Technical Series

A Prolexic White Paper

Web vulnerabilities: The foundation of the most sophisticated DDoS campaigns

PROLEXIC

Now part of Akamai

As cybercriminals constantly pursue new ways to achieve their ends, defenders keep thwarting them by hardening workstations and shutting down unnecessary services and protocols on servers. These defensive actions have driven malicious actors to find new vulnerabilities, including those that are exposed on the Internet in web services and web application frameworks.

The open source community develops web services and web applications for many distinct purposes including content management, accounting, marketing, blogging and web server administration. This community provides plenty of applications that malicious actors can probe for vulnerabilities and then exploit. It is nearly impossible to develop web services and applications without any vulnerabilities.

In computer security, a vulnerability is defined as: *a weakness [that] allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw*.[1]

Content Management Systems (CMS) and web server management applications are popular, and consequently are among the applications most often targeted by malicious actors seeking web vulnerabilities. Popular open source CMS applications include WordPress, Joomla, Drupal, DotNetNuke, cPanel, Kloxo and others. Most of these are based on the Linux, Apache, MySQL, PHP (LAMP) stack – the most popular web server configuration on the Internet. Popularity creates a commonality and economy of scale for criminal developers.

Further advances in virtualization and cloud services technology have resulted in a proliferation of Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) vendors, as well as cloud hosting providers. These services also provide a commonality and economy of scale for malicious actors. As a result, web vulnerabilities are actively researched and are prime targets for exploitation by malicious actors when they build a botnet for DDoS attacks.

By exploiting and embedding malware and crimeware on sites hosting web applications, DDoS attackers take advantage of site reputation and defense technology, because these reputable sites are less likely to be blacklisted or blocked by automated DDoS mitigation technologies. Also, unless the attacked environments use deep-packet inspection technology, the malicious inbound and outbound network traffic on commonly used ports, such as ports 80 or 443, is likely to pass through without detection.

In recent years, malicious actors have launched effective distributed denial of service (DDoS) attack campaigns with botnets built almost entirely through the exploitation of web vulnerabilities. The most notorious and most studied attack campaign of this type is Operation Ababil, which was based on the Brobot DDoS kit *itsoknoproblembro*. These attack campaigns continued for more than two years, until they appeared to wane in the third quarter of 2013. However, third-party intelligence as well as recent PLXsert observations of recent DDoS attack campaigns suggest the Brobot botnet is still in place, is expanding and is still being used, though not as consistently and focused as it had been used during Operation Ababil.

1 "Vulnerability (computing)." Wikipedia. Wikimedia Foundation

In this white paper, PLXsert will delve into specific examples of the exploitation of popular web content management systems and web management suites and how these compromises have led to the development of some of the most advanced and difficult-to-mitigate DDoS campaigns. In particular, we will discuss PHP Remote File Inclusion (CAPEC-193), Local Privilege Escalation (CAPEC-232) and Symlink Attack (CAPEC-132). These campaigns, while not exhaustive, provide insight into how these attacks are executed. At the end of this white paper, there are links that provide detailed procedures to remediate and protect against these attacks.

Frequently seen botnet-building methods

Akamai's Prolexic Security and Engineering Research Team (PLXsert) has observed and measured web-based botnet-originated DDoS campaigns, identifying the following commonalities in the process of botnet buildup, organization, orchestration and execution:

- Targeting of popular, commonly used web administration, content management and web server frameworks
- Targeting of Internet service providers (ISPs), and Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) infrastructures where these vulnerabilities can be exploited in large numbers
- Using mainly publicly available exploits against targeted frameworks and web providers
- Uploading attacking scripts and binaries to compromised hosts followed by obfuscation
- High-levels of sophistication indicating coordination in organized groups with the backing of resources not available in the common criminal underground. In some cases the attack signatures suggest the attackers' knowledge of DDoS mitigation technology
- Orchestration of campaigns from multiple geographically distributed command and control (CC, C2) hosts, with a preference for locations slow or unlikely to take security enforcement action

Mitre Corporation developed a Common Vulnerabilities and Exposures (CVE)[2] nomenclature for the security community that provides a mechanism for communicating and publicly sharing vulnerabilities. These vulnerabilities are usually published after a number of significant compromises or by discovery by system owners. Information security researchers drive the discovery and publishing of these vulnerabilities on their own or at their place of work. Mitre Corporation has also developed a framework to identify attack patterns. Named Common Attack Pattern Enumeration and Classification (CAPEC)[3], this framework seeks to identify patterns in the way vulnerabilities are exploited.

When attackers seek to build a botnet, they look for web vulnerabilities that will replicate in the greatest number of hosts possible to speed the buildup of botnet bandwidth and diversify the distribution of attack sources. The LAMP stack, the most popular server distribution on the Internet, along with the WordPress and Joomla content management systems, are prime targets. The popularity of these CMS applications has also driven the development of plugins – tools aimed at improving the efficiency, automation and ease-of-use of many functions of the CMS that would otherwise take many manual steps to achieve.

2 "Common Vulnerabilities and Exposures." (CVE). Mitre Corporation
3 "Common Attack Pattern Enumeration and Classification." CAPEC. Mitre Corporation

Attackers looking to build a botnet will conduct a massive scan on the Internet, looking for LAMP servers with configurations, applications and plugins that are known to be vulnerable to exploitation. A visualization using the LM Kill Chain threat model of the botnet development process from the attacker's perspective is shown in Figure 1. The critical phase occurs when the attacker is able to establish command-and-control on compromised hosts and can subsequently execute campaigns.

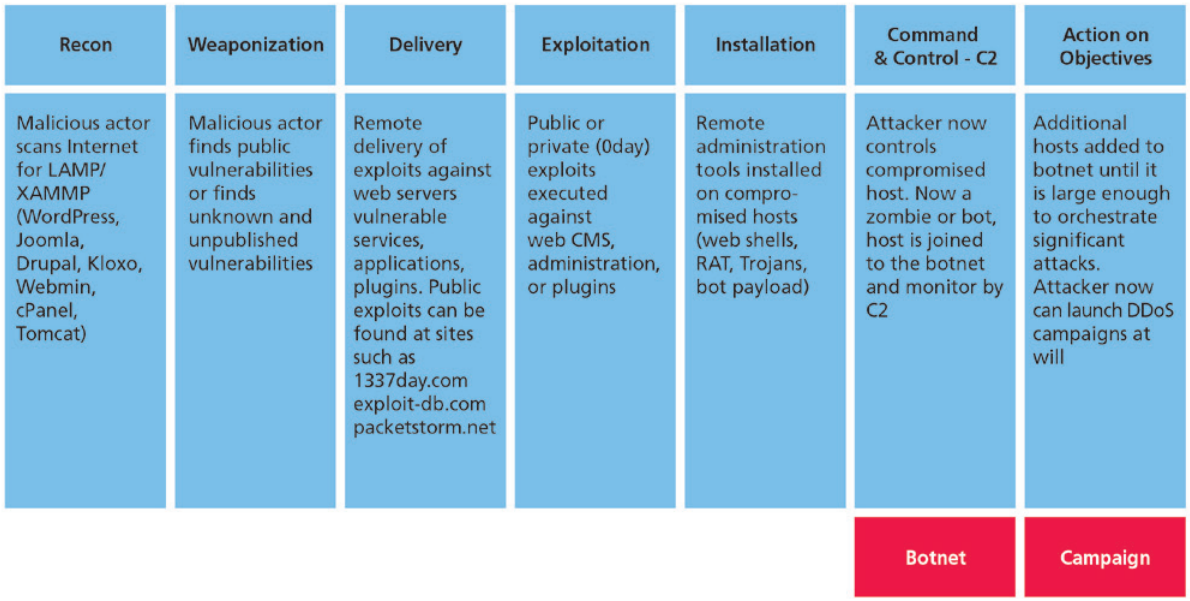

Figure 1: Botnet buildup attack phases, a visualization[4]

Vulnerabilities present in some plugins

Plugins extend the functionality of a content management system, such as to allow a user to post a calendar of events, display a registration form, or upload and display a picture gallery. The capabilities of plugins are intrinsic to such functions of the CMS application and are of great benefit to website developers. At the same time, however, plugins expand the attack surface of an application; a vulnerability or misconfiguration may lead to the compromise of the application.

Vulnerabilities in plugins range from unsafe permissions to the failure of input sanitizing and opportunities for code injection, SQL injection and remote code execution. As a result, plugins are actively researched and exploited by malicious actors, because they are frequently present and may be the quickest way to compromise the CMS application.

Malicious actors will scan the Internet for specific web frameworks with known vulnerabilities or may develop exploits specifically targeting popular web application frameworks, thus creating the greatest opportunity to add compromised hosts, bandwidth and geographical distribution to the planned botnet.

4 "Cyber Kill Chain®." Lockheed Martin.

How malicious actors identify vulnerable hosts

Security researchers publicize vulnerabilities to aid in community cleanup, but even after public advisories are released, very large numbers of systems remain unpatched, offering malicious actors an easy path. Some of the biggest campaigns observed have been launched from botnets built upon publicly known vulnerabilities.

Malicious actors develop their own scanning tools or use publicly available tools, such as wpsnitch (Figure 2) to identify vulnerable systems. By reporting the WordPress version, wpsnitch provides insight that a malicious actor may then use to search for web vulnerabilities on sites such as 1337day.com and packetstormsecurity.com. Other tools, such as Golismero (or GoLismero) web penetration testing tool (Figure 3) are used for fingerprinting the system to pinpoint the exact location of specific files often targeted for exploitation. BlindElephant (Figure 4) detects several types of content management systems such as WordPress, Joomla and Drupal. Once the targets have been identified, tools such as WPScan (Figure 5) are used to discover the presence of vulnerabilities on targets.

Figure 2: Wpsnitch tool is used by malicious actors to identify WordPress sites and version

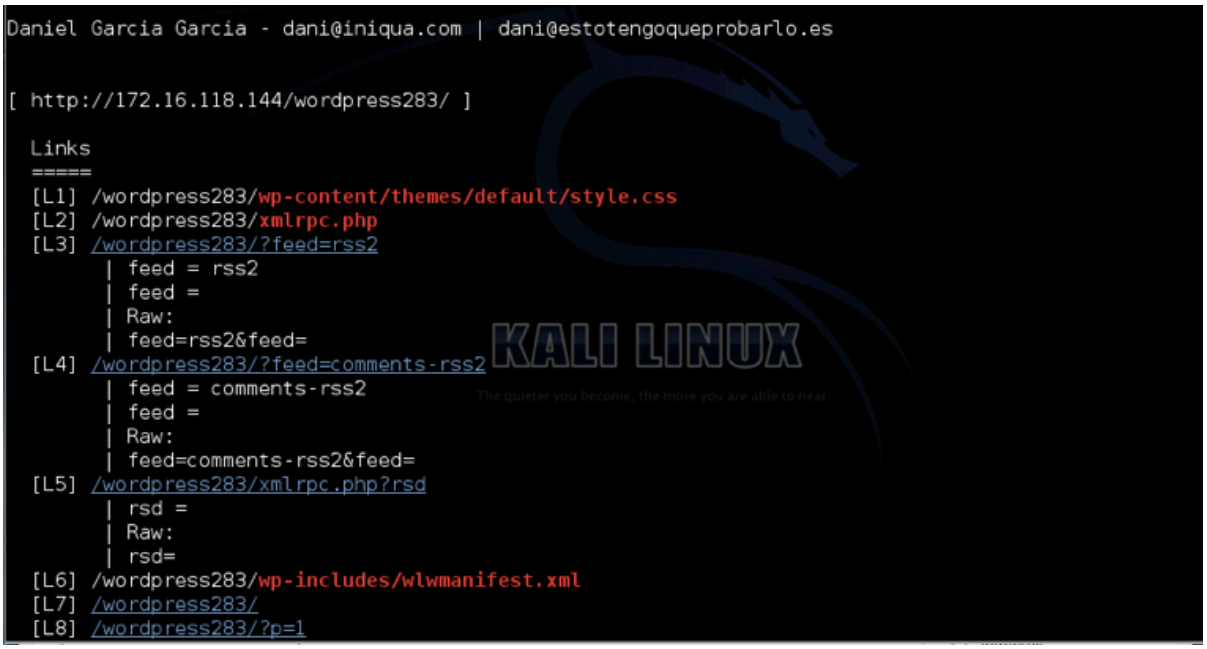

Figure 3: Golismero tool is used to fingerprint a WordPress installation, identifying files that can be targeted for attack

Figure 4: BlindElephant tool is used to fingerprint Joomla installations

Figure 5: WPScan shows vulnerabilities in WordPress and plugins found in a lab target

The availability of ready-to-use tools makes discovering vulnerabilities rather easy. What's more, in some instances, botnet building is not even a necessary next step. For example, the WordPress XML-RPC pingback DDoS attack described in the Q1 2014 Global DDoS Attack Report requires only the identification of a vulnerable host, crafting a request and directing it to a target.

Web administration panels targeted

Exploits that targeted the Kloxo web administration panel (Figure 6) were the source of recent, sophisticated layer 7 DDoS campaigns that matched the Brobot DDoS toolkit signature used during Operation Ababil against U.S. financial institutions in 2011-2013. Malicious actors likely used repositories of publicly known vulnerabilities and exploits, identified a large number of vulnerable Kloxo web hosts and then proceeded to control them to launch significant DDoS campaigns. The Kloxo web administration panel is in a category of web application that allows users to administer multiple hosts in a master configuration, a feature that malicious actors may have used to exploit other hosts managed by the same administrator after compromising a master Kloxo install.

After gaining access to the hosts, malicious actors proceed to exploit the hosts, escalate privileges and establish persistence. Once persistence has been established, malicious actors entrench by uploading malicious code with capabilities such as call-home, remote management and DDoS payloads.

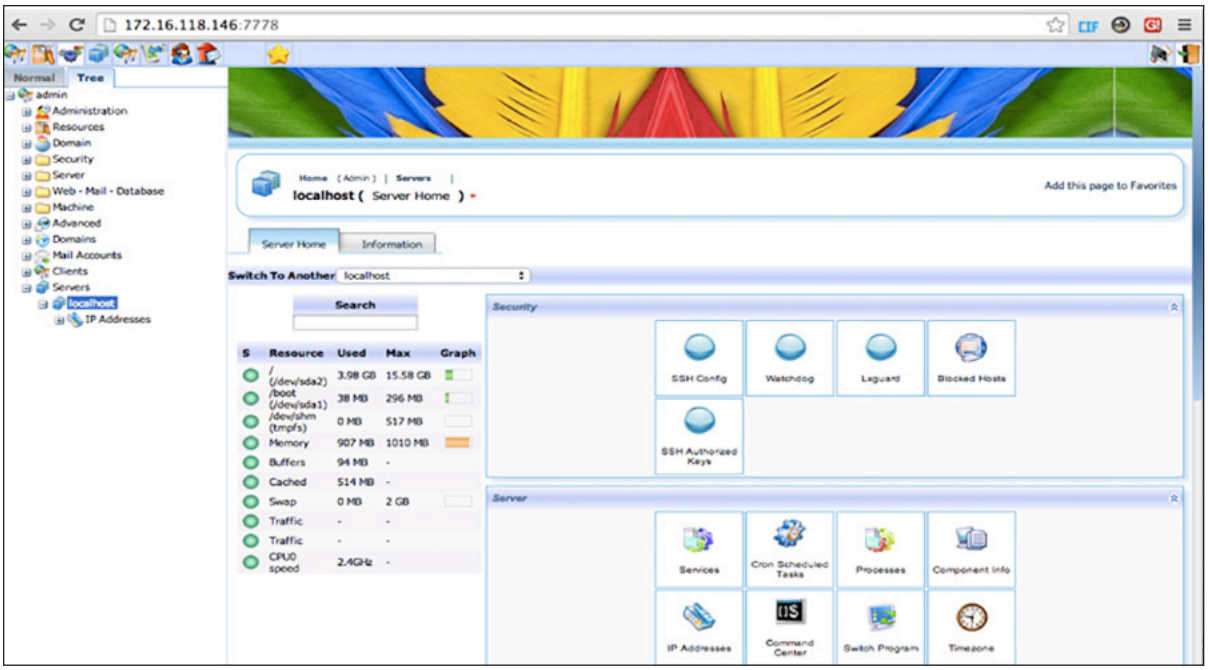

Figure 6: Kloxo web administration panel functions

How the cloud extends the attack surface

Malicious actors look to virtualization, vulnerable cloud services and their web applications as potential entry points to gain access to resources, bandwidth and good IP reputations. Some of the security risks faced by cloud providers include:

- Attacker access to the management interface or the hypervisor – a piece of computer software, firmware or hardware that creates and runs virtual machines – by escalating from guest to host using exploits such as Cloudburst[5] and VM escape techniques[6]
- Attackers targeting services with access to the hypervisor
- Attackers pivoting inside a private network, taking advantage of co-tenancy, shared guest storage, and guest-to-host relationships
- Abuse of provisioning, resource management, configuration and patch management
- Abuse of trust relationships, via services, management protocols

5 Higgins, Kelly Jackson. "Hacking Tool Lets A VM Break Out And Attack Its Host." Dark Reading

6 "What Is VM Escape?" The Lone Sysadmin RSS

How botnet builders upload files to vulnerable hosts

In order to build botnets, attackers must effectively exploit the vulnerabilities they find in their prospective victims. PLXsert has observed that malicious actors prefer to take the path of least resistance and target publicly available vulnerabilities and exploits. Publicly known remote access and pre-authentication exploits for popular web frameworks are favored. Skilled and motivated attackers may also develop customized exploits.

Operation Ababil is an example of a typical server-side botnet-building approach. Malicious actors mainly exploited large numbers of Joomla and WordPress instances and other web frameworks such as AWStats log file analyzer, Plesk web hosting automation program, cPanel web hosting control panel, and phpMyFAQ database-driven frequently asked questions (FAQ) system.

PHP remote file inclusion (CAPEC 193)

One of the most frequently exploited web vulnerabilities during the building of the Brobot botnet was the WordPress TimThumb plugin vulnerability, CVE-2011-4106[7]. TimThumb is a PHP script for resizing images in a WordPress blog. Version 0.11 has multiple exploitable vulnerabilities that allow attackers to upload a malicious web shell and then escalate privileges, take over the host and upload botnet files.[8]

A web shell is a web page coded in the targeted web framework language that provides access to system and administrative functions and remote access. Web shells provide a backdoor for malicious actors to remotely control compromised hosts. The C99 web shell, shown in Figure 7, is one of the most known and used web shells.

Figure 7: The C99 web shell is frequently used in web compromises

7 "Vulnerability Summary for CVE-2011-4106." National Vulnerability Database. US-CERT

8 Schmidt, Ben. "Multiple Wordpress Plugin Timthumb.php Vulnerabilites." Exploit Database. Offensive Security 2014

Another popular vulnerability used to upload malicious files and take over hosts is the unrestricted file upload vulnerability.[9] This vulnerability allows attackers to take advantage of unchecked upload content in some plugins and forms, which can enable the uploading of a web shell to a targeted web site. The following figures demonstrate a proof-of-concept exploit in a laboratory environment targeting WordPress 3.2 with a vulnerable plugin that allowed front-end upload. Figure 8 shows the lab environment with the plugin installed, and Figure 9 shows the malicious web shell file uploaded to a directory in WordPress. Figure 10 shows the b374k web shell running on the targeted WordPress instance.

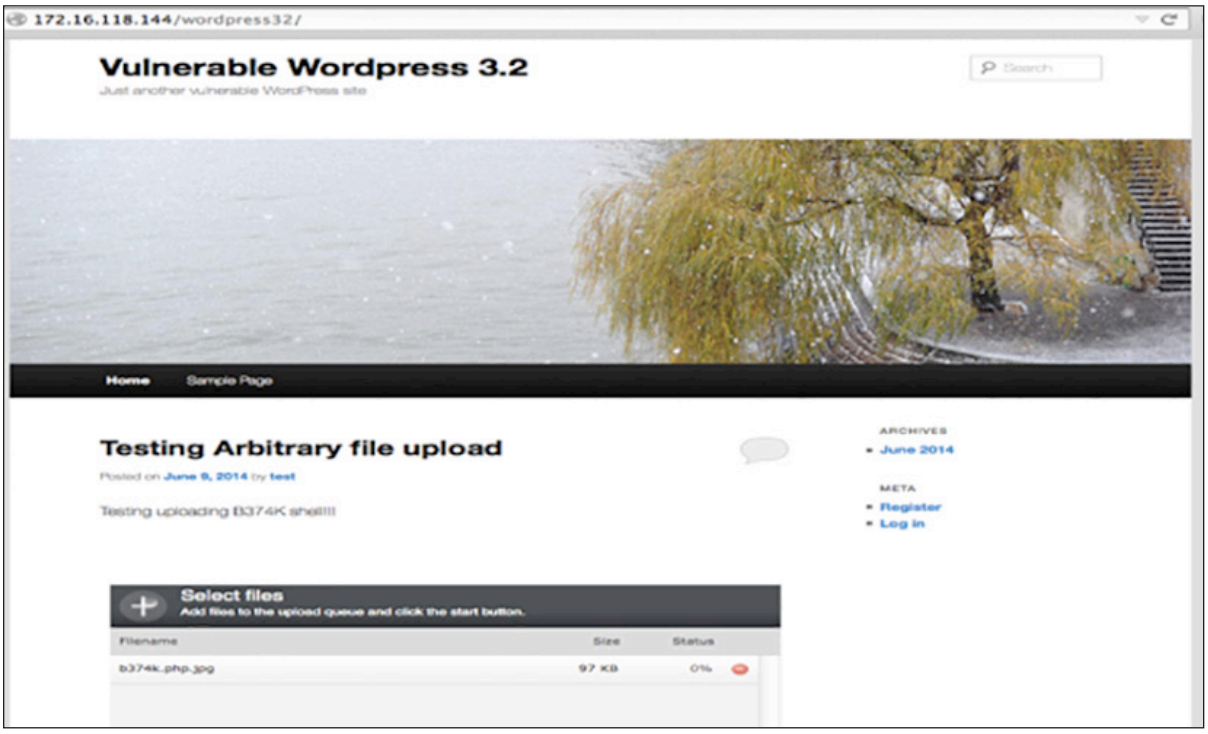

Figure 8: Installation of WordPress 3.2 with a vulnerable front-end upload plugin in a laboratory environment

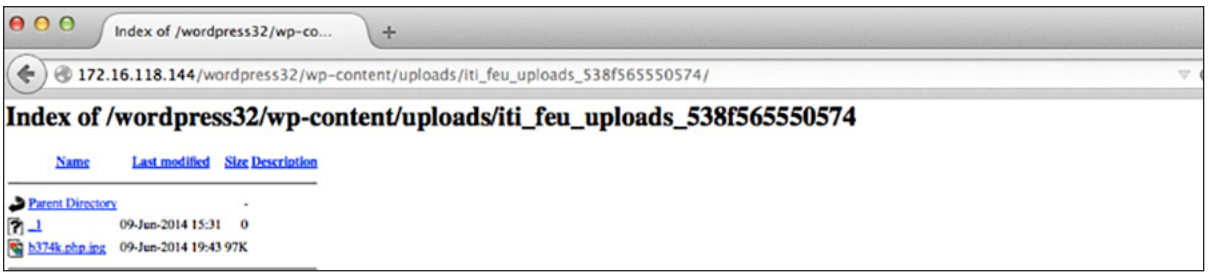

Figure 9: Confirmation of the installation of the b374k web shell to the WordPress 3.2 target in a laboratory environment

9 Dalali, Soroush, and Dirk Wetter. "Unrestricted File Upload." OWASP

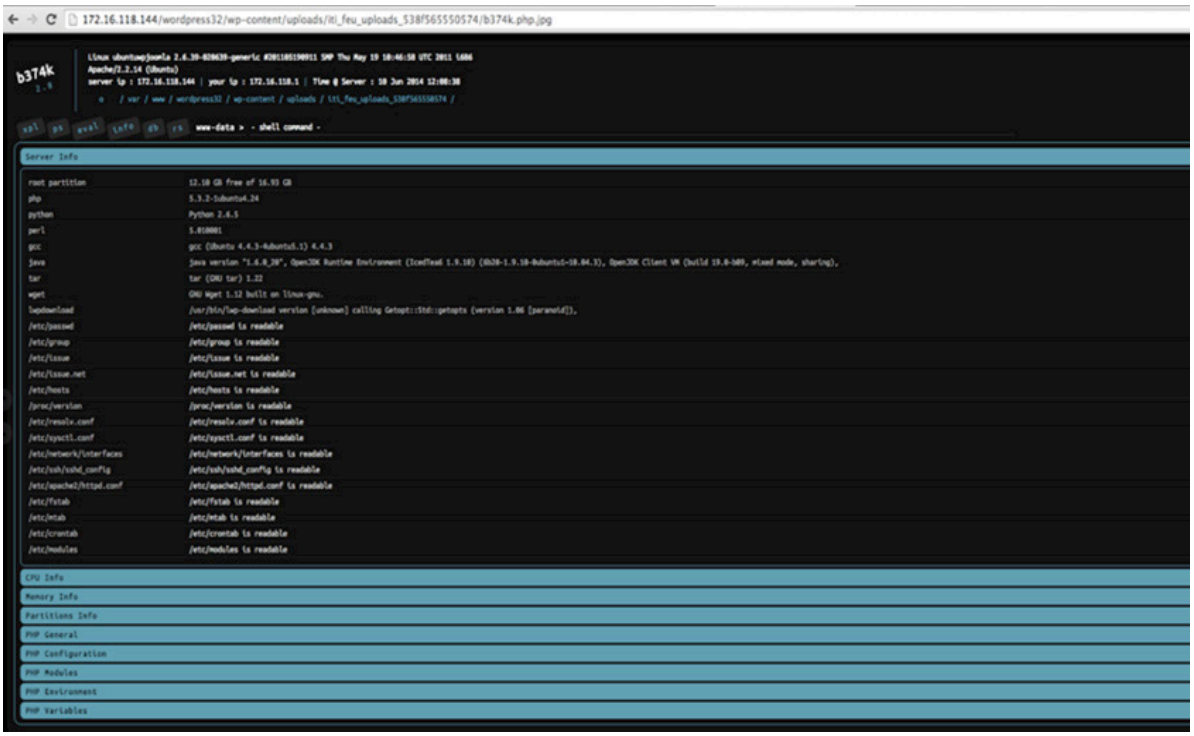

Figure 10: The b374k web shell running on the targeted WordPress server in a proof-of-concept test

Local privilege escalation

After uploading a web shell, the next step is often to escalate privileges. For example, CVE-2012-0056 allows local users to escalate privileges by modifying a memory process.[10] Such exploit code may be uploaded via a web shell and executed to gain root privileges, as shown in Figure 11.

10 "Vulnerability Summary for CVE-2012-0056." National Vulnerability Database. US-CERT

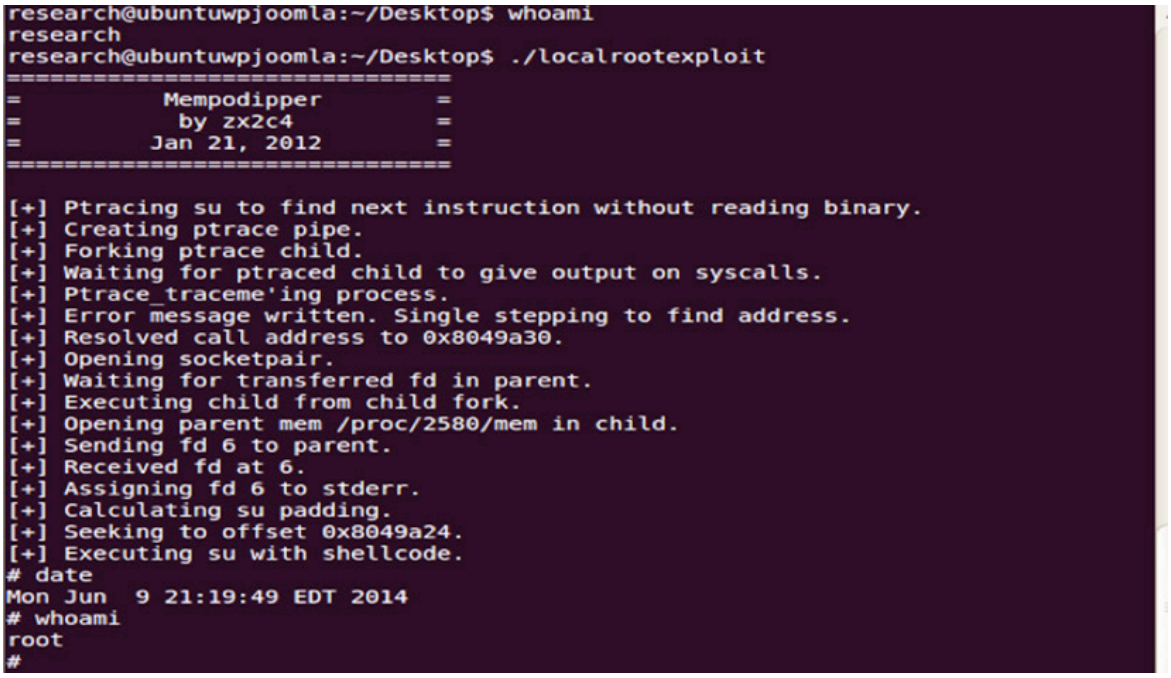

Figure 11: Example of local root exploit on Linux kernel 2.6.39 CVE-2012-0056

The Joomla Bluestork template vulnerability was also used extensively by attackers to escalate privileges and take over the administration of a site.[11]

Symbolic link (symlink) attack

Another frequently used botnet building technique observed during Operation Ababil was the use of symlink shells, in which an attacker creates a symbolic link that can lead to the compromise of files and folders on other applications and user information installed on the same hosts at shared hosting sites. This capability often allows a malicious actor to pivot to other installs, sometimes in very large numbers, thus speeding the botnet building process. A symlink shell is shown in Figure 12.

11 "Vulnerability in Joomla." Combell Blog.

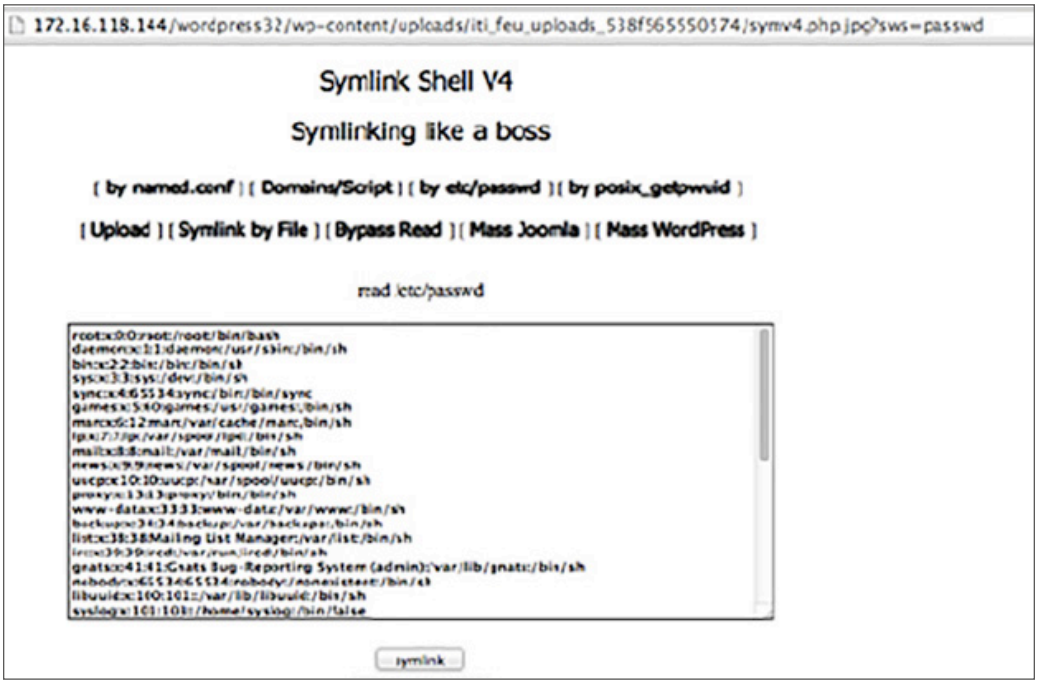

Figure 12: Symlink shell

An application targeted by brobot botnet builders using a symlink attack was the cPanel web hosting control panel. This was observed by researching the source IP addresses of Brobots, many of which belonged to the same hosting provider. cPanel for CentOS, which is shown in Figure 13, support creation and hosting of popular web blogging and CMS frameworks such as WordPress and Joomla. Figure 14 shows a symlink shell reading a multiple-site WordPress configuration file from a cPanel installation.

Figure 13: cPanel web hosting administration panel

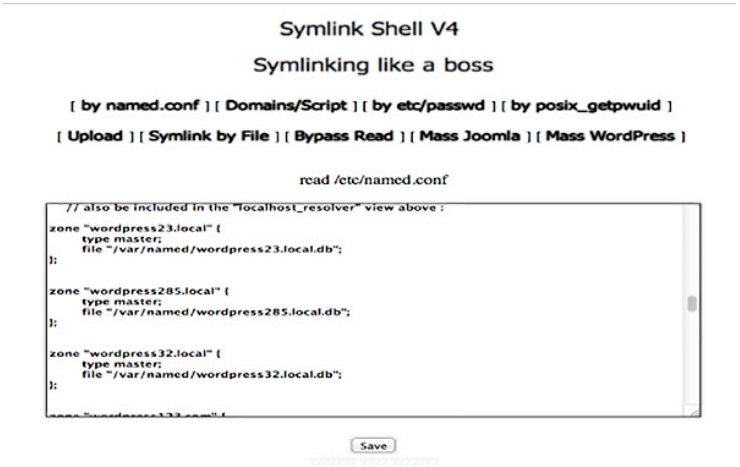

Figure 14: A symlink shell reading a mass WordPress configuration file from a cPanel installation

A similar result was enabled by the targeting of another web panel and hosting administration tool with remote code execution vulnerabilities.[12] Webmin is similar to Kloxo and cPanel for CentOS. In the case of Webmin, some public vulnerabilities and exploits are incorporated into the Metasploit Penetration Testing Framework. The exploit involves several steps that make it more difficult to execute, such as requiring the fingerprinting of the application, installing the exploitation framework and identifying users with privileges to use Sudo to gain security privileges to run programs as a superuser.

The figures below demonstrate a laboratory proof-of-concept of the use of this vulnerability. Figure 15 shows the Webmin interface, Figure 16 shows the Metasploit module, and Figure 17 demonstrates the exploitation of Webmin 1.580 as it reveals information about the targeted web frameworks.

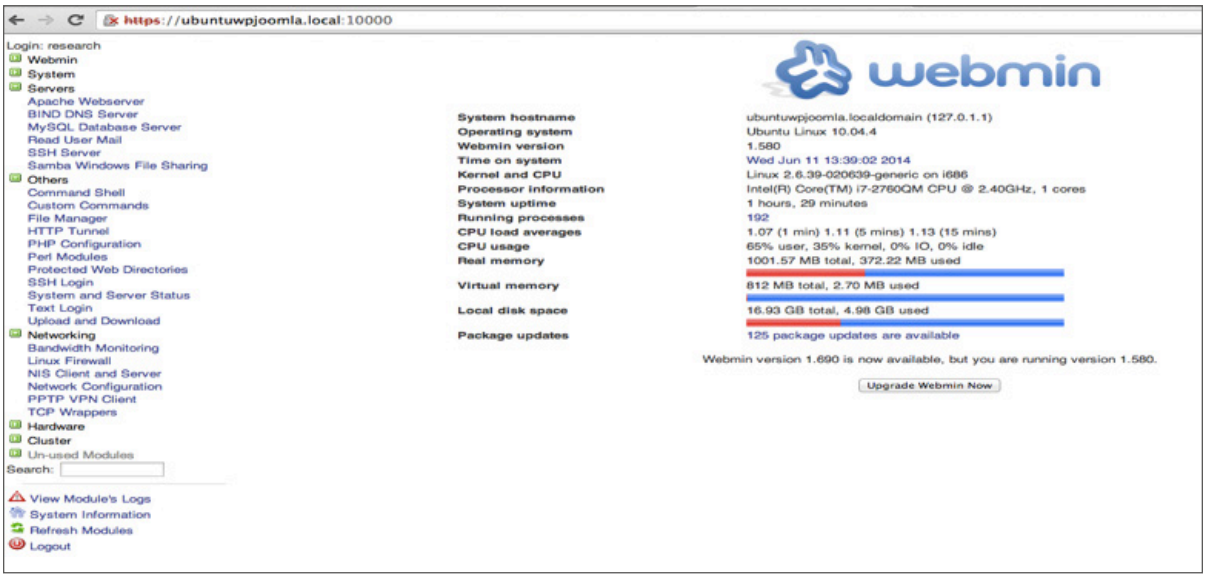

Figure 15: Webmin panel version 1.580

12 Vazquez, Juan. "Webmin /file/show.cgi Remote Command Execution - CVE-2012-2982." Vulnerability and Exploit Database. Rapid7

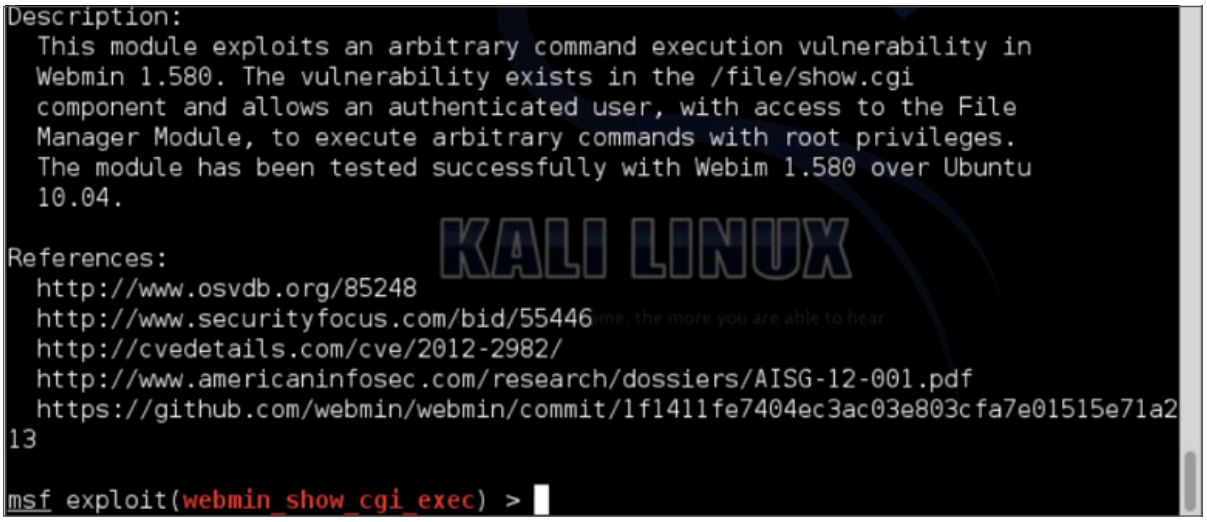

Figure 16: The Metasploit module

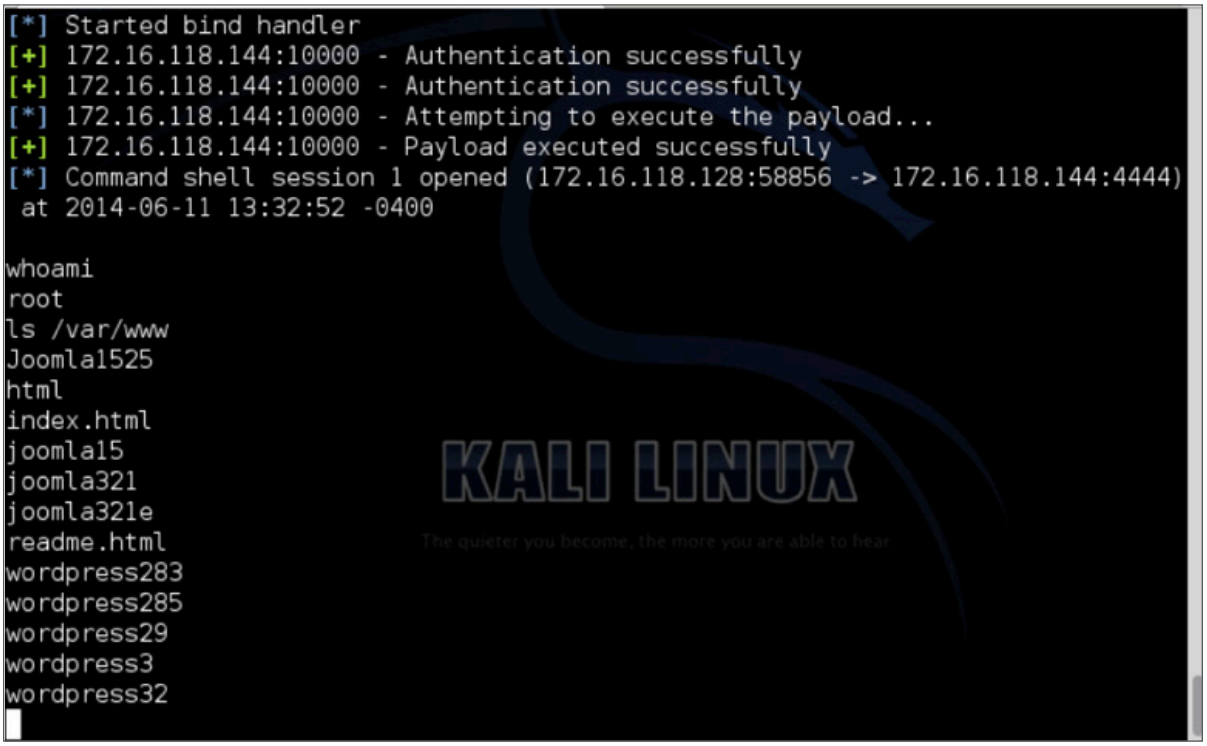

Figure 17: The result of exploitation of Webmin 1.580 provides information about the targeted web frameworks

The above laboratory examples are a few of the many attack vectors that malicious actors employ to build botnets by compromising web applications and targeting the large server farms that host them. After compromising a large number of web hosts during Operation Ababil, attackers uploaded their PHP Brobot scripts. One the first observations by PLXsert researchers was the ability to execute a simple GET request to compromised web hosts to determine if they were infected. Snippets of the requests from 2011, 2012 and 2013 are shown in Figure 18.

2011	2012	2013

if ($_GET['action']=="status")
{
print "Per Fatima";
exit():
}
	if ($_GET['action']=="status")
	{
	print "itsoknoproblembro";
	exit():
	}
		if ($_GET['action']=="status")
		{
		print "That is good";
		exit():
		}

Figure 18: Three itsoknoproblembro GET request checks throughout the campaign

PLXsert has analyzed Brobot and Operation Ababil extensively. These campaigns set the standard for the reach and power of advanced botnets that execute multiple layer 3 and layer 7 DDoS attacks. The operation ended around the third quarter of 2013, and since then no message from authors about renewing the operation had been recorded as of July 2014.

Brobot and its brethren live on

The genesis of server-side botnets like Brobot depends on two factors:

- Unpatched, unattended, mismanaged vulnerable hosts
- A group of organized malicious actors with sufficient skills to orchestrate massive exploitation, entrenchment and management of large numbers of compromised hosts to build botnets and orchestrate attacks

During the first and second quarters of 2014, PLXsert observed very significant combined layer 3 and layer 7 DDoS attacks with signatures similar to Brobot. A matching modus operandi was verified during the campaign in which malicious actors exploited large installs of the Kloxo web panel along with other web frameworks. Kloxo versions 5.75 and 6.1.6 are known to have several vulnerabilities and exploits[13].

These DDoS attacks continued intermittently in the second quarter against financial institutions, with self-attribution in April by a group named European Cyber Army (ECA). ECA claimed affiliation with the philosophy of Anonymous, as well as anti-U.S. interests. Attribution remains unproven, although the campaign shared many technical and strategic traits with Operation Ababil.

During Q2 2014 PLXsert observed a very large and significant attack targeting Akamai name servers. The vectors were principally of three types: reflected DNS amplification, DNS query flood and SYN flood attacks. Two of the payloads are shown in Figure 19.

13 "Kloxo Vulnerabilities." Exploits Database. Offensive Security.

```
SYN Flood
15:37:30.799944 IP 162.221.15.121.6548 > 209.200.164.3.53: Flags [S], seq
1600753593, win 62288, options [mss 1460], length 0
15:37:30.799946 IP x.x.x.x.59880 > 209.200.165.3.53: Flags [S], seq 255410057, win
60368, options [mss 1460], length 0
15:37:30.799949 IP x.x.x.x.19923 > 209.200.165.3.53: Flags [S], seq 2346548077,
win 56276, options [mss 1460], length 0
15:37:30.799950 IP x.x.x.x.4829 > 209.200.164.3.53: Flags [S], seq 3736223314, win
62321, options [mss 1460], length 0
15:37:30.799952 IPx.x.x.x.59199 > 209.200.165.3.53: Flags [S], seq 2711056711, win
50174, options [mss 1460], length 0

DNS Query
15:37:30.869895 IP x.x.x.x.3694 > 209.200.165.3.53: 17440+ A? <target domain>.
(33)
15:37:30.869896 IP x.x.x.x.3357 > 209.200.164.3.53: 1315+ A? <target domain>. (33)
15:37:30.869897 IP x.x.x.x.4504 > 209.200.165.3.53: 32+ A? <target domain>. (33)
15:37:30.869897 IP x.x.x.x.2808 > 209.200.165.3.53: 33+ A? <target domain>. (33)
```

Figure 19: Two example payloads observed during the attacks: SYN flood and DNS query

The multi-layer attacks combined to produce a peak of 119 Gigabits per second (Gbps), a level comparable to Operation Ababil. The Q2 attacks reached the highest packet per second (pps) rate observed by PLXsert – 110 million packets per second, which far exceed the pps rates of Operation Ababil and ECA. Such high pps rates can quickly overrun standard DDoS mitigation technology and can very quickly take down a standard web host. A comparison of attack peaks and packets per second for the three campaigns are shown in Figure 20.

Operation Name & Time Frame	Attack Peak (Gbps)	Packet per Second (pps)
Operation Ababil, 2011-2013	148 Gbps	78.3 Mpps
ECA, 2014	190 Gbps	97 Mpps
Q2 attacks, May 2014	119 Gbps	110 Mpps

Figure 20: A comparison of attack peaks and packets per second for three campaigns

The sources of this attack were located mainly in United States and China. The attacks appeared to be timed and orchestrated to target a specific blog on Asian affairs at the end of May. Further investigation by the PLXsert revealed the presence of malware binaries .IptabLex and .IptabLes that target Linux distributions and are spread by the exploitation of web vulnerabilities. The vulnerability targeted in many of the reported cases seems to be Apache Struts[14], Apache Tomcat[15] and outdated Linux kernel servers. Some of these Apache vulnerabilities allow the escalation of privileges and the takeover of hosts and some old Linux kernel distributions are susceptible to local root exploits as well.

14 "Apache » Struts : Security Vulnerabilities." CVE Details. MITRE Corporation.
15 "Apache » Tomcat : Security Vulnerabilities." CVE Details. MITRE Corporation.

Analysis of these binaries identified the presence of SYN and DNS DDoS payloads. Figure 21 shows evidence of DNS flood and SYN flood payload generating functions. One binary was found connecting back to IP addresses owned by China Telecom[16], Many of the reports about the use of this binary are published in Chinese[17], and reports suggest the use of the binary is reaching additional regions.[18] The majority of these incidents report IP call backs to Chinese infrastructure.

```
public DnsFloodSendThread
DnsFloodSendThread proc near

var_20= dword ptr -20h
var_1C= dword ptr -1Ch
var_18= dword ptr -18h
var_14= dword ptr -14h
var_10= dword ptr -10h
arg_0= dword ptr  8

push    ebp
mov     ebp, esp
push    edi
xor     edi, edi
push    esi
push    ebx
sub     esp, 2Ch
mov     ebx, [ebp+arg_0]
mov     [ebp+var_1C], 0
mov     [ebp+var_14], 0
mov     [ebp+var_10], 0
mov     eax, [ebx+34h]
mov     word ptr [ebp+var_1C], 2
mov     word ptr [ebp+var_1C+2], 3500h
mov     [ebp+var_18], eax
movzx   eax, word ptr [ebx+1Ah]
imul    eax, 1388h
mov     [ebp+var_20], eax
```

```
public DnsFloodSendThread
DnsFloodSendThread proc near

var_20= dword ptr -20h
var_1C= dword ptr -1Ch
var_18= dword ptr -18h
var_14= dword ptr -14h
var_10= dword ptr -10h
arg_0= dword ptr  8

push    ebp
mov     ebp, esp
push    edi
xor     edi, edi
push    esi
push    ebx
sub     esp, 2Ch
mov     ebx, [ebp+arg_0]
mov     [ebp+var_1C], 0
mov     [ebp+var_14], 0
mov     [ebp+var_10], 0
mov     eax, [ebx+34h]
mov     word ptr [ebp+var_1C], 2
mov     word ptr [ebp+var_1C+2], 3500h
mov     [ebp+var_18], eax
movzx   eax, word ptr [ebx+1Ah]
imul    eax, 1388h
mov     [ebp+var_20], eax
```

Figure 21: Evidence of DNS flood and SYN flood payload generating functions

Mitigation

The mitigation of web vulnerabilities starts with monitoring and updating vulnerable server installations. This action will prevent malicious actors from continuing to compromise servers and distribute malicious files. It is imperative to establish mechanisms and procedures for version control and change management at Internet Service Providers (ISPs) and hosting providers that have very large installs of popular LAMP distributions and outdated Windows servers. There is an extensive list of procedures and methods provided by the National Institute of Standards and Technology (NIST) to secure public facing web servers.

16 "Help! My Server Has Been Hacked - .IptabLes and .IptabLex in /boot [closed]." Ask Ubuntu. Stack Exchange
17 "Search for IptabLes IptabLeX." Google.
18 "MMD-0025-2014 - ITW Infection of ELF .IptabLex & .IptabLes China #DDoS Bots Malware." Malware Must Die!

Researchers in the information security community are leading the effort to discover and disclose web vulnerabilities. Channels of communication and collaboration among developers, vendors and security researchers will need to be streamlined to promote faster and more efficient mitigation, as well as instituting regular update and patching procedures. Many of the described vulnerabilities were promptly patched even while the attack campaign occurred, but for the majority of vulnerable hosts, the patches went unapplied, therefore enabling further attacks.

Mitigation becomes more difficult when these campaigns combine the use of specially crafted binaries such as the Linux based IptabLes/IptabLex bot. A multi-layer DDoS mitigation approach is necessary to protect and defend the attack surface of Internet-facing servers and cloud-based SaaS and PaaS providers. Best practices require application patching, hardening and updating as well as system updating and management.

Cybersecurity defense is all about anticipation. It is only with the collaboration of all participants to develop, research, discover and fix vulnerabilities that it will it be possible to harden systems and prevent future attack campaigns. Solving these problems can prevent attacks that could otherwise cause significant disruption to businesses, organizations and governments.

In order to protect against the attacks and possible campaigns described in this white paper, it is necessary to have specialized protection that includes a multi-layer approach with skilled defenders and technology. Akamai Technologies provides web security products that protect Internet-facing applications and servers. Some of the principal benefits of these products include:

- DDoS defense
- Application firewall
- Rate controls
- Top web attacks (SQLi, XSS, XSRF, etc.)
- DNS protection
- User validation
- Custom mitigation rules against specific attack signatures

PLXsert researchers constantly test and verify the latest attack vectors to incorporate appropriate defenses into DDoS and cybersecurity protection technologies.

Conclusion

Web vulnerabilities have become the gateway for and the genesis of the most sophisticated DDoS attack campaigns ever launched. Organizations and vendors including PaaS and SaaS companies, which are becoming more pervasive, cannot remain ignorant of current and future threats. Failure to take action to fix vulnerable web applications and services enables and promotes the abuse of these popular and dispersed applications.

This white paper illustrates the feasibility of building botnets through the compromise of large installs of commonly used web frameworks. Malicious actors actively seeking to build botnets are likely to use server-side bots as their main attack vectors in concert with client-based attacks. In addition, malicious actors gain benefits by compromising web-based applications, specifically PaaS and SaaS instances, to take advantage of these vendors' reputations, bandwidth and defense technologies.

There is a false sense of security in believing cloud providers are not vulnerable or are less prone to compromise than single hosts. The current surge of PaaS and SaaS providers extends the attack surface and provides malicious actors with resources not previously available. Attackers will pursue these resources to amplify their resources and produce larger attack payloads. Campaigns orchestrated by large web-based botnets have created some of the largest payloads and more sophisticated attack signatures. Akamai's DDoS mitigation team has been successful in defending against this type of attack by implementing a multi-layer defense that combines of human experts and best-of-breed DDoS protection technology.

Server-side botnets have only been observed in well-orchestrated and sophisticated DDoS campaigns, indicating the presence of attackers with a higher skill level. These campaigns have gained notoriety for, and offer prestige to, malicious actors in the underground. Because server-side botnets present a very effective attack vector, it is likely that malicious actors will use and monetize this type of botnet in the DDoS-for-hire market. There is reason to believe that the actors behind earlier Brobot attacks can simply resume their attacks at any time, since they were able to obfuscate and grow the botnet without being detected.

About the Prolexic Security Engineering and Research Team (PLXsert)

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.

About Akamai

Akamai® is the 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.

PROLEXIC
Now part of Akamai

v.091214