Simple. Powerful. Precise.

How’d That End Up On Pastebin

Ryan Linn
Principal Consultant, Cyber Threat Analysis

Agenda

- Introduction
- Why are we here ?
- Scenario 1: Wordpress Hack
  - Attack Walkthrough
  - Analysis and Countermeasures
- Scenario 2: Backoff POS Attack
  - Attack Walkthrough
  - Analysis and Countermeasures
- Strategic Defenses
- Conclusion

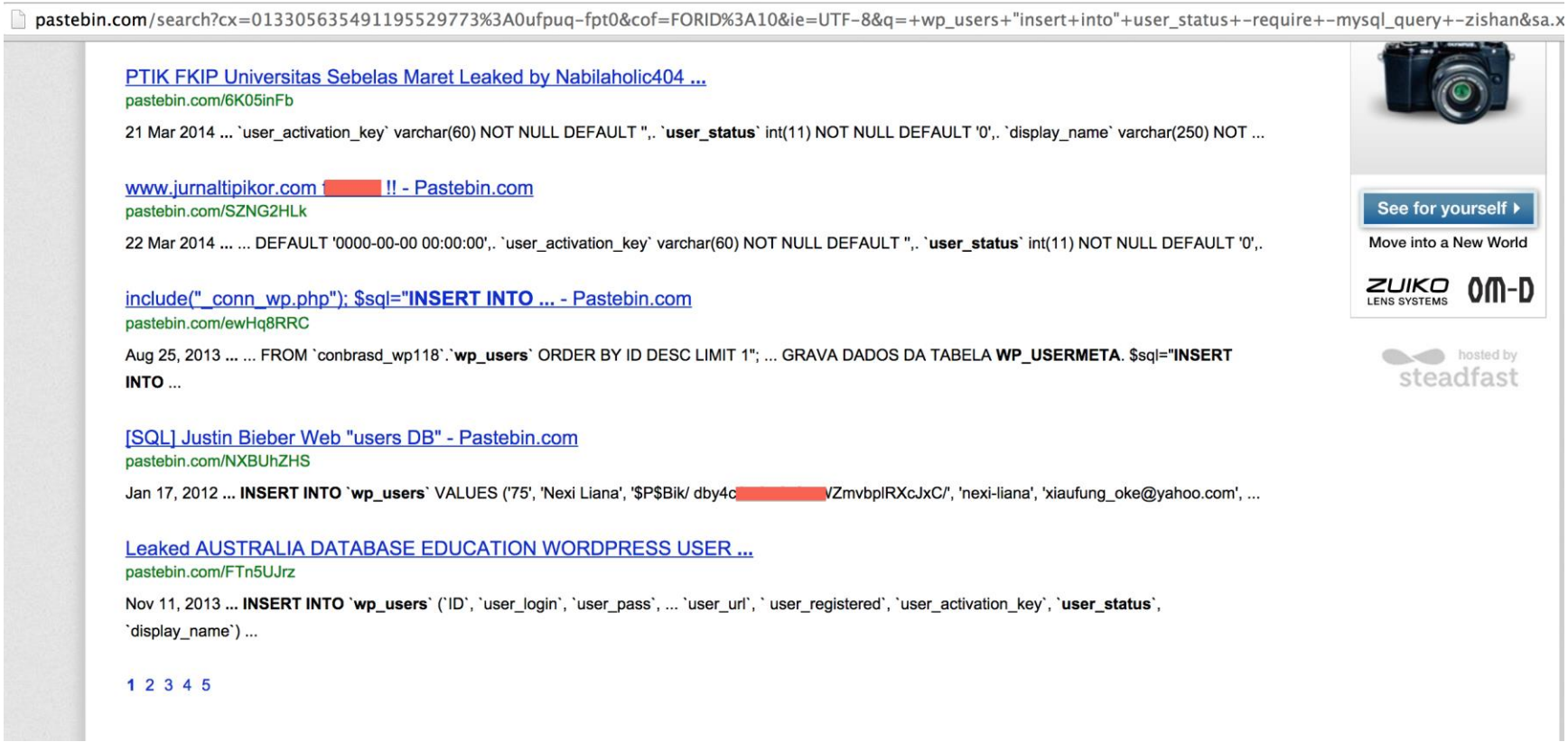
`whoami`

- Principal Consultant – Penetration Testing at Nuix
- Author
  - Coding for Pen Testers
  - Browser Hacker's Handbook (contributing)
  - Gray Hat Hacking (in Novemberish)
- Open Source Projects
  - Metasploit
  - Ettercap
  - Browser Exploitation Framework
- Background
  - Sys Admin
  - Penetration Testing
  - Forensics

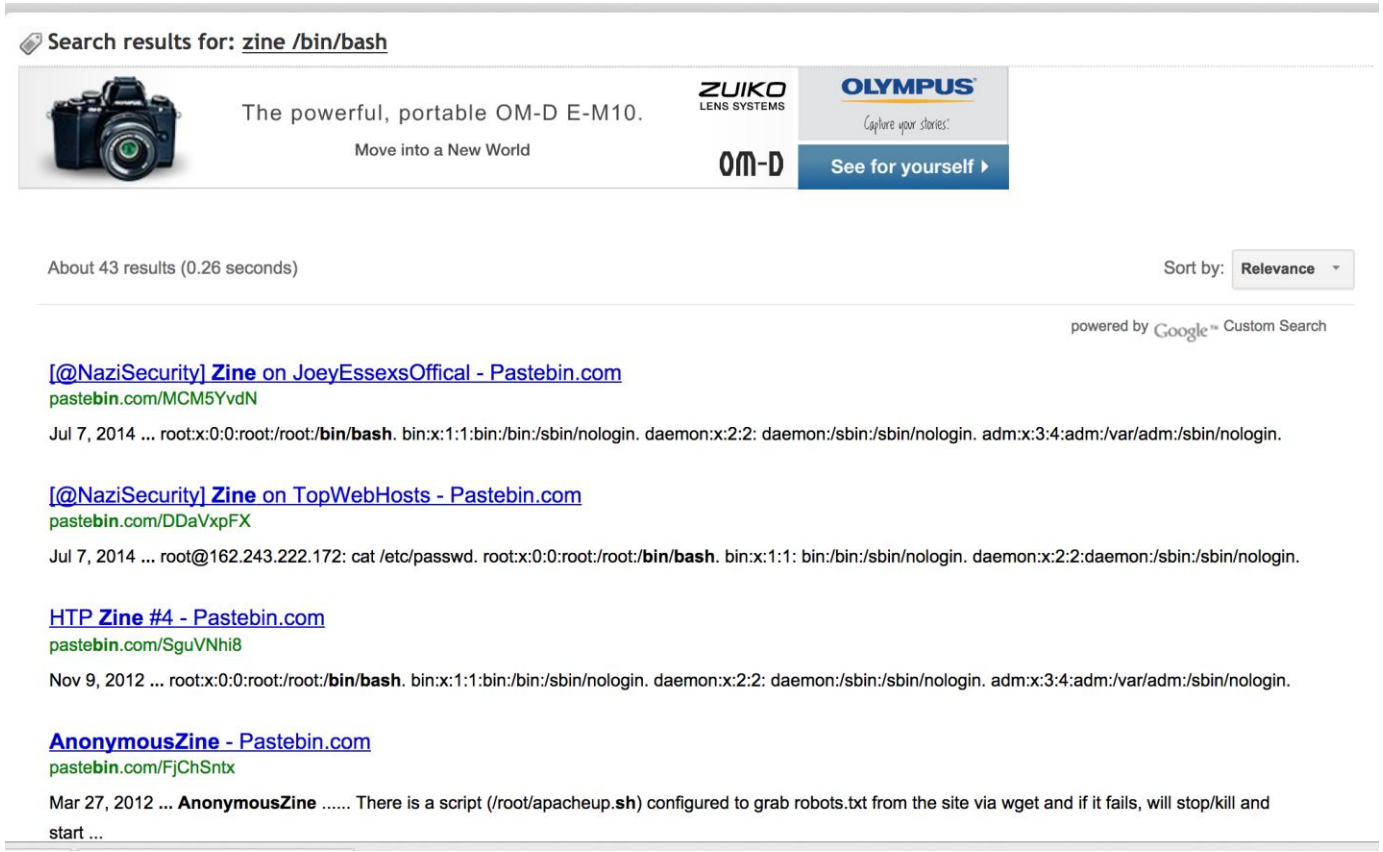
Why are we here ?

- As security professionals, we're busier than ever before
- New large scale breaches happening every month
- Many more are happening that aren't as public
- Blue team is having a rough go at it
- In part, understanding what you're defending against is hard
- Defense is no longer enough, you need detection

What are the stakes ?



Have a zine published about you?



None of us are immune.

INTERNET ARCHIVE WayBackMachine

http://milw0rm.com/papers/297 Go

5 captures
2 Mar 09 – 19 Jun 10

____

```
       _   _     _       _ _       _
  ___| |_| |__ (_) ___ __ _| | |__   __ _  ___| | _____ _ __
 / _ \ __| '_ \| |/ __/ _` | | '_ \ / _` |/ __| |/ / _ \ '__|
|  __/ |_| | | | | (_| (_| | | | | | (_| | (__|   <  __/ |
 \___|\__|_| |_|_|\___\__,_|_|_| |_|\__,_|\___|_|\_\___|_|
```

```
Blackhats bitching about no whitehats getting owned so here [redacted]. Ethicalhacker.net is one of the big players
in the compsec world. I hack to laugh and have fun but some of these die hard 'blackhats' epitomize their struggle quite
similiar to the struggle between vampires and lykens(wtf? See Underworld). I don't hate them they are pretty amazingly
hilarious though but lets get down to the basics.

uname -a:
Linux infongd3972 2.6.24-20080613a-grsec #1 SMP Wed Jul 16 18:05:29 CEST 2008 i686 GNU/Linux

cat /etc/passwd:
root:x:0:0:root:/root:/bin/bash
man:x:6:12:man:/var/cache/man:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
www-data:x:99:99:www-data:/var/www:/bin/sh
ocuser:x:43:600:oneclick-user:/:/bin/false
sshd:x:100:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:111:101:MySQL:/usr/local/mysql:
dummywwwexecuser:x:1000:600:Dummy WWW User:/nonexistent:/bin/false
nobody:x:655:65534:nobody:/nonexistent:/bin/sh
u45188088:x:1002:600:2127:/kunden/homepages/8/d204887813/htdocs:/bin/bash

cat configuration.php:
```

- Attacker finds a website
- Fingerprints it
- Finds a vulnerable LFI module
- Uploads a shell
- Escalates
- Gets all the data…..
- DEMO

Simple. Powerful. Precise.

Analysis

Goals

- Find webshell
- Identify access pattern
- Determine attacker
- Determine other files touched

- We are using Nuix for analysis.
- These things will work with other products as well
  - FTK has a free version for processing data offline
  - Make a dupe and Linux can parse many of these things natively
- Grep and regexes are your friend.
- Find what makes you comfortable, and get to really know it.
- DEMO

- Regularly run wpscan against wp instances
- Focus on detection
- File Integrity Monitoring
- Web Application Firewalls
- Web App Pen Test
- Create canary and regularly search for it on the Internet

Simple. Powerful. Precise.

Backoff Malware

Backoff Attack Walkthrough

- Starts with phishing
- Attacks an integrator
- Compromises POS system
- Installs malware
- Exfiltrates data
- DEMO

Simple. Powerful. Precise.

Analysis

- Goals
  - Determine If a system is infected
  - Identify IOCs
  - Find files and registry values
  - Determine how services are running

Sample Backoff IOCs

- 1.55 “backoff”
  - Packed MD5: F5B4786C28CCF43E569CB21A6122A97E
  - Unpacked MD5: CA4D58C61D463F35576C58F25916F258
  - Install Path: %APPDATA%\AdobeFlashPlayer\mswinhost.exe
- Mutexes:
  - Undsa8301nskal
  - uyhnJmkuTgD

- Files Written:
  - %APPDATA%\mskrnl
  - %APPDATA%\winserv.exe
  - %APPDATA%\AdobeFlashPlayer\mswinhost.exe
  - %APPDATA%\AdobeFlashPlayer\Local.dat
  - %APPDATA%\AdobeFlashPlayer\Log.txt
- Static String (POST Request): ihasd3jasdhkas

- Registry Keys:
  - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\identifier
  - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Windows NT Service
- User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
- URI(s): /aero2/fly.php

Analysis Walkthrough

- Walk through finding things with Nuix
- Find the malware in a variety of ways
- Determine attack point

- Limit integrator access
- Audit all 3rd party access
- Strong network segregation
- File and Filesystem integrity monitoring

Final Thoughts

- Blue team is an outdated concept, lets fix that
- Red team members need to focus on more than breaking
- Attackers are going to get in, our only hope is mitigation and detection
- Let's keep up the discussion

Simple. Powerful. Precise.

Questions?