

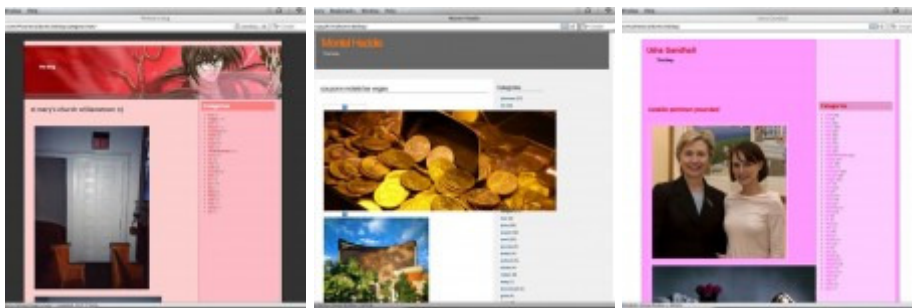
New Large Scale Malware Attack Targets Google Users

Date: November 16, 2009

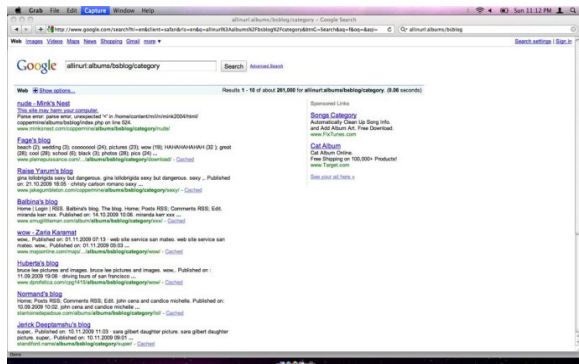
Overview

Cyveillance has discovered a complex attack vector that uses Google search results to distribute malicious software (malware) to unsuspecting Internet users. Using this attack vector, users click on links within Google search results and are routed to sites that attempt to download malware to their computers. The attack method also relies on inattentive webmasters who do not update the software on their sites and often unknowingly provide the material that appears in the search results.

The screenshots below display examples of blogs with posts that are simply images and contain no text or stories:



The common string “albums/bsblog/category” is found in the URLs for all of these blogs. By simply using the Google search parameter *allinurl* alone, you can see how many other sites contain the same string.

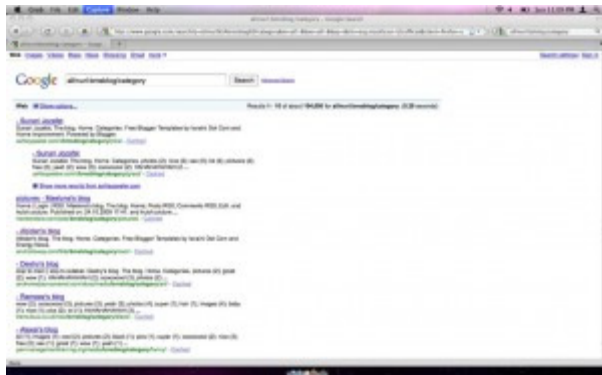


More than 260,000 poisoned Google results. If you carry out the same Google search, DO NOT click on the results.

As can be seen in the image above, more than 260,000 URLs are presented in Google’s search index leading to blogs similar to the ones illustrated in our example. *Beware: if you were to visit one of the above blogs after clicking on the URLs in Google search results, then you would be redirected to two different websites. The second site would attempt to install fake anti-virus software on your computer. (For safety purposes, we are not directly linking to infected search results, but if you enter the query shown in the image, you can recreate the above results.)*

Readers can simply copy and paste the destination URL into your browser to direct it to the desired website, you would be taken to the boring but otherwise harmless blog posting like those pictured earlier in this discussion. The attack only happens when the compromised blog site determines that you arrived by way of Google by checking the HTTP referrer.

An earlier search similar to the one above produced 104,000 infected URLs:



Another 104,000 results that will lead to malware. Again, if you carry out the same Google search, DO NOT click on the results.

As you can see, only a small portion of sites in the search results carry a warning provided by Google. The reason for the small number of warnings is likely because the actual attacks do not take place on the website URLs in the search results, but on the sites you're redirected to thereby decreasing the chances that Google will designate the destination sites as harmful.

Digging Deeper

On all the infected sites found there is rogue blog publishing software installed, sometimes in the popular online photo gallery software Coppermine. (The most recent version of Coppermine we observed being used in this attack was 1.4.24, and Coppermine is now on release 1.4.25.) These rogue blogs automatically and regularly publish new posts that are titled with esoteric terms like "las vegas rental no credit check", "real world melinda and danny", or "uninvited song lyrics alanis morrisette morisette". These posts are intentionally not titled just with simple terms that are very popular like "Britney Spears", "Obama" or "Paris Hilton" to avoid having to compete in search rankings with the millions of pages which already exist for these topics. Instead, the authors of this exploit take advantage of the [long-tail of search](#) where rare combinations of search terms in aggregate make up a very large portion of the queries made by web surfers in search engines. In fact, a surprising amount of Internet searches [contain four and five words](#), and the authors of this attack appear to have titled their blogs' titles with this in mind to be exposed to as many potential victims as possible.

No words are found in these blog posts. The content of each post consists solely of images that are found among “images.google.com” results of queries for the same terms found in the post’s title. Each of the images are then presented inside the new blog post and contain *alt* and *title* tags which also match the post’s title in an attempt to maximize the relevancy in Google’s eyes for any query matching those terms. For example, if one of these blog postings was titled “common and kanye west”, the blog posting would simply contain four or five of the images shown in the results of a Google image search for “common and kanye west”, and each of these images would in turn be given alt and title tags that read “common and kanye west”.



The repetition of the same terms in the post title and image tags is a clumsy but straightforward mechanism of suggesting to Google that the page contains highly relevant information about those topics, hoping Google will then present these pages to searchers. When the searchers click on these links in Google search results, the blog will redirect that visitor to the fake anti-virus installation site.

The Attack

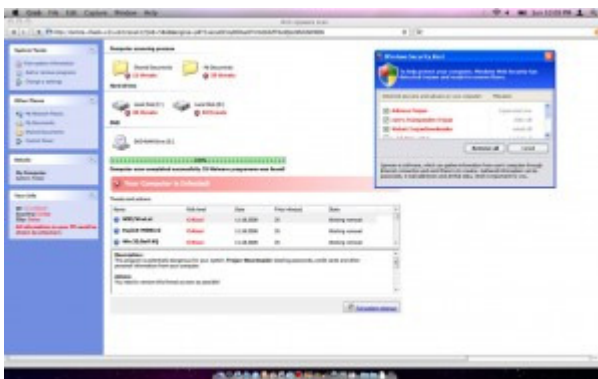


Image of an attack site in progress.

The fake anti-virus site displays what appears to be the results of a computer scan, warning the user that “31 Malware programmes was found!” (*sic*). The fake notifications display illegitimate Windows anti-virus warnings regardless of the user visiting the site on a Macintosh, as happened in the pictured example. However, it did dynamically insert this researcher’s computer’s IP address into the image (which has now been

blurred out). Clicking on anything in the fake infection findings, including the blue framed popup, will result in a file named **Inst_58s6.exe** being downloaded to the user's computer.

Where the Wild Things Are

The path from the infected websites to the fake anti-virus software drop sites is swift and likely not noticed by the user. A user will click on one of the innocent-looking Google search results and is transported to a "middle man" domain like `ionisationtools.cn` or `moored2009.cn`. The server at these domains will then redirect the web surfer to a final destination where the fake anti-virus is pushed on the user, as described above.

The middlemen domains like `ionisationtools.cn` or `moored2009.cn` are registered for just a day or two and quickly go offline. Their DNS records briefly point to the free DNS service provider `EveryDNS.net`.

The actual fake anti-virus drop sites are found on domains such as:

- `premium-protection6.com`
- `file-antivirus3.com`
- `checkalldata.com`
- `foryoumalwarecheck4.com`
- `antispyscan1.com`

All these domains observed by Cyveillance were registered with Chinese registrar `TodayNIC.com` and like the middlemen sites above, these domains are registered one or two days before the inbound Google search traffic will be arriving, suggesting that the software now directing search traffic from the infected websites may know in advance where the drop sites will be in advance.

Only Google?

It appears that Google is the only search engine with knowledge of these infected sites. We learned this by taking several domains that contained the infected Coppermine installs and used Bing's `site:` command and Yahoo!'s Site Explorer; neither of these search engines returned any URLs which contained this particular exploit in action, suggesting that Google is the only major search engine being used as the attack vector by these malware distributors.

It is possible that the attackers took advantage of the ability to submit .xml sitemaps in Google to stimulate the search engine to visit and index the rogue blogs' postings. A suitable .xml file was found on the sites examined to support this technique.

What can be done?

Cyveillance recommends that Google investigate all URLs in its main index which contain albums/bsblog/category or bmsblog/category in the URL and take the appropriate action to minimize the potential danger to users. Additionally, webmasters need to ensure that software is constantly kept up-to-date with the latest revisions and site content is periodically reviewed for potential malicious activity.

While not necessarily practical, users can minimize the exposure to the attack vector described in this writing by copying and pasting the link in the Google search results directly in their browser rather than a directly clicking on the search result link. Additional steps to minimize the harm from the attack vector are ensuring all computer software is up-to-date and practicing safe Web surfing habits.

Heading in to 2010 and beyond, Cyveillance will continue to make the investments in personnel and technology needed to warn the Internet community of new threats, protect our customers, and stay one step ahead of the bad guys.