



Anti-Phishing

How to Prevent Identity Theft and Safeguard Information Assets with Finjan's Active Real-Time Code Inspection

Finjan White Paper

April 2008

THIS DOCUMENT INCLUDES PROPRIETARY INFORMATION OF FINJAN SOFTWARE INC. AND/OR ITS AFFILIATES AND MAY NOT BE USED, CIRCULATED OR QUOTED EXCEPT IN ACCORDANCE WITH EXPLICIT WRITTEN AUTHORIZATION FROM FINJAN

© Copyright 1996 - 2008. Finjan Software Inc. and its affiliates and subsidiaries ("Finjan"). All rights reserved.

All text and figures included in this publication are the exclusive property of Finjan and are for your personal and non-commercial use. You may not modify copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, use or sell any part of its content in any way without the express permission in writing from Finjan. Information in this document is subject to change without notice and does not present a commitment or representation on the part of Finjan.

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. IBM Proventia Web Filter technology is a registered trademark of IBM Internet Security Systems. 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:

<p>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</p>	<p>Europe Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com</p>
<p>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</p>	<p>Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com</p>
<p>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</p>	<p>Printerweg 56 3821 AD Amersfoort The Netherlands Tel: +31 33 4543555 Fax: +31 33 4543550 salesne@finjan.com</p>

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

Table of Contents

1. Introduction	1
2. Phishing Techniques	2
3. Finjan’s Anti-Phishing Solution	4
4. Conclusion	5
5. About Finjan	5

1. Introduction

Today's cybercriminals are motivated by *financial gain*, and their main vector of attack has become the Web. One of the techniques they use is Phishing (pronounced "fishing"), which relates to Web attacks aimed at fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity.

Phishing presents a problem for corporations. If their employees are not protected, enterprises could be held liable for not putting protections in place to prevent fraud. An attack could also result in employee login information being compromised, allowing a phisher to get access to an employee's network account and thus accessing confidential information.

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social engineering techniques, such as spoofed emails and fraudulent websites, are used to trick recipients into revealing personal data such as credit card numbers, account usernames and passwords and social security numbers.

Phishing attacks lure their targets to a fraudulent site designed to look like one from a legitimate institution, in most cases a bank or e-commerce company.

Phishing is aimed at obtaining consumers' personal identity data and financial account credentials for criminal purposes.

The [Anti-Phishing Working Group](#) noted that in the December 2007 reports from the field, phishing attacks spoofed websites of national tax revenue agencies in the United States, Australia and the UK and, at the same time, previously untargeted segments, such as motorists associations.

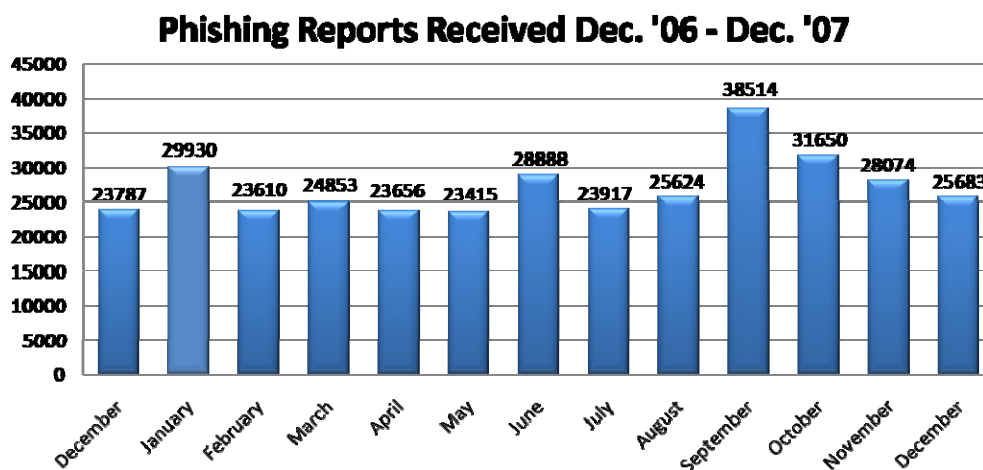


Figure 1 – Unique Phishing Reports Received, Dec 2006 – Dec 2007

2. Phishing Techniques

Cybercriminals lure consumers into accessing websites from companies or organizations where they have an account, such as banks, shopping sites or community sites. The legitimate websites are replaced with fraudulent ones that are almost indistinguishable from the real ones.

These malicious sites contain replaced fake web browser address bars, using JavaScript. Once the consumer logged in with his account name and number and password, these data were collected by the phisher for financial gain.

This method was used in the well-documented phishing attack against Citibank. When clicking on the link provided by the cybercriminal, the user arrived at a page, which appeared to be a secure HTTPS website. The phisher hid the real address of the site by exploiting an Internet Explorer-vulnerability related to non-printing characters.

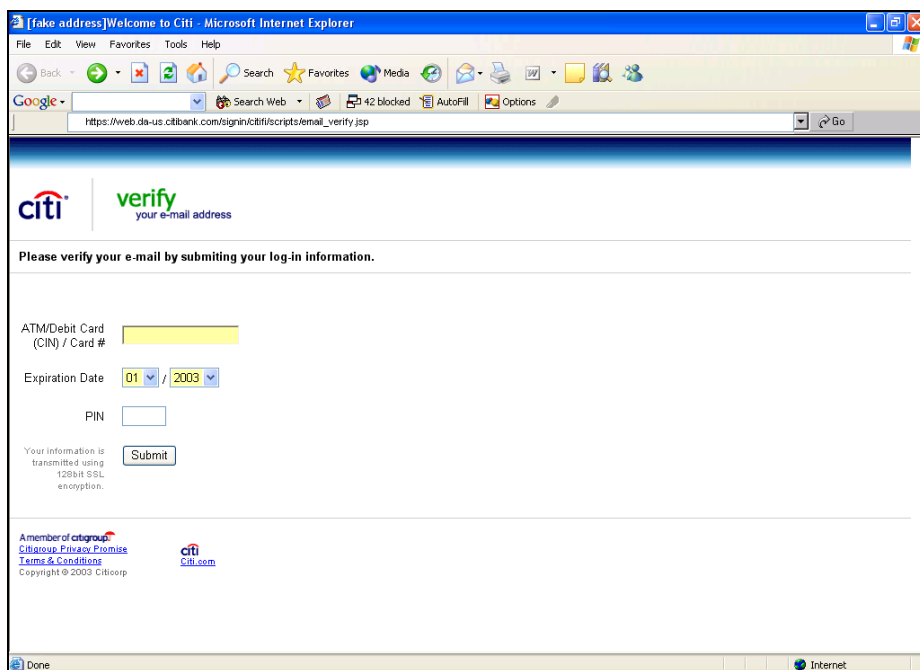


Figure 2 – Example of a malicious phishing website

Another popular phishing strategy is the deployment of Spyware. Cybercriminals use Spyware such as keyboard loggers (or keyloggers) to capture information entered at legitimate websites, such as Internet banking sites. This type of spyware can be planted on a user's computer using a Trojan infection. Any information the spyware captures is sent to a predetermined computer on the Internet.

A recent phishing scam directed the users' browsers to a site which downloads keyboard logging spyware before redirecting the user to the genuine Internet banking website. This spyware captured the login information entered, and sent this information to the cybercriminals via a remote computer on the Internet.

Finjan's active real-time code inspection analyzes the behavior of applications arriving from the Internet and determines whether they violate the security policy as defined by the network administrator.

During the summer of 2007, a new phishing technique emerged. Sophisticated Crimeware is now being deployed to steal bank account information for profit from financial institutions around the world without leaving any trace behind. This was covered in Finjan's [Malicious Page of the Month \(MPOM\) of July 2007](#)

This malware implements rootkit capabilities; monitors Web traffic; changes its behavior according to the websites accessed by users; as a proxy to intercept users' Web traffic and activate customized responses for financial gain.

Its modus operandi:

- Detecting user's interaction with a login page of a financial institution
- Collecting login credentials and sending them to both the institution's and the cybercriminal's servers over SSL
- Cybercriminal's server provides the Crimeware with a custom-designed page to deceive the institution and user
- Crimeware runs on the infected user's PC injects the customized bank page into the user's browser
- End users enter sensitive data into the customized page
- Crimeware sends data to the cybercriminal's server over SSL
- Crimeware mines the data for financial gain

3. Finjan's Anti-Phishing Solution

As shown above, attacks have become more evasive and obfuscated. This poses a challenge for traditional security, since anti-virus, reputation-based services and URL filtering solutions were not designed to handle these threats.

Active real-time content inspection protects the networks and vital information assets of organizations around-the-clock.

Finjan's Secure Web Gateway products utilize active real-time content inspection to understand the intended criminal behavior of web content. Each and every piece of incoming and outgoing web content in HTTP/HTTPS/FTP is analyzed in real time regardless of its originating URL and without signature matching. It therefore detects and blocks phishing attacks, thus protecting enterprises from any phishing that may result in severe business damage.

Finjan's Anti-Phishing Solution combines Finjan's active real-time content inspection technology with industry-leading URL filtering engines to provide superior protection against phishing attacks. Finjan's Anti-Phishing Solution identifies malicious active content associated in URLs, and blocks it at the gateway. It therefore provides excellent protection against sophisticated phishing attacks.

Features include:

- Scans for known hacking techniques, such as replacing the web browser address bar with a fake one, and proactively blocks such attempts.
- Leading URL Filtering engines categorize known phishing sites and blocks users from accessing them.
- Protects against phishing attacks that use invalid, revoked or otherwise problematic certificates by enforcing your organization's certificate policies at the gateway.
- Phishing attacks using **SSL-encrypted content** are also identified and blocked by Finjan's active real-time code inspection.
- If the fraudulent site also contains malicious Web content (such as Crimeware, Spyware, Trojans and other types of malware), such content is detected and blocked by Finjan's active real-time content inspection technology.

4. Conclusion

Financial gain is the driving force behind the explosive growth of Crimeware such as phishing, obfuscated code methods, and targeted attacks. Professional hackers use sophisticated Crimeware to evade signature- and database-reliant security tools. Website content is becoming more and more volatile and domain names can be set up for brief periods of time. As a result, “keeping track” of the malicious content has become extremely difficult. Attempts to pattern malicious code and create signatures, or to categorize known malicious sites, are not enough to sufficiently defend against the wave of dynamic Web threats. It is clear that an additional security layer is needed.

Evasive Crimeware attacks are hard to stop by products designed to prevent employees from visiting known non-productive sites (URL filtering), known malicious sites (reputation services) or downloading known malicious programs (anti-virus).

The answer is the use of real-time content inspection techniques.

More and more enterprises and organizations are looking at a multi-layered approach, consisting of real-time security and reactive (e.g., signature-based) IT security technologies.

Finjan’s **Vital Security™** with **active real-time code inspection** technology achieves the highest rate of malicious code prevention.

Finjan’s secure web gateway solution analyzes each and every piece of incoming and outgoing Web content in real-time, regardless of its original source, and understand its potential effects before it executes itself. By understanding the true intent of Web content, Finjan’s active real-time content inspection technology detects and prevents Crimeware despite the propagation techniques and anti-forensics methods in use. This prevents any malicious Web content from entering or exiting the corporate network, thus protecting enterprises from Crimeware that may result in severe business damage.

5. 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.