



The future of malware: Trojan horses

10 / 13 / 06 |

MONTREAL--Some of the most dangerous cyberattacks are the least visible ones.

Widespread worms, viruses or Trojan horses spammed to millions of mailboxes are typically not a grave concern anymore, security experts said at the Virus Bulletin conference here Thursday. Instead, especially for organizations, targeted Trojan horses have become the nightmare scenario, they said.

"Targeted Trojan horses are still a tiny amount of the overall threat landscape, but it is what the top corporations worry about most," said Vincent Weafer, a senior director at Symantec Security Response. "This is what they stay up at night worried about."

The stealthy attacks install keystroke-logging or screen-scraping software, and they are used for industrial espionage and other financially motivated crimes, experts said.

Cybercrooks send messages to one or a few addresses at a targeted organization and attempt to trick their victim into opening the infected attachment--typically, a Microsoft Office file that exploits a yet-to-be-patched vulnerability to drop the malicious payload.

Security technology can stop common attacks, but targeted attacks fly under the radar. That's because traditional products, which scan e-mail at the network gateway or on the desktop, can't recognize the threat. Alarm bells will ring if a new attack targets thousands of people or more, but not if just a handful of e-mails laden with a new Trojan horse is sent.

"It is very much sweeping in under the radar," said Graham Cluley, a senior technology consultant at Sophos, a U.K.-based antivirus company. If it is a big attack, security companies would know something is up, because it hits their customers' systems and their own honeypots (traps set up to catch new and existing threats), he said.

Targeted attacks are, at most, a blip on the radar in the big scheme of security problems, researchers said. MessageLabs pulls about 3 million pieces of malicious software out of e-mail messages every day. Only seven of those can be classified as a targeted Trojan attack, said Alex Shipp, a senior antivirus technologist at the e-mail security company.

"It is very much sweeping in under the radar."

--Graham Cluley, senior technology consultant, Sophos

"A typical targeted attack will consist of between one and 10 similar e-mails directed at between one and three organizations," Shipp said. "By far the most common form of attack is to send just one e-mail to one organization."

In the past two years, MessageLabs has seen such attacks hit multinational companies, governments and military bodies. Other recurring targets include law firms, human rights organizations, news organizations and educational establishments, Shipp said.

Most attacks include Office files that use yet-to-be-patched vulnerabilities in the Microsoft application to install malicious code on vulnerable systems. The software giant has patched many such flaws on recent Patch Tuesdays.

Office files are also popular with attackers because organizations typically allow people to receive those files in e-mail, while executables or other files seen as more likely to be malicious are often blocked, Shipp said. "By and large, the best way of getting into an organization is to use something that the company lets in," he said.

The future of malware

The use of zero-day flaws circumvents traditional signature-based security products. These products rely on attack signatures (the "fingerprint" of the threat) to block the attack, which requires the attack to have been identified at least once before.

"This is the future of malware attacks," said Andreas Marx, an antivirus software specialist at the University of Magdeburg in Germany. "People affected by this won't be protected by antivirus software because there is no signature."

A signature is created when antivirus companies get a report from an infected company, when they see samples in their own honeypots, or get samples from other antivirus companies. "This doesn't happen with targeted attacks, as only an extremely small number of people get infected," Marx said.

As an example, Shipp said that only four antivirus products today detect one specific targeted attack that was first spotted months ago. Other products still let it through. MessageLabs is able to identify some of the threats by looking at the specific details of Office documents attached to e-mail and pinpointing unusual code in them, he said.

The identity of the attackers is mostly unknown. Security experts have theories of multiple gangs in different parts of the world, but haven't been able to pinpoint them.

The motivation of the attackers is also topic of dispute. From his analysis, Shipp believes the intent is to steal information. "In other words, corporate espionage," he said.

But Symantec's Weafer isn't so sure. "Whether they are for hire, or whether they are simply trying stuff out is not clear," he said.

Security companies are working on behavioral blocking and other techniques that go

beyond signature-based detection to protect systems. Heuristics, which are programs that use pattern recognition, instead of being based on algorithms, are one example.

"Antivirus companies have moved in leaps and bounds in terms of heuristic attacks," Cluley said. "It is not completely disastrous, even if it doesn't appear on the radar. Good proactive protection can still defend against a lot of this stuff," he said.

The real good news is that there is only a very low probability that any specific company was attacked last year, Shipp said. "The bad news is, if you were attacked and it was successful, it is of very high value," he said.

