

# Global Threat Report

October 2009

## Key Highlights

- 29% of all Web malware blocks in October 2009 were the result of Gumblar;
- Enterprises experienced an average of 119 Web malware encounters each in the month of October compared to an average of 76 each in September 2009;
- At least 2000 backdoored websites are acting as malware hosts in the Gumblar attacks;
- Tens of thousands of other websites are acting as conduits for that malware;
- Backdoored websites may now be under the control of multiple attackers.

## The Gumblar Effect

**G**umblar, originally discovered by ScanSafe researchers in the first quarter of 2009, is arguably one of the most insidious threats facing both Web surfers and website operators today. Gumblar takes a multi-pronged approach, installing traffic sniffers and backdoors on Web surfers' PCs and then using stolen FTP credentials to compromise and backdoor websites.

In short, Gumblar has been simultaneously building and maintaining a dual set of botnets throughout 2009 - one for client computers and another of backdoored websites.

In October 2009, Gumblar began leveraging its botnet of backdoored websites, using them as the malware host itself. The malware hosted on the sites is dynamically constructed at the time of access. Thus different users, dependent on their browser type and other considerations, will be delivered different exploits and potentially different malware. The malware is also dynamically obfuscated, hampering detection via traditional signature strings.

Perhaps most disturbingly is that the backdoor left in place on the compromised websites by the Gumblar attackers can be rather easily leveraged by other attackers. Currently, it is estimated that Gumblar controls at least 2000 backdoored websites. It is further believed that this is an extremely conservative measurement.

In early November, some of the backdoored compromised websites began exhibiting behavior indicative that the sites were indeed under the control of separate groups of attackers, thus exacerbating the seriousness of the situation.

### Website Botnet

In an ordinary website compromise, attackers use SQLi or other code injection methods to embed hidden iframes on susceptible websites. These iframes load malware that is hosted on an attacker owned domain. In an evolutionary departure from norm, the Gumblar attackers are:

- gaining access via stolen FTP credentials;
- installing PHP backdoors on the compromised websites ;
- using the backdoored websites as the actual malware host.

The implications are rather staggering. When a typical outbreak of website compromises occur, there are generally only a few actual malware domains involved. Thus even in an attack impacting hundreds of thousands of websites, the attack can be stopped by targeting efforts at shutting down the few actual malware hosts from which those compromised sites load the malware.

In the case of Gumblar, conservatively there are at least 2000 backdoored websites serving as actual malware hosts. As a result, there is no single or few points at which to target efforts to shutdown the source of the malware.

### Iframe Attack

To load the malware from the backdoored websites, tens of thousands of other compromised websites have had malicious iframes embedded. (In some cases, a backdoored website acting as malware host may also contain embedded iframes pointing to different Gumblar-compromised hosts.)

Whether a site is backdoored (host) or merely has the iframe embedded (conduit) is dependent on architecture. PHP-based sites will be backdoored and become hosts, non-PHP-based sites will have iframes embedded and become conduits.

### Client-Side Malware

Web surfers who visit one of the conduit sites will be exposed to a collection of exploits designed to silently install the Gumblar malware. On Windows systems, the installed malware:

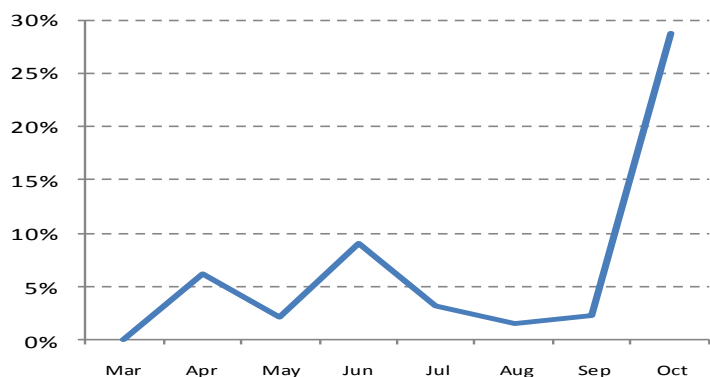
- loads when sound-enabled sites or devices are accessed;
- injects itself into the Internet Explorer process;
- intercepts all Web traffic to and from the computer.

Any captured FTP credentials are sent to the attacker thus furthering the growth of the Gumblar website botnet. Additional malware downloaded to the PC installs an IRC bot. Some evidence suggests a possible connection to the Zeus botnet.

*ScanSafe customers were and continue to be protected from the attacks discussed herein.*

# The Gumblar Effect

## ❖ 2009 Gumblar Blocks by Volume



## ❖ How Gumblar Got Its Name

During the first stage of the Gumblar attacks in 1Q09, the compromised websites were embedded with iframes loading malware from 94.247.2.195. Investigating the malware, ScanSafe discovered that Google search results (SERPs) were being tampered with. ScanSafe notified Google of the attacks and Google began delisting websites containing the malicious 94.247.2.195 iframe.

In April 2009, as delisted site owners began cleaning up their sites in an effort to regain listing in Google SERPs, the attackers immediately re-compromised the websites with dynamically obfuscated script references pointing to gumblar.cn. It was at this stage of the attacks that ScanSafe researchers dubbed the threat "Gumblar".

## Secondary Attacks

### ❖ Backdoors potentially being leveraged by other attackers

Ongoing analysis suggests the PHP backdoors left behind by the Gumblar attackers are potentially being leveraged by a second (and possibly third) group of attackers.

In one example, in early November, code on some of the backdoored sites was changed to loosely obfuscated script that coincidentally contained the word "gumblar" in non-obfuscated form:

```
(<22<3c<73<63rip<74<20src<3d<2f<2fgumblar<2e<63<6e<2frs<73
```

Predictably the deobfuscated script revealed an iframe pointing to gumblar.cn, one of the earlier malware hosts used in late April and early May and from which Gumblar was named. A domain check revealed that gumblar.cn was once again live, though DNS hosting was suspended in less than 36 hours.

With thousands of malware hosts at its disposal, it's unlikely the true Gumblar attackers would have any need for an additional malware host, much less gumblar.cn specifically. Further, the obvious gumblar contained in the script is more reminiscent of a "shout out" to the actual Gumblar attackers versus anything they might do themselves.

### ❖ Malware is regionally targeted

Interestingly, an examination of the source code for the malware delivered via the Gumblar-backdoored websites reveals the malware is language-specific, targeting English, Dutch, German, Italian, and Spanish users.

## ❖ Gumblar Quick Facts

- Method of compromise is via stolen FTP credentials;
- No server-side vulnerabilities are involved;
- PDF, Flash, and OWC exploits are used to deliver the malware;
- PHP-based sites have PHP backdoor installed;
- HTML-based sites are used as conduits;
- The injection method used in the October attacks can cause errors that prevent a site from displaying normally;
- The errors are not hampering the success of the October 2009 Gumblar attacks, which totaled 29% of all Web malware blocks for that month.

## ❖ October 2009 Top Ten Blocks

Trojan.Gumblar	29%
Win32.Krap.ah	10%
JS.Agent.bd	5%
JS.PrygSkok.a	3%
OI.Script.Shellcode	3%
OI.PDF.Susp	2%
OI.Win32.Susp.EG	2%
Trojan.Win32.Scar.zmi	2%
OI.PDF.Explt.07-5659	1%
Exploit.JS.Agent.art	1%

## About ScanSafe SaaS Web Security

ScanSafe's SaaS Web Security protects organizations of all sizes against Web-based malware attacks and enables the safe, productive use of the Web without incurring hardware, upfront capital, or IT management costs.

Real-time proxy-based Web scanning stops web-based malware at the Internet level, before it reaches corporate networks. Inbound scanning protects against new malware threats and outbound detection alerts to malware communications resulting from pre-existing infections.

The Web Filtering service enables the creation, enforcement, and monitoring of Web usage policies. It includes streamlined configuration through a graphical dashboard, real-time rules-based filters, and a best-in-class URL database.

ScanSafe IM Control enables customers to control the rapidly growing use of public IM, such as AOL, Yahoo!, and Windows Live, in corporate networks. With IM Control, you can control and standardize your IM network; monitor, log, and audit IM use and generate customizable scheduled reports; and access compliance logging that integrates with your organization's email archiving solutions.

## About Outbreak Intelligence™

ScanSafe's Web security applications are built on Outbreak Intelligence (OI™), a proprietary security platform that detects both new and known malware threats. By leveraging its unique position at the Internet level and processing several terabytes of Web data each day, OI has unmatched visibility of global Web data to proactively identify zero day malware threats.

OI uses multiple signature-based anti-malware scan engines, multiple reputation and behavior detection engines, and automated machine-learning parameter development to detect new malware and avoid false positives.

This combination of multiple, correlated detection technologies, automated machine-learning heuristics, and the industry's largest Web data set makes OI the most effective solution against new Web-based malware attacks.

## Contact ScanSafe

### ScanSafe US

185 Berry Street  
San Francisco, CA 94107

T: +415 692 2000  
F: +415 536 5949

### ScanSafe EMEA

Qube, 90 Whitfield Street  
London, W1T 4EZ

T: +44 (0) 20 7034 9300  
F: +44 (0) 20 7034 9301

...or email [info@scansafe.com](mailto:info@scansafe.com)

## Subscribe to the Global Threat Report

To receive ScanSafe's Global Threat Report each month, visit:

[http://www.scansafe.com/threat\\_center/gtr](http://www.scansafe.com/threat_center/gtr)

## STAT Blog

Timely, expert analysis and insight on the latest Web-borne threats and scams, tips on how to protect corporate assets from infection and observations on the threat landscape. Visit:

<http://blog.scansafe.com>.