Warning: New email phishing tactics appear

Hackers specializing in phishing email campaigns have always 'invented' new techniques to bypass popular security tools. Email security solutions provider Inky (USA) has just discovered three new phishing email campaigns that disguise the Microsoft logo, but it is very difficult to stop.

New scam technique

This technique takes advantage of HTML code to integrate a table (table) containing the fake Microsoft logo into email sent to the user. It works well because email security programs don't parse tables, since the tables have never been used in phishing emails. The fake Microsoft logo looks a lot like the real Microsoft logo, so emails easily slip through security filters and appear legitimate and unsuspecting to the email recipient.

What is quite surprising is that it was Microsoft inadvertently supporting this technique. The old Microsoft logo was a stylish design with 4 colors and 3-dimensional border. By 2012, Microsoft changed and simplified its logo, keeping the same 4 colors but switched to a 2-dimensional flat design. It is this simplicity that makes the new Microsoft logo very easy to fake because anyone can create a 4-cell board, with 4 colors like the Microsoft logo.

Phishing email campaigns

Fake SharePoint email

During this campaign, an HTML logo disguised as Microsoft appears in fax messages. Along with the SharePoint mark (Microsoft's collaborative work platform), these emails contain a link with the words "Preview

or Download Here" (to preview or download the fax attachment). However, if the user clicks on it, it will go to the UNICEF China website, then redirect to a website about a legitimate web development tool called CodeSandbox, but from there the malware will be installed into user's computer. The fake billboards and logos combined with redirects to legitimate websites leave many users unsuspecting.

+ Office 365

For users of the Office 365 premium office applications service, the phishing campaign sends emails that recommend the user that their password has expired. These emails contain a link with the words "Keep My Current Password". However, if you click on that link, it redirects the user to a legitimate email marketing platform that has been hijacked, and then goes to the CodeSandbox website to install the malware.

+ Voice message

To Microsoft's Voice Message users, the phishing campaign sends emails reporting new voice messages. These emails also contain malicious links, which are hidden in a hexadecimal encrypted HTML attachment. By using fake Microsoft logos, hidden malicious links, and hexadecimal strings, phishing emails were able to bypass security solutions and deceive users.

Stop solution

Phishing emails are increasingly sophisticated and difficult to distinguish. They look very legitimate and unsuspecting, can bypass the common email filtering and security solutions, even leading Microsoft solutions.

Therefore, the best way to analyze and prevent these types of attacks is to combine both humans and machines and compare the results. Users tasked with capturing information, detecting suspicious cues and a good anti-phishing tool equipped with artificial intelligence, will be able to determine if the email was actually sent from Microsoft.