

M86 Security

Internet Security Predictions for 2010

January 2010

Today's Speaker



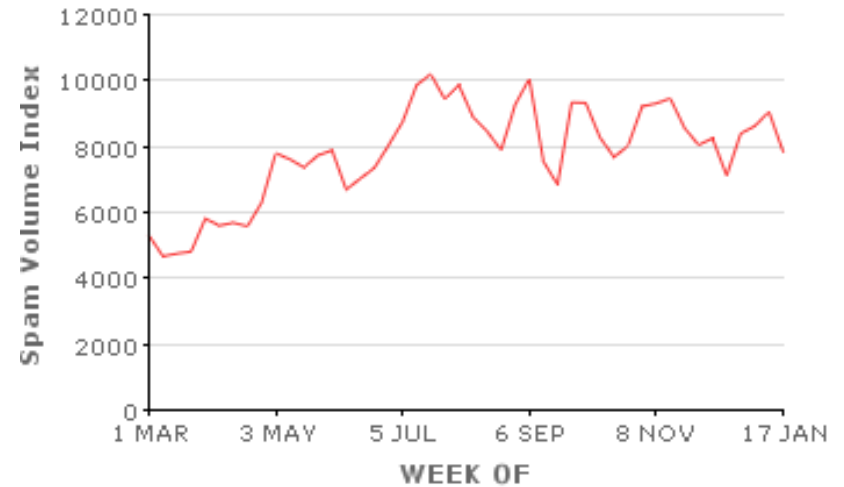
- Bradley Anstis
- Vice President, Technology Strategy, M86 Security
- Speaker on security technology and malware trends
- Former VP Products, Marshal Ltd.
- Over 20 Years of IT industry experience

Review of 2009

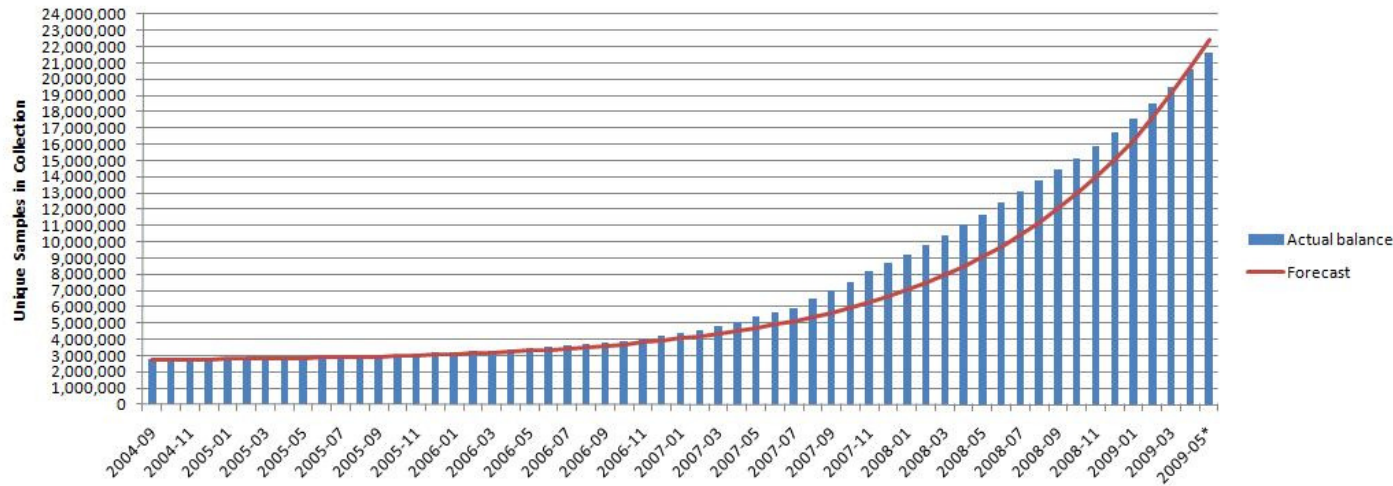
Some wins...

- Rouge ISP takedowns
- Botnets disabled

But also plenty of 'business as usual'



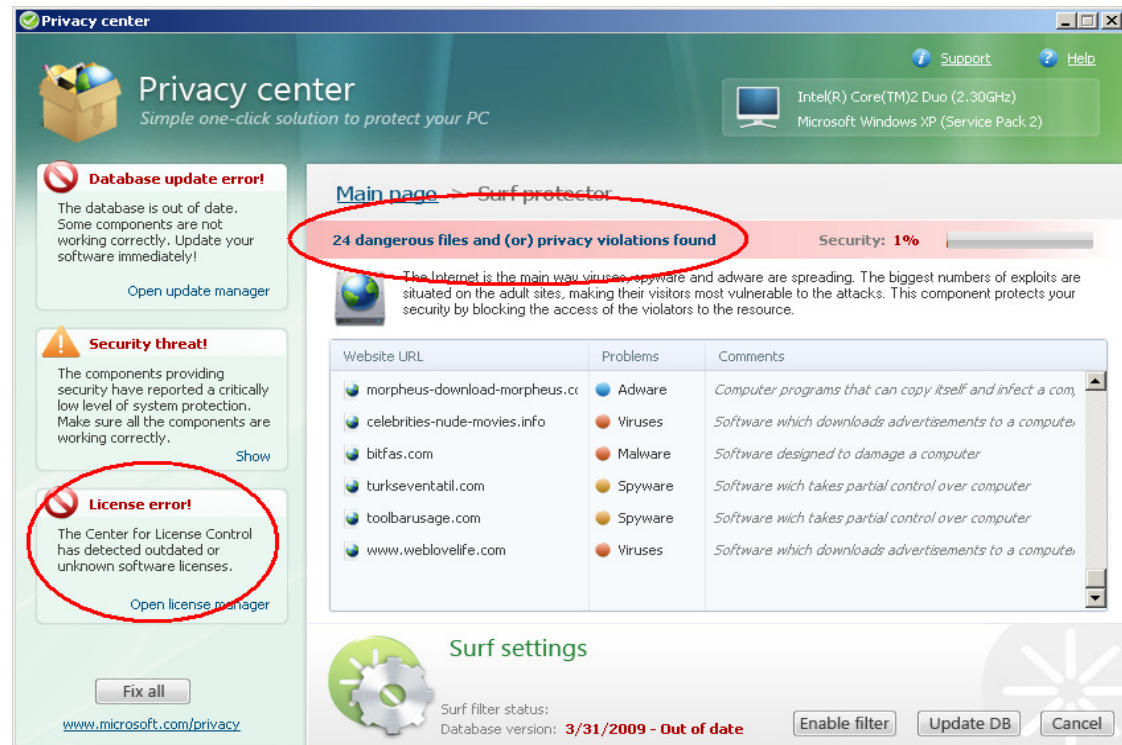
Total Number of Unique Samples in AV-Test.org's Malware Collection



2010 Threat Predictions

1. Continued Rise of Scareware

- Rouge applications that appear to be genuine
- Some users are even paying for the privilege of using them
- Aimed at the home user but have been seen in the enterprise
- Redirects users funds away from security companies
- How do you tell the difference?
- How can technology help?
- User training can also help...



2. Search Engine Optimization & Poisoning

- Great way of directing unsuspecting users to your site
- Works by manipulating search results to elevate malicious landing pages up search results
- Many different methods but many work by loading up the malicious page with keywords and phrases related to any hot trend
- Trends can be collected from services like Google trends
- Takes advantage of the users inherent trust in search engine results

✓ TagALLY - Haiti Donations

People continue to bring **donations** to Rays of Hope in Grand Rapids slated to be shipped to **Haiti** for earthquake relief efforts. ...

tagally.com/main/article/3301 - [Cached](#) -

⚠ January 13 2010 - Haiti Donations

Calls for **Haiti donations** spread thru social Web. 33 minutes ago. (AP:NEW YORK) Calls for **donations** spread through social media sites Facebook and Twitter

[donations](#) - [Cached](#) -



Use caution: Potentially malicious behavior was detected on this page
[More info >>](#)

⚠ Donations - Politics News Story - WISC Madison

Mayor Declares Sunday 'Haiti Relief Day'. Updated: 10:40
E - Milwaukee Mayor Tom Barrett ...

[07/detail.html](#) - [Cached](#) -

⚠ Haiti Disaster Relief Donations - Kathleen Sebelius | January 14 ...

Jan 14, 2010 ... ColbertNation.com video - Kathleen Sebelius shows everyone how to donate to the Red Cross by texting 'Haiti' to 90999.



Tip: Use commas to compare multiple search terms.

Examples

[memorial day_labor day](#)
[ebay.com_craigslist.org](#)

[red_hat_debian_gentoo_slackware](#)
[gizmodo.com_engadget.com](#)

[the meaning of life](#)
[yelp.com_citysearch.com](#)

Hot Topics^{New!} (USA)

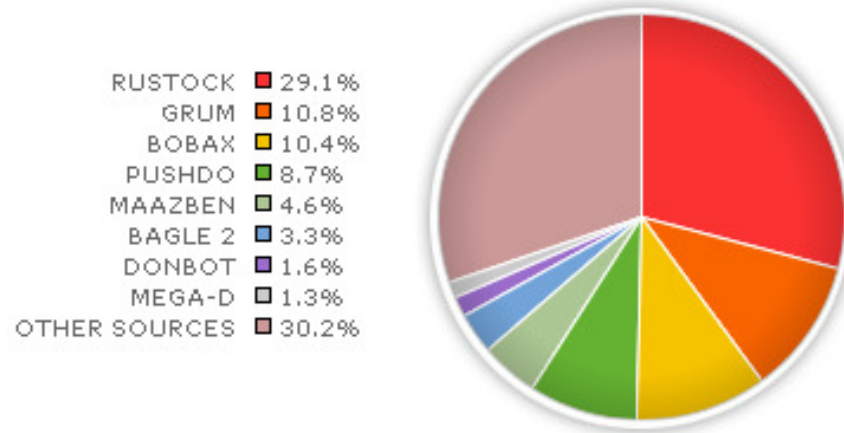
1. [tablet apple](#)
2. [obama state of the union](#)

Hot Searches (USA)

1. [toyota recall models](#)
2. [jenni farley pics](#)

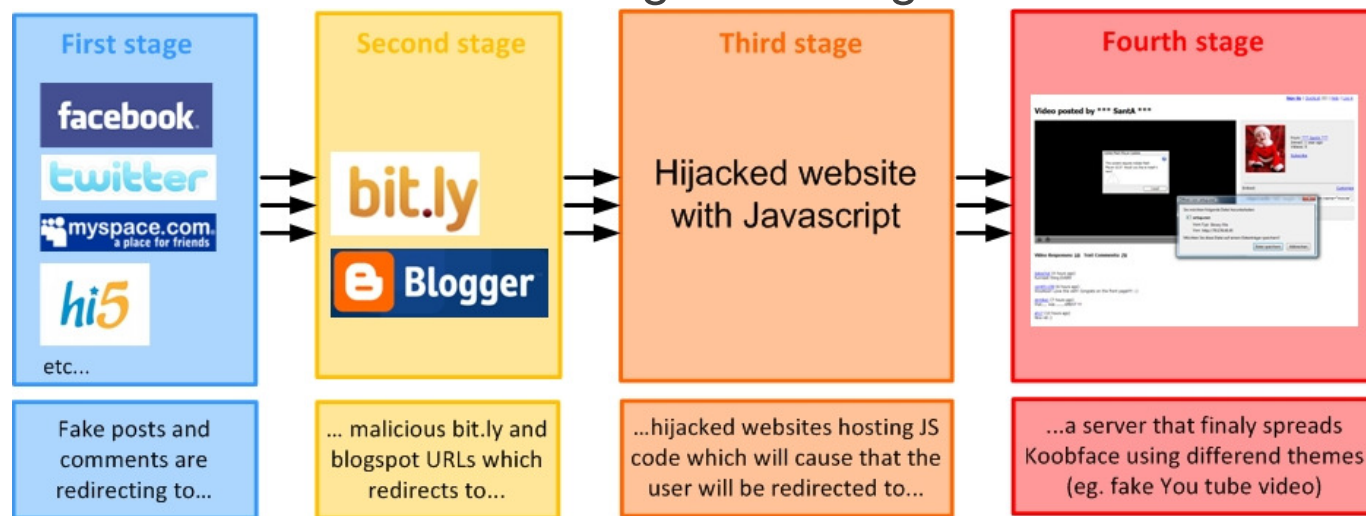
3. Botnets to Grow in Sophistication

- Most successful Botnet take downs revolve around the disruption of the botnets command & control system
- New protocols being used for C&C
 - Twitter
 - Google groups
 - Mobile version of Facebook
- This means the C&C activity is harder to detect and stop
- Also moving from rudimentary hardcoded IP's to domain names and fast flux domain registrations to evade detection



4. Evolution of Compromised Website Infections

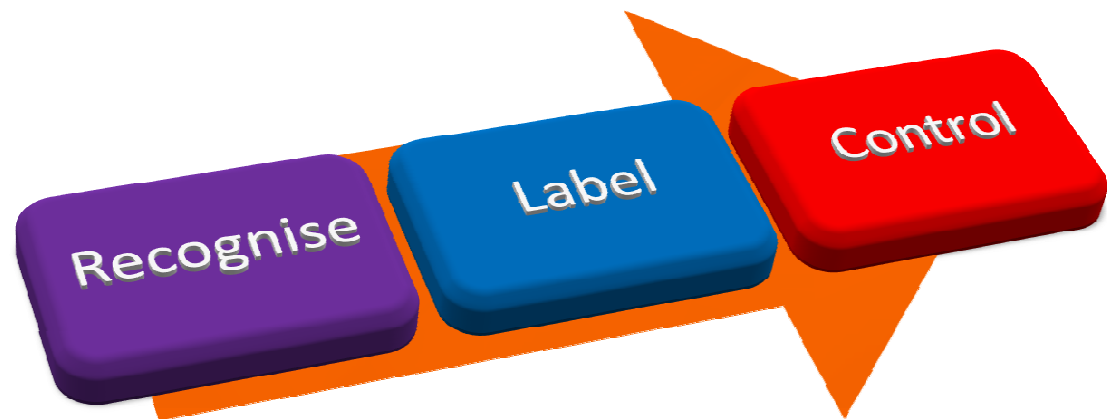
- Dramatic shift from hacker established sites to the infection of legitimate sites already happened
- Legitimate websites less likely to be blocked or are viewed with a higher reputation, both of which can circumvent traditional web security tools
- In the past injected Iframes pointing to malicious websites were common, now starting to see more direct infection of sites with the actual malicious code residing on the legitimate website



*Graphic from www.abuse.ch

5. SaaS Service/Cloud Based Architecture Buzz

- “Cloud” was the new buzz word in 2009, many organizations shifting internal applications and their data to the “cloud”
- The shift is inevitable, and brings a lot of great features, just make sure you consider the security implications
 - Security can be greater with the cloud due to the ‘fuzzy’ location nature
 - Or it can be more of a target if an attacker gained access through some base level vulnerability, many attractive targets sitting in the same place



6. Targeting 3rd Party Applications

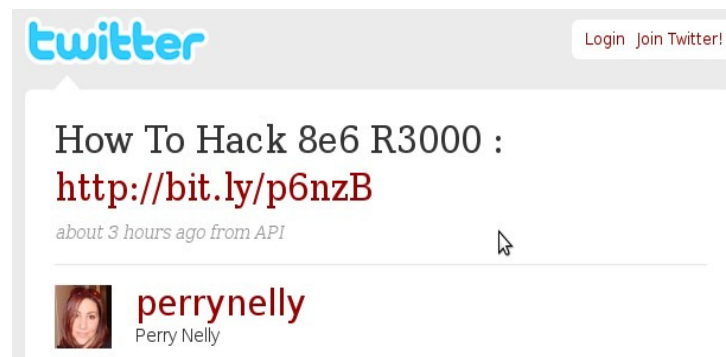
- It's not just operating system vulnerabilities that are being used for attacks
- Many of these applications become so large and complex with their own programming capabilities that they resemble OS's as well, unfortunately this often also means a higher level of vulnerabilities
- Application vendors are typically less able to release urgent updates compared to OS vendors
- Many technologies such as JavaScript for Acrobat are themselves used for the attack for example websites using Flash banners provided from advertising networks find themselves unwittingly launching malicious code

7. Internationalized Domain Name Abuse

- Non-Latin characters supported since October 2009
- Implications for URL Filtering and Reputation lists
- Also can be used for phishing attacks
 - IDN homograph attacks

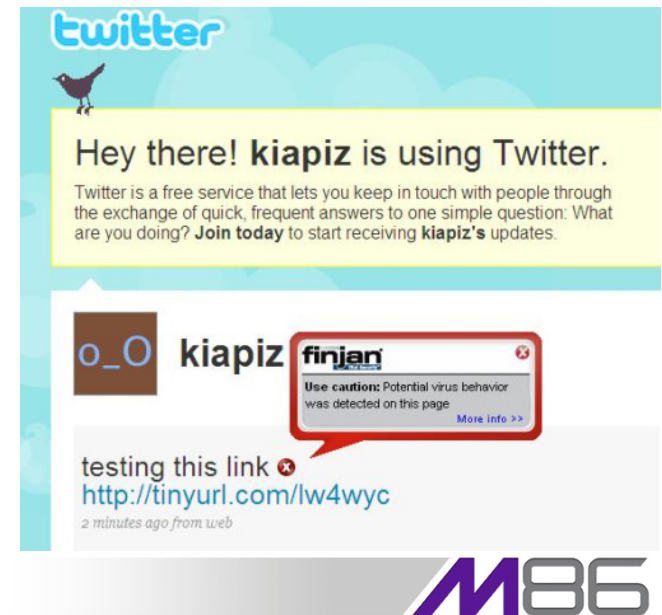
8. Expanded Use of Web API's

- Many sites such as Twitter & Facebook are expanding their support for 3rd party development through API's
- These API's designed for positive use can just as easily be used for bad
- Rouge application can take advantage of the implicit trust of the hosting site, do users actually realize the application they are now using is not actually part of Facebook?
- We have seen a lot higher growth rate in the bad applications rather than the good



9. URL Shortening Services

- Problem is that the user is not fully sure where the link will lead them
- Many different providers of Shortened URL services (Way over 100)
- Some like bit.ly are providing capability for browsers to show the actual destination URL, but this is not usual and there is no common method
- Already we have seen many cases of providers solely dedicated to nefarious usage
- The current hype of Twitter is not helping



Summary

- 2010 will see further increases in the volume of threats and the complexity of threats (We said the same thing last year!)
- Excellent opportunity to revisit your current Email & Web security platforms – how are they keeping up?



**Stopping Today's Threats
While Discovering Tomorrow's.**

Get Vital Threat Intelligence with **M86 SecurityLabs.**

M86TM
SECURITY