Email 'phishing' attacks by hackers growing in number, intensity

July 30 2013, by Paresh Dave

At least 2 million people received the email May 16 notifying them that an order they had just made on "Wallmart's" website was being processed, though none of them had done any such thing.

Still, thousands of people clicked on the link in the email, taking many of them to a harmless Google search results page for "Walmart." Others weren't so fortunate. The link led to the invisible download of malware that covertly infected their personal computers, turning them into remotely controlled robots for hackers, according to email security firm Proofpoint Inc.

These sorts of "phishing" attacks are not only becoming more common but also are getting more lethal, with fake emails becoming harder to distinguish from real ones.

In the fake-Wal-Mart attack, people missed clear warning signs - such as the company name being misspelled and the sender's address being very long and strange. But in another case a month later, an email claiming to be from American Airlines carried no visible hints that it was illegitimate.

The sophisticated attacks are targeting the likes of attorneys, oil executives and managers at military contractors. The phishers are increasingly trying to get proprietary documents and pass codes to access company and government databases.

Nearly every incident of online espionage in 2012 involved some sort of a phishing attack, according to a survey compiled by Verizon Communications Inc., the nation's largest wireless carrier.

Several recent breaches at financial institutions, media outlets and in the video game industry have started with someone's log-in information being entered on a false website that was linked to in an email.

When an Associated Press staff member received an email in April that appeared to be from a colleague, the individual didn't hesitate to click on the link. But that link led to the installation of a "keylogger" that enabled a hacker to monitor keystrokes and see the password for the Associated Press' Twitter account.

The hacker posted a tweet from the account saying that someone had bombed the White House. As investors reacted to the tweet, the S&P 500 index's value fell $136 billion. The parody news site the Onion fell prey to a similar, though less costly, attack.

Chandra McMahon, the chief information security officer for military technology giant Lockheed Martin Corp., said phishing attacks aimed at its employees try to replicate emails and websites of industry organizations that its employees visit on a regular basis.

"They are compromised by adversaries because they are the perfect spot to put malware because a lot of the employees from the industry will go there," McMahon said.

As technology firms find ways to make emails safer for consumers, some security experts suggest treating every link skeptically. So if you can never click on a link in an email again, what options are left? Here are some suggestions from security experts:

Open links on an email app on Apple Inc.'s iPad or iPhone. These devices have fewer vulnerabilities so malware is unlikely to stick or get attached by clicking on a bad link. Android devices aren't as foolproof, but smartphones certainly have fewer holes than personal computers.

A few tech companies are promoting a new technology known as Domain-based Message Authentication, Reporting & Conformance, or DMARC, that offers users a visual indication that an email is coming from the legitimate vendor. For example, real emails from EBay Inc. in Gmail include a key next to the "from" field. In Microsoft Corp.'s Outlook, a green key is the sign. Despite a push from firms such as email security provider Agari Data Inc., not every major company has joined this effort.

Other companies are taking different approaches. Wal-Mart Stores Inc., for one, is devising its own tool. Others are trying to block bad emails from reaching the inbox by harnessing the power of big data to see whether a message has the right context clues, anyone's ever received a similar email or whether the sender's ever been replied to. Technology from Proofpoint rewrites a URL, redirecting users to a cloud-based environment in which the email is opened behind the scenes. If malware is found, the user is blocked from visiting the website.

In essence, Proofpoint Chief Executive Gary Steele said, "we click for you in a sandbox in the sky."

This last approach does raise some privacy concerns, but Steele says all information sent online is encrypted and stored under lock and key. Only the customer has the key, so a judicial body must go to the customer directly to get that key.

With the warnings about these sophisticated and consequential attacks starting to grow, it's possible employees could start facing repercussions

for not being cautious with links.

Peter Toren, a former Justice Department computer crimes prosecutor, said he hasn't heard of any companies firing someone for introducing malware into a corporate system by clicking a link. But he said a company might eventually have to make an example of someone.

"They certainly wouldn't sue an employee, because they don't have deep pockets to pay a claim," Toren said. "But it certainly could be grounds for termination. You failed to listen to us. You failed to follow training."