The Changing Nature of the Threats

Submitted by: Australia
APEC TEL 41
The changing nature of the threat

Rob Forsyth
Regional Vice President, Asia Pacific
Chinese Taipei, May 2010

Sophos Worldwide
What do ISP customers experience and read?

How can they tell what is good and bad?

How confident are they?

Who do they blame when things go wrong?

FBI reports* that cyberfraud losses doubled

<table>
<thead>
<tr>
<th>Year</th>
<th>Complaints Received</th>
<th>Dollar Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>336,655</td>
<td>$559.7 million</td>
</tr>
<tr>
<td>2008</td>
<td>275,284</td>
<td>$265.0 million</td>
</tr>
<tr>
<td>2007</td>
<td>206,884</td>
<td>$239.09 million</td>
</tr>
<tr>
<td>2006</td>
<td>207,492</td>
<td>$190.44 million</td>
</tr>
<tr>
<td>2005</td>
<td>231,493</td>
<td>$183.12 million</td>
</tr>
</tbody>
</table>

* FBI Annual Report on Internet Crime Released March 2010
Monetary Authority of Singapore

... the internet is a global network which is intrinsically insecure. Security threats arising from denial of service attacks, spamming, spoofing, sniffing, hacking, key logging, phishing, middleman interception, mutating virus, worms and other forms of malware pose heightened technology risk ...

* From the INTERNET BANKING AND TECHNOLOGY RISK MANAGEMENT GUIDELINES

The Australian Government - The Defence Signals Directorate

- 35 strategies to mitigate against targeted cyber intrusions

- ~70% of the targeted cyber intrusions could have been prevented if organisations had implemented the first four

"Australian computer networks are being targeted by malicious entities seeking access to sensitive data. A commonly used technique is social engineering, in which malicious emails are tailored to entice the reader to open them. … could lead to a compromise of network security."

* Mike Burgess, Deputy Director, Cyber & Information Security - March 2010
Spam hosts - in member economies – Q1 2010

<table>
<thead>
<tr>
<th>Rank</th>
<th>Abbreviation</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>US</td>
<td>12.62%</td>
</tr>
<tr>
<td>4</td>
<td>KR</td>
<td>5.32%</td>
</tr>
<tr>
<td>5</td>
<td>VN</td>
<td>4.98%</td>
</tr>
<tr>
<td>7</td>
<td>CN</td>
<td>3.83%</td>
</tr>
<tr>
<td>9</td>
<td>RU</td>
<td>2.86%</td>
</tr>
<tr>
<td>18</td>
<td>TH</td>
<td>1.81%</td>
</tr>
<tr>
<td>19</td>
<td>CL</td>
<td>1.47%</td>
</tr>
<tr>
<td>21</td>
<td>MX</td>
<td>1.28%</td>
</tr>
<tr>
<td>23</td>
<td>TW</td>
<td>1.11%</td>
</tr>
<tr>
<td>24</td>
<td>ID</td>
<td>1.03%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rank</th>
<th>Abbreviation</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>PE</td>
<td>0.77%</td>
</tr>
<tr>
<td>29</td>
<td>CA</td>
<td>0.72%</td>
</tr>
<tr>
<td>34</td>
<td>JP</td>
<td>0.64%</td>
</tr>
<tr>
<td>40</td>
<td>PH</td>
<td>0.44%</td>
</tr>
<tr>
<td>42</td>
<td>AU</td>
<td>0.42%</td>
</tr>
<tr>
<td>44</td>
<td>MY</td>
<td>0.33%</td>
</tr>
<tr>
<td>48</td>
<td>SG</td>
<td>0.29%</td>
</tr>
<tr>
<td>55</td>
<td>HK</td>
<td>0.22%</td>
</tr>
<tr>
<td>68</td>
<td>NZ</td>
<td>0.11%</td>
</tr>
<tr>
<td>81</td>
<td>BN</td>
<td>0.06%</td>
</tr>
</tbody>
</table>
SophosLabs estimate of zombies

1. About 200,000,000,000 spam-sending attempts each day
2. Each zombie sent a mean of 10,000 spams per day
3. AU produced about 0.4% of the world’s spam

<table>
<thead>
<tr>
<th>Region</th>
<th>Spams</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU</td>
<td>80,000</td>
</tr>
<tr>
<td>APAC</td>
<td>8,000,000</td>
</tr>
<tr>
<td>Worldwide</td>
<td>20,000,000</td>
</tr>
</tbody>
</table>

http://www.sophos.com/blogs/duck/g/2009/10/31/zombies-australia/
http://www.sophos.com/blogs/duck/g/2010/03/24/dezombifying-australia/

So what is the threat now and how has it evolved?

SOPHOS Security Threat Report: 2010
Social networking spam

Do you want a job with Google?
Social networking spam

Twitter might spot the message so the criminals hid it inside the profile picture instead.

57% of social networking users report being hit by spam via the services. That’s an increase of 70.6% from a year ago.
Social networking phishing

Does that address look correct?
Social networking phishing

Twitter is a service for friends, family, and co-workers to communicate and stay connected through the exchange of quick, frequent answers to one simple question: What are you doing?

http://www.tvviter.com/

Facebook Login

You must log in to see this page.

Email: 
Password: 

Remember me 
Login or sign up for Facebook

Forgot your password?
Social networking phishing

30% of social networking users report phishing attacks via the sites

That’s an increase of 42.9% from a year ago.
Email threats

Hackers are spamming out emails posing as breaking news stories about a bomb blast in your city, in the hope that you will follow the link and infect yourself with malware.
Email malware

Hello!
The courier company was not able to deliver your parcel by your address. Customer Error in shipping address.
You may pickup the parcel at our post office personally.
The shipping label is attached to this e-mail.
Please print this label to get this package at our post office.

Thank you for attention.

SAP Delivery Services.

Social networking malware
Social networking users report malware attacks via the sites

That’s an increase of 69.8% from a year ago.
SEO - Search Engine Optimisation

Internet users searching for phrases like “Oscars 2010 winners”
How to make money online! - THE PARTNERKA

The Partnerka or affiliate networks

What is it and why you should care
Dmitry Samosseiko at the Virus Bulletin Conference in Geneva
http://www.sophos.com/blogs/duck
Data loss

Business reputations are only as strong as the processes, and protective solutions in place.

One of the biggest data leaks of 2009 was part of a database of 76 million US Army veterans. Other leaks were recorded worldwide from universities, schools and colleges; banks and credit unions; hospitals and health centers; state, city and local government institutions.

The most important step in stopping data loss is to encrypt sensitive information, laptops, and removable storage devices.

Data is the ultimate business asset.
Mobile malware

/*
People are stupid, and this is to prove it so
RIPH. Its not that hard guys
Out hey who cares its only your bank details at stake.
*/

// This is the worm main()

#include "INVOKE_MCALL"
int main(int argc, char *argv[])
{
    if(argc == 0)
    {
        syslog(LOG_DEBUG, "I know when im not wanted *splat*!");
        return 1; // Already running.
    }
    sleep(2); // Lets wait for the network to come up 2 MINS
    syslog(LOG_DEBUG, "?????? Just want to tell you how in feeling!");
    char *srcRanges = srcAddRange;
    // Why did i do it like this I hear you ask.
    // because i wrote a simple python script to parse ranges
    // and output them like this
    // THIS WOR;
}
Cyberwarfare

The Third Age of Cybercrime

1. Hobbyist
2. Money, Organized crime
3. Economic, Political, Military
Twitter was hit by political fallout in August 2009, when a major DDoS against the site appeared to be targeting a specific anti-Russian blogger based in Tblisi, Georgia.

In December of 2009, Twitter DNS records were compromised and visitors redirected to a site claiming to have been 'hacked by the Iranian Cyber Army'.
The future

- Criminals are increasingly using social networking – and users will continue to share information inappropriately
- Hackers continuing to target ubiquitous software – such as Adobe Flash and PDF reader
- SEO poisoning and fake anti-virus will continue
- Data leaks will continue to embarrass firms
- More attacks against cloud-based systems
- More accusations of cyberwarfare and industrial espionage

Customers will continue to have problems and call support
APEC TEL 41
The changing nature of the threat

Rob Forsyth
Regional Vice President, Asia Pacific
Chinese Taipei, May 2010