Published on *The National Law Review* https://natlawreview.com

Q&A: The Risks of Social Media Spam Attacks

Article By:

Emily Holbrook

In mid-November, Facebook became the target of spam attack that infiltrated user's profile pages on which it posted disturbing images. The attack caused an uproar due to the nature of the violent and sexually explicit images. Facebook chalked it up to a **"**security bug in an internet browser**.**" But this was not the first (or, most likely, last) spam attack on the social media site. Over the Thanksgiving weekend, the Facebook community forum was flooded with spam messages that advertised links for streaming sporting events. And just today it was announced that a new worm spreading on Facebook is aiming to infect users with a data-stealing virus. Though not considered a spam attack, it is just another example of the risks of social media.

With questions on this topic, I turned to Dr. Hongwen Zhang, co-founder and CEO of Wedge Networks.

Facebook has been the target for several recent aggressive spam attacks. What makes the site so popular for spammers?

Spammers are moving their efforts away from email and towards social media, exploiting the ability to create fake profiles for free while quickly gaining a massive online presence across various platforms such as Facebook. In addition, hackers/spammers are capitalizing on the popularity of social media by manipulating end-users into downloading malicious content or browsing malicious sites. Studies conducted by security vendor Kaspersky Labs, show that social networking sites are 10 times more effective at delivering malware than previous methods of email delivery. This is a result of social media sites, such as Facebook, where development is based on human relationships and the ability to quickly and easily connect, creating a perfect breeding ground for malicious code and spam.

What were the implications of the recent Facebook spam attack?

With such a large online community, the increasing amount of spam and malware affects Facebook's operations as well as their users. While the most recent spam attack isn't new, the violent and pornographic nature of November's attack upset users more than usual, who went to their blogs, Twitter or Facebook accounts to discuss the outbreak. As of October of this year, Facebook said that spam represents less than 4% of content shared on the social networking website and affects under 0.5%, or 4 million users, on any given day. This is still a large number of people who are being affected on a daily basis and I suspect that this number only includes spam that

Facebook catches, therefore it's not 100% accurate.

Have there been any recent spam attacks on other social networking sites, such as Twitter or LinkedIn?

Twitter and LinkedIn both have faced similar attacks as Facebook, although we have not seen any published information on these attacks as large of a scale or as organized as what we saw in November with Facebook's stream of spam messages on user profiles and on their help forum. However, most social media sites follow the same principles of user-generated content on trustworthy sites and as such, hackers and spammers can quickly and easily publish their attacks on all sites and expect a similar effect. For example, there have been many documented cases of spam and malware on multiple sites at once, such as the Starbucks themed attack that used both Facebook and Twitter concurrently in November. According to Sophos, spamming on social networks rose in 2010, with 67% of people surveyed receiving spam messages, up from 57% at the end of 2009 and 33% in the middle of that year. Phishing and malware incidents were also rife, with 43% of users spotting phishing attempts and 40% receiving malware.

How can these spam attacks affect businesses who use social media for marketing purposes?

Twitter, Facebook and LinkedIn have entered the IT security landscape – bringing both advantages and dangers to your business. Organizations continue to utilize social media services for marketing and its employees utilize social media for personal usage. IT departments must balance use with control in order to protect a business in the social media world. It becomes a two-fold job:

1. Stopping Outbound Malicious Spam:

Proactively controlling outbound content mitigates the risk of disclosure, ensures appropriate information is being sent and stops the network from sending out spam or malware from your organization. Organizations need to take measures to ensure that its corporate accounts are safe. This includes limiting passwords, staying up-to-date on industry trends and providing education to staff that are managing social media accounts on behalf of the organization. In addition, outbound malware and spam threatens business relationships with customers and negatively impacts the reliability of the brand. Companies must use content protection strategies to strengthen their brand by preventing the distribution of bad outbound content, including spam and malware from their corporate IP or account.

2. Protecting You and Your Employees from the Dangers of Social Media:

Organizations must also protect their networks and assets from employees who use social media sites. With high click through rates, spam being sent through social media can damage corporate assets as well as cost organizations time and money while they clean infected devices. Inline real-time threat protection and malware analysis of all content, including hidden injected malware attacks and downloads, is necessary to efficiently analyze web traffic for malicious attacks against all endpoints. This provides organizations with the comfort of

knowing they are protected, even if their employees have been tricked.

What can businesses do to prevent, or at least minimize, the attacks?

Prohibiting employees from accessing social networking sites like Facebook, Twitter and LinkedIn is no longer realistic. Blocking and application control policies are becoming inefficient with dynamic user generated content and cross-site, drive-by attacks on good websites. Combined with access through multiple endpoints (mobile devices, PDAs and tablets), old approaches are no longer effective. Security solutions with the ability for deep content inspection give organizations the advantage of utilizing all social media, while guaranteeing compliance mandates are met and the organization is protected, regardless of what the end-user is accessing. The solutions provide visibility of the application content and the aptitude in which to apply flexible policies over users, applications and protocols based on the real-time understanding of the applications' intent.

It seems individuals and companies will always be one step behind when it comes to preventing such attacks. Hackers and spammers are just more sophisticated in terms of technical expertise. Do you agree?

I agree with this as many companies and individuals are struggling to protect themselves against attacks, especially when conventional approaches, such as blocking web access according to the reputation of the URLs, are used. However, there are innovative solutions out there that go beyond simply checking on the reputation of a link and go deep to make sure that the actual content is not malicious. These deep content inspection based solutions are effective tools to prevent the spreading of malicious content in social media use.

National Law Review, Volume I, Number 338