STRATEGIES FOR COMBATING SIGNAL PIRACY

Signal pirates have turned to the easy access of the internet and portable hard drives to help households gain access to pay-per-view channels for free. Despite these developments cable and satellite companies are far from throwing in the towel.

Graham Pollock reports

Swapping out legitimate smart cards for illegally decrypted access cards to steal satellite TV signals is now an outdated method of crime. Signal pirates have turned to the easy access of the internet and portable hard drives to help households gain access to pay-per-view channels for free.

Despite these developments cable and satellite companies are far from throwing in the towel. Instead they are rolling out new, high-tech crime fighting tools and investing in market intelligence and investigative programmes at unprecedented levels.

Like the initiation of Web 2.0, seen as a second generation of development and design for the internet, these new technologies and programmes are designed to build a stronger line of defence to maintain signal integrity and thwart the secondary and illegal market that makes signal pirates rich.

The goal is to thwart pirates from directing customers to websites where they can download decryption information into a thumb drive and then plug it into a set-top receiver in order to obtain thousands of free, premium channels, including sports packages, movies, pay-per-view events and adult subscription stations.

New technologies are constantly designed to stay ahead of the pirates. Unfortunately, many of those solutions are compromised within months of being launched. For example, pirates are now developing web-driven solutions that will automatically restart receivers that are blacked out by signal providers, without the consumer ever having to leave his easy chair.

And so it goes, an age old game of cat and mouse. As fast as new technology evolves, criminals find a way to beat it and steal signals, and revenue.

Decrypting the problem

It is not illegal to sell free-to-air receiver boxes, which can be used to access programmes like free public television or foreign-language stations. The receivers are often marketed to immigrant populations, interested in dialling into programmes from their home countries.

But the line of legitimacy is crossed when someone offers decoded cards or directs them to websites that will provide

the software necessary to decrypt the incoming signals. Often times system installers work in concert with decoders or hackers to drive legitimate customers to illegal signal piracy with the promise of more content for a one-time fee.

"It's not unusual for installers and decoders to co-mingle their illegal profits with money from one of their legitimate businesses which is a money laundering scheme that raises the level of the crime", says Vaughn Volpi, Vice Chairman of PICA Corporation, a 26-year old global brand protection consultancy.

Business is booming

The simplicity of downloading black market decryption information from the internet has emboldened pirates. It has become a multi-billion dollar industry and some estimate that illegal programming is beamed into more than one million homes in the US alone.

Piracy is truly a global plague, further evidenced by the free-wheeling signal theft that is occurring in Canada, despite courts having deemed it illegal for Canadians to watch American satellite TV. The loss in revenue is massive because the demand in Canada is huge and illegal decoding technology and decrypted access cards are readily available. "On average Canadians pay about 20% more for access to US television programming", says Paul Kocher, President and Chief Scientist for San Francisco-based Cryptography Research, Inc.

"It's a huge problem," Kocher says. "A couple of million Canadians get access through the black and grey markets because the programming is not legally available in Canada." "All that money drives cyber thieves to work even harder to beat the system", Kocher says.

Signal piracy is a significant crime worldwide. In the US dealers can be sentenced for up to five years in prison and up to $100,000 per violation for selling illegal decryption devices. The Digital Millennium Copyright Act in the US also allows authorities to seize the equipment they are using to perpetrate the crime. End users can face up to a year in prison, but most companies prefer to focus their attention on the distributors and hackers, says Leonardo Hernandez, Senior Vice President of Special Operations for PICA.

"Pursuing end users is a time consuming and expensive process with minimal end results", Hernandez says. "That's why PICA's Special Operations Unit focuses on identifying the significant organisations that are causing the most damage. Success in finding one of these operators often opens the door to many others."

Defeating the pirates

Signal pirates are a tight-knit community, and many know one another. It's a world that is largely invisible to many consumers, but their business expands exponentially through word-of-mouth from satisfied customers. Because many consumers view getting free TV signals as a victimless crime, these thieves' businesses continue to thrive. For them, the risk is low and the reward is great.

High-tech safeguards play a critical role in helping companies maintain control of their signals, but one tried and true, yet venerable security measure that remains constant, and successful, is a robust boots-on-the-ground investigation and intelligence programme.

"The only efficient way to consistently net the big fish is to invest resources in an aggressive global market intelligence campaign designed to identify and monitor the organised rings of hackers who are perpetrating these crimes", says Volpi.

Professional investigators work for the companies to gather information, determine the scope of the criminal organisations, calculate their losses, and then map out an enforcement strategy that often leads to civil or criminal charges.

Despite difficult times, many companies are not skimping when it comes to security, though many are not out in front of the problem, says Cryptography Research's Kocher.

"We've seen overall security spending going up," Kocher says. "But it's more reactive and less preventative spending. It seems like companies wait until problems become more acute before getting help."

Cryptography Research has been in the pay TV security business for a decade. The company has developed a new system it calls CryptoFirewall, a separate, hardware-based element that safeguards cryptographic keys and computations from attack. The technology is being used in more than 50 million devices and has not been compromised.

The combination of a good technology solution and vigilant monitoring of the illicit marketplace provides the one-two punch necessary to knock out signal piracy. Pirates often pursue the path of least resistance and will focus their efforts on easier prey if a company is aggressive in protecting their signal rights. ■

Graham Pollock is Senior Director of EMEA Operations at PICA Corporation

About PICA Corporation

PICA Corporation, established in 1982, is one of the largest companies in the world dedicated to brand protection, loss prevention, risk management and security consulting. PICA has 23 global offices and over 300 experience resident consultants in major metropolitan areas around the world.

For more information, please visit www.pica.net.