

## Predictions 2010

### M86 Security Labs Threat Predictions for the Year Ahead

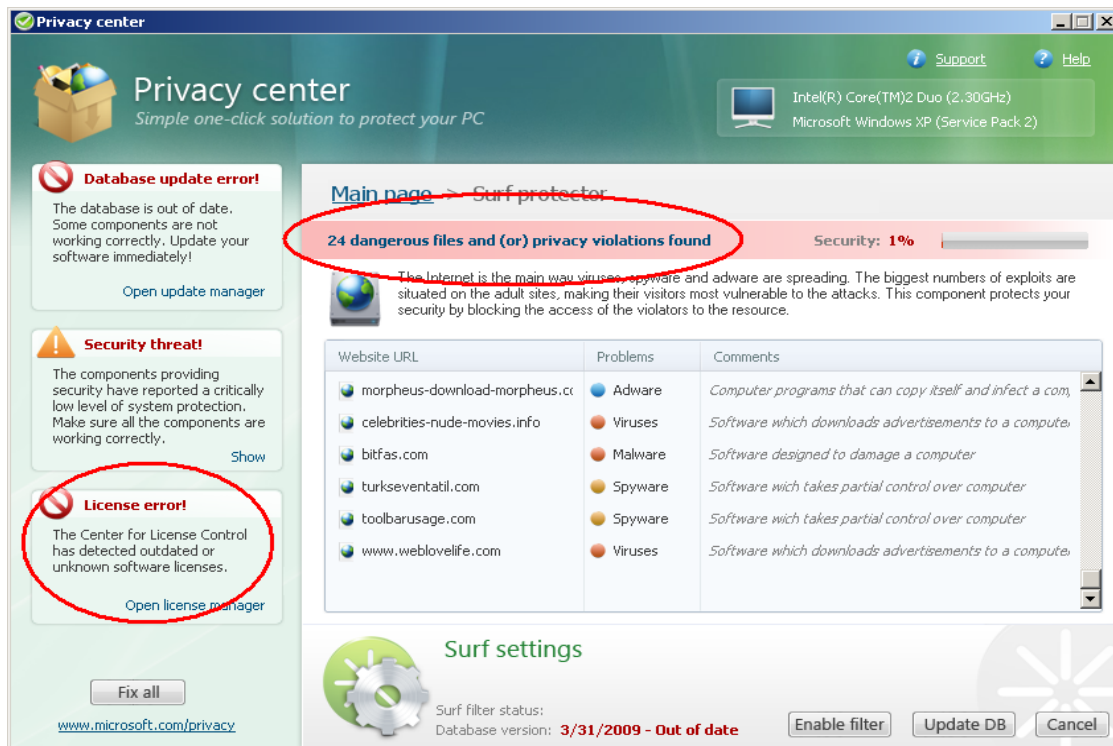
2009 has been notable for several high profile 'wins' such as the successful takedown of the 3FN hosting company, the second takedown in over a year of a rogue Internet Service Provider, followed by the disabling of the Mega-D botnet. While these successes are significant wins for the white hat community, they have resulted in a short term impact on spam levels. The volume of spam has in fact eclipsed the levels seen before these takedowns. In addition to the increased growth in spam, the soaring popularity of social networking sites has also led to a rise in spam and malware being spread through these services. The most predominant piece of malware being distributed across the Internet today has been the ZeuS bot (also known as Zbot); a nefarious Trojan that is primarily used to steal online banking credentials, but has been used to steal social networking and other types of credentials. All in all an active year both in volume of attacks and new innovations which can be used to predict what might be in store for next year.

#### The Continued Rise of Scareware:

We have seen this old tactic getting a lot more popular in the second half of 2009, and it's popular because people are falling for it. The applications themselves look a lot more professional and legitimate than ever before as can be seen from the example below.

Apart from the scammers making money out of unsuspecting end users and also installing all sorts of malware on their computers, these schemes erode confidence and trust from legitimate anti-malware/anti-virus vendors. As a result, vendors with lower brand recognition and smaller marketing budgets find it more difficult to differentiate themselves from the scammers. This scareware approach also diverts revenue from the very industry trying to address malware today, with the scammers laughing all the way to the bank!

We expect to see this type of attack escalate further in the coming year, as the look and feel of the scareware gets updated and new methods of reaching end users are targeted.



*Convincingly crafted scareware succeeds at frightening the average user*

### **Search Engine Optimization Poisoning:**

A growing trend is the use of Search Engine Optimization (SEO) techniques to drive users to Web pages hosting malicious code. Also known as SEO poisoning, the technique aims to elevate malicious landing pages up the search engine results ranking, thus ensuring a steady supply of victims. The techniques vary, but many center on loading Web pages with key words and phrases related to any hot trend, such as those derived from services like Google Trends, or other celebrity news, or popular topics. The 'enriched' Web pages help to push up the search engine rankings for the criminals' malicious landing pages. The systems the criminals are using are sophisticated and highly automated, leading to a continuing supply of fresh search terms and 'loaded' Web pages.

SEO poisoning is particularly treacherous as users tend to implicitly trust search engine results. Throughout 2009, the floggers of fake-anti-virus 'scareware', in particular, extensively used SEO poisoning techniques to drive users to their landing pages. Look for this trend to deepen in 2010, as the criminals continue to exploit users' natural tendencies, i.e., searching for their favorite stuff on the Web.

### **Botnets to Grow in Sophistication:**

Botnets continue to be a major problem, driving the majority of spam output and mass website attacks. The McColo takedown in 2008 and the 3FN takedown in 2009 demonstrated the effect of disrupting a botnet's command and control processes, producing immediate results in terms of spam volume decreasing. Unfortunately, not only has this volume recovered to previous levels, it has also caused the botnet controllers to start experimenting more, designing more resilient and stealthy command and control systems. Botnets have largely moved away from traditional IRC-based command and control, in favor of HTTP or other custom protocols. Individual bots have more sophisticated fall back mechanisms to locate command servers, such as using domain names instead of hard coded IP addresses, and automatic domain name generation. We have also seen experimentation with alternative command and control systems, notably those using Twitter, Google groups, and the most recent example involving the notes section of the mobile version of Facebook.

As Google Wave stabilizes, we expect to see it being used nefariously, as it provides the advantages of both P2P and HTTP based C&C and supports the features required by cybercriminals.

The increasing experimentation with different C&C control methods is worrying, as it means there are more protocols and applications to discover, track and attempt to control in an effort to block botnet command and control traffic.

### **Evolution of Compromised Website Infections:**

Over the last few years, the trend of legitimate websites being compromised and used to spread malware has become one of the go-to attack vectors for cybercriminals. We expect this trend to continue and evolve in the coming year.

Instead of relying on injected IFrames pointing to malicious websites, we believe that a majority of the malicious behavior will reside on the compromised websites themselves (such as with the KoobFace worm).

### **SaaS Service/Cloud Based Architecture Buzz:**

The term "cloud" has become the buzz word for 2009, leading to a vast increase in cloud-based service offerings. There has been a shift to store corporate data outside of the network, making it difficult for IT administrators to have direct control over this data. While the shift to the cloud is inevitable, it is best to do so while erring on the side of caution. This shift also means that the larger cloud based providers will become attractive targets for cybercriminals, and as such, the attacks on these cloud based services will increase.

### **Targeting 3<sup>rd</sup> Party Applications:**

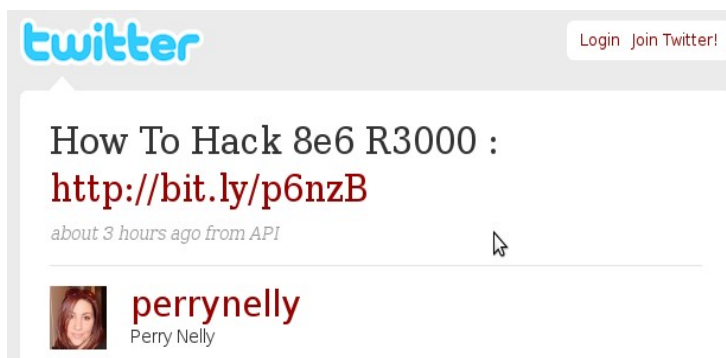
With its high deployment rate, Adobe based products, such as Flash and Acrobat Reader remain a prime target for exploitation. In addition to its high deployment rate, the major draw of these applications is the platform independence and programming capabilities (such as JavaScript for Acrobat). We expect attacks on these applications to continue to grow, with the addition of more complex attacks (such as embedding one file type in another) gaining more popularity, due to the ability to evade detection mechanisms.

### **Internationalized Domain Name Abuse:**

At the end of October 2009, ICANN approved the registration of Internationalized Domain Names. This step marks the first time that domain names can contain non-Latin characters and could open up the flood gates for abuse, especially in the realm of phishing websites. An attacker could register a bogus domain name for a bank using the non-Latin characters that look quite similar to the legitimate one. The end user might not be able to distinguish one from the other. This form of attack has already been proven to be feasible in the past, with a homographic attack on the Microsoft.com domain name using Russian letters. We believe this will become a growing trend, as we start to see countries registering these domains.

### Expanded Use of Web APIs – Another Threat Vector:

This area is rapidly expanding, with services like Facebook and Twitter extending their services for third party development through the use of APIs. Its growth rate makes this platform open to and ripe for abuse. We've already seen spammers using the Twitter API to post updates to the service with shortened URLs that lead to spam/malware.



*An example of the Twitter API being leveraged by spammers to spread malware*

There is an implicit trust level provided through the use of APIs, granting access to user profiles and data. The possibility of a rogue third party application that takes advantage of this implicit trust is there. The increased usage of APIs and the threats that target them are likely to intensify in 2010.

### URL Shortening Services – A Haven for Cybercriminals:

With the major players like TinyURL and bit.ly cleaning up their acts and working to thwart malicious/spam URLs from being introduced through their services, there's been a surge in new URL shortening service offerings. LongURL reports that there are over 100 services currently available today. Our own research has come across URL shortening services that are solely devoted to nefarious usage, spreading malware and phishing URLs to end users. The fact that these services are unchecked is a growing problem, especially with the increasing popularity of Twitter. The fact that Twitter isn't inspecting each and every URL posted to the service makes it difficult to identify legitimate URLs from malicious URLs. Browser extension offerings, such as our very own SecureTweets is a useful way to protect end users from shortened links, as long as the root issue remains unresolved, we expect to see more and more malware/phishing URLs being spread through these services.

The emphasis for cybercriminals revolves around emerging technologies, targeting hype and ensuring visibility amongst the biggest user base possible, whether that's through Twitter, Facebook, or Google search trends. Social Engineering has become the primary vector of attack and we expect this trend to continue and grow as more and more services establish a presence on the web.

---

### About M86 Security

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit [www.m86security.com](http://www.m86security.com).

**Corporate Headquarters**  
828 West Taft Avenue  
Orange, California 92865  
USA  
T: +1 714 282 6111

**International Headquarters**  
Renaissance 2200, Basing View  
Basingstoke, Hampshire, RG21 4EQ  
United Kingdom  
T: +44 1256 848080

M86 Security is a registered trademark of M86 Security. All other product and company names mentioned herein are trademarks or registered trademarks of their respective companies.