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

ISSUES AND THREATS THAT *FACEBOOK* USERS FACE

Most if not all of the 400 million active *Facebook* users would probably argue that the social networking site has become an integrated aspect of their daily lives.

Most if not all of the 400 million active Facebook *users would probably agree that the social networking site has become an integrated aspect of their daily lives. Unfortunately, users may not be aware that they face different threats every time they log in to their accounts. Just as staying connected and getting reacquainted with family and friends have become easier, even cybercriminals are now just one click away.*

Threats from Within

In 2008, the number of active *Facebook* users reached over 100 million. It was also around this time when a new worm first became notorious on the social networking site. Dubbed as "KOOBFACE," the malware family posted malicious links on users' walls by using the login credentials saved in cookie files to access user accounts. As such, it seemed as though the posted links came from registered users' *Facebook* friends, enabling the worm to leverage the trust that users place on their contacts.

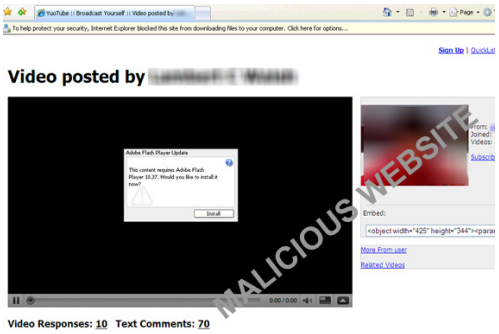

Figure 1. *Fake* YouTube *site*

While its routines were not entirely novel, the fact that KOOBFACE specifically targeted *Facebook* users made it noteworthy. With the site's users growing by the millions, cybercriminals quickly used its popularity and the false sense of security that the site creates to their advantage. The KOOBFACE gang, as its creators were called, likewise ensured that their malware stayed up-to-date. From simple links pointing to copies of the worm, a new KOOBFACE variant began sending personal messages to users. Clicking the link redirects users to a fake *YouTube* page where downloading a bogus *Adobe Flash Player* update leads to a malware infection.

The KOOBFACE malware family has since undergone major improvements, all designed to further increase its reach. These changes include a CAPTCHA-breaking component, a domain name setting (DNS) changer, a botnet upgrade to make it takedown proof, using applications for phishing attacks, a FAKEAV installer component, and a new component that imitates *Facebook* users.

A recently discovered bug, which allowed users to view the live chats of their friends, also proves that the site is not completely bug free and that other security flaws may still be discovered in the future.

TREND MICRO

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

Threats from Outside

Numerous threats targeting the site's users exist even beyond *Facebook's* walls such as spammed messages. Using this tried-and-tested tactic, spammers sent out messages supposedly from a friend who has just added the recipient to his/her social networking circle. It also arrives with a .ZIP file attachment, which is actually an executable malware.

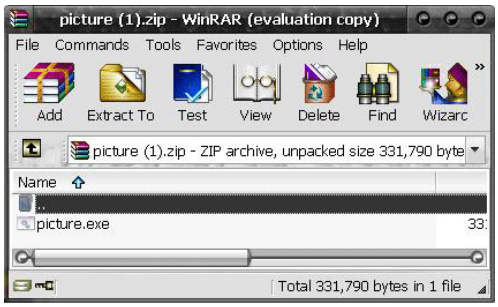

Figure 2. *Executable malware file attachment*

Another attack involves a dancing girl's video and a bogus *Facebook* website, the final payload of which is the download and installation of TSPY_PAPRAS.AX. PAPRAS variants are information stealers that launch a carnivore sniffer to retrieve passwords from network packets, which are sent to remote sites.

A more notorious information stealer, ZeuS/ZBOT, also targets *Facebook* users. Best known for stealing online banking credentials, certain variants of the ZeuS/ZBOT malware arrive via an email requesting users to update their login credentials. In another Zeus/ZBOT-related spam attack, users are not only led to a phishing page but may also be infected using a malicious .PDF file, which exploits a known *Adobe Acrobat* and *Reader* vulnerability.

The following are some issues and threats that *Facebook* users face both inside and outside the site:

- Users who log in to their accounts are in danger of:
  - Clicking malicious URLs included in posts or messages
  - Adding rogue applications to their systems
  - Encountering security flaws or bugs
  - Posting PII
- Users who receive spam are in danger of:
  - Clicking links embedded in the email body
  - Downloading attached files

These can ultimately lead to malware download or information theft.

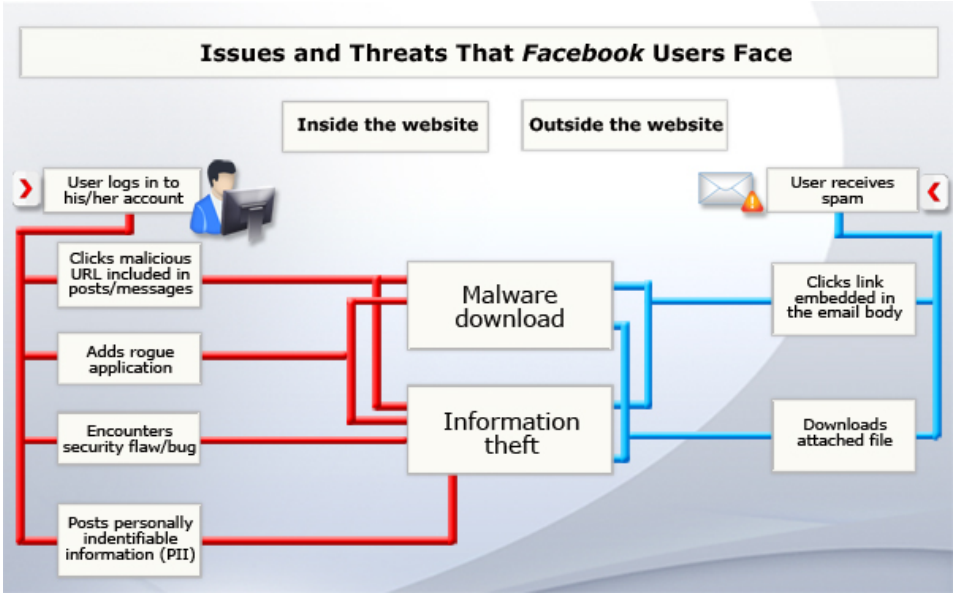

Figure 3. *Typical infection diagram for* Facebook*-related threats*

TREND MICRO

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

Building *Facebook* Safety Nets

Faced with threats both inside and outside the site, users have very little leg room left to move around in. Instead of allowing these threats to cripple them, however, staying informed and up-to-date are still the best ways to stay threat free.

While logged in to the site, users must be wary of clicking links even if these came from trusted contacts. Think twice before clicking generic-sounding posts. It is also a good idea to countercheck dubious posts and to verify if one's contacts really created questionable posts.

According to a Consumer Reports study, an estimated 1.7 million online households suffered from identity theft in 2009.

Making personally identifiable information (PII) such as one's complete birth date or home address accessible on one's *Facebook* account is a definite no-no, as these sensitive data are often used for identity verification in legal documents. In a study by Consumer Reports, an estimated 1.7 million online households suffered from identity theft in 2009. To avoid this, it would be best to assume that anything shared online will become publicly available.

Users should also be selective in adding contacts. While the site promotes expanding one's network, adding a total stranger could have dire consequences such as what happened to a teenager in the United Kingdom.

It is also advisable to use secure passwords and to avoid using the same password for all online accounts. Security experts also recommend changing one's password every six months to further help keep online information safe.

The oft-repeated reminder on unsolicited emails should likewise be kept in mind. Embedded links and attachments included in spammed messages result in either malware infection or information theft or both. It would thus be good practice to directly log in to the site by accessing it on a browser instead of clicking links inside emails.

Using a reliable security solution that provides overall smarter protection against all kinds of threats—malicious files, spammed messages, and malicious sites and domains—is critical as well. Lastly, users would greatly benefit from reading up on the latest changes on *Facebook.* By staying informed about the social networking site, users might be able to better use the site's features to their advantage.

References:

- Bernadette Irinco. (March 13, 2009). *TrendLabs Malware Blog.* "Bogus *Facebook,* Malware, and a Dancing Girl." http://blog.trendmicro.com/bogus-facebook-malware-and-a-dancing-girl/ (Retrieved May 2010).
- Helen Carter. (March 8, 2010). *The Guardian. "Facebook* Killer Sentenced to Life for Teenager's Murder." http://www.guardian.co.uk/uk/2010/mar/08/peter-chapman-facebook-killer (Retrieved May 2010).

TREND MICRO

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

- Jason Kincaid. (April 27, 2010). *TechCrunch.* "Senators Call Out *Facebook* on 'Instant Personalization,' Other Privacy Issues." http://techcrunch.com/2010/04/27/senators-call-out-facebook-on-instant-personalization-other-privacy-issues/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+Techcrunch+(TechCrunch) (Retrieved May 2010).

- Joey Costoya. (May 3, 2009). *TrendLabs Malware Blog.* "KOOBFACE Tries CAPTCHA Breaking." http://blog.trendmicro.com/koobface-tries-captcha-breaking/ (Retrieved May 2010).

- Joey Costoya. (December 15, 2009). *TrendLabs Malware Blog.* "ZBOT Targets *Facebook* Again." http://blog.trendmicro.com/zbot-targets-facebook-again/ (Retrieved May 2010).

- Jonathan Leopando. (August 19, 2009). *TrendLabs Malware Blog. "Facebook* Applications Used for Phishing." http://blog.trendmicro.com/facebook-applications-used-for-phishing/ (Retrieved May 2010).

- Jonell Baltazar. (July 22, 2009). *TrendLabs Malware Blog.* "New KOOBFACE Upgrade Makes It Takedown Proof." http://blog.trendmicro.com/new-koobface-upgrade-makes-it-takedown-proof/ (Retrieved May 2010).

- Jonell Baltazar. (September 17, 2009). *TrendLabs Malware Blog.* "Pick Your Poison: KOOBFACE or FAKEAV?" http://blog.trendmicro.com/pick-your-poison-koobface-or-fakeav/ (Retrieved May 2010).

- Jonell Baltazar. (November 10, 2009). *TrendLabs Malware Blog.* "New KOOBFACE Component Imitates *Facebook* User." http://blog.trendmicro.com/new-koobface-component-imitates-facebook-user/ (Retrieved May 2010).

- Jovi Umawing. (August 27, 2008). *TrendLabs Malware Blog.* "Worms Wriggling Their Way Through *Facebook."* http://blog.trendmicro.com/worms-wriggling-their-way-through-facebook/ (Retrieved May 2010).

- Rex Sumo. (September 25, 2008). *TrendLabs Malware Blog. "Facebook* Mystery Friend? No, Malware." http://blog.trendmicro.com/facebook-mystery-friend-no-malware/ (Retrieved May 2010).

- Rik Ferguson. (March 1, 2009). *TrendLabs Malware Blog.* "New Variant of KOOBFACE Worm Spreading on *Facebook."* http://blog.trendmicro.com/new-variant-of-koobface-worm-spreading-on-facebook/ (Retrieved May 2010).

- Robert McArdle. (February 9, 2009). *TrendLabs Malware Blog.* "Largest Bulletin PHP Board Providers Compromised." http://blog.trendmicro.com/largest-bulletin-php-board-providers-compromised/ (Retrieved May 2010).

- Ryan Flores. (June 28, 2009). *TrendLabs Malware Blog.* "New KOOBFACE Component: A DNS Changer." http://blog.trendmicro.com/new-koobface-component-a-dns-changer/ (Retrieved May 2010).

TREND MICRO

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

- Sharon Gaudin. (May 5, 2010). *PC World.* "Half of Social Networkers Post Risky Information, Study Finds." http://www.pcworld.com/article/195545/half_of_social_networkers_post_risky_information_study_finds.html (Retrieved May 2010).
- Steve O'Hear. (May 5, 2010). *TechCrunch.* "Video: Major *Facebook* Security Hole Lets You View Your Friends' Live Chats." http://eu.techcrunch.com/2010/05/05/video-major-facebook-security-hole-lets-you-view-your-friends-live-chats/ (Retrieved May 2010).
- Tony Bradley. (May 5, 2010). *PC World.* "Users Are Their Own Worst Enemy for Online Privacy." http://www.pcworld.com/businesscenter/article/195659/users_are_their_own_worst_enemy_for_online_privacy.html (Retrieved May 2010).
- Trend Micro Incorporated. (2010). *Threat Encyclopedia.* "TSPY_PAPRAS.AX." http://threatinfo.trendmicro.com/vinfo/grayware/ve_graywareDetails.asp?GNAME=TSPY_PAPRAS.AX (Retrieved May 2010).
- Verna Sagum. (November 7, 2009). *TrendLabs Malware Blog.* "Are You Being *(Facebook)* Phished?" http://blog.trendmicro.com/are-you-being-facebook-phished/ (Retrieved May 2010).

TREND MICRO