Emotet Phishing Scam Targets Financial Institutions with Malicious Fake Invoices

Widespread malware evolves, spreading rapidly in the US and UK

We've written a lot about phishing and spear phishing in this space, but a new series of attacks targeting banks and financial institutions in the US and the UK deserves your renewed attention. They are not only destructive but also leave doors open for future attacks.

Emotet Trojan

A banking trojan called Emotet has recently evolved into a botnet. It enables enterprising cyber criminals to profit from lending its powerful capabilities to others who seek to spread their own malware to unsuspecting victims.

> *Last year, Emotet delivered nearly two thirds of the malware infecting computers in phishing attacks.*

Emotet-based attacks appeared to taper off late last year but picked up again in January. Details of a new campaign identified by researchers at Menlo Security confirm that use of the phishing tool continues unabated.

Three fourths of the attacks have fallen on US and UK organizations. The Philippines, Spain and India account for the rest of the attempted infections. According to researchers, the attacks are primarily directed at **financial services** organizations. Limited numbers of **food, media** and **transportation** companies have also been targeted.

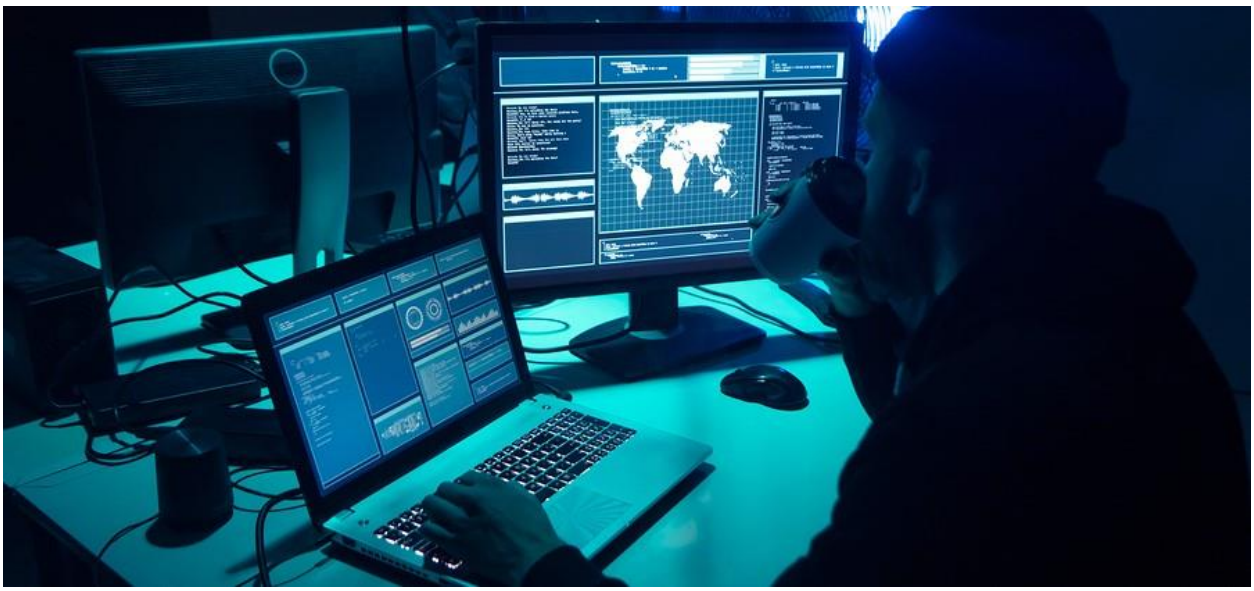
Infected Word Document Enables Back Door

The email subject lines are crafted to attract the attention of workers in financial services. Hence, they contain words and phrases relating to invoices, banking and related financial matters.

> *As in previous Emotet attacks, phishing emails deliver their malware payload via an infected Microsoft Word document.*

Users are asked to 'enable content' to view the document per instructions in the attachment. After doing so, malicious macros or URLs infect the machine with Emotet.

Once a machine is infected, Emotet enables a back door into the system, allowing the hackers to steal valuable information. They might also employ the infected machine to spread additional malware or allow access to other attackers who might exploit the machine for financial gain.



Stay Vigilant

The current attack peaked near the end of January but has tapered off somewhat. However, financial services organizations and others must stay vigilant as they remain attractive targets for this and other phishing campaigns.

"We are continuing to see Emotet traffic, though the intensity has reduced considerably," reported Krishnan Subramanian, researcher at Menlo Labs.

Having spread around the world, malicious Emotet emails are not limited to one or a few sources. Indeed, they can come from any infected Windows machine, anywhere.

To protect against Emotet and other phishing attacks, eMazzanti recommends that all computer users be suspicious of emails, documents or attachments requesting that they enable macros. This is true especially if the communication is from an unfamiliar source. IT managers can also assist users by setting opting to disable macros by default.

As always, IT managers should implement cyber security best practices, including patching and updating operating systems and software to their latest versions. Many attacks use known vulnerabilities that are readily patched. Thus, regular patching can be a front line of defense to thwart the effectiveness of malware.