Digital Music and Movies Report

The true cost of free entertainment

By Paula Greve

Introduction

Today's consumers, hungry for entertainment, are increasingly turning to online media such as digital movies, music, TV, radio, and videos. In fact, more than 177 million U.S. Internet users watched online video in June of this year alone, up from 157 million a year ago, according to comScore, Inc. While adults may click on streaming video to stay abreast of world news, teens search for posters from their favorite movie or the ringtone of the latest Lady Gaga hit. And consumers everywhere want to visit fan sites, download movies, or indulge in the latest celebrity news. Online media gives it all to us, quickly and easily, but at a price.

It used to be It used to be that poisoned search results—with links to malware—were the number one risk consumers faced when looking for digital entertainment and information. But recently, Internet users have become more aware of this threat, and cybercriminals have shifted their lines of attack to dangerous websites, malicious ads, and video viewing tools designed to do harm. Cybercrooks also know that we are hooked on social networks and video services such as YouTube, so they use these destinations to distribute malware and other threats. YouTube, for instance, had 144.5 million unique viewers in June, according to comScore, making it highly attractive to cybercriminals looking to target mass audiences.

What's more, cybercrooks take advantage of our fascination with breaking news and hot topics to get us to click on spam emails or download so-called "must-see videos." For example, a cybercrook might target younger Internet users with a spam email about teen singer Miley Cyrus, knowing that some kids are probably Cyrus fans (and also knowing that younger Internet users are generally more naive about security best practices).

So, what are all the risks associated with today's online media, and what can you do to avoid them?

Cybercrooks take advantage of our fascination with breaking news and hot topics to get us to click on spam emails or download so-called "must-see videos."

This report gives you an informative look at the dangers associated with digital music, movies, and other forms of online media so that you can understand the risks and protect yourself and your family.

Here's a summary of key findings:

- **"Free" can be costly**—Adding the word "free" to a search for music ringtones results in a three-fold increase in the riskiness of the sites returned by major search engines in English. Translating "free" to the appropriate foreign language word had similar results in other native search engines.
- **MP3s add risk**—Searching for "MP3s" adds risk to music search results, while searching for "free MP3s" makes music search results even riskier. Even when a consumer indicates that they want to pay for the MP3 in their search, results still send them to pirated content.
- **"Fans" attract dangerous URLs**—McAfee has discovered thousands of malicious and highly suspicious URLs associated with fan clubs or comments made on fan pages, even if the comments are made via social avenues such as Facebook, MySpace, YouTube, and Twitter.
- **Bad ads run rampant**—Malicious advertising (where an online ad is used to distribute malware or exploit the user's browser) is a common means of infection. For instance, on June 1, 2010, McAfee identified "malvertising" on perezhilton.com that redirected users to a domain that delivered a malicious payload.

- **Illegal content sites often fool consumers**—Sites that are set up to distribute illegal content are very sophisticated and may leave a user not understanding the nature of the site to which they have been directed. These sites often distribute malware and expose users to other risks. The criminal associations behind the sites can often be found by tracking the ownership of the domains and the relationships and tools that were used to develop the sites.

Digital Movie Risks

Focusing on movies, our research revealed that these types of threats revolve around traffic and trends. Whether it's screensavers or the latest in-demand movie, cybercriminals are attracted to sites that draw the most consumer interest.

Streaming media: radio, TV and live video feeds

Video is an expected component of most sites and, according to Target Marketing, 71% of Internet users watch streaming video. The popularity of Internet videos is not surprising, given that searching online for a live video feed or news story can be the fastest and most convenient way for a consumer to stay up to date. Consumers are drawn to videos about world events, such as the earthquake in Haiti, or sporting events such as the U.S. National Collegiate Athletic Association (NCAA) March Madness, or the Fédération Internationale de Football Association (FIFA) World Cup.

On the downside, the sheer demand for streaming content makes it very appealing to cybercriminals. For example, in April 2010, McAfee identified websites hosted in Russia and Brazil that were advertising images and videos for the FIFA 2010 World Cup. But instead of leading to World Cup content, they actually advertised rogue anti-virus programs, phished for the consumer's personal or financial information, or attempted to install malware on the user's computer.

This streaming radio dance music website from the Czech Republic has been exploited with the Conficker worm, which uses this site to send or retrieve information for malicious purposes.

"Free" movies, screensavers and posters

How safe is it to search online for movie-related information, such as ratings, reviews, and theaters? Surprisingly safe! However, consumers encounter significant risk when they search for "free" movies or "free screensavers" related to movies. In addition, movie posters and photos often hold unwanted surprises.

McAfee first became aware of movie-related threats in 2009 when the *New Moon* trailer debuted at the MTV Music Awards. The very next day, McAfee researchers noted the sudden appearance of various malware-infected *New Moon* poster .JPG and .GIF files in places across the Internet, such as fan forums and wiki pages. Since that time, this trend has continued for high profile, much-anticipated movies.

In general, when people look for entertainment content and information without realizing where it is coming from or without knowing the legitimacy of the site they are on, they are exposed to more risk.

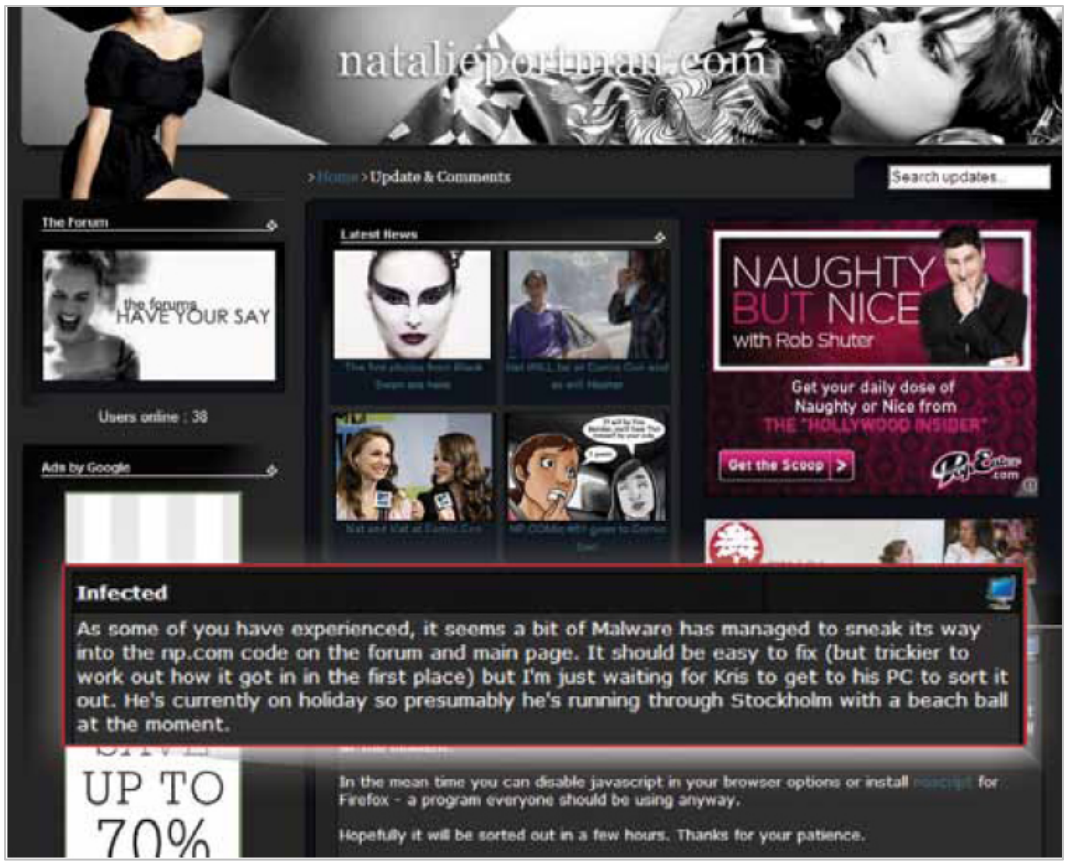
Movie fan sites

McAfee® Labs™ found more risk on various movie star fan sites. When a well-meaning movie fan, who may have little knowledge of security, visits a website to follow a celebrity that he or she admires, they often eventually find the celebrity site infected and compromised.

However, many times the attacks aren't even that sophisticated. Anyone can post a link to a malicious website or post a picture that is embedded with malware. Historically, these minor (low-traffic) sites are the easiest and most successful at infecting users. In fact, it is fairly common to find multiple fan sites built by cybercriminals with the express purpose of attempting to corral traffic to sell ads or infect users.

Minor sites owned by well-meaning movie fans are less likely to notice the security breach and therefore clean them up. McAfee has discovered a number of such sites that still retain traces of attacks that occurred several months prior.

It is fairly common to find multiple fan sites built by cybercriminals with the express purpose of attempting to corral traffic to sell ads or infect users.



One example is a fan site about Natalie Portman. It became infected with malicious JavaScript.

Movies

Movies that are not yet widely available are known to be highly popular search targets by cybercriminals who anticipate that a large number of people will be searching for these films online.

Consumers are wading into dangerous waters when they search for movies that are only in local theaters and not available globally or when they search for movies that are not yet available, such as the latest Harry Potter film.

Cybercrooks lay traps by advertising these in-demand movies. The crooks give consumers fake anti-virus security software scams, dangerous tools (that are supposedly designed to help users download and view films or shows), or drive-by exploits/downloads. (A “drive-by” attack occurs on the user’s PC with no action required by the consumer, so he or she is not even aware that it has occurred.)

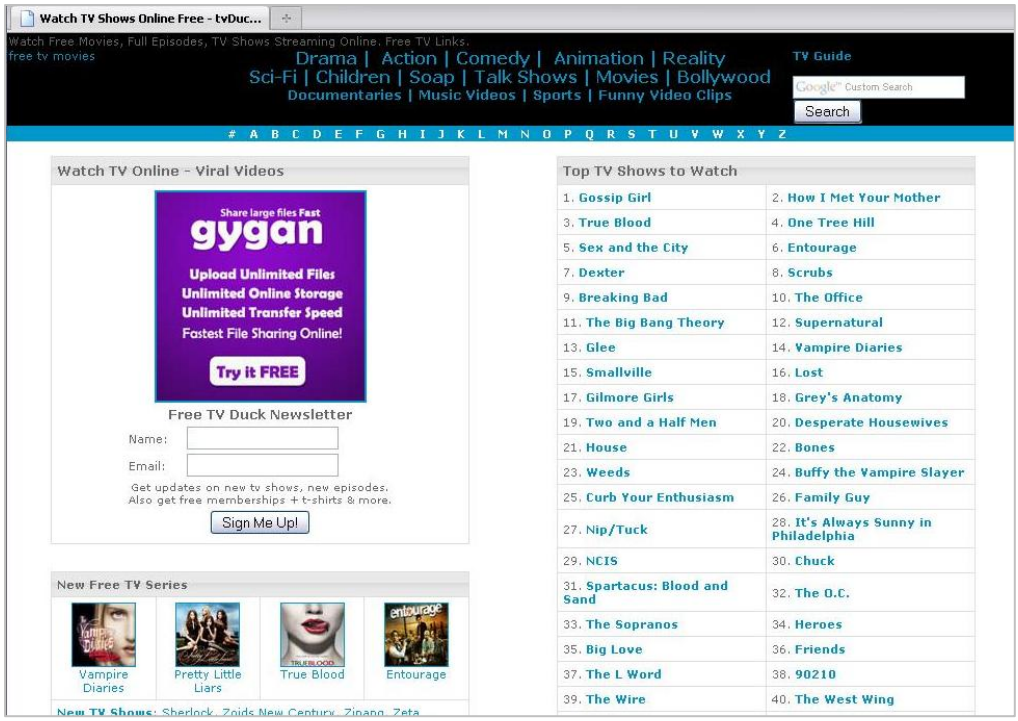
With unauthorized, illegal content, movie fans are exposing themselves to a host of risks, including malvertising, identify theft, and malicious code downloaded with a streamed movie.

Consumers using illegitimate sites for movies and tv shows

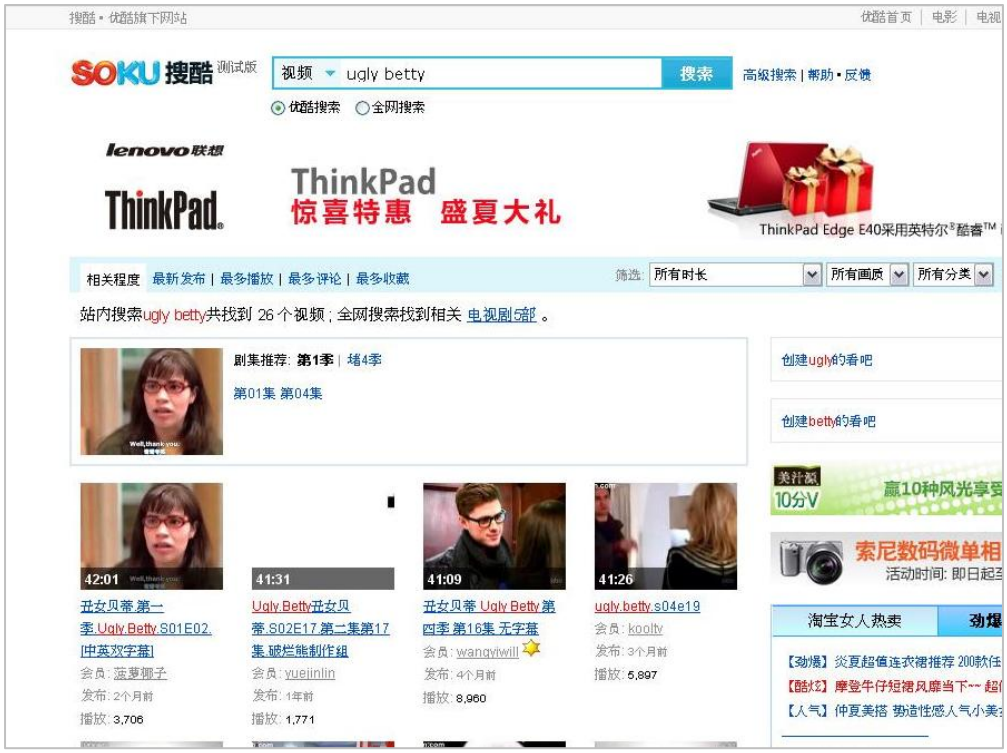
When we talk about digital media, we often talk about the widespread availability of unauthorized content on the web. With few exceptions, people around the globe are more and more willing to try to find something for free as opposed to paying for it—even if it is of lesser quality.

Governments and various industry associations have publicised the fact that pirating content violates the law, but people still continue to do it. Beyond legal considerations, consumers need to understand the risks they bring to themselves and their computers by accessing these sites. Most notably, even if a site looks legitimate, it may not be.

In recent years, McAfee has noticed a marked increase in the variety of sites associated with unofficial content. These sites are not only numerous and sophisticated in their design, but they also draw a large amount of traffic.



This is a screen capture of a site that illegitimately hosts many TV shows; note the list of programs to choose from.



This is a screen capture of a Chinese media sharing site that has many unauthorized TV shows available, in this case, *Ugly Betty*.

Television

After debuting in the United States, the *Lost* television series finale was widely watched around the world. However, there were restrictions in some countries, such as Germany. That didn't stop some global *Lost* fans from watching the finale, however, because they found a way to bypass these restrictions—with anonymization services that allow users to mask or fake the location from which they were viewing the television show.

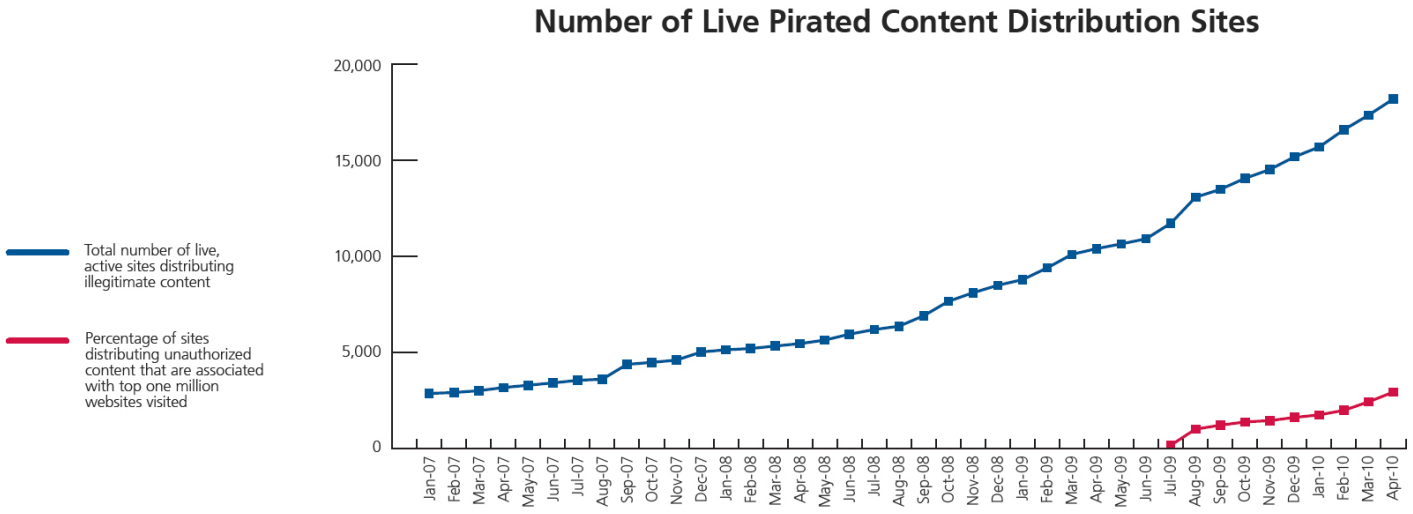
While anonymization services are convenient, consumers should be aware that these services cost money to maintain. Sites that distribute illegal content (movies, television shows, and even music) need to sell advertising to pay for bandwidth and storage needs, and they aren't necessarily choosy about where the money comes from. In light of this, users should be wary of providing information to these sites or downloading any tools that they offer. For example, McAfee research has found a user can encounter significant "spammy advertising" once he or she registers with one of these sites.

In addition, users have been trained to update to a "new version" of a tool to work with the latest video, so it is quite easy for malware authors to prompt users to update their tools and install their malware instead.

This is a screenshot of a TV website from the U.S., Dramaserials.com, that has been exploited with the Zeus Trojan, which uses this domain to send and receive information for malicious purposes.

Meanwhile, we are seeing a growing number of websites designed solely for attracting users and directing them to illegitimate sites. The chart below represents servers that host websites that send users to illegitimate content. The blue line details the total number of live, active sites distributing this content. The red line indicates what percentages of the sites that are distributing unauthorized content are associated with the top one million websites visited (according to Alexa).

Sites that distribute unauthorized content are not only numerous, they can also be highly deceptive. It can be very difficult for the average consumer to determine whether these are legitimate services. On these sites, users can rank movie downloads on quality, provide ranking systems, set up RSS feeds, and find links to legitimate websites, such as IMDb.com (The Internet Movie Database), making them more convincing to users.



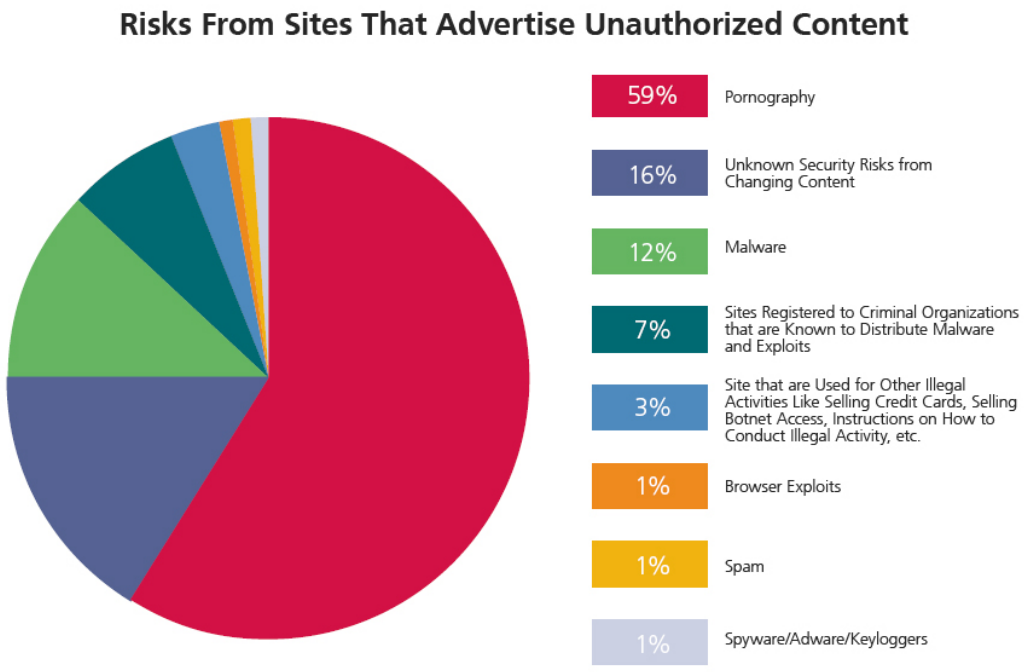
The popularity of pirated content sites is increasing.

Risks associated with sites that distribute unauthorized content

The chart below illustrates the risks that consumers face when making the decision to use sites that advertise unauthorized content. While many users are aware that there are some risks, it is important to show how dangerous these sites can be. Visitors may be exposed to pornography, identity theft, information theft, malware distribution, distributed denial-of-service (DDoS) attacks, and more. What's more, 12% of all known sites that distribute unauthorized content, represented by the color green, are actively distributing malware to users who download content.

Keep in mind that 7% of the websites distributing unauthorized content have associations with known cybercrime organizations. The sites often look very professional and attempt to lure the user with the idea of a "trial period" or even some nominal fee that is much less than what may ultimately be charged. Once the user agrees, they have to authorize their computer to access and interact with computers that are involved in a wide range of schemes—from money laundering to stealing credentials such as user names and passwords. In addition, with this access, your computer is profiled—with all of its software versions, user agents, and any other data—and this information can be provided to third parties for malicious purposes. (This is often called "fingerprinting.")

The take-away for the consumer who is tempted to get something for free instead of purchasing it is this: long gone are the days when risks were easy to identify. With the massive advances in cybercrime, illegal content becomes one more platform designed to attract and exploit consumers with sophisticated technology, leaving the user unaware of the risks to which they have been exposed.



This chart provides the details on risks associated with accessing sites that distribute unauthorized content.

Digital Music Dangers

There are many aspects of digital music—from lyric sites and fan pages to streaming radio and MP3 download sites—giving cybercriminals a multitude of avenues to trick unsuspecting consumers. While certain platforms, such as Apple Inc.'s iTunes store, have helped to make it easy for users to buy reputable, legitimate content, strong demand for free content, interaction, and entertainment has introduced numerous risks.

Malvertising

Online advertising on digital media sites is an especially effective way to get consumers to click on a dangerous link (that usually leads to an exploit, virus, or fake anti-virus website) because cybercrooks can tailor their ads to the site's audience. For instance, in 2008, Rhapsody.com made headline news when it served banner ads that sent users to a fake anti-virus site.[1] Because the cybercriminals knew that Rhapsody.com's users were concerned about viruses, the ads were attractive to visitors.

Since that time, several other sites have been identified as serving malicious ads, including *The New York Times* and Yahoo! Inc. And, in April of this year, players of the popular online game FarmVille (Farm Town in the U.K.) were exposed to malicious advertising that displayed fake security warnings in an effort to get personal details from consumers.

Malvertising is an increasing popular threat, but consumers, unfortunately, are often completely unaware they have been infected.

Links and Tweets

Online advertising on digital media sites is an especially effective way to get consumers to click on a dangerous link.

Besides malvertising, cybercrooks have several other tricks up their sleeves for music lovers. For instance, they often post malicious links in blogs and forums and drive traffic by tweeting these URLs to fans. Users click freely, and it is only after they've clicked on a link that they can view the content, giving cybercrooks the opportunity to spread malware without users' knowledge.

Because it is so easy for cybercrooks to spread threats in this way, it is not uncommon for consumers to encounter websites that deliver malicious downloads or browser exploits. (A browser exploit is a piece of code that exploits a software bug in a web browser, making the browser do something unexpected, such as crash, read or write local files, propagate a virus, or install spyware.)

For example, McAfee conducted a search for "Lady Gaga" in May 2010. The search results turned up a link to a Lady Gaga website and fan forum. But when we clicked the link, we saw advertising leading to adult-oriented anime content as well as links to a "telephone video service." The video service directed consumers to a web address where they could meet "hot, sexy, singles." Just imagine what vulnerable teens and tweens could be exposed to if they performed this search and continued clicking!

[1] http://www.securecomputing.net.au/News/102351,malicious-ads-infect-expedia-and-rhapsody.aspx

YouTube and music downloads

YouTube is a website that has greatly impacted the music industry. Any band can record their performance and post it on YouTube to be discovered, build a fan base, or just share videos with each other.

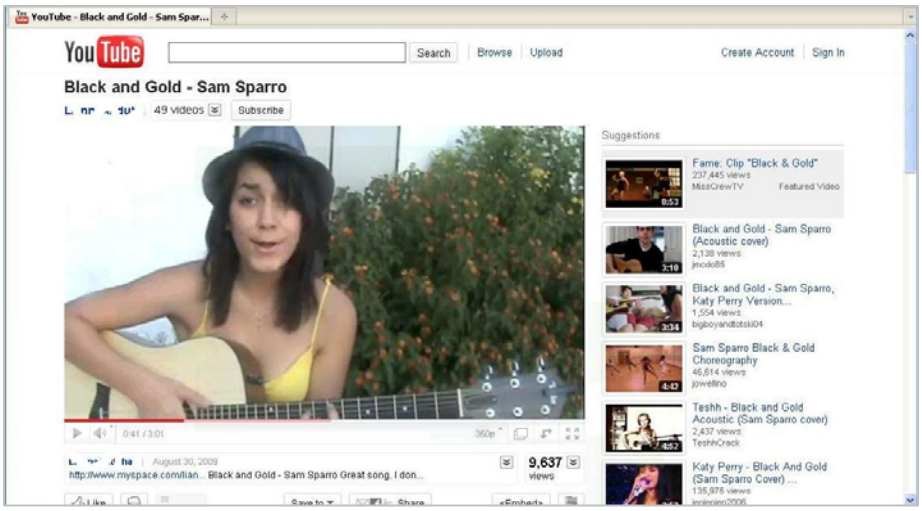
A number of bands, such as The Arctic Monkeys, have evolved via this route. YouTube offers a quick path to fame by building a large fan base fast.

For the past few years, the malware authors have been well aware of the popularity of YouTube—and they have taken full advantage of this. The YouTube incident of July 4, 2010 is one example. Users searching for Justin Bieber on YouTube were redirected to pornography websites and/or videos reporting that he had died in a car accident.

Another incident involved a YouTube video of the 2010 *Black Entertainment Television* (BET) Awards. The video owner said he could not upload the full video of the awards due to copyright issues. He then asked users to visit the posted link instead. That link led to a site that required visitors to download a potentially unwanted program (PUP), a program with features that may cause concern about security or privacy.

In June of this year, researchers also discovered more than 700,000 web pages designed to look identical to YouTube, except that they were created to spread malware. They hooked consumers with the promise of a "must-see video" associated with the British Petroleum oil spill, the National Basketball Association (NBA) Playoffs, Harry Potter movies, and other popular topics. The spoofed pages even contained a YouTube logo. When users attempted to play the video, they were prompted to download and install a program; clicking "OK" caused their browsers to be redirected through several other sites before landing on a final malware distribution site.

What we've learned is that users' desires for digital music and media has opened yet another door for cybercrooks to propagate malware, redirect users to content they did not want to see, or spread disinformation. Furthermore, the growing popularity of social media, and the ability to send out mass tweets to friends, is only making it easier to spread threats.



This is a screenshot of a YouTube video that contains a malicious data stream that will infect a user's PC.

Music-related searches

It's not who you are that makes you dangerous; it's your ranking. That's what McAfee found when researching which music artists are the most risky search terms. Artists with top ranking on the local hit list—whether it's the *Billboard* Top 40 in the U.S. or Australia's *ARIA* Top 50 list—were consistently riskier for fans to search for.

In June 2010, McAfee conducted searches for B.o.B with OMG and Justin Bieber's song "Baby." McAfee found that these artists, who were at the top of the charts across multiple countries, yielded similar and consistent risky results across various global search engines.

When we looked at just the Justin Bieber song "Baby," we found that 4% of the search links in both the U.S. and Japan led to risky sites, while about 3% of the links were risky when searched in Brazil. In Russia, on the other hand, around 15% of the search links turned out to be risky.

You will come across more risks when you try to get something for nothing, such as "free music."

Looking for music and artists on the top of Russia's charts, using Russian search engines or even Google.com, is the most dangerous kind of music search a consumer can perform. In fact, the danger was ten times higher than in other countries we examined.

Below are more detailed risk findings. Keep in mind that "risk" refers to users being exposed to any of the following: adware, spyware, PUPs, fake anti-virus software, malware, and pornography.

Overall, this research illustrates that you will come across more risks when you try to get something for nothing, such as "free music."

Here are key music-related search findings:

- **Rank brings risk**—Searching for a popular artist and his/her current ranked hit brings up more risk than just searching for the artist.
- **Lyrics versus ringtones**—Searching for "lyrics" for a particular artist is twice as risky (on average) as searching for "ringtones" for the same artists within the first five pages. However, if a user continues beyond the first five pages of results, "ringtones" overall is a riskier term.
- **"Free" proves to be costly, again**—Adding the word "free" to ringtones results in a three-fold increase in the riskiness of the sites returned by the major search engines.

- **Pay to be safe**—Add the word "buy" to "ringtones," and search results immediately become safer than searching for ringtones by themselves.
- **Screensavers won't save you**—Searching for the artist plus "screensaver" yielded an additional 50% increase in risk over the risk associated with "ringtones." (Ironically, adding the word "free" before music-related screensavers actually reduces the riskiness of returned search results.)
- **MP3 dangers**—Searching for "MP3s" is even more risky than leaving "MP3" out of the search terms. For example, a recent search for "Rude Boy Rihanna" turned up only three "risky" sites in the top 50 results (6%) using Google. However, searching for "Rude Boy Rihanna MP3" resulted in 30% of the top 10 results showing definite, definable risks. When we expanded that out to the top 50 search results, we found seven "risky" sites (14%), which is more than double the risk. And while "free" does make it a riskier search, indicating that you want to pay for the MP3 in your search still sends you to both pirated and free content.

Summary

Cybercrime is big business, and online media is one of cybercriminals' biggest moneymakers. Demand for digital media—whether it's music, videos, television, or other streaming content—is at an all time high, and cybercrooks are looking to exploit its popularity in every way that they can.

For example, between 2009 and 2010, McAfee has noted a 40% increase in the websites that are delivering infected MP3 files or seem to be built with the sole purposes of conducting some type of cybercrime (identity theft, financial fraud, malware infection, for example) on individuals looking for MP3 media files online.

As online media expands, and devices change, we expect the threats to adapt and become subtler, but we don't expect them to go away. Simply searching for online media may seem safer, but the truth is cybercriminals use many different ways to distribute threats. The threats have evolved past high-level search and are more prevalent than ever.

The only way for users to protect themselves is to stay aware of the risks associated with digital media, and to be on the lookout for potential new dangers.

Here are some important tips for staying safe while enjoying digital media:

- Avoid searching for "free" content. Instead, stick to legitimate, paid sites to get your music and movies.
- Don't click on links in banner ads on music, movie, and download sites that aren't well-established.
- Use comprehensive security software, such as McAfee Total Protection™ software and keep it up to date, to safeguard you from the latest threats.

- Use common sense—don't click on links posted in forums or on fan pages, and seek out well-established, legitimate media sites.
- Use a safe search plug-in, such as McAfee SiteAdvisor® software, to warn you of potentially risky sites in your search results.
- Realize that the more in-demand a topic, a movie, or an artist is, the higher the risk you face when searching for them.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is committed to relentlessly tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

http://www.mcafee.com