State of the Nation
A SNAPSHOT OF THE ONLINE THREAT ENVIRONMENT

Key Findings

The key findings of this report are:

- Cyber attacks continue to occur frequently and result in serious financial losses for private sector and government institutions
- Threats have evolved to become more silent and more insidious
- The most successful online threats combine social engineering and technical attacks to gain access to systems
- Spam continues to be an important vector for spreading malware, phishing and social engineering attacks
Key Findings ............................................................................................................. 1
Introduction............................................................................................................. 3
The Internet .............................................................................................................. 4
Threats ..................................................................................................................... 5
  Malicious Software ............................................................................................... 5
  Targeted Attacks ................................................................................................. 5
  Zero-day Vulnerabilities ....................................................................................... 6
  Software ............................................................................................................... 6
  Social Engineering ................................................................................................ 6
  Phishing ............................................................................................................... 7
  Identity Theft ........................................................................................................ 8
  Data Breaches ...................................................................................................... 8
  Spam .................................................................................................................... 9
  Mobile Threats ..................................................................................................... 11
Costs ....................................................................................................................... 12
Trends ..................................................................................................................... 12
Recommendations .................................................................................................. 13
References ............................................................................................................. 14
Introduction

IT security vendors, academics, government agencies and researchers are constantly evaluating cyber threats using a variety of tools and techniques and reporting on their findings.

But what can we make of all these facts, figures and industry predictions?

This report is an amalgamation of over 30 Internet security reports produced during late 2010 and 2011. It is a snapshot of key aspects of online security during this period and attempts to correlate and review the differing pieces of advice and trends available.

At the start of this review it was hoped to compare ‘apples with apples’, however it soon became apparent that there is no consistency in analysis and reporting making it impossible to make true comparisons of collected data. However, the result is still informative, an array of data and analysis giving a detailed snapshot of the online threat environment.

About the Author

Nigel Phair is an influential analyst on the intersection of technology, crime and society. He has published two acclaimed books on the international impact of cybercrime, is a regular media commentator and provides executive advice on cyber security issues. In a 21 year career with the Australian Federal Police he achieved the rank of Detective Superintendent and headed up investigations at the Australian High Tech Crime Centre for four years.

About the Centre for Internet Safety

The Centre for Internet Safety at the University of Canberra was created to foster a safer, more trusted Internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cybercrime and threats to cyber security.

The Centre for Internet Safety is hosted within the Faculty of Law at the University of Canberra. The University of Canberra is Australia’s capital university and focuses on preparing students for a successful and rewarding career.

www.canberra.edu.au/cis
The Internet

The table below gives a breakdown of Internet uptake and penetration across continental boundaries. This breakup serves as a guide to correlate across borders the impact, including the costs of global cyber crimes.

As Internet penetration increases in developing nations, specifically through the uptake of mobile devices, it follows that government, business and consumers in those nations will fall prey to a greater number of cyber crimes. It is likely the victimisation will mirror the cyber crime experienced by users in early Internet adopter nations.

Source: Internetworldstats

<table>
<thead>
<tr>
<th>World Regions</th>
<th>Population</th>
<th>Internet Users</th>
<th>Penetration (% Population)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>1,037,524,058</td>
<td>118,609,620</td>
<td>11.4 %</td>
</tr>
<tr>
<td>Asia</td>
<td>3,879,740,877</td>
<td>922,329,554</td>
<td>23.8 %</td>
</tr>
<tr>
<td>Europe</td>
<td>816,426,346</td>
<td>476,213,935</td>
<td>58.3 %</td>
</tr>
<tr>
<td>Middle East</td>
<td>216,258,843</td>
<td>68,553,666</td>
<td>31.7 %</td>
</tr>
<tr>
<td>North America</td>
<td>347,394,870</td>
<td>272,066,000</td>
<td>78.3 %</td>
</tr>
<tr>
<td>Latin America / Carib.</td>
<td>597,283,165</td>
<td>215,939,400</td>
<td>36.2 %</td>
</tr>
<tr>
<td>Oceania / Australia</td>
<td>35,426,995</td>
<td>21,293,830</td>
<td>60.1 %</td>
</tr>
<tr>
<td>WORLD TOTAL</td>
<td>6,930,055,154</td>
<td>2,095,006,005</td>
<td>30.2 %</td>
</tr>
</tbody>
</table>
Threats

Online threats come in all shapes and sizes, and although many of these threats are blended, below is a list of the most common.

Malicious Software

Malicious software (malware) is software inserted into an information system to cause harm to that system or other systems, or to subvert them for uses other than those intended by their owners. Over the last 20 years, malware has evolved from occasional ‘exploits’ to a global multi-million dollar criminal industry.3 Criminals no longer produce malware for notoriety, they produce it for financial gain.

There are over 60,000 unique new malware samples discovered every day, equating to a new piece of malware being created every 1.5 seconds. Trojans account for about 60% of new signatures.4

The U.S. remained at the top of the list of locations where malware is hosted. However, the percentage decreased nearly 10% in the first half of 2011 to 32.3%, compared to 42.1% in the second half of 2010.5

One of the more widely covered malware stories of the year concerned the Stuxnet worm. Stuxnet targeted highly sensitive SCADA systems, which monitor and control industrial, infrastructure or facility-based processes, and was remarkable for the sophistication of the code and the amount of work involved in its creation.6

Targeted Attacks

Almost forgotten in the wake of Stuxnet was Hydraq. Hydraq’s intentions were different compared to the cyber-sabotage of Stuxnet as it attempted to steal intellectual property from major corporations.7

Hydraq and the discovery of similar exploits has lead to the prediction that in time we will see a reduction in general global malware outbreaks, as criminals concentrate on localised, targeted attacks.8

The majority of attacks now originate from interaction with the Web. Whether these attacks occur during visits to legitimate websites that have been infected, through, malvertising or “drive-by downloads”, they have all contributed to this growing trend.

Email is still an important threat vector and needs to be given continued attention by organisations, due to its importance as a communications tool. Internal communications must be designed well enough to allow users to discern the difference between a legitimate
company communication and one crafted by a cyber criminal.\(^9\)

Zero-day Vulnerabilities

A zero-day exploit is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known. Exploiting zero-day vulnerabilities is one part of keeping an attack stealthy since these enable attackers to get malicious applications installed on a computer without the user’s knowledge.

Once inside an organisation, a targeted attack attempts to avoid detection until its objective is met. In 2010, 14 such vulnerabilities were discovered. Rootkits – software that enables continued privileged access to a computer while actively hiding its presence from administrators – also play a role. While rootkits are not a new concept, techniques continue to be refined and redeveloped as attackers strive to stay ahead of detection tools.\(^\text{11}\)

Software

Cybercriminals tend to target Microsoft, because its Office and Internet Explorer solutions have a higher market penetration than their competitors. But it is wrong to then label Microsoft code as more vulnerable than others: it is a numbers game and criminals target the larger numbers.

Attacks have continued to shift from operating systems and browsers to applications running on the computer. Researchers have noted problems with Adobe PDF documents for some years now, since the ability to run active scripts is enabled by default in Adobe’s Reader software. In 2010, PDF exploits became more widespread, and new vulnerabilities in Reader emerged regularly.\(^\text{11}\)

Social Engineering

The weakest link in the Internet security chain is the person in front of the computer (or digital device). The rise of online social networks has lead to increased social engineering.

Social engineering is a catch-all term for psychological tricks used to persuade people to give up personal information and/or money, or to take an action they shouldn’t (such as to inadvertently download malware). Social engineering targets human desires, fears and curiosity, convincing the victim to open an email attachment, follow a link, or fill in a form with sensitive personal information.\(^\text{12}\)

Scammers have found many social engineering sweet spots. One tactic preys on those who sympathise with victims of natural disasters around the world. For example, the earthquake in Japan that led to tsunamis and a nuclear incident was exploited in SEO poisoning attacks, social networking scams and malicious spam campaigns.

By using sensational headlines, scammers coax users into clicking on the links in their blended threat attacks, which lead to malicious web pages that can exploit client-side vulnerabilities.\(^\text{13}\)
Social networks are a Godsend to cyber criminals. The built-in trust among “friends” on social networks makes it easier for criminals to deploy successful attacks.  

Whether the attacker is targeting a CEO or another member of staff, the Internet and social networks provide rich materials for criminals to research for tailoring an attack. By sneaking in among our friends, hackers can learn our interests, gain our trust, and convincingly masquerade as friends.

A contributing factor to the dangerous efficiency of social engineering attacks is the URL shortener, a Web based service such as bit.ly and tinyurl.com that condenses long website addresses to better fit the character limits in Twitter and Facebook (now with over 500m users) messages. An attacker can use the shortened address to hide malware.

In addition, Facebook comes under regular criticism for its provision, implementation and explanation of user privacy features. Directions for setting privacy preferences are vague and unclear— if and when they’re provided.

Clickjacking attacks carry out actions such as granting access to valuable personal information and even making purchases.

Among the individuals in the EU27 who used the Internet, 4% reported that they suffered from an abuse of personal information sent on the internet and/or other privacy violations, 3% had a financial loss due to phishing, pharming, or payment card misuse.

### Phishing

Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers’ personal identity data and financial account credentials by pretending to be communications from a legitimate company or government department.

Phishing scams continue to flourish.

The technical resources needed to execute phishing attacks can be readily acquired through public sources. Some technical resources have been streamlined and automated, allowing use by non-technical criminals. This makes phishing both economically and technically viable for a large population of less sophisticated criminals.

A variety of tools are used for email delivery, phishing site hosting, and specialised malware and include:

- Bots/Botnets
- Phishing Kits
- Session Hijacking
- Abuse of Domain Name Service
- Specialised Malware

One ploy phishers have adopted is to attach an HTML file to the
spam message (as opposed to the HTML being part of the email body). This better avoids anti-spam filters and anti-phishing filters built into browsers. The HTML attachment, stored locally, is opened in the user’s browser. A form is then presented which is sent to a remote Web server.\textsuperscript{20}

The top five locations for Internet users falling prey to phishing scams:\textsuperscript{21}

- South Africa – 1 in 133
- United Kingdom – 1 in 221
- Canada – 1 in 317
- Norway – 1 in 343
- Netherlands – 1 in 377.2

Identity Theft

Theft of identity includes the fraudulent use of personal details such as a drivers licences or tax file numbers, without permission, or illegally appropriating another person’s identity for unauthorised gain.

Spyware monitors what a person does, particularly the password and username combinations they type in to access their bank and other accounts.

Even then, cyber criminals may progress subtly - logging on with fake credentials and diverting small amounts of money to another bank account - before eventually increasing the value of goods purchased through the bank account or diverting larger sums of money to their own accounts.\textsuperscript{23}

Data Breaches

Identity theft continues to be a high-profile security issue, particularly for organisations that store and manage large amounts of personal information.

Not only can compromises result in the loss of personal data undermine customer and institutional confidence, they can result in damage to an organisation’s reputation and can be costly for individuals recovering from the resulting identity theft.

Data-harvesting campaigns routinely steal passwords using malware or illegal technology like keyloggers that monitor a computer user’s activity. They are also occasionally leaked by poorly secured websites. The biggest such incident in 2010 affected over a million users of several popular sites operated by the Gawker Media group, while Mozilla’s leak of 44,000 sets of logins from its add-ons system

Online users’ identity is valuable to criminals. The following is a guide to the average price for identity documents within the criminal underground:\textsuperscript{22}

- Credit card – $3 (EU), $1 (US)
- Drivers License – $20
- PayPal accounts – 30% of the current balance

Cyber criminals gather online user identities through the use of spyware (also referred to as keystroke loggers). Rather than disrupt a computer, spyware does not let the owner know they have been infected.

45

The number of days to contain an insider attack. (HIP)
A snapshot of the online threat environment seems to have only affected inactive accounts.\textsuperscript{24}

In April 2011, Sony suffered a massive breach in its PlayStation video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts.

Spam

As spam expands into other areas online, traditional email spam still remains a significant problem, especially in business.

Spamming on social networks rose further in 2010, with 67% of people surveyed receiving spam messages, up from 57% at the end of 2009 and just 33% in mid-2009. Phishing and malware incidents were also rife, with 43% of users spotting phishing attempts and 40% receiving malware, plus it is likely that others are unknowing victims.\textsuperscript{25}

One of the biggest email scams is selling pharmaceuticals from offshore services. These emails promise to get around local drug control measures.

With the convergence of spam and malware, a growing proportion of spam messages are moving away from these more direct scams. Sending out malicious attachments continues to be widely practiced, but even more prevalent is the mailing of links to poisoned webpages. Operating in the same manner as any other scam, victims are tricked into clicking a link in a mail and are then led to a site that attacks their system with exploits.

The following graphs represent the type of spam received (Barracuda Networks) and the origin for spam (as a percentage) according to four vendors. Whilst there are some patterns, they are not representative across all graphs and therefore the statistics all tell different stories. Needless to say, spam is the vector of significant malware, phishing and social engineering attacks. It continues to work and as such will continue to be a major factor affecting online security.

With nearly half of the world’s Internet population coming from Asia, it appears quite under represented in these statistics, whilst the U.S and Europe are over represented.

\begin{center}
\begin{tabular}{|c|c|c|}
\hline
\textbf{10} & The percentage 18 – 35 year old who fail to keep anti-virus software up to date. (AVG) \\
\hline
\end{tabular}
\end{center}

\begin{center}
\begin{tabular}{|c|c|}
\hline
\textbf{67} & The percentage of people received spam messages on social networking sites. (Sophos) \\
\hline
\end{tabular}
\end{center}
A snapshot of the online threat environment
Mobile Threats

As smartphones and tablets, particularly with an Android operating system, become ever more popular, cyber criminals are increasingly relying on mobile devices for spreading malware, albeit from a small base.

One in six people had access to a high-tech mobile device by the end of 2010. The rapid upswing in sophistication of mobile technology resulted in a change in the way content is provided and how people interact with it. However, this change brings with it a wealth of new problems for security. For example, trojans hiding in legitimate applications sold on app stores provided a simple and effective propagation method.27

Many security issues focus on jailbroken devices, where the mobile security settings are unlocked to get more functionality.

Just as with other computing devices, hackers can gain access to a phone’s information by tricking a user into clicking on an unsecured link that contains malicious code. This would give the hacker a backdoor entry into a phone and all the information on it.28

Cross-platform trojans are beginning to dominate the malware landscape. In the first half of 2011, one new malware strain was discovered every twelve seconds. Most of these viruses are designed to enable spamming or other criminal activities.29

Some of the malware are legitimate pieces of software that were reversed engineered and malicious code injected prior to a re-publishing of the binary on non-Google markets around the globe. This malware takes advantage of users’ interest in the popular application for distribution.30

The more open nature of the Android app market and the design ethos of the operating system make the Android more exposed to attack than the locked-down iPhone.31

Cyber criminals are becoming increasingly adept at infecting smartphones with malware that sends out premium SMS messages, from which they can net money for every message.

As mobile devices become mainstream, online service providers will create special versions of applications to match each device platform. This process will cause older vulnerabilities to surface once again. In particular, mistakes around identification and authentication.

SMS, MMS, Bluetooth, and the synchronisation between computers and mobile devices are all examples of potential attack vectors that extend the capabilities of malicious actors.

Organisations struggle to accommodate the increase in number and variety of mobile devices employees bring to work and expect to connect with the corporate network, while maintaining traditional data and application security practices.32
Costs

There are many vendors and research centres who attempt to identity the cost of cyber crime. However the methodology used in some of these is untested and relies on a number of assumptions.

As with a legitimate business, cybercrime is driven by return on investment. The most costly cyber crimes are those caused by malicious code, denial of service, stolen devices and web–based attacks.33

Loss of data can have a devasting impact on an organisation. A cyber attack can result in financial damages and loss of reputation which may take years to recover.

In 2010, the average cost per incident of a data breach in the United States was $US7.2 million, an increase of 7 percent from 2009. The most expensive data breach to resolve cost one organisation $US35.3 million.34

According to the Cabinet Office, Cybercrime in the UK is estimated to have a yearly cost for:35

- Businesses £21bn
- Consumers £3.1bn
- Government £2.2bn

The global cost of cybercrime has also been calculated by Norton at $114 billion annually with men between 18 and 31 years old who access the Internet from their mobile phone as the most likely victims.36

Trends

The online threat environment continues to evolve. As governments, businesses and consumers look for more ways to interact online, criminals exploit such opportunities for financial gain.

Threats are becoming more silent, and more insidious, intertwined, comprising multiple components for attacking, infecting and compromising data.

In the future we will see:

- The proliferation of sophisticated mobile devices will have a substantial effect on application and data security.
- mHealth and eHealth systems are already using mobile devices to collect vital clinical health data and as such will be opened up to traditional network vulnerabilities.
- More pieces of critical infrastructure could also have their vulnerabilities to exploitation by attacks similar to Stuxnet.
- Near–field communication, such as smart wallets which enable users to send information quickly to electronic readers by simply tapping their phones against them will be open to exploitation.
Recommendations

Government must lead and provide people with clearer advice about what they should be doing to protect themselves from online fraud and theft.

Businesses are also at fault, with too many organisations delegating responsibility to IT specialists within their firms rather than consider them as a whole of business issue. There are a number of aspects to protecting the modern enterprise. These include:

- Constant monitoring for network threats
- Identify and encrypt sensitive data
- Keep critical systems patched
- Enforce an effective password policy
- Educate users on the changed threat landscape
- Remember not to reveal sensitive information online, particularly in social media
- Report cybercrime to the police

There are a number of aspects organisations need to consider when dealing with online consumers. These include avoiding sending “phishy”-looking email messages by following these guidelines:

- Do not request personal information through email.
- Do not redirect to another domain from the URL provided to customers.
- Do not rely on pop-up windows for data collection, especially those with no address bars or navigational elements.
References

7. n 3, above, Trend Micro
8. n 5, above, M86 Security
10. n 7, above, Symantec
11. n 6, above, Sophos
13. n 9, above, M86 Security
15. n 7, above, Symantec
16. n 6, above, Sophos
18. www.apwg.org
20. n 5, above, M86 Security
21. n 7, above, Symantec
22. n 4, above, Trend Micro
24. n 12, above, Sophos
25. n 6, above, Sophos
27. n 7, above, Symantec
28. n 14, above, AVG
30. n 14, above, AVG
31. n 6, above, Sophos