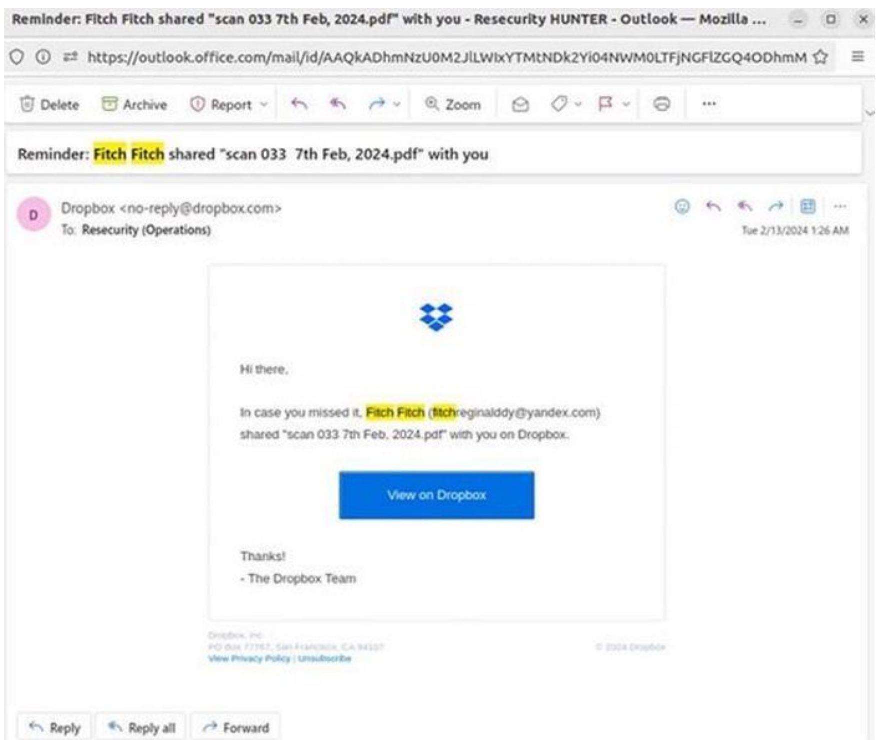
Phishing campaign via email, abusing Microsoft Office templates to spread malicious code

A new phishing campaign is targeting US organizations with the aim of deploying the NetSupport RAT remote access trojan and is being tracked by Israeli security firm Perception Point as Operation PhantomBlu…



According to researcher Ariel Davidpur, Operation PhantomBlu uses a very sophisticated exploitation method. Different from the normal NetSupport RAT distribution mechanism, it abuses interference with OLE (Object Linking and Embedding) templates, exploiting Microsoft Office document templates to execute malicious code.

NetSupport RAT is a malicious variant (malicious offshoot) of the legitimate remote computer access tool NetSupport Manager. NetSupport RAT allows threat actors to collect data from compromised devices.

The most common scenario for this attack is to start with a phishing email with the subject 'salary' to trick the recipient into opening the attached Microsoft Word document to view the monthly salary report.

The word file, when opened, will ask the victim to enter the password provided in the email body and allow editing, then double-click the printer icon in the document to view the salary chart.

This will open a ZIP file ("Chart20072007.zip") containing a Windows shortcut file. This file acts as a PowerShell tool that allows NetSupport RAT malware to be downloaded and executed from a remote server. From there, the subject will attack and commit acts of appropriation of property on the victim's device.

To minimize the risk of becoming a victim of such attack campaigns, users should always be vigilant when receiving strange emails, DO NOT access links or download/open attachments in emails IF this email is sent from an unreliable source or the email content has any suspicious elements.

Faced with information about the above international phishing campaign, the Department of Information Security (Ministry of Information and Communications) recommends that people be careful with files sent from unreliable sources or email content. suspect.

'It is necessary to carefully check the sender's email address and the content in the email; Do not arbitrarily click on any attachments or links in emails when you notice anything suspicious. Do not provide any personal or bank account information when requested to declare information from emails, recommended by the Department of Information Security.

In addition, users should use anti-virus software to scan email attachments. At the same time, pay attention to safety issues if using email when connecting to public wireless networks.

Besides, it is also important to note that you should not use one email for many Internet services, especially important services; Regularly change strong email passwords, do not leave default passwords; Set up two-layer security for email to authenticate with your phone so you can recover emails when attacked.

You finished reading the article "**Phishing campaign via email, abusing Microsoft Office templates to spread malicious code**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.