

CELEBRITY NEWS ROLL OUT THE RED CARPET FOR CYBERCRIME

Users flock to the Internet for the latest news on their favorite celebrities, awards shows, and other entertainment events. Unfortunately, cybercriminals also take this opportunity to reach out to a large base of targets for their profiteering schemes.

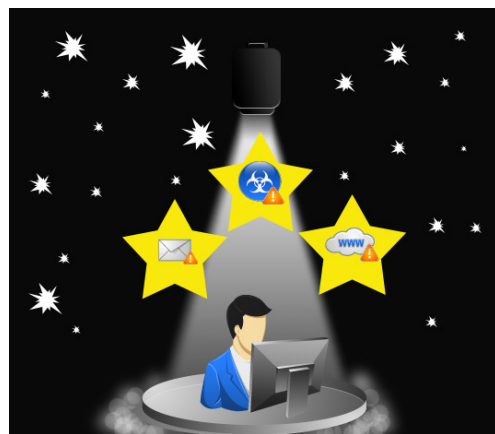
How Entertainment Paves the Way for Security Threats

The Internet is arguably the world's preferred information source when searching for the latest news and events. Apart from providing a rich multimedia experience and from boasting interactive features, Web content is also updated in real time and is available from virtually anywhere at anytime.

Some of the most sought-after news online concern celebrities and show business.

Browsing for entertainment news has become a popular pastime among Internet users. In fact, this year, *Yahoo! omg!*, *People*, and *TMZ* posted more than **16 million unique visitors each**, as estimated by eBizMBA. *Yahoo! omg!* topped the list with an estimated 24.5 million unique visitors in the featured month.

A comScore study in 2009 also confirmed that U.S. online users **spent approximately 15 million hours on entertainment sites**. These studies confirm the existence of a large entertainment site following and the so-called celebrity culture. In this light, cybercriminals are expected to utilize this venue even more.



Cybercriminals Hog the Spotlight

The above-mentioned facts, of course, did not escape the prying eyes of cybercriminals, as they are known for seizing every opportunity to make as much money as they can. Users in search of entertainment news via *Google* and other search engines may, for instance, easily fall prey to a multitude of security concerns, topmost of which are blackhat search engine optimization (SEO)-FAKEAV infections.

The Blackhat SEO-FAKEAV Tandem

FAKEAV variants are notorious for effectively leveraging social engineering tactics. The cybercriminals behind FAKEAV make use of popular topics, particularly entertainment news. FAKEAV malware infect systems via different vectors, including spam and sites that openly market their variants as legitimate antivirus software, these are best known as blackhat SEO payloads.



Please help us improve our reports by taking our quick survey.

SEO is a legitimate marketing and promotional practice, as it increases the visibility of Web sites by increasing their page ranking in search results. Cybercriminals, however, also **employ the same technique** to lure unknowing users in search of information to so-called poisoned results that ultimately lead to FAKEAV-hosting sites.

Over the past years, TrendLabsSM has come across several blackhat SEO-FAKEAV cases that leveraged topics like the deaths of celebrities and well-known awards shows. These include the following:

- Sometime in March last year, the “Kids’ Choice Awards” was used for a FAKEAV campaign. Users in search of information related to the said show were served poisoned results that led to sites that hosted **TROJ_FRAUDLO.IA**.
- Sites supposedly containing news on **Brittany Murphy’s untimely death** in December 2009 also led users to sites that have been injected with the malicious script **HTML_FAKEAV.WAF**. Users who mistakenly clicked poisoned links saw fake message prompts and scanning results. Even worse, however, the malicious script accessed several URLs to download more files, including **JS_RENOS.WCJ** and **TROJ_KRAP.DAM** onto infected systems.
- **Farrah Fawcett’s death** in June 2009 was not spared as well. Users who clicked links to several sites hosted on is-the-boss domains ended up with **TROJ_FAKEAV.BBM** infections.

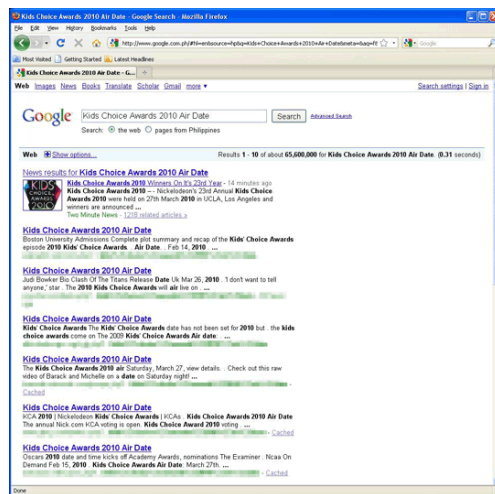


Figure 1. Poisoned search results for “Kids’ Choice Awards” in 2010

Each year, TrendLabs engineers monitor various possible search strings that may turn up poisoned results. The following list comprise just some of the top Emmy Awards-related search strings our engineers monitored last year:

- 2010 Emmys
- 2010 Emmy winners
- Best and Worst Dressed Emmys
- Emmy awards
- Emmy awards 2010



Please help us improve our reports by taking our quick survey.

This year, our engineers are also monitoring keywords related to two of the biggest awards shows—the Oscars and the Grammys—that may be used for blackhat SEO-FAKEAV runs, which include the following:

- Javier Bardem
- James Franco
- Nicole Kidman
- Jennifer Lawrence
- Mark Ruffalo

FAKEAV Spam

As previously mentioned, cybercriminals use every single trick in the book to profit off users' misery. Apart from blackhat SEO, they also used spam riding on the popularity of celebrities like Michael Jackson to spread malware. One particular spam run used email messages supposedly from *CNN Mexico* that contained bogus links to never-before-seen videos of the King of Pop. Even though some of the links in the said messages were inaccessible, one link redirected users to a page that was injected with **HTML_DLOADR.ARM**. This script prompted the display of a prompt that urged users to download a fake *Adobe Flash Player* installer, which was actually a backdoor detected by Trend Micro as **BKDR_IRCBOT.BW**.

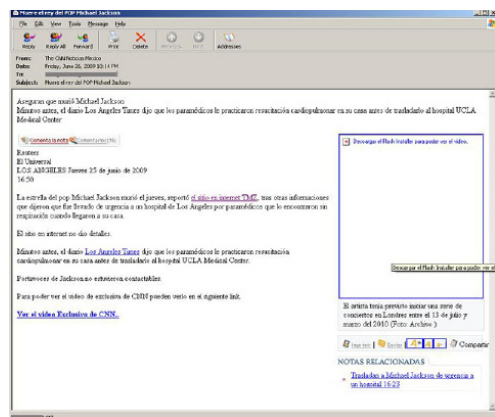


Figure 2. Malware-laden Michael Jackson video spam

Why Should Users Care?

Apart from cleverly manipulating SEO technology and using social engineering techniques, FAKEAV infections also prey on users' desire to keep their systems and data secure. FAKEAV malware are known for displaying fake warnings and scanning results to inform users of system infections. These then urge users to purchase rogue antivirus software. Cases such as when cybercriminals used the "Kids' Choice Awards" also put young users at risk, as they were more likely to search for information on the event.

▶ Apart from cleverly manipulating SEO technology and using social engineering techniques, FAKEAV infections also prey on users' desire to keep their systems and data secure.



Please help us improve our reports by taking our quick survey.

Payloads like BKDR_IRCBOT.BW were also considered huge threats, as these connected to Internet Relay Chat (IRC) servers and joined specific channels without the users' consent. This and similar malware payloads also received and sent commands from remote users that could compromise infected systems' security. These can also lead to data loss or theft, as backdoor programs are known for monitoring users' activities, depending on what their malicious creator's intention is.

The previously mentioned comScore study also noted that American users were more likely to view entertainment sites from their workplaces. comScore, in fact, estimated that users spent almost half of their total reading time within their workday. This means threats that plague users at home can also affect their workplaces. Businesses should take note of this, as their employees may unwittingly fall prey to threats that leverage celebrity news, which can lead to system or, worse, network infection.

Protection Should Take Center Stage

No matter how cunning cybercriminals become, the key to ensure secure online experiences is to remain vigilant and to observe safe computing practices. Users should always be cautious of clicking links that appear as search results even if these are top-ranking ones.

• **No matter how cunning cybercriminals become, the key to ensure safe online experiences is to remain vigilant and to observe best computing practices.**

The safest option is to directly access trustworthy entertainment news sites. With regard to email messages that promise the latest celebrity news or exclusive scoops, users must think twice before clicking the links embedded in them. It is still best to immediately delete dubious-looking email messages from one's inbox.

Here are some **signs of the most common payload of falling for celebrity-related scams—FAKEAV infection**:

- **Slow computer performance.** Infected systems take longer to reboot or to connect to the Internet.
- **New desktop shortcuts or switched home pages.** Some rogue antivirus software change an infected system's Internet settings such as the home page. These may also add new desktop shortcuts or change a system's wallpaper.
- **Annoying pop-up windows.** Several FAKEAV applications bombard affected users with annoying pop-up messages even when they are offline in an attempt to convince them to buy fake antivirus software.
- **Blue-screen errors.** Rogue antivirus software also pretend to cause blue-screen errors with the use of convincing images to urge users to buy the products.
- **Constant system rebooting.** Some FAKEAV malware cause infected systems to repeatedly reboot while automatically downloading software from links.
- **Connecting to adult sites.** Some FAKEAV malware also cause infected systems to access adult sites without the users' permission.



Please help us improve our reports by taking our quick survey.

- **Memory issues.** Last but not least, some FAKEAV malware can corrupt infected systems' secondary memory or boot sectors, which prevent these from properly booting up.

To stay protected, however, it is still best for users to invest in a **security software** that detects potential threats even before these reach their systems.

References:

- Argie Gallego. (June 29, 2009). *TrendLabs Malware Blog*. "Michael Jackson Video Leads to Malware Download." <http://blog.trendmicro.com/michael-jackson-video-leads-to-malware-download/> (Retrieved February 2011).
- Det Caraig. (December 21, 2009). *TrendLabs Malware Blog*. "News on Brittany Murphy's Death Lead to FAKEAV." <http://blog.trendmicro.com/news-on-brittany-murphy%E2%80%99s-death-lead-to-fakeav/> (Retrieved February 2011).
- eBizMBA Inc. (February 1, 2011). *eBizMBA*. "Top 15 Most Popular Gossip Web Sites: February 2011." <http://www.ebizmba.com/articles/gossip-websites> (Retrieved February 2011).
- Macky Cruz. (June 25, 2009). *TrendLabs Malware Blog*. "Blackhat SEO Quick to Abuse Farrah Fawcett Death." <http://blog.trendmicro.com/blackhat-seo-quick-to-abuse-farah-fawcett-death/> (Retrieved February 2011).
- Sarah Radwanick. (July 1, 2009). *comScore*. "More Americans Reading Entertainment News Online, with Much of It Occurring During Work Hours." http://www.comscore.com/Press_Events/Press_Releases/2009/7/More_Americans_Reading_Entertainment_News_Online_With_Much_of_it_Occurring_during_Work_Hours (Retrieved February 2011).
- Sheryll Tiauzon. (March 30, 2010). *TrendLabs Malware Blog*. "'Kids' Choice Awards' Used for FAKEAV." <http://blog.trendmicro.com/kids-choice-awards-used-for-fakeav/> (Retrieved February 2011).
- Ryan Flores. (November 2010). *TrendWatch*. "How Blackhat SEO Became Big." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/how_blackhat_seo_became_big__november_2010_.pdf (Retrieved February 2011).
- TrendLabs. (June 2010). *TrendWatch*. "Unmasking FAKEAV." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/unmasking_fakeav__june_2010_.pdf (Retrieved February 2011).
- Trend Micro Incorporated. (January 2011). *Threat Encyclopedia*. "TROJ_KRAP.DAM." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=TROJ_KRAP.DAM (Retrieved February 2011).
- Trend Micro Incorporated. (December 2010). *Threat Encyclopedia*. "TROJ_FRAUDLO.IA." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=TROJ_FRAUDLO.IA (Retrieved February 2011).



Please help us improve our reports by taking our quick survey.

- Trend Micro Incorporated. (July 2010). *TrendWatch*. "FAKEAV: The Growing Problem." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/threatbrief_final.pdf (Retrieved February 2011).
- Trend Micro Incorporated. (December 2009). *Threat Encyclopedia*. "BKDR_IRCBOT.BW." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=BKDR_IRCBOT.BW (Retrieved February 2011).
- Trend Micro Incorporated. (December 2009). *Threat Encyclopedia*. "HTML_FAKEAV.WAF." http://about-threats.trendmicro.com/Malware.aspx?language=us&name=HTML_FAKEAV.WAF (Retrieved February 2011).
- Trend Micro Incorporated. (December 2009). *Threat Encyclopedia*. "JS_RENOS.WCJ." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=JS_RENOS.WCJ (Retrieved February 2011).
- Trend Micro Incorporated. (June 2009). *Threat Encyclopedia*. "HTML_DLOADR.ARM." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=HTML_DLOADR.ARM (Retrieved February 2011).
- Trend Micro Incorporated. (June 2009). *Threat Encyclopedia*. "TROJ_FAKEAV.BBM." http://about-threats.trendmicro.com/Malware.aspx?language=us&name=TROJ_FAKEAV.BBM (Retrieved February 2011).



Please help us improve our reports by taking our quick survey.