Technology Spectator, A corporate hack counter-attack (19 June 2012)

Frustrated by their inability to stop sophisticated hacking attacks or use the law to punish their assailants, an increasing number of US companies are taking retaliatory action.

Known in the cyber security industry as "active defence" or "strike-back" technology, the reprisals range from modest steps to distract and delay a hacker to more controversial measures. Security experts say they even know of some cases where companies have taken action that could violate laws in the United States or other countries, such as hiring contractors to hack the assailant's own systems.

In the past, companies that have been attacked have mostly focused on repairing the damage to their computer networks and shoring them up to prevent future breaches.

But as prevention is increasingly difficult in an era when malicious software is widely available on the Internet for anyone wanting to cause mischief, security experts say companies are growing more aggressive in going after cyber criminals.

"Not only do we put out the fire, but we also look for the arsonist," said Shawn Henry, the former head of cybercrime investigations at the FBI who in April joined new cyber security company CrowdStrike, which aims to provide clients with a menu of active responses.

Once a company detects a network breach, rather than expel the intruder immediately, it can waste the hacker's time and resources by appearing to grant access to tempting material that proves impossible to extract. Companies can also allow intruders to make off with bogus files or "beacons" that reveal information about the thieves' own machines, experts say.

Henry and CrowdStrike co-founder Dmitri Alperovich do not recommend that companies try to breach their opponent's computers, but they say the private sector does need to fight back more boldly against cyber espionage.

It is commonplace for law firms to have their emails read during negotiations for ventures in China, Alperovich told the Reuters Global Media and Technology Summit. That has given the other side tremendous leverage because they know the Western client company's strategy, including the most they would be willing to pay for a certain stake.

But if a company knows its lawyers will be hacked, it can plant false information and get the upper hand.

"Deception plays an enormous role," Alperovich said.

Fighting back

Other security experts say a more aggressive posture is unlikely to have a significant impact in the near term in the overall fight against cybercriminals and Internet espionage. Veteran government and private officials warn that much of the activity is too risky to make sense, citing the chances for escalation and collateral damage.

"There is no business case for it and no possible positive outcome," said John Pescatore, a National Security Agency and Secret Service veteran who leads research firm Gartner's Internet security practice.

Nevertheless, the movement shows the deep anger and sense of futility among security professionals, many of whom feel that a bad situation is getting worse, endangering not only their companies but the national economy.

"There's nothing you can do" to keep determined and well-financed hackers out, said Rodney Joffe, senior technologist at Internet infrastructure company Neustar Inc and an advisor to the White House on cyber security.

Joffe recently looked at 168 of the largest 500 US companies by revenue and found evidence in Neustar forensic logs that 162 of them owned machines that at some point had been transmitting data out to hackers.

Frustration by security professionals is not new. Some privately admitted to rooting for Lulz Security last year during that hacking group's unprecedented spree of public crimes, when it broke into and embarrassed Sony Corp, an FBI affiliate and others with routine hacking techniques. They said the resulting media coverage finally caught the attention of CEOs and legislators, although tougher cyber security laws have yet to pass Congress.

Although some strike-backs have occurred quietly in the past, Facebook popularized going on offense, said Jeff Moss, founder of the influential Black Hat security conferences and an advisor to the Department of Homeland Security.

In January, Facebook Inc named some of the Russian players behind the malicious "Koobface" software that spread through spam on various social networks, earning the gang an estimated $2 million.

Industry failures

The security industry's shortcomings were underscored most recently by the discovery of the Flame spying virus in the Middle East.

Mikko Hypponen, the well-regarded chief research officer at Finland's F-Secure Oyj, told the Reuters Summit his company had a sample of Flame in 2010 and classified it as clean and later missed another virus called Duqu that was suspected of being backed by Western governments.

"These are examples how we are failing" as an industry, Hypponen said. "Consumer-grade antivirus you buy from the store does not work too well trying to detect stuff created by the nation-states with nation-state budgets."

Because some national governments are suspected in attacks on private Western companies, it is natural that some of the victims want to join their own governments to fight back.

"It's time to have the debate about what the actions would be for the private sector," former NSA director Kenneth Minihan said at the RSA security conference held earlier this year in San Francisco.

In April, Department of Homeland Security Secretary Janet Napolitano told the San Jose Mercury News that officials had been contemplating authorizing even "proactive" private-entity attacks, although there has been little follow-up comment.

Many large security providers no longer preach that keeping the enemy out is paramount. Instead, they adopt the more recent line taken by the Pentagon, which is to assume that hackers have gotten inside and will again.

The mainstream advice now is to focus on trying to detect suspicious activity as quickly as possible in order to shut it down.

Hitting back with force is only the most colourful of possible responses after that. More common alternatives include deep analysis of what data has been sent out and attempts to learn whether the recipients were competitors, criminals who might try to resell it, or national governments, who might be inclined to share it with local industry.

Some experts also say executives should identify their most prized intellectual property and keep it off of networked computers and consider evasive action - such as having 100 versions of a critical digitized blueprint and only one that is genuine, with the right one never identified in emails.

"There is a reason that people fly halfway around the world to have a one-hour meeting," Joffe said of intelligence agencies.