**Introduction**

In this Q3 2011 edition of the State of the Web from Zscaler ThreatLabZ, we take a closer look at Enterprise web traffic, aggregated across over a hundred billion transactions and millions of business users across the globe.

This quarter we continued to see the social elements of the web dominate advanced threats and attacks in Enterprise networks. Leveraging sophisticated social engineering techniques to launch their attacks, malicious groups and hactivists know that human interest, curiosity and oversight represent the weakest link in any enterprise security chain. For that reason, ThreatLabZ wasn't surprised to see popular social networking applications leveraged as a top attack channel and target.

While these trusted social networks and applications continue to dominate enterprise Internet use, employees often have a false sense of security – trusting their favorite tools and apps to provide them ‘safe’ information. However, hackers this quarter continued to take advantage of this trust to exploit corporate victims through web apps, web searches and targeted email scams.

**Three major trends noticeable in this report include:**

- **Facebook still dominates enterprise web application use**
  - Facebook still remains the dominant web application in enterprise traffic – risking like-jacking, fake videos, and spear-phishing

- **Corporate mobile devices split between business and personal use**
  - While social networking remains the dominant source of mobile device traffic, business-related traffic follows closely behind

- **Blended threats continue to target browser plug-ins**
  - Browser plug-ins and extensions remain well out of date, providing a large target base for attacks.

**In This Issue:**

- Decline in Facebook
- Mobile device usage in the workplace
- Browser plug-ins/extensions remain out of date in enterprise
## Contents

A Look Beyond the Browser ................................................................. 4

The Hidden Risks of Plug-ins and Extensions .................................. 6

Android Reclaims its Title in the Enterprise .................................... 8

Mobility Meets Productivity ............................................................. 10

Facebook ‘Likes’ the Enterprise ..................................................... 12

When Malware Strikes ................................................................. 14

A Safe and Productive Network ................................................... 16

Conclusion .................................................................................. 17
Looking Beyond the Browser

Every quarter, Zscaler ThreatLabZ tracks enterprise HTTP and HTTPS traffic—including the specific browsers in use. This allows us to show trends in Web and browser use, as well as the vulnerabilities associated with them.

With the dominance of Microsoft end-user operating systems in the enterprise, Internet Explorer (IE) maintained its position as the most popular browser observed this quarter. Although Web browsers make up over 75% of HTTP and HTTPS traffic, the other, non-browser traffic is worth looking at. This is made up of browser plug-ins, add-ons and extensions – as well as HTTP and HTTPS traffic from native applications.

In Q3, we continued to see a rise in non-browser web traffic – being driven by mobile and desktop applications that leverage HTTP(S) for outbound communication. This is not entirely surprising, as most enterprises have ‘firewalled’ off most ports beyond the ones needed for web and email traffic. As a result, ports 80 and 443 represent a viable egress point for any application.

“Much of enterprise web traffic originates from native apps, and browser extensions - not just web browsing”
Q3 Enterprise Browser Traffic

Despite its dominance, the enterprise traffic share for Internet Explorer has been dropping as Apple becomes a more accepted desktop and laptop solution. This is fueling a growth in Safari, and enterprise employees continue to adopt other alternatives such as Firefox. We have yet to see significant adoption of Chrome in the enterprise, despite increasing adoption in the consumer space. Below are the Q3 traffic shares by browser type:

![Q3 HTTP(S) Browser Traffic by Type](image)

“Internet Explorer 9 – despite its additional security features and HTML5 compatibility – has yet to see significant adoption at the enterprise level.”
Internet Explorer Versions in Use

As outlined in the graph above, Internet Explorer commands just over half of the total web traffic in the enterprise. Internet Explorer 9 – despite having been released in March of this year with additional security features and HTML5 compatibility – has yet to see significant adoption at the enterprise level. Drilling deeper into the Internet Explorer usage data over each month of the quarter, we see the following:

![Internet Explorer Traffic Share Q3 2011](image)

The Hidden Risks of Plug-ins and Extensions

Today, plug-ins, add-ons or extensions combine with nearly every browser running in the enterprise. Similar to most any kind of software, older versions of plug-ins typically have more security vulnerabilities.

Zscaler offers a unique solution known as Secure Browsing. Secure Browsing identifies the type and version of web browser that is in use. As well – and even more importantly – it also identifies the browser plug-ins
that have been employed. As we can see in the chart below, enterprise browser plug-ins are dominated by Microsoft and Adobe, with Adobe Flash remaining the most popular overall browser plug-in in the enterprise.

![Most Common Web Browser Plugins Q3 2011](image)

Unfortunately, Secure Browsing reveals a highly concerning statistic. Beyond simply revealing which plug-ins are most popular, it also provides insight into the plug-ins that are most commonly outdated. These statistics do tend to fluctuate from quarter to quarter. This is due to typical quarterly patch release cycles, which tend to cause a spike in outdated versions for specific plug-ins as end-users fail to implement the updates.

This is an area where enterprises are currently struggling. As ThreatLabZ continues to highlight, browser plug-ins are made up of a potentially dangerous combination of characteristics – all of which adds up to a tempting target for hackers.

Looking at the statistics below, it becomes clear that most companies have little control over the type of plug-ins that their employees are using, or the specific version of plug-ins in use.

---

**Why it Matters to Your Enterprise:**

**Browser plug-ins offer a dangerous combination of characteristics**

- Readers and players are ubiquitous, across browsers
- Most users aren’t aware of which plug-ins they have installed
- Most enterprises have no patch management deployed to keep plug-ins up to date
Android Reclaims its Title in the Enterprise

Both mobile device usage and mobile device web transactions logged through Zscaler’s global security cloud infrastructure continue to grow. The highest percentage of Q3 mobile transactions through Zscaler’s cloud was from Android devices – followed by Blackberry, and Apple IOS devices.

As mobile transactions from our enterprise customers continue to grow, we notice that the Android platform accounts for the largest and geographically dispersed user-population. As well, it represents the mobile platform with the highest number of transactions through our cloud. The Apple IOS platform moved to third place this quarter, falling to 22.38% from 42.37% in Q2 2011. This is likely due to a growing sample size of mobile use outside the US.
Figure 6 provides a geographic breakdown on web client transactions that used standard Android, BlackBerry or Apple iOS user-agents. The United States made up about 80% of the mobile client transactions from Zscaler’s enterprise customer base.

Android Percent by Country
Among our global enterprise customers, Android has the largest geographic coverage. Whereas, among US-based customers, BlackBerry and iOS devices represented more than 80% of the mobile usage. The following charts break out device usage by-country. (Note that IP addresses that did not resolve to a particular country were excluded from the percentages.)

**Why it Matters to Your Enterprise:**

- Enterprise users continue to leverage a variety of smartphones and tablets for both personal and business use
- Supporting and securing an increasing variety of mobile devices remains a significant challenge for enterprises
Mobility Meets Productivity

Zscaler ThreatLabZ tracks the most prominent website categories viewed by enterprise mobile platforms. For Q3 2011, social networking topped all others among website categories most viewed on enterprise mobile devices. This differs, however, from overall enterprise web browsing—where corporate marketing, professional services, web search and news/media sites are more popularly visited than social networking.
When looking at various website categories browsed by specific mobile device platforms, few differences are noticed. However, Android and iPod have a much higher percentage of social networking browsing than other mobile device platforms. As well, the iPhone is more popular for music, streaming audio and professional services than other platforms. In some usage areas, the Blackberry and iPad platforms seem closely related – with both being popularly used for news and media.

Interesting to note is the mix of business and recreational traffic on all devices – these are being used for some productive purposes, not just personal apps and browsing.

Facebook ‘Likes’ the Enterprise

Maintaining the trend seen in Q2 2011, social networking was once again the most dominant category of browsed web applications through the Zscaler cloud in Q3. And, given its dominance in enterprise web application use, Facebook once again lead the pack. Yet, for the first time, ThreatLabZ saw a slight month-to-month drop in enterprise client Facebook usage. Meanwhile, other popular web applications like Gmail, YouTube, Twitter and LinkedIn experienced a slight increase.

“Shopping is more popular on desktop systems than mobile platforms, while sports is more popularly viewed on mobile platforms than desktops.”
Similar to last quarter, social networking and webmail made up the majority of the total web application transactions for the quarter – with web search representing a comparatively smaller percentage. The chart below provides a detailed drill-down of overall web usage (by site) throughout the quarter:

**Q3 Web Application Usage Drill-Down**

- Facebook: 45.72%
- Gmail: 16.16%
- YouTube: 6.58%
- LinkedIn: 6.51%
- Yahoo Mail: 3.00%
- MSN IM: 2.78%
- Twitter: 1.94%
- Hotmail: 1.39%
- Blogger: 1.15%
- Pandora: 0.81%
- Other: 1.15%

**Top Q3 Web Application Usage by Month**

- Facebook: September 50%, August 40%, July 30%
- Gmail: September 45%, August 40%, July 35%
- YouTube: September 35%, August 30%, July 25%
- LinkedIn: September 30%, August 25%, July 20%
- Hotmail: September 20%, August 15%, July 10%
- Blogger: September 10%, August 5%, July 0%
- Pandora: September 5%, August 3%, July 1%

**Why it Matters to Your Enterprise:**

- Facebook remains the predominant web 2.0 app in the enterprise—making up nearly 50% of overall usage for the quarter.
- As Facebook, Twitter, LinkedIn and YouTube continue to dominate overall web application use, enterprises are often allowing unrestricted employee access to social networking apps.
- Allowing, yet securing, social networking apps is a paradox for today’s IT teams.
When Malware Strikes

Zscaler ThreatLabZ identifies and tracks malicious content in real time – across both HTTP and HTTPS. This gives Zscaler ThreatLabZ the information needed to identify the sources of malware, while tracking general trends in malware threats.

The top trend in malware continues to be the inclusion of IFrames within malicious content (often an exploit kit). In September 2011, greater than 67% of the anti-virus signatures that triggered were on web pages that had malicious IFrame inclusions. We have continued to notice a steady increase in security blocks—over time and throughout Q3—that resulted from malicious web responses. Below are the top 10 malware types for Q3.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Malware Type</th>
<th>Rank</th>
<th>Malware Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Malicious HTML IFrame</td>
<td>6</td>
<td>Malicious JS in PDF</td>
</tr>
<tr>
<td>2</td>
<td>Malicious JS Redirector</td>
<td>7</td>
<td>Malicious JS IFrame</td>
</tr>
<tr>
<td>3</td>
<td>Malicious binary, heuristic detection</td>
<td>8</td>
<td>Malware/Spyware Toolbar</td>
</tr>
<tr>
<td>4</td>
<td>Malicious SWF</td>
<td>9</td>
<td>Malicious W32 Trojan</td>
</tr>
<tr>
<td>5</td>
<td>OnlineGames Malware</td>
<td>10</td>
<td>JS Shellcode</td>
</tr>
</tbody>
</table>

* based on A/V detection only for the most recent month of the quarter (September)
Blackhat Sites and Phishing Spikes

Blackhat SEO continues to be a tactic used by cyber criminals to increase web traffic to their sites. Compared to last quarter, the number of search results leading to malware has decreased. However, the number of spam sites (fake stores, fake search engines, etc.) using hijacked sites has increased. University websites (.edu) are still the main source of hijacked sites. The following chart breaks out the types of sites being served in these campaigns.

![Blackhat SEO Site Types](image)

Figure 14
A Safe and Productive Network

Throughout Q3, Zscaler noticed a monthly drop in web policy blocks in social networking, webmail, and malware transactions. Conversely, there was a monthly increase in botnet, instant messaging, and anti-virus transactions.

Malicious web responses continue to be on the rise – with malicious IFrame or Javascript inclusions being the primary threat blocked. This malicious content redirects browsers, often to an exploit site that attempts to exploit known vulnerabilities within web browsers or browser plug-ins. The most common plug-ins that our customers have installed and left unpatched/vulnerable are Adobe Shockwave, Java, and Adobe Reader. Each of these plug-ins has more than 50% of its installs left out-of-date. This is a sharp increase from the previous quarter.

“Malicious web responses continue to be on the rise – with malicious IFrame or Javascript inclusions being the primary threat blocked.”
Conclusion

Every quarter Zscaler ThreatLabZ publishes our State of the Web report to provide some high-level trends observed from the large number of enterprise web transactions traversing the Zscaler security cloud. Given the scale of transactions we see (over a hundred billion across millions of global users), ThreatLabZ is able to provide interesting data-points on enterprise browser usage, browser plug-ins, mobile devices, website categories and various security trends we observe.

Of the trends and data-points noticed this quarter, a few stand-out:

• A month-to-month percentage decline in enterprise Facebook usage.

• While Android mobile devices continue to be in the lead within our global user-base, we noticed Apple IOS devices representing the largest quarterly increase.

• Malicious web-site responses – particularly those containing malicious IFrame or Javascript inclusions – appear to be on the rise.

• At the same time, the number of clients with vulnerable versions of browser plug-ins also seem to be on the rise.
About the Authors

This report was written by Michael Sutton, Julien Sobrier, Mike Geide, Pradeep Kulkarni, and Umesh Wanve.

About Zscaler: The Cloud Security Company™

Zscaler enforces business policy, mitigates risk and provides twice the functionality at a fraction of the cost of current solutions, utilizing a multi-tenant, globally-deployed infrastructure. Zscaler’s integrated, cloud-delivered security services include Web Security, Mobile Security, Email Security and DLP. Zscaler services enable organizations to provide the right access to the right users, from any place and on any device—all while empowering the end-user with a rich Internet experience.

About Zscaler ThreatLabZ™

ThreatLabZ is the global security research team for Zscaler. Leveraging an aggregate view of billions of daily web transaction, from millions of users across the globe, ThreatLabZ identifies new and emerging threats as they occur, and deploys protections across the Zscaler Security Cloud in real time to protect customers from advanced threats.

For more information, visit www.zscaler.com.