



Flash Security Hole Advisory

Trusteer
August 13, 2009

Two weeks after Adobe released a critical patch for Flash and Acrobat Reader our research shows that almost 80% of Internet users are still vulnerable. This is the biggest security hole on the Internet today and the failure of Adobe to address it in a timely manner is extremely troubling.

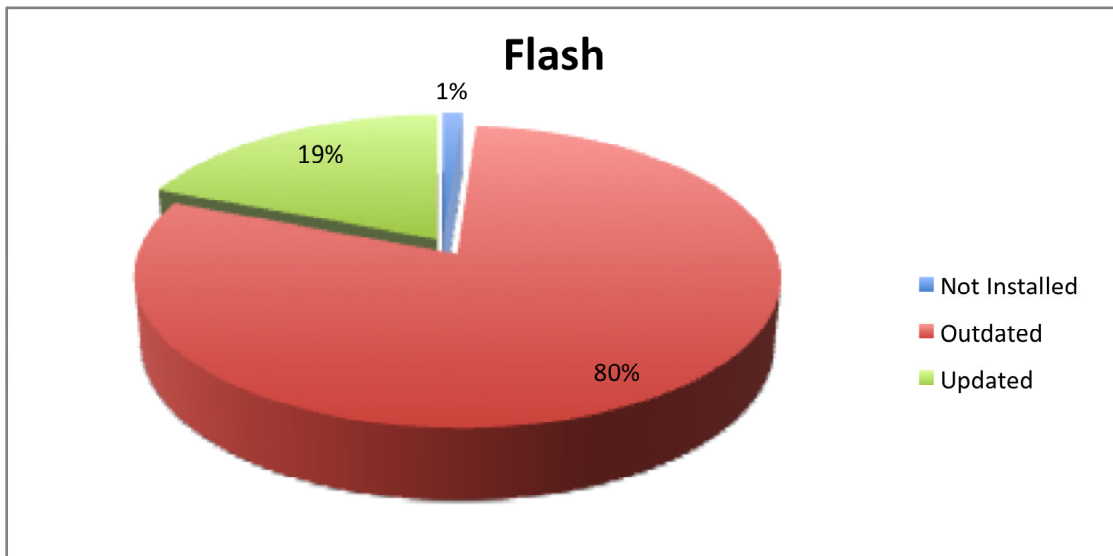
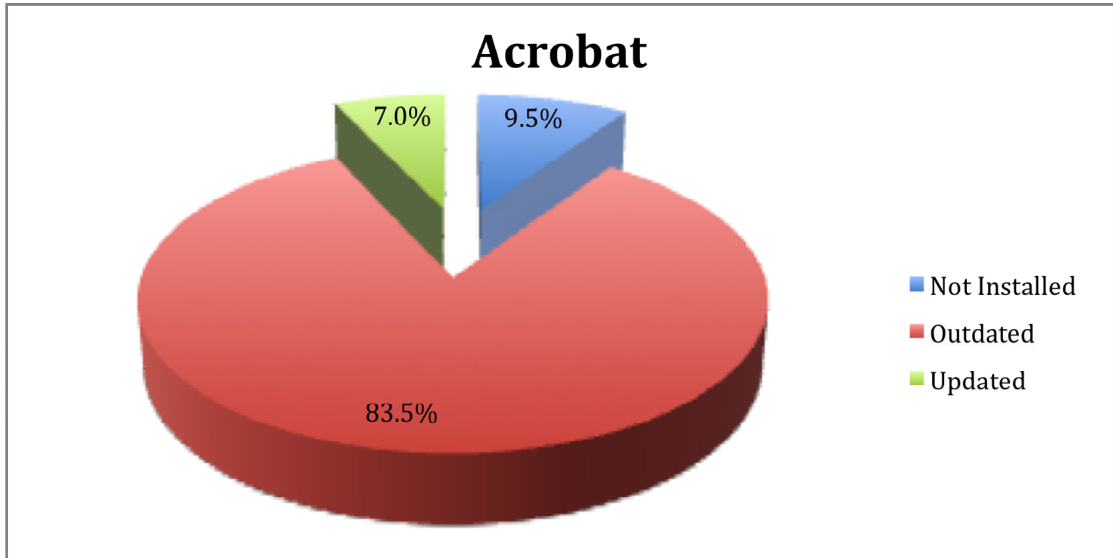
The penetration of Adobe Flash and Acrobat is unparalleled. According to Adobe, 99% of Internet users run Flash (http://www.adobe.com/products/player_census/flashplayer/). The Trusteer security system, which protects more than 2.5 million Internet users in North America and Europe, reports that 98.8% of users have Flash active in their browser.

From a security-avoidance standpoint Flash is the ultimate platform for distributing malware. The malware business consists of a few sub categories. Malware distribution is one of the most important aspects of this business. Criminals can build the most lethal Trojan, but without proper distribution it doesn't pose a real threat to anyone. Over the last three years Trusteer has monitored various Trojans that target financial data. Some of these Trojans were extremely effective in hijacking bank accounts and moving money around, but lacked an effective distribution method. Others had superb distribution, but carried a poor payload. Zbot (<http://www.trusteer.com/poor-antivirusantimalware-coverage-major-malware-threat>) is one example of a Trojan that has achieved broad distribution and causes significant damage. It tops our list in terms of distribution, far more common than any other financial Trojan in the wild today. Zbot uses various distribution methods including Adobe.

Targeting Flash and Acrobat vulnerabilities is extremely efficient since it enables criminals to target 99% of Internet users. By comparison, targeting vulnerabilities in Internet Explorer only reaches approximately 65% of Internet users. While Firefox-based attacks only reach 30%. Given these numbers, it is not surprising that criminals are much more focused today on Flash and Acrobat. Trusteer researchers are seeing more and more malware variants spreading through vulnerabilities in Flash and Acrobat.

According to Adobe, the company is trying to address the problem (http://blogs.adobe.com/asset/2009/05/adobe_reader_and_acrobat_secur.html). However, Adobe is facing some major challenges. One of its biggest hurdles is its software update mechanism, which lags industry standards for effectively distributing security patches to the field.

For example, since the release of Adobe's latest security patch on July 31st (<http://www.adobe.com/support/security/bulletins/apsb09-10.html>), Trusteer researchers have been monitoring systems that run versions of Adobe Acrobat and Flash affected by this fix. Based on findings from over 2.5 million users of our Rapport security service, 79.5% still run a vulnerable version of Adobe Flash and 83.5% run a vulnerable version of Acrobat. At this rate of adoption, users are likely to be running vulnerable versions of these products for a long time to come. Meanwhile, these vulnerabilities are already being exploited in the wild.



This is a serious problem. According to Adobe's advisory: "Critical vulnerabilities have been identified in the current versions of Adobe Flash Player (v9.0.159.0 and v10.0.22.87) for Windows, Macintosh, Linux and Solaris operating systems, and the authplay.dll component that ships with Adobe Reader and Acrobat v9.x for Windows, Macintosh and UNIX operating systems. These vulnerabilities could cause the application to crash and could potentially allow an attacker to take control of the affected system."

In tests conducted by Trusteer to verify whether Windows XP and Mac versions of Adobe Flash had been updated on two random machines, our researchers visited <http://www.adobe.com/software/flash/about/>. Both machines were running older versions 10,0,22,87 (XP) and 10,0,22,87 (Mac), and as such were unpatched. This page indicated that the machines were not running the latest version of Flash, but surprisingly did not issue a notification that the system was at risk and did not strongly urge that the update be installed.

Adobe's software update mechanism does not meet the requirements of a system that is used by 99% of users on the Internet and is highly targeted by criminals. In comparison, Google Chrome and Mozilla Firefox typically achieve an update rate close to 90% and 80% respectively within one week of releasing an update (<http://www.techzoom.net/publications/silent-updates/>)

Internet users and businesses remain at risk until they update to the latest versions of Flash and Acrobat. We believe few people understand the magnitude of this problem. Trusteer recommends that all enterprises and individuals install the updates immediately.