# APWG Web Vulnerabilities Survey:

Principal Investigator and Correspondent Author:
**Dave Piscitello**
dave.piscitello@icann.org

Contributing Researchers:
John LaCour, Russ McRee, Robert W. Capps II, Rod Rasmussen,
Ebrima Ceesay, Thomas J. Holt and Gary Warner

*Published June 3, 2011*

## Table of Contents

**Disclaimer:** PLEASE NOTE: The APWG and its cooperating investigators, researchers, and service providers have provided this study as a public service, based upon aggregated professional experience and personal opinion. We offer no warranty as to the completeness, accuracy, or pertinence of these data and recommendations with respect to any particular company's operations, or with respect to any particular form of criminal attack. This report contains the research and opinions of the authors. Please see the APWG web site – apwg.org – for more information.

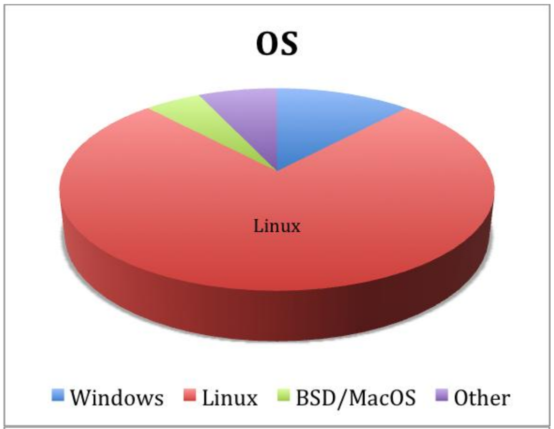
## Overview

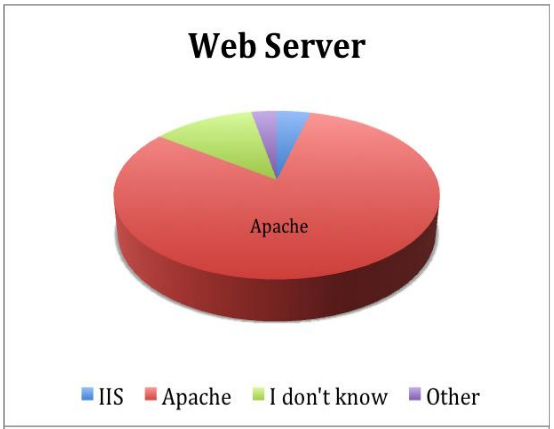
The Internet Policy Committee of the Anti-Phishing Working Group (APWG IPC) began an open survey in late 2009 of web sites that had been compromised and subsequently used to host phishing pages. The survey asked victims of attacks to describe the web site operating environment, the nature of the attack, and actions the victim took in response; the survey also asked the victim to share other details to obtain a clearer understanding of attacker methodologies and target preferences. In this analysis, the author provides a summary of the results and calls attention to important findings based upon 270 incidents reported through 22 March 2011.

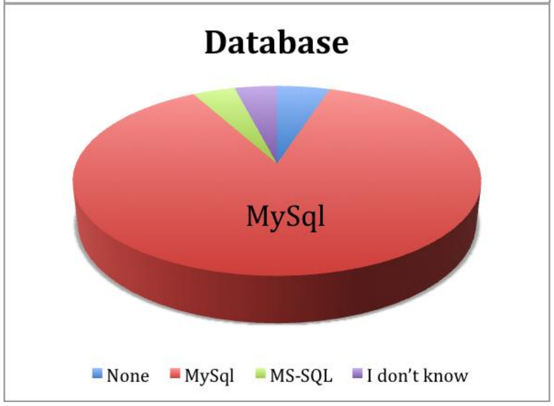
## What Hosting Environments Attract Attackers?

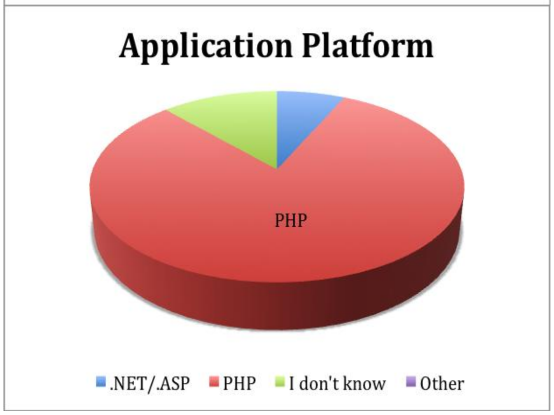
The most frequently attacked operating system among survey respondents was Linux OS (76%). Attack victims reported that they used Apache as their web server in 81 percent of the responses, MySQL as their database application in 81 percent of the responses, and PHP/Java as their application platform in 82 percent of responses.

While we acknowledge that "LAMP"—Linux, Apache, MySQL, PHP—is the most popular web operating environment, the APWG IPC is concerned that this profile is exploited with such apparent frequency.









The majority of victims (88%) indicated that neither default passwords nor default software configurations were present at the time of the attack.

Eighty-seven per cent (87%) also indicated that they were unaware of vulnerable software or default passwords at the time of the attack.

These responses suggest that web sites would benefit from broader implementation of preventative measures to mitigate known vulnerabilities and also from monitoring for anomalous behavior or suspicious traffic patterns that may indicate previously unseen or "zero day" attacks.

## What Are The Attackers After?

Only seven per cent (7%) of victims reported that the compromised web site was used for e-merchant purposes.

Seventeen percent (17%) reported that customer data were stored on the compromised hosts and only 4 percent reported theft of customer data.

Seventy four percent (74%) of the victims indicated that this was the first attack on this web site that resulted in the creation of a phishing or spoof web site. These responses corroborate our claim that the primary goal of phishers is to gain control of hosts for use in subsequent attacks and that the attacker did not target the reporting victim for the purpose of stealing data directly from his enterprise.

Eighty-four percent (84%) of the victims reported that attackers uploaded phishing or spoof web pages and scripts onto these sites for use during their phishing campaigns. Additionally, 24 percent of victims reported that attackers installed malicious software on their sites.

These finding are consistent with the findings reported in the *Global Phishing Survey: Domain Name Use and Trends*, published bi-annually by the APWG.[1] Phishers prefer to compromise web sites with reputable domain names. These domains are more difficult to suspend because the domain holder is also a victim.

## Discovery, Response, and Remediation

Victims are frequently unaware that they are hosting phishing sites until external parties notify them. Companies that specialize in phishing detection and remediation most often report attacks to victims (52%). Victims indicated that their web hosting service (18%) or the company that was phished (18%) were as likely to notify victims as the organization's staff was to discover the attack (19%). Only 8 percent of victims reported that law enforcement was called in to investigate the attack.

[1] http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf

Forty percent (40%) of attacks were discovered in less than one day and 18 percent were discovered within 2-3 days. However, one in four respondents did not know how much time elapsed between the compromise and discovery.

Only six percent (6%) of victims (or their hosting provider) discovered the attack as a consequence of reviewing web server logs and only sixteen percent (16%) discovered changes to web content.

Intrusion detection, antivirus, or other security software is credited for only four percent (4%) of the discoveries.

Implementation or improvement of web site monitoring that observes changes in activity and traffic behavior is clearly indicated as a means to reduce discovery or response time for attacks.

The typical response actions reported by victims are summarized in Table 1:

| **Table 1. What actions did you take to stop the attack? Please check all that apply** | |
|---|---|
| We removed phishing web pages | 85% |
| We repaired altered web pages related to our site | 33% |
| We changed passwords for web programs (e.g., content management system, blog, etc.) | 52% |
| We changed passwords for access to web server (e.g., Unix accounts) | 54% |
| Our hosting provider shut down web site entirely | 14% |
| We shut down the web site entirely | 15% |
| We patched or update the operating system | 11% |
| We patched or updated the web server software (e.g., Apache, IIS) | 9% |
| We patched or updated vulnerable software packages | 21% |
| We had our developers fix our custom software | 8% |
| Reviewed system and web server log files | 34% |
| We redirected the phishing site to the APWG phishing education page | 14% |

Many of these responses and remediation actions are consistent with practices the APWG recommended in its report, What to Do if Your Website Has Been Hacked by Phishers.[2] This report explains important incident response measures to take in the areas of identification, notification, containment, recovery, restoration, and follow-up when an attack is suspected or confirmed.

[2] http://www.antiphishing.org/reports/APWG_WTD_HackedWebsite.pdf

## More To Come

This article barely scratches the surface of the intelligence the APWG IPC has accumulated from the Web Vulnerability Survey. A complete analysis of the survey results—with specific recommendations, remedies, and practices—is in preparation by APWG IPC members John LaCour, Russ McRee, Robert W. Capps II, Rod Rasmussen, Ebrima Ceesay, Thomas J. Holt, Gary Warner, and Dave Piscitello. The APWG expects to publish this report later this year.

The online survey instrument remains open so that we can take periodic snapshots and observe whether phishing attacks change over time, and if so, how. If you are a victim of an attack, your web site was used to abet a phishing attack, and you would be willing to complete the survey, please contact the APWG or have your investigator contact the correspondent author, Dave Piscitello, at dave.piscitello@icann.org. The APWG IPC respects the sensitivity of the information you disclose. No individual survey results are disclosed and only aggregated data are used.

## Appendix A – Survey Data

# APWG Vulnerabilities Study

## Results Overview

zoomerang

Date: 3/22/2011 8:18 AM PST
Responses: Completes | Partials
Filter: YES RESPONSES ONLY

Before the Attack Occurred We would like to learn about the environment in which the attack occurred. This will allow us to determine what environments and practices are more likely to allow or prevent phishing attacks.

**1.** Have you or your organization been a victim of an attack that resulted in unauthorized access of a web site involving a phishing attack or publication of a spoofed web page?

| | | | |
|---|---|---|---|
| Yes | | 270 | 100% |
| No | | 0 | 0% |
| | Total | 270 | 100% |

If you answered "NO", please exit the survey. If you answered "YES", answer the remaining questions specifically with regard to the attack that you experienced.

**2.** What is your web site hosting environment?

| | | | |
|---|---|---|---|
| In-house hosting | | 45 | 17% |
| Web hosting provider. Your site is hosted on a dedicated server | | 58 | 21% |
| Web hosting provider. Your site is hosted on a virtualization platform (Virtual Machine infrastructure) | | 37 | 14% |
| Web hosting provider. Your site is hosted along with other customers on a shared server. | | 109 | 40% |
| I don’t know | | 21 | 8% |
| | Total | 270 | 100% |

**4.** Please identify the operating system (OS) software used in support of your web site.

| | | | |
|---|---|---|---|
| Windows | | 30 | 12% |
| Linux | | 187 | 76% |
| BSD/MAC OS X | | 12 | 5% |
| I don't know | | 17 | 7% |
| Other, please specify | | 9 | 4% |

**5.** Please identify the web server platform/software used to support your web site:

| | | | |
|---|---|---|---|
| IIS | | 11 | 4% |
| Apache | | 199 | 81% |
| Google Web Server | | 2 | 1% |
| I don't know | | 30 | 12% |
| Other, please specify | | 6 | 2% |

**6.** Please identify application platforms used in support of your web site:

| | | | |
|---|---|---|---|
| .NET/.ASP | | 16 | 7% |
| PHPJava | | 200 | 81% |
| I don't know | | 30 | 12% |
| Other, please specify | | 11 | 4% |

**7.** Which of the following web applications or web site management software are using on your web site? Check all that apply:

| | | | |
|---|---|---|---|
| Joomla | | 83 | 34% |
| Mambo | | 15 | 6% |
| Wordpress | | 45 | 18% |
| OS-Commerce | | 34 | 14% |
| ColdFusion | | 5 | 2% |
| cPanel | | 68 | 28% |
| Trixbox | | 3 | 1% |
| I don’t know | | 31 | 13% |

| | | | |
|---|---|---|---|
| Other, please specify | | 71 | 29% |

**8.** Please identify any database software used in support of your web site:

| | | | |
|---|---|---|---|
| No databases are used at this site | | 12 | 5% |
| MySQL | | 214 | 87% |
| PostGres | | 2 | 1% |
| MS-SQL | | 11 | 4% |
| Oracle | | 1 | 0% |
| I don't know | | 13 | 5% |
| Other, please specify | | 5 | 2% |

**9.** Was the web site used for e-commerce (e.g. online store, shopping cart, process payments, etc.)?

| | | | |
|---|---|---|---|
| Yes | | 73 | 30% |
| No | | 173 | 70% |
| | Total | 246 | 100% |

**10.** Were any customer data stored on the same host system as your web server (e.g., billing or credit card information)?

| | | | |
|---|---|---|---|
| Yes | | 40 | 16% |
| No | | 204 | 84% |
| | Total | 244 | 100% |

About the Attack The following questions ask about the actual attack experienced and what you learned about the attack itself.

**11.** Was this the first attack on this web site resulting in a phishing or spoof web site?

| | | | |
|---|---|---|---|
| Yes | | 131 | 74% |
| No | | 47 | 26% |
| | Total | 178 | 100% |

**12.** If you answered NO, above, how many times has this web site been hacked to create phishing sites in the past year that you know of?

| | | | |
|---|---|---|---|
| 2 | | 39 | 22% |
| 3 | | 12 | 7% |
| 4 | | 4 | 2% |
| 5 | | 2 | 1% |
| 6 | | 0 | 0% |
| 7 | | 0 | 0% |
| 8 | | 0 | 0% |
| 9 | | 0 | 0% |
| 10 | | 3 | 2% |
| More than 10 | | 6 | 3% |
| Not certain | | 112 | 63% |
| | Total | 178 | 100% |

**13.** Who discovered the attack initially?

| | | | |
|---|---|---|---|
| You, your colleague(s), your IT staff, or someone else with your organization | | 34 | 19% |
| Your web hosting service provider staff | | 32 | 18% |
| An Internet user / consumer | | 7 | 4% |
| The company whose site was spoofed or phished | | 33 | 19% |
| An Anti-Phishing company | | 92 | 52% |
| Law Enforcement | | 2 | 1% |
| I don’t know | | 8 | 4% |
| Other, please specify | | 10 | 6% |

**14.** How was the attack discovered or reported?

| | | | |
|---|---|---|---|
| A notification was received from the web hosting company | | 57 | 32% |
| A complaint was received from the organization that was spoofed or their representative | | 70 | 39% |
| You or your colleagues discovered file changes on the web site | | 28 | 16% |
| You or your colleagues discovered it from web server logs | | 11 | 6% |
| You or your colleagues discovered it from an Intrusion Detection system, AntiVirus Software, or other security system/software | | 8 | 4% |
| I don't know | | 16 | 9% |
| Other, please specify | | 20 | 11% |

**15.** How much time elapsed from the first compromised and the when the phishing web site was discovered?

| | | | |
|---|---|---|---|
| Less than 1 day | | 72 | 40% |
| 2 to 3 days | | 32 | 18% |
| 3 to 7 days | | 13 | 7% |
| 7 to 14 days | | 3 | 2% |
| More than 14 days | | 13 | 7% |
| I don't know | | 45 | 25% |
| | Total | 178 | 100% |

**16.** What means did the attackers use to access or compromise your web site?

| | | | |
|---|---|---|---|
| The attacker used the default passwords for an application on the web site | | 3 | 2% |
| The attacker guessed or hacked passwords for an application on the web site | | 3 | 2% |
| The attacker used the default password for the control panel or web site administration console. | | 3 | 2% |
| The attacker guessed or hacked passwords for the control panel or web site administration console. | | 3 | 2% |
| The attacker used a backdoor installed by other attackers. | | 7 | 4% |
| The attacker exploited a vulnerability in the Operating System (e.g. bug in Linux or Windows) | | 1 | 1% |
| They exploited a vulnerability in the web server software (e.g. Apache, Microsoft IIS) | | 2 | 1% |
| They exploited a vulnerability in a web application software package (e.g. PHP programs installed on the web site) | | 61 | 34% |
| I don’t know | | 80 | 45% |
| Other, please specify | | 15 | 8% |

| | | | |
|---|---|---|---|
| | Total | 178 | 100% |

**18.** If the attackers exploited web application software, did default 'out of the box' software configuration(s), sample data files, or other information and programs allow the attackers to compromise your web site?

| | | | |
|---|---|---|---|
| Not applicable, default software settings were not hacked | | 156 | 88% |
| Yes | | 22 | 12% |
| | Total | 178 | 100% |

**20.** When investigating the most recent incident, was there any evidence that the system had been compromised or hacked by more than one attacker?

| | | | |
|---|---|---|---|
| We suspect only one individual (or group) compromised our system | | 54 | 32% |
| We suspect that more than one individual (or group) independently attacked our system (i.e., we found evidence of unauthorized activities that seem to be unrelated). | | 30 | 18% |
| I don't have any information about that | | 85 | 50% |
| | Total | 169 | 100% |

**21.** Once a attacker succeeds in compromising a hosting server, he may attempt additional or opportunistic attacks beyond the system compromise. Do you have evidence of any additional attacks against or using your web site? Please check all that apply:

| | | | |
|---|---|---|---|
| A phishing site was created on our web site | | 149 | 84% |
| The attackers also stole our data or customer data | | 7 | 4% |

| | | | |
|---|---|---|---|
| The attackers hacked into other sites from our site | | 12 | 7% |
| The attackers installed malicious software on our web site | | 43 | 24% |
| The attackers changed our web pages to attack our web site visitors | | 18 | 10% |

**23.** If your web site is hosted on a shared server (with other web sites), were those web sites also attacked?

| | | | |
|---|---|---|---|
| Not applicable – not on a shared hosting system | | 29 | 16% |
| No – other web sites were not affected | | 59 | 33% |
| Yes – other web sites were affected | | 23 | 13% |
| I don't know | | 70 | 39% |

After the Attack: Response and Analysis The following questions are designed to determine what lessons were learned from this attack and what actions were taken by you, your colleagues, or your hosting provider in response. Again, we will not share any specific answers provided by you but will aggregate your responses with others to understand the bigger picture.

**24.** Before the attack, were you aware of any vulnerable software or default passwords on your web site?

| | | | |
|---|---|---|---|
| Yes | | 21 | 13% |
| No | | 139 | 87% |
| | Total | 160 | 100% |

**25.** If YES, were these issues exploited by the attackers in the most recent incident?

| | | | |
|---|---|---|---|
| Yes | | 29 | 18% |
| No | | 131 | 82% |
| | Total | 160 | 100% |

**26.** Did law enforcement investigate this attack?

| | | | |
|---|---|---|---|
| Yes | | 13 | 8% |
| No | | 141 | 92% |
| | Total | 154 | 100% |

**27.** What actions did you take to stop the attack. Please check all that apply:

| | | | |
|---|---|---|---|
| Removed phishing web pages | | 136 | 85% |
| Repaired altered web pages related to our site | | 53 | 33% |
| Changed passwords for web programs (e.g. content management system, blog, etc.) | | 83 | 52% |
| Changed passwords for access to web server (e.g. unix accounts) | | 86 | 54% |
| Nothing – our hosting provider took care of it | | 5 | 3% |
| Hosting provider shut down web site entirely | | 22 | 14% |
| We shut down the web site entirely | | 24 | 15% |
| We patched or update the operating system | | 18 | 11% |
| We patched or updated the web server software (e.g. Apache, IIS) | | 15 | 9% |
| We patched or updated vulnerable software packages | | 33 | 21% |
| We had our developers fix our custom software | | 13 | 8% |

| | | | |
|---|---|---|---|
| Reviewed system and web server log files | | 55 | 34% |
| We redirected the phishing site to the APWG phishing education page | | 22 | 14% |
| Other, please specify | | 16 | 10% |

**28.** Which of the following hacker tools and files were found on the system? Check all that apply:

| | | | |
|---|---|---|---|
| Phishing kit (.zip file of all of the phishing files) | | 45 | 28% |
| PHP shell (backdoor written in PHP) | | 60 | 38% |
| Log file of stolen customer data from the phishing site | | 4 | 2% |
| Vulnerability scanner | | 12 | 8% |
| Emailing programs | | 19 | 12% |
| Phishing Email Message / Template | | 32 | 20% |
| I don't know what these are | | 20 | 12% |
| None of these | | 17 | 11% |
| I don't have access to that information | | 25 | 16% |
| Other, please specify | | 11 | 7% |

**29.** Have you changed any of your practices or policies regarding web site security as a result of this incident? Please check all that apply:

| | | | |
|---|---|---|---|
| Changed hosting providers | | 13 | 8% |
| Changed our password management policy | | 74 | 46% |

| | | | |
|---|---|---|---|
| or practices | | | |
| Changed application patching/updating practices | | 50 | 31% |
| Installed antivirus software | | 21 | 13% |
| Installed other security software | | 27 | 17% |
| Other, please specify | | 35 | 22% |

**30.** Did you know that the APWG has published a document about what to do if your web site has been hacked by phishers? It is available at www.antiphishing.org/reports/APWG_WTD_HackedWebsite.pdf

| | | | |
|---|---|---|---|
| Yes and I used it | | 23 | 15% |
| Yes but I did not use it | | 9 | 6% |
| No | | 126 | 80% |
| | Total | 158 | 100% |