Enabling Malware, Phishing Attacks to be Hosted from Genuine Sites

Versafe helps organizations protect their online users from the spectrum of online threats including malware, MITB, zero-day exploits, phishing attacks, and more. The Versafe Security Operations Center, an experienced team of researchers who work 24x7x365 to provide quick, efficient response to the latest online threats, recently discovered a vulnerability that puts websites hosted on the Joomla content management system at particular risk of being hijacked for use in malware payload and phishing attacks.

White Paper

Executive Summary

Versafe helps organizations protect their online users from the spectrum of online threats including malware, MITB, zero-day exploits, phishing attacks, and more. The Versafe Security Operations Center, an experienced team of researchers who work 24x7x365 to provide quick, efficient response to the latest online threats, recently discovered a vulnerability that puts websites hosted on the Joomla content management system at particular risk of being hijacked for use in malware payload and phishing attacks.

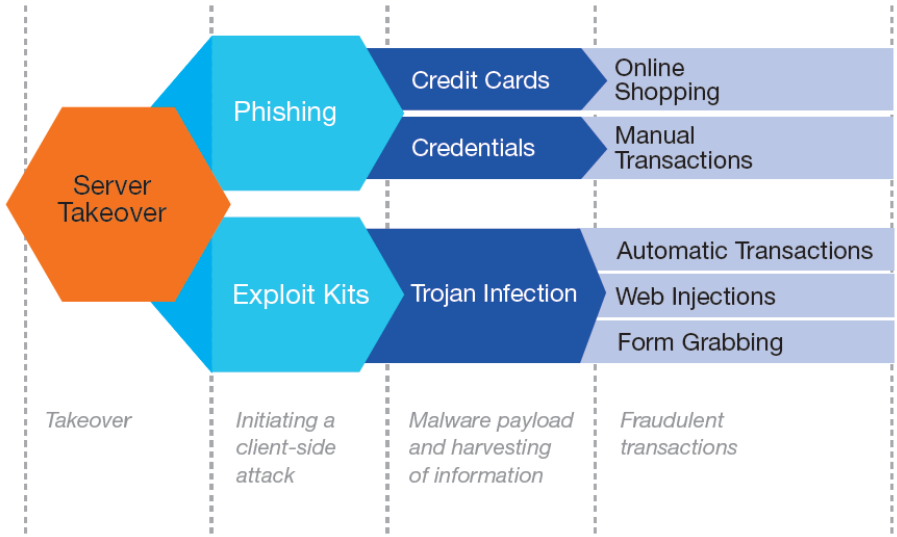
A forensics investigation of the sites involved to-date revealed a zero-day attack that was found in the wild – which enables an attacker to gain full control over the compromised system – causing over 1 million Joomla-based websites to be readily susceptible to takeover. The exploit was detected by Versafe and its TotALL Online Fraud Protection Suite, as deployed via F5 Network's BIG-IP product suite.

This report offers insight into the nature of the exploit, providing a step-by-step description of how attacks were initiated, from vulnerability assessment to server takeover and malware deployment.

Overview of the Attack

Though cybercriminals' motives naturally differ – ranging from new account fraud, to stealing credit card data, to capturing additional user authentication information and more – this Versafe Intelligence Brief focuses on the use case of account takeover.

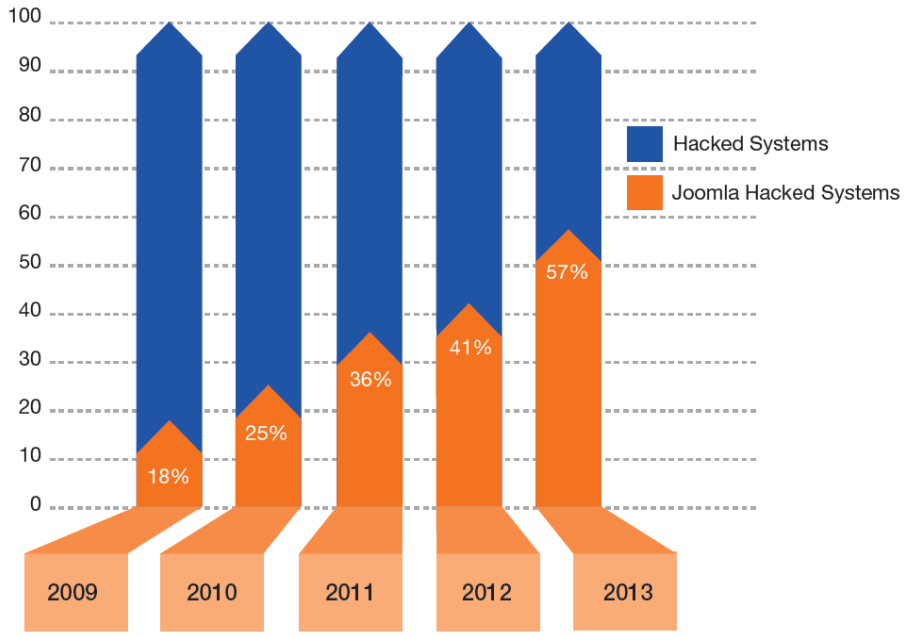
The attacks were comprised of four key stages:



1. **Takeover:** Gaining control of the web server.
2. **Initiating a client-side attack:** Phishing and malware infections via the exploit kit.
3. **Malware payload and harvesting of information:** Malware infection and information harvesting from compromised users, including login credentials, additional authentication information, etc.
4. **Fraudulent transactions:** Cash-out from compromised accounts.

Discovery

While the Versafe Security Operations Center had noticed an increasing percentage of phishing and malware attacks against its clients being hosted from legitimate Joomla-based sites since 2009, the spike in the first-half of 2013 strongly suggested a particular vulnerability in the Joomla platform was being more readily exploited by attackers.



The locations of the attacks spanned four continents, some of which are represented below, with server takeover having occurred at a particularly rapid rate.

Investigation

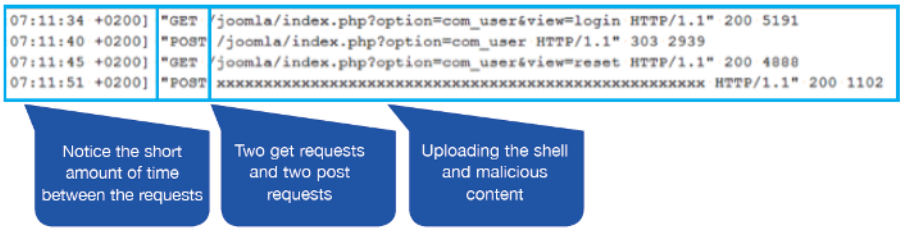
During communication with the hosting providers, Versafe began to investigate the logs from several of the compromised servers.

1. **All attacks originated from the same source.** The attackers' IP addresses

were located in China.

2. **The same exploit was used against all systems.** The attackers' shell was found on the same relative path on each of the compromised servers.
3. **Takeover shell and malicious content upload was automated.** Given the compressed timeframe of the attack, Versafe surmised the attackers were using a new zero-day exploit.

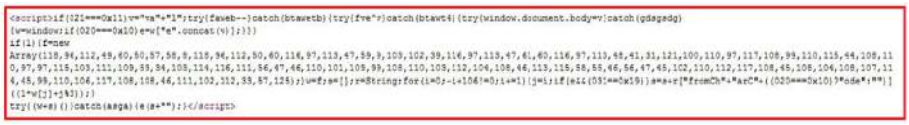
The logs showed the following steps in each takeover:



Several of the compromised servers redirected users to a Blackhole landing page, thereby infecting them with a Zbot variant. A snapshot of the discovered Blackhole code follows:

"Blackhole": An Overview

The most popular drive-by malware investigated of late is "Blackhole". It is marketed and sold to cybercriminals as a professional malware kit, providing web administration capabilities and sophisticated techniques to generate malicious code. Blackhole is particularly insidious by means of its aggressive use of server-side polymorphism and heavily-obfuscated scripts to evade detection from endpoint software.



About Versafe

Versafe enables organizations to proactively ensure the integrity of each online customer relationship, protecting against the spectrum of malware and online threat types, across all devices, while being fully transparent to the end-user. Clients have actualized a significant decrease in the number and impact of malware, phishing, and other online attacks – enabling step-change reduction in both fraud losses, as well as an increase in fraud management efficiencies – routinely yielding investment payback in just weeks. With over 30 customers internationally, and a partner network including F5, CA, Check Point, and others, Versafe is backed by Susquehanna Growth Equity.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com