

Malformed Image

Specially crafted image files containing malicious code that exploits browser and OS vulnerabilities.

Banner Advertising

Banner ads served on legitimate websites are a growing source of malicious code.

Peer-to-Peer

Links to "dubious" websites containing malicious scripts that "silently" install spyware on the user PC.

Drive-by Spyware Installation

Malicious code uses unpatched browser vulnerability to "silently" install malicious code to log keystrokes and steal passwords.

Copyright Infringement

Downloading copyrighted material, such as software, art and music, expose companies to potential copyright infringement issues.

Ad Serving Sites

Ad serving sites install desktop utilities, Spyware and other unwanted software without user consent.

Spoofed File Types

Executable malicious code disguised as a text file to gain user trust.

MediaPedia | Torrentz.to | BushBorrent.com | BorrentZeactor.net | BitAip.com | PorrentTortal.com | FullDls.com

[The Daily] My Personalised Home Page!

Sponsored Links

- Car Rental - www.find-me-a-car.com
Only the best offers on car rentals, huge savings!
- Insurance - www.insure-me.com
Only the best offers on personal insurance, huge savings!
- Health - www.silver-shield.com
Only the best offers, personal health plans, huge savings!

New Face of the Day

- Meet Monique Linden
18 yrs. from France
She enjoys horseback riding and listening to rap music. She loves the color red, and finds politics boring...

Your Weather!

Get weather forecasts for your hometown and favorite places around the globe.

Enter your ZIP code:

Sports snap of the day

- The boys are at it, again!
Why on earth did they put these two on the same field? It was so obvious that the truce between Derek Williams and Bart Simian wouldn't hold water...

Pic of the Day

Like this image? Make it your desktop wallpaper!

Your Daily Horoscope

Teamwork between partners is excellent today. Enjoy an evening out with good friends. You can expect a stimulating exchange of ideas. You (star-) wisely avoid a pushy Leo-like "bully-ram" personality this morning.

Download Center

- "The Submerged"
Andy recommends this "groovy" new band.... Find out what the buzz is all about by downloading their entire new CD now!
- "ZipAway!"
A cool new application that puts you in charge!

Celebs Center

- Vienna & Nancy are living it simple
It's season 7, and the girls are living the outback life in the great Down Under! Find out more...

Today's Top Stories

- Iran Says Nuclear Enrichment Reaches Industrial Scale (Update4)
Bloomberg - [all 749 related >>](#)
- Three People Shot in Troy Office Building
Toronto Daily News - [all 333 related >>](#)
- Bush to Renew Effort on Immigration Plan
New York Times - [all 394 related >>](#)
- Canadians help dedicate monument at Vimy Ridge
National Post - [all 408 related >>](#)
- Optimism as East Timor Votes
BBC News - [all 651 related >>](#)

Invisible Threats

Sponsored Search

Sponsored search results are prominently displayed and carry a higher risk of leading to malicious sites.

Adult Material

Inappropriate and non work-related content may be in violation of corporate policy and expose organizations to legal liability.

Unwanted Software

Simple utilities, peer-to-peer and messaging applications are often bundled with unwanted software that is installed without user knowledge.

Exploratory Script

Invisible script identifies system settings, determines exact vulnerabilities, and delivers a payload that cannot be stopped.

Malware Using Obfuscated Code

Over 80% of malicious web content is obfuscated in order to bypass signature-based detection methods.

Appended JavaScript

Once the page has loaded, hidden code turns previously static text into executable script that runs malicious code.

Clipboard Referencing

Invisible scripts copy clipboard content (which may contain sensitive data) and send it to a server on the Internet.

Cybercrime and the Sophisticated Crimeware Used to Support It

Today's professional cyber-criminals are **motivated by financial gain**, and their **main vector of attack has become the web**. New sophisticated web-based attacks are being developed specifically to attack the "blind spots" of reactive security systems (e.g. anti-virus, URL filtering, heuristic-based security). Commercially-driven cyber-criminals understand that signature- and database-reliant solutions are not designed to counter obfuscated malicious code, Web 2.0 platforms and technologies, and other dynamic attack vectors in today's web scenario.

Crimeware attacks typically target internal user systems within the corporate perimeter, using invisible "web-borne" techniques to take control of internal 'endpoints' from the Internet. With the necessary tools readily available on the Internet, gaining remote access to an internal workstation is only a matter of determination. From there, it only takes a few days or hours to stealthily gain access to and take control of a company's critical internal business systems and data.

The Business Impact of Cybercrime

Cyber-criminals use a wide variety and combination of web-based techniques (shown on the flip side of this chart) to perpetrate, for example, the following illegal activities:

- 1) Gain access to the balance sheets of your company and manipulate stock behavior
- 2) Locate your payroll information
- 3) Get hold of your business' bank statements and transfer money from your business or make transfers between accounts
- 4) Gain access to your company's budgets and private financial statements
- 5) Steal your company's product roadmap and R&D workplan for industrial espionage
- 6) Capture your company's credit card numbers for purposes of fraud

It is clear that the damage to a business from these types of attacks could be devastating.



"The Internet and Internet applications will be the primary sources of malware infections in the enterprise in 2008 and beyond (0.8 probability)."

"Malware filtering in the Web gateway will increase from a penetration level of 10% to 15% of enterprises in 2006 to 70% of enterprises by 2011, driven by the emerging supply of more consolidated and scalable solutions and the increasing threat of Web applications (0.8 probability)."

Source: Gartner's 'Magic Quadrant for Secure Web Gateway, 2007' Report, June 2007

How to Keep Your Business Protected against Today's Cybercrime

As website content is becoming ever more dynamic, the surest way to detect modern malicious code is to be able to **understand what the code intends to do, before it does it**. Finjan's award-winning Vital Security™ Web Appliances utilize patented, real-time code inspection technology to prevent any malicious web content from entering the corporate network. Finjan's secure web gateway solution achieves the highest rate of malicious code detection with virtually zero false positives, by **analyzing each and every piece of web content in real-time**, regardless of its original source. Using real-time code analysis, Finjan's security engines break down the code, understand its potential effects, and block/allow the content before it executes on the end user machine. Finjan's patented real-time code inspection technology, enables enterprises to block malicious web attacks (e.g., crimeware, spyware, phishing, etc.) on-the-fly, without requiring signatures or patches.

To see what's really happening on the "dark side" of your browser and to learn more about today's threats, check out our **interactive demo** at:

<http://www.finjan.com/objects/multimedia/movie/finjan.html>,

or watch our **movie** at:

<http://www.finjan.com/objects/multimedia/jigsaw/jigsaw.htm>

Finjan real-time web security solutions have received industry awards and recognition



finjan
Vital Security™
securing your web
www.finjan.com