

Online criminals take on the trappings of business

By Alan Cane

Published: July 8 2009 16:34 | Last updated: July 8 2009 16:34

It was a fine evening. Michael "Mousewise" Moriarty was drinking in his favourite bar, foot on the rail, fedora pushed to the back of his head. He was smiling at the thought of an exquisite piece of malware he had created that afternoon.

The unwelcome arrival of a sharp if overcrowded suit, however, turned the grin to a grimace. At six feet three and 250 pounds, the suit was heavy mob singular personified.

"Hey Moriarty," he rasped, "the boss says to tell you that your undetectable information stealin' trojan ain't so undetectable after all. Your Service Level Agreement ain't worth nothin' to nobody.

"You come through with somethin' better or you'll be typin' with your toes."

Suddenly, Mousewise thought, the evening did not seem so fine after all.

Can you believe it? Service Level Agreements for software written specifically for criminal purposes? Welcome to cybercrime in the Web 2.0 world.

"It's an ecosystem," says Rik Ferguson, senior security advisor at [Trend Micro](#). "People have defined functions within that system."

He says he has been criticised for using terms such as malware-as-a-service – malware being malicious software. "But the business has become as mature as that. The latest viruses are extremely well written and coded, even incorporating up-to-the-minute bug fixes in the encryption technology."

Security experts are agreed that the nature of cybercrime has changed over the years. There have been three phases, says Greg Day, analyst with the security group, McAfee.

The first was the heyday of the amateur hacker – the writer, for example, of the Melissa virus: "These were stereotypical, sat-in-the-bedroom types doing it to prove they were very smart." In the second phase, criminally minded hackers used their skills to commit cybercrimes on their own account.

In the third and current phase, professional criminals have moved in en masse and malware writers are adopting a lower profile, selling their products over the internet, rather than exposing themselves to legal sanctions.

Mr Day gives the example of "Shark", a piece of software sold over the internet. It is simple to use, featuring a Windows interface with boxes to be ticked and icons to be clicked: "It lets you create your own equivalent of a botnet (a malicious software robot network). It will let you set up your own command and control server so that you can compromise other people's systems – control them, do all sorts of horrible things to them."

The vendors of these pieces of malware protect themselves by adding disclaimers along the lines of "for educational purposes only" and "not to be used in the real world".

What kind of software tools can be obtained by someone with the where-with-all to purchase them?

Some, like Shark, subvert other computer systems. Some are targeted at personal computers, while others attack innocent websites turning them into cyberweapons by proxy. Some developers provide e-commerce style software to run websites that can act as auction sites to sell personal details such as credit card numbers, bank accounts and passwords intercepted from infected computers.

The existence of these malware-creation kits has exacerbated an already perilous situation in cyberspace. According to the consultancy Gartner, more than 5m US consumers lost money to phishing attacks – fraudulent acquisition of passwords and/or financial details – last year, an increase of almost 40 per cent on the year before.

Orla Cox, security operations manager in the UK for the security group Symantec, says that the flood of malware is huge and growing: "We have reached that point where we believe there are more malicious files out there than clean files."

While "blacklisting" – denying access to known pieces of malware – and "whitelisting" – allowing access only to software known to be clean – are recognised defences against malicious code, Symantec has introduced the concept of "reputation-based" software which involves looking at where a program can be found among Symantec users, giving a value to the reputation of those users' systems, and estimating whether the software poses any security risks.

The impression remains, however, that in the race between the criminals and the security groups, the criminals may be edging ahead.

Wade Baker, executive director for research and intelligence at the communication group Verizon Business, has been collecting information on security issues for years: "In the past, I would have said that it might be difficult to stay ahead of the criminals but I think it could be done.

"But based on data we have collected over the past year, I've changed this opinion. I do not think we can anticipate and prevent everything criminals are going to fling at us.

"Nothing is going to stop a criminal who has managed to break into a system from installing malware there."

The arrival of Web 2.0, which encourages interaction between users and which blends services which had previously been separate, has not made the situation easier. Carlos Solari of Alcatel-Lucent says: "We are so dependent on the infrastructure, yet we still have not figured out how to manage the security."

In a recent book*, in which he urges a standards-based approach to security, he points to the weakness of security policies based on firewalls, detection and prevention systems – all essentially add-ons to existing infrastructure: "The 'aftermarket' delivery must change to one in which security is a design consideration at the point of creation and is applied consistently. The only parties who can change this relationship are the buyers. The current model is too deeply rooted to be able to change of its own accord."

"Applied consistently" is the key phrase. Mr Baker of Verizon Business says he has only rarely seen instances where a company lacked the resources, human and technical, and the policies to protect itself. But in day-to-day business, he notes, these policies were not implemented or trusted security measures had failed: "Attackers look for these weaknesses," he says. He urges the adoption of measures to ensure that security policies are fully implemented.

The fight back against the cybercriminals has two dimensions. The first involves the security specialists such as [Symantec](#) and [McAfee](#). These companies have the technology and know-how to tackle the cyberterrorists on their own ground, developing better tools to combat phishing and denial of service attacks and ways of recognising when a system has been compromised.

Just as, if not more, important, however, are the defensive measures adopted by individuals and organisations – and these need be neither complex nor overly expensive. Criminals operating scams based on sophisticated software frequently access their targets by low-level means – stolen passwords, computers left on and poor or faulty firewalls.

Who should take responsibility for security within an organisation? "Everybody," quips Mr Baker adding that successful security requires the active support of senior management.

Mike Gillespie from the consultancy Advent IM, however, says that putting security in the hands of a "techie" will result in a "techie" solution: "For an efficient information security solution, a specific security manager should be employed; someone who is objective and is responsible for addressing the security of the organisation as a whole.

"Senior management, although ultimately responsible for any breach that takes place, is not necessarily equipped to maintain the information management side of the business. Therefore there is a need to ensure that staff throughout the organisation are educated and trained to the best of their ability, ensuring that the correct approach is taken to handling data both securely and in keeping with legislation."

David Elton, a security expert with PA Consulting, says two pieces of long-standing wisdom retain their importance: "First, security is as strong as the weakest link and will never be failsafe. Second, invidious forces will never be more than one step behind the latest security measures."

He warns that individuals can inadvertently become victims: "There is a lot of good advice available to the private individual but even if you follow this, you are still vulnerable. What about those who hold information about you? Your employer, your bank, your mobile phone provider, your mortgage company, any organisation that you pay or receive money from on a regular basis, has your bank account and credit card details.

"We should all demand greater security standards from the organisations we trust with our information, but finding out how effective these organisations are at holding our information is difficult.

"Encouraging compliance with industry and international standards is one way of measuring effectiveness but standards do not help distinguish tick-box compliance from a mature and genuinely customer-focused approach to security."

* *Security in a Web 2.0 World*, Carlos Solari and contributors, Wiley, 2009

Copyright The Financial Times Limited 2009