

The Web Hacking Incident Database 2010
Semiannual Report
January to June 2010



About the Web Hacking Incident Database

The Web Hacking Incident Database (WHID) is a project dedicated to maintaining a list of Web application-related security incidents. The purpose of the WHID is to serve as a tool for raising awareness of Web application security problems and provide information for statistical analysis of Web application security incidents. Unlike other resources covering Web site security, which focus on the technical aspect of the incident, the WHID focuses on the impact of the attack. To be included in the WHID an incident must be publicly reported, be associated with Web application security vulnerabilities and have an identified outcome. Trustwave's SpiderLabs (https://www.trustwave.com/spiderLabs-projects.php) is the WHID project sponsor. For further information about the WHID refer to https://projects.webappsec.org/Web-Hacking-Incident-Database.

Related Research Work

There are numerous community projects such as Bugtraq (http://www.securityfocus.com/bid), XSSed (<a href="http://www.securityfocus.com/bid), XSSed (<a href="http://www.securityfocus.com/bid) Statistics Project (<a href="http://www.securityfocus.com/bid) Statistics Project (<a href="http://www.securityfocus.com/bid), Associated (<a href="http://www.securityfocus.com/bid) Statistics Project (<a

Another project that collects information about real-world Web hacking incidents is Zone-H (http://www.zone-h.org/), which serves as the world's largest Web defacement mirror site. While Zone-H is more comprehensive and includes a large number of incidents, the majority of these are random hacks or crimes of opportunity rather than targeted attacks against a specific organization. By excluding random attacks, the WHID can provide a better tool for analyzing targeted non-random attacks on Web sites.

The unique value in tracking targeted Web incidents is that it allows measuring the actual effect of the incidents, transferring research from the technology domain to the business impact domain. In order to manage risk, one needs to understand the potential business impact as opposed to technical failure. This makes the WHID the right tool for making business decisions concerning Web site security.

Only the Tip of the Iceberg

Since the criteria for the WHID is restrictive by definition, the number of incidents that are included is not very large; only 158 incidents made it to the database for the first half of 2010. This is merely a sample of the overall Web application compromises that are actually occurring but are not publicly disclosed and/or reported on by media outlets. Therefore, the analysis in this document is based on relative percentage rather than on absolute numbers.

Report Summary Findings

An analysis of the Web hacking incidents from the first half of 2010 performed by Trustwave's SpiderLabs Security Research team shows the following trends and findings:

A steep rise in attacks against the financial vertical market is occurring in 2010, and is currently the
no. 3 targeted vertical at 12 percent. This is mainly a result of cybercriminals targeting small to
medium businesses' (SMBs) online banking accounts.





- Corresponding to cybercriminals targeting online bank accounts, the use of Banking Trojans (which
 results in stolen authentication credentials) made the largest jump for attack methods (Banking
 Trojans + Stolen Credentials).
- Application downtime, often due to denial of service attacks, is a rising outcome.
- Organizations have not implemented proper Web application logging mechanisms and thus are unable to conduct proper incident response to identify and correct vulnerabilities. This resulted in the no. 1 "unknown" attack category.

About this Report

While we have not seen a staggering increase in the number of reported attacks, we must also keep in mind that only the tip of the iceberg is reported. For each incident the WHID views attributes from many different angles:

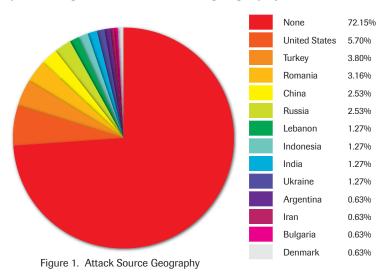
- Attack Method: The technical vulnerability exploited by the attacker to perform the hack.
- Application Weakness: The underlying vulnerability within the application that is exploited.
- · Outcome: The real-world result of the attack.
- Country: The country in which the attacked Web site (or owning organization) resides.
- Origin: The country from which the attack was launched.
- Vertical: The field of operation of the organization that was attacked.

In this report we discuss the following issues:

- · Drivers, business or other, behind Web hacking
- Vulnerabilities hackers exploit
- Attack methods used
- Types of organizations attacked most often

What are the Top Attack Sources?

The WHID attempts to track the origin of the attacks (attack source geography) however this data is seldom available in the news reports or disclosed by the victim sites. The data gathered in Figure 1 reports the percentages of attack source geography from the data available in the WHID.



If we focus in on the events which do list a confirmed attack source country, the fact that the United States is currently listed as no. 1 may be because the majority of news stories read by the WHID contributors are written in English. This fact may have skewed this measurement. The representation for Romania, Russia and Ukraine seems appropriate when considering the confirmed prevalence of professional cybercriminal organizations in these countries such as the Russian Business Network (RBN) (http://en.wikipedia.org/wiki/Russian_Business_Network). From the Advanced Persistent Threat





(APT) perspective, it is important to highlight the fact that China is no. 4. That China is not no. 1 in the WHID is mainly attributed to the fact that very complex attacks are originating from China, such as Aurora (http://www.wired.com/threatlevel/2010/01/operation-aurora/). APTs often use complex attack scenarios which target internal organization user's Web browsers versus directly targeting flaws within externally facing Web applications.

What are the Drivers for Web Hacking (Outcome)?

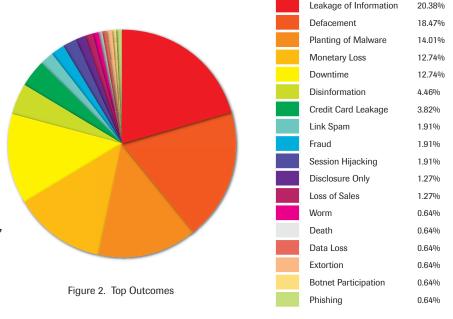
Why do people hack? What is their motivation and end goal? Figure 2 lists the various outcomes of the successful attacks listed in the WHID.

In the first half of 2010, leakage of information is the no. 1 outcome, while defacements of Web sites are no. 2 and planting of malware is no. 3. It is important, however, to note that monetary loss is on the rise and is a major goal for profit-driven cybercriminals.

Hacking for Profit

Professional criminals are developing new ways to generate revenue from compromising Web applications. The top outcome, leakage of information, is largely comprised of attackersextracting sensitive customer data from e-commerce Web sites. This data can then be sold on the underground black market for identify theft purposes and fraud.

The no. 4 ranked outcome, monetary loss, is largely the result of criminals figuring out different methods of fraudulently transferring funds out of victim's online bank accounts. They are leveraging client-side Banking Trojans (the most



popular one is called Zeus), which monitors victim's Web activity, and when they interact with online banking sites it will either steal their login credentials or alter transfer request data. The result is that criminals are able to siphon off chunks of funds to off-shore accounts.

Planting of malware is a related outcome. By adding malicious code to the attacked Web sites, the attackers convert hacked Web sites to a primary method of exploiting client's computers and installing the Banking Trojan software.

WHID Examples

WHID 2010-33: New York Firm Faces Bankruptcy from \$164,000 E-Banking Loss (http://krebsonsecurity.com/2010/02/n-y-firm-faces-bankruptcy-from-164000-e-banking-loss/)

WHID 2010-80: Hacked US Treasury Web Sites Serve Visitors Malware (http://www.theregister.co.uk/2010/05/03/treasury_Web sites_attack/)





Ideological Hacking

On the other end of the spectrum, ideologists use the Internet to convey their message using Web hacking. Their main goal is to disrupt the operation of Web sites with whom they have an opposing political or social view. Their top outcome goals are either knocking the site off line through denial of service (DoS) attacks or by defacing Web sites with their messages of opposition.

With the rise of botnets, attackers are able to flood Web sites with traffic and make them unresponsive to legitimate clients, resulting in the downtime outcome listed in the WHID. While most large organizations have been able to increase their network layer defenses to combat TCP/UDP, lower-network layer DoS attacks, they have not adequately improved their layer 7 defenses to defend against HTTP-level flooding attacks.

WHID Example

WHID 2010-155: S. Korean Government Web Sites Hit by Hacker Attacks (http://english.cri.cn/6966/2010/07/07/1461s581567.htm)

Web defacements are a serious problem and are a critical barometer for estimating exploitable vulnerabilities in Web sites. Defacement statistics are valuable as they are one of the few incidents that are publicly facing and thus cannot easily be swept under the rug.

Traditionally, defacements are labeled as a low severity issue as the focus is on the impact or outcome of these attacks (the defacement) rather than the fact that the Web applications are vulnerable to this level of exploitation. The resulting risk of Web defacement might be low because the impact may not be deemed a high enough severity for particular organizations. What should not be overlooked, however, is that the threat and vulnerability components of the equation still exist. What happens if the defacers decided to not simply alter some homepage content and instead do something more damaging? Web defacement attacks should not be underestimated.

When further analyzing defacement incidents, we found that the majority were of a political nature, targeting political parties, candidates and government departments, often with a very specific message related to a campaign. Others seem to have a cultural aspect.

In order to concentrate on the impact of incidents, the WHID does not include most Web site defacements, such as those covered by Zone-H (http://www.zone-h.org/), as they are random attacks with relatively low impact. We do, however, include defacement incidents that carry a greater significance. We consider an incident significant mainly based on who the victim was and, in some cases, how the attack was done. We also require the defacement to be reported publicly and not just by the hacker.

WHID Example

WHID 2010-68: Daily Telegraph Web Site Hacked

(http://www.guardian.co.uk/media/2010/apr/15/daily-telegraph-hacking)





What Attack Methods do Hackers Use?

Cross-site scripting (XSS) has dominated other vulnerability research projects. XSS is the most common vulnerability found by penetration testers according to the Web Application Security Consortium's Statistics Project (http://www.Webappsec.org/projects/statistics/) and is no. 2 in the Open Web Application Security Project (OWASP) Top 10 2010 release. While there is little debate that XSS vulnerabilities are rampant, the WHID focuses instead on monitoring actual security incidents and not vulnerabilities. Incidents are security breaches in which hackers actually exploited a vulnerable Web site, whereas vulnerabilities only report that a Web site could be exploited. Actual security breaches are more significant as they indicate both that a vulnerable Web site is exploitable and that hackers have an interest, financial or other, in exploiting it.

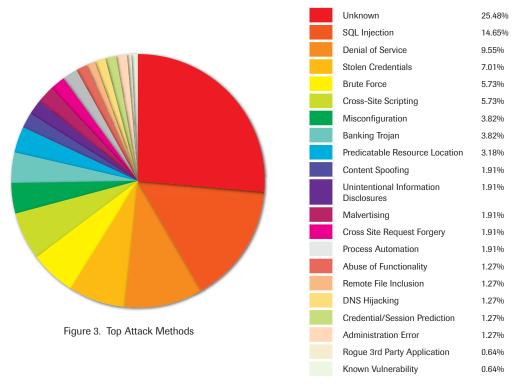


Figure 3 highlights an important finding: the top attack category is unknown; 25 percent of the incidents reported were reported without specifying the attack method. This lack of attack vector confirmation may be attributed to a combination of two factors:

1. Lack of Visibility of Web
Traffic: Organizations have not
properly instrumented their
Web application
infrastructure in a way to
provide adequate monitoring
and logging mechanisms. If
proper monitoring mechanisms
are not in place, often attacks

and successful compromises go unnoticed for extended periods of time. The longer the intrusion lasts, the more severe the aftermath. Visibility into HTTP traffic is one of the major reasons why organizations often deploy a Web application firewall.

2. Resistant to Public Disclosure: Most organizations are reluctant to publicly disclose the details of the compromise for fear of public perception and possible impact to customer confidence or competitive advantage.

In many cases we feel that this lack of disclosure, apart from skewing statistics, prevents the fixing of the root cause of the problem. This is most noticeable in malware-planting incidents in which the focus of the remediation process is removing the malware from the site, rather than fixing the vulnerabilities that enabled attackers to gain access in the first place.





The other attack vectors that topped the list are as follows:

- SQL injection is still the top known attack category and this re-enforces the vulnerability statistic reports from both WASC and OWASP.
- Banking Trojans monitor victim's Web activity and when they interact with online banking sites will
 either steal login credentials or alter transfer request data. The result is that attackers are able to steal
 funds and funnel them to off-shore accounts.
- Application DoS attacks are still causing big problems with Web sites. These attacks often result in downtime for applications. Application DoS attacks are such a problem mainly because there are many methods for rendering a Web application inaccessible rather than simply flooding the sites network connection with requests. Web applications are relatively fragile and attackers are able to send precise requests which target Web application resources that require large processing power and thus may more easily consume the site's available resources.

WHID Example

WHID 2010-67: Apache.org Hit by Targeted XSS Attack, Passwords Compromised (http://www.zdnet.com/blog/security/ apacheorg-hit-by-targeted-xss-attack-passwords-compromised/6123)

Which Types of Application Weaknesses are Exploited Most Often?

A new addition to the WHID in 2010 is the inclusion of tracking the underlying application weaknesses which are exploited by the various attack methods. This addition sheds light upon the missing, misconfigured or broken application program coding practices that allow these attacks to be successful. This is an important metric to track as it can be used by developers to identify the root causes of application vulnerabilities and the various methods in which they may be abused. The weaknesses specified are taken from the WASC Threat Classification (http://projects.Webappsec.org/Threat-Classification).

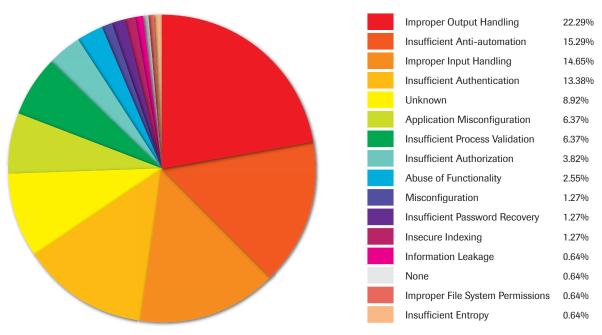


Figure 4. Top Application Weaknesses



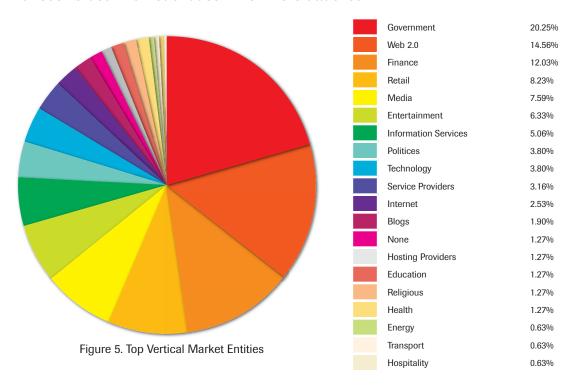
Figure 4 lists the top application weaknesses identified in the first half of 2010. These weaknesses map directly to the various attack methods listed previously. Here are some examples of this mapping:

- Attack -> Application Weakness
- XSS -> Improper Output Handling
- DoS/Brute Force -> Insufficient Anti-automation
- SQL Injection -> Improper Input Handling

It is important to note that there exists a many-to-one ratio with regards to attacks and weaknesses. There are many different types of attacks which may leverage the same underlying application weakness. This means that, from a defensive perspective, it is possible to reap a very high mitigation return on investment (ROI) when organizations are able to address the root causes of vulnerabilities.

Which Types of Organizations are Attacked Most Often?

Another aspect we looked into is the type of organizations attackers choose as targets. Figure 5 shows the various vertical market entities which were attacked.



Government-related organizations rose from no. 4 in 2009 to no. 1 mainly due to an increase in international "hacktivism," which may include Web site defacements, DoS attacks and other nonviolent attacks. Web 2.0 sites. such as Twitter and Facebook, are high on the list as cybercriminals are exploiting the user-driven, dynamic content on these sites. There have been a number of the WHID incidents that

show that attackers are unleashing XSS/CSRF worms on the sites which spread virally across the wide user-base. Financial institutions attacks, which rose to no. 3 on the list, were mainly attributed to attacks that leveraged Banking Trojans such as Zeus.

On the commercial side, retail holds the no. 4 position. The trending data seems to support the idea that retail will always be listed high with the WHID due to the fact that they are subject to both Payment Card Industry Data Security Standard (PCI DSS) and state regulatory requirements to publicly disclose when a data breach has occurred.





WHID Example

WHID 2010-109: Viral Clickjacking 'Like' Worm Hits Facebook Users (http://www.sophos.com/blogs/gc/g/2010/05/31/viral-clickjacking-like-worm-hits-facebook-users/)

Summary

With regard to real-world hacking, we are seeing an increased focus by professional criminals to launch combination attacks with the ultimate goal of making money. They are leveraging many different methods to find ways to steal end-customer data and transfer funds from banking accounts. It is highly recommended that organizations utilize the WHID data presented within this report to better prioritize their internal Web application security remediation tasks.

About Trustwave's SpiderLabs

SpiderLabs is the advanced security team within Trustwave focused on incident response, ethical hacking and application security testing for our premier clients. The team has performed hundreds of forensic investigations, thousands of ethical hacking exercises and hundreds of application security tests globally. In addition, the SpiderLabs Research team provides intelligence through bleeding-edge research and proof of concept tool development to enhance Trustwave's products and services.

For more information, visit https://www.trustwave.com/spiderLabs.php.

Incident Response Contacts	
Americas	Colin Sheppard 312.873.7474 csheppard@trustwave.com
EMEA	Stephen Venter +44 207 070 5982 sventer@trustwave.com
APAC	Marc Bown +61 2 9089 8870 mbown@trustwave.com

About Trustwave®

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses throughout the world. Trustwave analyzes, protects and validates an organization's data management infrastructure—from the network to the application layer—to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include ondemand compliance management, managed security services, digital certificates and 24x7 multilingual support. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

Corporate Headquarters 70 West Madison St. Suite 1050 Chicago, IL 60602

-D 040 070 7500

P: 312.873.7500 F: 312.443.8028 EMEA Headquarters
Westminster Tower
8th floor
3 Albert Embankment
LondonSE1 7SP

P: +44 (0) 845 456 9611 F: +44 (0) 845 456 9612 LAC Headquarters Edificio E-Tower Rua Funchal, 418—35 Andar Vila Olímpia—São Paulo—SP

CEP 04551—BRASIL P: +55 (11) 3521-7314

F: +55 (11) 3521-7070

APAC Headquarters Level 26 44 Market Street Sydney NSW 2000, Australia

P: +61 2 9089 8870 F: +61 2 9089 8989



Copyright © 2010 Trustwave Holdings, Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave. While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions.

Trustwave and Trustwave's SpiderLabs names and logos are trademarks of Trustwave. Such trademarks shall not be used, copied or disseminated in any manner without the prior written permission of Trustwave.