1.1 / OVERVIEW / Following a series of vulnerability disclosures throughout 2014, the popular content management framework Joomla has been actively targeted for exploitation by malicious actors. These exploitation campaigns usually pursue the compromise and entrenchment of large numbers of servers, or Software-as-a-Service (SaaS) providers, that can then be used to distribute malware and phishing campaigns or can be used to serve as zombies in distributed denial of service (DDoS) botnets. In 2014, PLXsert published a white paper on how vulnerable web frameworks are used for botnet building.

In a recent joint investigation with the PhishLabs R.A.I.D (Research, Analysis and Intelligence Division), PLXsert observed traffic signatures from Joomla distributions used in DDoS attacks. The attack campaigns contain traffic signatures that match sites known for providing DDoS-for-hire services. The traffic appears to match attacks staged using tools developed specifically to abuse XML and Open Redirect functions, which then produce a reflected response that can be directed to targeted victims and result in denial of service. These tools are rapidly gaining popularity and are being adapted by the DDoS-for-hire market.

Observed attack traffic and data suggest vulnerable hosts are being added to the menu of attacks on known DDoS-for-hire sites. The new attack type uses compromised Joomla servers as zombies or proxies to stage denial of service GET floods.

1.2 / INDICATORS / With cooperation from the PhishLabs R.A.I.D, PLXsert matched signature traffic originating from multiple Joomla sites. It varies slightly depending on the reflector used, due to configuration details.

In February 2014, multiple vulnerabilities were discovered in the Google Maps plugin for Joomla. One of the vulnerabilities allows the plugin to act as a proxy. Vulnerable installations are being used en masse for reflected floods using tools such as DAVOSET and UFONet.

1.2A / DAVOSET ATTACK TOOL / A publicly available tool called DAVOSET (DDoS attacks via other sites execution tool), was built to take advantage of these types of attacks and automates the process. For attackers, the most difficult task is building and maintaining a valid list of vulnerable reflectors. However DAVOSET ships with a default list of servers that leverage the vulnerability of the Google Maps plugin.

DAVOSET takes a list of known blind proxy scripts and services and uses them to stage a reflected GET flood against a target. DAVOSET allows an attacker to configure their lists
of reflectors, the number of requests per reflector, and proxy configurations to automate these attacks. Figure 1 shows DAVOSET being used to stage an attack against a target using Joomla reflectors.

```
# ./davoset.pl l=list_test.txt u=http://domain.com

DDoS attacks via other sites execution tool
DAVOSET v.1.2.3
Copyright (C) MustLive 2010-2014

Site http://domain.com is attacking by ZZ zombie-servers...
1
...
ZZ

Attack has been conducted.
Time: 1:54:47.
Requests: ZZ, Bytes: 10913.
Speed: 0.14496 req/s, 26.81327 B/s.
```

Figure 1: DAVOSET in use to stage an attack against a target using multiple Joomla reflectors

Malicious actors also find reflectors by dorking (advanced search techniques) or scanning. PLXsert was able to identify more than 150,000 potential reflectors, although many appear to have been patched or updated, locked down via PHP or server configuration hardening, or had removed the plugin.

**1.2²/UFONET ATTACK TOOL** / More recently, another tool available on the Internet called UFONet has received attention. As with DAVOSET, it uses a web interface and a point-and-click configuration process. These user-friendly features provide attackers with an easy-to-use interface for proxy (e.g. Tor) configuration, customizable headers, attack options and more. Figure 2 illustrates how an attack works with a proxy, and Figure 3 shows the tool’s interface.
Figure 3: The UFONet web interface allows users to quickly configure and launch DDoS attacks.

The next figure provides sample output for the command-line version of UFONet. This was tested within PLXsert’s lab environment.
UFONet also automates the process to find and test vulnerable reflectors, and supports community-based list sharing and updating, which will likely serve to escalate the popularity and scale of these attacks over time.

At the time of this advisory, UFONet had a very small set of community reflectors and its search and reflector testing logic contained bugs. This made finding vulnerable Joomla instances more difficult. It was, however, functional in administering the attack with minor modifications when given a list of reflectors acquired externally.

1.3 / MALICIOUS PAYLOADS / PLXsert identified three distinct signatures produced by the DAVOSET and UFONet tools. They differ in the type of HTTP GET request header (1.0, 1.1) and the presence of the PHP language version in the User-Agent field. An extra line
break after the last header in each packet is part of the observed request. These signature
details are shown in Figure 5.

**Figure 5:** Three attack payload traffic samples show GET Flood requests used during DDoS attacks

The HTTP headers vary due to the server configuration and versions of the plugin. Some
requests are issued using curl_exec() via PHP, and others are file_get_contents() calls.

One variation is the use of HTTP/1.0 for requests. HTTP/1.1 has been the more popular
standard since its introduction in 1999. Newer browsers since Internet Explorer 6.0 have
standardized on HTTP/1.1, as have tools such as curl and wget.

Another trait in these signatures is the lack of a User-Agent HTTP header in a majority of
the requests. However some boxes that use the PHP curl request include a User-Agent
string that contains the PHP version used by the curl_exec() request.

**1.4 / Observation Campaign /** The signatures of this attack have been observed since
September 2014. So far in 2015, eight attacks against Akamai customers have contained the
Joomla! attack signatures. Figure 6 contains a sample of the signatures observed during
active attack campaigns.
As seen in Figure 7, malicious actors usually launch these attacks in combination with other attack vectors. In fact, only one attack launched on January 14, 2015 consisted of the Joomla! GET flood alone. Application attacks like this aren’t known to generate significant bandwidth – the goal of the attack is to generate realistic user connections on the target server to cause a denial of service.

Figure 7: Dates, peak bandwidth and total vectors per attack

1.4A / Attack Distribution / The majority of the top attacking IP addresses that participated on this DDoS attack originated from Germany as shown in Figure 8.
The attacks were mostly focused in the Education vertical. Figure 9 provides a breakdown of the remaining attack target verticals.

1.5 / DDoS Mitigation / PLXsert has identified the following three DDoS mitigation procedures that can help mitigate this attack vector. These recommendations are by no means exhaustive and should not be taken as a sole means of DDoS protection.

- Block HTTP GET /1.0 request traffic if support for legacy clients is not needed.
- Block HTTP requests with a PHP-based User-Agent string if they are not needed.
- Use the three Snort rules provided in Figure 10. The signature can be adapted to other mitigation techniques in order to detect or block these DDoS attacks.
Figure 10: Three Snort rules to match the three attack variations

```plaintext
alert TCP $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS 
(msg: "Joomla GET flood"; 
flow: to_server; 
content: $User-Agent:":; dsize:<128; 
content: "GET / HTTP/1.1"; depth:14; 
content: "Host": ""; distance:2; within:6; 
content: "Accept": "/*"; distance:2; within:56; 
content: "Content-type": text/xml"; distance:2; within:22; 
content: "Content-length": 0"; distance:2; within:17; 
content: "|0d0a 0d0a|"; distance:0; within:4; 
classtype: GET-Flood; 
rev:1;)

alert TCP $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS 
(msg: "Joomla GET flood PHP UA"; 
flow: to_server; 
content: "GET / HTTP/1.1": depth:14; dsize:<109; 
content: "User-Agent": PHP/5."; distance:2; within:18; 
content: "Host": ""; distance:5; within:7; 
content: "Accept": "/*"; distance:2; within:56; 
content: "|0d0a 0d0a|"; distance:0; within:4; 
classtype: GET-Flood; 
rev:1;)

alert TCP $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS 
(msg: "Joomla GET flood missing headers"; 
flow: to_server; 
content: $User-Agent:"; dsize:<72; 
content: "GET / HTTP/1.0"; depth:14; 
content: "Host": ""; distance:2; within:6; 
content: "|0d0a 0d0a|"; distance:0; within:45; 
classtype: GET-Flood; 
rev:1;)
```
The Prolexic Security Engineering and Research Team (PLXsert) monitors malicious cyber threats globally and analyzes these attacks using proprietary techniques and equipment. Through research, digital forensics and post-event analysis, PLXsert is able to build a global view of security threats, vulnerabilities and trends, which is shared with customers and the security community. By identifying the sources and associated attributes of individual attacks, along with best practices to identify and mitigate security threats and vulnerabilities, PLXsert helps organizations make more informed, proactive decisions.

Akamai® is a leading provider of cloud services for delivering, optimizing and securing online content and business applications. At the core of the company’s solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 40 offices around the world. Our services and renowned customer care enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.

©2015 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice. Published 02/25.