RISK ATLAS
CYBER CRIME

Hacking into insecurities

Cyber crime is becoming increasingly sophisticated, and increasingly malicious

ON 2 NOVEMBER 1988, 22-YEAR-OLD CORNELL UNIVERSITY student Robert Morris released an internet worm capable of exploiting vulnerabilities in UNIX operating systems, infecting an estimated 10% of the internet. Over 20 years on, the scale of computer crime has grown astronomically. Internet attacks today are organised and designed to steal information from consumers and corporations.

The scale of global cyber criminal operations has reached such proportions that internet security firm Sophos discovers one new infected webpage every 4.5 seconds – 24 hours a day, 365 days a year. In addition, Sophos is sent some 20,000 new samples of suspect code every single day.

The USA, China and Russia account for almost three-quarters of the world's websites that spread malware, according to research by Sophos. The US tops the chart, with just under three in every eight infected webpages based there. China, which was responsible for hosting more than half (51.4%) of all the world's malware in 2007, has now almost halved its contribution to the problem.

The Czech Republic is a new entrant on the list and hosts over 1% of all the world's malware. Poland, France, Canada and the Netherlands were in positions six, eight, nine and 10, respectively in 2007, but now have too few malicious websites to appear on the chart.

No one is immune

A number of well-known organisations have fallen foul of malware, including thousands of websites belonging to Fortune 500 companies and government agencies, which were infected in January 2008.

Traditionally done through emails, cyber criminals now primarily use the web to infect computers, often driven by political motivations. Immediately before releasing a series of leaked diplomatic cables, Sweden-based WikiLeaks (the whistleblowing website) suffered several distributed denial of service (DDOS) attacks, which succeeded in putting the website temporarily offline.

In an apparent act of revenge, sites that had refused to support WikiLeaks were targeted in return, with Mastercard briefly being forced offline and Amazon also targeted. The 'hacktivist' group Anonymous, which had previously mostly confined its actions to anti-pirate organisations and the Church of Scientology, was widely believed to have had a hand in these attacks, dubbed 'Operation Payback'. **SR**

Top malware hosting countries

Rank	Country	
1	**USA**	37%
2	**China**	27.7%
3	**Russia**	9.1%
4	**Germany**	2.3%
5	**South Korea**	2.1%
6	**Ukraine**	1.8%
7	**UK**	1.7%
8	**Turkey**	1.5%
9	**Czech Republic**	1.3%
10	**Thailand**	1.2%

NB: Figures from US-based organisations

Where internet criminals reside

Rank	Country	
1	**USA**	65.9%
2	**UK**	10.4%
3	**Nigeria**	5.8%
4	**China**	3.1%
5	**Canada**	2.4%
6	**Malaysia**	1%
7	**Spain**	1%
8	**Ghana**	1%
9	**Cameroon**	1%
10	**Australia**	1%

Iran

In October 2010, a computer virus called Stuxnet disrupted nuclear facilities in Iran. Stuxnet represented a significant leap forward in malware in that it specifically attacked software used in industrial infrastructure. There are rumours that Stuxnet may have also caused the failure of India's INSAT-4B satellite in July 2010.

Belgium

In May 2008, Belgium accused the Chinese government of cyber-espionage, claiming that hacking attacks against the Belgian government had originated in China. Separately, Belgian minister of foreign affairs Steven Vanackere said that his ministry had been the subject of cyber-espionage by Chinese agents.

Georgia

As tensions rose over South Ossetia in August 2008, Russian and Georgian hackers launched attacks against each other. This included distributed denial of service attacks and the defacement of the Georgian Ministry of Foreign Affairs website using pictures of Georgian president Mikheil Saakashvili and Adolf Hitler.

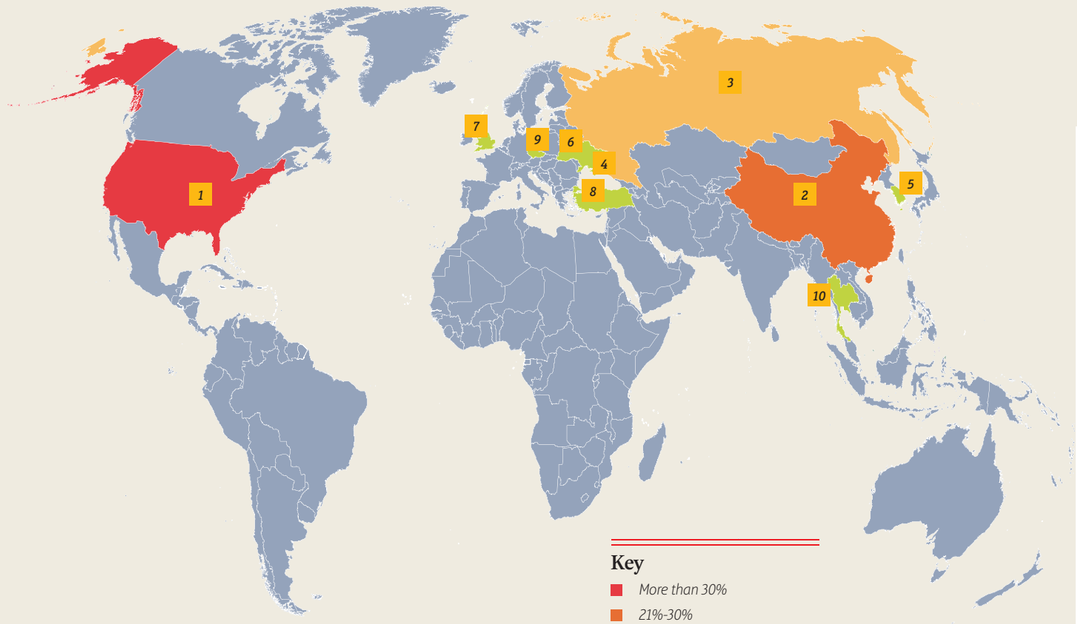
South Korea

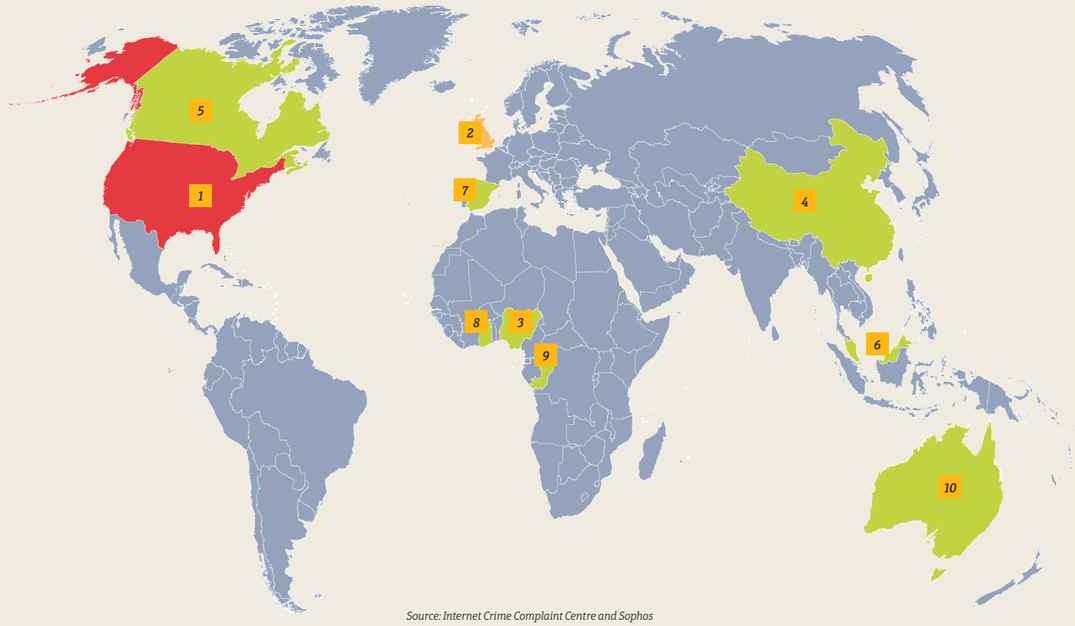
In September 2008, Seoul accused adversaries North Korea of stealing documents from military officers using spyware and a female agent. The spyware attack saw malicious email attachments designed to steal documents from infected computers.

India

Government officials in New Delhi were said to have confirmed that Chinese hackers targeted the Ministry of External Affairs and the National Informatics Centre, which provides the network backbone for central and state government. The unnamed officials claimed that this was China's way of gaining "an asymmetrical advantage" over a potential adversary.

Source: Various media and Sophos 2009 Security Threat Report





Source: Internet Crime Complaint Centre and Sophos

EXPERT VIEW

Evelyn Rieger is a senior underwriter at Allianz

No certain safety

IT networks are essential to company management on all levels, including for example, R&D, production, purchasing and sales of goods, and provision of services. Processes, performance and results of a company therefore heavily depend on reliable IT systems, and any disruption of those systems can have a major impact.

IT risks such as malicious code attacks, user errors, wrong command input, and non-availability of systems can result in significant additional expenditures and even business interruption (BI). Today, corporations use electronic data exchange for communication – internally and externally – so what happens if a company causes damage to another during this process?

Far too often, these scenarios are underestimated and companies deem themselves secure by the use of firewalls and data back-ups, but total security is not achievable. Why is that? Data is invisible, and so are data claims at first. We all know the pictures of collapsed bridges and flooded landscapes – but the loss of data doesn't conjure up any images at all.

Attainable security is limited and needs to be supported by prudent risk management. However, management, mitigation and avoidance of risk also raise the question of how to handle the remaining risk; whether this is borne by the company itself or whether it is transferred to a third party – the insurer – to protect the company's balance sheet. Therefore both corporations and insurers are faced with the question of insurability of IT risks.

Traditional insurance pays for lost profit and standing charges as well as additional costs following a property damage. However, in many cases, BI and additional costs caused by IT faults occur without property damage (human error, misconduct, cyber crime, malicious code). Protection against such scenarios is becoming increasingly important.