West Texas Cyber Security Consortium

# Mobile & Social: The Tipping Point For Cybercrime

**Spamming and scamming has moved to social media in full force, according to new research on the Twittersphere from Trend Micro.**

Social media *is* fantastic. It continues to piece together the fabric of our lives, personally and professionally. Not only can you connect and socialize with friends new and old, but you can also network with colleagues about the latest in your field from around the globe at the speed of thought. It really is up to you to control how you interact with, consume, and share content.

The number of users flocking to platforms such as Facebook, Twitter, Instagram, Pinterest, and LinkedIn is exploding. Social media continues to permeate all demographics and all countries across the globe. With a population of hundreds of millions for each given platform, social media has become quintessential in how we live and carry out our daily lives.

Cybercriminals and threat actors will always shift focus to platforms of interest and capitalize on the popularity of an ecosystem. They do this to hunt easy prey and to carry out their elaborate and sophisticated business models. Even more so, they have come to realize that many consumers are accessing these platforms from unprotected devices. This would include mobile devices and PCs not equipped with standard anti-malware and web/domain reputation services, as well as packages that take direct aim at protecting user security and privacy within the social media realms.

We have fundamentally reached a tipping point in the amount of online services we access via our mobile devices versus traditional PCs and desktops. This has created new challenges as we look to consume and browse safely among these social media services.

I have conducted informal surveys at nearly every speaking event in which I have participated. In most cases, not even 25% of the respondents indicate they have some form of security software on their mobile device. This question is usually

raised after the question of how many use their mobile device more to access the Internet than a PC. Most people in the room raise their hand after that inquiry.

Certainly, with IOS and other closed mobile app stores, it is difficult to acquire these types of security countermeasures. Android has approximately 80% of the mobile market share globally, and users can buy protection against high-risk and mobile malware attacks, in addition to web and domain reputation services to check malicious links. But many consumers and organizations are not taking these critical precautions, and the malware producers and attackers are taking notice. Social media platforms and their unprotected users are directly in their cross hairs. Ultimately, the attacker's end goal is to continue the proliferation of their craft and the long-term viability of their business model.

**The research**

Senior threat researchers from Trend Micro and Deakin University in Australia collaborated on an effort to look at nefarious Twitter activity. Communication with Twitter support was part of this process to ensure the research benefited everyone involved with the social media platform.

The researchers used the Trend Micro Smart Protection Network, our cloud-based threat intelligence platform, to parse and categorize tweets and feedback data. The e-platform collects more than 100 TB of sensor data a day, enabling the team to compile massive lists of bad web neighborhoods, files, and domains. The results were sobering and frightening. Spamming and scamming has moved to social media in full force, without question. In contrast to a similar study completed within the Twittersphere in 2010, blacklisting URLs indeed was effective at reducing the number of malicious links used in spam/scam campaigns.

Another major disconcerting factor in this research was the cascading problem resulting from the large numbers of compromised Twitter accounts. It truly is a vicious cycle. Compromised Twitter accounts can create exponential pain. Hijacked accounts trick other users into clicking on links and then continue to branch out to grab more credentials. In short, spam is sent to followers indicating that they should click on a link of interest. When the user clicks on the link from what appeared to be a trusted resource, the link produces a page that says the user's session has ended, and the user needs to log back into Twitter to read the message. Once this action occurs and the user inputs the credentials, it is game over. The user has been phished. The account becomes suspect and ripe to be hijacked with known credentials and used for malicious purposes.

This is most likely why we have seen such an increase in hijacked Twitter accounts from the news media and other highly visible industries. Couple this with the fact that many users still don't leverage two-factor authentication to protect their Twitter or other social media accounts, and you have a recipe for social media disaster. Fundamentally, this translated into 20,000 accounts a day potentially being compromised due to phishing campaigns, according to this research.

This can impact both mobile devices and traditional PCs -- anything leveraging a browser to input Twitter credentials. The Rand Corporation indicated in a recent Wall Street Journal article that compromised Twitter accounts were going for $16-$325 each within the shadow economy. Ironically, these are worth more than the going rate for stolen credit cards.

Social media platforms like Twitter are commanding the attention of threat actors. No matter if it is for hacktivism, cybercrime, or cyber-espionage, this is fertile ground for malicious intent and ill will. Actions can be leveraged to damage reputations and provide misinformation that can impact lives across the globe. Our own personal and professional brands are showcased in all of our social media activities.

Complete details on this research will be released at the Virus Bulletin International Conference this fall in Seattle. Please provide your comments in this forum, and we will be happy to try and address them. Also, check back here when the research is published in its entirety to see all the compelling findings made by the threat researchers.

http://www.darkreading.com/mobile/mobile-and-social-the-tipping-point-for-cybercrime/a/d-id/1234908?