01 – 08 – 2023

News: Akira Ransomware

Akira Ransomware

- The Computer Emergency Response Team of India (CERT–IN) has warned about the Akira Ransomware.
- The ransomware, found to target both Windows and Linux devices, steals and encrypts data, forcing victims to pay double ransom for decryption and recovery.
- The Akira ransomware is designed to encrypt data, create a ransomware note and delete Windows Shadow Volume copies on affected devices.
- The ransomware gets its name due to its ability to modify filenames of all encrypted files by appending them with the ".akira" extension.
- The ransomware is designed to close processes or shut down Windows services that may keep it from encrypting files on the affected system.
- It uses VPN services, especially when users have not enabled two factor authentications, to trick users into downloading malicious files.

- Once the ransomware infects a device and steals/encrypts sensitive data, the group behind the attack extorts the victims into paying a ransom, threatening to release the data on their dark web blog if their demands are not met.
- The ransomware deletes the Windows Shadow Volume copies on the affected device. These files are instrumental in ensuring that organisations can back up data used in their applications for day–to–day functioning.
- VSS services facilitate communication between different components without the need to take them offline; thereby ensuring data is backed up while it is also available for other functions.
- Once the ransomware deletes the VSS files it proceeds to encrypt files with the predefined the ".akira" extension.
- The ransomware also terminates active Windows services using the Windows Restart Manager API, preventing any interference with the encryption process.
- It is designed to not encrypt Program Data, Recycle Bin, Boot, System Volume information, and other folders instrumental in system stability.
- It also avoids modifying Windows system files with extensions like .syn. .msl and .exe.
- Once sensitive data is stolen and encrypted, the ransomware leaves behind a note named akira_readme.txt which includes information about the attack and the link to Akira's leak and negotiation site.

- Each victim is given a unique negotiation password to be entered into the threat actor’s Tor site.
- Unlike other ransomware operations, this negotiation site just includes a chat system that the victim can use to communicate with the ransomware gang.

CERT – IN advice to the users

- CERT–IN has advised users to follow basic internet hygiene and protection protocols to ensure their security against ransomware.
- These include maintaining up to date offline backups of critical data, to prevent data loss in the event of an attack.
- Additionally, users are advised to ensure all operating systems and networks are updated regularly, with virtual patching for legacy systems and networks.
- Companies must also establish Domain based Message Authentication, Reporting, and Conformance, Domain Keys Identified Mail (DKIM), and Sender policy for organisational email validation, which prevents spam by detecting email spoofing.
- Strong password policies and multifactor authentication (MFA) must be enforced.

- There should also be a strict external device usage policy in place and data at rest and data in transit encryption along with blocking attachment file types like .exe, .pif, or .url to avoid downloading malicious code.
- The agency has also advised periodic security audits of critical networks and systems, especially database servers.

Cybercrimes

- Cybercrime is a crime that involves a computer and a network.
- The computer may have been used to commit the crime and in many cases, it is also the target. Cybercrime may threaten a person or a nation's security and financial health.

Definition

- Any offenses committed against individuals or groups of individuals to harm the reputation or cause physical or mental trauma through electronic means can be defined as Cybercrime. Electronic means can include but are not limited to, the use of modern telecommunication networks such as the Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).

Types of Cybercrimes

- **Identity theft** – Identity theft is defined as theft of personnel information of an individual to avail financial services or steal the financial assets themselves.
- **Cyberterrorism**–Cyberterrorism is committed with the purpose of causing grievous harm or extortion of any kind subjected towards a person, groups of individuals, or governments.
- **Cyberbullying**–Cyberbullying is the act of intimidating, harassment, defaming, or any other form of mental degradation through the use of electronic means or modes such as social media.
- **Hacking**–Access of information through fraudulent or unethical means is known as hacking. This is the most common form of cybercrime know to the general public.
- **Defamation**–While every individual has his or her right to speech on internet platforms as well, but if their statements cross a line and harm the reputation of any individual or organization, then they can be charged with the Defamation Law.
- **Trade Secrets**–Internet organization spends a lot of their time and money in developing software, applications, and tools and rely on Cyber Laws to protect their data and trade secrets against theft; doing which is a punishable offense.

- **Freedom of Speech**–When it comes to the internet, there is a very thin line between freedom of speech and being a cyber-offender. As freedom of speech enables individuals to speak their mind, cyber law refrains obscenity and crassness over the web.
- **Harassment and Stalking**–Harassment and stalking are prohibited over internet platforms as well. Cyber laws protect the victims and prosecute the offender against this offense.