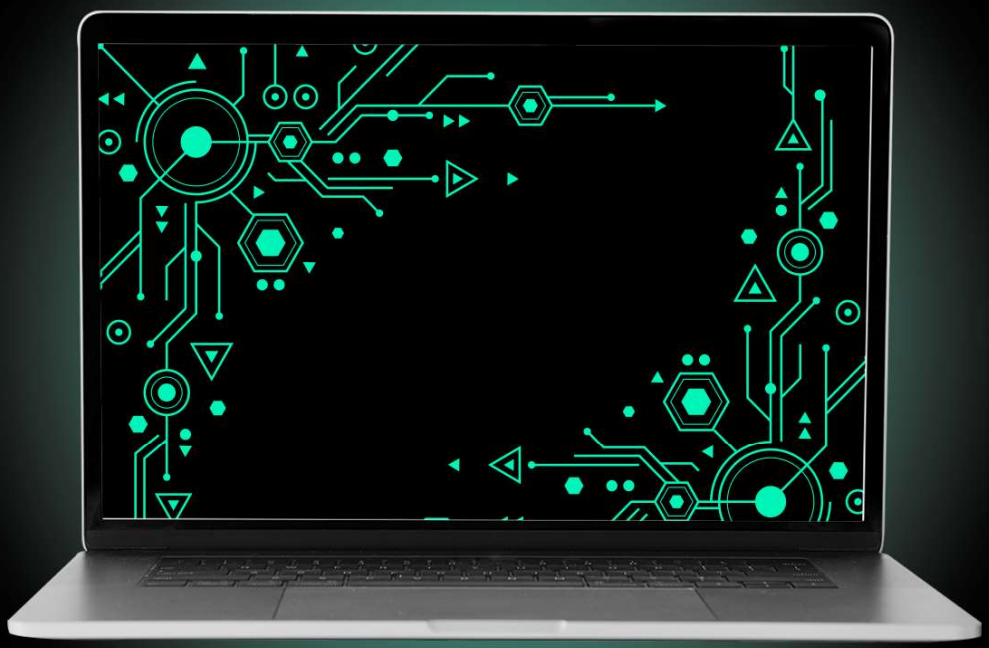
CENTRAL TRAINING COLLEGE

TELECOM & INFORMATION TECHNOLOGY

March 2025

e-Newsletter



@ctctitranchi CTC(T&IT)_CRPF_RANCHI ctctitcrpfranchi

INDEX

Chief Patron

Sh. Harjinder Singh, DIGP,Principal

Editorial Advisory Board cum R&D Team Chairman

Sh. Brijish Kumar Dubey, Dy. Comdt,Vice Principle

Members

Sh. Aman Deep , Dy. Comdt.
Insp/C Praveen Sagar
Insp/T Harish Prasad
Insp/RO Ramdas K B
Insp/T Biju S T
Insp/RO N.Anil
SI/T Virender Bisht
ASI/T Saneesh S
ASI/Ro Satender Singh Suhag
HC/RO Pradeep Kumar Singh

Editor

Smt. Gauri Singh, Asst. Comdt
Sh. Vinod Kumar Choudhary, Asst. Comdt

Proof Reader

Insp/RO K.B Ramdas
Insp/RO Vijay Kumar Sharma

Designing & Layout

SI/T Rajesh Kumar Rajput
ASI/T Deepak

Photography

Precis Cell

Contents

1. CYBER THREAT TRENDS
2. MAYA OPERATING SYSTEM

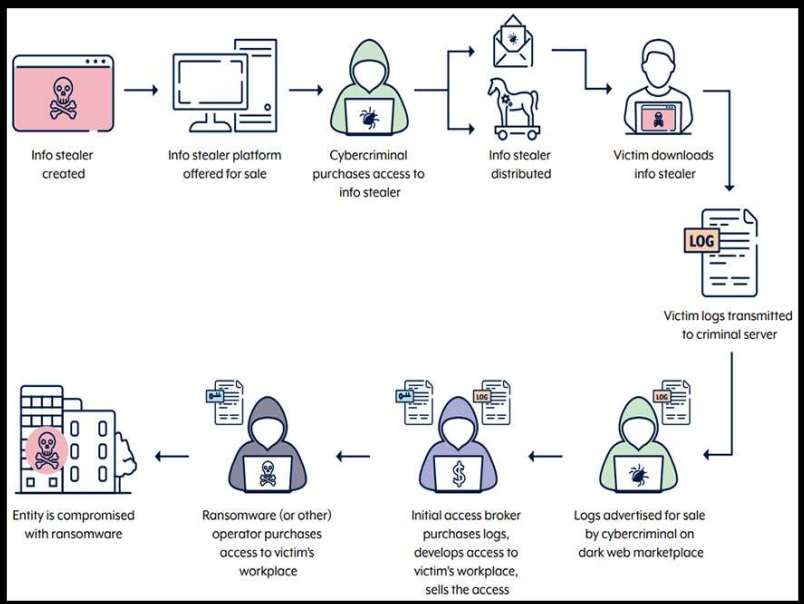
Published by:-
CTC(T&IT),RANCHI

Cyber Threat Trends

Threat #1
Information Stealers

First identified around 2020, Redline has the capability to steal various types of personal information from an infected computer, including stored passwords from browsers, credit card information, cryptocurrency wallets, VPN login credentials, FTP logins, cookies and session data, and more. It's typically delivered via email and malvertising campaigns, either directly or via exploit kits and loader malware; recent research suggests that some cybercriminal groups are targeting the gaming community, leveraging fake Web3 gaming lures to deliver malware capable of stealing sensitive information from macOS and Windows users.





What is Information Stealers ?

Information stealers are malicious programs designed to collect various kinds of personal and financial information from an infected system. They can capture keystrokes, extract files,steal browser data like passwords and cookies, and more. Information stealers generate large amounts of DNS traffic,given that the threat exfiltrates data from compromised organization.

Cyber Threat Trends

Threat #3
Ransomware

Lockbit is one of the more active ransomware variants today; its ransomware operations accounted for over 25 percent of the total number of posts made to data leak sites. In February 2024, multi-agency international law enforcement task force managed to disrupt LockBit operations. However the group managed to quickly resume operations, utilizing new servers and encryptors.

Ransomware activity jumped in January and stayed high for the rest of the observed time frame. The trends seen in ransomware closely shadow the trends seen in the dropper category, suggesting a correlation between the two. It's likely that the droppers we're seeing are being used to seed ransomware payloads. Ransomware remains a prevalent threat as it directly monetizes attacks by holding data or systems hostage for ransom. It's high profitability, coupled with the increasing availability of ransomware-as-a-service platforms, allows even less skilled attackers to launch campaigns. Organizations' often inadequate backup and recovery processes, and the willingness of many to pay the ransom, perpetuate the cycle of attacks.

Ransomware?

Ransomware is a type of malware that encrypts the files on a victim's computer or network, making them inaccessible, and demands a ransom payment to decrypt them. Victims are often threatened with permanent loss of data or exposure of stolen data if the ransom isn't paid.

Cyber Threat Trends

Threat #4
RAT (Remote Access Trojans)

As early as 2009, a RAT known as Gh0st RAT was used in targeted attacks. It's known for its stealthiness and for being difficult to detect. It allows attackers to take full control over the infected device and has been used in espionage campaigns. Cisco Talos Threat Intelligence noted that this threat has evolved, citing a malicious campaign that likely started as early as August 2023, delivering a new RAT dubbed "SugarGh0st", with evidence suggesting the threat actor is targeting the Uzbekistan Ministry of Foreign Affairs and users in South



What is a Remote Access Trojan?

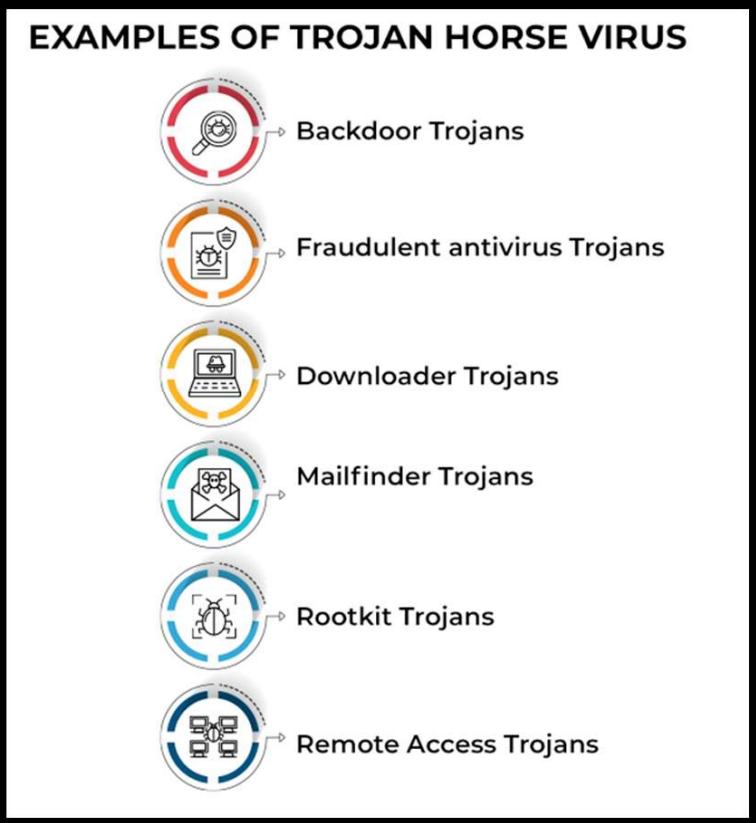
RATs are a type of malware that provide a backdoor for administrative control over the targeted computer. RATs enable intruders to do almost anything on the targeted computer,such as monitoring user behavior, accessing confidential information, activating the system'swebcam, and distributing more malware.

Cyber Threat Trends

Threat #2

Trojan

Qukbot is multifunctional and sophisticated Trojan with capabilities that include stealing banking credentials and other personal information, as well as providing a backdoor for attackers to install additional malware on infected systems. Over time, QakBot has envolved with various updates and improvements to its evasion and propogation techniques. It can propagate itself across networks by exploiting vulnerabilities and using brute force attacks on acccount credentials, allowing it to spread rapidly with in corporate networks.



Trojan

A Trojan horse is a type of malware that tricks users into installing malicious software that appears to be legitimate. Trojans are used by hackers and cybercriminals to gain access to users' systems.

"Maya Operating System"

India's Indigenous Shield for Strengthening India's Cyber Frontiers in Defense and Internal Security

Apple's founder, Steve Jobs, once stated that if a world war were to occur in the future, the true battleground would be the control of information. In other words, cyber warfare would become the most formidable weapon, capable of crippling an entire nation within hours by seizing control of its information systems.

Even today, our military, DRDO (Defense Research and Development Organization), ISRO (Indian Space Research Organization), electricity boards, water boards, banking systems, stock markets, and various government operations still rely on decades-old Windows Operating systems. A professional hacker can easily breach these systems within minutes.

Similarly, most of the surveillance cameras installed in these institutions are manufactured in China, which means China can collect and transfer India's sensitive data to its own country. This was a major security loophole in India's defense system, and it was crucial to address it.

In recent years, various ministries and agencies have been victims of multiple cyber-attacks. A 2019 cyber report mentioned that the Indian Army faces at least two cyber-attacks every month. Most of these attacks originate from neighboring countries, Pakistan and China. These cyber-attacks are not limited to defense organizations and ministries.

Last year, Solar Industries Limited India, a company involved in the production of explosives, became a victim of a ransomware attack. Similarly, last year, Central Depository Services Limited (CSDL) detected malware in some of its internal machines.

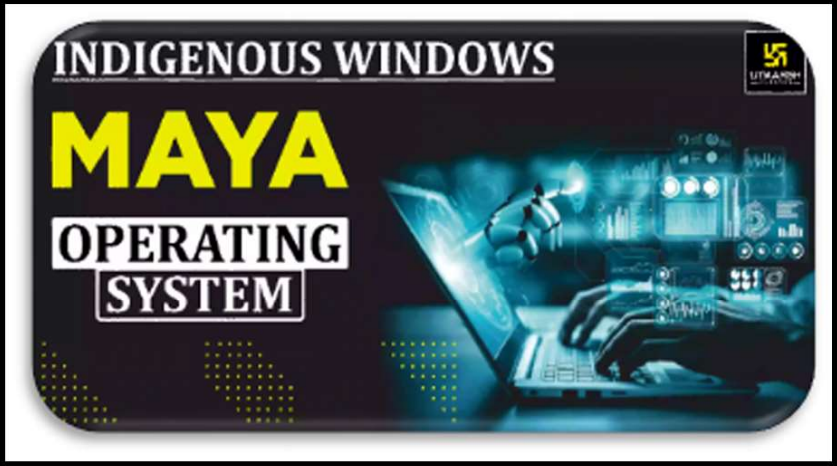


The Government of India has been working on cyber security at a war footing for the past several years. In this effort, new laws have been made for various social media companies. Now, considering the rising cases of cyber-attacks and the threat of data leaks, various Indian organizations and indigenous agencies made tireless efforts for months, resulting in the creation of an excellent operating system named Maya.

Maya OS is India's indigenous operating system, developed as a collaborative effort by the Defense Research and Development Organisation (DRDO), the Centre for Development of Advanced Computing (C-DAC), the National Informatics Centre (NIC), Indian software companies, and academic institutions. It is based on Ubuntu Linux and has many security features. Maya OS is designed to replace Windows, which is widely used on computers in India's Ministry of Defense.

The development of Maya OS began in 2021, and the Indian Ministry of Defence officially introduced it during August, 2023. It is gradually being implemented on all computers in the Ministry of Defense. It is expected that Maya OS will help protect India from cyber-attacks and strengthen national security

The name "Maya" is derived from the Sanskrit word for "illusion," reflecting the system's capability to provide deceptive layers of security, effectively cloaking the Defense Ministry's computers from potential cyber threats.



Some key security features of Maya OS are: -

- A built-in firewall that prevents hackers from entering the computer system.
- An antivirus and anti-malware software that protects the computer from malware.
- A rotational disk imaging system that regularly backs up the computer system, allowing data recovery in case of data loss.
- Maya OS has a feature called Chakravyuh, which is an endpoint anti-malware and antivirus software. It acts as a protective layer between users and the internet, preventing hackers from accessing sensitive data.

• Maya OS is optimized for Indian conditions and is available in multiple Indian languages. It is also an open-source operating system, meaning it can be freely downloaded and distributed.

The objective behind the development of Maya OS: -

1. The primary goal of Maya OS is to enhance the security of defense systems and data, reducing reliance on foreign software and promoting indigenous innovation.
2. The user interface of Maya OS is designed to resemble Microsoft Windows, facilitating a smoother transition for users accustomed to the Windows environment.
3. Maya OS is built upon the open-source Ubuntu Linux distribution, offering a user-friendly interface similar to Microsoft Windows to facilitate a seamless transition for users while maintaining high security standards. It supports commonly used applications like Microsoft Office, Adobe Photoshop, and AutoCAD, and incorporates advanced features such as cloud storage, encryption, digital signatures, and biometric authentication etc.
4. As of March 2025, Maya OS, India's indigenous operating system, has been successfully implemented across various branches of the Defense Ministry, including the Navy, Army, and Air Force. This transition aims to enhance cyber security and reduce dependence on foreign software.

The successful deployment of Maya OS marks a significant milestone in India's pursuit of technological self-reliance and cyber security enhancement.

CRPF: Fortifying Internal Security with Indigenous "Maya Operating System"

The Central Reserve Police Force is the backbone of India's internal security, tirelessly serving in some of the most challenging environments. Whether it is fighting Naxal insurgency, countering terrorism, tackling Maoist threats, restoring law and order, managing election duties, or operating in remote and sensitive areas, CRPF stands as a pillar of strength and resilience.



The Central Reserve Police Force is committed to adopting the latest technologies to ensure national security and sovereignty. Implementing the indigenous operating system Maya OS in the Central Reserve Police Force will not only enhance data security but also serve as a significant step towards digital self-reliance.

To enhance operational efficiency and cyber security, CRPF must adopt cutting-edge technology. One such initiative is the implementation of Maya OS, a Made-in-India operating system designed to safeguard sensitive data

Strategic Advantages of Adopting Maya Operating System in CRPF: -

1. Cyber security for Sensitive Operations:-

CRPF plays a vital role in counterinsurgency and anti-terror operations. The force collects and processes large amounts of intelligence data, operational plans, and communication records. Maya OS provides an advanced security layer that prevents cyber intrusions, hacking attempts, and data leaks, ensuring that critical mission data remains protected.and strengthen digital security.

3. Securing Communication in Remote Areas

CRPF operates in remote forests, hilly terrains, and conflict-prone regions where secure communication is crucial. Maya OS offers encrypted communication tools and secure data transmission, reducing the risk of external surveillance or cyber espionage.

3. Cost-Effective & Customizable Solution

Maya OS is an open-source and indigenous operating system, making it more cost-effective compared to expensive foreign software. It can also be customized according to CRPF's specific needs, integrating features like secure document handling, encrypted storage, and mission-specific applications.

4. Reliable Security for Election & Law Enforcement Duties

During elections, CRPF is deployed nationwide to maintain law and order. Officers use digital tools for tracking deployments, monitoring security situations, and reporting incidents in real-time. With Maya OS, CRPF can ensure that its election-related data and operations remain protected from cyber threats.

5. Digital Independence & Atmanirbhar Bharat

By adopting Maya OS, CRPF aligns with India's "Atmanirbhar Bharat" (Self-Reliant India) mission, reducing dependency on foreign software and promoting Made-in-India cybersecurity solutions. This move strengthens national security by preventing foreign governments or cybercriminals from accessing CRPF's crucial data.



Final Thoughts and Future Outlook

CRPF has always been at the forefront of safeguarding India's security, from Naxal-affected regions to election duties and counter-terrorism operations. In today's digital era, the force must also remain secure in cyberspace. The adoption of Maya OS will provide CRPF with a robust, secure, and indigenous alternative to foreign operating systems, ensuring mission-critical data remains protected.

By embracing Maya OS, CRPF will not just strengthen its cyber defense but will also reinforce its position as India's most resilient, self-reliant, and technologically advanced Paramilitary Force.

Source:- https://en.wikipedia.org/wiki/Maya_(operating_system), https://indianexpress.com/article/technology/tech-news-technology/maya-os-windows-replacement-defence-ministry-computers-8885509/