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

SLIPPING THROUGH THE CRACKS OF WEB SERVICES TO SERVE MALWARE

Today's generation of cybercriminals continue to find more ways to abuse commonly used Web services for spamming and to spread malware. Leveraging the ever-growing number of Web 2.0 and computing platforms to facilitate operations, cybercriminals have moved away from simple and straightforward sales tactics in the form of spamming to more complicated techniques to spread infection.

Misuse of Legitimate Services for Spamming

Cybercriminals have long adapted to the fast-paced technology shift to spread malware. This poses a growing and alarming trend, as the majority of sites identified on free Web services such as blogs and forums are constantly abused for malicious intent.

In recent news, *My Opera* pages were found to host malware with the discovery of a botnet script hosted on its servers. *My Opera* is the support community for the *Opera* Web browser, which offers free services such as blogging and photo sharing and serves as a social network.

Leveraging the ever-growing number of Web 2.0 and computing platforms to facilitate operations, cybercriminals have moved away from simple and straightforward sales tactics in the form of spamming to more complicated techniques to spread infection.

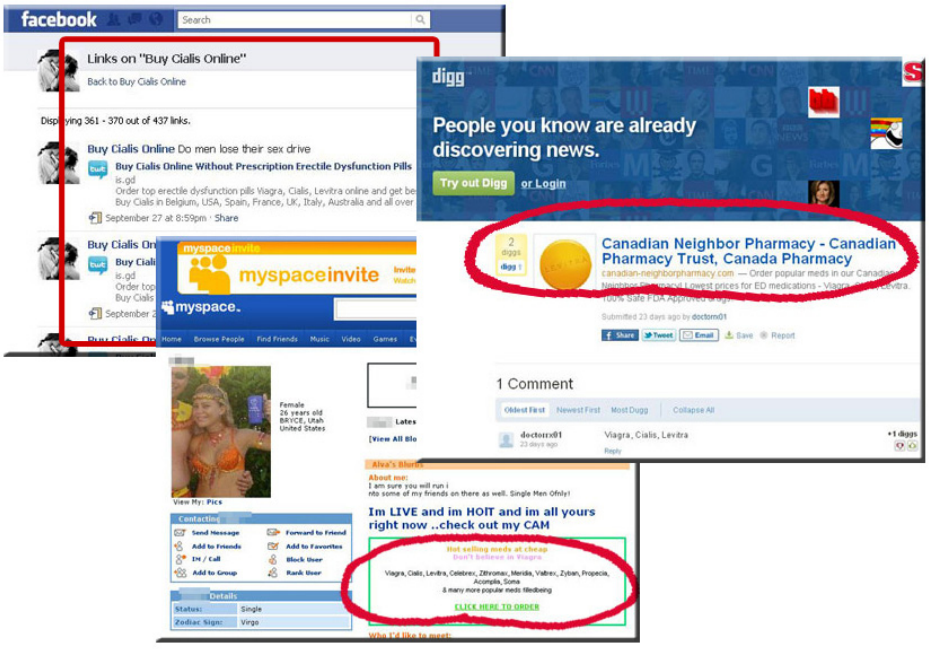

Figure 1. MySpace, Digg, *and* Facebook *pages used for ad spam*

Spammed messages were also found on a *Yahoo! Groups* page, which used embedded images to promote dating sites. Clicking the said images leads to a mail-order bride service website, which may be used for phishing.

TREND MICRO

Free blogging service *Blogspot* was also abused by spammers to redirect users to malicious sites that sell fake Rolex watches. The obvious culprit was the clever insertion of a JavaScript code, a function that *Blogspot* users are allowed to use in their blogs. This method does not veer away from the usual infection vectors. Instead, it just goes to show that given this free and legitimate service, potentially more devastating payloads have yet to unfold.

Like other free Web- or file-hosting services, *Google Groups* also serves as a place wherein cybercriminals can distribute malware and spam without having to shell out huge amounts of money for bandwidth. TrendLabs engineers have, in fact, found several poisoned search results leading to spam pages on the free service.

Google Groups is a free online discussion forum service available to anyone with or without a *Google* account. Conducting simple searches with strings like "porn," "software," "hot topics," "hot issues," and "hot events" led TrendLabs engineers to a slew of FAKEAV URLs on *Google Groups*.

Like any other free Web service, *Google Groups* was profusely abused by cybercriminals, defeating the service's intended purpose. The freedom and flexibility the service offers also effectively made it a venue for content poisoning. Thus, as long as users are allowed to register for a service, to post content, and to join several groups for free, there will be no end to such instances of platform abuse.

Google Groups' Search Engine as a FAKEAV Launchpad

Cybercriminals who peddle FAKEAV often leverage popular events, newsworthy topics, and current affairs to trick users into downloading rogue applications.

Cybercriminals who peddle FAKEAV often leverage popular events, newsworthy topics, and current affairs to trick users into downloading rogue applications. They make use of trending and popular topics found in *Google Trends* and *Yahoo!'s* Trending Now section for blackhat search engine optimization (SEO) attacks. News of celebrity deaths, juicy rumors, and gory stories have also been notable means of spreading FAKEAV, as these are always bound to stir controversy. In such attacks, users are usually led to poisoned search results that lead to either compromised or spoofed sites.

Conducting a quick search with the keyword "software" on *Google Groups,* for instance, yields several FAKEAV links on the first page. Without even utilizing many of the aforementioned blackhat SEO techniques, *Google Groups* immediately displayed FAKEAV links as top search results due to immense keyword stuffing in the message body.

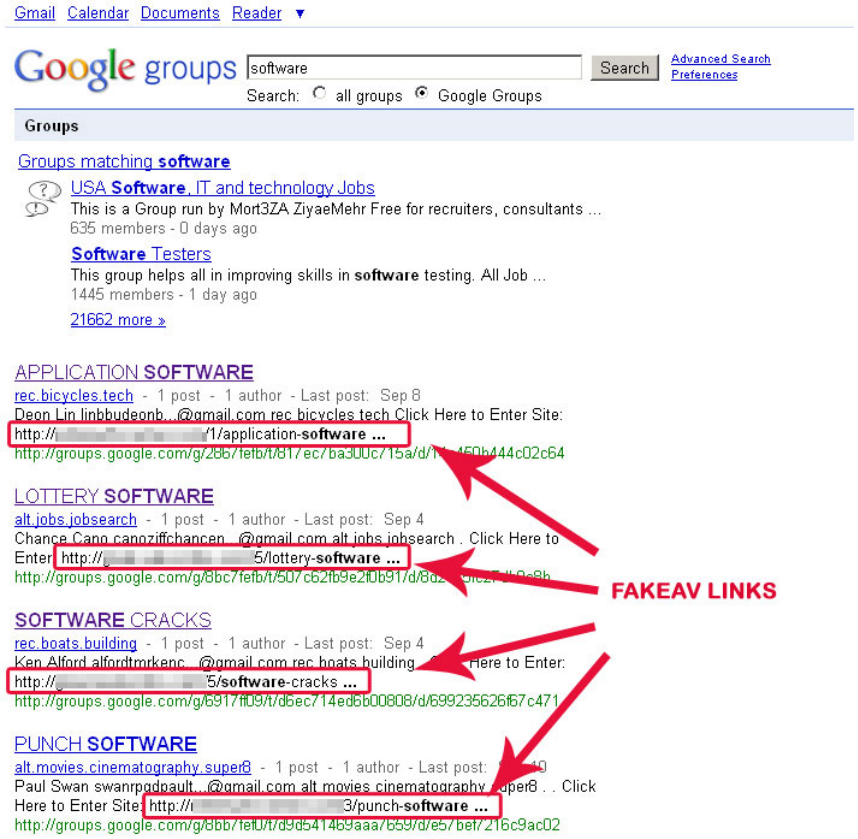

Figure 2. Google Groups *search that leads to several FAKEAV links*

Clicking the first result leads users to a page that contains a link that points to another URL that serves as a gateway to FAKEAV pages. Notice that the search strings in the URL are similar to the specific topic the user searched for, which means that the spammers used the pages they created in free Web-hosting services and in other third-party sites that allow content to be uploaded. A series of redirections will finally lead users to a final payload—a FAKEAV site—that alerts them to fake system infections and that asks them to purchase rogue software to remove supposed "malware."

Figure 3. *FAKEAV page URL in the spammed message's body*

How then do cybercriminals get away with abusing *Google Groups?*

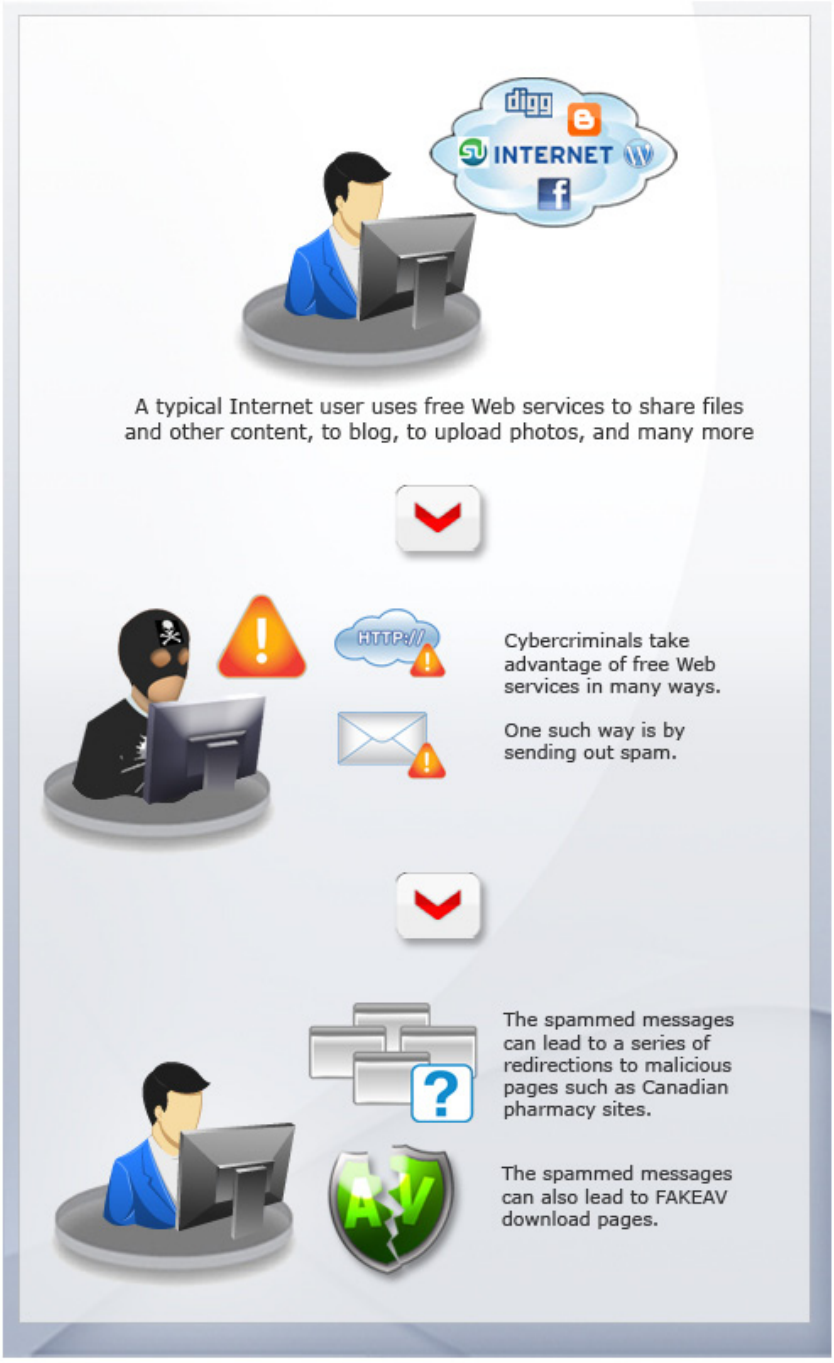

Figure 4. *How cybercriminals can abuse free Web services*

Cybercriminals are quick to adapt to turning a good thing bad. They may use specialized sites such as *Google Insights* to determine how popular certain terms and phrases are. Frequently searched keywords can also be retrieved from bot herders who leverage these to boost their own site campaigns. Zombie computers also serve as major threats to the current security industry. A herd of zombie PCs aka a botnet is remotely controlled by a group of individuals or an individual. Armies of these compromised PCs are behind some of the most notable spam, phishing, and other Web-based attacks.

Botnets have always emerged as some of the top spam sources, giving spammers access to almost-unlimited bandwidth. Realizing the presence of these distributed networks and the widespread use of free Web services such as blogs, forums, and social networking sites, it seems that security-related problems and challenges will continuously evolve.

Staying Safe from Web Threats

Cybercriminals will continuously monitor the Web to find more creative ways to infect users' systems as long as the opportunity to profit remains.

Installing security software, though advisable, is sometimes no longer enough to protect one's system. Cybercriminals will continuously monitor the Web to find more creative ways to infect users' systems as long as the opportunity to profit remains. Infecting systems then becomes a highly profitable business, especially if this translates to stealing bank account information, credit card numbers, and other personally identifiable information (PII).

Users can adopt the following best practices to minimize threats that come with the misuse of free Web services:

- Moderators should take responsibility for the groups they moderate to increase the members' level of privacy by:
  - Ensuring that only members of their groups can post messages on their pages
  - Setting the member settings so that other people can only join by invitation
  - Not listing the groups as public pages
- Users on the receiving end should fully utilize the "report as spam" option of their email inboxes. This may reinforce *Google Groups'* spam-filtering capability.
- Directly contact reputable sites or institutions that one receives email messages from to respond to requests or verify information. This allows users to verify the authenticity of the email messages that land in their inboxes.
- Be wary of the messages and links one receives from social networks like *Facebook* or *Twitter.*
- When putting up a blog, make sure that the site one signs up for does not allow people to post JavaScript code on comment boxes, as these can be used for malicious purposes. Web services such as *WordPress* already exercise safety precautions related to scripting.

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

Users should take a proactive stance toward Web threats to ultimately defend their systems from infections.

Users should take a proactive stance toward Web threats to ultimately defend their systems from infections. It will also help if users can tell a FAKEAV from a legitimate antivirus software. Avoid executing attachments or clicking links embedded in email messages, especially if these come from unknown senders or sources.

In the end, it is always important to exercise vigilance before installing suspicious-looking programs or before conducting searches on the Web.

References:

- David Sancho. (September 16, 2010). *TrendLabs Malware Blog.* "How Cybercriminals Hide Behind Multiple Web Layers." http://blog.trendmicro.com/how-spammers-hide-behind-multiple-web-layers/ (Retrieved October 2010).
- Det Caraig, (October 19, 2009). *TrendWatch.* "'Trendy' Search Results Lead to FAKEAV." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/101909_-_security_spotlight_44_-____trendy____search_results_lead_to_fakeav.pdf (Retrieved October 2010).
- Erika Mendoza, Jasper Manuel, and Roland Dela Paz. (August 27, 2010). *TrendWatch.* "Why FAKEAV Persist." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/66_why_fakeav_persist__august_27__2010_.pdf (Retrieved October 2010).
- John Resig. (October 27, 2009). *John Resig. "Google Groups* Is Dead." http://ejohn.org/blog/google-groups-is-dead/ (Retrieved October 2010).
- Lucian Constantin. (September 24, 2010). *Softpedia. "My Opera* Pages Used to Host Malware." http://news.softpedia.com/news/My-Opera-Pages-Used-to-Host-Malware-158007.shtml (Retrieved October 2010).

TREND MICRO