KIET GROUP OF INSTITUTIONS
Connecting Life with Learning
www.kiet.edu
Delhi-NCR, Ghaziabad
Toll Free No.: 1800-1200-106
CELEBRATING 25 YEARS OF EXCELLENCE
CYBER PEACE CENTRE

Edition 3
(Jan-Mar) 2024

CYBER कवच

CYBER PEACE CENTRE

Contents

Articles

- Navigating the Cyber Battlefield
- Unvelling the Latest Cybersecurity Trends
- The Looming Quantum Threat
- Deepfakes
- What Real Hacking Looks Like

Case Study

- LockBit vs FBI - A High-Stakes Cyber Showdown

Cyber bytes

Glimpses

Edited by:-
Vijay Yadav (ECE 2nd Year)
Anmol Rana (CSE(AI) 1st Year)
Vikas Rajput (CSE(AI&ML) 1st Year)

Coordinated by:-
Aditya Pandey (IT 3rd Year)
Pradeep Kumar (IT 3rd Year)
Riya Singhal (CSE 3rd Year)

ARTICLES

Navigating the Cyber Battlefield: Addressing Challenges in Cybersecurity for 2024

Complied by:- Supriya Dubey
Assistant Professor (CSIT Department)

As we step into the realm of 2024, the landscape of cybersecurity is as complex and dynamic as ever. Here, we delve into some of the key challenges that demand attention in the realm of cybersecurity for the year ahead.

1. Cyber Warfare and Nation-State Threats: The emergence of nation-state cyberattacks poses one of the most significant challenges to global cybersecurity. State-sponsored actors leverage advanced techniques to infiltrate critical infrastructure, disrupt services and steal sensitive information. With geopolitical tensions on the rise, the potential for cyber warfare looms large.

2. Ransomware Epidemic: In recent years, ransomware attacks have surged, targeting organizations of all sizes across various sectors. These attacks not only cause financial losses but also result in operational disruptions and reputational damage. Threat actors are continually refining their tactics, employing encryption techniques and leveraging vulnerabilities in software and systems. Combatting the ransomware epidemic demands a multi-faceted approach, including enhanced cybersecurity measures, proactive threat intelligence sharing and greater resilience in data backup and recovery strategies.

3. IoT Security Vulnerabilities: The proliferation of Internet of Things (IoT) devices presents a double-edged sword in terms of cybersecurity. While these devices offer convenience and efficiency, they also introduce new entry points for cyber threats. Many IoT devices lack robust security features, making them vulnerable to exploitation by malicious actors. In 2024, addressing IoT security vulnerabilities requires industry-wide standards, rigorous testing protocols and the implementation of secure-by-design principles to mitigate risks effectively.

4. Insider Threats and Human Error: Despite technological advancements, human error remains a prevalent cybersecurity challenge. Insider threats whether intentional or unintentional, can result in data breaches, intellectual property theft or sabotage. As remote work becomes more prevalent, the attack surface expands, amplifying the risks associated with insider threats. Mitigating this challenge necessitates comprehensive training programs, robust access controls and continuous monitoring to detect and address anomalous behavior effectively.

5. AI-Powered Cyber Attacks: As artificial intelligence (AI) technologies continue to evolve, so too do the capabilities of cyber attackers. AI-driven attacks can automate tasks such as reconnaissance, evasion and exploitation, enabling adversaries to launch sophisticated and targeted campaigns at scale. Furthermore, the malicious use of AI can exacerbate the challenges of detecting and mitigating cyber threats. To counter this emerging threat, cybersecurity professionals must leverage AI and machine learning for defensive purposes, developing AI-driven tools capable of identifying and neutralizing malicious activities in real-time.

6. Supply Chain Security Risks: The interconnected nature of global supply chains introduces inherent cybersecurity risks. Adversaries often target supply chain components such as software vendors or third-party suppliers to infiltrate their intended targets indirectly. Supply chain attacks can have far-reaching consequences, compromising the integrity and security of products and services across various sectors. Strengthening supply chain security requires enhanced due diligence, greater transparency and the implementation of robust security controls throughout the procurement process.

As we embark on the journey through 2024, the challenges confronting cybersecurity are manifold and ever-evolving. From nation-state threats to ransomware attacks and IoT vulnerabilities, the digital landscape remains fraught with peril. However, by fostering collaboration, innovation, and resilience, we can navigate this cyber battlefield and safeguard our digital future. It is imperative that stakeholders across all sectors prioritize cybersecurity efforts, invest in robust defense mechanisms, and remain vigilant against emerging threats. Only through collective action and unwavering commitment can we effectively address the challenges that lie ahead and build a more secure and resilient cyberspace for generations to come.

ARTICLES

Unveiling the Latest Cybersecurity Trends : Safeguarding the Digital Frontier

Complied by:- Kartikeya Srivastava
Former President CPC

In an era dominated by digital landscapes, the evolving nature of cyber threats continues to challenge organizations worldwide. From sophisticated ransomware attacks to data breaches compromising sensitive information, the cybersecurity landscape remains dynamic and complex. Here are some key insights into the current cybersecurity landscape:

1. Rise of Artificial Intelligence and Machine Learning in Cybersecurity: With cyber threats becoming more sophisticated, the integration of AI and ML technologies is increasingly vital in detecting and mitigating threats in real-time. These technologies empower cybersecurity systems to identify patterns, anomalies and potential risks, enhancing overall defense mechanisms.

2. Zero Trust Architecture (ZTA): Traditional perimeter-based security models are no longer sufficient in today's interconnected environments. Zero Trust Architecture advocates for a 'NEVER TRUST, ALWAYS VERIFY' approach, where every user and device accessing the network is continuously authenticated and authorized, regardless of their location.

3. Emphasis on Cloud Security: As organizations embrace cloud computing for its scalability and flexibility, ensuring robust cloud security measures is paramount. This involves implementing encryption protocols, access controls and regular audits to protect sensitive data stored in the cloud from unauthorized access and breaches.

4. Cybersecurity Automation: With the growing volume of cyber threats, automation plays a pivotal role in streamlining security operations. Automated incident response, threat detection and vulnerability management enable organizations to respond swiftly to emerging threats, reducing the risk of breaches and minimizing downtime.

5. Focus on Supply Chain Security: Cyberattacks targeting supply chains have become increasingly prevalent, posing significant risks to organizations and their partners. Strengthening supply chain security involves conducting thorough risk assessments, implementing vendor security protocols and fostering collaboration among stakeholders to mitigate potential vulnerabilities.

6. Enhanced Identity and Access Management (IAM): Identity theft and credential-based attacks remain persistent threats in the cybersecurity landscape. Adopting robust IAM solutions such as multi-factor authentication and privileged access management, helps organizations safeguard sensitive data and prevent unauthorized access to critical systems.

7. Quantum-Safe Cryptography: As quantum computing advancements loom on the horizon, the threat to conventional cryptographic algorithms grows. Quantum-safe cryptography, based on algorithms resistant to quantum attacks, is emerging as a proactive measure to protect data integrity and confidentiality in the quantum era.

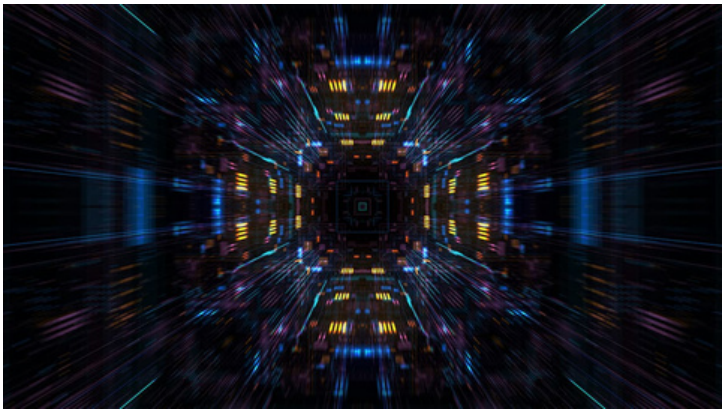
8. Cybersecurity Skills Gap Mitigation: The shortage of skilled cybersecurity professionals continues to challenge organizations in maintaining effective security postures. To address this gap, investing in cybersecurity education, training programs and workforce development initiatives is essential to cultivate a skilled talent pool capable of tackling evolving cyber threats.

9. Increased Focus on IoT Security: The proliferation of Internet of Things (IoT) devices presents unique cybersecurity challenges, as these interconnected devices often lack robust security measures. Securing IoT ecosystems involves implementing encryption, authentication mechanisms and regular firmware updates to mitigate potential vulnerabilities and prevent unauthorized access to sensitive data.

10. Heightened Regulatory Compliance Requirements: Governments and regulatory bodies worldwide are enacting stricter data protection laws and compliance standards to safeguard consumer privacy and mitigate cyber risks.

The Looming Quantum Threat: Why We Need Quantum-Resistant Cryptography?

Complied by:- Sarvagya Pradhan
Member CPC



The internet is built on trust – Trust that the information we send and receive stays secure. This trust is underpinned by cryptography, the science of scrambling data so only authorized parties can unscramble it. For decades, the workhorse of cryptography has been public-key encryption, where a public key is used to encrypt messages and a private key is needed to decrypt them.

However, this trust is under threat. Quantum computers, harnessing the bizarre properties of quantum mechanics, are rapidly evolving. While still in their early stages, these machines have the potential to crack the encryption methods currently used to secure our online world. This vulnerability could have far-reaching consequences, jeopardizing everything from online banking and financial transactions to secure communication and national security.

This is where Quantum-Resistant Cryptography (QRC) comes in. It's a new generation of encryption algorithms designed to withstand the onslaught of quantum computers. These algorithms rely on complex mathematical problems that are believed to be difficult, if not impossible, for even the most powerful quantum machines to solve.

Why is Quantum Computing a Threat?

Traditional public-key cryptography relies on mathematical problems like factoring large numbers or finding discrete logarithms. These problems are computationally expensive for classical computers, making it impractical to break the encryption within a reasonable timeframe.

However, quantum computers operate on the principles of superposition and entanglement, allowing them to perform certain calculations much faster than classical computers. This speed advantage makes them a potential threat to current encryption methods. Researchers believe that a sufficiently powerful quantum computer could break widely used encryption algorithms like RSA and Elliptic Curve Cryptography (ECC) in a matter of hours.

The Race for Quantum-Resistant Solutions

The need for QRC is becoming increasingly urgent as quantum computing continues to advance.

Several promising QRC approaches are being explored. Some rely on lattice-based cryptography, which utilizes the properties of mathematical lattices – arrangements of points in a multidimensional space. Others focus on code-based cryptography, which uses error-correcting codes to create complex encryption schemes. Additionally, there's multivariate cryptography, which involves solving complex systems of equations with multiple variables.

Challenges and the Road Ahead

Developing and deploying QRC does not come without its challenges. These new algorithms can be computationally more expensive compared to existing ones, potentially impacting processing speed. Additionally, transitioning existing infrastructure to entirely new cryptographic systems will be a complex and time-consuming process.
Standardization is also crucial. Different QRC algorithms offer varying levels of security and performance. Selecting and adopting a single, robust standard will be essential for ensuring widespread adoption and interoperability.
Despite the challenges, the development of QRC is critical for the future of the internet. Governments, businesses and individuals all depend on secure communications and data storage. Implementing QRC now will ensure we stay ahead of the quantum threat when it materializes.

What You Can Do

While the technical aspects of QRC are complex, there are steps individuals and organizations can take to prepare for the transition:

- **Stay informed:** Keep yourself updated on the latest developments in quantum computing and QRC.
- **Invest in future-proof solutions:** Look for products and services that are already incorporating or planning to incorporate QRC.
- **Support standardization efforts:** Advocate for the adoption of robust and widely accepted QRC standards.

Deepfakes

Complied by:- Ayush Siloiya
CS (4th Year Student)

What are Deepfakes?
For those unfamiliar, deepfakes are AI-generated content that convincingly mimic real human voices and appearances. Unfortunately, these tools are being misused by scammers to manipulate and deceive individuals.

The Reality of Deepfake Scams:
Reports of deepfake scams are on the rise, and many unsuspecting individuals have fallen victim to sophisticated impersonations. It's more crucial than ever to stay vigilant and informed.

How to Protect Yourself:
1. Verify Unusual Requests: Be skeptical of unexpected requests, especially those urging quick action. Verify the identity of the person through alternative means.

2. Enable Two-Factor Authentication (2FA): Strengthen your account security by enabling 2FA. This adds an extra layer of protection, making it harder for scammers to gain unauthorized access.

3. Educate Yourself and Your Network: Stay informed about the latest deepfake techniques and educate your network. Awareness is a powerful defense.

4. Use Trusted Communication Channels: Stick to verified communication channels when dealing with sensitive information. Avoid sharing personal details through unfamiliar platforms.

5. Report Suspicious Activity: If you encounter a potential deepfake or suspicious behavior, report it promptly. We can collectively contribute to a safer online environment.

6. Stay Informed: Keep yourself updated about the latest developments in deep fake technology and its potential implications.

7. Verify Sources: Verify the authenticity of media content by cross-referencing with multiple trusted sources.

8.Use Trusted Platforms: Prefer using reputable platforms and websites for consuming news and media content.

9.Educate Yourself: Educate yourself about the characteristics of deep fakes, such as realistic facial expressions, lip-syncing, and voice mimicking.

10. Use Watermarking and Digital Signatures: Content creators and distributors can use digital watermarking and signatures to authenticate their media content.

11. Use AI-Based Detection Tools: Leverage AI-based tools and software designed to detect and analyze deep fake content.

12. Promote Media Literacy: Encourage media literacy programs and initiatives that educate individuals, communities, and organizations about deep fakes and their impact.

13. Critical Thinking: Develop critical thinking skills to analyze media content critically. Question the context, timing, and authenticity of videos or images that seem suspicious.

What Real Hacking Looks Like !

Complied by:- Ramit Gangwar
CSE (2nd Year Student)

Introduction:
The reality of hacking is way different from how it is depicted in movies and television shows. You might have seen in movies that hackers gain access to secure systems within seconds by rapidly typing on their keyboards. Many movies depict hacking through flashy graphical user interfaces, with a big "ACCESS GRANTED" flashing on the screen. We all know it's not the truth and we watch it for dramas and have fun, but we all have wondered once how it might exactly look in real life.

Understanding Hacking:
At its core, hacking involves a deep curiosity about how systems work and finding ways to manipulate these systems. These ways are termed as vulnerabilities or bugs . When we talk about websites and how they work, there are two main parts involved: the server and the client. The server is like a big library that stores the website and all the information it contains, whereas the client is more like a visitor to that library. In general, clients send requests to the server to fetch the contents of the website. A certain logic is written by programmers on the server to handle these requests and return information based on them.

Hackers constantly search for bugs like these, which are very common even in big MNCs like Google(yes, you heard it right). Bugs like IDOR can lead to data leaks, and you hear news like the xyz website was hacked and 22 million user details were leaked, whereas some bugs can even manipulate servers doing tasks of our own, which means we can takeover the whole server. These bugs are harder to find and exploit. Bugs can be both very simple and very complex, depending on the application logic on the server.

Clarifying Misconceptions:
Hacking is always illegal, hacking requires a lot of technical skills and hacking a website is instantaneous. Hacking involves a diverse range of skills, motivations, and methodologies, reflecting both ethical and malicious intentions. Hacking is the art and science of exploring and manipulating computer systems, networks, and software to achieve specific goals.

Ethical hackers, also known as white hat hackers, use their skills for constructive purposes, such as identifying vulnerabilities in systems to improve security. They often work as cybersecurity professionals, penetration testers, or consultants, helping organizations strengthen their defenses against cyber threats.

Ethical hacking involves a systematic approach that includes reconnaissance, scanning, exploitation, and post-exploitation phases. Hackers begin by gathering information about the target, including its infrastructure, software versions, and potential entry points. This phase, known as reconnaissance or information gathering, may involve passive techniques like OSINT (Open-Source Intelligence) gathering or active scanning to identify live hosts and services.

The exploitation phase is where ethical hackers demonstrate their technical prowess by exploiting identified vulnerabilities to gain unauthorized access or execute specific actions within the target system. This may involve leveraging known exploits, developing custom scripts, or conducting social engineering attacks to trick users into revealing sensitive information or granting access.

Post-exploitation activities focus on maintaining access, escalating privileges, and conducting further reconnaissance within the compromised environment. Ethical hackers aim to simulate real-world cyber threats and provide actionable recommendations to mitigate risks and enhance security posture.

Their motives range from financial gain, espionage, activism, to sheer vandalism. Black hat hackers often operate in clandestine networks, selling stolen data, launching cyberattacks for ransom, or disrupting critical infrastructure.

LockBit vs FBI - A High-Stakes Cyber Showdown: Case Study

Complied by:- Indu Shekhar Pandey
Coordinator CPC

LockBit's evolution:

LockBit 1.0 (Early 2020):

Initial Access: Exploited vulnerabilities like EternalBlue (SMBv1 vulnerability) or
CVE-2017-0144 (Microsoft Office RTF vulnerability) to gain initial access to victim networks.

Lateral Movement: Utilised tools like PowerShell Empire, a post-exploitation framework, for privilege escalation and lateral movement within the compromised network. Empire leverages PowerShell scripting for these activities, making it difficult to detect as it utilises legitimate functionalities.

Encryption: Employed robust encryption algorithms like AES-256 in CBC mode with a Random Initialization Vector (RIV) to encrypt victim data, rendering it inaccessible without the decryption key.

LockBit 2.0 (2021):
Data Exfiltration: Introduced "StealBit" a custom data-stealing tool written in a language like C++ or Go for increased efficiency. StealBit might target specific file types containing sensitive information and exfiltrate them to the attacker's controlled server before encryption, adding pressure through "double extortion".

LockBit 3.0 (Late 2022): Modularity: Embraced a modular design, allowing affiliates to customise the ransomware at compile time.

Anti-Analysis Techniques: Likely employs advanced anti-analysis techniques like code obfuscation (packing, encryption) and anti-debugging measures (detecting debuggers and terminating processes) to impede investigation and potential decryption efforts. These techniques make reverse engineering the malware more challenging.

Living-off-the-Land (LoLbins): May utilise legitimate system administration tools (LOLbins) for malicious purposes. These tools can be used for tasks like privilege escalation, lateral movement, or persistence within the victim network, making detection more challenging as they appear as legitimate processes. The LockBit Threat Landscape: LockBit primarily targets vulnerable systems through various attack vectors:

Remote Desktop Protocol (RDP) Exploits: LockBit exploits weak RDP configurations and brute-force attacks against RDP passwords to gain initial access. They may also target vulnerabilities in RDP itself.

Phishing Campaigns: They may deploy phishing emails containing malicious attachments (e.g., weaponized Microsoft Office documents) or links to download LockBit payloads disguised as legitimate files. Supply Chain Attacks: Compromising legitimate software vendors or service providers can provide LockBit with a wider attack surface and access to potentially more trusted systems within a victim's network.

Social Engineering: Beyond phishing emails, LockBit may incorporate social engineering tactics like exploiting human vulnerabilities through phone calls or impersonating IT personnel to gain access or bypass security measures.

Reverse engineering: Reverse engineering is the process of deconstructing a product, system, or software to understand its inner workings, design principles, and functionality. It involves analyzing the product's components, structure, and behavior to gain insights into how it operates or is constructed.

Feature	LockBit 1.0	LockBit 2.0	LockBit 3.0
Initial Access	Vulnerabilities (e.g., EternalBlue)	Vulnerabilities (e.g., EternalBlue)	Vulnerabilities (unknown)
Lateral Movement	PowerShell Empire	PowerShell Empire	Likely similar
Data Encryption	AES-256 (CBC)	AES-256 (CBC)	Likely various options
Data Exfiltration	No	StealBit tool	Likely similar
Command and Control (C2)	HTTP/HTTPS	HTTP/HTTPS	Likely more sophisticated (custom protocols)

Table 1. Differences in LockBit variants.

FBI Inclusion:

The battle between LockBit and the FBI is a prime example of the ongoing struggle against cybercrime. Below is the timeline of acts between them:

1. **The FBI Sets the Trap (Early 2021):** The FBI, aware of LockBit's growing threat, initiates a multi-pronged operation. Working in the shadows, they gather intelligence and devise strategies to disrupt LockBit's infrastructure, finances, and communication channels. This is a slow and meticulous process, building a case against the cybercriminals.

2. Introduction of LockBit 3.0 (June 2022): LockBit unveils their latest weapon - LockBit 3.0, a more sophisticated ransomware variant. They aim to show their dominance by offering bizarre rewards - financial incentives for individuals who get LockBit tattoos and post pictures online. This audacious move highlights the group's recklessness.

3. The Ransomware Strike on Fulton County (January 2024): LockBit launches a successful ransomware attack on Fulton County, Georgia. Sensitive data is potentially compromised, throwing the county into chaos. This attack serves as a wake-up call, prompting the FBI to accelerate their plans.

Extortion operations. Additionally, indictments are unsealed against some LockBit affiliates, aiming to hold individuals accountable. News of the operation surfaces, and LockBit's websites disappear.

Conclusion:

The Future: An Unending Battle: The LockBit vs FBI saga highlights the evolving nature of cybercrime. While Operation Cronos dealt LockBit a blow, it's uncertain if their resilience is broken. The FBI's fight against ransomware requires constant vigilance, international cooperation, and innovative strategies. This is a battle that will likely continue for the foreseeable future.

Resilience of Cybercriminals: Despite law enforcement operations and disruptions, cybercriminals often adapt and evolve their tactics. This resilience is fueled by the lucrative nature of cybercrime, where ransomware attacks can yield substantial profits.

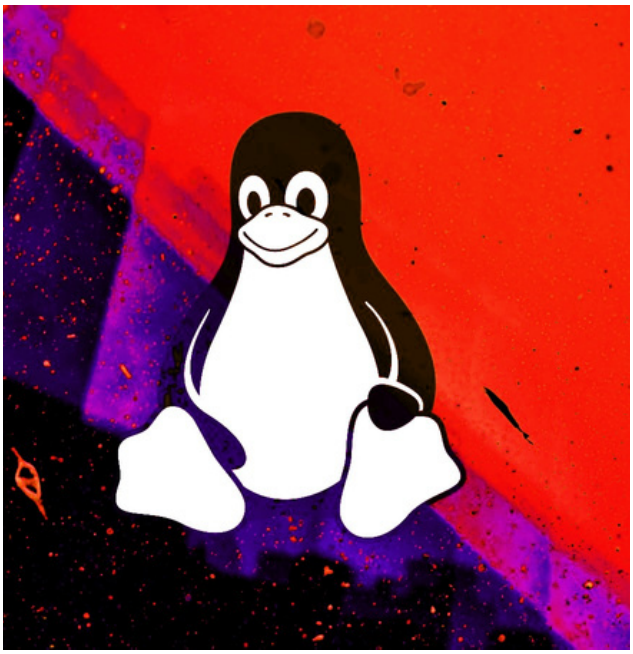
Technological Sophistication: Cybercriminals continually enhance their techniques and tools, leveraging advanced encryption and anonymity networks.

CYBERBYTES

Secret Backdoor Found in XZ Utils Library, Impacts Major Linux Distros

On Friday, Red Hat issued an urgent security alert regarding two compromised versions of XZ Utils, previously known as LZMA Utils. Versions 5.6.0 (Feb 24) and 5.6.1 (Mar 9) contain malicious code allowing unauthorized remote access. This software supply chain compromise, labeled CVE-2024-3094 with a critical CVSS score of 10.0, poses a severe threat. The exploit involves a sophisticated attack where liblzma extracts a prebuilt object file from a disguised test file within the source code, altering specific functions. This results in a modified liblzma library used by linked software, intercepting and modifying data interaction. The embedded code aims to disrupt sshd daemon processes for SSH via systemd, potentially compromising authentication. Discovered by Microsoft's Andres Freund, the code was traced to commits by 'JiaT75' on GitHub. GitHub disabled the repository due to terms of service violations. Fedora 41 and Rawhide are affected, prompting CISA to recommend downgrading to XZ Utils 5.4.6 Stable.

Source: TheHackerNews



Hackers Hit Indian Defense, Energy Sectors with Malware Posing as Air Force Invite

Indian government entities and energy firms are under severe cyber threat from unknown actors distributing a modified HackBrowserData malware variant. Using Slack for command-and-control (C2), attackers employed phishing emails disguised as Indian Air Force invitations. Dubbed "Operation FlightNight" by Dutch cybersecurity experts since March 7, 2024, the campaign targeted sectors like electronic communications, IT governance, and national defense. Private energy companies were breached, resulting in theft of financial records, employee details, and oil and gas operation data, totaling 8.81 GB of exfiltrated data. The malware, hidden in phishing emails as "invite.iso," executed "scholar.exe" via a Windows LNK shortcut from mounted ISO files. This variant of HackBrowserData includes document siphoning, Slack communication, and improved evasion techniques. xelemental's January 2024 findings revealed similarities to the GoStealer campaign, indicating a concerning trend of threat actors exploiting open-source tools like Slack for cyber espionage. Büyükkaya emphasized the evolving cyber threat landscape and actors' use of available offensive tools.

Source: Security Week's Newsletter

CYBERBYTES

Over 39,000 WordPress Sites Compromised by Extensive Sign1 Campaign with Scam Redirects

The Sign1 malware campaign has compromised 39,000+ WordPress websites, using JavaScript injections to redirect users to fraudulent sites. A recent variant infected 2,500+ sites in the last two months alone, per Sucuri. Attackers inject rogue JavaScript into legitimate plugins and widgets, executing remote files for redirection through a VexTrio-operated traffic system. The malware employs time-based randomization for dynamic URL fetching every 10 minutes, with domains registered just prior to use. Notably, it checks visitor origins from major websites before executing, redirecting them to scams via additional JavaScript. Suspected entry points include brute-force attacks or exploiting vulnerabilities in plugins and themes, keeping the malware undetected.

Source: SANS

Fresh Wave of StrelaStealer Phishing Strikes 100+ Organizations Across E.U. and U.S

Cybersecurity researchers have detected a new phishing attack leveraging the StrelaStealer, affecting 100+ organizations in the EU and US. These campaigns employ spam emails with evolving attachments to deploy the StrelaStealer's DLL payload, aiming to steal email login data. Initially disclosed in November 2022, StrelaStealer targets various sectors, with recent campaigns in November 2023 and January 2024. The attacks have evolved to introduce improved obfuscation and anti-analysis techniques. Additionally, Symantec has flagged fake software installers hosting the Stealc malware on GitHub, Mega, and Dropbox. Phishing efforts have also been observed delivering Revenge RAT and Remcos RAT, posing significant cybersecurity threats.

Source : SANS

Tech giant Fujitsu says it was hacked, warns of data breach

Multinational tech giant Fujitsu confirmed a cyberattack, warning of potential personal data and customer information theft. Malware was found on numerous work computers, leading to the discovery of illegally accessible files, the company stated in a translated Japanese announcement. Affected systems were promptly disconnected from the network, and investigations are underway regarding the malware's entry and potential data leaks. Fujitsu did not disclose the specific malware used or the nature of the attack. The company, with about 124,000 employees, serves global government and private sector clients. The incident was reported to Japan's Personal Information Protection Commission, anticipating stolen personal data.

Source: Naked Security

Hundreds of Thousands of Systems Affected by New 'Loop DoS' Attack

A newly discovered denial-of-service (DoS) attack method, known as Loop DoS attacks, targets User Datagram Protocol (UDP)-based application-layer protocols, posing a significant risk to hundreds of thousands of hosts. Researchers from the CISPA Helmholtz-Center for Information Security described the approach as pairing servers to endlessly communicate, exploiting UDP's lack of source IP address validation, leaving it vulnerable to IP spoofing. This results in a reflected DoS attack, with certain UDP implementations like DNS, NTP, TFTP, and others being weaponized. Once triggered, these paired servers generate immense traffic, rendering involved systems or networks unresponsive. Approximately 300,000 hosts and networks are potentially exploitable, with affected products from Broadcom, Cisco, Honeywell, Microsoft, MikroTik, and Zyxel. Though not yet observed in the wild.

Source : WeLiveSecurity

New "GoFetch" Vulnerability in Apple M-Series Chips Leaks Secret Encryption Keys

A new "GoFetch" vulnerability in Apple M-series chips enables the extraction of secret encryption keys through a microarchitectural side-channel attack. Exploiting the Data Memory-Dependent Prefetcher (DMP), the flaw targets constant-time cryptographic implementations to access sensitive CPU cache data. Discovered in December 2023, the attack manipulates prefetchers, which predict program memory access, by leaking data speculatively. This bypasses constant-time programming restrictions, posing significant security risks. While unfixable in current Apple CPUs, developers can mitigate by adjusting cryptographic libraries, possibly impacting performance. Enabling Data-Independent Timing (DIT) on M3 chips thwarts the attack, not available on M1 and M2 models.

Source: The Hacker News

GLIMPSES

NULL Meetup Delhi 2024

The first Null Delhi Meetup of 2024 was held on 6th January 2024. Our club members Jhalak Jain, Shambhavi, Indu Shekhar Pandey, Suryansh Deshwal, Rohit Gangwar, and Yatharth Singh attended this meetup where they gained knowledge realated to software devleopment trends in cybersecurity and new valuable insights.

BREACHVERSE : An Ethical Hacking Workshop

An ethical hacking workshop was organized by Cyber Peace Centre, KIET Group of Institutions, Ghaziabad on 8th-9th January 2024 in which 40 students participated and gained knowledge about the cutting-edge cybersecurity tools such as Wireshark, Burp Suite etc.

CRACCON Conference

CRACCON organized a conference on 27th-28th January 2024, at the Indian International Centre, Delhi, where our club members, Indu Shekhar Pandey and Aryan Sharma attended it as volunteers. They interacted with CISOs and leaders from industries like IOCL, KPMG, HPCL, and Nokia who were part of the CXO Panel.

RECKON-5.0 , JIET Jodhpur

RECKON 5.0 is a 24 hours long hackathon where participants build something uniqueto solve problems from various spheres of modern human life.On 17th-18th Feburary 2024, our club members Aditya Aggarawal, Soumya Gupta and Kanishk Joshi participated in this hackathon and secured first position and cash prize worth Rs.70,000.

GLIMPSES

Understanding Networking Basics Session

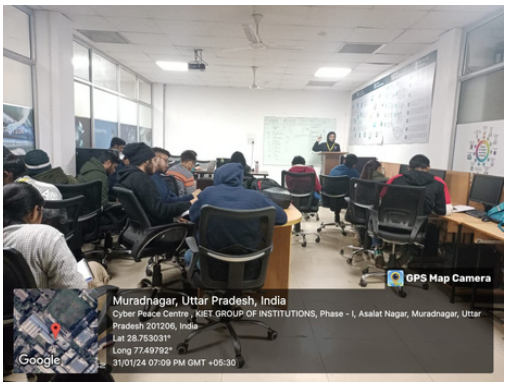
Dr. Arun Kumar Tripathi, faculty coordinator at CPC, conducted an enlightening session on networking basics. Our club members gained valuable insights and practical knowledge about networking fundamentals such as IP address, networking devices etc. His expertise and experience enriched the session, providing attendees with a solid understanding of networking concepts and enhancing their fundamental knowledge.

Expert Sessions

The monthly expert sessions at the Cyber Peace Centre, KIET Group of Institutions offer valuable insights into cybersecurity. These sessions feature industry experts sharing cutting-edge knowledge, best practices, and latest trends. Participants gain practical skills and stay updated with cybersecurity developments, enhancing their expertise and contributing to a safer digital environment.

Mentor Session

In the mentor session led by Mr. Kartikeya Srivastava, former President of CPC & 4th Year student of KIET CSE branch, students gained firsthand insights into real-world applications of cybersecurity. His experience offers invaluable lessons on tackling cyber threats effectively, navigating challenges, and implementing strategies for robust cybersecurity practices.



Regular Classes

Cyber Peace Centre conducts regular cybersecurity classes, providing comprehensive education on cyber threats, defense strategies and best practices. These classes cover a range of topics such as malware analysis, network security, ethical hacking and data protection, equipping students with essential skills for cybersecurity roles in the industry.