



In the last 3 months we have seen the first case of a consumer device shipping infected with a virus, another case of organised crime linked to malicious coders, and a marked increase in attacks coming from a nation that shows little regard for legislation surrounding digital intellectual property and copyright. This report provides a selection of industry news and extracts conclusions to help CSOs prepare for what lies ahead.

• Executive Intelligence Q2/05

Regulatory, Legal, and Governmental Developments

Legislation tabled in 2002/2003 and approved in 2004 is now yielding prosecutions in 2005. The Australian Communications Authority (ACA) has taken action against a spammer in the first case to be brought under Australia's Spam Act. Wayne Mansfield has been charged with sending 56 million commercial emails in twelve months after the Spam Act 2003 commenced in April 2004. Meanwhile in the USA Mr. Jeremy Jaynes, originally found guilty of similar offences in November last year had his 9-year sentence upheld after a recent appeal. Early indicators are that spammers are re-locating their servers to countries known to be soft on computer crime and lacking in appropriate legislation.

Significant Global Security Events

Chinese researchers have 'broken' the one-way hash function known as SHA-1 and have significantly weakened a similar function known as MD5. One-way hash functions are a cryptographic construct used in many applications. They are used in conjunction with public-key algorithms for both encryption and digital signatures. They act as a sort of checksum indicating that the message in question has not been altered. Typically MD5 and SHA-1 are used in authentication systems, VPNs, and file integrity checks. Hash functions are supposed to have two properties; One, they're one way. This means that it is easy to take a message and compute the hash value, but it's impossible to take a hash value and recreate the original message. Two, they're collision free. This means that it is impossible (impractical) to find two messages that hash to the same hash value. The Chinese researchers have shown that SHA-1 is not collision free, and that MD5 is significantly weaker than originally thought.

This dry mathematics has serious repercussions. The point of cryptographic hash functions is to give an extremely high level of assurance that the data being examined has not been tampered with. Although it is not yet time to abandon these two algorithms in favour of newer, stronger alternatives, it is prudent to plan migration away from them. As one Security Company CTO put it;

"It's time to walk, but not run, to the fire exits. You don't see smoke, but the fire alarms have gone off."

This quarter we saw what appears to be the first case of a consumer device shipping with a resident computer virus in it. The Creative Zen "Neeon" MP3 players in question were infected with W32.Wullik.B@mm, a mass-mailing Microsoft worm. We expect to see more of this kind of threat as embedded devices like MP3 players, movie players, consoles, and smart phones use variants of mainstream operating systems with a history of susceptibility to viruses and worms. No-doubt product liability laws will be carefully examined should a "Neeon" disrupt corporate networks.

Successful Operations

There have been several recent successful operations in the fight against computer crime. The most high profile of which has been the rapid identification and arrest of suspects associated with the Zotob worm. Atilla Ekici, aged 21 of Adana Turkey, and Farid Essebar, an 18-year-old resident of Morocco were arrested in connection with Zotob and with Mytob, another wide-spreading worm that first appeared in February. A further 16 arrests were made of suspects associated with the pair, and who are believed to be connected to a credit card theft and identity theft ring. This is another sign that organised crime is actively forming relations with virus writers.

Security and The Macro Environment

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, often for illicit or fraudulent purposes, such as obtaining access to their funds via online banking. These attempts are made via Email and a Web browser. In an attempt to combat phishing, banks are using more secure channels to communicate with customers. Increasingly they are deploying 'captive mail' systems where customers must log in to the web site in order to read messages. HSBC and Ebay have adopted this tactic. With both phishing and spam on the rise, captive mail systems are surely a growing trend.

360 Information Security and others have noticed a marked increase in attacks originating from China. Upon further investigation, the originating systems were found to have very poor security. Anecdotal evidence suggests some systems administrators in the Europe and the US are now blocking all Chinese IP space, making only specific exceptions for known partners and clients. Given the difficulty in pursuing attacks from China, increasing political tensions over trade, and the rapid rise in Internet use, we expect to see more organisations black-holing traffic from the P.R.C. Ironically the country with the worst record for having compromised 'zombie' PCs is the UK. A combination of rapid broadband take-up and reluctance by ISPs to tackle the problem has lead to a recorded 25% of all 'bot infected PCs' originating from the UK according to Symantec.

Executive Intelligence Q2/05