

THE
HACKERS



CYBERCRIME SCENE

*Crime dramas bring whizz bang technology for tracking down the baddies into our TV rooms every night, but what happens when it's the criminals with the high-tech? **STUART CORNER** takes a look at how security intelligence software is helping those involved in corporate security and justice to narrow the field of suspects, and keep the cybercriminals at bay...*

Somewhere out in cyber space there's a group of criminals that has been busy hoovering up commercially and politically sensitive data from the IT systems of hundreds, maybe thousands, of organisations for over a decade. And it's showing no signs of stopping.

The group's activities and its technique, known as NetTraveler after the tool they use, have been spelt out in great detail by IT security technology company Kaspersky (<http://bit.ly/1ONUPVw>) "They have successfully compromised more than 350 high profile victims in 40 countries... [but] we estimate the total number of victims worldwide to be around 1000," the report says.

"The group has infected victims across multiple establishments in both the public and private sector including government institutions, embassies, the oil and gas industry, research centres, military contractors and activists."

Initial penetration of compromised systems was made via seemingly innocuous emails about the Dalai Lama's visit to Switzerland and a report on defence spending in Asia, amongst others.

don't know it yet," he says.

"It is more likely now that intrusions will go undetected because criminals are very well resourced. It is now a question of how to have holistic and complete management of the risks, rather than a belief that you are secure because you have updated your anti-virus software."

Interestingly he points out that remote countries can be particularly vulnerable to cyber attacks. While their location insulates them from biological threats to a greater degree, Richardson says there is no such protection from cybercrime. "The attack can be someone in a garage in Russia, or in China, or any other country for that matter."

He says a new openness from normally secretive national cyber security bodies is evidence of the magnitude of the problem, and of how seriously governments are taking it.

"You're seeing the NSA in the US, the GCHQ in the UK and GCSB in New Zealand being very open about the fact that there are significant challenges and that engagement with the private sector is fundamental to meeting these challenges.

"That is a big shift. Those agencies have traditionally operated in isolation, but they are now saying 'this is a big challenge and without public sector collaboration, criminals will find the weakest point in the chain'."

The biggest worry of all is the Advanced Persistent Threat. This is where the bad guys target you because you have something very specific that they want - perhaps the intellectual property on which your entire business depends - and they will explore every avenue to get in to your systems and then spend as long as it takes to invade and manipulate them until they get what they want.

According to David Owen, director of strategy for security consultancy BAE Systems Detica, the time it takes the criminals to find what they are looking for after a successful infiltration provides the best opportunity to stop them.

"From initial infiltration to information leaving the organisation can take months because the bad guys have to do the reconnaissance, spread inside the environment and find the information they are looking for. It is a misconception that hacking activity happens really quickly. So there is >>

INVESTIGATION

CRACKING THE SAFE

That's just one of hundreds of threats that IT security managers face every day. Take a look at the multitude of reports on cyber security issues produced regularly by security technology companies like Trend Micro, Symantec, Trustwave, etc. You'll wonder how any chief security office (or CSO) gets a decent night's sleep. These reports are the stuff of nightmares: the range of threats is multiplying; the bad guys are getting smarter.

According to Craig Richardson, managing director of Wynyard Group, a specialist in intelligence-led software and solutions, every organisation has been compromised and most don't discover this for months. "There are two sorts of organisations: those that have been hacked, and those that have been hacked and

a window there to take steps to prevent it.”

It seems that many organisations are missing out on this window of opportunity. “We have found that on average when we get called in to an organisation they have been compromised for more than 300 days,” Owen says.

One reason for this long delay he says is that, “Attackers are very focused on making sure their attacks are not detected. If they can elongate the window before the organisation realises they have been compromised it gives them more time to get the information out of the organisation.”

“THERE ARE TWO SORTS OF ORGANISATIONS: THOSE THAT HAVE BEEN HACKED, AND THOSE THAT HAVE BEEN HACKED AND DON'T KNOW IT YET.”

CRAIG RICHARDSON, MANAGING DIRECTOR OF WYNARD GROUP

He says that security is about constant vigilance, an acknowledgement that compromise is inevitable and therefore a focus on protection of the ‘crown jewels’.

“One of the key questions for a lot of clients is to identify, out of all the information they have, the key information that is really worth protecting and then trying to constrain the proliferation of that information to some extent.”

OPEN UP TO BE SECURE

Owen says technology alone cannot provide security. Constant vigilance and expertise to understand and interpret what the technology has to say are just as important. Here organisations face a choice between using internal expertise or outsourcing to a managed security service provider. Both options have their limitations: to be effective an external provider must have sufficient understanding of the client’s business to be able to identify the most important information. At the same time, it’s hard for an internal security professional, working in isolation to keep abreast of current threats and the weapons to fight them.

In this respect security professionals can be their own worst enemy. IBM has just released a white paper *‘Truth behind the trends’*, a distillation of learnings gleaned from interviewing 87 IT leaders from companies across a range

of industries. Commenting on the findings, Scott Ainslie, security expert for IBM A/NZ, says, “Security people tend to be somewhat introspective and a little insular. So it is always a challenge to get them to speak about the problems they have within their company. It was quite interesting to discover that they don’t share information. As a consequence they think that the problems they are encountering are unique to themselves.”

Ainslie says that this insularity compromises security professionals’ ability to protect their

companies. “It means they try and tackle their problems independent of external advice, and from our experience getting external advice or seeking collaboration from like-minded people is very helpful. More often than not the problems they are facing are not unique and if they work together collaboratively their chances of finding a solution are much greater.”

The importance of information sharing to boost IT security has been recognised by Gartner. It has just published a research paper *‘Information sharing as an industry imperative to improve security’* in which it “assesses the current state of data sharing and provides recommendations for enterprises and vendors”.

According to author, Anton Chuvakin, “Security-data-sharing tools and practices are gaining mind share. Increasingly, enterprises are realising that they must break with insular ‘every one for themselves’ mind-sets and band together to confront escalating threats.”

He says that every organisation should “establish a new functional group to undertake and co-ordinate sharing efforts and should expand sharing efforts and relationships to involve supply chain partner organisations, customers and end users.”

It seems, however, that a fortress mentality still pervades much of the thinking in IT security. According to Jason Clark, chief security officer

of IT security vendor Websense, CSOs need to change the way they engage with the business and the board and the way they look at risk.

“Today organisations have infrastructure and compliance-based security programmes, which means they just check the box and go and buy what their friends are buying, or what the vendors tell them to buy.

“Eighty percent of the spend on security goes on firewalls, IPS [intrusion protection systems] and endpoint security. And that is according to Gartner, Forrester, IDC and all the top resellers in the world,” he says.

Much of this is money down the drain, according to Clark. “Those stop about 25 to 30 percent of the problem. That is insanity!”

Clark says that more of the security budget should be diverted to new methods of detection and prevention and the money spent on what he calls ‘compliance’ technology, like firewalls, be reduced by buying basic products.

Clark argues that being constantly on the lookout for abnormal activity and keeping a constant check on what data is leaving a company (and companies ought to know what should and should not be going out) presents a much better chance of preventing data loss and minimising damage.

THE ‘BIG DATA’ MUSCLE

A relatively new approach to IT security is big data analytics. ‘Big data’ is all the large amounts of related but unstructured data that can be gathered and analysed in the hope of finding useful information. It is being widely applied to improve sales and marketing strategies and customer retention, but the technique can equally be used to track down malware or an intruder ferreting around inside a computer network.

According to IT security vendor, McAfee, the full potential of big data is not being exploited. It has just released a report *‘Needle in a datastack’* that, it says, “reveals how organisations around the world are ... vulnerable to security breaches due to their inability to properly analyse or store big data”.

According to McAfee, “The sheer volume of security-relevant data facing an organisation these days can make identifying a threat like looking for a needle in a haystack. Yet collecting

more data can also play a transformational role in information security and organisations must become smarter at harnessing the right information to protect themselves from the unrelenting threats they face every day.”

There is some urgency to businesses realising the potential of big data, before the cybercriminals do. According to Kate McGavin, senior product marketing manager with EMC subsidiary RSA, cybercriminals are also using big data principles to improve their own efficiency. “Cybercriminals can now sort their collections of data more quickly to extract financial details and view performance metrics for current malware applications,” she warns.

A major hurdle for business is finding people skilled in IT security and big data analytics, both fields that are growing rapidly and where skills are in short supply. According to Detica’s David Owen, “There is a real question as to how we educate more people to have the sophisticated skills in the IT security space. If we don’t do that there will be massive salary inflation.”

And he says we cannot look to universities to fill the gap. “The teaching in some of the

university courses in computer science is quite classical. It is very expensive for a university to evolve its syllabus every year.”

In the meantime, more specialised institutions are filling the gap, however, according to Websense’s Jason Clark, successful security professionals need more than technical skills: they need high-level interpersonal communications skills to get the security message to company boards. “The average tenure of a CSO in the US is 16 months,” says Clark, and lack of communication skills is the number one reason for their precipitous departures.

“They might be very smart and very good at IT, and they might know how to stop the bad guys, but they don’t know how to articulate that. They don’t know how to talk to the board and sell the business on why they need to do certain things. They start locking things down and they don’t last very long. Either they get frustrated because nothing changes or the company gets rid of them because they are causing problems.” 

“TECHNOLOGY ALONE CANNOT PROVIDE SECURITY. CONSTANT VIGILANCE AND EXPERTISE TO UNDERSTAND AND INTERPRET WHAT THE TECHNOLOGY HAS TO SAY ARE JUST AS IMPORTANT.”

DAVID OWEN, DIRECTOR OF STRATEGY AND MAJOR CLIENT GROUP FOR BAE SYSTEMS DETICA