Top 10 Reasons Hackers Use the Web for Attacks

1 Desktop Vulnerabilities

Internet Explorer, Firefox, and the Windows operating system offer a widespread, target-rich environment for exploitable vulnerabilities, particularly since users don't always have patched systems. Some exploits depend on unpatched exploits to automatically download malware code without user consent – also known as a drive-by download.

2 Server Vulnerabilities

Internet Information Server (IIS) and Apache webservers offer another target-rich environment with unpatched systems for existing vulnerabilities and server administration configuration errors.

3 Webservers Virtual Hosting

The co-location of multiple, sometimes thousands of websites on the same server present effective targets for nefarious exploits.

4 Explicit/Open Proxies

Exploited computers can be setup as proxy servers to obscure traffic from URL Filtering controls, offer anonymity for websurfing, or act as a man-in-the-middle on data streams to legitimate websites.

5 HTML can embed objects from completely different servers in a webpage

Users may request a webpage from a particular site, only to automatically fetch objects from legitimate sites like Google analytics servers; advertising servers; malicious software download sites; or redirecting malware sites.

6 Typical Users aren't security-savvy

Most users don't understand the reasons for the three SSL browser checks; don't understand how to verify the legitimacy of downloaded programs; don't understand when their computer is behaving anomalously; don't use firewalls for their home networks; nor know how to discern phishing pages from legitimate pages.

7 Mobile Code use is widespread on Websites

While it sounds like a good idea to disable JavaScript, Java applets, .NET applications, Flash or ActiveX on your web browser, as these all automatically execute scripts or code on your computer, many websites can't be viewed unless some of these are enabled. This opens the door to poorly coded web applications that accept user input and use cookies, as in the case of cross-site scripting (XSS). In that case, the fact that some web applications need access to data (cookies) tied to other open pages is subverted. Any web application that accepts user input (blogs, wikis, comment sections) may inadvertently accept malicious code which can be returned to other users unless user-supplied input is checked for malicious code.

8 Widespread adoption of always-on highspeed broadband Internet access

While most corporate networks are protected by firewalls, home users without a Network Address Translation (NAT) firewall are exploited to harvest personal information; act as zombies in botnets for Distributed Denial of Service (DDOS) attacks; or have crude webservers installed to host malware code – all without the home user suspecting anything.

9 Universal access to HTTP and HTTPS

As use of the web is inherent in access to the Internet, all computers are given access through firewall to HTTP and HTTPS (TCP ports 80 and 443). We can always assume all computers have access out of their networks to the Web. Many programs adjust their communications to work through HTTP as a last resort to the Internet, such as IM and P2P applications. Also, these hijacked applications offer open channels to send botnets commands.

10 Adoption of embedded HTML in email

With the effectiveness of SMTP email gateways restricting delivery of questionable email, hackers don't always bother sending malicious payloads in email messages anymore. Instead, HTML in an email message is used to 'fetch' the malware payload from the web without the user knowing they just initiated a request to a questionable website.

Secure Web Gateway Requirements Stop Malware

You can thwart many web attacks with protections at the Web Gateway. Make sure your Secure Web Gateway provides the following:

- URL Filtering to stop malware downloads, phone-home transactions, and fat-fingering
- Malware Scanning for Virus, Spyware, Malicious Mobile Code (MMC), Unwanted Software, Trojans, Botnet, Worms, etc.
- Protection for HTTPS web traffic, not just HTTP and FTP
- Checks the payload for the true file type, instead of trusting the file extension or other file modifications done specifically to elude detection
- Enforcement of SSL browser checks
- Block access to URLs with IP addresses instead of hostnames
- Only allow executable and mobile code from trusted websites
- Allow selective access to a gray-list of executables by User (such as IT administrators)
- Regular, multi-day, automatic updates from a respected Anti-Malware provider
- Scaleable scanning optimized for webtraffic, since latency is very noticeable to users
  - Avoids rescanning repeated traffic in between virus updates for cacheable and non-cacheable objects
  - Large web, atypical downloads (> 200kb), don't impair regular web traffic scanning performance
  - Doesn't waste resources maintaining large numbers of active TCP connections (<150 active)
- Enforces Safe Searching for popular web search engines, to minimize redirection to malicious software servers
- Offers choice of scanning engines, to better complement your desktop scanning
- Doesn't trust the IP address supplied by users for webpage requests
- Can recognize infinite streams, such as Internet radio broadcasts, that never end and hence never be scanned

Blue Coat Systems, Inc. 1.866.30.BCOAT • 408.220.2200 Direct • 408.220.2250 Fax • www.bluecoat.com

Copyright © 2007 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor translated to any electronic medium without the written consent of Blue Coat Systems, Inc. Specifications are subject to change without notice. Information contained in this document is believed to be accurate and reliable, however, Blue Coat Systems, Inc. assumes no responsibility for its use, Blue Coat is a registered trademark of Blue Coat Systems, Inc. in the U.S. and worldwide. All other trademarks mentioned in this document are the property of their respective owners. v.SGT10HACK-0907