Save Time. Make Money. End Abuse Today.

BART MEKKES
PRODUCT SPECIALIST - PATCHMAN

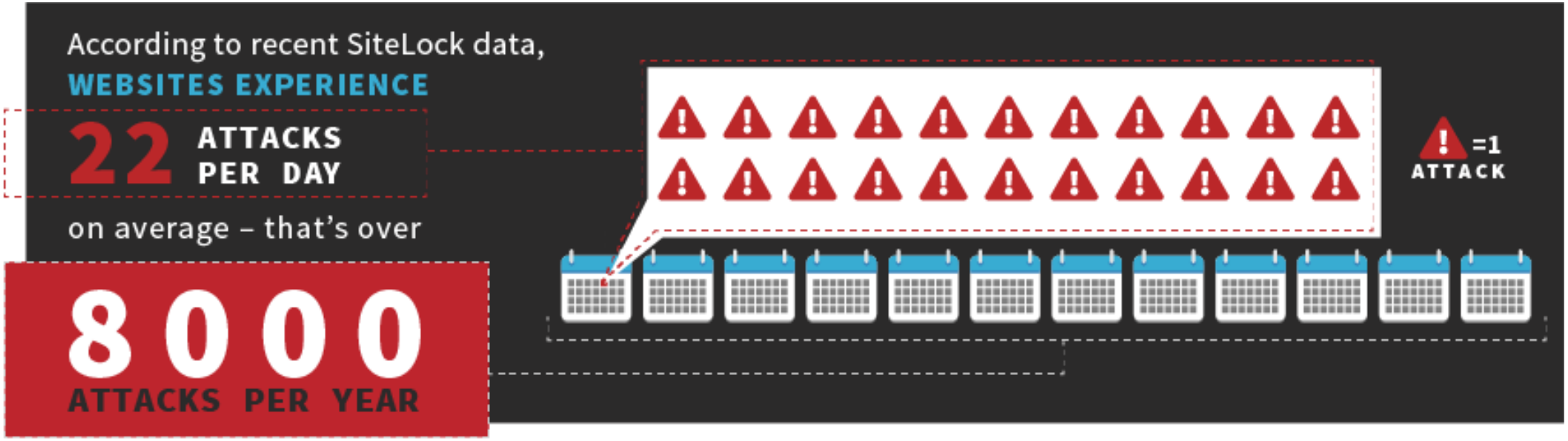
cPanel 2017

Agenda:

- Industry Analysis and Hacking Trends
- Recent Security Breaches
- Proactive Security Approach
- Impact on Customers

Industry Analysis
& HACKING TRENDS

Every Website is at Risk



Every Website Can Provide Resources

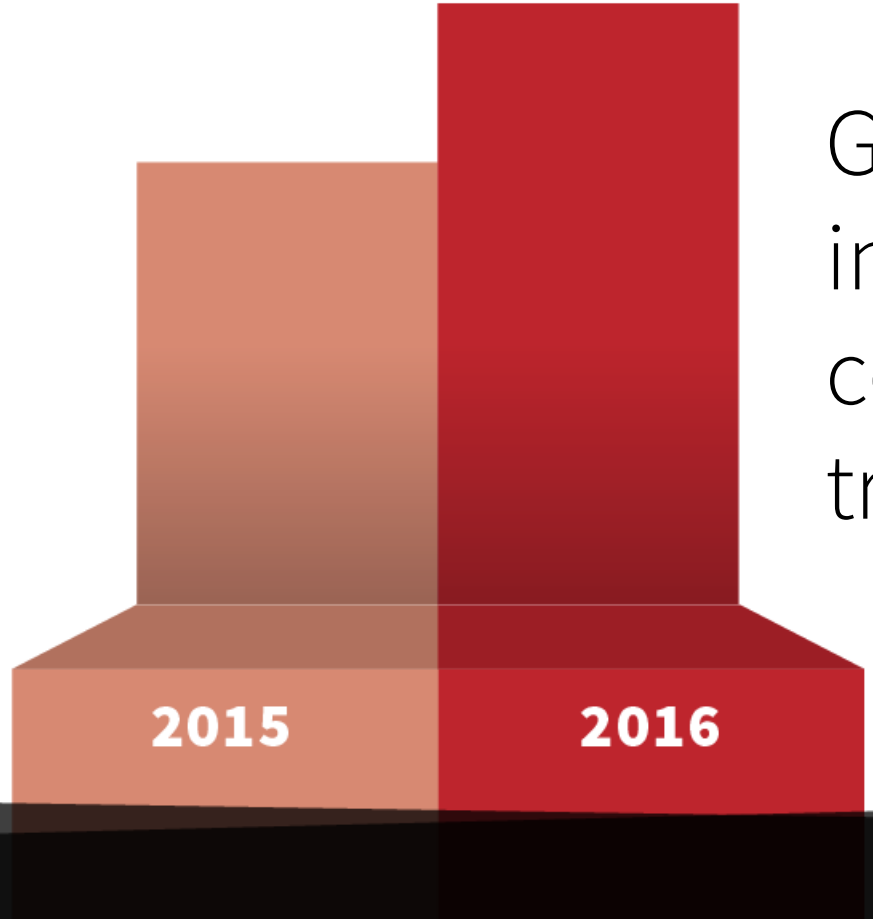
VISITOR DATA

TRAFFIC

BANDWIDTH

EMAIL ADDRESSES

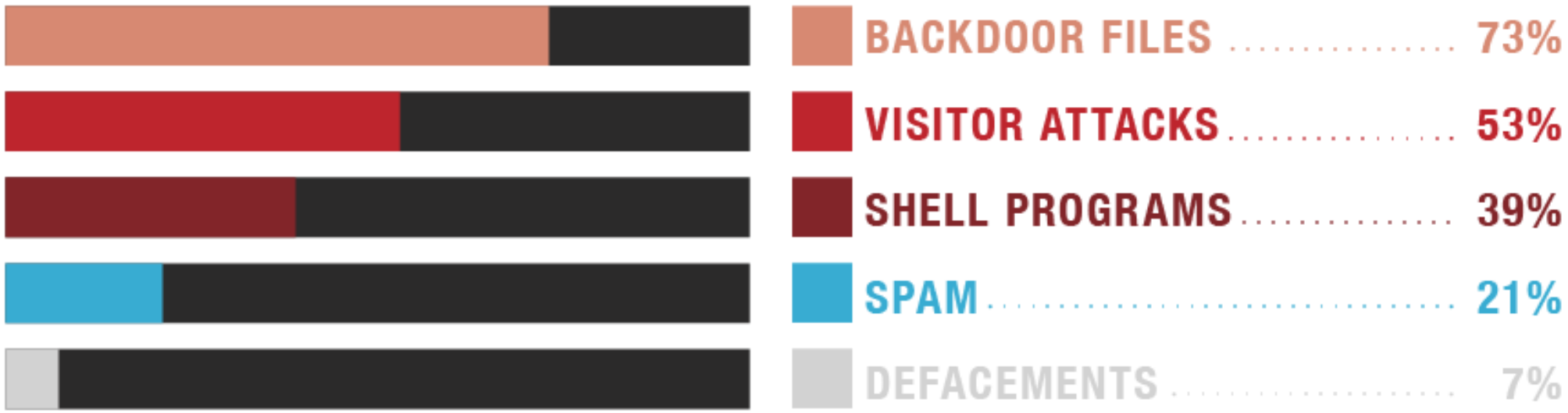
Rates of Abuse Keep Increasing



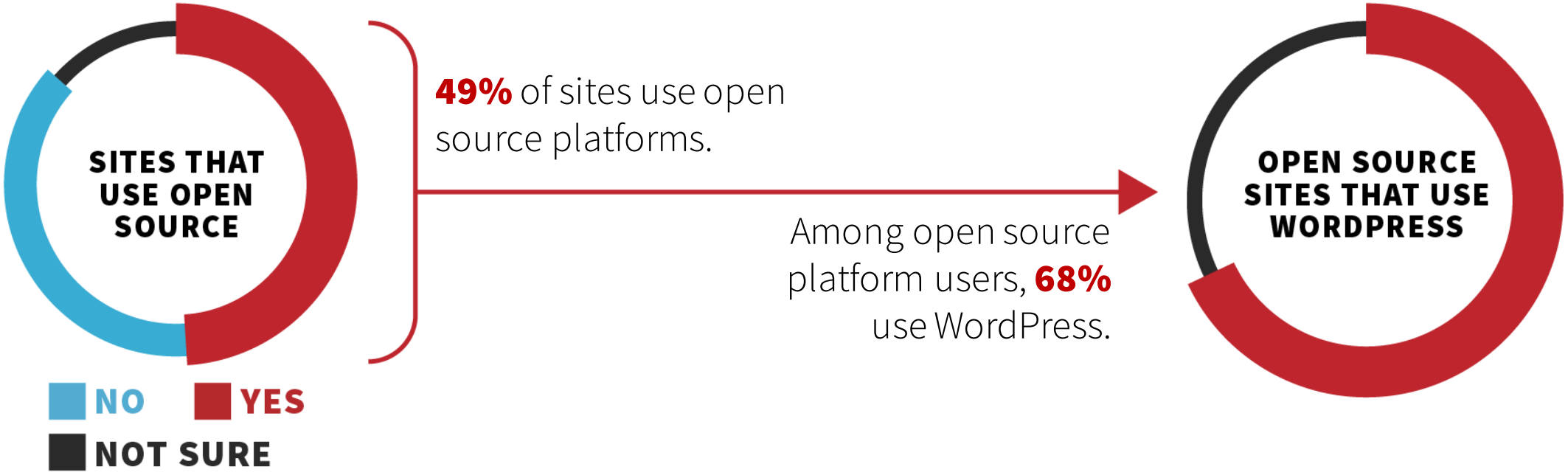
Google reported a 36% increase in hacked sites detected in 2016 compared to 2015, and this trend shows no signs of slowing.

Source: Google Webmaster Central Blog

A Snapshot of Attacks by Type



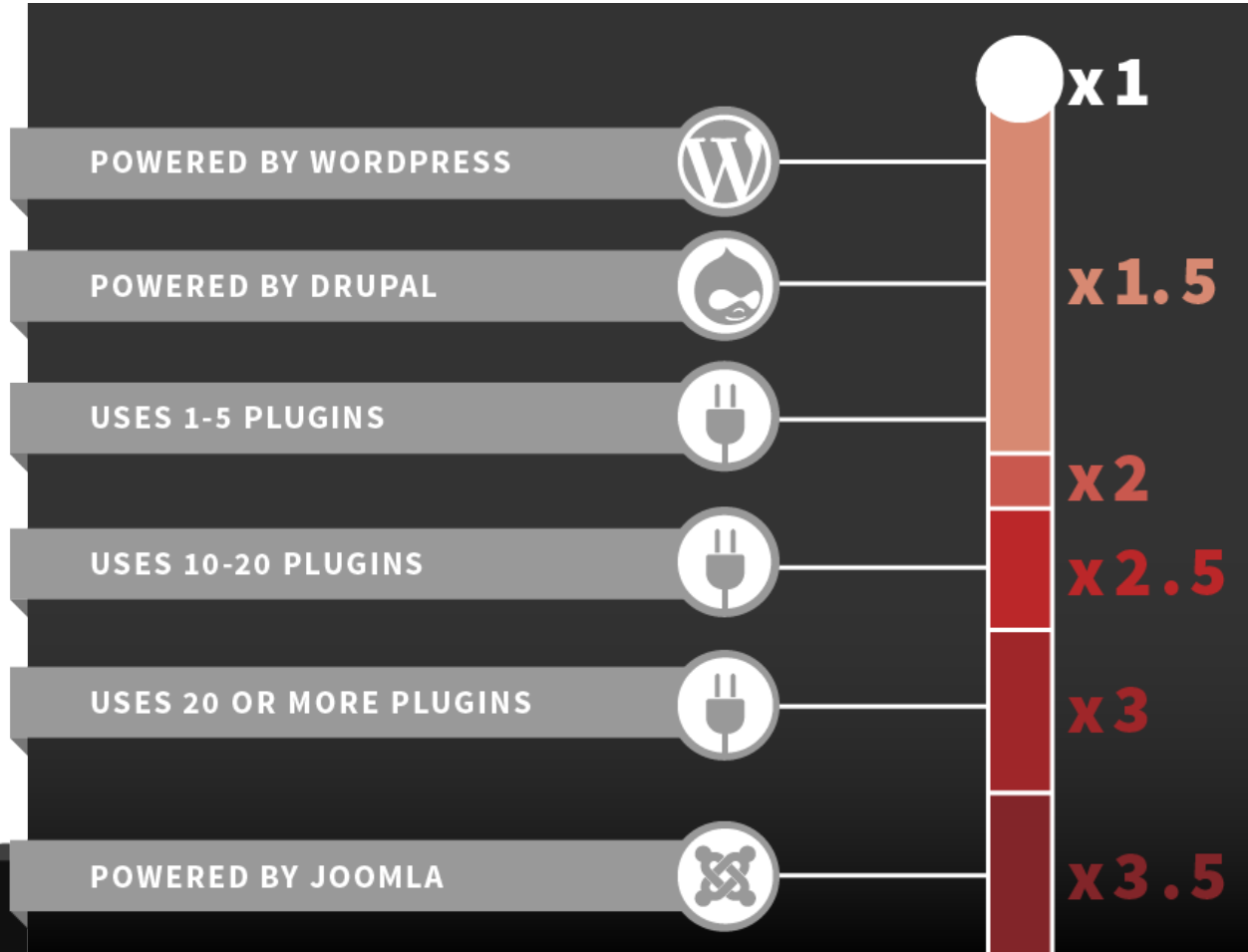
Open-Source Platforms Dominate



Source: SiteLock Survey of Website Owners and Consumers

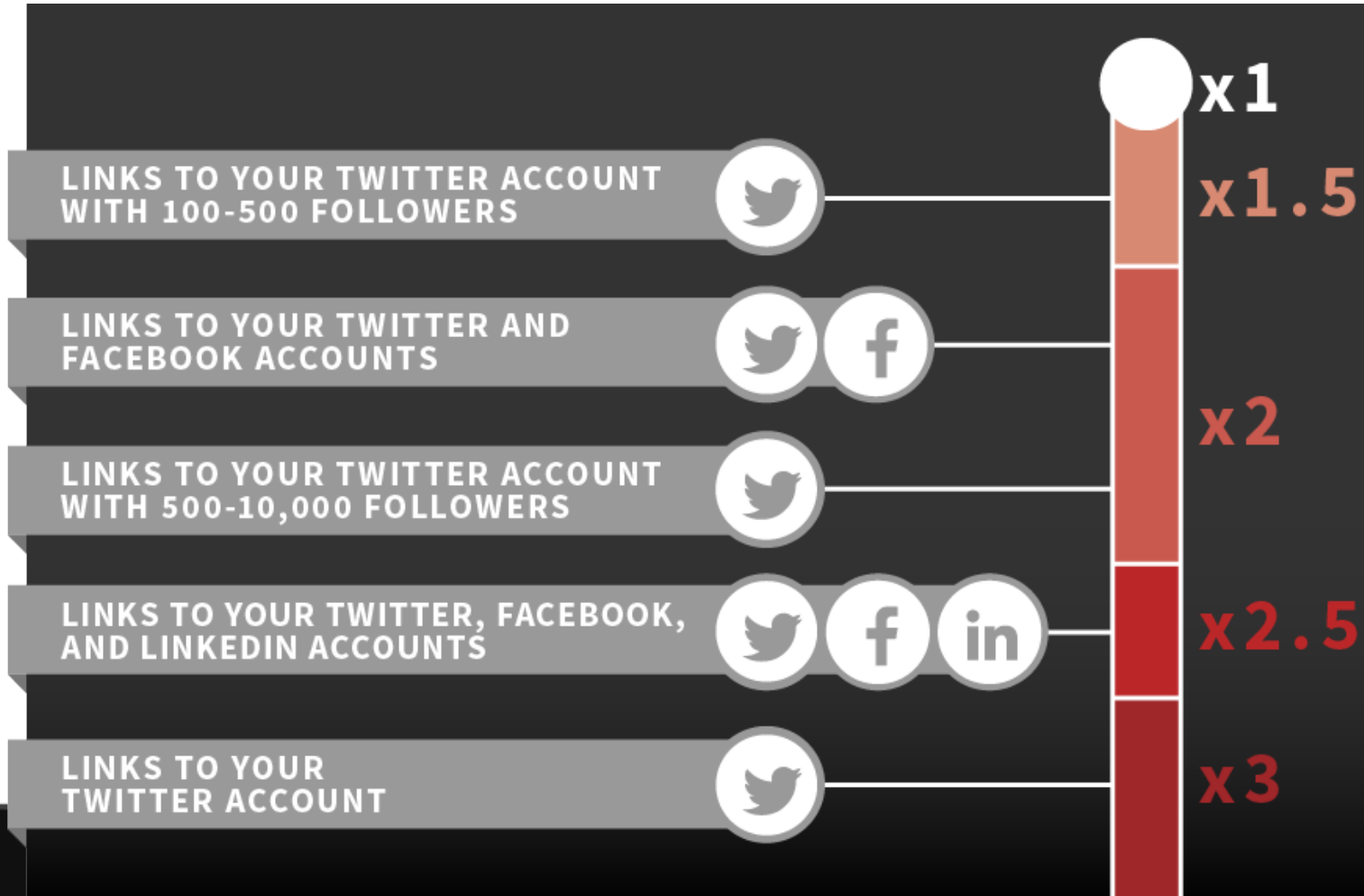
But CMS Sites See Increased Abuse

Some popular website features, like CMS, have been found to correlate to increased risk of website compromise.



Social Media also Relates to Risk

Linking to social media can also increase a site's risk of being compromised



Costs of a Data Breach

44% of SMBs have been the victim of a successful attack

$8,700 total cost per attack on average

Source: National Small Business Association *Small Business Technology Survey*

Costs of a Data Breach

2/3 of consumers do not return to shop at a store from which their personal data was stolen or compromised.

Source: SiteLock Survey of Website Owners and Consumers

Ignoring These Facts May Cost You

BREACHES ARE EXPENSIVE

1-5% of your sites are compromised per month, stealing your resources and consuming your time.

ONE IN TWO ARE VULNERABLE

57% of hosted sites run on CMS, 80% of which are out of date. That means 46% of your sites are vulnerable to abuse.

ONE IN THREE CUSTOMERS CHURNS

According to StopBadware and Commtouch, 28% consider moving to a new provider after their site is compromised.

Recent Security

EXPLOITS

WooCommerce XSS Vulnerability

A reflected cross-site scripting vulnerability in the “Product Vendors” plugin for WordPress compromised sensitive user session data.

- **IMPACTED VERSIONS 2.0.35 AND OLDER**
- **EACH ATTACK IS COMPLETED IN DURATION OF A SINGLE SESSION**
- **TRANSMITS PRIVATE DATA FROM THE SESSION TO THE ATTACKER**
- **CURRENT PLUGIN VERSION REMEDIATES THE VULNERABILITY**

Trend Miami: Malicious Redirects

A legitimate database administration utility led to the infection of websites with injector scripts that often redirect to malicious sites.

- **UTILITY NOT SECURED THROUGH ANY AUTHENTICATION AND LAX PUBLIC FILE PERMISSIONS**
- **SEARCH ENGINE DORKING METHODS BEING USED TO FIND WEBSITES USING THE UTILITY**
- **REDIRECTS INCLUDE FAKE MICROSOFT TECH SUPPORT AND DEFRAUDING AD NETWORKS**

Trend Tusayan: Shell Injection

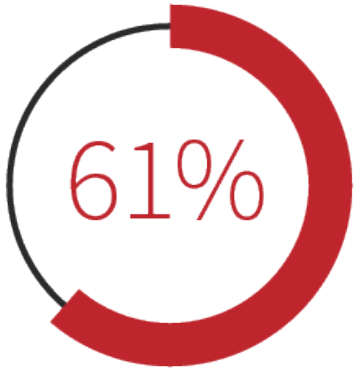
Taking advantage of out-of-date CMS platforms, this exploit injects an IDX shell which, in turn, provides the attacker with admin access.

- **EXPOSES SENSITIVE WEBSITE CREDENTIALS PUBLICLY OVER THE INTERNET**
- **IMPACTS OLDER VERSIONS OF WORDPRESS, JOOMLA! AND MAGENTO**
- **CAN BE DETECTED FOR REMOVAL VIA WEBSITE SCAN**
- **CAN BE PREVENTED BY UPDATING CMS**

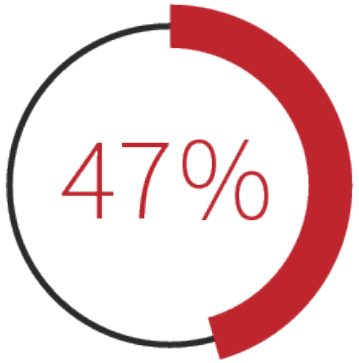
PROACTIVE

Security Approach

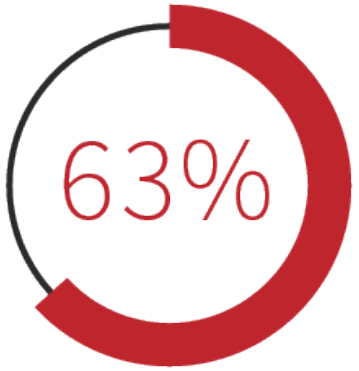
Customer Security Snapshot



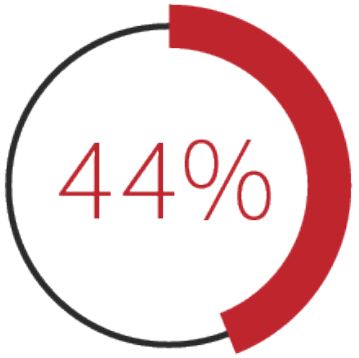
LACK ANY WEBSITE SECURITY



OF THOSE WITH WEB SECURITY DON'T KNOW WHAT TYPE



HAVE NO BREACH RESPONSE PLAN



BELIEVE THEIR HOST IS RESPONSIBLE FOR WEBSITE SECURITY

Source: SiteLock Survey of Website Owners and Consumers

This Impacts Hosting Companies

Hackers generally want to take advantage of your server's resources for spam runs, DDoS attacks, etc. However, it also exposes you to much more severe risks: root exploits, data loss, data theft, or worse.

Each month at least 1% of your customers get hacked, and it takes your team 90 minutes to resolve the issue, clean up the mess and assist affected customers, meaning increased operational costs.

Webmasters blame the provider for the compromise, are unhappy with the (lack of) support they receive, are not able to resolve the issue themselves or are simply fed up with it and quit.

Make Security Collaborative

BOOST HAPPINESS FOR EVERYONE WITH INTERNAL SECURITY MEASURES

Implement internal security tools to free up your employees from dealing with angry customers by making sure your customers don't get angry in the first place.

Prevent issues before they happen using application security testing in development and vulnerability scanning at the server level.

Make Security Collaborative

EMPOWER CUSTOMERS WITH WEBSITE-LEVEL SECURITY TOOLS

Website scanners and malware removal tools can help empower customers to resolve security breaches on their own when they strike.

Better yet, offering customers access to a preventative security strategy with a web application firewall and the ability to fine-tune its settings.

Impact on **CUSTOMERS**

Flip the Script

Communicate with customers in order to foster increased awareness and knowledge of website security issues.

Build your relationship with your customers by showing your dedication to keeping their site safe.

Increase value by increasing transparency for your customer and efficiency for your support team.

THANK YOU

Visit sitelock.com/cpanel
for more information

Feedback? Visit:
go.cpanel.net/tuesday