors.

Citrix Systems, Inc. has released fixes for several versions of its Application Delivery Controller (ADC) and Gateway products in response to the recently disclosed vulnerabilities. These fixes are intended to address the issues and help protect against potential exploitation by threat actors. It is important for users to update their systems and apply these patches as soon as possible to ensure the security of their network and sensitive data.



CONSULTATION IN THE MONTH

DEFTECH

India Future Foundation was the Knowledge Partner of the National DefTech Summit 22, an initiative by Tech Observer Magazine.

The summit was supported by The Southern India Chamber of Commerce and Industry, Startup Odisha, Qlik, ArubaitO, Felix Advisory Private Limited and Alliance Mantra.

The Summit was an initiative towards - Reimagining Digital Foundation for an Aatmanirbhar Defence Sector.

Our founder Kanishk Gaur shared his views on innovations and the need to strengthen infrastructure security.



Deliberations underway at the DefTech Summit 2022

IFF IN THE MEDIA

ETGov Explained: Why end-to-end encryption matters in India

In today's time, in spite of the increase in cyber-attacks around the globe, it is mandated that privacy should be an essential component to ensure human dignity, safety, and self-determination.

ETGovernment • November 06, 2022, 23:49 IST



By Kanishk Gaur

Social media intermediaries like WhatsApp, Signal, iMessage, and so on use End to



Kanishk Gaur, Founder, IFF, shares his views on Why end-to-end encryption matters in India, published in ETGovernment.com.

Gauging India's readiness in an era of cyber warfare

Two Indian think tanks came together to discuss India's readiness in the event of a Hybrid War at a seminar named Cyber Manthan.

Written by Express Defence

November 24, 2022 9:13:30 pm



Two Indian think tanks (IFF and USI of India) came together to discuss India's readiness in the event of a Hybrid War at Cyber Manthan.

ction Bill | 19 November, 2022



Amit Dubey, Co-Founder, IFF, speaks on "Digital Personal Data Protection" on Sansad TV

ctive: RBI's Digital Currency | 01 November, 2022



Amit Dubey, Co-Founder, IFF, shares his views on "RBI's Digital Currency" on Sansad TV



INDIA FUTURE
FOUNDATION

India Future Foundation

Phone: +91-1244045954, +91-9312580816

Email: helpline@indiafuturefoundation.com

Building no. 2731 EP, Sector 57, Golf Course Ext. Road, Gurugram,
Haryana, India - 122003

www.indiafuturefoundation.com

