Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

BUILDING BUSINESSES AND POTENTIAL THREATS WITH ONLINE SOCIAL NETWORKS

Many companies are turning to social networks to build and advance their business relationships. For some companies, social media are becoming more important than traditional approaches. While the acceptance of social networking tools in business environments is efficient and serves as a definite advantage, the trade-off of such an active online presence may also be risky.

Facebook Background

Facebook is one of the most popular social networking sites in the world with over 400 million members and still growing.

Facebook is one of the most popular social networking sites in the world with over 400 million members and still growing.

According to 2010 statistics recently provided by the *Website Monitoring Blog*, *Facebook's* milestones with regard to its international growth include the fact that 70 percent of its users do not come from the United States. It is also noteworthy that half of the site's total number of members log in every day.

Table 1 shows some pertinent *Facebook* statistics for 2010.

Country	Number of Users
United States	111,212,840
United Kingdom	23,449,100
Indonesia	19,528,560
Turkey	18,679,460
France	15,928,000
Italy	14,931,580
Canada	13,424,180
Philippines	10,647,100
Spain	8,861,140
Mexico	8,236,020

Table 1. *2010* Facebook *statistics*

Nothing encapsulates the Web 2.0 concept more than social networking sites such as *Facebook,* which provide users the ability to connect, communicate, and share information and other stuff with others. With billions of content posted daily, the site's challenges have been defined with in terms of facilitating interactions with personal and professional contacts and their respective locations.

TREND MICRO

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

Use of *Facebook* and Other Social Networks in Business

Facebook slowly transformed the computing landscape with its application framework. The vision of making the browser a platform is slowly materializing with every new application developed for and by *Facebook*.

According to *BNET,* social networking sites can bring about benefits to a company because maintaining online networks helps breach the walls of a corporate firewall. *Facebook* slowly transformed the computing landscape with its application framework. The vision of making the browser a platform is slowly materializing with every new application developed for and by *Facebook.*

Within3 is a social network for doctors to discuss medical journals and find unexpected collaborators. *LinkedIn, Flickr,* and *Facebook* allow people to build a global business from scratch through various connections they make on these sites. Finding talent in blogs and *Twitter* is another way by which social networking sites benefit businesses when hiring the right people. Integrated collaboration tools such as these build profile capabilities, hence creating social networks.

Social networking sites also serve as a platform for the advertising industry. They allow businesses to become known globally with ease since their members are distributed in different geographical locations.

Business Involvement in Online Social Media

Facebook is considered a business application by some companies, as more than 30 percent of their staff may be registered on the site. Computing work and social networking seemed to have merged with the sudden emergence of IT-savvy employees and employers.

Brand awareness can efficiently be realized through the *Facebook* fan interaction feature as well. In fact, insurance company Aflac uses its fan page feature to develop its brand equity and awareness through a social media program rather than via corporate presence. Allstate also uses its social media program as a tool to interact with its agents and staff.

Social media are also benefiting American Express, as one of its objectives includes meeting and communicating with small businesses and their owners to ensure their growth and success by keeping a certain level of engagement. FedEx also uses its blog and official *FedEx Facebook* page as online engagement spaces.

Companies such as Aflac, Allstate, American Express, and FedEx are finding social media tools to generate authentic responses, therefore keeping everyone engaged. However, this approach seems to be in direct conflict with another principle of utilizing the medium—protecting users from identity theft. *Facebook* contains a wealth of personal information people share with others such as their birth dates, email addresses, home addresses, family ties, and pictures. A trail of information is left behind because of active online social networking, which makes stealing one's identity a whole lot easier.

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

Malware Threats on *Facebook*

Figure 1. *Possible actions an attacker can do with a large network in a social networking site*

As an increasing number of people communicate through social networks, these will become more viable malware distribution platforms.

As an increasing number of people communicate through social networks, these will become more viable malware distribution platforms. The shift from desktop- to Web-based applications also presents a new vector for cybercriminals to abuse. Exploiting programming flaws also serves as another attack vector that can compromise a site's security measures.

TREND MICRO

Social networking site *MySpace,* for instance, was attacked in 2007 by a cross-site scripting (XSS) worm aka the Samy worm because of a security flaw that could have caused its victims to run any command such as redirecting page visitors to a malicious site. This attack gained significant media attention at the time of its release. It was also believed to be the first self-propagating XSS worm.

In line with social networking sites' security flaws, it was no surprise when the KOOBFACE malware rode this means of propagation. The KOOBFACE worm is a revolutionary malware, being the first to have a successful and continuous run through social networks. Last year saw KOOBFACE run a *Twitter* campaign to spread a malicious file detected as WORM_KOOBFACE.V. Recently, the KOOBFACE worm made a comeback as a new variant was again found in the social networking scene.

A KOOBFACE infection typically starts with a spam sent through *Facebook, Twitter, MySpace,* or some other social networking site containing a catchy message with a link to a "video." This link directs to a fake *YouTube* site where the user is prompted to install an .EXE file to be able to watch the said video. The KOOBFACE botnet is made up of several components, including this downloader, which in itself is also a malware.

KOOBFACE Components

The KOOBFACE downloader, aka the fake *"Adobe Flash* component," aims to determine what social networks the user is a member of and to connect to the KOOBFACE command and control (C&C) server to download the following components:

- **Social network propagation components.** These components may be referred to as the actual KOOBFACE worms since they are responsible for sending out messages in social networking sites that lead to the KOOBFACE downloader. More information on the KOOBFACE C&C and its propagation on social networks can be found in the research paper, "The Heart of KOOBFACE: C&C and Social Network Propagation."

> Senior advanced threats researcher Ryan Flores says, "KOOBFACE installs a Web server component into an infected machine, which effectively makes it part of its distribution network."

- **Web server component.** Senior advanced threats researcher Ryan Flores says, "KOOBFACE installs a Web server component into an infected machine, which effectively makes it part of its distribution network." More details on this KOOBFACE component can be found in "8 Things You Probably Didn't Know About KOOBFACE."

- **Ads pusher and rogue antivirus installer.** This component retrieves a command from the KOOBFACE C&C server to download a rogue antivirus software for which the user has to pay. It also opens new browser windows that have the ability to push ads or misleading warnings commonly employed by rogue antivirus.

- **CAPTCHA breaker.** This component does not solve CAPTCHA image tests through the use of sophisticated computer algorithms. Instead, it gets the infected user himself/herself to solve the challenge-response tests.

- **Data stealer.** This is a variant of the TROJ_LDPINCH malware family, which steals *Windows* digital product IDs, Internet profiles, email credentials, FTP credentials, and instant-messaging (IM) application credentials.

- **Web search hijackers.** These have the ability to intercept search queries to *Google, Yahoo, MSN, Ask,* or *Live* and to redirect them to dubious search portals.

- **Rogue Domain Name System (DNS) changer.** This modifies the DNS server of the affected machine by pointing its DNS to a rogue instead of a legitimate DNS server.

Countermeasures

A lot of social network users do not realize that the people in their contact lists should be viewed as a circle of trust. Adding a stranger to these or accepting random requests means opening data to just about anyone.

"Social networking sites keep adding to their security controls and refining their existing ones but, as in any development project, they also continue to innovate their platforms and add exciting new features. These new options need to keep up with new security features or they, too, will suffer from security weaknesses," says senior advanced threats researcher David Sancho.

Best Practices

While companies can leverage community-based online services to build their brands and to get valuable information about their customers, they should be wary of the fact that these can also become malware attack vectors if not used cautiously.

Malware exist for one major purpose alone—profit. *Facebook's* popularity is a major reason why it has been a favorite cybercriminal target. The Internet is undoubtedly a dangerous place to post general information. Sancho adds, "There have been many instances of security flaws on *Facebook* that allowed anybody to access the 'basic information' data of any user, no matter what his/her security settings were." While *Twitter* has taken some steps to keep members' data secure with its URL filtering to address threats, this is not enough to protect users in the end.

Ways to Minimize Risks in Social Networks

The following are some ways by which users can minimize risks even while engaging in social networking:

- Only publish information that you are comfortable with, depending on what you want to accomplish.

- Add only people you trust to your contact list.

- Avoid clicking unexpected links coming from people you do not know.

- Never fully trust anyone you do not know that well.

To minimize risks in social networks, senior advanced threats researcher David Sancho advises users to:

- Only publish information that you are comfortable with, depending on what you want to accomplish.
- Add only people you trust to your contact list.
- Avoid clicking unexpected links coming from people you do not know.
- Never fully trust anyone you do not know that well.

Read more best practices in our research paper, "Security Guide to Social Networks." Corporate users can refer to these prevention methods. Home offices and small and medium-sized businesses (SMBs) can further be informed of threats and prevention through these useful articles. In addition, make sure your system is protected by a solution that effectively blocks malicious URLs and prevents malware from running on systems.

With the increasing number of malware that can trigger attacks, it will not hurt to employ the necessary measures on systems that recognize dangerous components on social networking sites before actually downloading a malicious binary.

With the increasing number of malware that can trigger attacks, it will not hurt to employ the necessary measures on systems that recognize dangerous components on social networking sites before actually downloading a malicious binary.

References:

- David Sancho. (August 2009). *TrendWatch.* "Security Guide to Social Networks." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/security_guide_to_social_networks.pdf (Retrieved March 2010).
- *Digital Buzz Blog.* (March 22, 2010). *"Facebook* Facts and Figures for 2010." http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/ (Retrieved March 2010).
- Jake Swearingen. (2010). *BNET.* "Four Ways Social Networking Can Build Business." http://www.bnet.com/2403-13070_23-219914.html (Retrieved March 2010).
- Jennifer Leggio. (September 22, 2009). *ZDNet.* "Fortune 500 Series: FedEx Delivers Success Through Social Media." http://blogs.zdnet.com/feeds/?p=1685 (Retrieved March 2010).
- Jennifer Leggio. (November 9, 2009). *ZDNet.* "American Express OPEN Keeps 'Pulse' on Small Business with Social Media." http://blogs.zdnet.com/feeds/?p=2019 (Retrieved March 2010).
- Jennifer Leggio. (November 12, 2009). *ZDNet.* "What the Duck? Aflac Gets Quackin' on *Facebook."* http://blogs.zdnet.com/feeds/?p=2044 (Retrieved March 2010).
- Jennifer Leggio. (Fenruary 1, 2010). *ZDNet.* "Xerox Pushes Social Media from the Inside Out." http://blogs.zdnet.com/feeds/?p=2351 (Retrieved March 2010).
- Joey Costoya. (August 17, 2009). *TrendLabs Malware Blog.* "KOOBFACE Ramps Up Its *Twitter* Campaign." http://blog.trendmicro.com/koobface-ramps-up-its-twitter-campaign/ (Retrieved March 2010).
- Jonell Baltazar, Joey Costoya, and Ryan Flores. (October 2009). *TrendWatch.* "The Heart of KOOBFACE: C&C and Social Network Propagation." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface_final_1_.pdf (Retrieved March 2010).
- Oscar Abendan. (March 1, 2010). *TrendLabs Malware Blog.* "KOOBFACE Makes a Comeback." http://blog.trendmicro.com/koobface-makes-a-comeback/ (Retrieved March 2010).

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

- Rik Ferguson. (February 26, 2009). *TrendLabs Malware Blog.* "Rogue *Facebook* App Linked to Blackhat SEO." http://blog.trendmicro.com/rogue-facebook-app-linked-to-blackhat-seo/ (Retrieved March 2010).
- Rodney Gedda. (February 24, 2009). *Network World.* "Social Networking for Business: Plan Less for Less Pain." http://www.networkworld.com/news/2009/022409-social-networking-for-business-plan.html?page=1 (Retrieved March 2010).
- Ryan Flores. (July 9, 2009). *TrendLabs Malware Blog.* "KOOBFACE Increases *Twitter* Activity." http://blog.trendmicro.com/koobface-increases-twitter-activity/ (Retrieved March 2010).
- Ryan Flores. (October 7, 2009). *TrendLabs Malware Blog.* "8 Things You Probably Didn't Know About KOOBFACE." http://blog.trendmicro.com/8-things-you-probably-didn%E2%80%99t-know-about-koobface/ (Retrieved March 2010).
- Ryan Flores. (December 16, 2009). *TrendLabs Malware Blog.* "How KOOBFACE Makes Money." http://blog.trendmicro.com/how-koobface-makes-money/ (Retrieved March 2010).
- TopTenREVIEWS Inc. (2003–2010). *TopTenREVIEWS.* "Social Networking Websites Review: Don't Let Your Social Life Fade Away." http://social-networking-websites-review.toptenreviews.com/ (Retrieved March 2010).
- Trend Micro. (2010). *Threat Encyclopedia.* "WORM_KOOBFACE.V." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_KOOBFACE.V (Retrieved March 2010).
- Trend Micro Incorporated. (2010). *Trend Micro.* "Prevention Methods—Best Practices." http://us.trendmicro.com/us/threats/enterprise/web-threats/prevention/ (Retrieved March 2010).
- Trend Micro Incorporated. (2010). *TrendWatch.* "Awareness and Prevention." http://us.trendmicro.com/us/trendwatch/awareness-and-prevention/index.html (Retrieved March 2010).
- Website-Monitoring.com. (2010). *Website Monitoring Blog. "Facebook* Facts and Figures (History and Statistics." http://www.website-monitoring.com/blog/2010/03/17/facebook-facts-and-figures-history-statistics/ (Retrieved March 2010).

TREND MICRO