



e-Espionage: how safe is your IP?

On July 30, 2010, David Irvine, Director General of the Australian Security Intelligence Organisation (ASIO), warned that 'corporate networks were as much a target as defence and security systems from increasing attempts by foreign cyber sleuths seeking to steal Australia's secrets'¹. John Faulkner, the Australian Defence Minister, added that, of more than 2400 'incidents on networks considered to be medium to high risk' in 2009, only 200 were directly related to defence.

What is e-espionage, how common is it, who is at risk and why are these attacks not detected? This White Paper answers these questions and more, and includes input from analysts and industry commentators.

What is e-espionage?

The term espionage means obtaining valuable or confidential information by theft, stealth and other illegitimate means, and the internet is now the most common route. These days electronic 'espionage by malware' is carried out by organised syndicates who have effected successful 'break-ins' on targets as diverse as the White House², Google³, Security Software vendor Kaspersky⁴ and the East Anglia University Climate Research Unit.⁵

A recent report to the US Government by aerospace company, Northrop Grumman, describes state-sponsored economic espionage as 'the single greatest threat to U.S. technology.'⁶ Estimates put the cost to US companies at around \$300 billion a year, with 'proprietary information being gathered by governments, local and international competitors, organizations, criminals, terrorists and individuals.'⁷ Experts in Europe estimate

¹ Australian Financial Review, July 30, 2010; p.1

² <http://www.zdnet.com/blog/gadgetreviews/report-chinese-hack-into-white-house-network/477>

³ <http://www.wired.com/threatlevel/2010/01/google-censorship-china/>

⁴ http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1347341,00.html

⁵ <http://news.bbc.co.uk/2/hi/8370282.stm>

⁶ Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Steve de Weese & Bryan Krekel, October 2009

⁷ http://www.globalsecuritygroup.com/services/counter_espionage.php

that espionage is costing German industry in excess of 50 billion Euros a year.⁸ In Australia in 2009, Deloitte set up a specific counter-espionage team in response to the growing number of incidents.

Mandiant, a specialist security firm working with Fortune 500 companies, says it 'has seen a dramatic change in information security incidents. Superbly capable teams of attackers have successfully expanded their intrusions at government and defence-related targets ... to researchers, manufacturers, law firms, and even non-profits.'⁹

These attacks use bespoke malware specifically designed for espionage and which, most importantly, 'standard security tools usually do not detect.' That is, the likelihood of undetected penetration by this type of attack is high.

Who is at risk?

Common targets for electronic espionage are:

- Intellectual property (IP) like inventions and new design concepts;
- Production techniques, processes and formulas, R&D;
- Customer and prospect databases kept by sales people;
- Data on pricing, prospective bids, sales, product or marketing plans/ideas.

Organisations most likely to be targeted include:

- Organisations in technology-centric industries like IT, biotechnology, aerospace, automotive, telecoms, energy and transportation;
- Financial organisations and those who trade online with high transaction volumes;
- Government bodies in defence or intelligence activities, and those who hold highly confidential data of commercial value or of value to other countries.

Stealthy and anonymous

Google described the attack on its operations in China as a 'highly sophisticated and coordinated attack on its corporate network'. The attackers penetrated apparently secure networks by using newly-identified vulnerabilities; they avoided detection by making seemingly normal outbound connections via common network ports and services; they used these normal connections to remotely access critical infrastructure controls and sensitive

⁸ <http://www.guardian.co.uk/world/2009/jul/22/germany-china-industrial-espionage>

⁹ Mandiant M Trends Report on Advanced Persistent Threats, February 7, 2010

information. Because of its stealth, this sort of attack is often only detected well after the assets are gone, if at all.

In 2008 Marathon Oil, ExxonMobil, and ConocoPhillips were unaware that they'd become the victims of electronic espionage. To make matters worse, it was not the IT security people who raised the alarm: the FBI alerted these oil companies early in 2009 that proprietary information had been flowing out to computers overseas.¹⁰ The espionage was focused on valuable 'bid data' detailing the quantity, value, and location of oil discoveries worldwide.

For obvious reasons espionage perpetrators operate in secrecy, but the victims of espionage tend to avoid exposure as well. Understandably, they want to avoid negative publicity and maintain the confidence of shareholders and consumers: revelations of break-ins may reveal long term vulnerabilities and encourage future attacks. In recent times there has been an undeniable trend in the increasing numbers of "isolated" cases.

How the attacks are made

According to Alan Paller, director of research at SANS Institute 'the attack of choice involves targeted spear phishing with attachments, using well-researched social engineering methods to make the victim believe that an attachment comes from a trusted source.'¹¹

These 'social engineering' methods involve little more than gathering information about people of interest via 'open sources' like *LinkedIn*, *Facebook* and *MySpace*. Hackers' messages frequently masquerade as those from legitimate sources, by including specific content such as a reference to recent meeting or a seemingly *bone fide* attachment. These techniques have been successful in breaching even high security research institutes like Oak Ridge National Laboratory and Los Alamos in the USA.¹²

Often the seemingly *bone fide* attachments contain exploit code which instructs the user's machine to download an undetectable malware Trojan. Once activated, the Trojan allows the attacker to gain control of the user's PC to upload specific files or e-mails or, more importantly, to access the broader network.

¹⁰ <http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved>

¹¹ http://www.pcworld.com/businesscenter/article/141474/cyber_espionage_a_growing_threat_to_business.html

¹² <http://www.networkworld.com/news/2007/120707-cyberattack.html>



Once access to the network is gained, the intruder can steal domain administrative credentials and use them to impersonate legitimate users, sending and receiving apparently genuine e-mails and documents. They can also install multiple backdoors across the network to gain a broader foothold in the organisation and secure a reliable return route for a future visit.

Persistent attacks target dozens of systems and steal the user credentials needed for access. They plant various utilities to capture data and steal e-mails, they list running processes and install dormant executables. Stolen data is then sent to the attackers' remote servers and, if they detect remediation efforts, they'll try to establish additional footholds and modify their malware. Don't be fooled; this isn't conjecture, it's reality.

Why they're not detected

You probably have a full array of defences in your organisation, and your security team is watching their logs and reports, so how could attackers get through your firewalls, intrusion detection systems, spyware catchers, virus scanners and SIEM systems?

The answer is simple. These attacks are far more difficult to detect or prevent than the hacks of old. They are specifically designed to circumvent your organisation's defences. More than this, most security point solution vendors concede that rules-based *detect and prevent* techniques are almost powerless against these targeted malware attacks.

Applying the rules of supply and demand to this darker parallel universe; if a prospective thief covets your information assets, it's all too easy to find malware to target and upload them. Some authors of malware even provide *performance guarantees and help desk facilities to maintain and support their illicit software*. This is why most security scanners fail to detect this sort of malware. It doesn't match known signatures or patterns, because it is designed not to. According to some experts, current antivirus solutions only detect between 5 to 25% of this kind of malware.¹³

Allan Paller from the SANS Institute says that the people engaged in economic espionage are often the same people doing military espionage, using similar techniques to steal information from commercial organizations working in the attackers' country.¹⁴ Specialised

¹³ Malware: Stopping Cyberattacks, SC Magazine May 25, 2010

http://whitepapers.scmagazineus.com/index.php?option=com_categoryreport&task=viewabstract&title=8845&pathway=no

¹⁴ http://www.pcworld.com/businesscenter/article/141474/cyber_espionage_a_growing_threat_to_business.html

Trojans have long been used by security agencies to siphon off vital intelligence, as Mossad reportedly did to obtain information on nuclear facilities in Syria.¹⁵

However, it's not only military intelligence at risk. For example, a Trojan attack on an Australian financial institution in 2008 fooled the firewall security and enabled documents to be sent to a hostile website straight through an open firewall port. However, the firewall showed the offending port closed and there were no alerts to the contrary from other security systems. The attack was stopped when behaviour-based security technology detected that, unusually, significant amounts of information were trying to traverse the firewall.

Attacks from inside too

Sometimes even members of your own staff steal company information. Disgruntled employees or departing employees often take confidential information out of spite or a misguided sense of entitlement. Stolen data are often customer details, prospect or price lists, marketing plans, new product details, financial information and IP.

In a high-profile 2009 example, US company Starwood (owner of Sheraton, Westin and Le Meridien brands) filed suit against the Hilton Hotel group after it hired a number of Starwood executives. According to the lawsuit, trade secrets were taken which Hilton used to develop its new Denizen Hotels concept. Starwood claims that the former head of its luxury brands group downloaded 'truckloads of documents when printed' on his laptop computer.¹⁶ Other times, when thieves target smaller amounts of specific information, their loss is more difficult to spot.

What about DLP?

To address this, many vendors have developed Data Loss Prevention (DLP) solutions which promise to prevent accidental or deliberate removal of sensitive information from the enterprise. To use these systems, assuming you know where all your sensitive information resides, you first must classify it by degree of sensitivity and then keep it all updated as sensitivity changes over time. For many organisations, this set-up process can be complex and ongoing operation overly onerous.

¹⁵ <http://www.haaretz.com/print-edition/news/der-spiegel-mossad-hacked-syrian-computer-to-uncover-nuclear-site-1.4911>

¹⁶ <http://www.guardian.co.uk/business/2009/apr/17/industrial-espionage-hotel-industry-lawsuit>



Nick Selby, head of enterprise security research at The 451 Group, makes the point that 'enterprises don't know where their unstructured data is, let alone where their sensitive data is. Putting a box at the gateway doesn't solve the (data loss) problem, but highlights it.'¹⁷ Most importantly, any self-respecting, prospective thief will be well-informed about these sorts of systems and able to achieve his objectives without detection.

These attackers are different

Traditional security solutions were conceived in the days when malware was launched by mischievous students in dark basements. Modern targeted malware attacks mark the transition from basements to highly organised entities, who seek significant profits from the information they steal. It's no surprise that the incidence of espionage is growing.

For instance, also in July 2010, Siemens reported a disturbing development: targeted USB-borne malware, called Stuxnet, was detected on the company's Security Control and Data Acquisition (SCADA) networks. SCADA systems are used globally by most industrial, utility and infrastructure companies to monitor and control automated plants. This Trojan was designed specifically to attack these systems, to steal corporate information or seize control of SCADA networks without detection¹⁸. This development, predicted for some years now, has obvious implications for us all.

Better tools are needed. More of the same will not do the job, as Ernst & Young confirms: 'simply shoring up existing and conventional defenses is not enough ... because these types of threats require several layers of defense to counter.'¹⁹

A need for higher intelligence

Changes in user and IT system behaviour are often the earliest indicators of imminent malicious or profit-motivated activity, such as the employee unusually downloading 'sensitive information'. This is why many organisations with highly sensitive data who want protection from targeted malware and internal misuse, choose technologies based on Behavioural Anomaly Detection (BAD) and Analysis. These intelligent systems learn about the nature of activities in the enterprise, detect any that are unusual, interpret them within

¹⁷ <http://www.networkworld.com/research/2008/010708-data-leak-selby.html>

¹⁸ <http://www.itnews.com.au/News/220389,virus-targets-siemens-industrial-control-systems.aspx>

¹⁹ [http://www.ey.com/Publication/vwLUAssets/Insights_on_IT_risk_-_04_2010_-_Countering_cyber_attacks/\\$FILE/EY_Insights_on_IT_risk_04_2010_-_Countering_cyber_attacks.pdf](http://www.ey.com/Publication/vwLUAssets/Insights_on_IT_risk_-_04_2010_-_Countering_cyber_attacks/$FILE/EY_Insights_on_IT_risk_04_2010_-_Countering_cyber_attacks.pdf)



the context of information available, and alert IT security staff to investigate discernable threats.

Using behavioural analysis, attempted theft of valuable information, be it launched from without or planned from within, can be detected at the time the unexpected activity is occurring, rather than after the loss has been detected, days or months later. This is the difference between rules-based security systems that rely on rules to be broken and those that add a layer of behavioural interpretation to the data they collect.

For the informed insider or organised outsider planning e-espionage, the rules and where they apply are already anticipated. If the rules are known and the attack is almost impossible to anticipate, many organisations conclude that the best protection is the intelligence to detect, investigate and respond to unusual, potentially malicious activity - as it is happening.

* * *

Author: Peter Woollacott, Co-Founder & CEO, Tier-3

<http://www.tier-3.com/>



Peter has 25 years of senior executive experience including almost 15 years with Lend Lease Corporation. He has extensive strategic advisory and operational expertise having provided specialist consulting services to a number of major companies in Australia and internationally including: AXA, PWC, Bain International and others.

Peter holds an Honours Degree in Building (Melbourne), a Master of Applied Finance and Master of Business Administration (Macquarie), and he continues to lecture in executive post graduate education at Macquarie and Sydney Universities.

Other White Papers by this author include:

[*Cloud Computing: How Secure are You?*](#)

[*Compliance: More Opportunity than Obligation*](#)

[*Security: Are you really OK?*](#)

[*How to Break Down Information Silos*](#)

[*How to get Serious ROI from Security Software*](#)

[*How to Avoid Painful Security Catchup*](#)