finjan®
Vital Security™
securing your web

Cybercrime on the Net

“Behind the Scenes” of the new Web economy

By Mr. Iftach Ian Amit

February 2008

The Finjan technology and/or products and/or software described and/or referenced to in this material are protected by registered and/or pending patents including U.S. Patents No. 6092194, 6154844, 6167520, 6480962, 6209103, 6298446, 6353892, 6804780, 6922693, 6944822, 6993662, 6965968, 7058822, 7076469, 7155743, 7155744, 7185358 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Finjan, Finjan logo, Vital Security, Vulnerability Anti.dote and Window-of-Vulnerability are trademarks or registered trademarks of Finjan. Sophos is a registered trademark of Sophos plc. McAfee is a registered trademark of McAfee Inc. Kaspersky is a registered trademark of Kaspersky Lab. SurfControl and Websense are registered trademarks of Websense, Inc. Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation. All other trademarks are the trademarks of their respective owners.

For additional information, please visit www.finjan.com or contact one of our regional offices:

USA 2025 Gateway Place Suite 180 San Jose, CA 95110, USA Toll Free: 1 888 FINJAN 8 Tel: +1 408 452 9700 Fax: +1 408 452 9701 salesna@finjan.com	**Europe** Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com
Chrysler Building 405 Lexington Avenue, 35th Floor New York, NY 10174, USA Tel: +1 212 681 4410 Fax: +1 212 681 4411 salesna@finjan.com	Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com
Israel/APAC Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 salesint@finjan.com	Printerweg 56 3821 AD Amersfoort The Netherlands Tel: +31 33 4543555 Fax: +31 33 4543550 salesne@finjan.com

Email: info@finjan.com
Internet: www.finjan.com

Table of Contents

1. Background

Crimeware has been around for a long time. The reason why it deserves an in-depth look now is based on its rapid advancements in malicious Web technology in recent years.
The Web has become the no.1 attack vector for spreading and controlling Crimeware (which by itself has evolved from simple malware to criminally intent software – hence Crimeware).

2. Terminology

It is important to understand that the transition from malware to Crimeware happened in conjunction with the shift from crackers to criminals when looking at the recent history of malicious code on the Net.
Malicious code is still written by skilled hackers, but now they are employed by savvy criminal organizations that can offer them quick bucks for their latest and greatest.

These criminals are also the driving force behind the technological advancements made by hackers, as the needs are defined by the financial goals of their criminal organizations. Captcha breaking algorithms, zero-day vulnerabilities, malicious code hiding techniques, and other toolkits and frameworks show up on the market as an answer to the rapidly growing needs of these “clients”.

Cybercriminals use sophisticated Web-based attacks that are specifically designed to hit the “blind spots” of traditional security systems that rely on signatures or database (such as anti-virus, URL filtering and reputation-based security).

3. The Business of Cybercrime

The main goal of criminals commencing in cybercrime is obtaining business data.
Although personal data is still highly valuable (and can be fairly easily traded in “carder” forums), business data translate into lots of money in one hit.
Organizations have been the target of such online criminal activity for some time now, and targeted attacks that look for corporate data are seen “in the wild”.

For a business, the fallout of stolen corporate data varies from one industry to another.
The bottom line though remains the same for all of them – loss of data equals loss of money, reputation, and often also loss of customer and market trust.
Later on, additional costs incur, including costs for insurance, data recovery, IT measures that need to be put in place, forensics, as well as the actual losses from the usage of information and loss of employee productivity. These post-attack costs are a significant part of the total losses suffered by enterprises, but don’t get the kind of public attention that the initial breach got.

The “commercial” value of such data has its own marketplace and dynamics.
Credit card details are constantly traded with values that fluctuate between $5 and $30; adding a valid PIN to it almost multiplies the price tenfold (due to the immediate commercial value that is attached to such data). Financial reports are traded for around $ 5,000 each and a product design is priced at around $ 1,000.
Other information depends on the corporate market from where it was stolen, the competitors in the market, and the extent of the data.
Studies estimate that Cybercrime accounts for 8% loss of customers and 8% decline in revenue.

4. Technology

Now that we understand the main motives for cybercrime, let’s have a look at the main technological characteristics that modern Crimeware have spawned.
Since the main motive for having malicious code changed, the technological requirements followed. Instead of running amok and wrecking havoc, modern Crimeware needs to go undetected while having a fast propagation ratio (amongst their prime targets of course).
These requirements have been used as an “MRD” for the malicious software development.

The evasive nature that has become the trait of such Crimeware during the past year has manifested itself in many ways – most of it by selective delivery of the malicious content. Geographical discrimination, one hit per unique visitor, and randomly named resources that disappear after a single access are the main techniques used to keep the malicious code in hiding.

Another important trait is the code itself – which is obfuscated in more than 90% of the incidents that we have seen over the past 12 months.
Dynamic code obfuscation has found its way into the Crimeware toolkits that serve the malicious code. Criminals just have to check out the latest version of the exploits, which then will be delivered completely obfuscated in order to extend their lifespan by evading AV signatures.
Code obfuscation has turned to be the no.1 technique over 2007.
Our MCRC noticed that code obfuscation has risen from a bottom percentile at the end of 2006 to more than 90% by mid-2007.
The ease of generating such code enabled it to gain such a tremendous momentum in the malware writing industry. Coupled with the fact that signatures were unable to cope with this technique (to this day), its popularity skyrocketed.

In addition to the obfuscation signatures, we saw that the IFRAME technique of including malicious code in sites started to grow rapidly towards the end of last year.
The response from the industry was quick. But once again, the reaction was in the form of blocking the IFRAME element creation itself and not by looking at the code itself and stopping it. And again, we see how the malicious activity on the Net stays a few steps ahead of the traditional security technologies provided by many vendors, leaving the consumer with solutions that treat the symptom rather than the illness.

As discussed before, a prominent technique that distinguishes modern Crimeware from the rest of the crime crop is its evasive anti-forensics behavior.
In order to minimize the scrutiny that malicious code could receive from security researchers and AV companies, toolkits these days are actually minimizing their exposure to not-so-interesting visitors. These include second time visits from the same IP (usually crossed with the user agent of the browser to allow more than one PC from the same IP to "see" the malicious code), geographical segregation in order to focus on a more potent infection victims (weed out 3rd world countries, look for modern and therefore richer areas), and shy away from known security-firm-rich geographies (yes, security firms know how to run through anonymous IPs, but scanners, crawlers and such would usually be coming out of a specific block of IP addresses).

It's interesting to see how the security industry deals with the latest Crimeware techniques. As defense mechanisms, the traditional security technologies remain popular despite their limited capabilities.
Let's look at them more closely.

Network firewalls block TCP/IP protocol spoofing attacks, but cannot block a JavaScript code from accessing the local disk to get users' passwords, since those kind of attacks relate to webpages or Web content that spread over many packets and including code at different locations.

IDS/IPS can detect and partly block the spread of Crimeware in the network as long as the signature of such Crimeware is known and loaded to the IDS/IPS, but it cannot block a JavaScript code from accessing the local disk to get users' passwords, since these attacks relate to a webpage or Web content that is spread over many packets including codes at different locations. It also cannot block any attack over an encrypted protocol like SSL/HTTPS.

Gateway-based anti-virus detects known viruses since virus signatures for these attacks were created at the vendors labs. It cannot fully block JavaScript code from accessing the local disk to get user's session details stored in a cookie. These JavaScript codes can be written in different ways, and can also easily be changed. To block such code, the anti-virus requires a signature for each possible code structure, which is technically not feasible.

Client-based security products are installed on the operating system (e.g., Microsoft Windows) of the end user and are therefore as vulnerable as the operating system on which they are running. It is also more reactive in nature and a lot of times detects an infection after the attack has succeeded.

Gateway-based URL filters can detect and block websites as long as these websites are stored in the URL database, but cannot block websites with Crimeware advertisements or Crimeware code, such as iframes, from installing keyloggers for accessing confidential corporate information and taking control of the end user's computer. It is not designed to detect and block malicious code stored in legitimate caching servers, search engines or Web 2.0 sites and also cannot detect and block sites that it hasn't categorized yet.

Reputation services can block questionable websites, but can also block recently registered websites that are harmless. It cannot block websites with Crimeware advertisements or Crimeware code (such as iframes) from installing keyloggers for accessing confidential corporate information and taking control of the end user's computer, nor can it block malicious webpages on Web 2.0 websites that have a good reputation score.

Real-time content inspection analyzes each and every piece of content regardless of its source. It is therefore able to detect malicious codes without using signature updates or databases of classified URLs, thus preventing Crimeware and Web 2.0 attacks.
It succeeds where other technologies lag behind – providing an excellent defense against malicious inbound and outbound content.
The security industry has to start adopting this kind of technology that can analyze the intended criminal action of content and doesn't rely on signatures, URLs or reputation attributes to provide all-round protection against Crimeware, including malicious content hiding in HTTPs/SSL traffic.

5. Crimeware Toolkits & Distribution Channels

To achieve their goals, cybercriminals are looking for easy-to-use techniques with a low detection rate.
For this purpose, highly effective Crimeware toolkits have been developed. These toolkits are available in several forms for the last 2-3 years. Although the early toolkits were simply an aggregation of exploits that had been bundled for easy deployment, modern toolkits are built to support multiple users (attackers), deploy all the evasive and code obfuscation techniques, advanced reporting, and online updates for new vulnerabilities and attack techniques.

These modern toolkits are responsible for the creation and distribution of botnets such as the storm worm, and other massive infection vectors we have seen in the past year.
In order to really get to the profitable victims, the malicious code needs to be available from sites that these innocent victims browse to. Interestingly enough, the most "profitable" users normally do not browse at '.cn', '.ru', or sites with just an IP for identification. Attackers therefore are looking for a way in from the major popular sites that mom-and-pop would end up browsing to.

Hence enter Trojan affiliations. These affiliations offer website owners an incentive program – they are rewarded for putting a snippet of HTML code on their site (which is not visible in any way). They would be receiving money for each user that came across it (and had an "installation" completed on).

What happens behind the scenes is that the HTML code (usually a zero-size IFRAME element pointing to a Crimeware toolkit installation) would run malicious code on the browser of the unsuspecting visitor, and infect it (the aforementioned "installation" or "load" in cybercrime-speak). The end result of such a scheme is a massive infection incentive for attackers and script-kiddies to generate money. Obviously the upside to the affiliation owner (usually the criminal entity) is much higher and profitable as all these infections result in fully functional Crimeware-Trojans that bring in loads of precious data.

6. Future Directions and Practical Use

Since the motivation and incentive for criminals is to make quick (and substantial) profit from the Web as an attack vector, the only way to go ahead in the security industry is to think ahead.
Malicious technology will keep on evolving dramatically and will keep on trying to surpass defensive technologies as it has successfully done so in the last two years.
Until the security industry catches up and closes the gap, it will not go stagnant, but keep on evolving in order to widen the gap. The usage of Web2.0 technology has not been fully adopted yet by modern malware, and we can expect more sophisticated Trojans, control centers, and toolkits to pop up and challenge the security industry even more.

The Web itself is gaining more ground with smartphones browsing the Net as well as the installation of widgets and gadgets on desktops.
Mashups would be a proving ground for the Web security market in terms of how to handle code coming from different places and joining forces when combined into a functional entity. URLs and domains are insufficient as security parameters.
The security industry needs to realize that it must start developing innovative engines to answer the current and future threats instead of patching up against the old ones.

For security professionals, this current state of Web security provides new and exciting ways to look at corporate security from different and new angles. Extrusion testing is becoming a viable field of research and consulting, since the kind of corporate information that can be harvested from it is similar as it was in the old days of pen-testing.

7. About Finjan

Finjan is a global provider of secure web gateway solutions for the enterprise market. Our real-time, appliance-based web security solutions deliver the most effective shield against Web-borne threats, freeing enterprises to harness the Web for maximum commercial results. Finjan’s real-time web security solutions utilize its patented behavior-based technology to repel all types of threats arriving via the Web, such as Crimeware, phishing, trojans, obfuscated codes and other malicious codes, thus securing businesses against unknown and emerging threats, as well as known Crimeware. Finjan's security solutions have received industry awards and recognition from leading analyst houses and publications, including IDC, Butler Group, SC Magazine, eWEEK, CRN, ITPro, PCPro, ITWeek, Network Computing, and Information Security. With Finjan’s award-winning and widely used solutions, businesses can focus on implementing Web strategies to realize their full organizational and commercial potential. For more information about Finjan, please visit **www.finjan.com**.