Cyber Security Challenges of Modern Days

Safeguard oneself by staying informed about state-of-the-art cyber-security challenges

Edited by **MOHAN DAS VISWAM**

Cyber-security landscape is becoming increasingly complex, driven by sophisticated cyber threats, increased regulation, and rapidly evolving technology. Organizations will be challenged with protecting sensitive information of their users while continuing to provide seamless and easy user experiences. Here's a closer look at emerging challenges and threats set to shape this year.

AI-Driven Social Engineering Threats

With the advancement of AI, algorithms based on Natural Language Processing (NLP) and Machine Learning (ML) are being used to automate cyber-attacks by creating highly convincing phishing campaigns and producing DeepFakes for Social Engineering. AI can generate messages that seem more authentic, targeted, and convincing by analyzing social media profiles, online interactions, and leaked data. Threat actors can easily create convincing audio and video DeepFakes that impersonate company executives to deceive employees for transferring funds or disclosing sensitive credentials. AI can automate large-scale social engineering campaigns by generating numerous and unique targeted messages, responses, or scenarios thereby increasing the volume of attacks while reducing the need for manual effort.

Misconfigurations in Digital Infrastructure

Misconfigurations of cloud environments such as missing access controls, unsecured storage locations and inefficient implementation of security policies form the most frequent reasons for data breaches. Improper configurations enable attackers to hijack cloud resources for malicious activities such as crypto currency mining and launching cyber-attacks from compromised cloud accounts by masking their identity. Weak or overly permissive access management policies can allow users or third parties to access critical cloud resources without proper verification, thereby providing a path for attackers to exploit these privileges. Cloud services may expose APIs that are not secured or are given excessive permissions, making it easier for attackers to exploit them and gain unauthorized access to cloud resources.

R Bindu Madhavi
Scientist - D
r.bindumadhavi@nic.in

A RamaDevi
Scientist - D
rama.a@nic.in

Cyber threats are evolving at breakneck speed as adversaries become more sophisticated and the number of connected devices worldwide continues to rise, with remote work and cloud adoption increasing, endpoints and data flows become attractive attack targets. In this article, we explored the latest cyber security trends affecting global organizations and being informed can decrease your risk profile.

Mobile Device Exploits

With increasing reliance on mobile devices, attacks on these platforms are expected to rise substantially in the days to come. This includes exploiting vulnerabilities in mobile operating systems, mobile apps, and mobile-centric technologies, like 5G. Mobile malware has seen significant growth, and this trend is expected to continue as mobile devices are increasingly used for banking, shopping, and accessing sensitive information. Combined with a compromised key, the attackers can downgrade a secure HTTPS connection to an unencrypted HTTP connection in a man-in-the-middle attack, enabling them to steal sensitive information (like passwords and credit card numbers) as it is transmitted over the network. Jailbroken (iOS) or rooted (Android) mobile devices enable attackers to install unauthorized apps or software and thus open-up the device to various attacks.

IoT Device Vulnerabilities

IoT devices are often found to lack robust security, making them easy targets for attackers seeking to hijack devices for botnets or other malicious purposes. IoT devices such as smart cameras and wearables collect personal data. If compromised, these devices can expose sensitive information or be used for surveillance. IoT devices frequently rely on weak encryption or unsecured communication protocols, making them vulnerable to interception and exploitation. Compromised IoT devices are frequently used in large-scale botnet attacks like DDoS attacks that overwhelm networks and servers. Attackers may hijack IoT devices to use their processing power for mining cryptocurrency without the user's knowledge. Devices like smart refrigerators, cameras, and even medical devices with computational power can be exploited to mine crypto, thereby causing system slowdowns, hardware damage, and increased power consumption.

Insider Threats

As businesses become increasingly digital and interconnected, the threat posed by insiders - individuals within the organization who has access to systems and data - remains a significant concern. Employees might inadvertently expose sensitive information by sending eMails to the wrong recipients, misconfiguring cloud settings, or failing to use secure communication methods. Disgruntled employees may deliberately sabotage company systems, steal data, or disrupt operations if they feel mistreated or dissatisfied with their employer. Contractors and vendors,

who are not subject to the same security protocols as permanent employees, can be a weak link. Employees working remotely or using personal devices (BYOD) may inadvertently expose the company network to malicious software or attackers if their devices and access are not secured properly. Remote employees may access systems from insecure networks, making it easier for unauthorized individuals to intercept data or gain access to corporate resources.

Encryption-Less Ransomware Attacks

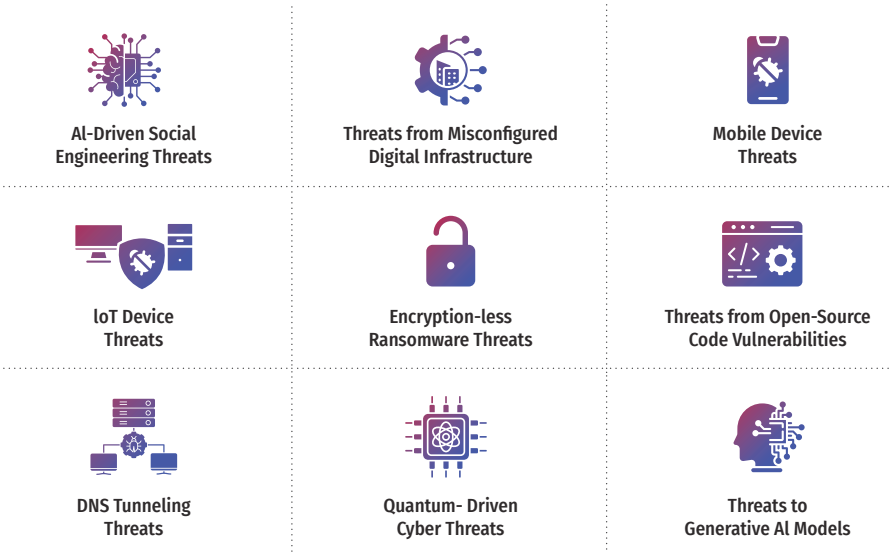
Encryption-Less ransomware attacks represent a new and evolving threat where attackers extort victims without relying on the traditional method of encrypting files. Instead of locking data and demanding a ransom for decryption keys, these attacks typically involve the theft of sensitive information or the disruption of systems in ways that cause less immediate operational disruption. The attackers thus operate undetected for longer periods gathering sensitive information and then threaten to publish it unless a ransom is paid. Even though the data is not encrypted, the consequences can still be severe, as they target critical business assets and compromise privacy. Attackers are becoming increasingly sophisticated in their methods of data exfiltration by deploying tools like remote access Trojans (RATs) or file less malware to steal data without triggering traditional detection systems. 'Ransomware-as-a-Service' models which enables even less skilled attackers to launch devastating ransomware campaigns is another security challenge which is on the rise in modern days.

DNS Tunneling Threats

Domain Name Service (DNS) traffic often has the privilege of traveling freely across network perimeters to ensure smooth functioning of the network communication. Threat actors explore this privilege to exploit DNS traffic to achieve their malicious goals. DNS tunneling is one such cyber attack technique where malicious actors abuse the DNS protocol to create a covert communication channel for data exfiltration or command and control. Instead of using DNS for its intended purpose, the attackers embed data or commands within DNS queries and responses. This allows them to bypass network security measures and communicate with compromised systems without raising red flags. DNS Tunneling can be detected by inspecting payloads, monitoring DNS queries for unusual patterns and conducting deep packet inspection to identify signs of data encoding. Other preventive measures include regularly monitoring DNS traffic, implementing DNS Security Extensions, enforcing firewall rules to block DNS traffic to unauthorized servers, and limiting unnecessary DNS queries.

Quantum Driven Threats

As the world advances towards the era of quantum computing, the security landscape is undergoing a significant shift. The arrival of quantum computing technology has the potential to disrupt existing cryptographic systems and render current security measures obsolete. Preparing for quantum-driven threats will become essential as quantum computers evolve and their capabilities materialize, particularly for the cybersecurity community. Quantum computers have the potential to break widely used public-key cryptography algorithms as well as to disrupt symmetric-key cryptography. Modern algorithms allow quantum computers to search unsorted databases (or brute-force encryption keys) faster than classical computers. This would reduce the security of encryption by effectively halving the key length, making systems that use 128-bit keys as vulnerable as 64-bit keys are today



▲ Fig 12.1 **Evolving cyber Threats**

Open-Source Code Vulnerabilities

Open-source code has become a fundamental building block for modern software development, enabling developers to leverage existing tools, frameworks, and libraries to expedite their projects. It offers numerous benefits such as reducing development time, increasing collaboration, and promoting innovation. However, while open-source software provides these advantages, it also introduces potential risks that organizations and developers must be aware of. Malicious contributors or attackers could introduce backdoors into open-source projects, which could later be exploited to gain unauthorized access to systems or steal sensitive data. These backdoors can be hidden within seemingly benign parts of the code, making them difficult to detect. Open-source projects are often developed and maintained by volunteers or small teams, which may lack comprehensive security testing. Inadvertent License Violations, License Conflicts, Lack of Vendor Support, Lack of Accountability in Vulnerability Disclosure, Abandoned Projects, Poor Documentation, etc.make the issue all the more complex.

Threats to Generative AI Models

As organizations integrate GenAI into their operations, they expand their attack surface. GenAI models process and generate data that could inadvertently contain sensitive information. Inaccurate, biased, or compromised data used in training these models can lead to data leaks or privacy violations. GenAI systems are not immune to adversarial attacks, where attackers manipulate input data in a way that causes the AI model to behave unpredictably or generate malicious outputs. Attackers may attempt to reverse-engineer or steal proprietary GenAI models, gaining access to intellectual property and insights that could be exploited for malicious purposes. This could lead to intellectual property theft or the illicit use of trade secrets.

Conclusion

These predictions for the future period will demand a heightened focus on proactive defense strategies. Organizations must focus on improving baseline cybersecurity posture by increasingly adhering to related regulations. They must prioritize a zero-trust architecture, harness the power of AI-powered security controls, and foster a culture of security awareness among the stake holders to overcome these threats.

Contact for more details

State Informatics Officer
NIC, TamilNadu State Centre
E2-A, Rajaji Bhavan, Besant Nagar
Chennai, Tamil Nadu – 600090
Email: sio.tn@nic.in , Phone: 044-44992425