

## **New Methodologies in Cyber-crime and How to Protect Against Them**

**by Yuval Ben-Itzhak, Chief Technology Officer, Finjan**

A decade ago, cyber-crime used to be referred to as “computer-assisted crime”, owing to the fact that the not-so-humble computer was used to give criminals a significant leg-up in the perpetration of their criminal activities.

In the modern information age, however, cyber-crime means that crimes can now be perpetrated wholly or near-wholly in cyberspace or, to be more accurate, the web and its environs.

Finjan’s ongoing research and analysis of web security trends suggests that cyber-crime techniques are evolving at a very rapid rate, driven by a criminal fraternity that employs advanced programmers to develop new types of malware attack vectors.

Conventional signature-based detection of web activity - as well as traditional anti-virus, anti-spyware and anti-malware applications - have their place in the IT security arsenal, but hackers are now using encrypted data streams and code obfuscation techniques to hide their tracks.

Our security lab has found, for example, that 70 per cent of hacker data streams are now encrypted – not all to SSL standards, of course, but it’s clear that hackers are seeking to hide their tracks from casual and/or basic data stream analysis.

As regards to code obfuscation – which is defined as program code that is almost impossible to read or understand – our research suggests that criminals are using this approach to bypass traditional security systems that use pattern matching/signature-based methods.

Using encrypted data streams and code obfuscation creates the perfect environment for a cyber-crime to take place, since it allows almost any form of web-loading malware to be loaded without most existing IT security systems and software being aware of the problem.

The only way to stop dynamically obfuscated code (in which each user is exposed to a different variant of the code) and other advanced cyber attacks is to analyze and understand the code embedded within web content on-the-fly before it reaches the end users. Solutions using real-time code inspection techniques are capable of understanding what the code is actually going to do (e.g., steal a file) on the end user machine, and blocking it before it executes.

We have also observed that the criminal usage of data obtained by web-loading malware is changing. The old system of manual misappropriation of e-banking funds has given way to automated low value transactions carried out by servers which continually harvest malware-obtained data. Using this information, they fire off rapid salvos of minor e-banking transactions that can drain an attacked bank account in a few hours.

These automated e-banking transactions are usually small enough not to trigger a bank’s security systems for several hours. By the time the hapless customer and/or his/her bank discover the fraud, it’s usually too late to do anything about it.

To help protect against web-loading malware and its potentially disastrous cyber-crime consequences, Finjan’s patented behavior-based security technology, offered in its web security appliances, analyzes each and every piece of web content in real-time (regardless of its source), breaking down the code and understanding its potential effects without executing it. In this way, it identifies the true intent of the code and blocks only that content which needs to be blocked in accordance with your organization’s security policy. Leveraging this unique technology, Finjan

has developed a future-proof web surfing security assistance tool which it plans to offer to end users as a free download later this month.

Web protection is a central component of an organisation's overall security infrastructure. In order to combat sophisticated cyber criminals, security-conscious organisations would be well-advised to deploy real-time code inspection security technology as an additional layer, on top of their traditional security solutions, to minimize the dependency on signature updates.

### **Predictions on Cyber-crime Futures**

Looking ahead, Finjan expects that the web will remain the main vector for malicious code propagation as hackers continue to target the "weak spot" of traditional security solutions. Our analysis suggests that hackers will progressively use legitimate Web 2.0 sites and AJAX technology as means to perpetrate drive-by malware attacks (in which the innocent web surfer gets infected with Trojan or other form of malware by merely visiting a website).

Hackers are already aware of the weaknesses of security solutions based on URL categorization and signature or heuristics-based technologies. Accordingly, they will bypass these traditional security systems by injecting malware into web pages in reputable sites that would not be filtered by any URL filtering solution (as the site category is legitimate). Code obfuscation techniques will be applied in order to evade traditional malware detection techniques that are not capable of analysing the behaviour and intent of obfuscated code. Furthermore, dynamic code obfuscation (that generates a different code variant for each user) will be increasingly used to evade even the most robust signature based systems, as there is no way to maintain the infinite number of signatures required to identify dynamically obfuscated code.

### **About the Author**

Yuval Ben-Itzhak is a security industry veteran who brings strong technology leadership capabilities to Finjan, which he gained in over 15 years of high-level management positions. Prior to joining Finjan, Yuval was the founder and CTO of KaVaDo Inc., a leader in web application security (acquired by Protegrity). Prior to KaVaDo, Yuval was CTO at Ness Technologies, a global provider of end-to-end IT solutions and services. As a senior project manager at Intel Corp., Yuval was in charge of the design and development of multi-million dollar software projects.

Yuval has been selected as InfoWorld's "Top 25 Most Influential CTOs of 2004" and earned a BSc. in Information Systems and Engineering, cum laude from Ben-Gurion University, Israel.