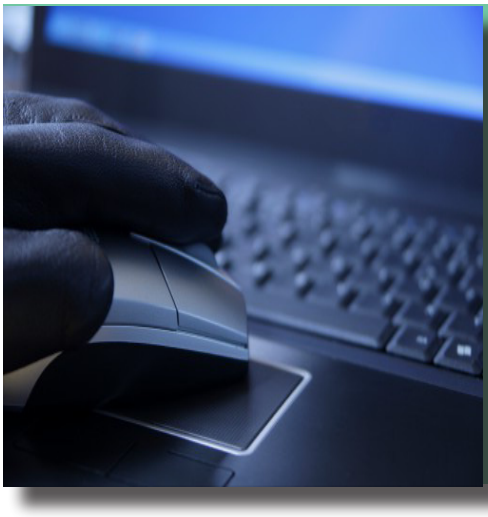
BREACH



THE WEB HACKING INCIDENTS DATABASE 2009

BI-ANNUAL REPORT

AUGUST 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

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 the web application security problem and provide information for statistical analysis of web application security incidents. Unlike other resources covering website security, which focus on the technical aspect of the incident, the WHID focuses on the impact of the attack. To be included in WHID an incident must be publicly reported, be associated with web application security vulnerabilities and have an identified outcome. Breach Security Labs (http://www.breach.com/resources/breach-security-labs/) is a WHID project contributor. For further information about the Web Hacking Incidents Database refer to http://www.xiom.com/whid-about.

RELATED RESEARCH WORK

Many projects such as Bugtraq (http://www.securityfocus.com/bid), XSSed (http://www.xssed.com/) and the Web Applications Security Consortium's Statistics Project (http://www.webappsec.org/projects/statistics/) track vulnerabilities in software or in 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 us with 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 (http://www.zone-h.org/). 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 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 WHID the right tool for making business decisions concerning website 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 44 incidents made it to the database for the first half of 2009 this year (compared to 57 in 2008 and 49 in 2007)**. Therefore the analysis in this document is based on relative percentage rather than on absolute numbers.

REPORT SUMMARY FINDING

An analysis of recent web hacking incidents performed by Breach Security Labs shows that Web 2.0 sites are becoming a premier target for hackers. Based on analysis of recent 'web hacking incidents of importance,' Breach Security Labs found that:

- The first half of 2009 showed a steep rise in attacks against Web 2.0 sites. This is the most targeted vertical market with 19% of the incidents.
- 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 number 2 "Unknown" attack category.
- Attack vectors exploiting Web 2.0 features such as user-contributed content were commonly employed: Authentication abuse was the 2nd most active attack vector, accounting for 11% of the attacks, and Cross Site Request Forgery (CSRF) rose to number 5 with 5% of the reported attacks.
- Defacements, which combined both Planting of Malware and standard overt changes, remains the most common outcome of web attacks (28%), while Leakage of sensitive information came in 2nd with 26% and Disinformation came in 3rd with 19%, mostly due to the hacking of celebrity online identities.

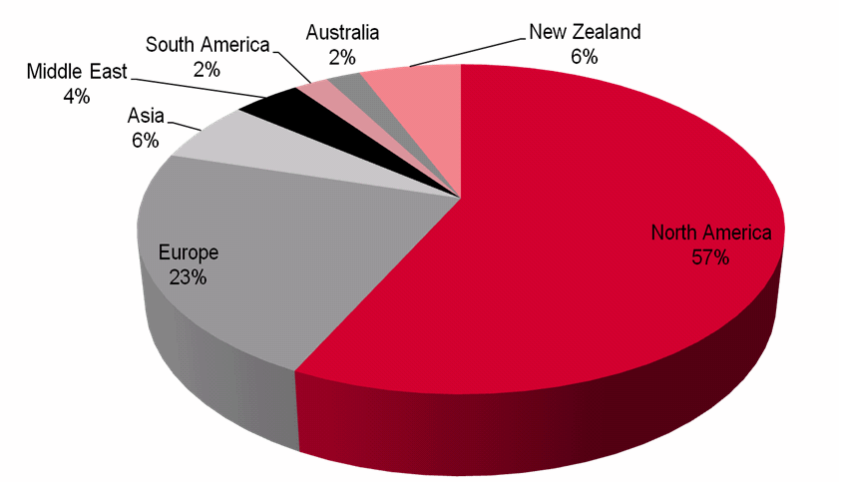
BREACH

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.
- 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. The 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 rather than a world status.



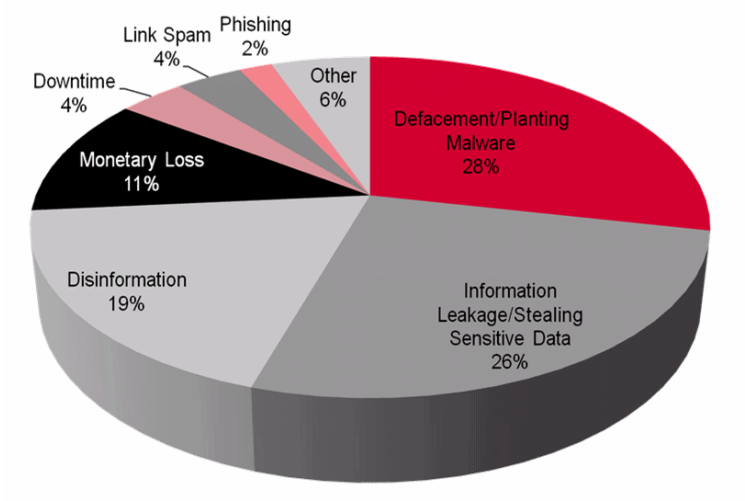
In this report we try to cover the following issues:

- 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 2009, defacements of websites are still the #1 outcome. It is important, however, to understand the definition of a defacement which is — **Unauthorized change to web site content**. With this in mind, the defacement category contains both overt, visible defacements, as well as, the planting of malicious code.

HACKING FOR PROFIT



Criminals are focusing on exploiting web application vulnerabilities in order to plant malware and thus infect clients who visit the website. 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.

> WHID Example: WHID 2009-22: Federal Travel Booking Site Spreads Malware (http://www.xiom.com/whid/2009/22/federal_travel_booking_site_spreads_malware)

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 websites. 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 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 decided to do something more damaging? Web defacement attacks should not be underestimated.

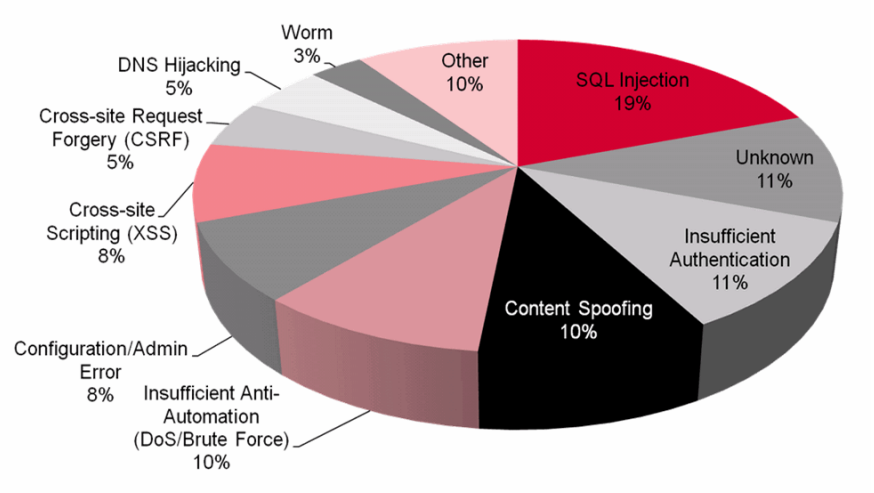
When further analyzing defacement incidents, we found that the majority were of a political nature, targeting political parties, candidates and government departments, often with a very specific message related to a campaign. Others have a cultural aspect, mainly Islamic hackers defacing western web 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 (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 2009-40: SQL injection Hits Sensitive US Army servers (http://www.xiom.com/whid/2009/40/US_army_SQL_injection)

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 (http://www.webappsec.org/projects/statistics/) 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.



SQL Injection remains the top vulnerability exploited by hackers (19%), only slightly losing ground since previous reports. The other attack vectors that topped the list are as follows:

- Insufficient authentication – while not a new attack vector, insufficient authentication attacks have become increasingly severe due to the proliferation of user-contributed and managed web sites. As such, it is not surprising to see more incidents this quarter.
- Automation is fast becoming a major security threat to web applications. Abuse examples range from brute force password attacks, to bypassing the wait queue in reservation systems, to opinion poll skewing.
- Cross-Site Request Forgery (CSRF) was recognized several years ago as a potentially potent attack vector. While it took longer than expected to appear, this year it has become a mainstream hacking tool. A rise in the exploit of CSRF vulnerabilities is in line with authentication abuse, since it essentially provides an alternative mechanism for performing actions on behalf of a victim. CSRF attack techniques were also leveraged to create worm-based attacks that rapidly propagated throughout social networking sites such as Twitter.

The table displayed above highlights another important factor - the unknown. 11% percent of the incidents reported where 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.

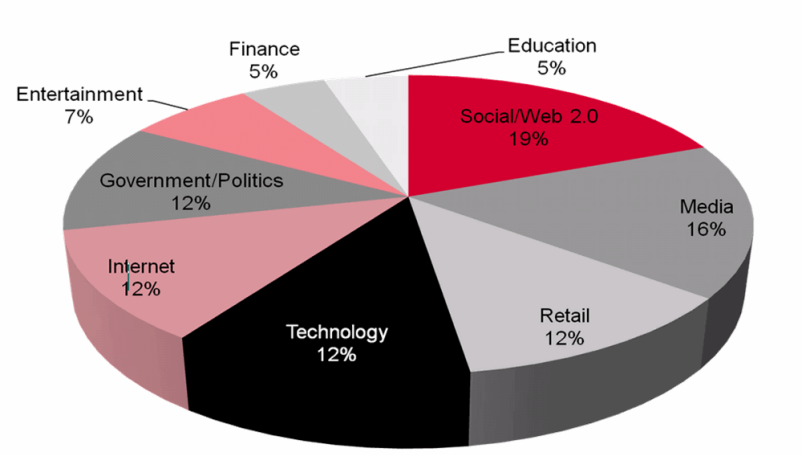
In many cases we feel that this lack of disclosure, apart from skewing statistics, prevents the fixing of the root cause of the problem. This is most noticeable in malware-planting incidents, in which the focus of the remediation process is removing the malware from the site rather than fixing the vulnerabilities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

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.

WHID Example: WHID 2009-37: Twitter XSS/CSRF worm series (http://www.xiom.com/whid/2009/37/twitter_csrf_xss)

WHICH TYPES OF ORGANIZATIONS ARE ATTACKED MOST OFTEN?

Another aspect we looked into is the type of organizations attackers choose as targets. We found out that the largest category jump of hacked organizations is Web 2.0 sites which rose to #1 on the list. This is mainly attributed to attacks on social networking sites such as Twitter where XSS/CSRF worms were unleashed. Government related organizations (Law Enforcement and Politics) dropped from the #1 spot in 2008 to #4 in 2009.



On the commercial side, Media, Retail, Technology and 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, who were much higher on the list in 2008, dropped down to 5th place. Two possible explanations are that they have being targeted less by for profit attackers or that with the current Economic situations are being forced to improve their security posture.

SUMMARY

As far as real-world hacking is concerned we are still seeing many 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 XSS/CSRF attacks against social networking sites such as Twitter.