How’d That End Up On Pastebin
Ryan Linn
Principal Consultant, Cyber Threat Analysis
• 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
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?

PTIK FKIP Universitas Sebelas Maret Leaked by Nabilaholic404 ...
pastebin.com/6K05snFb
21 Mar 2014 ... 'user_activation_key' varchar(60) NOT NULL DEFAULT ",,'user_status' int(11) NOT NULL DEFAULT '0',, 'display_name' varchar(250) NOT ...

www.jurnaltipikor.com \[censored\] - Pastebin.com
pastebin.com/SZNG2Hlk
22 Mar 2014 ... DEFAULT '0000-00-00 00:00:00', 'user_activation_key' varchar(60) NOT NULL DEFAULT ",,'user_status' int(11) NOT NULL DEFAULT '0',,

include("-_conn_wp.php"); $sql="INSERT INTO ... - Pastebin.com
pastebin.com/ewHq8RRC
Aug 25, 2013 ... FROM `conbraad_wp118` . wp_users ORDER BY ID DESC LIMIT 1"; ... GRAVA DADOS DA TABELA WP_USERMETA. $sql="INSERT INTO ...

[SQL] Justin Bieber Web "users DB" - Pastebin.com
pastebin.com/NXBuhZHS
Jan 17, 2012 ... INSERT INTO `wp_users` VALUES ('75', 'Nexi Liana', '$P$BhikIcJj4c$ZmvbplRXcJxY', 'nexi-liana', 'xiafung_oke@yahoo.com', ... 

Leaked AUSTRALIA DATABASE EDUCATION WORDPRESS USER ...
pastebin.com/FTn5UJrz
Nov 11, 2013 ... INSERT INTO `wp_users` (ID', 'user_login', 'user_pass', ... 'user_url', 'user_registered', 'user_activation_key', 'user_status', 'display_name') ...

1 2 3 4 5
Have a zine published about you?

[@NaziSecurity] Zine on JoeyEssexsOfficial - Pastebin.com
pastebin.com/MCM6YvdN

[@NaziSecurity] Zine on TopWebHosts - Pastebin.com
pastebin.com/DDaVxpFX

HTP Zine #4 - Pastebin.com
pastebin.com/SguVnh8

AnonymousZine - Pastebin.com
pastebin.com/FjChSntx
Mar 27, 2012 ... AnonymousZine ...... There is a script (/root/apacheup.sh) configured to grab robots.txt from the site via wget and if it fails, will stop/kill and start ...
None of us are immune.

Blackhats bitching about no whitehats getting owned so here my take. 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 similar 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
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:
Wordpress Attack

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

- 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
Backoff Attack Walkthrough

- Starts with phishing
- Attacks an integrator
- Compromises POS system
- Installs malware
- Exfiltrates data
- DEMO
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%\mskrm
  – %APPDATA%\winserv.exe
  – %APPDATA%\AdobeFlashPlayer\mswinhost.exe
  – %APPDATA%\AdobeFlashPlayer\Local.dat
  – %APPDATA%\AdobeFlashPlayer\Log.txt

• Static String (POST Request): ihasd3jasdhkas
Backoff IOCs

- 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, let's 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
Questions?