The Threat Landscape in 2013

- Cyberespionage
- Privacy
- Malicious Insider

Internet Security Threat Report 2014 :: Volume 19
Agenda

• Data Breach
• Targeted Attacks
• Vulnerabilities
• Ransomware
• Mobile & Social Media
• Internet of Things
The Year of the Breach

2013 was the Year of the Mega Breach

<table>
<thead>
<tr>
<th>Year</th>
<th>Breaches</th>
<th>Identities Exposed</th>
<th>Breaches &gt;10M</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>208</td>
<td>232M</td>
<td>5</td>
</tr>
</tbody>
</table>
Mega Breaches

• 8 of the top 10 breaches were of more than 10 million identities
• Average Identities exposed were 4 times greater than 2012
• The average number of identities exposed per data breach for Hacking incidents was approximately 4.7 million.

• Theft or loss of a device was ranked third, and accounted for 27% of data breach incidents.
Mega Breaches

- Healthcare, education and the public sectors accounted for 58% of all data breaches
- But the retail, computer software and financial sectors accounted for 77% of all the identities exposed in 2013.
Mega Breaches – What Was Lost

- Real Names
- Birth Dates
- Government ID Numbers (Social Security)
- Home Address
- Medical Records
- Phone Numbers
- Financial Information
- Email Addresses
- User Names & Passwords
- Insurance
Targeted Attacks

Increase in targeted attack campaigns

2012

+91%

2013

## Targeted Attack Campaigns

<table>
<thead>
<tr>
<th></th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email per Campaign</strong></td>
<td>78</td>
<td>122</td>
<td>779</td>
</tr>
<tr>
<td><strong>Recipients/Campaign</strong></td>
<td>61</td>
<td>111</td>
<td>23</td>
</tr>
<tr>
<td><strong>Campaigns</strong></td>
<td>165</td>
<td>408</td>
<td>779</td>
</tr>
<tr>
<td><strong>Duration of Campaign</strong></td>
<td>4 days</td>
<td>3 days</td>
<td>8.3 days</td>
</tr>
</tbody>
</table>

**Internet Security Threat Report 2014 :: Volume 19**
Targeted

Top 10 Industries Targeted in Spear-Phishing Attacks, 2013

Source: Symantec

1. Public Administration (Gov.) - 16%
2. Services – Professional - 15
3. Services – Non-Traditional - 14
4. Manufacturing - 13
5. Finance, Insurance & Real Estate - 13
6. Transportation, Gas, Communications, Electric - 6
7. Wholesale - 5
8. Retail - 2
9. Mining - 1
10. Construction - 1
Spear Phishing Attacks by Size of Targeted Organization, 2011 – 2013

Source: Symantec

<table>
<thead>
<tr>
<th>Size of Organization</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,501+ Employees</td>
<td>50%</td>
<td>50%</td>
<td>39%</td>
</tr>
<tr>
<td>1,501 to 2,500</td>
<td></td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td>1,001 to 1,500</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>501 to 1,000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>251 to 500</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 to 250</td>
<td>18%</td>
<td>31%</td>
<td>30%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>
Targeted

Risk of Job Role Impact by Targeted Attack
Sent by Spear-Phishing Email

Source: Symantec

Risk
- Personal Assistant (Executive Assistant)
- Media
- Senior Management
- Sales
- C-Level
- Recruitment
- R&D

Internet Security Threat Report 2014 :: Volume 19
• Most frequently occurring words used in targeted spear-phishing email attacks throughout 2013.
An employee of a multinational company receives an email referencing an INVOICE ...

Dear Employee,

Please take a moment to open the attached invoice:

Sincerely,
Sender

Invoice
Minutes later, she receives a phone call...

Please process the invoice...
Vulnerabilities

• There were a total of 23 zero-day vulnerabilities discovered in 2013. This is up from 14 in 2012.

• There have been more zero-day vulnerabilities discovered in 2013 than in any year since Symantec began tracking them, and more than the past two years combined.
Vulnerabilities

Scanned Websites With Vulnerabilities ...

53% 2012

78% 2013 +25% pts

... % of Which Were Critical

24% 2012

16% 2013 -8% pts

1 in 8 sites had critical unpatched vulnerabilities
Vulnerabilities

New Unique Malicious Web Domains

- 2013: 56,158
- 2012: 74,001
- 2011: 55,000

-24%

• With so many vulnerable web sites cybercriminals have no need to set up their own web sites to host malware
Vulnerabilities

Web Attacks Blocked Per Day

<table>
<thead>
<tr>
<th>Year</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>568,700</td>
</tr>
<tr>
<td>2012</td>
<td>464,100</td>
</tr>
<tr>
<td>2011</td>
<td>190,000</td>
</tr>
</tbody>
</table>

+23%

• And web based attacks continue to grow
• FakeAV depended on fear to work
• When everyone knows its fake, there is no fear and the scam fails.
• So cybercriminals moved to ransomware

• Fear of arrest

• Simple and for bad guys safe method of paying “fine”

• At $100-$400 a victim, very profitable.
Ransomware exploded globally in 2013

With only online payment options limiting its reach

With 1.5 million internet connected computers even the Palestine Territories is a big enough target for criminals
Ransomware

500% increase in Ransomware attack in 2013
Ransomcrypt

- What happens when people stop fearing ransomware – Cryptolocker!
- Cryptolocker most prevalent threat – category called ransomcrypt
- No pretense of a fine.
- Pay to get your files back.
Ransomcrypt - Some Perspective

Number of attacks small

- December only 0.2 percent of all ransomware identified as CryptoLocker.

This type of threat is not new

- Trojan.Gpcoder (May 2005)
- Trojan.Ransomcrypt (June 2009)

What is new is

- Online payment methods
- Good encryption
  - Cryptolocker uses RSA 2048 Encryption

It is poised for growth
Mobile

Creation of new mobile malware slowed as malware authors focused on improving existing malware.

The average number of variants per family in 2012 was 1:38, increasing to 1:57 in 2013.
50% DON’T USE BASIC PRECAUTIONS SUCH AS PASSWORDS, SECURITY SOFTWARE OR BACK UP UP FILES FOR THEIR MOBILE DEVICE

Source: 2013 Norton Report
Mobile & Social

DELETE SUSPICIOUS EMAILS FROM PEOPLE THEY DON’T KNOW

HAVE AT LEAST A BASIC FREE ANTIVIRUS SOLUTION

AVOID STORING SENSITIVE FILES ONLINE

Source: 2013 Norton Report

Internet Security Threat Report 2014 :: Volume 19
Mobile & Social

- Fake Offering Scams Continue to Grow
Mobile & Social - Scams

Typical social media scam

- Promise something of value
- Trick users into giving up personal information, signing up for unwanted services, installing unwanted software, etc.
- Get victim to help make scam viral
Mobile & Social - Scams

OMG An accident on Roller Coaster in Disneyland Paris

Another Facebook hoax which hunts for unaware users

Posted on May 20, 2014 by CWZ in Facebook Malware #1 Comment

WOW - Guarda che storia
Saturday at 3:17 PM

:O TERRIBILE :O

(Video SHOCK) INCIDENTE TERRIBILE A DISNEYLAND PARIS...

688.9K Likes
What Happens When Social & Mobile Come Together?
Mobile & Social

• Everyone Likes to be Liked
• And there’s an App for that!
Mobile & Social

- Instlike gives you 20 free likes on your Instagram photos
- And you can buy more
Mobile & Social

- Just give the app developer your login and password
- Don’t worry, he promises not to steal your account
Mobile & Social

• Thousands of mobile users willing gave away their email addresses and passwords for nothing more than a Like.

• Mobile users are at risk, even from themselves.
Thank you!

Bill Wright
Director, Cybersecurity Partnerships
Bill_Wright@symantec.com