Cyber Security Digest

Bi-Weekly Update by the CISO section of Meghalaya Rural Bank

Vol: I Issue 2

Date: 01-10-2024

Lebanon's Kinetic Cyber Attack

On Tuesday 17th September, hundreds of pagers in Lebanon exploded simultaneously in a coordinated chain attack, targeting members of the political party and paramilitary group Hezbollah which had in previous months ordered, shipped and distributed the pagers to some of its members.

A day later, a similar attack struck again when hundreds of walkie-talkies used by Hezbollah detonated.

But how could these tiny, old-school pagers and humble walkie-talkies be forced to explode?

Experts points out to two possibilities– the first is a cyber attack in which malware forced the pagers' lithium batteries to overheat and then explode.

The second and more likely scenario points to a supply chain attack in which a shipment of pagers bound for Lebanon was intercepted and a tiny amount of explosive surreptitiously inserted with extra electronics to trigger the detonation, which was then remotely activated.

While the world focuses on securing modern digital platforms, this incident highlights a significant vulnerability in older technology. The use of exploding pagers and walkie-talkies indicates that 21st century warfare is not only about technological advancements but also about the creative use of existing tools. This incident underscores that security is not just about the latest technology but understanding the full spectrum of potential threats, including those from seemingly antiquated devices.

Exploding Walkie –Talkie

Exploding Pager

Centre to train 5000 'Cyber Commandos' in next five years to fight cyber threats

Recently, the Central Government announced the plan to train and prepare 5000 cyber commandos over the next five years to tackle the rising cybercrime threats. This announcement was made during the first Foundation Day celebration of the Indian Cyber Crime Coordination Centre (I4C). I4C is a national-level coordination centre for addressing cybercrime issues. These cyber commandos will be trained in IT infrastructure security, digital forensics and incident response. Other launches along with Cyber Commandos: Centralized Suspect Registry, Samanvaya Platform and Cyber Fraud Mitigation Centre (CFMC)

CYBER CRIME NEWS

- **Cyber fraudsters misuse 1930 helpline number to scam people : *Times of India***
- **BookMyShow under the radar as lawyers file cyber crime complaint over Coldplay tickets : *CNBC TV18***

EMAIL ATTACKS

First , let's see how an email works. Suppose John is sending an email to Jack. The email first goes to the email server. Then it goes to the DNS server to find the IP address of the destination. From the source email server, the email goes to the destination server. From there, the email is sent to the IP Address on which Jack is working. It is illustrated in the picture below.

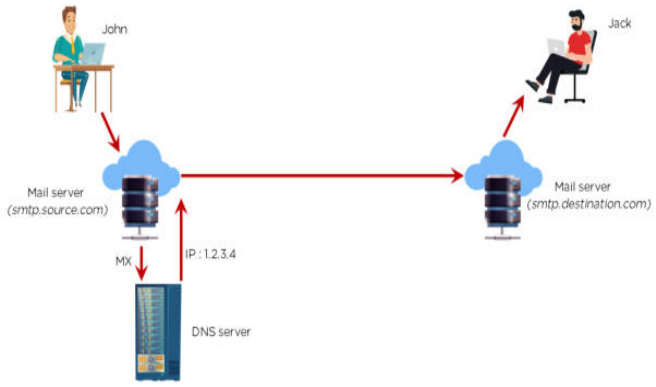

Fig: How email works

2) **Spoofing**: The attacker pretends to be another person or organization and sends you an email stating that it is a legitimate email. For example: Fig 2

After seeing this email, you might share the password to your computer. Always ask the person from whom you received the email one more time to confirm that he is the right person.

3) **Email attachments**: You can send files through emails. These files may be images, documents, audio, or videos. Attackers send you an email, and you are encouraged to open the attached file. For example: Fig 3

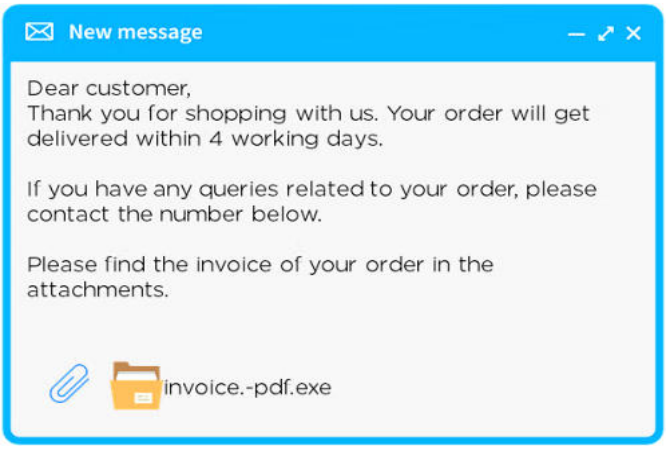

Fig 3

There are three types of email attacks:

1) **Phishing**: The attacker sends bait, often in the form of an email. It encourages people to share their details. For example, you receive an email like this:

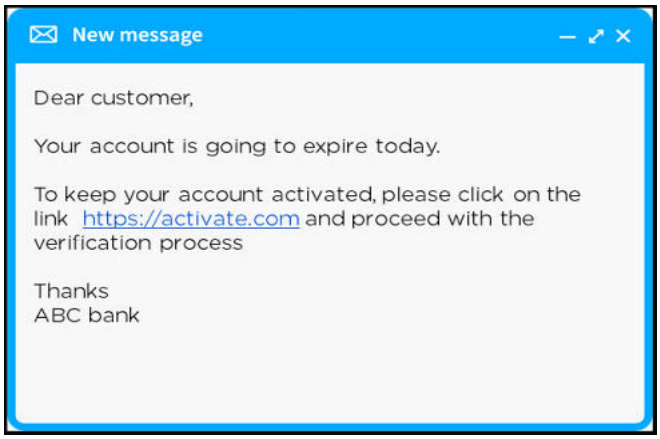

Fig 1

If someone is a customer of ABC bank, he would probably open the link and give the details. But these kinds of emails are always phishing; banks do not send emails like this.

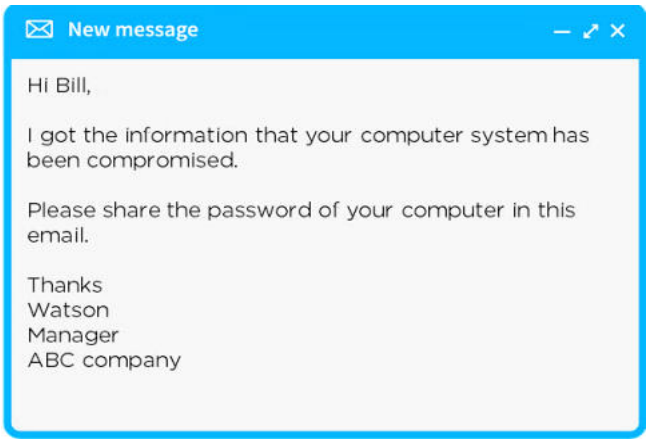

Fig 2