

THE PERILS THAT MALVERTISEMENTS POSE

How many ads do you typically see every time you open a page while surfing the Web? Have you ever had the misfortune of accidentally clicking an ad? Where and what did it lead you to? Did you know that malicious advertisements or malvertisements are typically employed as malware infection vectors and can pose grave security risks to users like you? Read on to find out what malvertisements are, how these can affect you, and how you can protect yourself from the perils these pose.

AD-SUPPORTED FACEBOOK APPLICATION ANYONE?

A Facebook application tied to malvertisements recently surfaced. The ad-supported application led users to a series of redirections that ended on a page that hosted exploits. Some of the exploits used in the attack targeted vulnerabilities in *Internet Explorer (IE)* and *Java*. Successful exploitation of the said vulnerabilities led to the download of other malicious files onto affected systems. It also allowed remote attackers to execute malicious commands on affected systems, thus compromising their security. Based on TrendLabs analysis, the malvertisements automatically loaded without the users' knowledge, starting the infection chain with the simple act of accessing the ad-supported Facebook application.

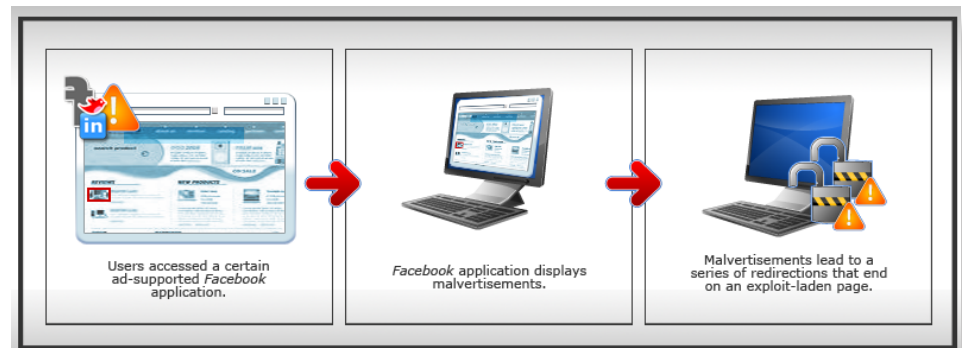
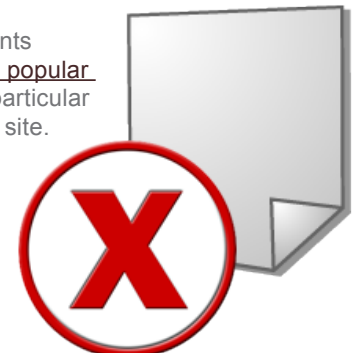


Figure 1. How the ad-supported Facebook application redirected users to exploit-laden pages

MALVERTISEMENTS AS MALWARE DISTRIBUTORS

The above-mentioned incident is yet another example of how cybercriminals utilize malvertisements to victimize users. Over the years, Trend Micro has been reporting about similar attacks such as the following:

- At one time, users were victimized by malvertisements pointing to malicious sites while browsing through a popular webmail service provider's site. In this attack, one particular ad redirected victims to a vulnerability exploit-laden site. Users who landed on the site the ad pointed to unknowingly downloaded two Trojans disguised as .PDF files onto their systems and executed a malicious JavaScript.



After careful analysis, TrendLabs engineers found that the malicious .PDF files exploited several vulnerabilities in *Adobe Reader* and *Acrobat* while the malicious JavaScript exploited a bug in *Microsoft Virtual Machine (VM)*. Successful exploitation of the said bugs all led to the download of more malicious files onto already-infected systems, putting affected users at even greater risk.

- In another incident, users browsing through the *New York Times* site were met by [a malicious pop-up ad](#) warning them of a system infection. The said ad for a rogue antivirus software called *Personal Antivirus* boasted of having the capability of ridding systems of malware infections for a small sum of money. Since the antivirus software was fake, the incident prompted the *New York Times* staff to issue an advisory telling users that the pop-up ad was a malvertisement and that they should not click it.



Figure 2. Fake scanning window the Personal Antivirus malvertisement victims see

- Malvertisements also turned up as [a sponsored result](#) for users in search of *Chrome* download sites via *Bing* at one time. The said ad redirected victims to a spoofed page where clicking the *Download* button led to [a Trojan spyware infection](#) instead of *Chrome* browser installation. Analysis revealed that the spyware added malicious strings to infected systems' *Windows HOSTS* file that redirected users to a phishing site.

Malvertisements are usually found on legitimate sites to trick users into thinking they are the real deal. Even worse, victims do not even have to visit malicious sites to end up with compromised systems. When clicked, malvertisements typically lead to malicious web pages that either host exploit packs or install malware in victims' systems. The malware some malvertisements lead to are often related to pay-per-install (PPI) or pay-per-click (PPC) affiliate schemes. Note, however, that even legitimate ads are also used in various malicious PPC schemes.

More Installations or Clicks, More Money

Cybercriminals profit from spreading malvertisements via the use of one of two business models—PPI or PPC.

In the PPI business model, clients develop malicious software that providers, aka “middlemen,” distribute to their affiliates. The affiliates then spread the malicious software via malvertisements or spam. How? Users who unwittingly click a malvertisement are redirected to a page that hosts malicious software or malware. Each malicious software (typically [FAKEAV variants](#)) or malware (e.g., [BREDOLAB variants](#)) installation in users' systems translates to profit for the cybercriminals behind each scheme.



In some cases, malware-laden systems end up becoming unwilling participants in click-fraud schemes, acting as another income source for the cybercriminals.

In the PPC business model, on the other hand, cybercriminals hijack search results to lead users to their traps. How does this work? PPC providers give cybercriminals access to their ad URL database. The ad URLs are then tied to frequently searched keywords. Users who click rigged search results are led to the ad URLs the PPC providers gave. Every click translates to profit for the cybercriminals behind the schemes. In essence, PPC providers act as “middlemen” between legitimate ad providers and bot masters. Cybercriminals typically leverage legitimate advertising companies to get placements on sites that use online banners. The malicious online banners point users to sites that host exploit packs.

A couple of weeks ago, Trend Micro researchers, in collaboration with the Federal Bureau of Investigation (FBI), the Estonian Police, and other industry partners discovered [a botnet operation](#) that compromised 4 million systems. The said botnet earned money primarily via click-fraud schemes and distributing Domain Name System (DNS)-changing Trojans. Changing the DNS settings of users’ systems allowed cybercriminals to lead their victims to malicious sites. DNS-changing Trojans can also replace the ads that users frequently click.

Apart from FAKEAV and BREDOLAB variants, KOOBFACE and TDSS variants are also frequently associated with the PPI business model. Note, however, that the PPI and PPC business models are both legitimate. Cybercriminals just used them for their own malicious gains. Case in point, the KOOBFACE gang earned [a whopping US\\$2 million](#) from June 2009 to June 2010 using both business models.

It is therefore not surprising why cybercriminals use malvertisements for their operations. A lot of people click online ads, as shown by the rise in online advertising. In fact, the North American online advertising spending as of June this year amounted to [US\\$33.4 billion](#). In addition, the Asia/Pacific online advertising spending is expected to increase from US\$16.4 billion in 2010 to US\$34.6 billion by 2015.



The North American online advertising spending as of June 2011 amounted to US\$33.4 billion.



Figure 3. Worldwide online advertising spending from 2010 to 2015

Bad Ads and Security Risks

Malvertisements put users at risk because these act as readily accessible avenues for malware to get into systems. As has been said, users do not even need to access malicious sites for their systems to get infected. Malware variants like FAKEAV and HILOTI, for instance, have been known to serve malicious ads to redirect victims to sites that host other malicious files.

Moreover, malvertisements can act as a gateway for exploits to certain system vulnerabilities. As such, systems that are not regularly patched run risks of being infected. Apart from compromising systems' security, falling prey to malvertisements can also lead to identity and information theft. Should cybercriminals decide to sell the information they steal to the highest bidders, they stand to earn even greater profits.



Please help us improve our articles and other write-ups by participating in a quick survey. Just click the image above to start.

HOW TO BATTLE MALVERTISEMENTS

Powered by the Trend Micro™ Smart Protection Network™ infrastructure, Trend Micro security products' web reputation technology effectively blocks user access to all known malicious URLs, thus preventing the download of malicious files. The technology also breaks the infection chain by blocking access to exploit-laden sites. File reputation technology, meanwhile, detects all known malware that users may download onto their systems by clicking malvertisements.

For a free system scan, use the Trend Micro free tool HouseCall. In addition, Web Protection Add-On can help users avoid accessing malicious sites.

Users are strongly advised not to click the ads or pop-up messages they see online. Note that even trusted legitimate sites can be compromised to serve malvertisements. They should also keep their patch levels up-to-date, as clicking malvertisements can lead to vulnerability exploitation. Clearing their browser caches is also a good practice. Finally, awareness is key. Stay abreast of the latest threats to avoid becoming a victim of system redirection, malware infection, vulnerability exploitation, and information or worse identity theft.



REFERENCES

- Brooks Li. (October 4, 2011). *TrendLabs Malware Blog*. "Facebook Malvertisement Leads to Exploits." <http://blog.trendmicro.com/facebook-malvertisement-leads-to-exploits/> (Retrieved November 2011).
- David Perry. (July 6, 2011). *TrendLabs Malware Blog*. "Well, Bing My Google!" <http://blog.trendmicro.com/well-bing-my-google/> (Retrieved November 2011).
- eMarketer Inc. (June 13, 2011). *eMarketer: Digital Intelligence*. "Worldwide Ad Market Approaches \$500 Billion." <http://www.emarketer.com/PressRelease.aspx?R=1008479> (Retrieved November 2011).
- Feike Hacquebord. (November 9, 2011). *TrendLabs Malware Blog*. "Esthost Taken Down—Biggest Cybercriminal Takedown in History." <http://blog.trendmicro.com/esthost-taken-down---biggest-cybercriminal-takedown-in-history/> (Retrieved November 2011).
- Nart Villeneuve. (November 12, 2010). *nartv.org*. "KOOBFACE: Inside a Crimeware Network." <http://www.nartv.org/mirror/koobface.pdf> (Retrieved November 2011).
- Nart Villeneuve. (2011). *TrendWatch*. "Targeting the Source: FAKEAV Affiliate Networks." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/targeting_the_source-fakeav_affiliate_networks.pdf (Retrieved November 2011).
- Rik Ferguson. (September 14, 2009). *CounterMeasures*. "New York Times Pushes FAKEAV Malvertisement." <http://countermeasures.trendmicro.eu/new-york-times-pushes-fake-av-malvertisement/> (Retrieved November 2011).
- Trend Micro Incorporated. (2009). *TrendWatch*. "Trend Micro Threat Advisory: BREDOLAB Poses Increasing Pain Point." <http://us.trendmicro.com/us/trendwatch/current-threat-activity/bredolab/> (Retrieved November 2011).
- Trend Micro Incorporated. (March 2010). *Threat Encyclopedia*. "JS_BYTEVER.AX." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=JS_BYTEVER.AX (Retrieved November 2011).
- Trend Micro Incorporated. (March 2010). *Threat Encyclopedia*. "TROJ_PIDIEF.GBA." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=TROJ_PIDIEF.GBA (Retrieved November 2011).
- Trend Micro Incorporated. (March 2010). *Threat Encyclopedia*. "TROJ_PIDIEF.GBB." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=TROJ_PIDIEF.GBB (Retrieved November 2011).
- Trend Micro Incorporated. (July 2011). *Threat Encyclopedia*. "TSPY_ONLINEG.MU." http://about-threats.trendmicro.com/Malware.aspx?language=us&name=TSPY_ONLINEG.MU (Retrieved November 2011).
- Valerie Boquiron. (March 16, 2010). *TrendLabs Malware Blog*. "Malicious Ads Lead to PDF Exploits." <http://blog.trendmicro.com/malicious-ads-lead-to-pdf-exploits> (Retrieved November 2011).