The Changing Face of Malware Threats

...And What It Means for Your Business: Charting the history of cyber crime, exposing the current crop of techniques being employed and explaining the defensive steps your business would be wise to take.
The Changing Face of Malware Threats

Contents

Introduction: Read All About It ................................................................. 1
Timeline of Crime ..................................................................................... 2
Today’s ‘Hall of Shame’ ............................................................................ 2
June 2011: A Snapshot ............................................................................. 4
Face Down the Threats ............................................................................. 4
Introduction: Read All About It

• Sobig Virus is Biggest of All
  Hundreds of thousands of home users and businesses have been hit by the Sobig virus over the past couple of days.

[BBC News Online, August 21st 2003]

• International Monetary Fund Cyber Attack Aimed to Steal Insider Information
  An investigation had shown a desktop computer “had been compromised and used to access some Fund systems”...the assault had lasted several months.

[Yahoo News, June 12th 2011]

It’s now very rare for massive malware outbreaks to grab the headlines like Sobig did eight years ago as it overwhelmed email inboxes, choked networks and slowed PCs worldwide. But stories like the assault on the IMF are seizing more column inches.¹

This trend is symptomatic of a seismic shift in the internet threat landscape, with cyber-criminals increasingly forsaking their classic blunderbuss approach to spreading malware – an approach whose main aim was to disrupt, to inconvenience and to say ‘look at me’.

Now, a more targeted strategy has steadily gained ground, with surgical strikes launched at selected victims in a bid to access commercially valuable, confidential information. Bidding to stay undercover and drain away data for as long as possible, saying ‘look at me’ is the last thing the perpetrators want to do. And while most of these attacks never reach the newspapers, the (often undetected) damage sustained by victims – with losses resulting from an instance of data leakage, for example, amounting to perhaps many thousands of pounds – is frequently much more serious than the harm caused by the old-style weapons of mass disruption.

Furthermore, targeted attacks stand at the apex of a whole battery of new, increasingly sophisticated cyber-criminal techniques now assailing businesses.

So how and why have malware threats changed? And what does this mean for your organisation? In this White Paper, you can read all about the current breed of threats and the steps to take to defend your business from an array of dangers you really can’t afford to succumb to.

¹ See http://www.informationweek.com/news/government/security/229700151 (a suspected case of a company being targeted with keylogging malware) for another recent high-profile story.
**Timeline of Crime**

Malware has a long pedigree, from early specimens that spread slowly from machine to machine via floppy disk to the internet age of instant transmission anywhere in the world. And this history can be divided into four distinct eras, each with its own notable milestones:

<table>
<thead>
<tr>
<th>Era</th>
<th>Key Milestones</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dark Age</strong></td>
<td>• 1970s: Appearance of prototype viruses, e.g. Creeper.</td>
</tr>
</tbody>
</table>
| **Age of Expansion** | • 1980s: Malware exploits steady growth in email usage; term ‘computer virus’ becomes widespread.  
|                   | • 1987: First computer worm to cause widespread disruption – ‘Christmas Tree Exec’ – paralyses mainframes around world, sending copies of itself to every entry in victims’ email contact files. |
| **‘Golden’ Age**  | • 1990s-2000s: Exponential spread of internet ramps up threat.                |
|                   | • 1992: Early example of mass-media hysteria over ‘Michelangelo’ virus (a damp squib). |
|                   | • 1999: ‘Melissa’ virus shuts down email systems clogged with messages propagating it. |
|                   | • 2000: ‘ILOVEYOU’ (aka ‘Lovebug’), a virus sent in email attachments, attacks millions of computers and makes malicious changes to victims’ systems – the total cost to business estimated in millions of dollars. |
|                   | • 2003: ‘Sobig F’ sets record for volume of email triggered.                  |
| **Age of Stealth**| • 2007 onwards: Landscape starts to shift – new trend gathers pace as targeted attacks harnessing range of social engineering techniques and converged attacks operating across protocols pose game-changing danger to businesses. |
|                   | • 2010: ‘Stuxnet’ worm discovered in Iranian nuclear power plant.             |

As this timeline shows, we’ve arrived in an era where, alongside many tried and tested tactics, cyber-criminals make heavy use of innovative, devious methods for spreading malware that are characterised by subterfuge and stealth. Three key drivers have underpinned this evolution:

1. The evolving capabilities and increasing deployment of anti-malware security solutions, but the inability of conventional solutions of this kind to detect and block low-volume malware attacks.
2. The desire to generate profit by stealing information with a ‘street value’, or data that can be used in further attacks aimed at accessing such information.
3. Cyber-criminals’ perennial determination to exploit the changing ways people use the internet – with current fashions characterised by an increasing reliance on mobile/multimedia devices, fluidity between personal/work usage etc.

**Today’s ‘Hall of Shame’**

The specific malware threats now faced by businesses are multiplying and becoming more variegated on an almost daily basis. But in another sense, as noted above, they are also converging, as delivery techniques are mixed, matched and deployed across the spectrum of the internet.

Overall, then, today’s threat landscape looks more like a jungle. It’s a complicated terrain of smoke and mirrors that’s in a perpetual state of flux. But one feature remains unchanging – its vastness. In 2010, nearly 300 million new malware variants were in circulation around the internet (quite apart from the torrent of spam that continues to fly through cyberspace, clogging corporate inboxes and hogging bandwidth).

Yet it’s possible to see shapes in the mist and discern four core weapons that typify the cyber-criminals’ present modus operandi, summarised in the table overleaf:

---

<table>
<thead>
<tr>
<th>Weapon</th>
<th>Objective(s)</th>
<th>Strategy</th>
<th>Tactics/Methods</th>
</tr>
</thead>
</table>
| Targeted Attacks      | Locate confidential data tradable on cyber-black market and secretly extract it (often over extended period). | Dupe victim into downloading malware (trojan, spyware) by opening infected email/IM attachment or clicking infected weblink. | • Gather data on selected victim.  
  • Use data to develop email/IM designed to win victim’s confidence (e.g. from an ostensibly trustworthy source, on a trending news story of likely interest etc).  
  • Build up relationship with victim over extended period via email/IM.  
  • Send infected email/IM.  
  • Use viruses that embed themselves by exploiting zero-day vulnerabilities in widely used applications.  
  • Use ‘attack kits’ sold online via underground economy. |
| Infected Websites     | Access valuable corporate data, track browsing behaviour, cause networks to crash/ freeze, recruit computers to botnets, prepare terrain for serious malware infection etc. | Embed malware in bespoke ‘malsites’ or compromised legitimate websites, and lure victims into visiting them. | • Increase ‘footfall’ to infected sites by using weblinks embedded in email/IM.  
  • Insert infected banner adverts (‘malvertisements’) on legitimate sites.  
  • Infect legitimate sites through SQL (Structured Query Language) injection.  
  • Use ‘drive-by downloads’ to infect visitors without them taking any action.  
  • Use shortened URLs to evade suspicion. |
| Social Networking     | Spread malware or gather data for use in targeted attacks.                   | Exploit casual internet security habits of many social media users.       | • Use hijacked or spoofed accounts.  
  • Infiltrate user groups and send members emails containing infected weblinks likely to arouse their interest.  
  • Trawl Facebook etc for personal details, career data, names of friends, colleagues etc.  
  • Use personal data gathered from victims’ accounts to build up picture of them and so help frame convincing targeted attacks. |
| Mobile Threats        | Find ‘back door’ route into corporate networks for data-stealing and other malware. | Exploit informality of mobile devices (smartphones/laptops/tablets etc), which often breeds lower vigilance among users. | • Distribute malware via IM/email.  
  • Build trojans masquerading as legitimate apps and place them for sale on apps stores. |

**Table: Cyber-Crime Weapons in the Age of Stealth**
June 2011: A Snapshot

So what does this new landscape look like in an average month? Symantec.cloud’s threat data for June 2011 showed that:

- 1 in 301 emails harboured malware.
- 47% of this was contained in ‘bad’ weblinks – up 17% from May.
- 5,415 websites per day were blocked because they contained malware – up 71% from May.
- 87% of web blocks were made on legitimate, compromised websites.

Around 1 in 5,000 infected emails represented a targeted attack. While small in percentage terms, these attacks shouldn’t be underestimated – their overall volume is as substantial as the devastation they can cause. Indeed, between 2009 and 2010:

- the daily average number of targeted attacks grew by over 60%.
- the number of businesses targeted rose by over 17%.
- 7% of businesses faced over 50 targeted attacks during 2010 as the number of assaults on the most frequently targeted organisations dramatically increased.

And while 34% of the attacks were directed at Senior Managers, all levels of staff were potentially vulnerable as the perpetrators searched for weak points in corporate defences.

Face Down the Threats

The Age of Stealth has seen the malware threat to businesses – SMBs and enterprises – reach unprecedented heights in terms of volume, sophistication and potency.

So what can businesses do? A whole range of best practice IT measures can make an important contribution to security – from a vigorous patch/update management policy to ensuring all users are fully briefed on today’s threat landscape (for an extensive list of measures see Best Practices at www.symantec.com/business/threatreport/topic.jsp?id=best_practices).

But this won’t be enough to keep your organisation safe. Above all, most internet security vendors fail to deliver the requisite level of performance in two key sectors of today’s frontline in the war on cyber-crime:

- the need to protect against targeted attacks delivering bespoke malware.
- the need to secure web traffic and protect internet users from infected websites/weblinks.

Symantec.cloud’s suite of managed security services are equal to the task. With their blend of patented predictive heuristics technology (Skeptic™) and pioneering converged threat protection capabilities, they’ve consistently kept pace with – indeed kept a step ahead of – the evolution of the cyber-criminals’ toxic toolbox. Even completely new, one-off malware payloads are routinely stopped in their tracks, whatever the delivery mechanism.

Threats may change, but Symantec.cloud’s ability to protect your business doesn’t. To find out more visit our website at www.symanteccloud.com or contact us at CLD_Info@symantec.com.
Office locations

EUROPE

HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester GL3 4AB
United Kingdom
Main +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone +44(0)800917 7733

DACH
Wappenhalle,
Konrad-Zuse-Platz 2-5,
81829 München,
Deutschland
Tel +49(0)89 94320 120
Support +44(0)870 8503014

NETHERLANDS
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Main +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Freephone +44(0)800 917 7733

NORDICS
Business Center Nord
Lyngbyvej 20
2100 Copenhagen
Denmark
Tel +45 33 32 37 18
Fax +45 33 32 37 06
Support +45 88 71 22 22

FRANCE
17 avenue de l’Arche
Tour Egée
92671 Courbevoie
France
Tel +33 (0) 6 8089 8886
Support +44 (0) 870 850 3014

AMERICAS

UNITED STATES
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-Free +1 866 460 0000

HONG KONG
Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: +852 6902 1130

SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: +800 120 4415

CANADA
170 University Avenue
Toronto ON M5H 3B3
Canada
Toll-Free +1 866 460 0000

JAPAN
Akasaka Intercity
1-11-44 Akasaka
Minato-ku
Tokyo 107-0052
Japan
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: +531 121917

ASIA PACIFIC

AUSTRALIA
Level 14
207 Kent Street
Sydney NSW 2000
Australia
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1800 088 099
About Symantec.cloud
More than 55,000 organisations ranging from small businesses to the Fortune 500 across 100 countries use Symantec.cloud’s MessageLabs services to administer, monitor and protect their information resources more effectively. Organisations can choose from 14 pre-integrated applications to help secure and manage their business even as new technologies and devices are introduced and traditional boundaries of the workplace disappear. Services are delivered on a highly scalable, reliable and energy-efficient global infrastructure built on 15 data centers around the globe. A division within Symantec Corporation, Symantec.cloud offers customers the ability to work more productively in a connected world.