KASPERSKY

Automatic Exploit Prevention Technology

Kaspersky Lab's approach to security is based on multiple layers of protection. The majority of malicious programs are stopped in the first layer – for example, they may be caught by signature-based detection. Some malicioius objects, though, require special treatment: we have to ensure that even if they bypass one layer of security, they will be detected by another. For example, if a complex piece of malware is brand new and its signature is not known yet, it can still be blocked by Kaspersky Security Network, which collects information about fresh cyberattacks from millions of users and acts on it rapidly. The next layer is a wide range of proactive protection technologies that analyze the code of suspicious applications. Even if an application has managed to launch itself on the protected system, its actions will be tracked, and dangerous activity will be blocked by the System Watcher module.

Then there is one more area of cybercrime that we believe needs its own special new layer of protection: exploits for vulnerabilities in popular programs. Cybercriminals utilize well-known as well as new ("zero-day") vulnerabilities in software like Adobe Flash, Adobe Reader, Java Runtime Environment, web browsers and core Windows components as a gateway to launch malicious code on victim's PCs. The vulnerability exploits are widely used in malware, but also form the basis of targeted attacks that can be hard to discover and block using conventional protection methods. Our specialized layer of protection is based on technology called *Automatic Exploit Prevention* and is a brand new and very efficient way of detecting new and unknown exploits.

Typical exploit behavior

The purpose of any exploit is to trigger certain vulnerabilities in software in order to launch various types of malicious code. In order to infect a system via vulnerable software, a user must be lured on to a malicious website (or a legitimate one which has been doctored to contain a malicious module), or download and open a specifically crafted document (Office document, PDF file or even an image which may seem harmless). Malicious links to infected web pages or files may be distributed via email, instant messaging or social networks and can even be found in the search results for popular queries. Typical targeted attacks frequently start when a user opens a specifically crafted email attachment which often looks completely legit at first sight.

The most attacked software

Almost every program is vulnerable to software bugs, and some of those may lead to unauthorized execution of malicious code. But cybercriminals usually target only those programs which are installed on almost every PC – guaranteeing a large number of potential victims. According to Kaspersky Lab <u>statistics</u>, in 2011 the list of software most targeted by exploits included these programs or components:



On this chart you can see that Adobe Reader was clearly the most attacked software. Java Runtime Environment was in second place, and the Windows operating system itself occupied third place with 11% of recorded attacks. One-fifth of all attacks used other software. It means that for a targeted attack a cybercriminal may exploit a vulnerability which is rarely used or even unknown. Over time the list of the most targeted software may change. For example, in 2010 the most frequently attacked software was Microsoft Office, Java and Adobe Flash. In the first quarter of 2012 Kaspersky Lab's products blocked more than 1 million files containing exploits each month. Taking into account that most web pages containing exploits were blocked by Web Antivirus, the danger of this side of cybercriminal activity should not be underestimated.

General means of protection from exploits

Protection solutions like Kaspersky Internet Security utilize different methods to help block exploits. Special signatures are added for exploits that help to detect malicious files (for example, in an email attachment) even before it is opened. Proactive protection and other technologies allow the malicious payload to be detected and blocked after the vulnerable file was opened. Finally, a Vulnerability Scan feature allows users to find the vulnerable software and advises on how to update it. Of course, performing regular updates of Windows system components and installed software is the best way to avoid most exploits.

In some cases general protection techniques may not be effective. This is especially true when it comes to zero-day vulnerabilities – those which are either unknown or very recently discovered. In this case it is hard for security vendors to recognize exploits targeting a zero-day vulnerability using signature-based methods. Complex exploits may also use a number of techniques to overcome proactive protection technologies. Even if relatively few threats are capable of escaping from traditional protection, the huge damage they can wreak makes it essential to introduce an additional layer of security – and that's where Automatic Exploit Prevention comes in.

How Automatic Exploit Prevention works

Automatic Exploit Prevention technology specifically targets malware that utilizes software vulnerabilities. Its development started from thorough analysis of the behavior and features of the most widespread exploits. This research has helped to identify specific types of exploit behavior that help to distinguish this kind of malware from other malicious and legitimate programs. Besides that, it was possible to take into account the most frequently targeted software during the development of this software. As the result, new versions of Kaspersky Internet Security and Kaspersky Anti-Virus will feature Automatic Exploit Prevention in addition to the standard System Watcher module and will offer the following new security techniques.



Control potentially vulnerable applications

Automatic Exploit Prevention technology pays specific attention to the most frequently targeted programs, such as Adobe Reader, Internet Explorer, Microsoft Office, etc. Any attempt by these programs to launch suspicious executable files or code is the starting point for additional security checks. Such action may be legitimate – for example, Adobe Reader may launch another executable file to check for updates. But certain characteristics of the executable file, as well as actions that took place prior to the attempted launch may point to malicious activity.

Monitor prior actions before the launch attempt

Information about program activity before the attempt to launch suspicious code can also be used to identify malware. Automatic Exploit Prevention technology tracks this activity and discovers the source of the attempt to launch the code. The source may originate from the software itself, but may also be the result of the actions of an exploit. The data on the most typical exploit behavior also helps to detect this even in the case of a zero-day vulnerability being used.

Tracking the origin of code

Certain exploits, especially those used in drive-by downloads (when the exploit is launched by visiting a malicious web page) fetch the payload from a certain website before executing it. Automatic Exploit Prevention tracks the origin of files, knows the exact browser that initiated the download and the remote web address for the files. In addition, for certain programs Automatic Exploit Prevention can distinguish between files created with the consent of the user and unauthorized new files. When an attempt to launch suspicious code is made, this information helps to determine the actions of an exploit and block it.

Prevent the use of potential vulnerabilities

For a number of programs and software modules, Automatic Exploit Prevention will use a mode called "Forced Address Space Layout Randomization". The ASLR technology is also used by the Windows operating system (starting from Windows Vista), but Kaspersky Lab's technology extends it to those programs which do not support the default one. As a result, certain exploits will not be able to utilize the vulnerability, because the location of the malicious code in memory, otherwise static, will be unknown to them.

Availability

Automatic Exploit Prevention technology is available in 2013 versions of Kaspersky Internet Security and Kaspersky Anti-Virus. In these products it is activated when using the default settings, but can also be turned off separately or along with the entire System Watcher module that keeps tracks of program activity in the system in general. By default, Automatic Exploit Prevention blocks the launch of any suspicious code: the methods introduced by this new technology make the chances of false positive detection very low. This feature can be run in interactive mode as well.

Benefits

Automatic Exploit Prevention significantly reduces the chances of being infected by widespread malware or becoming the victim of a targeted attack using exploits, even in the case of a zero-day vulnerability being used. During internal testing the technology successfully blocked exploits using widely used vulnerabilities in Adobe Flash Player, QuickTime Player, Adobe Reader, Java and other programs. One of the most notable examples of the effectiveness of this technology is the successful detection of an exploit that utilizes one of the most recent vulnerabilities found in Windows Media Player. The <u>vulnerability</u> was discovered in January 2012 and affected all versions of Windows, starting from Windows XP. It allowed remote code execution using a specially crafted .MIDI file – a music file that may seem completely harmless to the user.

Automatic Exploit Prevention targets the most complex or previously unknown exploits: widespread malicious objects will be blocked by other security systems, such as Web Anti-Virus, File Anti-Virus or even the Anti-Spam filter. Therefore, it significantly enhances the overall security of the end user.

