Firewalls and firefights

A new breed of internet-security firms are encouraging companies to fight back against computer hackers

"If someone is shooting at you, the last thing you should focus on is the calibre of the bullet," says George Kurtz, the boss of CrowdStrike, a young tech company. Seated at a coffee table at Black Hat, a conference for the cyber-security industry held in Las Vegas recently, Mr Kurtz is expounding on the fundamental flaw he sees in the way many firms deal with cyber-intrusions. Most, he says, spend too much time trying to work out what hit them and far too little trying to understand the motivations of their attackers and how to counter future assaults.

CrowdStrike is a vocal advocate of "active defence" technologies that are generating much buzz in the cyber-security world. Their proponents argue that those who think firewalls, antivirus programmes and other security software are enough to keep their networks safe are kidding themselves. Instead, companies should work on the assumption that their systems have been breached, and take the fight to the hackers. The methods they prescribe include planting false information on their systems to mislead data thieves, and creating "honeypot" servers, decoys that gather information about intruders.

There are worries that such talk of active defence may encourage companies to go further, and "hack back" at their tormentors, even though many countries have laws that forbid such activity. In a survey of 181 delegates at last year's Black Hat event, just over a third said they had already engaged in some form of retaliation against hackers.

Concerns about cyber-vigilantism have not deterred financiers from investing in tech firms that see active defence as a money-spinning opportunity. Take the case of Endgame, a secretive outfit that is adapting technology developed for intelligence agencies for commercial use. In March it raised $23m in a second round of funding and added Kenneth Minihan, a former director of America's National Security Agency, to its board. Endgame has reportedly developed a system called "Bonesaw" that detects which software is being used by devices connected to the web. This could be used defensively by companies to detect vulnerabilities on their own devices, but could also be used to spot them on someone else's.

Gibberish and gobbledygook

Like many other information-technology businesses, the active-defence firms are deploying cloud computing (the delivery of software and data storage over the internet) and big-data crunching. CrowdStrike has developed a cloud-based service that scoops in intelligence about online threats from across the web and merges them with analysis from its own research team. It charges its customers from $25,000 to hundreds of thousands of dollars a year for its services. At the Black Hat conference researchers from Endgame demonstrated a system dubbed "BinaryPig", which crunches huge amounts of data swiftly to help identify and understand hackers by seeking patterns in the "malware" that they use to enter others' systems.

Other companies are concentrating on technology to foil software that hackers use to enter websites to indulge in wholesale "scraping", or extraction, of their content. CloudFlare, one such start-up, has developed a service called Maze, which it proudly describes as "a virtual labyrinth of gibberish and gobbledygook". The service detects content-scrapers and diverts them from the site's useful material into dummy web pages with useless content.

John Strand, an expert in active-defence techniques at SANS Institute, a computer-security training outfit, says the goal of all these technologies is to drive up the costs that hackers incur in the hope this will deter them in future. It is not to wreak havoc in enemy servers. "We deal in poison, not venom," he says.

But some security boffins argue that companies should be given more legal latitude to probe those servers. Stewart Baker, a former Department of Homeland Security official who now works for Steptoe & Johnson, a law firm, thinks firms should be allowed to "investigate back" in certain carefully prescribed situations. "There's a difference between being a vigilante and a private investigator," he insists. He also suggests that governments should consider licensing specialist firms to conduct investigations according to strict guidelines, rather than relying solely on their own cyber-detectives.

Other voices in the industry give warning that letting private companies hack into others' servers, even to protect their own property, could lead to trouble. "It's a foolish strategy to up the ante when you don't know who you are attacking," says Jeffrey Carr of Taia Global, a security consultancy. Mr Carr notes that hackers who are provoked might strike back even harder, triggering an escalation of hostilities.

Even some of the techniques employed by firms such as CrowdStrike could land firms in trouble. For instance, it might seem cunning for a company to try to trick hackers into losing money, by planting dummy accounts somewhere on their system that made the company's financial health seem much worse than it is. But if instead of just using the misinformation to make unwise trades, the hackers leaked the figures to the financial markets, the company could find itself in hot water with regulators.

In spite of such risks, which can be minimised through close co-ordination between companies' IT and legal teams, security experts are predicting that the popularity of active-defence techniques will grow. One reason is that businesses are making increasing use of cloud computing and mobile devices such as smartphones, which make it harder to establish clear defensive perimeters around their IT systems. "If you don't really know where your castle starts and ends, you can't really build an effective wall and moat around it," explains Nils Puhlmann, formerly chief security officer of Zynga, a social-gaming company, and a founder of the Cloud Security Alliance, an industry group.

He has a point. But it is not just the mentality of tech teams that will need to change. Today, many executives assume that what's inside the corporate firewall is pretty safe and what's outside it is not. But now that cyber-criminals are scaling even the highest of these walls with impunity, businesspeople must shed this binary view of security. Wherever data are held, they will need stronger, and smarter, protection from the hackers' digital bullets.

Fonte: The Economist, London, v. 408, n. 8848, p. 53-54, 10 a 16 Agu. 2013.