

Web Threat Spotlight

A Web threat is any threat that uses the Internet to facilitate cybercrime.

AUGUST 3, 2009
ISSUE NO. 43

Zero-Day Attacks Escalate

When a security hole is leveraged by cybercriminals before software creators ever have the chance to fix it via a patch, the risk that the attack successfully victimizes users is much greater. These are called zero-day attacks and, in July, we have seen several such attacks targeting popular applications, some of which are often used in common Internet browsing activities.

The Threat Defined

Adobe Reader and Flash Player *authplay.dll* Vulnerability

Adobe Systems, creator of the widely used, cross-platform *Adobe Reader* and *Flash Player*, has made life easier for multimedia creators, enthusiasts, and even casual Internet surfers worldwide. These software are among the many Web-ready applications that are installed in most browsers by users who intend to take advantage of the rich interactivity of Web 2.0 or who simply want to view now-ubiquitous Portable Document Format (.PDF) files.

In July, Trend Micro researchers came across samples that exploited an unpatched vulnerability in *Adobe Reader 9.1.2* and *Adobe Flash Player 9* and *10*. The exploit arrives inside a .PDF file embedded with Flash objects and malicious binary files. The Flash object contains a shell code that allocates large sections of unused blocks in a system's memory, a technique known as "heap spraying." It exploits a critical vulnerability in the interaction between *Adobe Flash Player 9* and *10* and *authplay.dll*, a component in *Adobe Reader 9.1.2*. Adobe immediately issued security bulletin [APSA09-03](#) upon learning of the in-the-wild attacks.

The .PDF file, one sample of which is detected by Trend Micro as [TROJ_PIDIEF.ANP](#), drops *SVCHOST.EXE* and *Temp.exe* in the current user's *Temp* folder. *SVCHOST.EXE* is actually a backdoor ([BKDR_AGENT.YTET](#)) while *Temp.exe* is a Trojan ([TROJ_AGENT.AXWS](#)).

The backdoor creates registry entries to ensure its automatic execution at every system startup. It drops a file with a random file name inside the Windows system folder. It then injects the dropped file into the legitimate *SVCHOST.EXE* application. It uses port 4000 to establish a connection to certain sites and to receive commands from a remote user. This allows cybercriminals to take control of the computer. Furthermore, the backdoor drops *sysmon.sys*, which is actually a rootkit component ([RTKT_AGENT.YTET](#)) that helps hide the backdoor so that users cannot easily identify its presence on a system.

The Trojan [TROJ_AGENT.AXWS](#), meanwhile, drops and executes a .PDF file named *Cao Chang-Ching The CPP made eight mista* in the current user's *Temp* folder. After this routine it deletes itself from the system.

The infection chain above is one of two that starts with the exploitation of the *authplay.dll* vulnerability. The other sample is [TROJ_PIDIEF.ANQ](#), which also involves a backdoor, a Trojan, and a rootkit.

When the attacks first ensued, Adobe was not able to immediately provide a patch for the said vulnerability but did offer a workaround, which required users to disable all Flash objects



ADOBE EXPLOIT INFECTION DIAGRAM

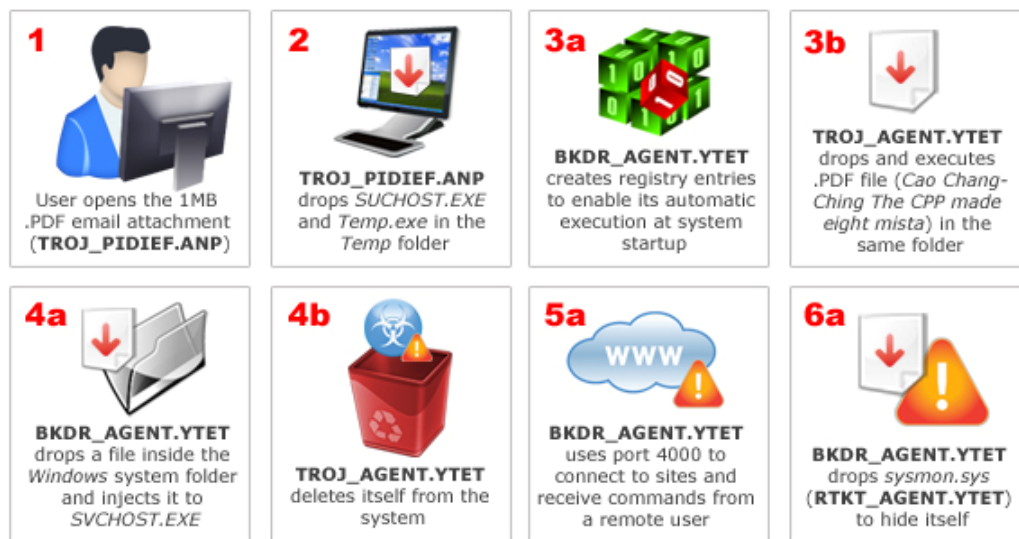


Figure 1. The same components were also utilized in the second Adobe vulnerability exploit attack.

Web Threat Spotlight

A Web threat is any threat that uses the Internet to facilitate cybercrime.

embedded in .PDF files. This practice, however, may not be acceptable to some users but since patches from Adobe were not expected until the end of the month, these users had no choice.

Browser-Related Vulnerabilities in July

July has been an exceptionally busy month for zero-day exploits. Early in the month, an [exploit involving ActiveX controls](#) was used to spread FAKEAV malware. This exploit took advantage of a vulnerability in Microsoft OSs' *Office Web Components (OWC) Spreadsheet ActiveX control* (OWC 10 and 11). The exploit seemed to have used script fragmentation—the same tactic used in a previous [zero-day mass Web compromise](#). In such an attack, the parts of the whole malicious script may not necessarily be malicious per se but when combined, the outcome—a full working exploit—can prove disastrous.

Just days ago, this was followed by an [exploit affecting Mozilla Firefox](#). This attack corrupted certain browser versions' (i.e., *Firefox 3.5*) just-in-time (JIT) compiler features, rendering them useless or vulnerable to arbitrary code run by a remote malicious user.

User Risks and Exposure

Zero-day exploits can ultimately result in the loss of Internet users' online identities, personal information, and financial assets. Backdoors can receive and perform virtually any given command from cybercriminals. Although as of this writing, the server the backdoor connects to is down, it can come alive anytime and start delivering commands.

The *authplay.dll* vulnerability is present in versions 9.0.159.0 and 10.0.22.87 of the *Adobe Flash Player* and the *authplay.dll* component in all versions 9.x of *Adobe Reader* and *Acrobat*. The illustrated attack can take advantage of the said vulnerability without the need for user interaction apart from opening the specially crafted .PDF file.

Trend Micro Solutions and Recommendations

Trend Micro [Smart Protection Network™](#) delivers security that is smarter than conventional approaches. It blocks the latest threats before they reach you. Leveraged across Trend Micro's solutions and services, Smart Protection Network combines unique in-the-cloud technologies and a lightweight client architecture to immediately and automatically protect your information wherever you connect. It is also the only antivirus technology that is able to correlate threats and identify their individual roles in an entire threat. In this particular attack, Smart Protection Network protects users in that downloaded files (TROJ_PIDIEF.ANQ and TROJ_PIDIEF.ANP) and the files they drop (BKDR_AGENT.YTET, TROJ_AGENT.AXWS, and RTKT_AGENT.YTET) are detected by File Reputation technology.

Users are advised to be wary of using add-on functions such as ActiveX controls and opening attachments that have suspicious-looking file names or come from unknown senders to avoid becoming victims of similar attacks. They should always install or upgrade to the latest versions of all the applications they use once updates are released by their corresponding vendors to avoid unnecessary risks. Adobe, has, for instance, released a patch for the said vulnerability. It can be downloaded from the [Adobe website](#).

The following posts at the *TrendLabs Malware Blog* discuss this threat:

<http://blog.trendmicro.com/ocw-activex-exploit-follows-mpeg2tunerequest%e2%80%99s-lead/>

<http://blog.trendmicro.com/more-zero-day-exploits-for-firefox-and-ie-flaws/>

<http://blog.trendmicro.com/2009/07/24/>

<http://blog.trendmicro.com/another-messy-mass-compromise-emerges/>

The virus reports are found here:

http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_PIDIEF.ANQ

<http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=BKDR%5FAGENT%2EYTET&Vsect=T>

<http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FAGENT%2EAXWS&Vsect=T>

<http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=RTKT%5FAGENT%2EYTET&Vsect=T>

http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_PIDIEF.ANP

Other related posts are found here:

http://www.computerworld.com/s/article/9135796/Adobe_confirms_Flash_zero_day_bug_in_PDF_docs

<http://www.adobe.com/support/security/advisories/apsa09-03.html>

<http://blogs.adobe.com/psirt/>

