ADVISORY REPORT ON
FBI’s email System Hack
Advisory report on FBI's email System Hack

Date: 30th November 2021

Executive Summary

Recently thousands of emails were sent to several people from the United States Federal Bureau of Investigation or FBI’s Servers. These emails were not a hoax or from phishing websites impersonating the FBI but from official and legitimate FBI servers and were officially acknowledged by the FBI as well. The content of these emails stated that the FBI had identified that recipient devices have been exfiltrated in some attack and an individual by the name of Vinny Troia, who is associated with a Dark web hacking group as well, is behind this attack. While the FBI is still investigating the issue and finding the individual behind this, they have identified that the said incident took place through the compromise of LEEP or the Law Enforcement Enterprise Portal, which is not connected to the FBI’s internal corporate portal or FBI’s internal data cannot be compromised with access to these portals.

Description

An authorised individual or group of individuals accessed the FBI email servers around 13th November 2021 and had sent thousands of security warnings. A non-profit organisation that tracks spam addresses, was first to identify and report these questionable messages and stated that these were sent from official FBI servers through their LEEP, which is the platform used by the FBI to talk with state and close law-enforcement associates. The message sent was as follows –

“Our intelligence monitoring indicates exfiltration of several of your virtualized clusters in a sophisticated chain attack. We tried to blackhole the transit nodes used by this advanced persistent threat actor, however there is a huge chance he will modify his attack with fast flux technologies, which he proxies through multiple global accelerators. We identified the threat actor to be Vinny Troia, who is believed to be affiliated with the extortion gang TheDarkOyerlord. We highly recommend you to check your systems and IDS monitoring. Beware this threat actor is currently working under inspection of the NCCIC, as we are dependent on some of his intelligence research we can not Interfere physically within 4 hours, which could be enough time to cause severe damage to your infrastructure. Stay safe, U.S Department of Homeland Security | Cyber Threat Detection and Analysis Network Analysis Group”
By going deep into the sender email id “eims@ic.fbi.gov” it is found that the IP address was 153.31.119.142 and going deep into this id the following details were identified.

The programmers utilized the FBI’s public-facing email system to send these messages and appear legitimate. The emails which were sent these messages were collected from the American Registry of Internet Number (ARIN). While they didn’t think any unusual attachment was added to the email, this was possibly a trick intended to frighten the beneficiaries.
How was the FBI’s email system hacked?

The threat actor’s access to the FBI’s email system began with an exploration of its Law Enforcement Enterprise Portal (LEEP), which the bureau describes as “a gateway providing law enforcement agencies, intelligence groups, and criminal justice entities access to beneficial resources.”

The Law Enforcement Enterprise Portal (LEEP) is a solid stage for law authorization offices, insight gatherings, and criminal equity substances. LEEP gives electronic insightful devices and logical assets, and the systems administration it upholds is unmatched by different stages accessible to law implementation. Clients team up in a solid climate, use apparatuses to reinforce their cases and offer departmental archives.

While filling up forms in the LEEP portal, advance in that cycle says candidates will get an email affirmation from eims@ic.fbi.gov with a one-time password apparently to approve that the candidate can get an email at the space being referred to.
**FBI's response:**

The Bureau and CISA, as soon as they discovered these issues, bought the relevant systems offline and released a press report on 13th November that they were investigating the issue and people responsible for the same and requested the public to stay cautious and report any unusual activity to ic3.gov or cisa.gov.

The next day the FBI also clarified the issue and highlighted the problem behind the said incident which was a temporary misconfiguration of the LEEP and had been fixed. They further clarified that no internal corporate systems or servers of the FBI were connected to or with this portal and therefore had not been compromised or affected in any way. They also informed that relevant people have been communicated with the issue and have been asked to disregard the email.

**CyberPeace Advisory:**

The relevant people i.e. who received the emails have been informed by the FBI about the same and have been asked to disregard the emails. While there is not much that one can do when a significant organisation is compromised and one becomes an ancillary victim of that incident. However, what one can do is to keep their security systems up to date and react accordingly, in case such an incident is repeated.

Having comprehensive Cyber security and safety mechanisms as per recomendation would include the following:

- Keeping the software and operating systems updated with all the latest security patches.
- Creating backups of all the data and keeping the important information in protected folders.
- Efficiently manage firewalls and not use the in-built antivirus of Windows i.e Windows Defender, without the internet.
- Investing in good Anti-virus software and personal cyber-insurance policy to avoid liabilities, losing of data and suffering from monetary loss.
- Maintain strong Password Policy :
  - Use a strong password for all devices and online accounts.
  - Passwords should be at least 8-13 characters long.
  - Passwords should contain at least one upper case [A-Z], numeric character [0-9] and a special character [@%&....].
  - Do not use the same password for all your online accounts. All the passwords should be different for different accounts.
- Avoiding ‘panic’ reactions to any emails that give a ‘warning’ of compromised systems.
References:


Revision Table:

<table>
<thead>
<tr>
<th>VERSION</th>
<th>DESCRIPTION</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Initial Public Release</td>
<td>Final</td>
</tr>
</tbody>
</table>

Issued by:

Research Wing, CyberPeace Foundation.
Research Wing, Autobot Infosec Private Ltd.