Websites vulnerable to hidden hacker attacks, warns Aladdin

The latest eCrime threat to computer users comes from unauthorised access to websites, which is difficult to identify as hackers insert code into legitimate sites to extract confidential information and access details.

According to Aladdin's Attack Intelligence Research Centre, eCrime is growing exponentially. "This is the first report that digs into the logistics behind eCrime and the business model that drives these crimes," said Aladdin Knowledge Systems director of security research Ian Amit.

"The main threat to SMEs is direct financial fraud. These web threats are not detectable by antivirus as they come from legitimate sites. They are difficult to identify as the site looks the same as a non-compromised site. From a user perspective, you do not see anything.

"Once the attack succeeds it enables the criminals to install the trojan, which lurks until the user either does a financial transaction online or logs onto financial information. It is designed to steal data.

"Once a PC is compromised, the hackers can see what the PC is seeing – they are looking for credentials, log-ins and company internal documents marked confidential, for example."

The data is being translated into money through ID theft and by accessing the data resources of the company, and then trading the data in the criminal economy.

"Law enforcement has a problem as it is too locked down in terms of geography; if the hackers move geographic location, there is no real cooperation. Law enforcement is too bureaucratic to pose a real threat to these criminals."

Amit: compromise

Companies need to have layered security on their networks to minimise the threat, using best of breed firewalls, network security, updated antivirus and antispam software so there is no room left for hackers to go inside the network.

"The bottom line is to always keep systems updated and patched. It is always a compromise. The focus going forward is the ISPs, we want to get to commoditisation of the solution."

The extent of the threat could force antivirus companies to review their products, particularly in the light of Microsoft's plan to offer free anti-malware security, which will disrupt the market. "We really welcome this development from Microsoft as it will force the AV companies to review their products and provide a stage for a lot of security research," said Amit.

Online meetings grow as travel budgets slashed

The use of web conferencing is increasing as companies look to cut travel costs and improve productivity with flexible work practices.

The launch of unlimited usage plans such as GoToMeeting, the web conferencing service from Citrix Online, has given users a break on pricing.

"The flat rate pricing model and the ability to buy online and not engage in a long sales cycle have been very important," said Citrix Online vice president Bernardo de Albergaria. "We are seeing higher usage from our existing customers who are reducing travel usage and more internal adoption of web conferencing. The new generation of workers is almost demanding it they are so used to leveraging the web."

A Frost & Sullivan (F&S) report into web conferencing services noted that the per minute pricing model has largely given way to unlimited usage. F&S principal analyst Roopam Jain said: "There is an even greater need for this kind of technology due to the current economic slowdown."

Citrix Online: GoToMeeting