INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

NEWS FROM THE INDUSTRY

GOOGLE CLOUD PLATFORM PARTNERS WITH FS-ISACS TO ENHANCE THREAT INTELLIGENCE CAPABILITIES

Google Cloud Platform has become the first major cloud provider to join the Financial Services Information Sharing and Analysis Center's (FS-ISAC) critical providers programme, which aims to reduce cyber-risk in the global financial system. The programme, launched in January 2022, focuses on enhancing supply chain security in the financial services sector by enabling non-financial entities that offer services and infrastructure to share threat intelligence and other information.

As part of this initiative, Google Cloud Platform will contribute valuable insights from its Threat Horizons reports and share the learnings of its Cybersecurity Action Team. According to a report by FS-ISAC and Akamai Technologies, Inc., a company that offers web and Internet security services, the financial services industry has seen a surge in cyberattacks, with Distributed Denial of Service (DDoS) attacks targeting financial services rising by 22%.

IN THIS NEWSLETTER

CISA SEEKS PUBLIC INPUT ON SECURING CLOUD BUSINESS APPLICATIONS WITH SCUBA GUIDANCE

The US Cybersecurity and Infrastructure Security Agency (CISA) is inviting public feedback on its Secure Cloud Business Applications (SCuBA) Hybrid Identity Solutions Architecture, which provides guidance for securely integrating cloud-based solutions with the already existing infrastructure on-premises. The SCuBA project consists of two documents that offer recommendations by Federal Agencies on adopting the best security and resilience practices when using cloud services. While primarily intended for Federal Agencies, the documents can be utilized by any organization. The first document (SCuBA) Technical Reference Architecture (TRA), aims to provide context, standard views and terminology that align with SCuBA. The second document outlines the extensible Visibility Reference Framework (eVRF), which assists organizations in identifying visibility data for threat mitigation and potential gaps in visibility products and services.

The public comment period for the Hybrid Identity Solutions Architecture guidance, which details identity management options and challenges associated with integrating on-premises and cloud-based solutions, will end on 17 April 2023. The SCuBA project seeks to establish consistent, effective, modern and manageable security for agency information assets stored in cloud operations, in line with Executive Order 14028.

FOUNDER OF BREACHFORUMS ARRESTED AND CHARGED

Conor Brian Fitzpatrick, the founder of BreachForums, a dark web forum has been arrested and charged, in Eastern District of Virginia, the United States of America, for operating a major hacking forum and marketplace for cybercriminals. Court documents state that Fitzpatrick allegedly ran BreachForums from March 2022, facilitating buying and selling of hacked or stolen data, including information about bank accounts, social security numbers and breached databases. The Federal Bureau of Investigation (FBI) and the Department of Health and Human Services Office of Inspector General (HHS-OIG) conducted a disruption operation that caused BreachForums to go offline. Fitzpatrick faces charges of conspiracy to commit access device fraud and if found guilty, could face a maximum sentence of five years in prison.

The forum facilitated criminal activities that impacted millions of citizens, as well as numerous companies, organizations and government agencies globally. The scope of the criminal activities was significant, with stolen personal information being sold for profit.

Following safety concerns, co-admin of BreachForums shut it down and plans to redirect all domains to baph.is. The decision was made after the co-admin discovered that an old server had been accessed, raising fears that law enforcement agencies may have gained access to their computer. To address these issues, the co-admin plans to create a new Telegram group for interested parties and continue discussions with other forum admins and service operators to establish a new community with improved security features.

SCARLETEEL HACKING CAMPAIGN TARGETS KUBERNETES ON AWS TO STEAL PROPRIETARY DATA

A new hacking campaign, dubbed SCARLETEEL, has been discovered targeting Kubernetes, an open-source container orchestration system, on Amazon Web Services (AWS). The hackers disguise their activities as a crypto jacking campaign while actually stealing proprietary data from their victims. The attackers exploit a vulnerable service in a self-managed Kubernetes cluster, downloading a decoy coin miner and extracting account credentials. With these stolen credentials, the hackers gain persistence and create backdoors, allowing them to spread further through the cloud environment. They also leverage stolen data and Terraform files to pivot to another AWS account, stealing even more data in the process.

To prevent lateral movement in the cloud and protect against attacks like SCARLETEEL, organizations are advised to conduct frequent audits to secure vulnerable applications. It is important to remain vigilant and take steps to ensure the security of cloud environments, as hackers continue to develop new and sophisticated techniques to target businesses and steal sensitive data.

CHALLENGES OF IMPLEMENTING ZERO TRUST IN ENTERPRISES

The CyberRisk Alliance (CRA), a USA based cybersecurity organization, conducted a survey on zero trust, and their findings revealed that many industry professionals understand the need for it and anticipate significant challenges ahead. Implementing zero trust solutions remains a challenge for many enterprises, even with those who have partially or fully implemented it, have been struggling to get buy-in from other departments. Despite its limitations, security professionals believe that zero trust is better suited for today's digital challenges, including the shift to cloud services and remote work environments. To manage the transition to zero trust, CRA offers four recommendations: survey all assets and resources, create zero-trust pilot programmes, look for applications with minimal friction and seek out expert organizations. While companies face difficulties finding employees with zero-trust skills, they must continue the journey to address the ever-evolving threat landscape.

SUN PHARMA REPORTS SECURITY BREACH

Sun Pharma, a Mumbai-based drug manufacturer, reported a security breach in their systems. The incident, which occurred on 2 March 2023 has resulted in theft of certain company and personal data. In response to the breach, Sun Pharma has taken steps to contain and remediate the situation, including isolating the impacted assets and initiating containment and eradication protocols to mitigate the threat. However, the company's business operations have been impacted, and revenues are expected to decline as a result.

Furthermore, Sun Pharma is currently unable to determine the full extent of the incident's potential adverse impact, including the possibility of additional security breaches or litigation. The company is committed to ensuring the integrity of its systems infrastructure and data and will continue to take measures to address the situation.

CYBERCRIMINALS EXPLOIT SILICON VALLEY BANK COLLAPSE WITH PHISHING AND SCAMS

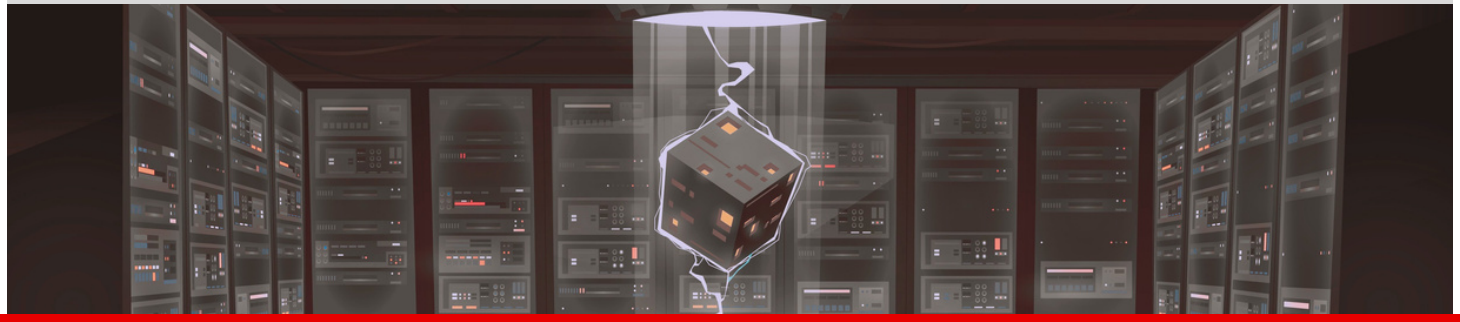
Recent reports suggest that cybercriminals are taking advantage of the crisis in the Silicon Valley Bank (SVB) to exploit potential victims through various means, including phishing scams, fake domains and BEC attacks. These criminals have already registered several suspicious domains and web pages to carry out their attacks, such as svbcollapse.com and svbclaim.com, among others. These domains are used to request personal information from individuals, such as their name, mobile number, email and balance amount (with the bank), to process claims.

In addition to the registration of suspicious domains, cybercriminals are also conducting various other scams, including cryptocurrency scams and BEC scams. Some customers have reported receiving new non-SVB account details from their existing vendors to facilitate payments, while others have been lured to websites where they can claim their crypto. Moreover, there have been reports of a significant KYC phishing campaign utilizing SVB branding in a DocuSign-themed template.

Experts warn that the SVB collapsing incident is a prime opportunity for fraudsters to target not only SVB's customers but also everyone involved in transactions with different entities. It is recommended that SVB clients stay vigilant and directly contact their vendors before changing any account information. Given the severity of the situation, it is likely that the more sophisticated scams may emerge in the future.

SOFT CELL LAUNCHES NEW ATTACKS AGAINST MIDDLE EASTERN TELECOM PROVIDERS

Between January to February 2023, a Chinese cyber espionage group associated with Operation Soft Cell launched new attacks against telecommunication providers in the Middle East. The hackers initially infiltrated the Internet-facing Microsoft Exchange servers to deploy web shells, then conducted reconnaissance, credential theft, lateral movement and data exfiltration activities. The Soft Cell group has been targeting telecommunications providers since at least 2012 and is known for using tools such as Mimikatz, which is used by hackers and security professionals to extract sensitive information, such as passwords and credentials, from a system's memory. The group also uses a backdoor named PingPull malware against companies in Southeast Asia, Europe, Africa, and the Middle East. In its latest campaign, the group used a custom variant of Mimikatz with new anti-detection features. However, the attacks were detected and blocked before any implants could be deployed.



ENGLAND BOOSTS CYBER SECURITY FOR HEALTHCARE

A new cyber security strategy for England has been published to protect the National Health Services (NHS) and to promote cyber resilience in the sector by 2030. The strategy aims to secure sensitive information and ensure patients can safely access care, particularly as the NHS continues to reduce waiting lists. As digital systems are increasingly adopted in the healthcare sector, it is vital to have the necessary tools to safeguard patients' information. The strategy includes five key pillars to minimise the risk of cyberattacks, improve response and recovery, and embed security into emerging technology. A full implementation plan with detailed activities and metrics will be published in summer 2023, with national cyber security teams working closely with local and regional healthcare organisations.

US AND INDIA TO COOPERATE ON EMERGING TECHNOLOGIES

Frank Kendall, the US Secretary for the Air Force, has announced that the US and India are working together on several emerging technologies, including intelligence surveillance reconnaissance (ISR), jet engine, artificial intelligence and space. During a press briefing, Kendall stated that the two countries are finalizing an air information-sharing agreement as part of growing defence cooperation. He also revealed that they are working towards signing certain clauses of the Basic Exchange and Cooperation Agreement (BECA) signed in 2020. The US official also expressed hope that a possible technology transfer of jet engines would be a step in the right direction. Furthermore, Kendall acknowledged that the US has been more open to technology sharing with India now than they had been in the past.

MOVIE RATING SCAM: WOMAN LOSES INR 76 LAKH IN GURUGRAM

A recent scam involved con artists promising people part-time employment in which they would get paid to watch and rate movies. A woman from Gurugram, Haryana fell for the scam and lost around INR 76 lakh. According to her complaint, she was contacted by a woman named Meera on Telegram who offered her a part-time job. Two days later, a different woman named Tejaswi contacted her and told her about a job that involved rating movies on the Bitmaxfilm.com app. The victim was asked to sign up and begin rating movies to earn extra cash. She was told to complete one set of 28 movies every day and was informed that she could withdraw her money once the set was completed, but she needed to recharge her account with Rs. 10,500+ to start rating. The con artist provided an account number for the victim to make payments and begin the job. The victim made multiple transfers but was later informed that she needed to complete more tickets and her balance on the website had gone into the red. She was asked to deposit more money to complete the final ticket. Eventually, the victim was asked to pay INR 21,23,765 to withdraw all her deposits, which she did but was unable withdraw her deposits. The total deposits made by her amounted to INR 76,84,493. The victim filed a complaint and an FIR was registered against unidentified fraudsters.

GURUGRAM POLICE ARRESTS GANG FOR MOBILE INVESTMENT SCAM

The Gurugram Cyber Police recently arrested four individuals for allegedly cheating more than 800 women by luring them to invest in a mobile application and work from home. The gang members were identified as Tushar Kohli, Vinod Kumar Bhasin, Ram Kumar Raman and Sahlesh Kumar, all residents of Delhi and Gurugram. One of the victims, filed a complaint against the gang for duping her of over INR 2 lakh through the app "BP PLC." Post which the police successfully busted the gang and arrested the four men.

GENESIS MARKET, A LARGE ONLINE MARKET FOR STOLEN DATA, BUSTED

European Union Agency for Law Enforcement Cooperation (Europol) recently announced that the international police had taken down one of the largest online markets for stolen identities and account details called “Genesis Market.” The operation, dubbed "Operation Cookie Monster," involved 17 countries, resulted in 119 arrests and was led by the FBI and the Dutch police. Genesis Market was a dangerous marketplace that sold stolen account credentials to hackers globally and had listed identities of over two million people for sale. The global sweep resulted in action against criminals in countries such as Australia, Britain, Canada, the United States, and in over ten European countries. The market offered "bots" for sale that had infected victims' devices through malware or other methods. Unlike other "dark web" services, Genesis was available on the open web, although it was obscured from law enforcement behind an invitation-only veil. The closure of Genesis Market follows several other cyber crackdowns involving Europol, including the shutting down of Raidforums, a massive online forum that sold access to hacked databases, and the disrupting of the world's most dangerous cybercrime malware tool called EMOTET.

WORLD CLOUD SECURITY DAY

World Cloud Security Day is observed annually on 22 March to raise awareness about the importance of cloud security. As the use of cloud computing becomes more widespread in both personal and professional spheres, it is crucial to understand the potential risks associated with it. Cloud security refers to the measures taken to protect data and applications that are hosted on cloud-based platforms. These measures include authentication and access control, data encryption, network security and disaster recovery plans.

As more companies and individuals store sensitive information on the cloud, the need for effective cloud security has become more critical than ever.
One of the most significant challenges of cloud security is the risk of data breaches. Hackers may attempt to gain access to sensitive information, such as personal or financial data, by exploiting vulnerabilities in cloud-based systems. In some cases, breaches occur due to lack of proper security measures or misconfigured systems, highlighting the importance of proper security protocols and regular security audits. Another challenge of cloud security is the risk of cyber-attacks that can cause significant damage to businesses and individuals. Cyber-attacks can take many forms, including malware, phishing and ransomware attacks. Such attacks can result in data loss, theft, or even complete shutdown of cloud-based systems, causing severe disruptions to business operations and financial loss.

To address these challenges, individuals and businesses need to take proactive steps to ensure cloud security. This includes implementing strong authentication and access controls, regularly updating security protocols and software and conducting regular security audits to identify potential vulnerabilities. Additionally, educating employees on best practices for cloud security is crucial. As the use of personal devices to access corporate data remotely becomes more common, employees need to be aware of the risks associated with using these devices and be trained on how to mitigate them.

World Cloud Security Day is an essential reminder of the need for strong cloud security measures. As we continue to rely more on cloud-based systems, it is vital to take proactive steps to protect sensitive data and prevent cyber-attacks. By implementing effective cloud security protocols and educating ourselves and our employees, we can ensure that our data remains secure in the cloud.

CYBER MANTHAN - SECURING INDIAN HEALTHCARE ECOSYSTEM FROM CYBER THREATS

India Future Foundation (IFF) in collaboration with Microsoft, organized a consultation under the brand name, Cyber Manthan - Securing Indian Health Ecosystem from Cyber Threats. The event was organized on 13 March 2023 at Marigold Hall, India Habitat Centre. The objectives of the event included dwelling on emerging trends, sophisticated nature of cyberattacks, existing vulnerabilities and solutions that can be provided to alleviate the risk of cyberattacks on the Indian healthcare sector. Through this consultation we aimed at highlight the need for establishing cyber security guidelines and regulations to safeguard the Indian healthcare ecosystem from cyberattacks.

Until the recent ransomware attack on All India Institute of Medical Sciences (AIIMS), New Delhi, the healthcare sector, in India, was not a part of the Critical Information Infrastructure (CII). The attack on AIIMS prompted the Government of India, to declare healthcare sector, to be a part of CIIs.

The discussions at the consultation were largely focussed on strategies that the sector needs to adopt to become cyber resilient. The discussions also shed light in the recommendations that can be implemented to enhance the security of the sector. Through this consultation, IFF aimed to highlight the need for not just securing but also training the healthcare professionals so that they are empowered to better protect the sector from cyberattacks. Further, the need for awareness about cybersecurity among healthcare institutions irrespective of their size was also highlighted.

The speakers at the event included Mr Rakesh Maheshwari, former Senior Director and Group Coordinator, Ministry of Electronics and Information Technology (MeitY); Maj. General (Retd) Dr Pawan Anand, Distinguished Fellow & Head USI-ANBI, The United Service Institution of India; Dr Debabrata Nayak, renowned Cyber Security Expert; Mr Tejdeep Singh Randhawa, Unit Head, Fortis Hospital, Greater Noida; Mr Salil Mittal, Lead Cyber Security - Emerging Technologies, Jio; Mr Kapil Madaan, Global Head, Information Security, Risk & Compliance (CISO & DPO), Max Healthcare; Mr Terrence Gomes, Country Head, Security, Microsoft India; Ms Smita Jain, Senior Cyber Security Technology Specialist, Microsoft; Ms Garima Rathore, Director, Government Affairs and Public Policy, Microsoft; Mr Kanishk Gaur, Founder, India Future Foundation, Mr Amit Dubey, Co-Founder, India Future Foundation.

CYBER MANTHAN - SECURING INDIA'S CRITICAL INFRASTRUCTURE FROM EMERGING DIGITAL THREATS

India Future Foundation (IFF) in collaboration with Microsoft, organized a consultation under the brand name, Cyber Manthan - Securing Indian Health Ecosystem from Cyber Threats on 31 March 2023 at The United Service Institution of India. The event focussed on security strategies for enhancing the cyber resilience of critical information infrastructures (CIIs), in India. With increasing digitization and integration, organisations present an expanding attack surface for cyber threats and thus face greater risks to both their Operational Technologies (OT) and Information technologies (IT) systems.

While the CIIs have standard operating procedures, guidelines, regulations and protocols, they still are within the radar of cybercriminals. In the recent past there have been a couple of instances of organisations, in the core sectors, that were at the receiving end of cyberattacks.

The consultation, provided a platform for industry leaders and stakeholders to discuss strategies and solutions that be implemented by organizations, to make themselves cyber resilient. The common concern that was raised by participants, in the consultation, was that organizations do not invest or take cybersecurity seriously which results in loss of data, reputation and loss of revenues. It even poses a threat to national security.

The speakers at the event included Lt Gen. Vinod G. Khandare, Principal Advisor, Ministry of Defence; Maj. Gen Manjeet Singh - Joint Secretary, National Security Council Secretariat; Maj. Gen. (Retd) Dr Pawan Anand, Distinguished Fellow & Head USI-ANBI, The United Service Institution of India; Col (Retd) Sanjeev Relia, Chief Strategy Officer, ThinkCyber India; Col (Retd) Suhail Zaidi, Head of Confederation of Indian Industry - Tata Communications, Centre for Digital Transformation; Dr Debabrata Nayak, Renowned Cybersecurity Expert; Dr Subi Chaturvedi, Chief Corporate Affairs & Public Policy Officer, InMobi; Dr Shruti Mantri, Associate Director, Indian School of Business; Dr Munish Sharma, Senior Advisor (Cyber and Technology), Australian High Commission, New Delhi; Mr Sandeep Aurora, Director - Government Affairs & Public Policy, Microsoft; Ms Smita Jain, Senior Cyber Security Technology Specialist, Microsoft; Mr Kanishk Gaur, Founder, India Future Foundation; Mr Amit Dubey, Co-Founder, India Future Foundation.

IFF IN THE MEDIA

Kanishk Gaur, Founder, IFF, expressed his views about OpenAI's ChatGPT on INDIA TODAY.

Kanishk Gaur, Founder, IFF, shared his views on OpenAI's ChatGPT and its usage for malicious activities on News18.

Kanishk Gaur, Founder, IFF spoke on why countries are following India's decision to ban Tik Tok on Mirror Now.

Kanishk Gaur, Founder, IFF writes about safeguarding businesses from emerging threat vectors in CIO&Leader.

INDIA FUTURE
FOUNDATION

Contact Us

+91-1244045954, +91-9312580816

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

helpline@indiafuturefoundation.com

www.indiafuturefoundation.com