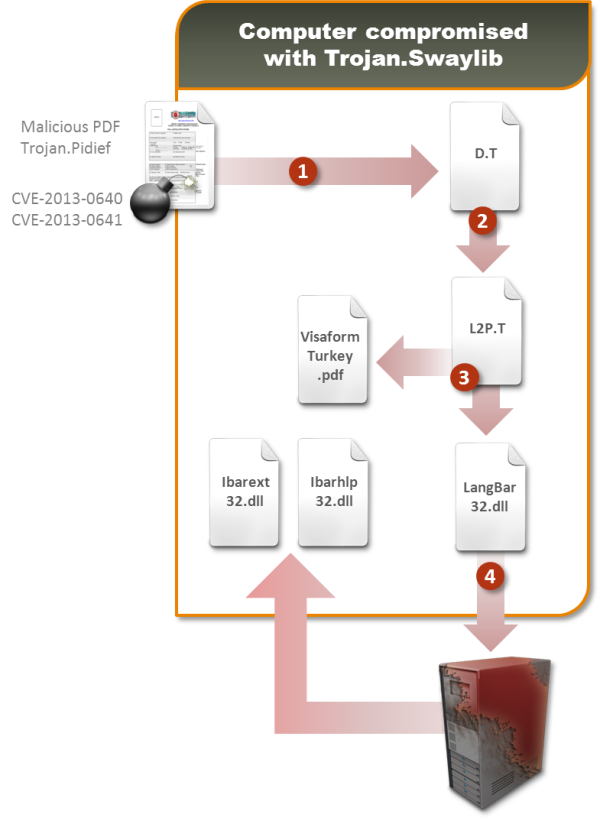
**New Adobe PDF Zero-day Unleashes Trojan.Swaylib**

Created: 14 Feb 2013 22:16:55 GMT • Updated: 23 Jan 2014 18:09:35 GMT • Translations available: [日本語](http://www.symantec.com/connect/blogs/adobe-pdf-trojanswaylib)

In a previous [blog](http://www.symantec.com/connect/blogs/new-adobe-vulnerabilities-being-exploited-wild), Symantec reported on a new Adobe zero-day vulnerability ([CVE-2013-0640](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0640), [CVE-2013-0641](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0641)) affecting Adobe Reader and Acrobat XI (11.0.1) and earlier versions, that was being actively exploited in the wild. Adobe has yet to release a patch for this zero-day, but in an [advisory](http://www.adobe.com/support/security/advisories/apsa13-02.html) they have provided a means of mitigation against the attack.

The initial report on this zero-day being actively used in the wild came from [FireEye](http://blog.fireeye.com/research/2013/02/in-turn-its-pdf-time.html). They [reported](http://blog.fireeye.com/research/2013/02/the-number-of-the-beast.html) that several files were being dropped and downloaded as a result of a successful exploit. Our research can confirm these findings.



***Figure 1.*** *Attack using CVE-2013-0640*

The steps in the attack, shown in Figure 1, are as follows:

1. A malicious PDF file drops a DLL file called D.T
2. D.T decrypts and drops a DLL file called L2P.T
3. L2P.T creates run keys and then drops and opens a clean PDF file. It also drops downloader component LangBar32.dll
4. LangBar32.dll contacts a malicious server and downloads additional malware with back door and key logging capabilities

Symantec has antivirus detections in place for the stages of this attack as [Trojan.Pidief](http://www.symantec.com/security_response/writeup.jsp?docid=2009-121708-1022-99) and [Trojan.Swaylib](http://www.symantec.com/security_response/writeup.jsp?docid=2013-021418-2701-99) (initially detected as [Trojan Horse](http://www.symantec.com/security_response/writeup.jsp?docid=2004-021914-2822-99)). The intrusion prevention signature (IPS) [Web Attack: Malicious PDF File Download 5](http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=26465) has also been released to detect usage of this specific Adobe exploit in further attacks.

Additional research has shown that the PDF used in this attack would have been caught by our [Symantec Mail Security for Microsoft Exchange](http://www.symantec.com/mail-security-for-microsoft-exchange) product and the dropped files used in this attack would have been detected as [WS.Malware.2](http://www.symantec.com/security_response/writeup.jsp?docid=2011-040714-3811-99) by Symantec’s cloud based detection technology.

Symantec is currently investigating further protections for this zero-day and will provide an update to this blog when possible. To protect against potential zero-day threats, Symantec recommends that you use the latest [STAR Malware Protection Technologies](http://www.symantec.com/page.jsp?id=star) to ensure the best possible protection is in place.