

# Using Nagios as a Security Tool



JARED BIRD  
JAREDBIRD@GMAIL.COM  
TWITTER: @JAREDBIRD



# Introduction



- Who is Jared Bird?

# Reasons to care

- Prevent data theft
- Deter identity theft
- Avoid legal issues
- Protect brand



# Similarities



WORDPRESS



epilora

SONY

RSA

**HACKED**



PBS



MySQL

## MySQL.com Sold for \$3k, Serves Malware

189  
tweets  
TOP ★1K  
retweet

A security firm revealed today that `mysql.com`, the commonly used Web database software, was hacked and booby-trapped with malicious software. The disclosure caught my eye because of the evidence that administrative access to `mysql.com` was available on the underground for just \$3,000.

Web security firm Armorize [stated in its blog](#) that `mysql.com` was poisoned with a script that could be used to inject malicious code into any MySQL database.

## Epsilon Hacked, Major Bank, Retailer Customers' Email Addresses Stolen

### Millions of Names and Email Addresses Gained From Major Email Marketing Firm

## WordPress Servers Hacked At Root Level

Source code exposed, putting passwords for WordPress.com-hosted blogs at risk of being cracked.

By [Mathew J. Schwartz](#) InformationWeek  
April 14, 2011 11:13 AM

On Wednesday, Automattic, which produces the WordPress blogging platform, disclosed that its servers had been hacked.

## Sony Hacked Again, 1 Million Passwords Exposed

Hacker group LulzSec releases 150,000 Sony Pictures passwords, in latest setback for consumer electronics giant

## RSA SecurID authentication tokens hacked

Published: June 7, 2011 at 1:57 PM

BEDFORD, Mass., June 7 (UPI) -- Computer hackers recently broke into RSA's SecurID two-factor authentication tokens.

RSA, which is based on the mathematical theory of prime numbers, has acknowledged that the intrusion in the system's security, CNET Web site reported Tuesday.

The intrusion is part of a series of hacking attacks against the networks of major U.S. military contractors, including Lockheed Martin, Raytheon and Northrop Grumman.

## NASA Computer Hacked, Satellite Data Accessed

May 17, 2011 | 6:40 PM ET | By Matt Liebowitz, SecurityNewsDaily Staff Writer



# “It wont happen to us”

- It can happen to anyone (even security vendors)



The screenshot shows the Core Security Technologies website. At the top left is the logo for Nagios World Conference North America. The main heading reads "It wont happen to us". Below this is a bullet point stating "It can happen to anyone (even security vendors)". The website header includes the Core Security Technologies logo, navigation links (Blog, Contact Us, Customer Portal), a search bar, and social media icons. The main content area features a large banner with the text "Do you know if your critical assets are exposed? We do." and a sub-headline "Welcome to Core Security Technologies". Below the banner are two buttons: "LEARN MORE" and "HEAR FROM OUR CEO". The right sidebar contains a "LATEST NEWS" section with three items: "SEP 15 Core Security to Address Market Leadership and Technology Innovation at Annual East Coast Emerging Growth and Digital Media Conference", "SEP 07 Core Security Names IT Industry Veteran as New Strategic Marketing Leader", and "AUG Core Security Introduces Groundbreaking". At the bottom, there are three tabs: "SECURITY EXECUTIVES", "PROFESSIONAL SECURITY TESTERS", and "SMALL & MEDIUM BUSINESSES".

**Do you know if your critical assets are exposed?**  
**We do.**

Our security test and measurement solutions continuously identify and prove real-world exposures to your most critical assets.

[LEARN MORE](#) [HEAR FROM OUR CEO](#)

**Welcome to Core Security Technologies**

Core Security Technologies offers the first and only real-world approach to security testing and measurement. By replicating actual threats across the enterprise, our solutions reveal where and how attacks can access your most important information.

- Get real visibility. • Get real validation. • Get real metrics.

[GET REAL ABOUT REAL-WORLD THREATS](#)

**LATEST NEWS** [VIEW ALL](#)

- SEP 15** Core Security to Address Market Leadership and Technology Innovation at Annual East Coast Emerging Growth and Digital Media Conference
- SEP 07** Core Security Names IT Industry Veteran as New Strategic Marketing Leader
- AUG** Core Security Introduces Groundbreaking

**ADVISORIES & SECURITY UPDATES**

[FROM OUR BLOG](#) [VIEW ALL](#)

[SECURITY EXECUTIVES](#) [PROFESSIONAL SECURITY TESTERS](#) [SMALL & MEDIUM BUSINESSES](#)



# What to protect



- Data
- Hardware
- Intellectual Property
- Brand



# Threats

- Default configurations
- Website defacement
- Missing patches
- DNS redirection
- Unused services
- Unauthorized use
- Many, many more



# Monitoring



- Automation
- Early detection
- Quick resolution
- Integrity

# Default Configurations

- Default passwords
- blank sa account
  - Once password is set, monitor with new credentials
- XI Auto-discovery check for insecure protocols
- Scheduled scans and output to Nagios

PASSWORD





- Monitor for defacement
  - `check_http -H www.yoursite.com -s "sekret"`
    - ✦ Checks for "sekret" string
- Check certificate
  - `check_http -H www.mysite.com -C 21`
    - ✦ Checks certificate for 21 days of validity
- DDOS alerts

# Software Installed

- Check url for content (version)
- Ex: <http://www.adobe.com/software/flash/about/>
  - Check for string “10.3.183.10”
- Manually update string
- Better way?





# DNS



- Have DNS entries changed?
- DNS hijacked
- High Impact

# Unused Services



- Auto-discovery
- Check for insecure services
- Check for previously disabled services



# Unauthorized Use

- LDAP check for account creation
- Syslog output from infrastructure
- Snort alert (snmp)



# Other Uses?



- Monitor video cameras
  - <http://bit.ly/bY2tjd>
- Ideas?



# Questions?



Jared Bird  
jaredbird@gmail.com  
Twitter: @jaredbird

Thank You