New Phishing Drive Launches A Double Attack with LokiBot Information Stealing Malware and Jigsaw Ransomware

Recently, a new phishing crusade is spreading a combination of LokiBot information-stealing malware followed by a second payload in the form of Jigsaw Ransomware. The **LokiBot malware first steals stored credentials from the victim's system and then deploys the Jigsaw Ransomware to collect a ransom.**

How is the phishing campaign conducted?

The latest LokiBot variant, without deviating from its previous mode of attacks, is distributed via spam emails. The miscreants use fabricated invoices, order confirmations, transfers, and other similar counterfeit documents in Excel format as an attachment with the email. This attack is using **spreadsheet attachments with names like "Swift.xlsx", "orders.xlsx", "Inquiry.xlsx", "Invoice For Payment.xlsx".** The attackers use skillfully designed or even **legitimate spreadsheets that have been weaponized** in order to seem credible. These attachments have been weaponized using LCG kit to make them exploit an old Microsoft Office remote code execution vulnerability tracked as CVE-2017-11882 in Equation Editor. LCG kit is an algorithm to generate a sequence of pseudorandom numbers to apply encryption to the terminating stage of the code, including the malware location.

Which MS Office vulnerabilities are being exploited?

The Microsoft Office vulnerability being abused in this campaign is CVE-2017-11882.

CVE-2017-11882 is a remote code execution flaw in Microsoft Office due to its failure to properly handle objects in memory. Post successful exploit of the vulnerability, a crook can run arbitrary code in the context of the current user. If the present user is an administrator, the hacker could take control of the vulnerable device and carry out all activities that an administrator is capable of.

What is Loki?

Loki is an info-stealer that can exfiltrate saved credentials from different web browsers, FTP, mails and terminal programs and transfer them to its C2 server.

What is Jigsaw?

Previously known as "BitcoinBlackmailer", Jigsaw is a ransomware family that encrypts files on a target machine and gradually deletes them unless a ransom is paid to decrypt the files.

What is the attack routine?

Once the recipient of the spam emails opens the malicious attachments, the weaponized spreadsheets exploit Microsoft Office CVE-2017-11882 remote code execution vulnerability in Equation Editor. After successful exploitation, the LokiBot malware will be downloaded from a remote site and executed. The Trojan launches the "cjjjjjjjjjjjjjjjj.exe" executable and starts scanning the system for valuable information. Once the sensitive information is obtained, it connects to a remote server to download a Jigsaw ransomware version that has a Salvadore Dali mask as its background from the renowned web show "Money Heist". Once it is downloaded and run, all files on the victim's device are encrypted with a .zemblax file extension and can no longer be accessed by the user.

What can we do to prevent the attack?

This campaign uses phishing emails as a distribution medium. Phishing or spam attacks are on the rise globally because they are highly effective and easy to implement.

Email users are advised to adhere to the following remedial measures to protect themselves against spam or phishing attacks:

1. **Users should always be alert and careful** even if the email appears to be from a familiar or reputed brand because in case of many phishing attacks, hackers prey on potential victims by masquerading as a popular brand. The best way to detect this is to check the sender address i.e. whether the email has been sent from a spoofed email address impersonating the domain of the legitimate brand.
2. Phishing emails can be detected even before opening them by merely taking a look at their subjects. A recipient should **check whether the subject is of any relevance to him or NHA**. If the subject contains any request for personal or financial data, it is an obvious clue of a suspected phishing scam.
3. It is also deemed sensible to verify the list of recipients to which the email has been sent i.e. whether the email has been sent to several addresses including some spoofed or fake ones, whether the recipient list is hidden etc.
4. If the tone of the email subject or body contains a sense of urgency i.e. the email is requesting the recipient for an immediate money transfer or to provide his personal and financial details at once, it is a possible red flag regarding a phishing attack.
5. Some obvious clues like **poor grammar or spelling** should be a potent indicator to detect phishing mails.
6. In order to verify the genuineness of an embedded link inside an email, **users should hover their mouse pointer over the link instead of actually clicking on it.** The actual URL to which the user will be redirected can be previewed on the bottom left/right corner of the browser window. If the embedded URL does not match the link description, it can be ascertained to be a suspected phishing scam.
7. Most phishing emails come with **malicious attachments in the form of Microsoft Office documents disguised as legitimate business** or financial documents to lure the recipient into opening them and enabling any embedded macro code to view their complete content that will ultimately lead to the installation of the malware payload.
8. If the attached document ends with a ".exe" extension, then it is certainly a malicious executable file disguised as a legitimate document. So, users should be extra careful in dealing with such attachments and **report any suspicious occurrence to the NHA IS Team.**
9. Legitimate email senders generally provide a full signature block at the end of the email body, the absence of which might suggest a possible phishing message.
10. If you know the sender by name and are still unsure as to whether he actually sent the email, it is always prudent to get in touch with the person personally over the phone to confirm the legitimacy of the email.