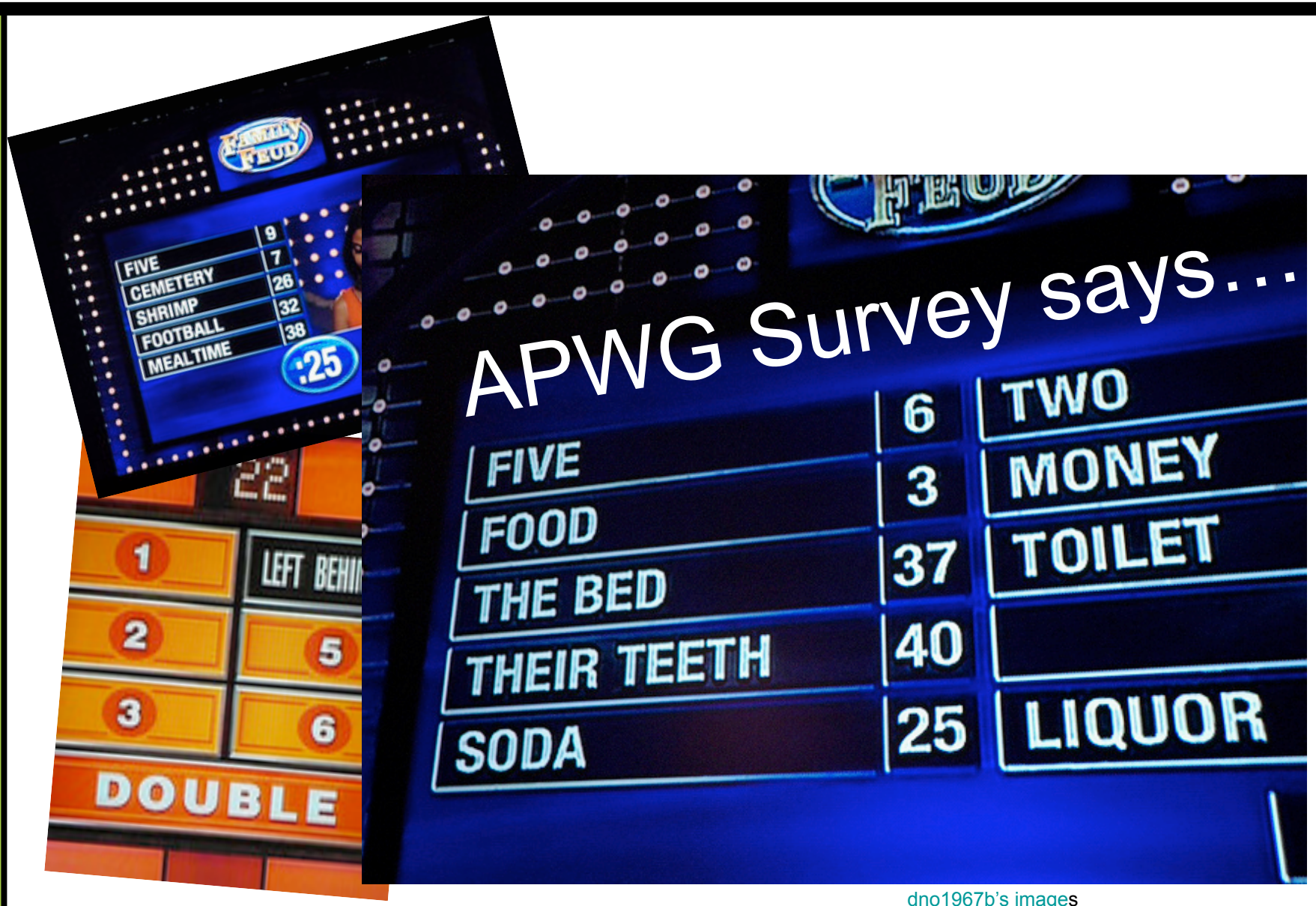
A Survey of Web Sites Exploited by Phishing Attackers

Dave Piscitello, ICANN
On behalf of the APWG IPC
dave.piscitello@icann.org

APWG
Unifying the
Global Response
to Cybercrime

Background

- Survey launched August 2009 by Internet Policy Committee of Anti-Phishing Working Group (APWG)
- Initial sample 1Q2012 (255 responses)
- Second sample 2Q2012 (143 responses)
- Sum of responses and samples (compared) considered for today's webinar



dno1967b's images

Do Attackers Target Site Hosting Environments?

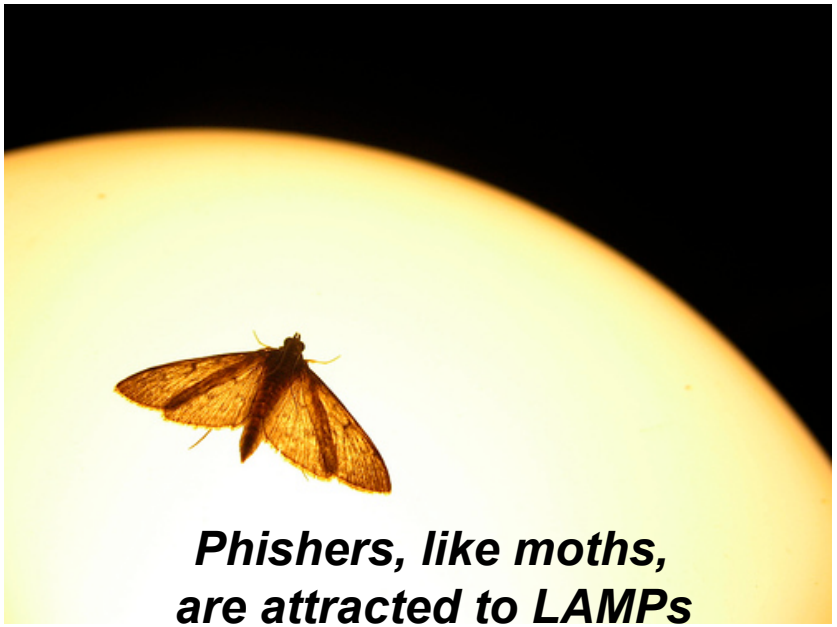
What is your web site hosting environment?	
In-house hosting	14 %
Web hosting provider. (Dedicated Server)	22 %
Web hosting provider. (Virtual Machine infrastructure)	14 %
Web hosting provider. (Shared server).	42 %
I don't know	7 %

Majority of victims use web hosting providers (78%)

Is this significant?

What hosting platforms attract attackers?

- What is LAMP?
  - Most popular hosting environment
    - Linux Operating System
    - Apache web server
    - MySQL database
    - PHP/Java dev platform

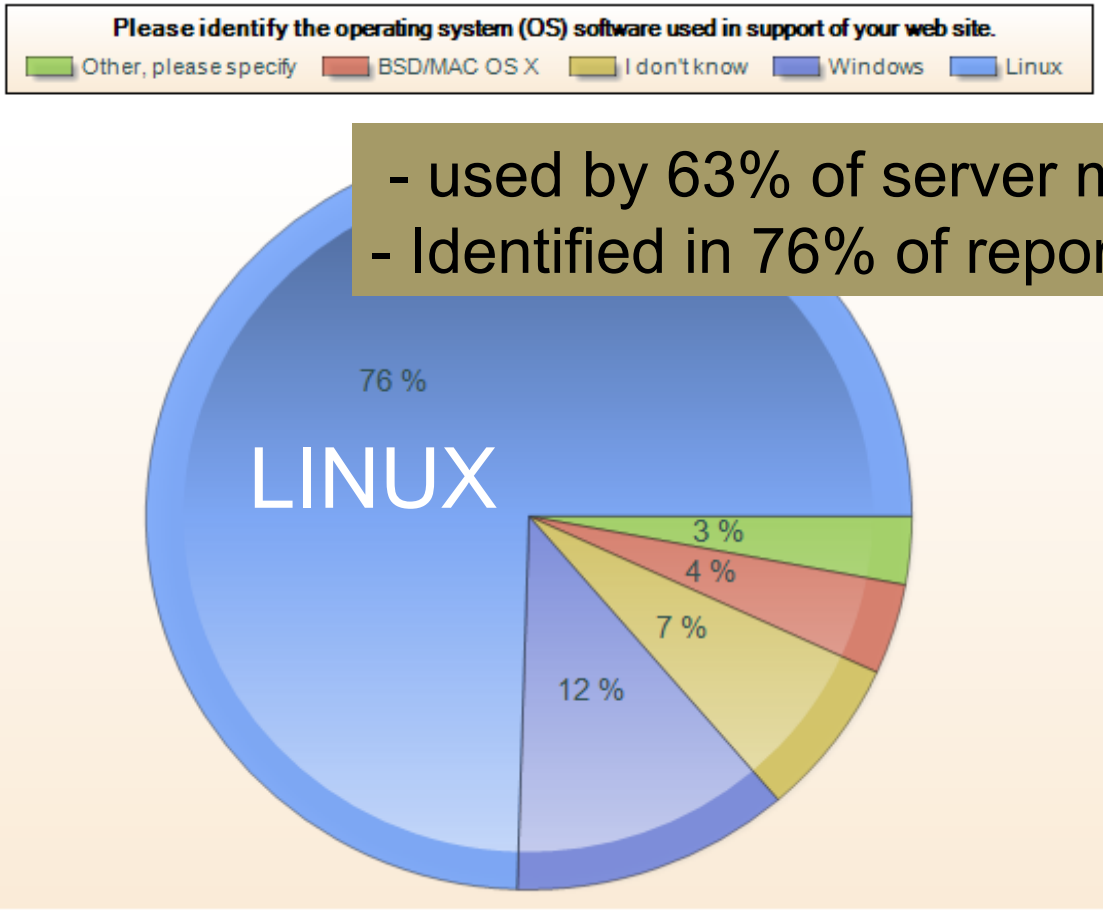


Phishers, like moths, are attracted to LAMPs

- *Is LAMP exploited at a higher frequency than usage and market share indicate?*

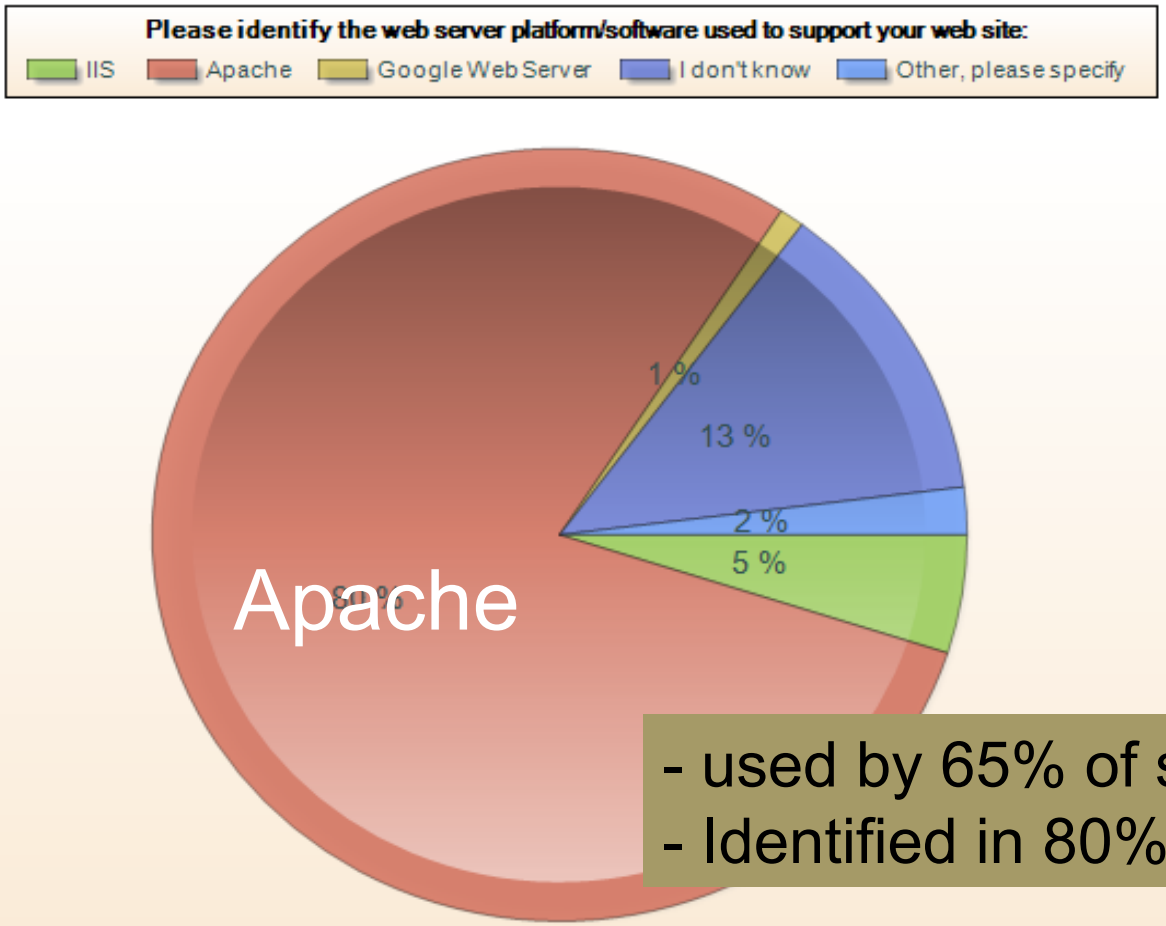
bepster K's image

LINUX



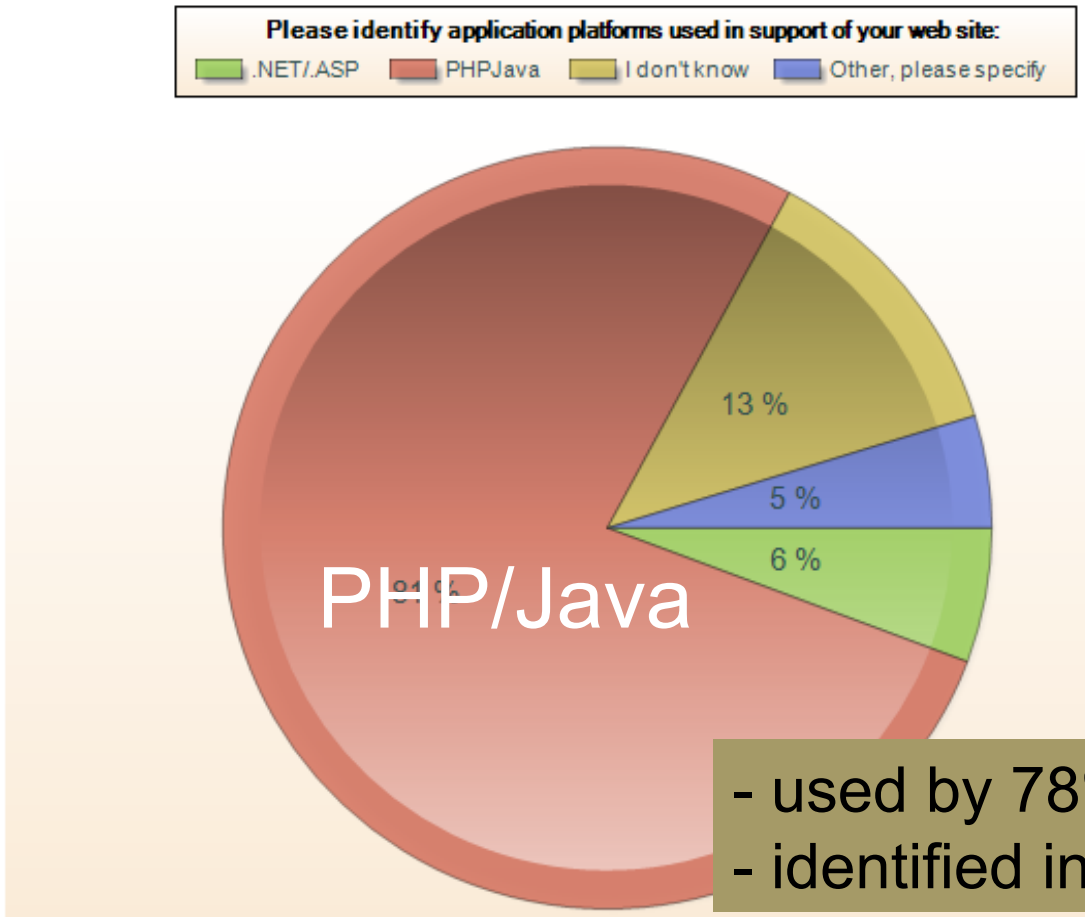
- used by 63% of server market
- Identified in 76% of reports

Apache Web Server



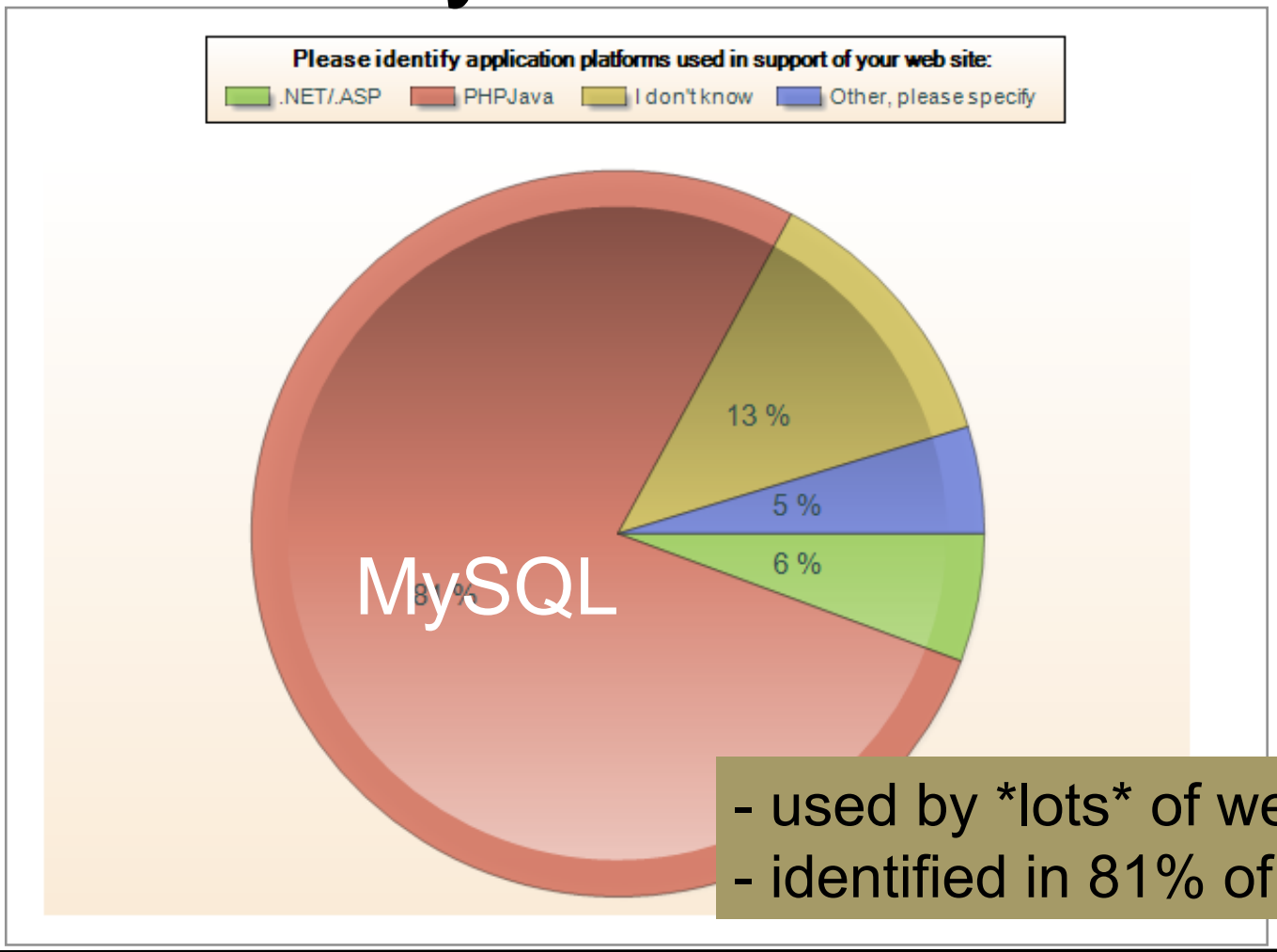
- used by 65% of server market
- Identified in 80% of reports

PHP/Java



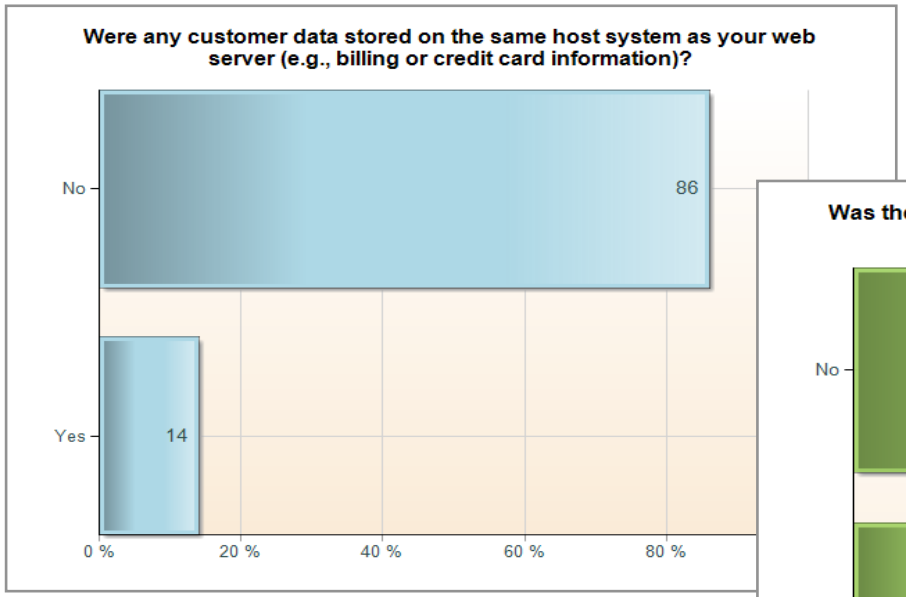
- used by 78% of web sites
- identified in 80% of reports

MySQL Database

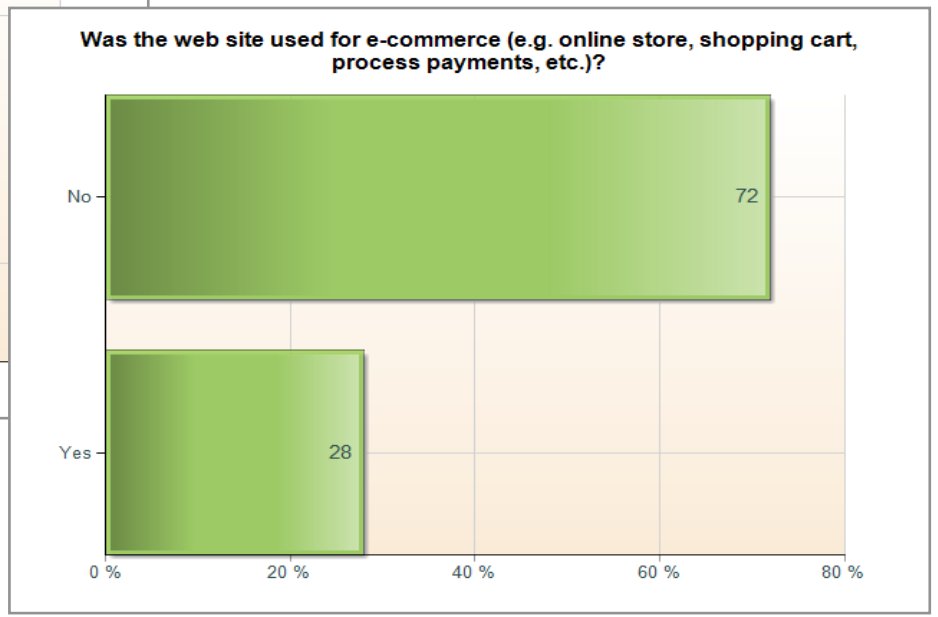


- used by *lots* of web devs
- identified in 81% of reports

What are the attackers after?



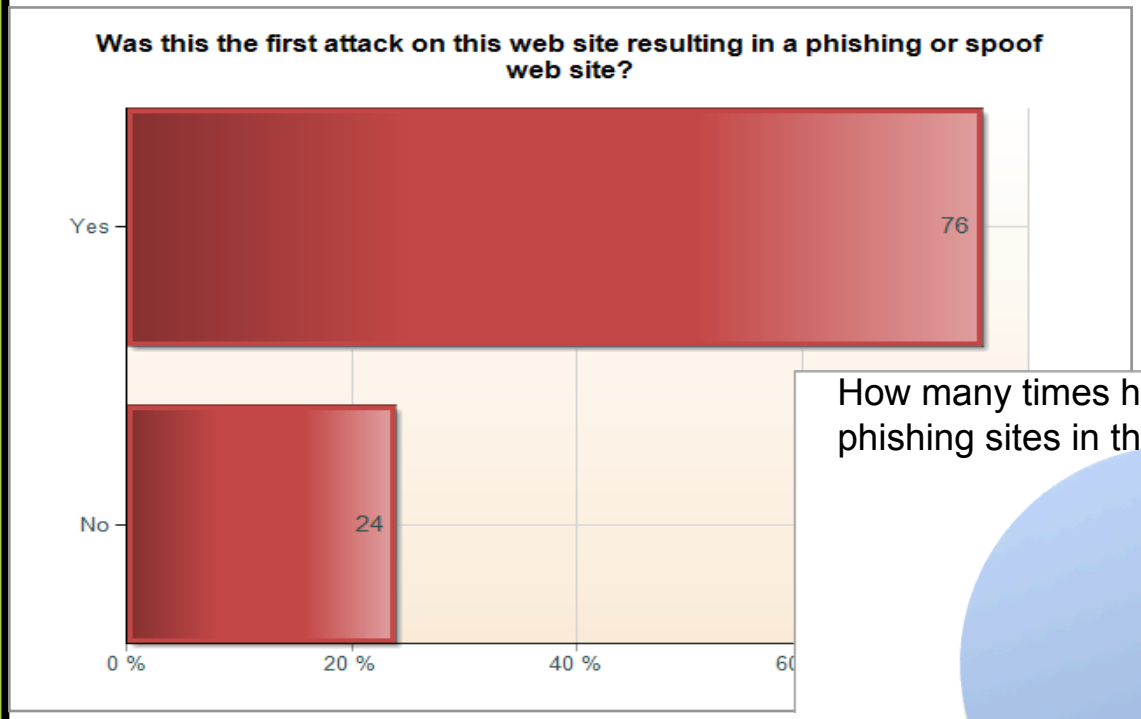
Presence of customer data is not a factor



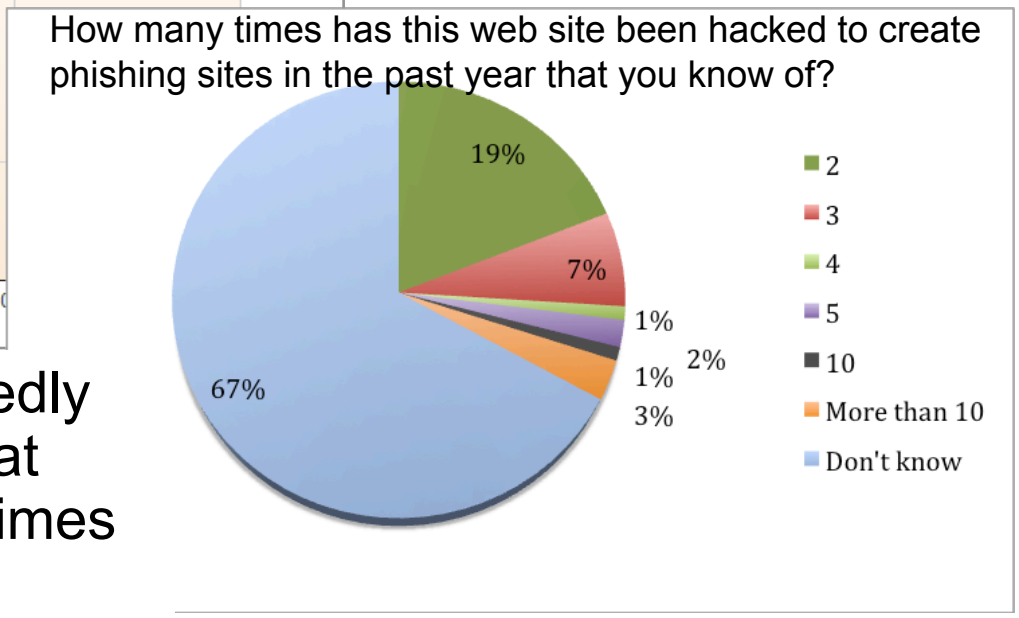
Majority of attacked sites do not support e-commerce

The primary objective among reported attacks appears to be "acquiring hosts for phishing pages"

Victimology



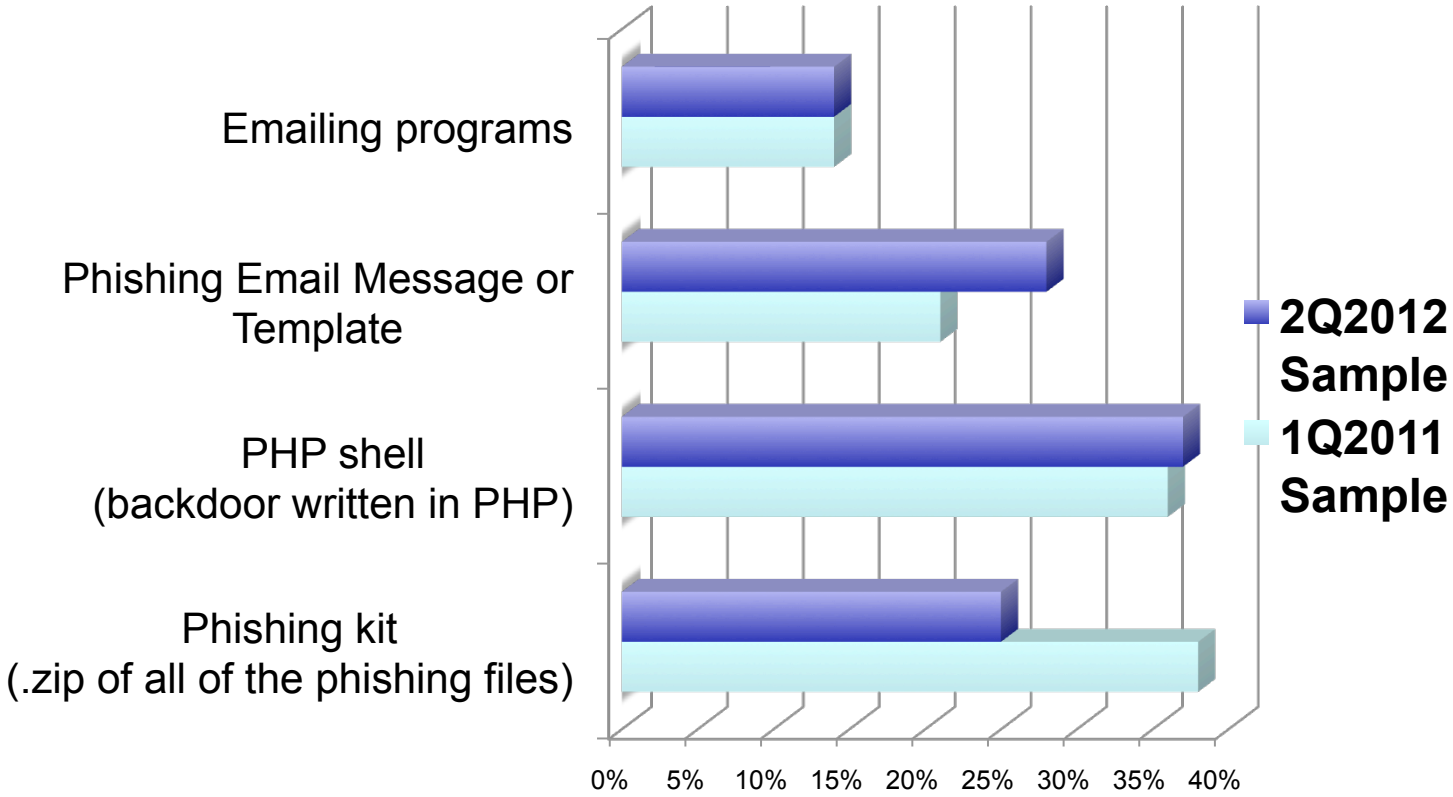
1 in 4 companies are attacked more than once



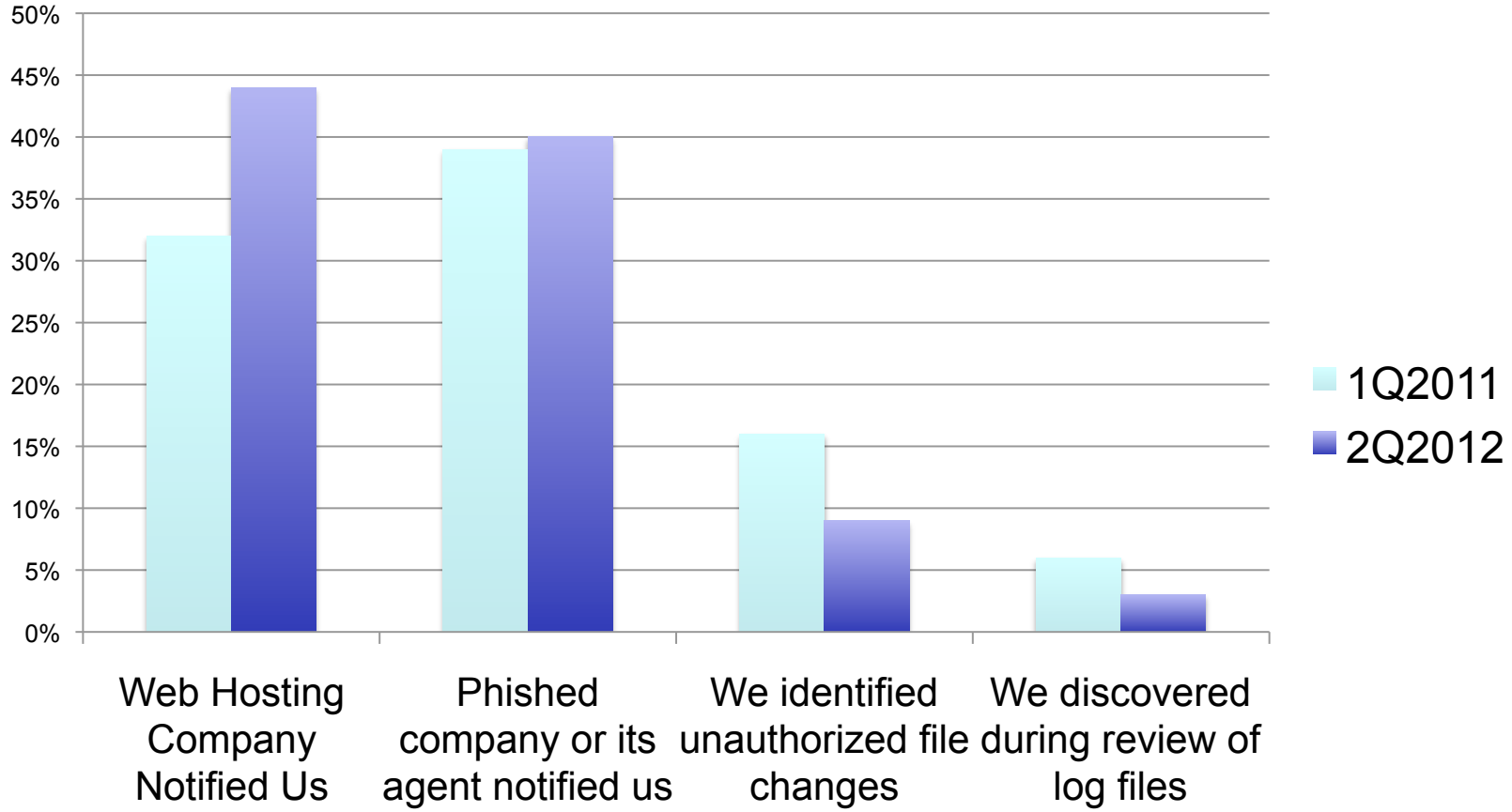
2 of 3 responses from repeatedly attacked companies report that *they do not know* how many times they've been attacked

What evidence of an attack did you find?

Attackers leave PHP shell code (backdoor), phishing kits, some means to send mail

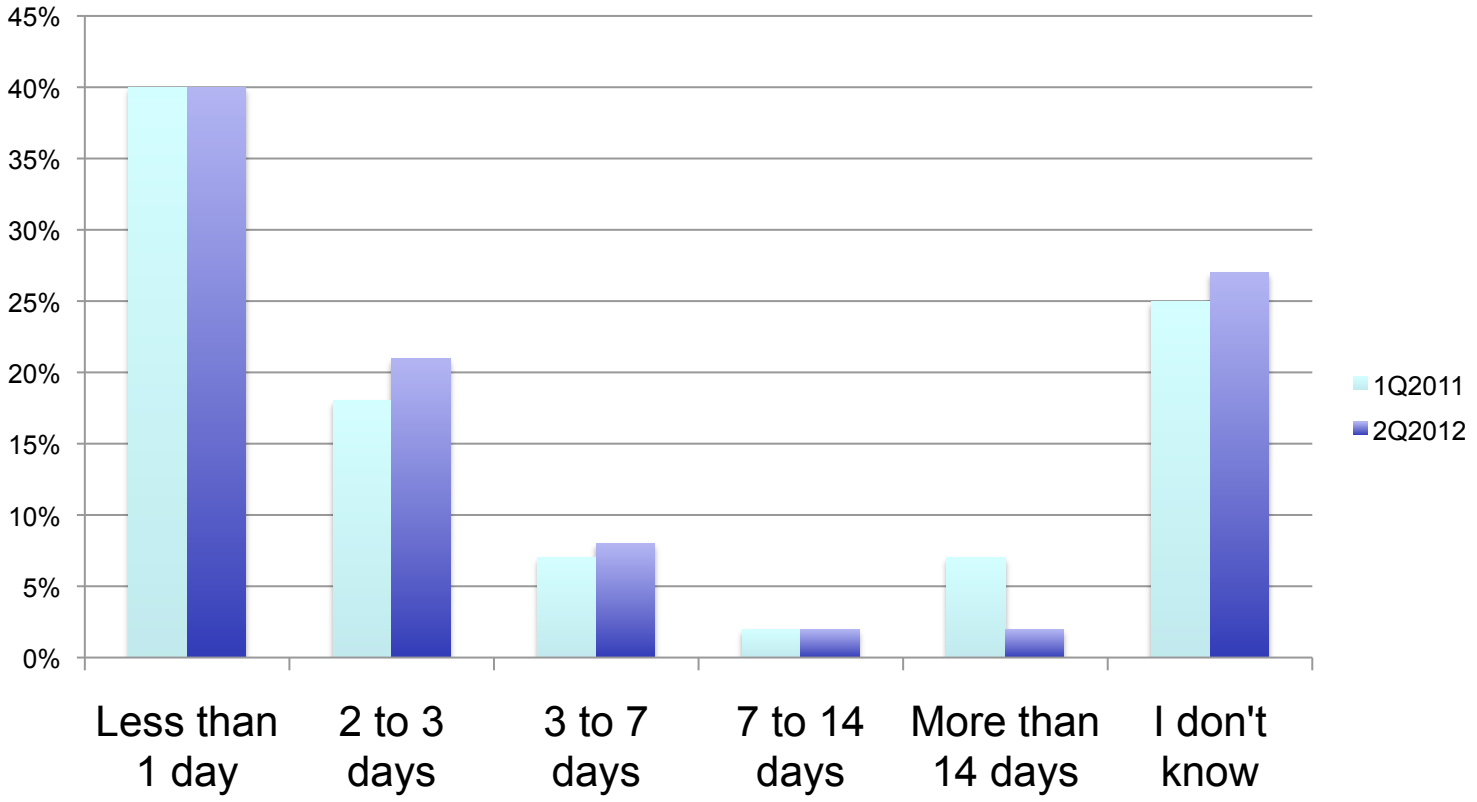


How was the attack discovered or reported?



How quickly did you respond to the attack?

How much time elapsed from the first suspicion (or report) of a compromise and when the phishing web site was discovered?

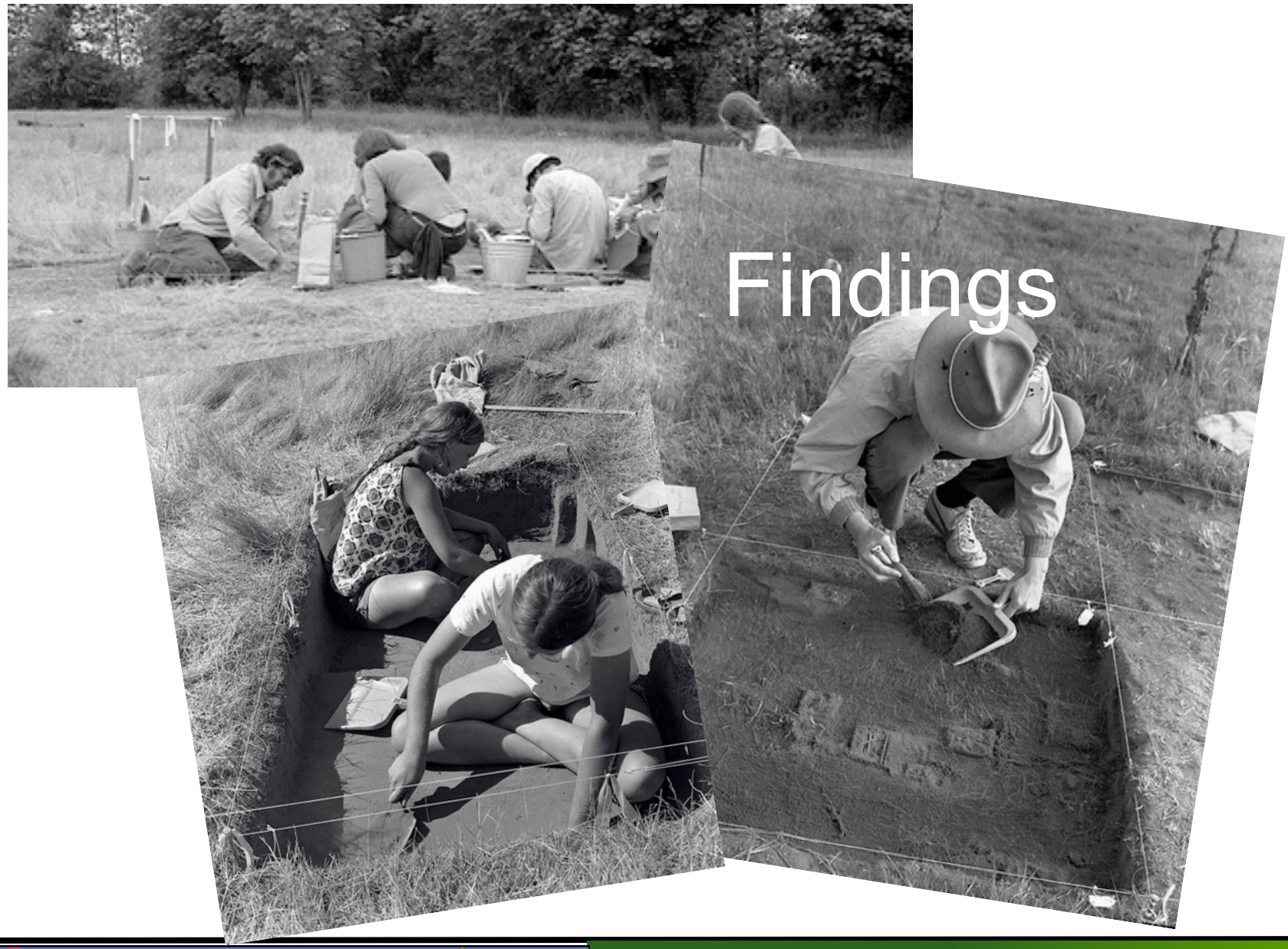


What actions did you take?

What actions did you take?	1Q11	2Q12
Removed phishing web pages	85%	82%
Repaired altered web pages related to our site	33%	32%
Changed web programs' passwords	52%	42%
Changed web server	54%	42%
Hosting provider shut down web site	14%	26%
Shut down the web site (internal)	15%	10%
Patched or updated operating system	11%	13%
Patched or updated web server	9%	8%
Patched or updated software	21%	20%
Had developers fix custom software	8%	8%
Reviewed system and web server log files	34%	26%
Redirected the phishing site to the **APWG phishing education page**	14%	9%

Do these actions leave you with a good feeling?

- Less than 100% for many remediating actions is just not good enough.
- Remove phishing web pages quickly to minimize the harm done to the target of the phishing attack
- Examine of all published content against the most recent, known-to-be-correct copies to ensure that all altered content is identified and removed
- Always change passwords (leave no room for doubt)
- Always make certain OS, web server, and other software are “patch current” following an incident



APWG

Unifying the
Global Response
to Cybercrime

What have we observed from survey responses?

- Phishers target legitimate web sites to host phishing pages
- Attack victims are often “the last to find out”
- LAMP is popular platform… and a popular target
- Incident response is spotty and slow
- Percent of “chronic victims” is unacceptable

What could have been done to prevent attacks?

- **Secure development**
- Review and secure applications during development cycles
- **Preparedness & Planning**
- Use penetrating testing or vulnerability scanning to mitigate vulnerabilities
- Develop an incident response *methodology* and plan
- **Secure deployment, Daily operations**
- Implement best practices for Linux and Apache server security
- Keep all software patch current
- Log system and network events, review frequently for suspicious activity
- Proactively monitor hosting and network facilities for suspicious activities

When you're the victim…

DeepWaterHorizonResponse's image

Erkka P.'s image

What should you do if your web site is attacked?

- **REPORT**

- **Should you report the incident? To whom?**
- Yes (may be influenced by business, regulatory, and legal constraints)

- **CONTAIN**

- **Should you make a copy of the unauthorized content?**
  - Save a copy of the phishing site pages and any unauthorized content, scripts, or executable programs you discover during your analysis
- **Should I take my site offline (temporarily)?**
  - Your call… but make this decision *in advance* and include in your incident response plan
  - If you keep your site running block access to unauthorized content

What should you do if your web site is attacked?

- **RECOVERY**

- **Should I restore from backup or rebuild from scratch?**
  - Rebuild from original install media or do an OS restore from known-good backups in offline mode
- **When should I update my software and check my configuration?**
  - Before you return your web site to a production environment, be certain that all software is up to date, patch and hot fix “current”
- **Should I change all my passwords?**
  - Yes, but only when you are confident that you have restored your web site to an authentic and normal operating state

What should you do if your web site is attacked?

- **Follow up**
- **Ask, "What lessons have I learned?"**
  - Share information about the incident with hosting partners
- **Ask, "How can I do better?"**
  - Adopt recommended practices for minimizing a web site's vulnerability to attack by phishers
  - see ***What to do if your web site has been hacked by phishers?***

http://www.antiphishing.org/reports/APWG_WTD_HackedWebsite.pdf