

Work laptops to trigger wave of online business fraud

Increasing rates of workplace laptop use mean that it's inevitable that cyber-criminals will turn their attention from attacking banks to profiting from [corporate fraud](#), a security expert has warned.

"The same kind of threats that are hitting the financial sector will start expanding to additional verticals," said Uri Rivner, head of new technologies, identity protection and verification for RSA, during a press briefing at the company's RSA Conference Europe gathering in London.

"Fraudsters have an easy way in because of infected endpoint machines."

The majority of current online fraud concentrates on accessing financial information such as credit card numbers and online banking logins, Rivner said. Sophisticated trojan software — often silently installed on unpatched PCs as part of a 'drive by download' when visiting a legitimate web site — routinely logs all information on a machine and transmits it via the Internet for processing to access useful details.

"Everything that is being transmitted to you online is being recorded and sent — and that's the most basic trojan," Rivner said.

The business of developing and marketing trojans has proved highly profitable. "Zeus today is the biggest-selling trojan kit around the Internet," Rivner said. "It sells for around \$1,000."

While attacking individual machines has been the main modus operandi for criminals to date, the increasing prevalence of laptops that are used in both home and work environments means that those trojans are now also recording significant amounts of information from corporate networks. "If you have a trojan that's on an enterprise computer, they can see whatever is going through," Rivner said.

Over time, criminals will likely start mining and exploiting that data, he predicted. "Already the fraudsters have a huge percentage of [corporate data](#) on their trojan motherships," Rivner said. "They're sitting on a pot of gold."

The blurring of work and personal equipment represents a major security headache for companies, though experts suggest that the trend is hard to counter.

While online crime against banks and other financial institutions remains a significant problem, the sector has done a good job of trying to combat it, Rivner said. "The threat is very high but the

financial sector has adopted a good defence strategy,” he said. “The trick is to put in multiple lines of defence, not to have a single point of technology.”

Conflict International Limited is a London detective agency specialising in ***Surveillance and Private and Corporate Investigations***, providing a bespoke private detective service for firms, banks, companies and private individuals

Categories: [1](#) · [PRIVATE DETECTIVE](#) · [PRIVATE INVESTIGATOR](#)