ERBIUM

A new malware called **Erbium** has been wreaking havoc on the internet for the last few months.

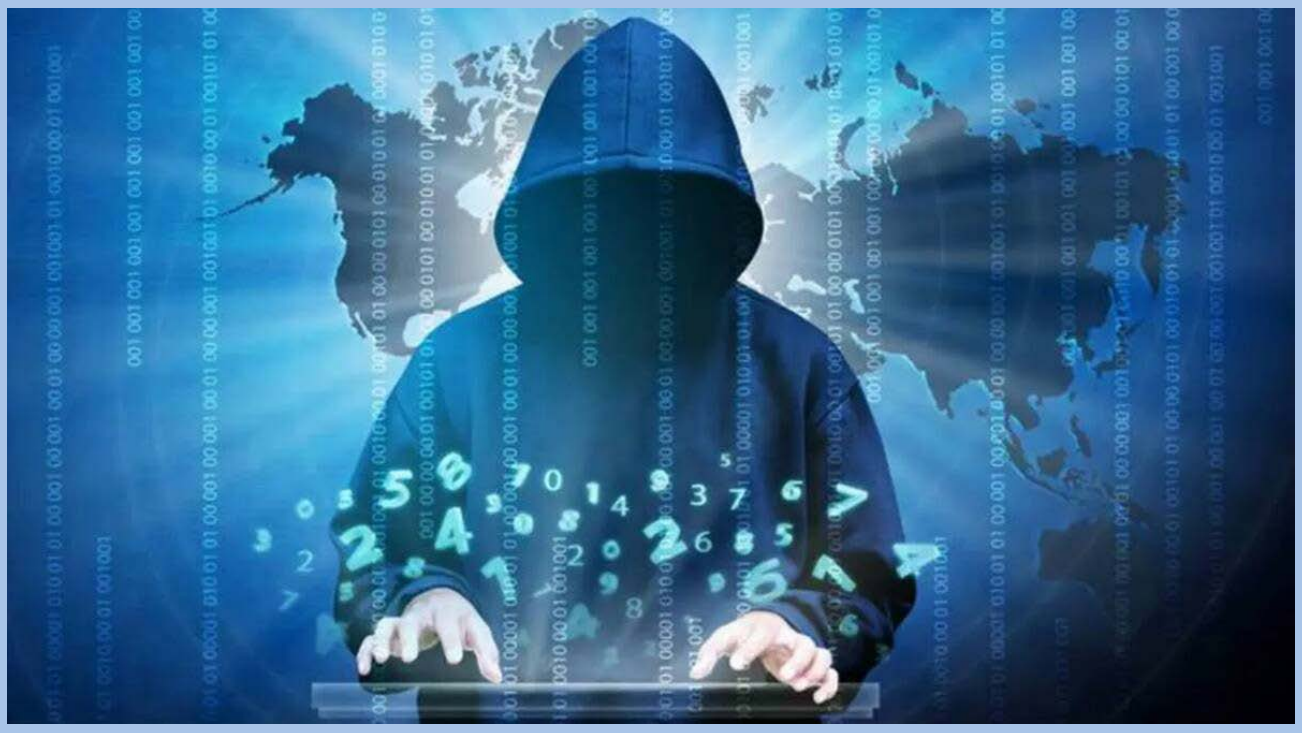

Image Source: The Indian Express

Key Points

About Erbium

- Erbium is a **Malware-as-a-Service (MaaS)**, which means anyone with enough money can get their hands on it.
- It is often injected into game cracks and pirated software.
- It **focuses on retrieving user data** stored in web browsers based on Chromium and Gecko like Google Chrome, Microsoft Edge and Mozilla Firefox.
- The malware steals information like passwords, cookies, autofill information and credit cards.

What is Malware?

- Malware is the **collective name** for a **number of malicious software variants**, including viruses, ransomware and spyware.
- It typically **consists of code** developed by cyberattackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network.
- It is **delivered in the form of a link or file** over email and requires the user to click on the link or open the file to execute the malware.

unacademy

Types of Malware

Virus
- A virus is a **malicious software** attached to a document or file.
- Once downloaded, the virus will lay dormant until the file is opened and used.
- It can cause significant operational issues and data loss.

Trojan virus
- Trojan viruses are **disguised as helpful software** programs.
- Once the user downloads it, the Trojan virus can gain access to sensitive data and then modify, block, or delete the data.

Worms
- These are malicious software that **rapidly replicates and spreads** to any device within the network.

Spyware
- Spyware is malicious software that runs **secretly on a computer** and reports back to a remote user.

Ransomware
- Ransomware is malicious software that gains access to sensitive information within a system and then demands a financial payout for the data to be released.

Challenges Related to Cyber Security in India
- There is **no separate procedural** code for the investigation of cyber or computer-related offences.
- There have been **half-hearted efforts by the States** to recruit technical staff for the investigation of cybercrime.
- Most cybercrimes are **transnational in nature** with extra-territorial jurisdiction. The collection of evidence from foreign territories is a difficult process.

Steps Taken by Government to Tackle Cyber Security Incidents:
- Establishment of **National Critical Information Infrastructure Protection Centre (NCIIPC)** for the protection of critical information infrastructure in the country.
- **Cyber Swachhta Kendra** (Botnet Cleaning and Malware Analysis Centre) has been launched for providing the detection of malicious programmes.
- **Issue alerts and advisories** regarding cyber threats and counter-measures by **CERT-In.**
- Formulation of a Crisis Management Plan for countering cyber attacks and cyber terrorism.
- Setting up a **Cyber Warrior Police Force (CWPF)** to tackle internet-related crimes such as cyber threats, child pornography and online stalking.

- CERT-In under **the Ministry of Electronics and Information Technology** is the **national nodal agency** for responding to computer security incidents as and when they occur.
- **2015:** The **office of the National Cyber Security Coordinator** was established for advising the Prime Minister on strategic cybersecurity issues.

Way Forward

- The Cyber forensic laboratories of States must be upgraded with the advent of new technologies.
- The Centre and States should work together and frame statutory guidelines to facilitate the investigation of cybercrime.
- It is essential that State governments build up sufficient capacity to deal with cybercrime.
- It could be done either by **setting up a separate cyberpolice station** in each district or range or by having technically qualified staff in every police station.

एर्बियम

Erbium नाम का एक नया मैलवेयर पिछले कुछ महीनों से इंटरनेट पर कहर बरपा रहा है।

छवि स्रोत: द इंडियन एक्सप्रेस

प्रमुख बिंदु

एर्बियम के बारे में:

- Erbium **एक मालवेयर-एज़-ए-सर्विस (MaaS)** है, जिसका अर्थ है कि पर्याप्त धन वाला कोई भी व्यक्ति इसके झांसे में आ सकता है।
- इसे अक्सर गेम क्रैक और पायरेटेड सॉफ्टवेयर में इंजेक्ट किया जाता है।
- यह क्रोमियम और गेको जैसे Google क्रोम, माइक्रोसॉफ्ट एज और मोज़िला फ़ायरफ़ॉक्स पर आधारित वेब ब्राउज़र में संग्रहीत उपयोगकर्ता डेटा को **पुनः प्राप्त करने** पर केंद्रित है।
- मैलवेयर,पासवर्ड, कुकीज, ऑटोफिल जानकारी और क्रेडिट कार्ड जैसी जानकारी चुरा लेता है।

मैलवेयर क्या है?

- **मैलवेयर वायरस, रैंसमवेयर और स्पाइवेयर सहित कई खतरनाक** सॉफ़्टवेयर वेरिएंट का **सामूहिक नाम** है।
- इसमें आमतौर पर साइबर हमलावरों द्वारा **विकसित कोड होता** है, जिसे डेटा और सिस्टम को व्यापक नुकसान पहुंचाने या नेटवर्क तक अनधिकृत पहुंच प्राप्त करने के लिए डिज़ाइन किया गया है।
- यह ईमेल पर एक **लिंक या फ़ाइल** के रूप में दिया जाता है और उपयोगकर्ता को लिंक पर क्लिक करने या मैलवेयर को निष्पादित करने के लिए फ़ाइल खोलने की आवश्यकता होती है।

unacademy

मैलवेयर के प्रकार

वाइरस

- वायरस एक खतरनाक सॉफ़्टवेयर है जो किसी दस्तावेज़ या फ़ाइल से जुड़ा होता है।
- एक बार डाउनलोड हो जाने के बाद, वायरस तब तक निष्क्रिय रहेगा जब तक कि फ़ाइल खोली और उपयोग में नहीं आ जाती।
- यह महत्वपूर्ण परिचालन मुद्दों और डेटा हानि का कारण बन सकता है।

ट्रोजन वायरस

- ट्रोजन वायरस सहायक सॉफ्टवेयर प्रोग्राम के रूप में प्रच्छन्न हैं।
- एक बार जब उपयोगकर्ता इसे डाउनलोड कर लेता है, तो ट्रोजन वायरस संवेदनशील डेटा तक पहुंच प्राप्त कर सकता है और फिर डेटा को संशोधित, ब्लॉक या हटा सकता है।

वॉर्म्स

- ये दुर्भाविनापूर्ण सॉफ़्टवेयर हैं जो नेटवर्क के भीतर किसी भी डिवाइस की तेज़ी से प्रतिलिपि बनाते हैं और फैलते हैं।

स्पाइवेयर

- स्पाइवेयर दुर्भाविनापूर्ण सॉफ़्टवेयर है जो कंप्यूटर पर गुप्त रूप से चलता है और किसी दूरस्थ उपयोगकर्ता को वापस रिपोर्ट करता है।

रैंसमवेयर

- रैंसमवेयर दुर्भाविनापूर्ण सॉफ़्टवेयर है जो एक सिस्टम के भीतर संवेदनशील जानकारी तक पहुँच प्राप्त करता है और फिर डेटा जारी करने के लिए वित्तीय भुगतान की मांग करता है।

भारत में साइबर सुरक्षा से संबंधित चुनौतियाँ

- साइबर या कंप्यूटर से संबंधित अपराधों की जांच के लिए कोई अलग प्रक्रियात्मक कोड नहीं है।
- साइबर अपराध की जांच के लिए तकनीकी कर्मचारियों की भर्ती के लिए राज्यों द्वारा आधे-अधूरे प्रयास किए गए हैं।
- अधिकांश साइबर अपराध अंतरराष्ट्रीय प्रकृति के होते हैं और अतिरिक्त-क्षेत्रीय क्षेत्राधिकार के साथ होते हैं। विदेशी क्षेत्रों से साक्ष्य एकत्र करना एक कठिन प्रक्रिया है।

साइबर सुरक्षा घटनाओं से निपटने के लिए सरकार द्वारा उठाए गए कदम:

- देश में महत्वपूर्ण सूचना अवसंरचना के संरक्षण के लिए राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC) की स्थापना।
- दुर्भाविनापूर्ण कार्यक्रमों का पता लगाने के लिए साइबर स्वच्छता केंद्र (बॉटनेट क्लीनिंग एंड मालवेयर एनालिसिस सेंटर) शुरू किया गया है।
- सीईआरटी-इन द्वारा साइबर खतरों और प्रति-उपायों के संबंध में अलर्ट और सलाह जारी करना।
- साइबर हमलों और साइबर आतंकवाद का मुकाबला करने के लिए एक संकट प्रबंधन योजना तैयार करना।
- इंटरनेट से संबंधित अपराधों जैसे साइबर खतरों, बाल अश्लीलता और ऑनलाइन पीछा करने से निपटने के लिए साइबर

योद्धा पुलिस बल (CWPF) की स्थापना करना।

- इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय के तहत सीईआरटी-इन कंप्यूटर सुरक्षा घटनाओं के होने पर प्रतिक्रिया देने के लिए राष्ट्रीय नोडल एजेंसी है।
- 2015: प्रधानमंत्री को रणनीतिक साइबर सुरक्षा मुद्दों पर सलाह देने के लिए राष्ट्रीय साइबर सुरक्षा समन्वयक का कार्यालय स्थापित किया गया था।

आगे बढ़ने की राह

- राज्यों की साइबर फोरेंसिक प्रयोगशालाओं को नई प्रौद्योगिकियों के आगमन के साथ उन्नत किया जाना चाहिए।
- केंद्र और राज्यों को मिलकर काम करना चाहिए और साइबर अपराध की जांच को सुविधाजनक बनाने के लिए वैधानिक दिशानिर्देश तैयार करने चाहिए।
- यह आवश्यक है कि राज्य सरकारें साइबर अपराध से निपटने के लिए पर्याप्त क्षमता का निर्माण करें।
- यह या तो प्रत्येक जिले या रेंज में एक अलग साइबर पुलिस स्टेशन स्थापित करके या प्रत्येक पुलिस स्टेशन में तकनीकी रूप से योग्य कर्मचारी होने के द्वारा किया जा सकता है।