Akira Ransomware

Source: TH

Why in News?

Recently, the Indian government's **Computer Emergency Response Team (CERT-In)** issued a warning about the Akira ransomware, which has emerged as a significant cybersecurity **threat**, targeting both Windows and Linux devices.

- Ransomware is a type of **malware that hijacks computer data and then demands payment** (usually in bitcoins) in order to restore it.

What is Akira Ransomware?

- **About:**
  - It is **malicious software** that poses a significant threat to **data security.**
  - It targets **both Windows and Linux devices,** encrypting data and demanding a **ransom for decryption.**
- **Key Characteristics of Akira Ransomware:**
  - Designed to **encrypt data and create a ransomware note** with a unique **".akira" extension** appended to encrypted filenames.
  - Capable of deleting Windows Shadow Volume copies and shutting down Windows services to prevent interference during encryption.
  - Exploits **VPN services and malicious files** to infect devices, making it challenging to detect and prevent.
- **Mode of Operation:**
  - Akira ransomware spreads through various methods, including spear phishing emails with **malicious attachments, drive-by downloads, and specially crafted web links** in emails.
  - **Insecure Remote Desktop connections** are another avenue for ransomware transmission.
- Implications of an Akira Attack:
  - Once infected, Akira ransomware **steals sensitive data and encrypts it, rendering it inaccessible to the victim.**
  - Attackers then demand a ransom for decryption and threaten to leak the stolen data on the dark web if their demands are not met.
- **Protection Measures Against Akira Ransomware:**
  - Regularly **maintain up-to-date offline backups to prevent data loss** in case of an attack.
  - Keep **operating systems and networks updated,** including virtual patching for legacy systems, to address potential vulnerabilities.
  - Implement **security protocols such as Domain-based Message Authentication, Reporting, and Conformance (DMARC), Domain Keys Identified Mail (DKIM), and Sender Policy for email validation.**
  - Enforce strong **password policies and Multi-Factor Authentication (MFA)** to enhance user authentication.
  - Establish a strict policy for **external device usage and ensure data-at-rest and data-**

    in-transit encryption.
    - Block attachment file types with suspicious extensions like .exe, .pif, and .url to avoid downloading malicious code.
    - Educate users to be cautious about clicking on suspicious links to prevent malware downloads.
    - Conduct regular security audits, especially for critical systems like database servers, to identify and address vulnerabilities.

What is CERT-IN?

- Computer Emergency Response Team - India is an **organisation of the Ministry of Electronics and Information Technology** with the objective of securing Indian cyberspace.
- It is a **nodal agency which deals with cybersecurity threats** like hacking and phishing.
- It collects, analyses and disseminates information on cyber incidents, and also **issues alert on cybersecurity incidents.**
- CERT-IN provides **Incident Prevention and Response Services** as well as Security Quality Management Services.

UPSC Civil Services Examination Previous Year Question (PYQ)

Prelims

Q. The terms ‘WannaCry, Petya and EternalBlue’ sometimes mentioned in the news recently are related to (2018)

(a) Exoplanets
(b) Cryptocurrency
(c) Cyber attacks
(d) Mini satellites

Ans: (c)

Q. In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)

1. Cost of restoration of the computer system in case of malware disrupting access to one’s computer
2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialized consultant to minimize the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

(a) 1, 2 and 4 only
(b) 1, 3 and 4 only
(c) 2 and 3 only
(d) 1, 2, 3 and 4

Ans: (b)

Q. In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only
(b) 1 and 2 only
(c) 3 only
(d) 1, 2 and 3

Ans: (d)

PDF Refernece URL: https://www.drishtiias.com/printpdf/akira-ransomware