DEFACED

An insight into methodologies, tools and motivations

Adam "@feabell" Bell – Security Consultant
Event – OWASP Day 2015
Date – 27th February 2015
Company Overview

Company
- Lateral Security (IT) Services Limited
- Founded in April 2008 by Nick von Dadelszen and Ratu Mason (Both Directors)
- Auckland, Wellington, Melbourne: ~20 highly specialised security consultants

Services
- Security testing (design & architecture, penetration testing, configuration, code reviews, security devices & controls, mobile apps)
- Security advisory (Lifecycle compliance & audit – ISO, PCI-DSS, NZISM, policy process development, threat modeling and risk assessment)
- Regular ongoing technical testing and assurance programs
Who’s This Guy?

It’s a me, MARIO!
"The internet is a hostile place, particularly if you are a charitable organisation.

Websites are compromised and defaced on a daily basis and sometimes their owners need a little help getting to the bottom of what happened.
So what if your website has been compromised and is getting reports of abuse... How do you react? What can you do?

This talk will cover a recent incident response and investigation I carried out and describe how you, as the developer-in-charge of an all-in-one webhost can investigate and respond.

Based on a true story, this talk will describe the incident response methodology I used, take a look at some of the tools that the defacer had left behind and give an insight into the badguys mindset and motives."
While this is a Lateral Security Presentation, this was an IR carried out on behalf of myself

As such, any incompetence is on me, not Lateral.

Names changed to protect the innocent
Dev <> Ops distance is closing

Your code doesn’t stand in isolation, it has to interact with tens of other tools and API’s.

Once your code leaves your hands, it’s often not even yours anymore. And will slowly become obsolete as it sits on a client disk somewhere
IT'LL HAPPEN TO YOU
Story Time
Our hero protagonists.

The BAHLMAN and Robell.
Our victim
Our antagonist
The Bahlman was approached by a third party

Third party is a charity organisation that was critical of their own government.

Third party had previously been compromised, and wanted a secure platform going forward.

The Bahlman and Robell LEAPED into action, with a new server, migrating their ageing WP install to latest. Pruning old addons and frankly making it idiot proof
In January 2015, our technical contact at the charity forwarded an email to us from a third party who had emailed their abuse@ address.

This third party claimed that our IP had been detected performing malicious attacks against wordpress instances that they controlled. This site looked sketchy as HELL

(and had an unrelated SQL injection vulnerability)
So, we sceptically started the incident response process.

I mean, our server was perfect... right?
But we found nothing.

There were no malicious users added, no signs of a system intrusion, no (detectable) rootkits. The system seemed secure.
403.php, 404.php (ignore) 500.php are not the real files for these error messages. There are dynamically generated by apache as we have not specified custom error handlers.

Also Salem.php is just obviously malicious.
While the previous incident response lifecycle may be unfamiliar to you, I am happy to present one that may be more recognisable.
We knew the host was compromised, so real incident response could begin. The first step?
The Bahlman delivered the customary fee for “free” incident response
So, where to start? Let's fix our timeline
So let's grab all of our log files and throw them into a log aggregation tool. I like Splunk
So how long has the box been compromised?
So that’s not good.

3 months online before compromise. 7 months of uninterrupted compromise. facepalm
So how did this even happen?

This is the first request for the ‘badguy’ file. To /wordpress/foo/bar/whatsit.

But /wordpress ISN’T THE ROOT DIRECTORY FOR THIS SITE. This is a DIFFERENT wordpress install. WHAT THE ACTUAL HECK.
So, where did this WordPress come from?

- Charity had previously had “sub” sites on their old WP install, that they had deemed ‘no longer needed’
- Charity had decided they were needed after all
- Dropped the old WP install folder into /wordpress
- Noticed that things didn’t work, because the backend database no longer existed.
How Did Those Files Get In The WebRoot?

- We can see that before they were in the webroot, they were in a WP theme.

```bash
[000] "GET /wordpress/wp-content/themes/default/404.php HTTP/1
```  

- And it appears that this client IP logged into the WP admin interface to put them there:

```bash
```
How Were Admin Creds Obtained?

- We see a different third party hits the WP install script for the old WP install
- They then login to the admin console
- And upload a DIFFERENT backdoor
So that’s not good.

3 months online before compromise. 7 months of uninterrupted compromise. facepalm
No facepalm.gif suitably demonstrates the magnitude of facepalming required.
June 2014
- 404.php (theme) used to drop:
  /Text/x/by.php
  /Text/x/403.php
- Adds a new Wordpress admin user

March 2014
Server Online

Then

August 2014
- slo.php dropped
- Akismet.php modified
- Salem.php dropped

September – December 2014
- Used to do naughty things

April 2014
Server Actually Compromised
- doc.php dropped
- Assumed 404.php dropped in WP theme

July 2014
- 403.php dropped in the webroot

January 2015
Server Offline

Now
1337mir is a well known website defacer, with a LOT of defaces. In the tens of thousands on zone-h

Rather than perform a deface, they just posted a MESSAGE to zone-h in a non-indexable file.

1337mirs website claims that he is a sub-17 year old guy “interested in security”.

Was this a charitable act to a company that is a charity?
This is MiR, and I have been hacking since I was 14, well over now me MiR. I love to hacking and like to break website
And this is where our actual evil hacker comes in.

1337mir wasn’t evil, he didn’t use our server for badness. But this third party did.

We don’t know what our server was being made to do, apart from that it was attacking other WP hosts. I’d guess either scanning for vulnerable components or bruteforcing login creds.
Tool time!
A quick note on obfuscation

This is how most of the dropped files look when opened in the text editor of your choice (which is Vim, naturally).
eval(gzipinflate(base64_decode(“massiveblobofbase64goesheremeanseriouslyhowlongisthisbigchunkofbase64?It’sso longthatit’ssevenlinewrappedonthe presentation slide.It’saseriesoulylargeamountof text.Gztodavidonhisnewarrival!Is the realistically more needed to pad this out? Can I keep typing gandfillthisslide? I’m pretty sure I can. #FobsthoughtleadertrainingatOWASP2016#dreamisalive”))
Pretty basic tool, no privescs to root or anything... but allows you to do what you want.
Just a 404, right?
Secret login on 404 page
So if these tools are all so amazing, why can’t we just google some unique strings and find all the compromised websites?

Because every tool, as its first line says “if you are in this list of useragents, i’m not showing you a thing”
What Went Well

- System Hardening
- Not allowing client root access
- Logrotate & logfile histories
- IR process
- A somewhat benevolent hacker?
- Poor opsec by the attackers
What Didn’t Go So Well

- Allowing client any kind of access at all
- Active log monitoring
- File integrity monitoring
- Client communications and siloing
What Can We Do To Prevent This?

- Share YOUR stories of compromise
- Understand the software stack
- Get cosy with your Ops team
- Don’t assume
Questions and Contacts

Lateral Security (IT) Services Limited

Wellington
38-42 Waring Taylor Street (level 7, Petherick Tower)
PO Box 8093, Wellington 6143, New Zealand
Phone:  +64 4 4999 756
Email:  sas@lateralsecurity.com

Auckland
187 Queen Street (level 8, Landmark House)
PO Box 7706, Auckland, New Zealand
Phone:  +64 9 3770 700
Email:  sas@lateralsecurity.com

Melbourne
200 Queen Street (level 13)
Melbourne, VIC 3000, Australia
Phone:  +61 1300 554745
Email:  sas@lateralsecurity.com

Presentation Download
www.lateralsecurity.com/prestations