HERITAGE CYBERWORLD LLP

drona
Detection Response Organization
Network Analysis

DRONAKSH™

WOMEN BUILDING THE FUTURE OF CYBERSECURITY

JUNE 2024
EDITION

Author:

Dhruv Pandit

#CyberSafeBharat

Heritage Cyberworld LLP signed MOU with Government of Gujarat committed to invest Rs.150 Crore & Create 2000 Skilled Cyber Security Expert Employment

Table Of Contents

Our **CEO's Words**

> Generate employment in India, Create 50 Integrated Cyber Security Command Control Center Labs by 2026 in India. Generate team of 1,00,000 Cyber Yodha's for nation to fight against cyber attacks.

Dr. Dhruv Pandit

Founder, CTO, and Director of Heritage Cyberworld LLP
Author - Dronaksh

Dr. Dhruv Pandit, the Founder, CTO, and Director of Heritage Cyberworld LLP, has started his remarkable journey towards industry prominence through a blend of knowledge and innovation. His visionary leadership has cemented the company's reputation as a trusted provider of cutting-edge cybersecurity solutions across diverse sectors.

Having received an Honorary PhD in Cybersecurity, Dr.Dhruv's significant contributions have not only elevated industry standards but also inspired countless individuals to pursue careers in this critical field. Starting at Ganpat University, his focus on cloud-based applications with IBM laid the foundation for his expertise.

Dr.Dhruv has launched DRONA, a pioneering Integrated Cybersecurity Command Center, as part of his commitment to combating escalating cyber threats. As he embarks on this journey, he also aims to establish Integrated Cyber Security Command Centers across various cities and train 100,000 cyber warriors, aligning with Prime Minister Narendra Modi's vision for national cybersecurity and job creation. Moreover, he is eager to collaborate on launching a cyber security magazine, ensuring that vital information reaches every corner of the cyber world.

The driving force behind launching Dronaksh, a cybersecurity magazine, is a passion for fostering a resilient cyber community. By providing the latest trends, news, and insights, Dronaksh aims to empower individuals and organizations with the knowledge to safeguard against emerging threats. Through knowledge sharing and proactive alerts, it seeks to build a united front against cyber threats while promoting preventive security measures.

Dronaksh, a cybersecurity magazine, is dedicated to fortifying the digital realm against evolving threats. By disseminating the latest trends and insights, it cultivates a vibrant cyber community and empowers safe navigation of the digital landscape. Its primary goal is to raise awareness about preventive security measures, provide timely alerts to mitigate risks, and foster collaboration and ethical conduct within the cyber community.

Dhruv Pandit

#CyberSafeBharat

AWARDS \ RECOGNITION:

* Represented India at the India Estonia Defence Delegation seminar in Estonia in 2024
* Hall of Fame from Google, Lenovo, Trend Micro, Intel, Alien Vault Microsoft and more.
* Times Men of The Year 2023 by Times of India
* India's Youngest Cyber security Entrepreneur by Knowledge Chamber Commerce Industry (KCCI)
* Cyber security researcher award from India Prime Awards
* Felicitated by Ministry of Education of India in National Education Summit 2022
* Felicitated by Ministry of Defence in India International Defence and Homeland Security Expo 2022
* Felicitated by Gujarat Police by solving the cases related cyber-crime investigation
* Represented India at the India Kuwait Defence Delegation seminar in Kuwait in 2022
* Chairman for Cyber Security at Knowledge Chamber of commerce and industry (KCCI)

FEATURED IN: The Indian Express · Law Street Journal · The Financial Express · Ahmedabad Mirror · The Times Group · Hindustan Times · NDTV इंडिया · ANI · abp न्यूज़ · दैनिक भास्कर · News18 इंडिया · tv9 · GTPL · Red Press · गुजरात मित्र

WOMEN IN CYBERSECURITY

There is growing diversity in the cybersecurity industry, which has long been dominated primarily by men. Women currently account for 25% of the cybersecurity workforce worldwide, and that number is expected to reach 30% by 2025.

The evolution of cyber threats requires this change to remain effective. Diverse teams provide stronger solutions and protections, enhancing safety through fresh perspectives.

Nevertheless, awareness about gender diversity's critical role in cybersecurity must be spread. Increasing the focus on narrowing the gender gap can accelerate the process of creating an inclusive work environment.

Types of Cyberattacks on Women

1. CYBER GROOMING

Online groomers build `relationships with someone with the intention of sexually abusing, exploiting, or trafficking them in the future.

It is the most common form of cybercrime against women. To gain women's trust, groomers use false methods to take advantage of that trust.

Under the new law, 10,000 cases of online grooming offenses were reported over the next two years. According to the Crimes Against Children Research Center, online child exploitation cases are initiated by perpetrators in 30% of the cases.

2. CYBER HACKING

Women are most often targeted by cybercriminals who use their sensitive information, such as addresses, financial information, and private conversations, to gain unauthorized access.

The act of hacking not only violates privacy, but can also result in serious financial losses and identity theft.

The chances of women being harassed online are 27 times greater than those of men, making them the most frequent victims of cybercrime.

Hacking and identity theft are a few of the financial consequences of cybercrime against women. It is estimated that the cost is around $1.5 billion a year.

3. CYBER BLACKMAIL

Using the Internet, people can share information and connect with each other. As a result, personal information is also revealed, putting them at risk of cyber-blackmail.

It is possible for perpetrators to threaten victims with exposing these sensitive data unless they fulfill their demands. Most of these incidents affect women and put their security at risk, as well as their emotional well-being and financial security.

People who blackmail others often prey upon social norms concerning sexuality to damage their reputations. This is done to force people to meet their needs.

4. CYBER STALKING

The act of cyberstalking involves monitoring someone's social media account and their activities. It may harm your reputation or relationships with loved ones when your online identity is impersonated.

It is possible to convert stalking into hacking by manipulating the victims so that their passwords are revealed.

30%

of women

National Intimate Partner and Sexual Violence Survey (NISVS) data indicates ***that 30% of women*** have faced stalking in their lifetime. Several studies have found that women who report experiencing online harassment report higher levels of depression, anxiety, and sleep disturbances compared to those who do not report experiencing it.

5. CYBER BULLYING

Cyberbullying" is when someone uses interactive digital technology or mobile phones to threaten, harass, humiliate, embarrass, or otherwise target a woman over the Internet or in other ways.

Cyberbullying is one form of online harassment experienced by 40% of women between 18 and 29

years old.
Young adults have experienced cyberbullying at least 64% of the time. The suicide rate among cyberbullying victims in middle school is almost twice that of non-victims.

Why are women underrepresented in Cybersecurity positions?

Multiple factors contribute to women's underrepresentation in cybersecurity. Historically, women have been underrepresented in the cybersecurity field for several reasons:

1. STEREOTYPES AND BIASES IN SOCIETY

It is possible for women to be influenced by societal norms and stereotypical views of gender roles in their career choices. As a male-dominated field, cybersecurity is often perceived as unwelcoming or unsuitable for women.

2. HAVING NO ROLE MODELS

Due to the lack of visible female role models in cybersecurity, girls and women may have trouble imagining themselves succeeding. An individual's role model is crucial in motivating and inspiring him or her to pursue a career path.

3. EDUCATIONAL DISPARITIES

Women face gender disparities in STEM education, which is necessary to become a cybersecurity expert. Early discouragement from STEM education can limit girls' exposure and interest in cybersecurity fields.

4. HIRING UNCONSCIOUS BIAS

It is not uncommon for unintentional bias to lead to employers overlooking female applicants when recruiting. In addition to affecting initial hiring decisions, bias can also influence career advancement and promotions.

25%

Reports indicate that only **25% of cybersecurity workers are women.**

Why must women build a career in Cybersecurity?

1. OPPORTUNITIES AND GROWING DEMAND

Cyber threats are fueling rapid growth in cybersecurity, creating vast career opportunities due to skill shortages. Job openings abound with competitive salaries, and women can advance swiftly in this dynamic field. A Cybersecurity Ventures report predicts 3.5 million unfilled cybersecurity jobs by 2025, highlighting a pressing need for diverse talent.

2. SECURITY BENEFITS FROM DIVERSE PERSPECTIVES

Cybersecurity hinges on problem-solving, risk minimization, and understanding human behavior. Diverse team perspectives are pivotal for successful security strategies, leveraging insights from women to craft inclusive measures that resonate across diverse audiences. Research underscores that diverse teams excel at efficient problem-solving, crucial in this dynamic field.

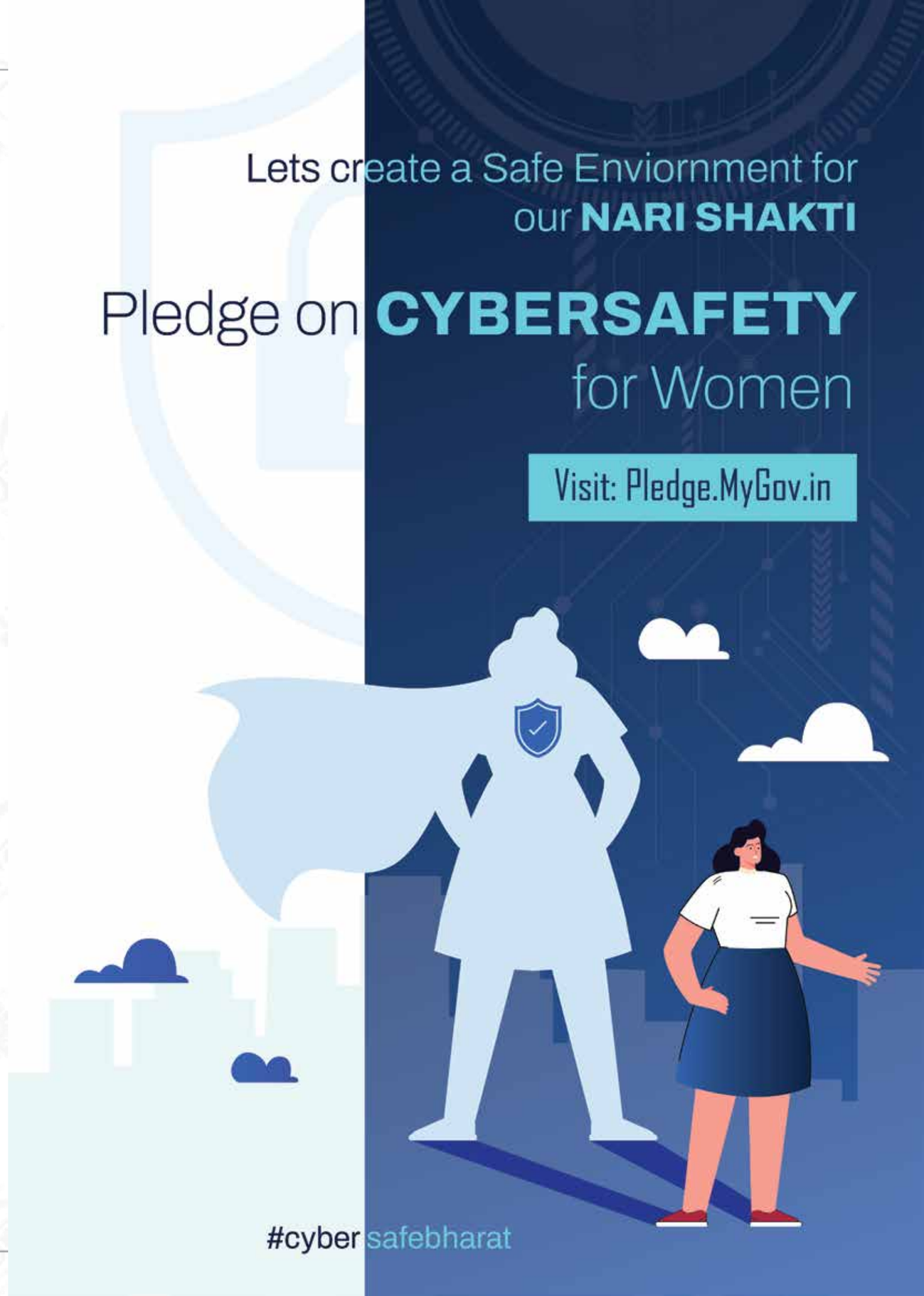
3. CLOSING THE GENDER GAP

Encouraging women in cybersecurity closes gender gaps, promotes equality, and brings diverse perspectives to the field, challenging stereotypes and setting new standards.

35%

of cybersecurity workers by 2025

Cybersecurity Ventures study indicates that women will comprise **35% of cybersecurity workers by 2025**.
There are nearly 50% of women in the world. However, only **24% are employed in cybersecurity**.



THE GROWING CYBER SECURITY THREAT IN CIVIL AVIATION INDUSTRY

Cybersecurity and aviation are both dynamic sectors but borderless in nature. Both require coordination at various levels: national and international. They also require immediate recognition of efforts to evolve, maintain, and raise cybersecurity on the same basis as MRO (maintenance, repair, and overhaul) with the aim of protecting the civil aviation sector from all cyber threats to safety and security.

It is interesting to see complexity and security as opposing factors within the Cyber Threats in Civil Aviation. For example, regarding the complexity associated with the Boeing 787 Dreamliner, research indicated that the aircraft has over eight million lines of software codes compared to the F-35 military aircraft, having 22 million lines of software codes. Modern aircraft are more vulnerable to bugs in the software, as the integration of technological advances causes aftereffects that degrade cyber defenses due to hyper-connectivity, which affects security and makes it difficult to test, analyze, and evaluate. It is imperative for system architectures to design the infrastructure to be technologically adaptable and secure from cyber threats.

Civil aviation is shifting from analog to vulnerable digitized communication systems, lacking adequate security measures against cyber threats. Current approaches are reactive, rather than proactive.

THERE ARE FOUR CATEGORIES OF TERRORIST THREATS TO CIVIL AVIATION:

1. The destruction of an aircraft with a bomb
2. Hijacking
3. A terrorist attack on the airport, and
4. A cyber-attack on the aviation infrastructure

It is shocking that 61% of all cyber-attacks in 2020 targeted airlines, almost twice as many as the two next most significant affected market segments combined (16% for manufacturers and 15% for airports), and 95% of these attacks were financially motivated. This led to financial loss in 55% of cases and the leaking or theft of personal data in an additional 34% of cases.

[ref : https://www.eurocontrol.int/publication/eurocontrol-think-pper-12-aviation-under-attack-wave-cybercrime]

The ICAO Cybersecurity Strategy for Civil Aviation is an interesting starting point. Of the roughly 12,000 standards and recommended practices (SARPs) in the Chicago Convention of 1944, only two deal with cybersecurity. ICAO's Resolution A40-10 also emphasizes Addressing Cybersecurity in Civil Aviation, focusing on developing an action plan and implementing a Cybersecurity Strategy as the core component for the civil aviation industry.

The current biggest challenge is not human exploitation but human irrelevance in the economic and political systems due to cyber wars. It's crucial to prioritize constant skill development and technological advancement, which are fundamental in the aviation industry.

Ms. Radhika Bhandari

Dean Aviation : Indus University
Director: Western India Institute of Aeronautics

PoC Exploit Released for macOS Root Access Vulnerability

Date: June 4, 2024

INTRODUCTION

A critical security vulnerability, CVE-2024-27822, has been discovered in macOS, allowing unauthorized root access, raising significant concerns among cybersecurity experts and macOS users.

VULNERABILITY DETAILS

Identified by security researcher Mykola Grymalyuk, CVE-2024-27822 affects Apple's Installer.app and the PackageKit. framework. The flaw resides in how installation scripts in PKGs are executed with root privileges, particularly those using the #!/bin/zsh shebang. These scripts load the user's .zshenv file, potentially executing any embedded malicious code with root permissions.

AFFECTED VERSIONS

•Affected: macOS 14.5 Beta 1 (23F5049f) and older, macOS 13.6.6 (22G630) and older, macOS 12.7.4 (21H1123) and older, and any version of macOS 11 or older.

•Resolved: macOS 14.5 Beta 2 (23F5059e) and newer, macOS 13.6.7 (22G720) and newer, macOS 12.7.5 (21H1222) and newer.

MITIGATION RECOMMENDATIONS

•Update Software: Ensure macOS is updated to the latest version.

•Limit User Privileges: Avoid using root or admin accounts for daily tasks.

•Monitor Systems: Implement robust monitoring for unusual activities.

•Backup Data: Regularly back up important data.

APPLE'S RESPONSE

Apple has acknowledged the vulnerability and is actively working on a patch. Users are advised to apply updates immediately once available. The release of the PoC for CVE-2024-27822 emphasizes the urgency for timely updates and vigilant security practices.

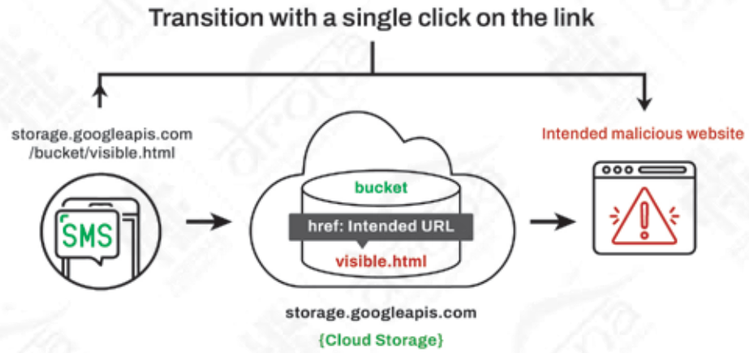
Reference: https://cybersecuritynews.com/macos-root-access-vulnerability/

Hackers Exploiting Amazon, Google & IBM Cloud Services To Steal Customer Data

Date: June 03, 2024

Criminals are exploiting cloud storage services like Google Cloud Storage, Amazon AWS, and IBM Cloud to host phishing websites for SMS scams. They abuse the static website hosting feature to store HTML files with malicious URLs, included in SMS messages that bypass firewalls due to trusted cloud platform domains.

Clicking the link in the SMS directs users to a seemingly legitimate cloud-hosted site, which then redirects them to a phishing site to steal information. Attackers use the "HTML meta refresh" technique to automatically redirect users from a malicious webpage hosted in a cloud storage bucket to their intended phishing site.



Scammers exploit these trusted cloud services by creating buckets with malicious HTML pages that leverage the meta refresh tag, often with a zero-second delay, to redirect users. This method, which disguises fraudulent websites as legitimate offers, aims to steal personal and financial information.Scammers exploit these trusted cloud services by creating buckets with malicious HTML pages that leverage the meta refresh tag, often with a zero-second delay, to redirect users. This method, which disguises fraudulent websites as legitimate offers, aims to steal personal and financial information. This technique allows scammers to bypass security filters, making the phishing attempts more credible and increasing their success rate since users are less likely to suspect links from reputable cloud service providers.

Reference: https://cybersecuritynews.com/hackers-exploit-cloud-services-steal-data/

Hackers Actively Exploiting Checkpoint 0-Day

Date: June 04, 2024

OVERVIEW

Cybersecurity experts have identified a critical zero-day vulnerability in Checkpoint's security software, designated as CVE-2024-24919. This flaw poses significant threat to organizations relying on Checkpoint's solutions, allowing attackers to execute arbitrary code remotely and potentially gain full control over affected systems.

DETAILS OF CVE-2024-24919

The vulnerability affects multiple versions of Checkpoint's security software. Discovered by a team of researchers and reported to Checkpoint, the flaw was exploited by malicious actors before a patch could be released. Hackers have used this zero-day flaw to launch sophisticated attacks, bypassing security measures and infiltrating networks, primarily targeting large enterprises and government agencies.

CHECKPOINT'S RESPONSE

Checkpoint has acknowledged the vulnerability and is working on a patch. The company has urged customers to remain vigilant and apply any available mitigations until the official fix is released. They recommend monitoring network traffic for unusual activity and applying temporary fixes provided by Checkpoint.

MITIGATION STEPS

While waiting for the official patch, experts recommend the following steps to mitigate the risk:

•**Apply Temporary Fixes:** Use the temporary fixes and workarounds provided by Checkpoint.

•**Monitor Network Traffic:** Keep a close watch on network traffic for signs of unusual activity or

potential breaches.

•Update Security Policies:
Review and strengthen security policies to handle potential threats.

•Educate Employees:
Train employees to recognize phishing attempts and other common attack vectors.

Reference: https://cybersecuritynews.com/hackers-actively-exploiting-0-day/

Cisco Webex Vulnerability Exposes Sensitive

Date: June 5, 2024

A critical vulnerability in Cisco Webex Meetings, CVE-2024 -24919, allowed unauthorized access to sensitive meetings, affecting both self-hosted and cloud instances. Discovered by Netzbegrünung and verified by Eva Wolfangel, the flaw stemmed from non-random meeting IDs and misconfigured mobile views, exposing metadata and meeting details. Hackers exploited this to access high-profile meetings, including those of the Bundeswehr and SPD. Cisco patched the vulnerability by May 28, 2024, and notified customers. The German BSI advised rescheduling meetings for security. This incident highlights the need for robust security and prompt patching in video conferencing tools.

Reference: https://www.helpnetsecurity.com/2024/06/05/cisco-webex-cloud-vulnerability/?web_view=true

Pakistan-linked Malware Campaign Evolves to Target Windows, Android, and macOS

Date: June 13, 2024

Threat actors linked to Pakistan have been running a malware campaign called Operation Celestial Force since at least 2018. This campaign uses Android malware GravityRAT and a Windows-based malware loader HeavyLift, managed by a tool named GravityAdmin. Cisco Talos attributes these activities to a group known as Cosmic Leopard, which shares tactics with Transparent Tribe.

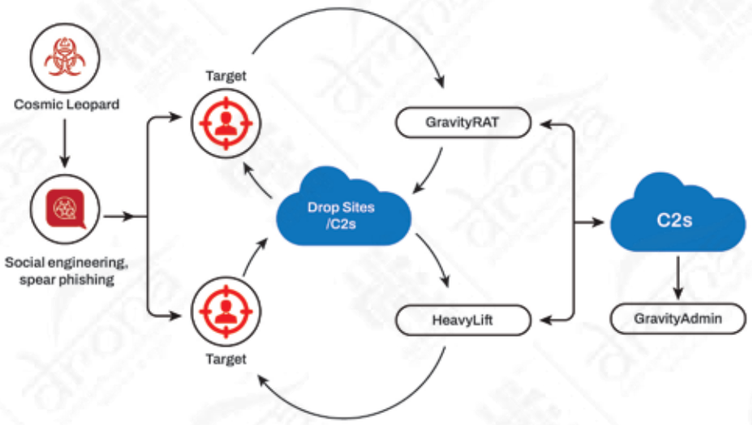
GravityRAT, initially discovered in 2018 targeting Indian entities, has evolved to work on Android and macOS. It has been used to target military personnel in India and the Pakistan Air Force by disguising as legitimate apps. Cosmic Leopard employs spear phishing and social engineering to distribute GravityRAT and HeavyLift, which gather and export system metadata to command-and-control servers. Cisco Talos' findings indicate that GravityAdmin has been used since August 2021 to control infected systems. The malware campaign targets Indian defense, government, and technology sectors, highlighting the persistent threat posed by these advanced cyber operations.

Reference: https://thehackernews.com/2024/06/pakistan-linked-malware-campaign.html

Grandoreiro Banking Trojan Hits Brazil as Smishing Scams Surge in Pakistan

Date: June 15, 2024

Operation Celestial Force: Infection Chain



Pakistan is the latest target of the Smishing Triad, a threat actor previously active in the EU, Saudi Arabia, UAE, and the US. This group uses phishing tactics by sending fake messages via iMessage and SMS, impersonating Pakistan Post to steal personal and financial information. They exploit stolen databases from the dark web to send these messages, tricking recipients into clicking on links related to false package delivery notifications, leading them to enter sensitive information on fraudulent websites.

The Smishing Triad also targets individuals expecting deliveries from couriers like TCS, Leopard, and FedEx. Meanwhile, Google has identified a threat actor named PINEAPPLE targeting Brazilian users with tax-themed spam, leading to the deployment of Astaroth malware. PINEAPPLE misuses cloud services like Google Cloud and AWS to distribute malware.

Additionally, Google highlighted Brazil-based UNC5176, which targets financial services and other sectors using the URSA backdoor to steal banking and crypto currency login credentials. This group spreads malware via emails and malvertising, leading victims to download and execute malicious scripts. Another actor, FLUXROOT, has been linked to the Grandoreiro banking trojan and phishing attacks impersonating Mercado Pago.

These developments underscore the evolving nature of cyber threats targeting financial information across different regions.

Reference: https://thehackernews.com/2024/06/grandoreiro-banking-trojan-hits-brazil.html

Microsoft Revamps Controversial AI Powered Recall Feature Amid Privacy Concerns

Date: June 08, 2024

Microsoft's upcoming Recall feature for Copilot+ PCs, set to launch on June 18, 2024, is facing significant backlash over privacy and security concerns. Designed as a visual timeline, Recall captures snapshots every five seconds to help users track their digital activity. Critics have labelled it as "unrequested, pre-installed spyware," expressing worries about the potential exposure of sensitive data like documents and private messages. Additionally, some experts highlighted the secretive development process by the company. In response to the criticism, Microsoft has emphasized user control and security.

They introduced updates requiring Windows Hello biometric authentication to access the Recall timeline, ensuring that snapshots are encrypted and only decrypted upon user verification. The company assures that all data is stored locally, not shared externally, and that users can pause, filter, or delete snapshots at any time. Furthermore, IT administrators in enterprise environments can disable the feature, though only users can enable it. Despite the backlash, Microsoft maintains that these measures provide a secure and beneficial tool for users to keep track of their activities.

Reference: https://thehackernews.com/2024/06/microsoft-revamps-controversial-ai.html

CERT-In Vulnerability Note CIVN-2024-0188: Multiple Vulnerabilities in Apple VisionOS

Date: June 13, 2024

Severity Rating: HIGH

SOFTWARE AFFECTED

• Apple visionOS:
Versions prior to 1.2

OVERVIEW

Multiple vulnerabilities in Apple visionOS (versions prior to 1.2) could allow attackers to execute arbitrary code with kernel privileges, cause app termination, bypass security protections, fingerprint users, cause denial of service (DoS), access sensitive information, and gain elevated privileges. These issues arise from use-after-free in the Kernel, errors in CoreMedia and libiconv, out-of-bounds write and access, integer overflow, and type confusion in WebKit. Attackers can exploit these by sending malicious web content, leading to memory corruption.

SOLUTION

Apply appropriate software updates as mentioned in the Apple Security update: https://support.apple.com/en-us/HT214108

Reference: https://www.cert-in.org.in-/s2cMainServlet?pageid=PUBVL-NOTES01&VLCODE=CIVN-2024-0188

CERT-In Advisory CIAD-2024-0030: Multiple Vulnerabilities in NVIDIA Products

Date: June 14, 2024

Severity Rating: HIGH

NVIDIA

SOFTWARE AFFECTED

• NVIDIA GPU drivers and virtual GPU (vGPU) versions R555, R550, R535, and R470

OVERVIEW

Multiple vulnerabilities have been reported in the NVIDIA GPU Display Driver that could enable an attacker to execute arbitrary code, escalate privileges, disclose sensitive information, and cause denial of service (DoS) on the targeted system.

SOLUTION

Apply appropriate fixes as mentioned in NVIDIA Security Advisory: https://www.nvidia.com/Down-load/index.aspx

Reference: https://www.cert-in.org.in-/s2cMainServlet?pageid=PUBVL-NOTES02&VLCODE=CIAD-2024-0030

CERT-In Vulnerability Note CIVN-2024-0189: Multiple Vulnerabilities in Google Chrome for Desktop

Date: June 14, 2024

Severity Rating: HIGH

chrome

SOFTWARE AFFECTED

• Google Chrome versions prior to 126.0.6478.54 for Linux

• Google Chrome versions prior to 126.0.6478.56/57 for Windows and Mac

OVERVIEW

Multiple vulnerabilities in Google Chrome could allow a remote attacker to execute arbitrary code on the targeted system. These issues arise from type confusion in V8, use-after-free in Dawn, V8, BrowserUI, and Audio, inappropriate implementation in Dawn, DevTools, Memory llocator, and Downloads, heap buffer overflow in Tab Groups and Tab Strip, and policy bypass in CORS. An attacker could exploit these vulnerabilities by persuading a victim to visit a specially crafted web page. Successful exploitation could lead to arbitrary code execution on the targeted system.

SOLUTION

Apply appropriate updates as mentioned by the vendor: https://chromereleases.-googleblog.com/2024/06/stable-channel-update-for-desktop.html

Reference: https://www.cert-in.org.in-/s2cMainServlet?pageid=PUBVL-NOTES01&VLCODE=CIVN-2024-0189

20. GRIEFING
19. DATA
18. SPOOFING
17. INTERNET
16. FIREWALLS
15. BOOKMARKS
14. IDENTITY
13. PROVIDER
12. SPYWARE
11. SERVICE
10. ONLINE
9. THEFT
8. ENCRYPTION
7. FRAUD
6. MALWARE
5. COOKIES
4. CACHE
3. ANTIVIRUS
2. SCAM
1. PHISHING

Solution

CYBERSECURITY UNSCRAMBLE WORDS

1. GHINHSIP _____
2. ASMC _____
3. VTURISANI _____
4. AHCEC _____
5. CKEOOSI _____
6. WELRMAA _____
7. ADRUF _____
8. RNITEYOCNP _____
9. HFTET _____
10. LONINE _____
11. SIEVECR _____
12. SPARYEW _____
13. DRIORVEP _____
14. YTIDTNEI _____
15. OKASKRMBO _____
16. WRFAELLSI _____
17. IENTTREN _____
18. SGOFONIP _____
19. TADA _____
20. EGIFRGIN _____

NAVIGATING PRIVACY AND FREEDOM: THE RIGHT TO BE FORGOTTEN IN INDIA'S LEGAL LANDSCAPE

The right to be forgotten, established by the EU in May 2014, allows individuals to request removal of personal information from online platforms. India lacks a specific law for this right, but the Personal Data Protection Bill introduced in December 2019 aims to address this, emphasizing individuals' ability to control the disclosure of their personal data.

EMERGENCE OF THE RIGHT TO BE FORGOTTEN IN THE INDIAN CONTEXT

The landmark case of Justice K.S. Puttaswamy v. Union of India affirmed the right to privacy, significantly influencing India's data protection discussion. The Justice B.N. Srikrishna Committee's 2018 data protection bill introduced the 'Right to be Forgotten.' Later, on December 11, 2019, Ravi Shankar Prasad introduced the Personal Data Protection Bill to the Lok Sabha.

THE RIGHT TO BE FORGOTTEN

Individuals can request the removal of personal information, including images and identifiable data, from publicly accessible platforms. While Section 43A of the Information Technology Act of 2000 mandates compensation for businesses failing to secure sensitive data, the 'Right to be Forgotten' is not explicitly included in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. However, these rules do allow complaints to be lodged with a designated Grievance Officer for content removal.

THE PROGRESS OF THE RIGHT WITHIN INDIA

In India, the 'Right to be Forgotten' was first considered in Dharamraj Bhanushankar Dave v. State of Gujarat, and later recognized in Jorawar Singh Mundy vs. Union of India, where the court mandated the removal of access to a judgment to protect privacy. While part of the broader right to privacy under Article 21 of the Constitution, its specific status as a fundamental right remains unclear. The Personal Data Protection Bill, 2019, could establish it as a crucial element of data protection in India.

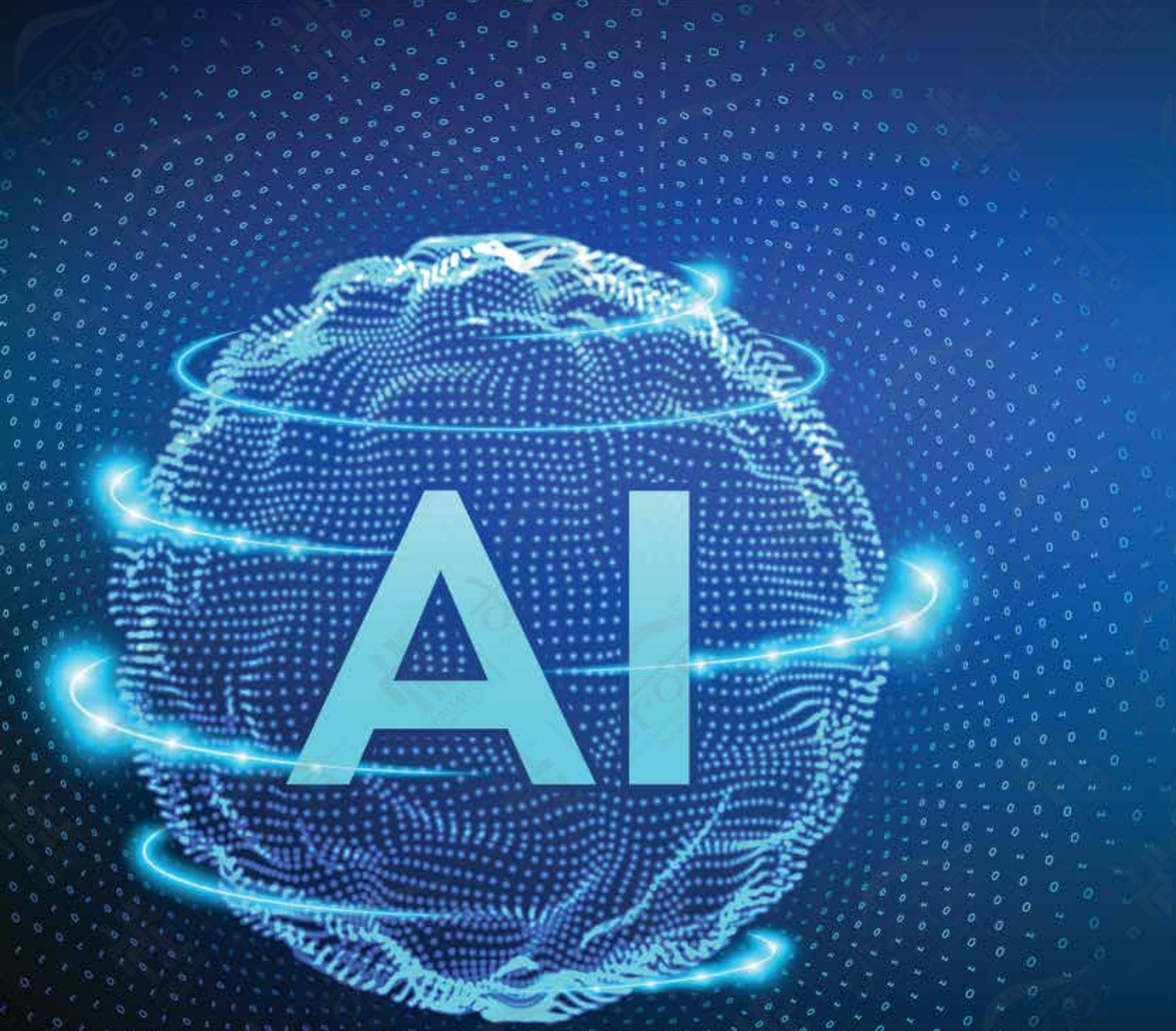
CHALLENGES AND POTENTIAL SOLUTIONS

Implementing the Right to Be Forgotten presents challenges in balancing personal rights with journalism, freedom of expression, and speech. This right could impede journalism by delaying news publication, infringe on the universal right to Freedom of Expression, and curtail open discourse and critical scrutiny

Adv. Jhanak Sharma

Managing Editor at LawStreet Journal
Senior Partner at Aquilas Legal

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY



AI in Cybersecurity: How AI in Changing Take on Cybersecurity?

The future of cybersecurity is already shaped by artificial intelligence.

Most hackers manipulate ChatGPT today to create malware, search for vulnerabilities in code and circumvent security controls.

Social engineers use artificial intelligence to conduct more advanced phishing scams and deepfakes.

AI-supported password guessing and CAPTCHA cracking have made sensitive data accessible to hackers.

Cyber attacks have increased over the past 12 months and 85% of security experts believe bad actors are using artificial intelligence to commit the attacks.

Additionally, machine learning, natural language processing, and AI-based algorithms strengthen cybersecurity by detecting concealed anomalies, pinpointing attack vectors and automating security breach responses.

Let's discover the AI in cyberattacks and how it is shifting cybersecurity measures.

GLOBAL FINDINGS OF CYBERATTACKS

A cyber attack has become the new norm across the public and private sectors, ranking fifth on the list of top risks. It's going to be a risky industry in 2024. It is predicted that IoT cyber attacks will double by 2025 alone. Here are further global findings of cyberattacks that are drowning fear in the cyber world.

IMPORTANCE OF AI IN IMPLEMENTING CYBERSECURITY

As cyber-attacks become more complex and advanced, conventional defences are harder to detect and prevent. A growing volume of data requires organizations to identify potential risks, leading to a higher priority for cybersecurity. The best way to combat these threats is to adopt innovative solutions.

Here is a list of the growing importance of implementing AI in Cybersecurity.

1. Reduction of costs

Automating cybersecurity operations with AI reduces costs in a variety of ways. AI automates functions like log analysis, vulnerability assessments, and patch deployment, saving time and resources by minimizing manual intervention. AI also contributes to cost reduction by improving threat detection accuracy.

2. Increased scalability

There are many problems with traditional cybersecurity approaches when dealing with complex, interconnected environments with large amounts of data. With AI, it is possible to process and analyze large amounts of data from many different sources at the same time.

The algorithms that AI uses are capable of analyzing logs from networks, computers, user behaviour, and threat intelligence as well. AI can detect subtly hidden threats humans may overlook due to its scalability, enabling proactive defence.

3. Analyzing attack precursors

AI algorithms, particularly machine learning and deep learning can analyse a large amount of information and identify patterns humans might never notice. System vulnerabilities will be detected earlier, resulting in a reduced risk of security breaches and an improved ability to detect threats. It's possible to train AI systems to recognize patterns and prevent ransomware attacks from spreading.

USES OF AI IN IMPLEMENTING CYBERSECURITY

Malware and Phishing Detection

A cybersecurity system based on artificial intelligence demonstrates enhanced efficacy. Deep Instinct reveals AI systems can detect malware with 80% to 92% accuracy versus 30% to 60% for traditional programs.

Using artificial intelligence, it is possible to identify spam, phishing messages, and legitimate emails based on their content and context. Artificial intelligence can adapt to new threats through machine learning algorithms, demonstrating the signs of sophisticated attacks such as advanced phishing. Corporate networks must be protected from suspicious activities before they cause harm.

Artificial intelligence excels at identifying phishing traps and thwarting potential attacks.

Analyzing code for vulnerabilities

Static analysis of source codeis often used to identify security vulnerabilities. This technique is great at identifying existing vulnerabilities and patterns of attack but may fail to identify new ones.

Using machine learning algorithms, security flaws can be identified in source code by examining code structures, patterns, or dependencies, even without the presence of known patterns.

Securing Authentication

Security layers must be added to websites that provide user accounts or contact forms with sensitive information.

For example, facial recognition, CAPTCHA, and fingerprint scanning provide this level of security. In order to prevent security breaches, it is important that fraudulent login attempts are detected and malicious login attempts are eliminated.

FUTURE INSIGHTS OF AI AND CYBERSECURITY

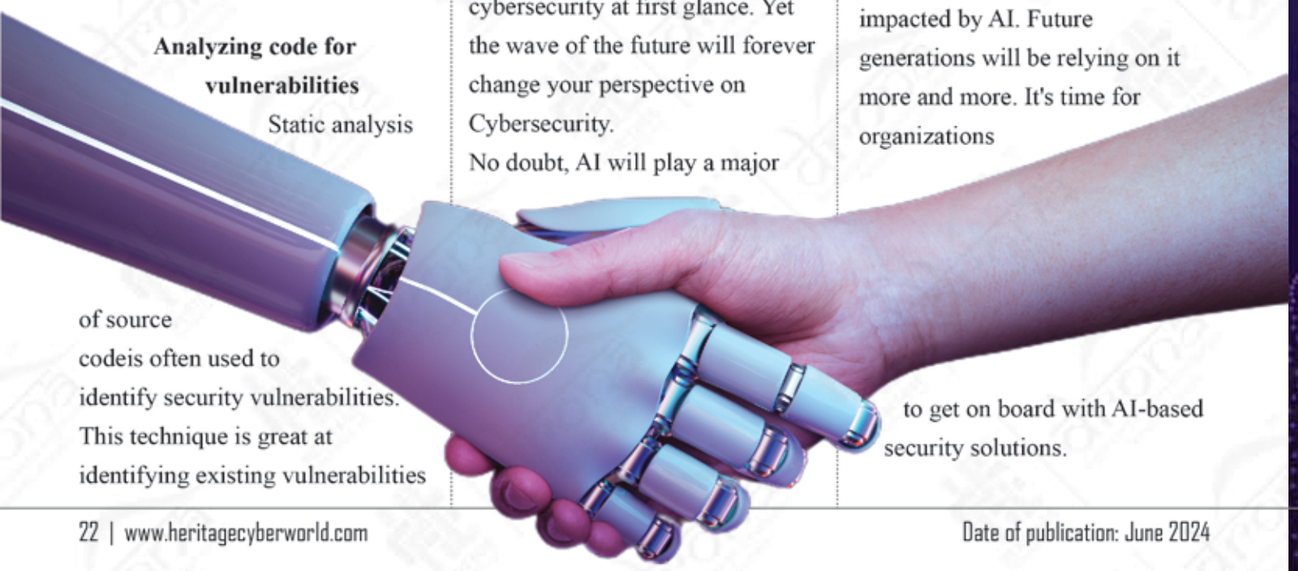
It may seem impossible to use artificial intelligence in cybersecurity at first glance. Yet the wave of the future will forever change your perspective on Cybersecurity.

No doubt, AI will play a major

role in cybersecurity in the future. Some of the reasons are as follows:

- Rapidly and accurately identify threats.
- Block suspicious activity automatically to prevent attacks.
- Enhance network resilience in the face of attacks.
- Reduce the time it takes to recover from a cyberattack.
- Digitize systems and make them more secure.

Cybersecurity has already been impacted by AI. Future generations will be relying on it more and more. It's time for organizations to get on board with AI-based security solutions.



$135 billion in 2030

Researchers estimate that AI-based cybersecurity products will total ***$135 billion in 2030.***

74%

According to the survey, **74% of respondents feel AI-powered cyber threats** are a major threat to their organizations.

Approximately **60% of respondents** worry that AI-powered threats are posing a threat to their organizations.

Verified Market Research estimates that the AI market size for cybersecurity will reach **$102 billion by 2032**.

Cybercrime is up 600%

After the COVID-19 pandemic, **cybercrime is up 600%**, from thefts to hacks and data breaches. IBM estimates that it takes **197 days for a company to discover a breach and 69 days** for it to resolve. With cybersecurity experts on your side, you can take all the steps to defend against cybercriminals and avoid losses caused by cybercrime.

Statista Market Report projects that cybersecurity revenues are expected to reach **$270 billion by 2029**.

More than **$1 million was saved by companies that contained a breach within 30 days** versus companies that took over 30 days to prevent a breach. When your company fails to respond to a data breach, it may face even greater problems.

A minimum of **81% of companies were infected with ransomware in 2023**
65% of Indian organizations are affected by ransomware attacks

85% of security professionals

Over ***85% of security professionals*** believe generative AI is to blame for the spike in cyber-attacks over the past year.

Platforms powered by AI streamline workflows, allowing teams to respond to incidents more quickly and accurately.

A ***$10 billion investment*** over five years is being made by Google's Project Zero to improve cybersecurity.

Meet Our CISO

Mr Ravinder Kumar, appointed as Chief Information Security Officer (CISO) for Heritage Cyberworld LLP, a cybersecurity professional with a military background and over twenty years of experience in Network Operations Center (NOC) and Security Operations Center (SOC) environments, his journey is a testament to flexibility, adaptability and excellence in protecting digital assets.

His military service gave him discipline, leadership strategic thinking, and other strong qualities that have been important in his security career. Based on this background, he mastered the intricacies of NOC operations, network monitoring, optimization, and troubleshooting. A deep understanding of network architecture and protocols allows him to ensure the smooth operation and security of critical systems even under high-pressure conditions.

Moving into the role of SOC, taking the challenge of protecting against cyber threats with vigilance and determination. He has experience in threat detection, incident response, and threat analysis in SOC. He can adapt quickly and effectively to identify and remediate security incidents, minimizing the impact on organizational operations, using advanced tools and techniques.

Mr Ravinder Kumar has an understanding of the Deep and Dark web landscape, his experience transcends the boundaries of traditional cybersecurity. With insight into the tactics and techniques used by threat actors, he can anticipate emerging threats and activate defenses against them. This experience allowed him to stay ahead of the enemy and ensure the integrity of the organization's security posture.

Mr Ravinder Kumar has been committed to continuous learning and professional development, monitoring the latest trends, technologies, and best practices in cybersecurity. His commitment to success, combined with his military background, makes him a trusted digital asset custodian to protect the integrity, confidentiality, and availability of critical systems and data in today's ever-evolving threat environment.

Mr. Ravinder Kumar - Air Veteran

Defence Cyber Agency HQ Integrated Defence Staff - MOD (Govt. Of India) CISM, ISACA
CISO - Heritage Cyberworld LLP

Date of publication: June 2024

HERITAGE CYBERWORLD LLP

drona
Detection Response Organization
Network Analysis

Dhruv Pandit
#CyberSafeBharat

1st ANNIVERSARY

YEAR

D.R.O.N.A

ONE YEAR OF DRONA! HEARTFELT THANKS TO OUR AMAZING TEAM FOR ALL THEIR EFFORTS.
HERE'S TO MANY MORE SUCCESSFUL YEARS!

www.heritagecyberworld.com

DOWNLOAD OUR **PREVIOUS EDITIONS**

May Edition:
Navigating CVES
and Breach Incidents

June Edition:
Navigating Cybersecurity
Challenges in Elections

SCAN ME