14,400 emails Go to afr.com

The Financial Review is publishing thousands of the emails, a sample from an archive of 14,400 emails held by former Metropolitan Police commander Ray Adams who was European chief for Operational Security between 1996 to 2002.

broadcast for all to see

Former Metropolitan Police commander Ray Adams. European chief for Operational Security between 1996 and 2002.
Photo: PANORAMA

The key to pay TV

Subscription television is controlled through the set-top box. The key to the set-top box is the conditional access system, which uses a smart-card to decrypt the cable or satellite signal and manage the customer record base.

High-tech pirates, or hackers, try to break the encryption coding by reverse engineering the smart-cards, disassembling them microscopic layer by layer to reveal the hardware circuitry and crack the software coding. The hackers might be commercially driven or just in it for the thrill.

There is a multi-million dollar black market for pirated smart-cards that enable buyers to access pay TV for nothing apart from the $100 or so for the dodgy card – no monthly fees and unlimited access to all channels, including premium services.

The pirated smart-cards are sold over the internet, by word of mouth, in pubs, flea markets and car-boot sales.

Once a broadcaster's encryption system has been hacked, there's a race between the pirates and the broadcaster. The pirates produce and sell as many of the corrupted cards as possible before the broadcaster can fix the problem, either by replacing the cards or disabling the pirated cards with a software patch, an ECM. As soon as a new card or patch is issued, the game begins again. Nobody, especially the pirates, wants blank screens.

In the mid 1990s only a few companies provided conditional access services: News Corp subsidiary NDS; Nagra owned by Kudelski in Switzerland; Irdeto owned by Netherlands-based Mindport; Seca owned by Canal Plus in France.

Foxtel was the only Australian pay TV company to use the NDS cards; the others used Mindport's Irdeto.

piracy situation was for NDS.

Pay TV piracy is a murky world of hackers, hobbyists, dealers chasing millions of dollars from selling pirate cards and the growing incursion of organised crime.

Operational Security, headed by Hasak, Ray Adams in Europe, former US Army intelligence officer John Norris in the US, and Avigail Gutman in Asia, quickly gained a reputation for handling complex criminal investigations, using more than 20 informants and undercover agents and executing "stings" on pirate groups, often working with law enforcement agencies.

NDS in a statement yesterday said it was common for conditional access companies to obtain code for competitors' products — either through raids on pirates or for research and analysis.

However, the Adams emails show that Operational Security also had its own agenda, pursuing broader corporate goals for News, at times to the cost of News Corp's allies and customers including Foxtel in Australia and DirecTV in the US.

In Australia, only Foxtel used NDS for conditional access. Australis, Austar and Optus all used Mindport's Irdeto conditional access system. After Australis collapsed Foxtel took over its Galaxy satellite customers and relaunched them as a new arm, Foxtel Satellite, in April 1999. But that service also had to be broadcast using Irdeto services.

Irdeto enjoyed a market niche in Australia that would be worth tens of millions of dollars if NDS could take it over. But to break that stranglehold, NDS had to be able to show that Irdeto had been pirated and was no longer secure.

The frustration wasn't just in Australia. News had bought into an Italian pay TV operation called Stream SpA that also used Irdeto.

Something had to be done.

"Hello Gentlemen, we've now managed to write to an Australian Irdeto card using the s/w [software] I got from Joyce," Avigail Gutman wrote to her boss Hasak and to Ray Adams in London, on May 29 1999.

Joyce was a codename for an informant Gutman used, and she was concerned that nothing could link back to him in the software "so that we do not expose Joyce in the process of exposing Irdeto".

Adams proposed that one of his hackers rewrite the software into a new pirate program. Gutman said the new pirate cards by Adams' contact could "be to our benefit if these came out on the market first". She was proposing to sell the Operational Security pirate card before the real pirate card could be distributed.

On May 5, Andy Coulthurst, a British hacker working for Operational Security, emailed Gutman: "Hacking Irdeto is SO EASY! All you need is . . ." and he rattled off the details.

"Andy this is great stuff," Gutman emailed back from Taiwan. She had been working with David Johnson, the business development manager at the NDS Sydney office, who had been testing the pirate software for her. "I am trying to get more cards (Foxtel this time) — but despite all the stories about crooked installers who will sell you extra cards—I have yet to find them."

Johnson now proposed to get a Foxtel service installed in his building as he had no contacts with Foxtel Satellite apart from people who worked at Foxtel.

"WE WILL NOT USE THE ONES AT FOXTEL," Gutman wrote.

"Somehow we ask the install crew for a de-authorised card," Johnson replied.

The reason Gutman wanted the old cards without telling Telstra or Foxtel was to test out pirate software that she had downloaded from a UK piracy site called thoic.com (The House of Ill Compute).

Lee Gibling, who ran Thoic, had built it into the world's leading piracy site, where hackers could download software programs, swap codes, and ask other hackers for help. Many hackers even used a Thoic email address.

"We currently see some 4 gigabytes of daily requests on all the sites averaging somewhere in the region of 300,000 hits a day," Gibling wrote to Bob Cooper, the publisher of the influential monthly trade magazine SatFACTS.

Gibling hoped Cooper would advertise on Thoic. What he didn't mention was that Thoic was funded, supervised and controlled by Operational Security. Copies of all postings were forwarded to Operational Security in NDS offices in Israel.

So the pirate codes that Gutman planned to use on Foxtel cards came from a piracy site run by Operational Security. And now Op Sec wanted to earn advertising revenue from it.

Gibling had set up a special site on Thoic for Australian piracy, and elite Australian hackers had access to Area 51, a closed section run by a Sydney hacker called David Cottle under his online name Bond 007.

The *Financial Review* contacted Cottle under the company name listed in the Adams emails. He said he had become aware of Thoic after reading of it in SatFACTS, but he knew nothing of the piracy scene or Thoic other than rumours and reports.

"Wow what an integrate twisted tale of events!" Cottle said. "Funny about someone same surname as me that's a coincidence in a very creepy way."

German hacker Rolph Deubel, aka MadMax, was arrested in Thailand on information provided by Operational Security Asia-Pacific head Avigail Gutman.

The Mad Max sting

By the end of May 1999, the piracy market in Australia had exploded. At its height more than 50,000 people were using pirate cards, which cost around $200. They were original Foxtel or Austar cards that had been reprogrammed to allow viewing of all programs without paying any subscription.

In that month, Rolf Deubel, a German hacker known as MadMax and based in South Africa, visited Australia to set up pirate dealerships. It was Deubel's Millennium Group — composed mainly of German hackers in Europe — which had been posting the Irdeto pirate software on the Thoic website.

MadMax began a public correspondence with Bob Cooper at SatFACTS, describing in emails published on the internet his business plans for Australia, insisting that the reprogrammed cards he was selling were perfectly legal under Australian law.

What followed then was one of the strangest episodes in the history of Operational Security. Lee Gibling discovered from an email in MadMax's Thoic account that he was travelling to Bangkok in September 1999.

Avigail Gutman alerted Mindport, the company making the Irdeto system, and arranged for

Continued page 49

MAY 1997
Murdoch breaks off talks with Echostar CEO Charlie Ergen to merge their US satellite interests, after Ergen refuses to use NDS. Ergen sues for $5bn damages

LATE 1997
NDS decides to use 'Black Hat' team to reverse engineer Echostar smartcard 'to prepare material in anticipation of litigation or for trial'

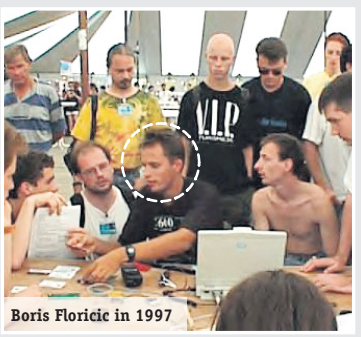
FEB 1998
BSkyB and NDS outraged when UK satellite TV rival OnDigital decide to launch using Canal Plus 'Seca' cards, not NDS

APR 1998
News Datacom settles Israel tax dispute for £3m. Later changes name to NDS

MAY 1998
Ray Adams unveils thoic.com: "This is my site." Thoic.com (The House of Ill-Compute) is a website-forum for pay TV hackers

Australis Media collapses, its satellite customers transferred to Foxtel using Irdeto cards

NDS Black Hat team uses Bristol University Focused Ion Beam to reverse engineer Echostar and Seca cards, after cracking Viaccess and Irdeto cards


Boris Floricic in 1997

OCT 1998
Black Hat team complete draft report on how to hack Echostar cards. Code from the card is posted four days earlier on pirate site DR7.com. DirecTV later abandons plan to drop NDS cards

German hacker Boris Floricic found hanging in a Berlin wood

NOV 1998
News in humiliating $1bn settlement with Echostar in return for stock


Pierre Lescure

MAR 1999
Rupert Murdoch breaks off talks to merge BSkyB with Canal Plus after CEO Pierre Lescure insists French control merged entity


Chris Tarnovsky

ROM codes for Canal Plus Seca card posted on DR7.com. NDS employee and hacker Chris Tarnovsky emails part of ROM code for Echostar card to Swiss independent hacker Jan Saggiori


Jan Saggiori

MAY 1999
South African hacker Rolf Deubel (MadMax) visits Australia to sell cards that can pirate Foxtel and Austar

News Corp buys 35% of Italian pay TV group Stream, which soon switches to NDS

SEP 1999
Deubel arrested in Bangkok after NDS read travel details in his Thoic email account

Continued next page