FINANCIAL REVIEW

SE	Information
HD	**Tracking spies: the rise of private cybersecurity**
BY	Christopher Joye
WC	1,620 words
PD	28 January 2014
SN	The Australian Financial Review
SC	AFNR
ED	First
PG	21
LA	English
CY	Copyright 2014. Fairfax Media Management Pty Limited.

LP

One of the world's fastest growing and most sophisticated private cyber intelligence agencies, FireEye, which on January 2 announced the $US1.6 billion ($1.8 billion) purchase of its equally spooky peer, Mandiant, is led by the archetype of the modern digital warrior.

The brawny and bronzed deal-maker David DeWalt – a wrestling champion who competed at the US Olympic trials – was previously CEO of the anti-virus provider McAfee, which he sold to Intel for $US7.7 billion in 2010.

TD

Trained as a computer scientist, DeWalt, 49, has bought and sold more than 50 technology companies and joined FireEye 15 months before its spectacular September 2013 NASDAQ listing, when its share price almost doubled on debut to $US40.

The Australian Financial Review has previously flagged cybersecurity as a space for investors watch.

FireEye's acquisition of the profitable Mandiant, which famously published 74 pages of evidence linking 40 malicious software ("malware") families to Unit 61398 of the People's Liberation Army signals intelligence department (known as "3 PLA"), sent its stock price soaring 39 per cent higher the next day. This trend continued through January with the share price touching $US73.57 in recent days, 79 per cent above its January 2 level.

DeWalt's equity has ballooned to $US322 million while FireEye's founder and chief technology officer, Ashar Aziz, has watched his holding's value jump to $US737 million.

FireEye and Mandiant are at the vanguard of the next generation of 24/7 network monitoring and incident response service providers that help big corporates battle committed and motivated intruders, called "advanced persistent threats" (APTs), that easily circumvent conventional firewall and anti-virus solutions.

APTs range from sovereign states to organised crime syndicates.

In an exclusive interview with The Australian Financial Review, DeWalt explained his rationale for absorbing Mandiant, which he independently chaired, and addressed criticisms sourced from local players.

Any question that cyber risks were being exaggerated has been answered by a spate of recent revelations, including the stunning disclosures by Edward Snowden and Mandiant about the extent to which countries like the US and China are spying on public and private targets. The devastating December breaches of eight major US retailers that allowed eastern European criminals to steal credit card data belonging to over 100 million people, again alerted the masses to the dangers.Huawei's ban from NBN

Pervasive state surveillance also raises the spectre of technology protectionism in sensitive industries like critical infrastructure, with Huawei's blanket ban from the national broadband network being one striking example.

And it is this parochialism, particularly acute in the cybersecurity domain, that is arguably the most significant **commercial** challenge FireEye faces in attempting to expand beyond its North American market on the "march to profitability".

While Mandiant's business is profitable, DeWalt says the combined entity remains three to four years away from this milestone.

DeWalt believes that Mandiant's disclosures of **China**'s relentless hacking of private enterprise coupled with Snowden's even more detailed leaks of how the US National Security Agency penetrates the internet's every pore, has been a big boon for his business.

"While both super powers had different motives, this news has elevated and educated the world on the monitoring and espionage that has been occurring in the cyber domain like never before," he says.

"We are seeing almost every **company** in the world being breached, whether that be by **Chinese** military stealing intellectual **property**, NSA intrusions for surveillance, or Russian crime groups heisting debit and credit cards."

"From FireEye's vantage these important events have created a much more compelling reason for companies to see whether they are being compromised."

A concern foreign clients might have about retaining FireEye and Mandiant is that they could be legally co-opted into facilitating US intelligence gathering as Google, Facebook and Microsoft have in the past.

One of FireEye's original investors was In-Q-Tel, a venture capital fund that invests in technology companies "to support the missions of the CIA and [the] broader US intelligence community".

A FireEye**board** member was also previously a senior NSA official, while DeWalt himself is a member of President Barack Obama's National Security Telecommunications Advisory Committee.

Yet the first wrestling inductee into the University of Delaware's Athletics Hall of Fame counters that "we have never once received a subpoena or warrant from a US agency; never once. Nor would I ever foresee that I would be issued with a warrant."

DeWalt maintains this is because FireEye is a "defensive product" that has no client information retention capabilities. "What we study are behaviours in the network. We don't have any information on our clients that would be of interest to military intelligence agencies."

"Australian companies and the Australian government can use our technology to help protect them against any adversary, without fear of any information sharing or ties to US agencies," DeWalt affirms.

Three of the four major banks, the Australian Federal Police, and the Department of the Prime Minister and Cabinet, are already clients.On-premises radar system

"The beauty of our technology is it is a radar system that is on-premise, and does not have to distribute data to any back-end infrastructure."

FireEye's founder, Aziz, adds that its products are deployed in more than 40 military intelligence agencies around the world, including non-"Five-Eyes" nations. Perhaps the spies want to **buy** the system to work out how to defeat it.

So who is a greater threat for business: America's NSA or **China**'s 3 PLA? "My perspective here has been that they have very different motives," DeWalt says.

"What I see from 3 PLA and **China**'s Ministry of State Security has been espionage orientated for the purposes of enriching their economic system. I've tracked hundreds of companies that **Chinese** agencies have stolen directly from.

"What I notice from US intelligence activities is that it is much more about monitoring and surveillance, signals interception, and related to understanding national security threats from global actors."

The Mandiant deal, which was struck at 10 times revenue, triggered murmurings of a cybersecurity bubble. Yet DeWalt rationalises it on the basis each **company** offers very different services. FireEye provides a real-time, enterprise-wide detection system for advanced intrusions.

"We deploy virtual machines at various levels of the company's network architecture that study behaviour.

The slightest deviation in behaviour in the network allows us to create a threat score that determines whether we should block that user or that application from being able to continue to perform."

With an average 243-day window between a breach and a remedy in the US, fingering the bad guys quickly can materially reduce a company's financial and brand damage.

But FireEye's critics say that while it can find the bad guys, it offers no incident response capability, which is Mandiant's specialty. "FireEye is really good at detecting problems, but all we do is give you an alert," DeWalt concedes. "The next challenge is fixing it. Mandiant allows us to do both."

DeWalt says Mandiant, which made waves assisting The New York Times track down and repel Chinese hackers, has "breach responders – cyber Seals, if you will – deployed all over the world that help organisations solve complex attacks as they occur."

"The intelligence they gather is then automated into Mandiant's software products that companies can use to compress the breach-to-remedy gap faster."

DeWalt does not think FireEye has any interest in getting into "offensive defence", where companies seek to physically destroy, or "fry", hosts and servers used by intruders.

"There is a market for offensive security capabilities that is creating economic opportunities for some companies, but it is not something FireEye or myself want to partake in."No place for vigilantes

"We don't want to be the vigilante that strikes back. That is a job for law enforcement."

Asked about what new attack techniques are emerging, DeWalt says that "over 90 per cent of incidents now use command and control servers located inside ISPs and ASPs based in the victim's country to try to lower suspicion".

Another development is the rise in intrusions originating from within the target itself.

"The adversary actually hijacks the company's own website, so it looks like the attack is coming from NAB on NAB itself, which is a technique called "water holing". In these cases components of the company's website architecture are used as the command and control server to exfiltrate information.

"That is why blacklisting products can be completely ineffectual because the attackers can come from friendly websites and ISPs, and you cannot blacklist yourself."

DeWalt also says that in the last 12 to 24 months he has seen growth in malware interacting with command and control servers via "state-of-the-art cryptography that is not off the shelf". "This is very-difficult-to-track cryptography out of China, the US and Russia."

A final trend he cites is bad guys widening their scope to target "off-band" devices.

"So you download an app on to a personal mobile device that sideloads a key logger that steals your corporate login credentials. They will then log back in as you on your corporate network, download an exploit, establish a command-and-control server, and then start exfiltrating data."

"The combination of social networking coupled with new smartphones is lethal, because I know everything about you online, and you're an active downloader of mobile apps, which is creating a perfect platform of evil for high-value targets to be compromised."

CO	fireei : FireEye Inc. | rclicl : Mandiant Corporation
IN	isecpri : Security/Privacy Software | inetwt : Network Monitoring/Testing Tools | i3302 : Computers/Electronics | i330202 : Software | i3302021 : Applications Software | i3303 : Networking | icomp : Computing | itech : Technology
NS	ghack : Computer Crime | gspy : Espionage | ccat : Corporate/Industrial News | gcat : Political/General News | gcns : National Security | gcrim : Crime/Courts | gdef : Armed Forces | ncat : Content Types | nfact : Factiva Filters | nfcpex : FC&E Executive News Filter
RE	austr : Australia | usa : United States | apacz : Asia Pacific | ausnz : Australia/Oceania | namz : North America
PUB	Fairfax Media Management Pty Limited
AN	Document AFNR000020140127ea1s00001