INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

NEWS FROM AROUND THE WORLD

RANSOMWARE HITS MANUFACTURING COMPANIES

In international trade, the manufacturing sector is a stalwart, the backbone upon which economies are built and progress is achieved. However, in recent years, this backbone of the global economy has been at the receiving end of ransomware attacks. A comprehensive analysis conducted by Comparitech, a UK based software firm, on manufacturing companies between 2018 and July 2023, threw open some interesting trends.

The Alarming Statistics

478 Confirmed Attacks
Over the period under study, a staggering 478 manufacturing companies were entangled in the web of ransomware attacks, revealing the pervasive nature of this digital menace.

$46.2 Billion in Downtime Loss
The financial repercussions of these attacks are nothing short of monumental, with downtime alone accounting for losses amounting to $46.2 billion. This financial haemorrhage sends shockwaves through the industry and has far-reaching economic implications.

IN THIS NEWSLETTER

Ransomware attacks do not merely strike at the periphery; they pierce the very heart of manufacturing. Production lines are severely disrupted and the ensuing ripple effect leaves customer orders unfulfilled and day-to-day operations in paralysis.

The key Findings of the analysis are as follows:

7.5 Million Records Breached

The insidious impact of these attacks extends beyond financial losses. Over 7.5 million individual records were breached, foreshadowing the potential for data theft at a grand scale.

Demands for Ransom Vary Widely

The spectrum of ransom demand ranged from $5,000 to a staggering $50 million, with an average demand hovering at around $11.2 million. During the study it was found that hackers have demanded an astounding $5.5 billion in ransom payments.

Few Companies Paid Ransom

While only four companies are known to have acquiesced to ransom demands made by hackers, it is imperative to note that many organizations refrained from disclosing such incidents to mitigate further vulnerabilities. The confirmed payments stand at a modest $750,000, spanning two attacks.

Varied Downtime

The duration of downtime resulting from these attacks is equally diverse, fluctuating from several hours to an astonishing 76 days of operational standstill.

Targeted Sectors

The transportation and automotive sectors bore the brunt of these attacks, enduring a staggering 92 incidents, closely followed by electronics and appliances manufacturers with close to 80 episodes.

Dominant Ransomware Strains

Egregor and Conti held sway as the primary ransomware strains in 2020 and 2021, while LockBit emerged as the dominant threat in 2022 and 2023 (till the time of writing this newsletter).

These sobering statistics underscore the inherent vulnerability of the manufacturing sector to ransomware attacks. The imperative for enhanced security measures could not be more pressing. Manufacturers must prioritize cybersecurity to safeguard their operations, maintain customer trust, and fortify financial stability.

In the face of this ongoing assault, resilience and vigilance are paramount. As we strive for a future of innovation and progress, it is incumbent upon us all to fortify the defences of this crucial economic pillar.

ANDROID BANKING TROJAN TARGETS SOUTHEAST ASIA

A previously undetected Android banking trojan, MMRat, has recently emerged as a threat to mobile users in Southeast Asia. In circulation since late June 2023, this malicious software has been designed to take control of mobile devices and execute financial fraud remotely.
The distinctive features of MMRat are as follows:

1. Customized Command-and-Control Protocol: MMRat sets itself apart by employing a customized command-and-control (C2) protocol based on protocol buffers (protobuf). This sophisticated approach allows for efficient data transfer from compromised devices, highlighting the increasing sophistication of Android malware.

2. Phishing Sites as Entry Points: The attacks initiate from a network of phishing sites that impersonate official app stores. While the exact method used to direct victims to these sites remains unknown, MMRat typically disguises itself as either an official government app or a dating app.

3. Abuse of Android Accessibility Service: MMRat heavily relies on Android's accessibility service and MediaProjection API, which other Android financial trojans like SpyNote have exploited. These components enable MMRat to perform various activities, including granting additional permissions and modifying settings.

MMRat exhibits several capabilities, including data collection, remote control and persistence between device reboots. It communicates with a remote server to give instructions and transfer the results of executed commands. This trojan targets users in Southeast Asia, focusing on Indonesia, Vietnam, Singapore and the Philippines, based on the language used in phishing pages.

MMRat can gather device data and personal information, such as signal strength, screen status, battery statistics, installed applications and contact lists. This information may be used to profile victims for further exploitation.

Moreover, MMRat can record real-time screen content and capture lock screen patterns, allowing threat actors to remotely access locked devices when not in use.

To protect against malwares like MMRat, users are advised to do the following:

1. Download apps only from official sources.
2. Scrutinize app reviews and ratings.
3. Review the permissions requested by apps before granting access.

NORTH KOREAN HACKERS TARGET PYPI REPOSITORY

In a concerning development, it has come to our attention that a series of sneaky Python packages hiding malware has surfaced in the Python Package Index (PyPI) repository. These packages are part of a tricky scheme called VMConnect and have been used to spread harmful software.

Three rogue Python packages have been discovered as part of the VMConnect campaign: tablediter, request-plus and requestspro. These packages pretend to be legitimate open-source Python tools by using tricks like typosquatting. They make themselves look like popular packages such as prettytable and requests to deceive developers.

The functionalities of the Malware are as follows:

Tablediter: This package constantly checks in with a remote server, asking for and running a hidden code. We don't know exactly what this code does, but it's designed to sneakily wait before doing anything harmful to avoid getting caught by security software.

request-plus and requestspro: These packages are made to secretly gather information from infected computers and send it to a command-and-control server. In return, the server sends back a unique code, which the infected computer sends back. This exchange most likely leads to downloading a more lousy code.

How this campaign uses a unique code system reminds us of what North Korean hackers did in a different campaign earlier this year. Interestingly, there are similarities in the infrastructure used in this Python package scheme and a cyberattack on JumpCloud, in June 2023. These connections make it more likely that North Korean hackers are involved, in this misadventure.

The PyPI repository keeps getting used by cyber attackers to spread malware. So, it's crucial to be cautious when you're downloading Python packages, especially from sources that aren't official. Always double-check where your software comes from, so that you are able to keep your computer and data safe.

SAPPHIRE STEALER MALWARE EXPLOITED

An open-source .NET-based information stealer malware known as SapphireStealer has become a tool for various threat actors looking to enhance their cyber capabilities. This malware, which focuses on stealing sensitive information, has created an ecosystem where different entities create customized variants to execute a range of cyberattacks.

The Cybercrime-as-a-Service (CaaS) Model
SapphireStealer is a prime example of information-stealing malware proliferating on the dark web. These malware variants are designed to collect a host information, like browser data, files and screenshots and can exfiltrate the stolen data in ZIP format via SMTP (Simple Mail Transfer Protocol). The evolving CaaS model allows financially motivated and nation-state actors to access these services to monetize the stolen data and conduct various malicious activities, including ransomware attacks and indulge in data theft.

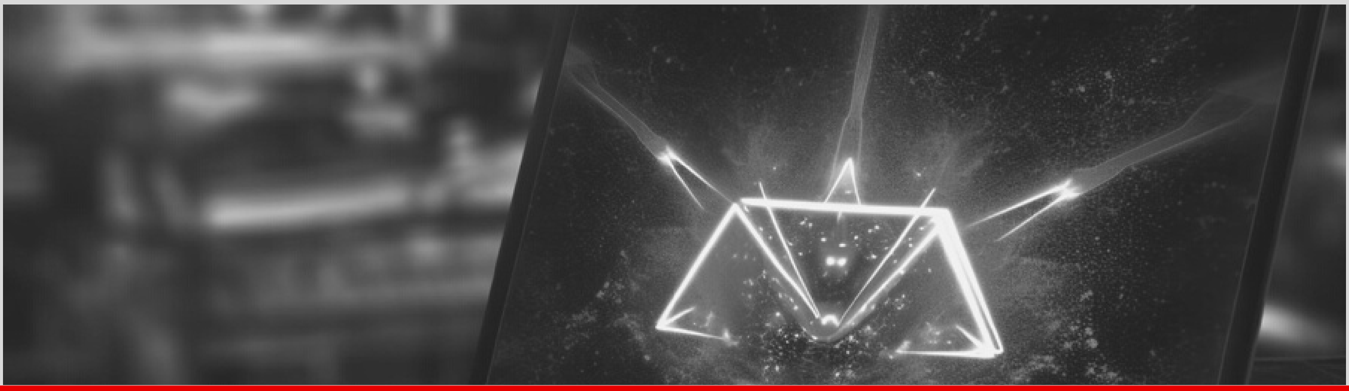
SapphireStealer's source code was released for free in December 2022, enabling cybercriminals to experiment with the malware and make it difficult to detect.

Customization
Threat actors have added flexible data exfiltration methods, including Discord webhooks and the Telegram API.

Ongoing Development
Multiple variants of SapphireStealer are already active, with threat actors continuously improving their efficiency and effectiveness.

The author of SapphireStealer also shared a .NET malware downloader known as FUD-Loader. This downloader enables the retrieval of additional binary payloads from attacker-controlled distribution servers. Cisco Talos detected this malware downloader being used to deliver remote administration tools like DCRat, njRAT, DarkComet and Agent Tesla.

The emergence of SapphireStealer and similar malware underscores the evolving threat landscape, where cybercriminals leverage open-source tools and customize them to suit their objectives. Organizations must remain vigilant and adopt robust cybersecurity measures to defend against these evolving threats.



WINDOWS CONTAINER VULNERABILITY DISCOVERED

Recent findings reveal a vulnerability in the Windows Container Isolation Framework that malicious actors can exploit to bypass endpoint security solutions. By manipulating the framework's features, attackers can evade detection and execute file system operations without alerting security software.

Microsoft's container architecture employs dynamically generated images to separate the file system of containers from the host while minimizing the duplication of system files. This results in "ghost files" that point to a different volume on the system.

The vulnerability involves leveraging the Windows Container Isolation FS (wcifs.sys) minifilter driver, which is responsible for the file system separation between Windows containers and the host. This driver handles the redirection of ghost files by parsing reparse points and reparse tags. Specifically, two reparse tag data structures are used: IO_REPARSE_TAG_WCI_1 and IO_REPARSE_TAG_WCI_LINK_1.

The attack methodology of the bad actors is as follows:

- The attacker runs a process inside a fabricated container.
- The minifilter driver is used to manipulate I/O requests, allowing for the creation, reading, writing and deletion of files on the file system without triggering security software.
- The minifilter driver operates at a lower altitude range than antivirus filters, preventing callbacks from being triggered.
- Successful execution of this attack requires administrative permissions.
- The attack cannot override files on the host system.

This vulnerability allows attackers to obfuscate file system operations, confusing security products and evading detection. It highlights the need for vigilance and robust cybersecurity measures to defend against evolving threats.

CHATGPT AND PLUGINS IN ONLINE BUSINESS

The proliferation of large language models (LLMs) like ChatGPT has introduced new challenges for online businesses. These AI models, while powerful, pose risks to enterprises, including content theft, reduced web traffic and potential data breaches.

The Risks Presented by LLMs and Plugins:

Content Theft
LLMs can scrape and republish data without permission, undermining the original content's authority and SEO rankings.
Reduced Traffic
Website traffic can decline as users turn to ChatGPT and plugins for answers.
Data Breaches
LLMs may inadvertently share sensitive data, harming brand reputation and competitiveness.
Industries with data privacy concerns, unique content and ad-driven revenue are most at risk. These include e-commerce, streaming and media, publishing and classified ads.

ChatGPT gets its knowledge from Common Crawl, WebText, Books and Wikipedia. Common Crawl uses a web-crawling robot called CCBot.

If you want to stop CCBot or similar robots from accessing your website, use tools like robots.txt or user agent blocking. However, relying solely on user agent blocking might cause unexpected issues.
When ChatGPT uses plugins, it can access extra information, which can be helpful but might also affect how ads work on your website and how much people interact with it.

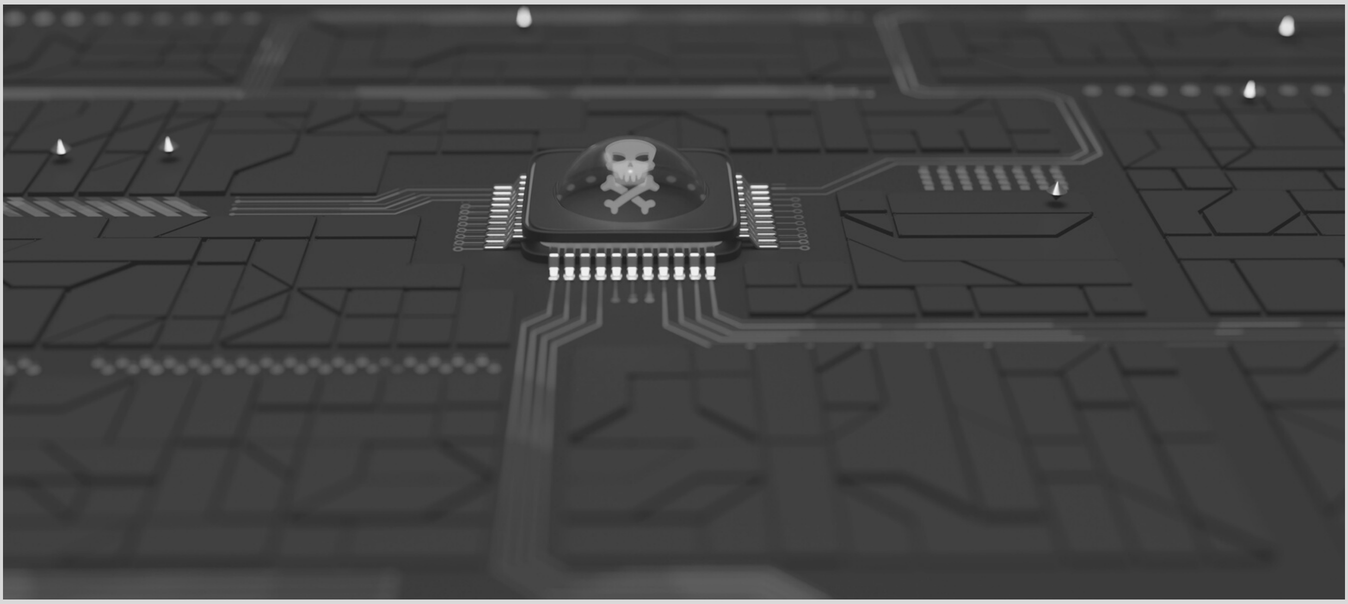
Sometimes, these plugins request your site and announce themselves with a unique code called a user-agent header. However, they can use different codes, too, so you'll need intelligent methods to tell them apart.

Let's talk about blocking requests from plugins that say they're "ChatGPT-User." While this can work, it might accidentally block regular users. To find plugins that don't declare themselves like that, we'll need advanced tools to spot them.

For websites with essential data, one should think about how to make money from it or give users a choice of not sharing their data with AI models like ChatGPT. To protect the website, one can use advanced AI and machine learning tools to detect and deal with these bots.

In the ever-changing digital world, being flexible and making informed choices it is crucial to keep your website safe and working.

CITRIX NETSCALER RANSOMWARE ATTACK



Unpatched Citrix NetScaler systems are attacked by unidentified threat actors suspected of being involved in a ransomware campaign exploiting a critical code injection vulnerability.

Their systems face a potential ransomware threat as unknown attackers exploit a critical code injection vulnerability. Cybersecurity firm Sophos has identified this activity as part of a cluster referred to as STAC4663. The attack chain exploits CVE-2023-3519, a critical vulnerability that can lead to unauthenticated remote code execution on NetScaler ADC and Gateway servers.

The attack, detected in mid-August 2023, involved the exploitation of CVE-2023-3519 to conduct a domain-wide attack.

The attackers injected payloads into legitimate executables such as Windows Update Agent (wuauclt.exe) and Windows Management Instrumentation Provider Service (wmiprvse.exe).

The attackers used obfuscated PowerShell scripts, PHP web shells and a service called BlueVPS for malware staging.

The attack resembles a campaign disclosed earlier in which nearly 2,000 Citrix NetScaler systems were breached.

Recommendations:

Citrix NetScaler ADC and Gateway appliance users are strongly advised to apply patches to mitigate potential threats.

WINRAR VULNERABILITY REQUIRES URGENT UPDATE

A high-severity security vulnerability has recently come to light in WinRAR, posing potential risks for Windows system users. This vulnerability falls into the category of improper validation while handling recovery volumes, potentially granting threat actors the ability to execute code remotely on Windows systems.

The root of this issue lies in the insufficient validation of data provided by users, which results in memory access extending beyond an allocated buffer. In simpler terms, it's a gap in how WinRAR checks the information it receives.

An attacker could exploit this vulnerability to run their code within the current process, but here's the catch: it requires some action from the user's side, like visiting a malicious website or opening a dodgy archive file.

This vulnerability was first detected and reported on 8 June 2023, by a security researcher using the alias "goodbyeselene." Fortunately, it hasn't gone unnoticed, and WinRAR has released a solution in version 6.23, made available on 2 August 2023.

Additionally, this latest WinRAR version addresses another issue identified as "WinRAR could start a wrong file after a user double-clicked an item in a specially crafted archive." Credit for reporting this problem goes to a researcher from Group-IB, a global leader in the fight against cybercrime, Andrey Polovinkin.

In light of these developments, it's strongly recommended that users promptly update their WinRAR to the most recent version. Doing so will help mitigate any potential risks associated with this security vulnerability, ensuring a safer digital environment.

MICROSOFT 365 PHISHING TARGETS EXECUTIVES

In a recent phishing campaign that successfully breached the accounts of senior business executives using Microsoft 365, cyber attackers have demonstrated an alarming level of sophistication. They employed a cunning phishing toolkit called EvilProxy, which uses reverse-proxy tactics to bypass multifactor authentication (MFA), which is a robust security measure. This campaign underscores the evolving abilities of cybercriminals to outmanoeuvre security measures, with a primary focus on high-value targets.

The attackers impersonated trusted services and applications, including Concur, DocuSign and Adobe Sign, to lure victims with seemingly legitimate content. Phishing emails, resembling official expense reports or documents requiring signatures, served as the initial bait. Victims clicking on embedded URLs were led through a series of redirects, cunningly concealed within legitimate websites, obscuring the trustworthy source of the impending attack.

This scheme culminated with victims landing on a phishing page painstakingly designed to mimic a Microsoft 365 login portal; all orchestrated through the deceptive capabilities of EvilProxy. What makes this toolkit particularly troubling is its claim of being able to bypass MFA on popular websites, that includes names like Apple, Gmail, Facebook, Microsoft, Twitter, GitHub, and GoDaddy.

Once high-value targets were compromised, attackers swiftly gain access to their accounts, facilitated by the Microsoft 365 application "My Sign-Ins," which granted them persistent control over organizational management, devices and authentication sessions. As an additional layer of stealth, attackers inserted their authentication app with time-based one-time passwords (TOTP codes) into the victim's account, ensuring continued access even if the victim changed his/her password.

Beyond mere account compromise, these attackers engaged in various activities, ranging from financial fraud to data theft, and even offered hacking-as-a-service transactions.

To bolster defences against such insidious threats, organizations are advised to implement MFA methods impervious to proxy interception. This includes physical USB keys following the FIDO2 standard or certificate-based authentication. Additionally, employing conditional access policies to scrutinize sign-in requests based on device identity and location and continuous access evaluation to detect anomalies in legitimate authentication token usage can enhance security measures.

INDIA'S DIGITAL TRANSFORMATION CHALLENGES

India has set its sights on having a $1 trillion digital economy by 2025. Recognizing the imperative of adaptable policies, platforms and partnerships in the borderless digital landscape, the nation is fervently pursuing this ambitious goal. A central pillar of this mission is to empower individuals with control over their data, striking a delicate balance between embracing cutting-edge technologies and safeguarding data rights.

In a significant development, On 9 August 2023, the Rajya Sabha gave its nod to the Digital Personal Data Protection Bill 2023 (DPDP Bill) with a resounding voice vote. This significant legislation, previously greenlit by the Lok Sabha, is designed to shield individual’s data from misuse by online platforms. It aligns with the principles established by the Supreme Court, which declared the "Right to Privacy" as a fundamental right, six years ago. The DPDP Bill places the privacy of Indian citizens at the forefront, prescribing penalties of up to Rs 250 crore for entities failing to preserve their digital data.

Key highlights of the DPDP Bill include provisions for robust data protection, obligating companies to ensure data safety even when entrusted to third-party data processors. It also mandates prompt reporting of data breaches to the Data Protection Board (DPB) and affected users. Special provisions are in place for children's data and data of physically disabled individuals, requiring consent from guardians for processing.

Companies are further mandated to appoint a Data Protection Officer and furnish relevant details to users. The DPB, on the other hand, assumes responsibility for handling data breach complaints and recommending actions in the public interest. This legislative stride marks a pivotal advancement in reinforcing India's cybersecurity framework, championing citizens' digital data privacy and security, and fostering an environment that is conducive to innovation and economic growth while providing clarity for businesses and individuals alike.

The DPDP Bill also underscores the significance of data localization, ensuring that the data remains within the country's borders. This safeguards privacy and fuels job creation within the cybersecurity sector. Furthermore, the Digital Personal Data Protection Bill 2023 is anticipated to encompass robust cybersecurity measures to guard against data breaches and unauthorized access. This, in turn, will ensure comprehensive protection for personal data throughout its lifecycle.

While the DPDP Bill 2023 signifies a monumental milestone, clear guidelines and standards must be established to aid organizations in comprehending their data protection and cybersecurity responsibilities. Continuous stakeholder engagement and consultations will be pivotal in refining the Bill and ensuring its seamless execution.

TIGHTER KYC RULES TO COMBAT CYBER FRAUDS IN INDIA

The Government of India has taken decisive steps to bolster KYC (know-your-customer) norms for mobile phone connections and crack down on fraudulent activities, particularly those involving fake links. These measures are a pivotal component of the government's broader strategy to combat cybercrimes and financial fraud, with mobile phones being a primary avenue for such illicit activities. Under the new KYC reforms, mobile phone users must submit their documents when requesting SIM replacements or making other alterations to their connections. Furthermore, dealers selling SIM cards or links are subject to verification by telecom companies, aiming to enhance accountability among dealers and streamline the verification process.

Three novel protocols have been introduced for user identity verification, encompassing Aadhaar QR code scanning, document submission for SIM card replacement and facial-ID-based authentication. Notably, phone numbers that have been disconnected will not be recycled for at least 90 days. These stringent rules will come into effect on 1 October 2023.

Telecom companies have a 12-month window to register franchisees, agents and distributors. Violators, particularly unscrupulous dealers, face severe consequences, including a three-year ban and penalties of up to ₹10 lakh. Additionally, the Department of Telecommunications (DoT) is set to introduce the concept of a business connection, making KYC mandatory for businesses and individuals receiving SIM handovers.

The KYC mechanism has faced challenges in ensuring all connections belong to verified customers. Cyber frauds frequently involves attackers using phone calls or SMS messages to deceive individuals into sending money or falling victim to hacking attempts, often orchestrated by interstate gangs, a classification not yet recognized as a separate crime by the government.

Recent statistics highlight the problem's magnitude, with 6.6 million out of 1.14 billion analyzed connections flagged as suspected. Over 5.2 million were disconnected due to verification failures, over 67,000 dealers were blacklisted and over 17,000 mobile handsets were blocked. Furthermore, over 300 FIRs were registered against dealers, and approximately 800,000 bank/wallet accounts used by fraudsters have been frozen.

These KYC reforms signify a concerted effort to combat cybercrimes, ensuring the authenticity of mobile phone connections and reducing the scope for fraudulent activities in the digital realm.

HACKERS TARGET 1,000+ INDIAN WEBSITES

In a meticulously orchestrated campaign to coincide with Independence Day, hackers launched a concerted attack on over 1,000 Indian websites operating under the banner of OpIndia. This hacktivist initiative drew participation from collectives from various countries and harnessed a spectrum of techniques, including Distributed Denial of Service (DDoS) attacks, website defacement and account takeovers. Political and religious motivations drove the campaign, singling out websites with lax security measures and vulnerable digital infrastructure. These targeted sites spanned diverse sectors, encompassing government entities, educational institutions, the banking and financial services industry (BFSI) sector and small-scale enterprises.

Under the OpIndia hacktivist campaign, Independence Day in India was marked by a cyberattack surge. The involvement of hacktivist collectives from different nations underscored the global reach and coordination of such operations, with their arsenal including disruptive DDoS attacks, website defacement and account compromises.

The impact of these actions was felt most profoundly in the government and BFSI sectors, where DDoS attacks caused significant disruptions. In contrast, the education sector and small businesses encountered website defacement and unauthorized access panel takeovers.

Cybersecurity researchers have sounded an alarm regarding the potential threat these hacktivist group's pose. The concerning factors include increased collaboration among such entities, their ready access to sophisticated attack tools and data and the possibility of support from state-sponsored hackers. This convergence of capabilities and motives raises the spectre of hacktivist groups evolving into a more formidable and sustained threat in the cybersecurity landscape.

In light of these developments, Abhinav Pandey, a cyber threat researcher at CloudSEK, underscored the need for vigilance and robust cybersecurity measures. He emphasized that the impact of hacktivist groups could be amplified by their collaborative nature, ease of access to potent attack tools, and potential backing from state-sponsored actors. This campaign targeting Indian websites on Independence Day is a stark reminder of the evolving threat landscape in cyberspace and the imperative for organizations and governments to fortify their cybersecurity defences.

SEBI'S NEW CYBERSECURITY GUIDELINES

The Securities and Exchange Board of India (SEBI), India's market regulator, has taken proactive steps to bolster cybersecurity and enhance the cyber resilience framework for Market Infrastructure Institutions (MIIs), encompassing entities like stock exchanges, clearing corporations and depositories. These newly unveiled guidelines respond to the evolving cybersecurity landscape within the Indian securities markets and underscores the increasing interdependence among MIIs, necessitating comprehensive security measures that go beyond their owned or controlled systems.

Formulated based on recommendations from the High Powered Steering Committee on Cyber Security of SEBI and developed in close consultation with MIIs, these guidelines introduce several vital provisions to fortify the cybersecurity posture of these critical institutions:

Offline Encrypted Backups: MIIs are mandated to maintain offline, encrypted data backups and conduct regular testing of these backups, with a minimum frequency of once every quarter. This ensures the confidentiality, integrity, and availability of data.

Spare Hardware: MIIs are encouraged to explore the retention of spare hardware in isolated environments. This strategy facilitates system rebuilding during operational disruptions, bolstering business continuity efforts.

Business Continuity Drills: MIIs must periodically conduct business continuity drills to assess their organizational readiness and the effectiveness of their security controls. These drills are particularly crucial in evaluating preparedness against ransomware attacks.

Vulnerability Scanning: Regular vulnerability scanning is mandated to identify and address vulnerabilities on internet-facing devices. This practice reduces the attack surface and strengthens overall security.

Cybersecurity User Awareness: MIIs must implement a cybersecurity user awareness and training programme. This programme should guide recognizing and reporting suspicious activities, enhancing the cybersecurity vigilance of staff.

Multi-Factor Authentication (MFA): MFA is made mandatory for all services provided by MIIs, adding a layer of security.

The significance of these guidelines lies in acknowledging the systemic importance of MIIs in ensuring the seamless functioning of the securities market. By bolstering cybersecurity and cyber resilience measures, SEBI aims to fortify the overall security posture of these critical institutions and safeguard the integrity of India's financial markets.

The introduction of these guidelines by SEBI reflects the growing emphasis on cybersecurity within the financial sector. It underscores the imperative need for robust measures to protect critical infrastructure, aligning with global efforts to combat cyber threats in finance.

Q2 2023 CYBERSECURITY GUIDELINES

The second quarter of 2023 witnessed a dynamic landscape in the realm of cybersecurity, that was marked by several noteworthy developments. This period brought forth the emergence of new Advanced Persistent Threat (APT) actors, toolkit adaptations, fresh malware variants and the ongoing evolution of cybercriminal techniques.

One standout development was the identification of a previously unknown threat actor group within the 'Elephants' family, aptly named "Mysterious Elephant." Operating predominantly in the Asia-Pacific region, this group distinguished itself by employing novel backdoor families capable of executing files and commands from malicious servers on compromised systems.

The Lazarus cybercrime group, known for its activities, elevated its MATA framework, a sophisticated multi-platform targeted malware framework, signalling its dedication to enhancing its attack capabilities. Within the Lazarus Group, the financial-focused subgroup BlueNoroff showcased remarkable evolution, adopting new delivery methods and programming languages, including Trojanized PDF readers, macOS malware and the Rust programming language.

ScarCruft, another prominent APT group, introduced novel infection methods that challenged cybersecurity professionals, particularly through their evasion of Mark-of-the-Web (MOTW) security mechanisms.

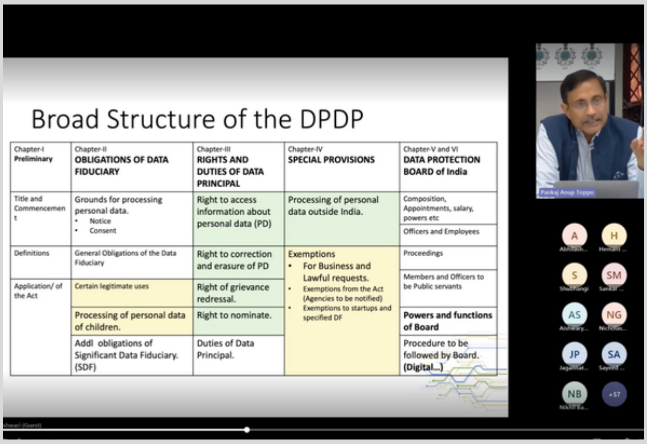
While APT groups operated across diverse geographical regions, concentrated attacks were observed in Europe, Latin America, the Middle East and various parts of Asia. Geopolitical motives often fuelled cyber espionage, remaining a dominant focus for these threat actors.

An intriguing development involved certain threat actors leveraging previously unknown iOS malware to execute zero-click iMessage exploits, signalling an evolving threat landscape, particularly concerning mobile devices, with businesses and critical infrastructure as prime targets.

Kaspersky, a significant player in the cybersecurity domain, actively monitored APT actors, with an expanded focus extending beyond mobile devices to encompass businesses and critical infrastructure.

In conclusion, these developments underscored the dynamic and ever-evolving nature of the cybersecurity landscape. APT actors persistently adapt their tactics and toolsets, highlighting the need for robust cybersecurity measures and continuous threat intelligence. To effectively navigate this evolving threat landscape, organizations must remain vigilant, regularly update their cybersecurity defences and collaborate with experts to defend against emerging threats effectively.

IFF'S DISCUSSION ON INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023



Broad Structure of the DPDP

Chapter-I **Preliminary**	Chapter-II **OBLIGATIONS OF DATA FIDUCIARY**	Chapter-III **RIGHTS AND DUTIES OF DATA PRINCIPAL**	Chapter-IV **SPECIAL PROVISIONS**	Chapter-V and VI **DATA PROTECTION BOARD of India**
Title and Commencement	Grounds for processing personal data. • Notice • Consent	Right to access information about personal data (PD)	Processing of personal data outside India.	Composition, Appointments, salary, powers etc
				Officers and Employees
Definitions	General Obligations of the Data Fiduciary	Right to correction and erasure of PD	Exemptions • For Business and Lawful requests. • Exemptions from the Act (Agencies to be notified) • Exemptions to startups and specified DF	Proceedings
Application/ of the Act	Certain legitimate uses	Right of grievance redressal.		Members and Officers to be Public servants
	Processing of personal data of children.	Right to nominate.		**Powers and functions of Board**
	Addl obligations of Significant Data Fiduciary. (SDF)	Duties of Data Principal.		Procedure to be followed by Board. **(Digital...)**

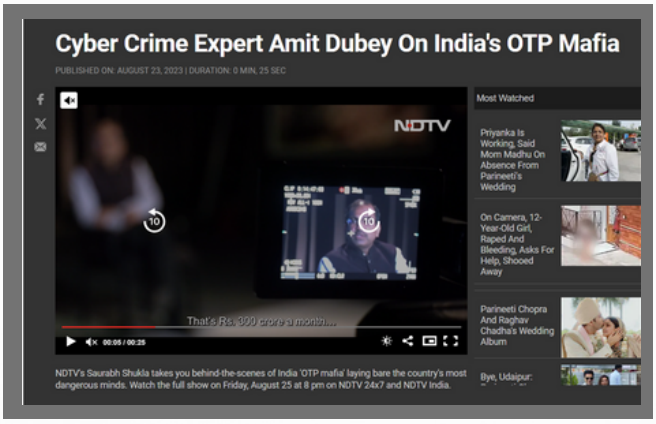
On 12 August 2023, India Future Foundation (IFF) played host to a momentous "Knowledge Session on India's Digital Personal Data Protection Bill, 2023 (now an Act)." Held at The United Service Institute of India in New Delhi, this event brought together luminaries and experts in the field to unravel the intricacies of the recently enacted legislation. The session began with Lt Gen. (Retd) (Dr) Rajesh Pant, chairman, India Future Foundation gave his opening remarks, where he provided a historical perspective on the development of the Data Protection Bill and underscored its paramount importance in fortifying the nation's cybersecurity infrastructure.

The event's focal point was a compelling presentation by Mr Rakesh Maheshwari, Member Advisory Board, India Future Foundation and Former Senior Director and Group Co-ordinator for Cyber Law and data Governance at the Ministry of Electronics and Information Technology (MeitY), Government of India. Mr Maheshwari's profound insights resonated with the audience as he elucidated on the far-reaching implications of the legislation across various sectors.

The session drew a diverse and distinguished audience of more than 75 participants, including prominent figures from both the public and private organizations. Despite the geographical diversity of the attendees, the event's virtual format facilitated their active engagement, fostering a dynamic exchange of ideas and perspectives.

The Knowledge Session served as a pivotal platform for comprehensive discussions and knowledge sharing, enabling attendees to better understand the intricacies of the Digital Personal Data Protection Act, and its pivotal role in shaping India's digital future. As the nation takes significant strides in enhancing data protection and privacy, such events continue to play a crucial role in fostering dialogue and collaboration among stakeholders across the digital landscape.

IFF IN THE MEDIA



Cyber Crime Expert Amit Dubey On India's OTP Mafia

PUBLISHED ON: AUGUST 23, 2023 | DURATION: 0 MIN, 25 SEC

That's Rs. 300 crore a month...

NDTV's Saurabh Shukla takes you behind-the-scenes of India 'OTP mafia' laying bare the country's most dangerous minds. Watch the full show on Friday, August 25 at 8 pm on NDTV 24x7 and NDTV India.

Most Watched

Priyanka Is Working, Said Mom Madhu On Absence From Parineeti's Wedding

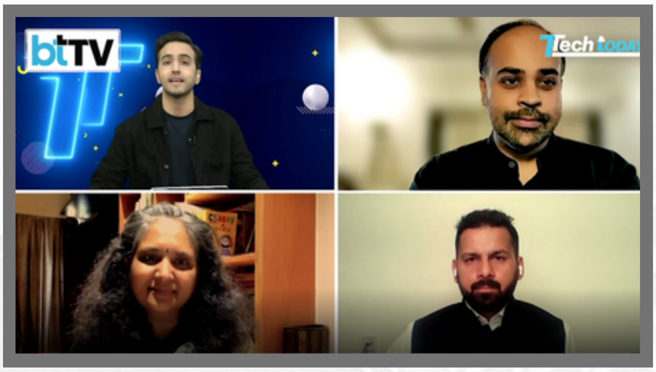
On Camera, 12-Year-Old Girl, Raped And Bleeding, Asks For Help, Shooed Away

Parineeti Chopra And Raghav Chadha's Wedding Album

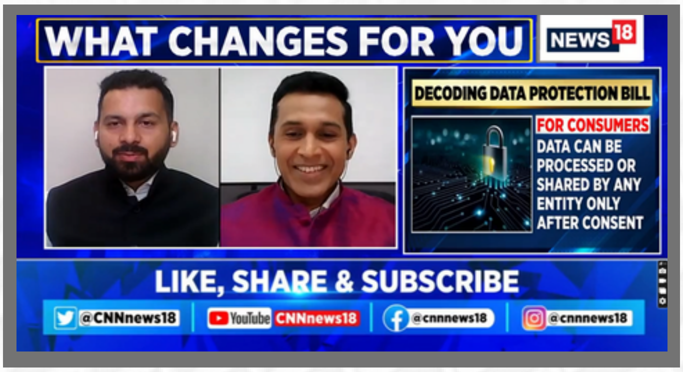
Bye, Udaipur:

Amit Dubey, Co-Founder, India Future Foundation (IFF) Exposed India's OTP Mafia on NDTV

Kanishk Gaur, Founder, IFF presented IFF's Report on Dark Web's Role in Drug Trafficking Exclusively on News18



Kanish Gaur, Founder, IFF shared his views on The Digital Personal Data Protection Act , 2023 with Tech Today



WHAT CHANGES FOR YOU

DECODING DATA PROTECTION BILL

FOR CONSUMERS

DATA CAN BE PROCESSED OR SHARED BY ANY ENTITY ONLY AFTER CONSENT

Kanishk Gaur, Founder, IFF decodes the Digital Personal Data Protection Act, 2023 and Its Impact on India's Digital Landscape with News18

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