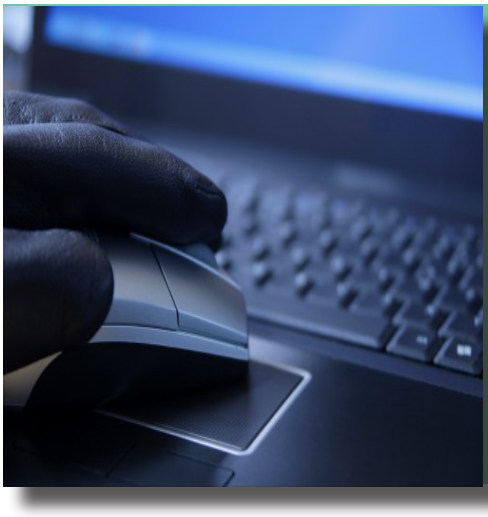
BREACH



THE WEB HACKING INCIDENTS DATABASE 2008

ANNUAL REPORT

FEBRUARY 2009

Breach Security, Inc. | Corporate Headquarters | 2141 Palomar Airport Road, #200 | Carlsbad, CA 92011 | USA
tel: (760) 268-1924 | toll-free: (866) 205-7032 | fax: (760) 454-1746 |www.breach.com

BREACH

ABOUT THE WEB HACKING INCIDENTS DATABASE 2008

The Web Hacking Incident Database (WHID) is a project dedicated to maintaining a list of web application-related security incidents. The WHID's purpose 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 an 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.

For further information about the Web Hacking Incidents Database visit http://www.xiom.com/whid-about.

RELATED RESEARCH WORK

Many projects such as Bugtraq, XSSed and the Web Applications Security Consortium's Statistics Project track vulnerabilities in software or web sites. However, vulnerabilities present only one dimension of the problem as they tend to be described in technical terms. Real-world incidents, on the other hand, provide additional information that enables research into actual trends in the hacking world, such as the types of organizations attacked, the motivation behind the attacks and the sources of the attacks.

Another project that collects information about real-world web hacking incidents is zone-h. While zone-h is more comprehensive and includes a large number of incidents, the majority of these are random hacks, something which shadows other types of attack. By excluding random attacks, WHID provides a better tool for analyzing targeted non-random attacks on web sites.

The unique value in tracking targeted web incidents is that it allows measurments of 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 WHID the right tool for making business decisions concerning web site security.

ONLY THE TIP OF THE ICEBERG

Since the criteria for inclusion of incidents in the WHID are restricting by definition, the number of incidents that are included is not very large - only 57 incidents made it to the database this year (compared to 49 in 2007). Therefore, the analysis in this document is based on relative percentage rather than on absolute numbers.

ABOUT THIS REPORT

The WHID has 294 entries of events occurring from 1999 to 2008. However, the inclusion criteria was changed in 2006 and additional attributes, such as incident outcome and type of organization attacked were added in 2007. To date, only incidents for 2007 and 2008 have been adjusted to the new criteria, so until the historical data is adjusted, year-over-year analysis is not possible. The current report, therefore, focuses on 2007 and 2008.

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.

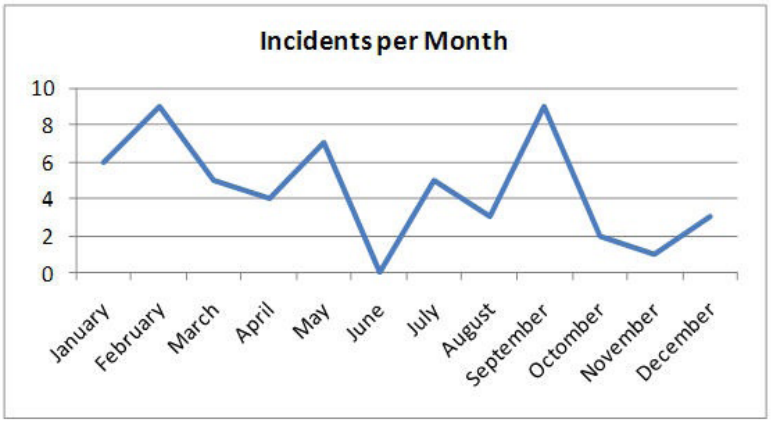
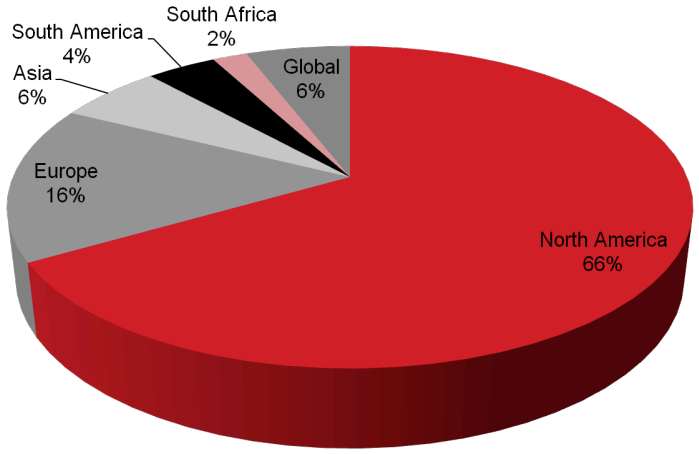


FIGURE 1 - 2008 INCIDENTS PER MONTH

For each incident in 2008, the WHID views attributes from many different angles:

- Attack Method – the technical vulnerability exploited by the attacker to perform the hack.
- 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.

The analysis in this paper is based on all of the above attributes, apart from origin and country. Information regarding the origin of attacks was too scarce for meaningful analysis. Contributors to the WHID tend to come more from English-speaking countries, presumably, because of the English-language interface of the WHID. This gives a leaning towards incidents in these countries rathethan a world status.



- The drivers, business or other, behind Web hacking.
- The vulnerabilities hackers exploit.
- The types of organizations attacked most often.

WHAT ARE THE DRIVERS FOR WEB HACKING?

The first question we confronted was **why do people hack**? In 2007, the motivations for hacking were evenly divided between for-profit and ideological attacks. In 2008, however, criminals unleashed an ingenious new web application attack the likes of which had never been seen.

THE IMPACT OF MASS SQL INJECTION BOTS

This year 2008 marked a major event for the web application security landscape. In early January, attackers unleashed a new type of SQL Injection attack that successfully compromised more than 500,000 websites. Due to the large number of sites successfully compromised, and the lack of one-to-one news stories of each compromise, the data that is represented within the WHID Outcome and Attack statistics do not accurately reflect the total impact of these attacks. There are a few high-profile WHID entries specific to, these attacks however, the data is significantly skewed and hide their true impact. **SQL Injection attacks that planted malware on target web sites were the #1 attack/outcome vectors for criminals in 2008**.

The mass SQL Injection bot payload was a script that would alter the contents of the back-end database and inject malicious JavaScript. The novel approach employed by these attacks was that the SQL Injection scripts could "generically" enumerate and update the database tables all in one request. Normally, attackers had to conduct manual reconnaissance in order to first enumerate the database details before they could inject the final payload. These steps were necessary because all custom coded web applications were different so there was no standard method to take the SQL Injection code and make wormable code. That is until the mass SQL Injection bots emerged. Breach Security Labs released three alerts related to these bots in 2008:

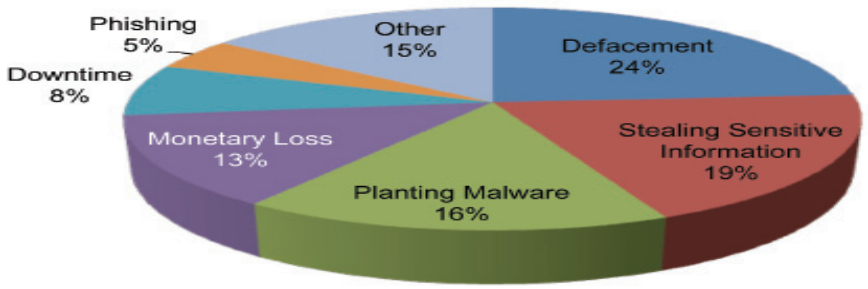
- Nihaorr1 Mass SQL Injection Bot
- Asprox Mass SQL Injection Bot
- Mass SQL Injection Bot Evolution

While the initial attack vector was SQL Injection, the overall attack more closely resembles a Cross-Site Scripting methodology as the end goal of the attack was to have malicious JavaScript execute within victim's' browsers. The JavaScript calls up remote malicious code that attempts to exploit various known browser flaws to install Trojans and Keyloggers in order to steal login credentials to other web applications.

Another notable attack methodology shift was that instead of targeting sensitive information within a web site's database, the attackers instead were focusing on the web site's large customer base. The web site essentially becomes a malware launching point when legitimate users visit the site.

HACKING FOR PROFIT

On the capitalistic side, 19% are aimed at stealing personal information. Such 'personal records' are easily traded on the internet and therefore are the easiest virtual commodity to exchange for money.



Attack Goal	%
Defacement	**24%**
Stealing Sensitive Information	**19%**
Planting Malware	**16%**
Monetary Loss	**13%**
Downtime	**8%**
Phishing	**5%**
Deceit	**2%**
Worm	**1%**
Link Spam	**1%**
Information Walfare	**1%**

Two other ways in which crooks exploit web sites to gain money are the planting of malware and phishing. The first demonstrates the role of web application hacks in the ever growing client security problem: by adding malicious code to the attacked web sites, the attackers convert hacked web sites to a primary method of distributing viruses, Trojans and root kits. They are replacing e-mails as the preferred delivery method.

IDEOLOGICAL HACKING

On the other end of the spectrum, the ideologists use the Internet to convey their message using Web hacking. Their main vehicle is defacing web sites. 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. It is important to remember the standard Risk equation:

RISK = THREAT x VULNERABILITY x IMPACT

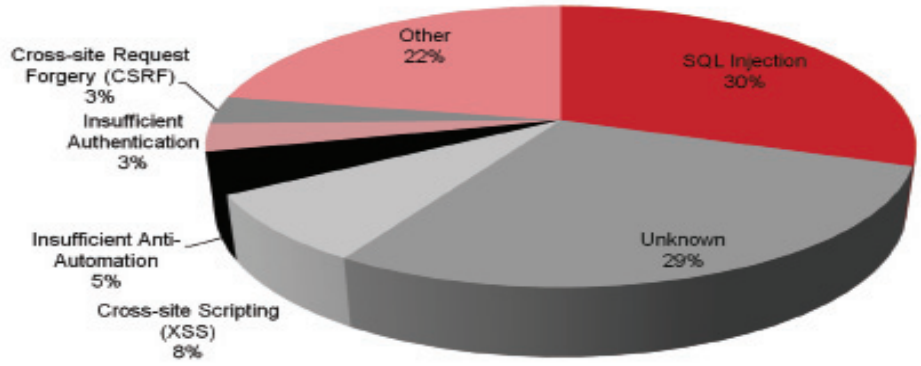
The resulting risk of a web defacement might be low because the impact may not be deemed of high enough severity for particular organizations. What should not be overlooked, however, is that the threat and vulnerability components of the equation still exist. What happens if the defacers decided to not simply alter some homepage content , but 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 have a cultural aspect, mainly Islamic hackers defacing western web sites.

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, 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.

WHAT VULNERABILITIES DO HACKERS USE?

Cross Site Scripting (XSS) has dominated other vulnerability research projects: XSS is the most common vulnerability found by pen testers according to the Web Application Security Consortium's Statistics Project and tops the OWASP Top 10 2007 release. While there is little debate that XSS vulnerabilities are rampant, 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.



Attack / Vulnerability Used	%
SQL Injection	**30%**
Unknown	**29%**
Cross-Site Scripting (XSS)	**8%**
Insufficient Anti-Automation	**5%**
Insufficient Authentication	**3%**
Cross-Site Request Forgery (CSRF)	**3%**
OS Commanding	**3%**
Denial of Service	**3%**
Drive By Pharming	**3%**
Known Vulnerability	**2%**
Brute Force	**2%**
Credential / Session	**2%**

When focusing on incidents rather than vulnerabilities, we found that SQL injection attacks top the list with 30% of the incidents (20% in 2007). As mentioned in the previous section, keep in mind that the actual number of successful SQL Injection attacks was actually much higher than what is reported in WHID due to the Mass SQL Injection Bot attacks. XSS attacks were only 3rd with 8% (4th with 12% in 2007). It seems that while it is easier to find XSS vulnerabilities as the vulnerability is reflected to the client, it is somewhat harder to take advantage of them for profit driven attacks.

The table displayed above highlights one important factor - the unknown. 29% 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 main 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 by unnoticed for extended periods of time. The longer the intrusion lasts, the more severe the aftermath is. 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.

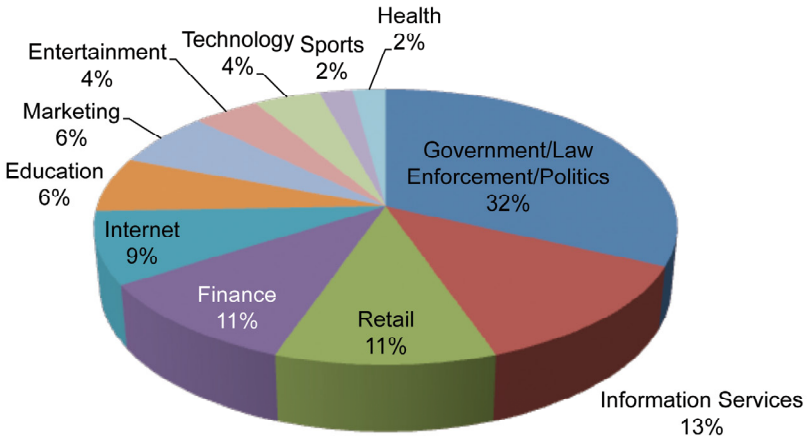
In many cases we feel that this lack of disclosure, apart from skewing statistics, prevents fixing the root cause of the problem. This is most noticeable in malware-planting incidents, in which the focus of the remediation process is removing the malware from the site rather than fixing the vulnerabilities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

But probably the main lesson is that we know too little. With so little information about real-world attacks, threat modeling requires collecting information from many different sources, each providing a partial and perhaps even biased view.

It is noteworthy that some top OWASP Top 10 vulnerabilities such as Cross Site Request Forgery (CSRF) and malicious file execution are not as widely exploited.

WHICH TYPES OF ORGANIZATIONS ARE ATTACKED MOST OFTEN?

Another aspect we looked into is the type of organizations attackers chose as targets. We found that the largest category of hacked organizations is government and related organizations (Law Enforcement and Politics). Combine those categories with education in 6th place and it appears that the non-commercial sector represents the primary target for hackers. Government is a prime target due to ideological reasons, while universities are more open than other organizations. These statistics, however, are biased, to a degree, as the public disclosure requirements of government and other public organizations are much broader than those of commercial organizations



Vertical	%
Government, Security and Law Enforement	**32%**
Information Services	**13%**
Retail	**11%**
Internet	**9%**
Education	**6%**
Marketing	**6%**
Entertainment	**4%**
Technology	**4%**
Sports	**2%**
Health	**2%**

On the commercial side, Internet-related organizations top the list. This group includes retail shops, comprising mostly e-commerce sites, media companies and pure internet services such as search engines and service providers. It seems that these companies do not compensate for the higher exposure they incur, with the proper security procedures.

Financial institutions on the other hand, were much lower on the list in 2007, and moved up to fourth place in 2008. Two possible explanations are that they have being targeted more by for profit attackers or that with the current Economic situations are being forced to disclose more.

SUMMARY

While financial gain is certainly a big driver for web hacking, ideological hacking cannot be ignored. Government and other organizations especially suffer from ideological hacking. Internet related organizations, especially hosting providers, are suffering from more and more serious for profit hacking incidents. Financial organizations are either starting to be targeted more or are disclosing more often.

As far as real-world hacking is concerned, we are still seeing the same basic attack vectors. While researchers are exploring ever more advanced attacks such as CSRF, hackers are still successfully exploiting the most basic application layer vulnerabilities such as SQL injection or information left accidentally in the open. Attackers are also becoming more proficient at automation so their attacks are more widespread as evidenced by the Mass SQL Injection Bots.