KASPERSKY lab

KASPERSKY LAB'S AUTOMATIC EXPLOIT PREVENTION TECHNOLOGY

Be Ready for What's Next

www.kaspersky.com

1. THE NEW INSIDER THREAT

Third party applications accounted for a massive 87 % of vulnerabilities in 2012.[1] That same year, Kaspersky Lab recorded more than 132 million applications at risk.

"Kaspersky Lab believes that the best way to address this rapidly evolving threat is through a dedicated technology that offers its own unique layer of protection against exploits aimed at vulnerabilities in popular applications."

Flaws in Oracle Java, Adobe Flash Player and Adobe Reader, along with weaknesses in Microsoft Office, are the most popular targets for criminal exploits. Between March and August 2013, Kaspersky Lab researchers registered 8.54 million attacks using Java exploits – an increase of 52.7 percent on the previous six months.

Kaspersky Lab believes that the best way to address this rapidly evolving threat is through a dedicated technology that offers its own unique layer of protection against exploits aimed at vulnerabilities in popular applications. By preventing these malicious pieces of code from executing in the first place, it's possible to prevent core enterprise applications and components from becoming gateways for larger scale attacks.

1 Secunia Vulnerability Review 2013, Secunia Research Lab, March 14, 2013.

2. THERE'S A GAP FOR THAT – TYPICAL EXPLOIT BEHAVIOR

The purpose of any exploit is to leverage vulnerabilities in widely used software to launch various types of malicious code. To infect a system using this technique, criminals adopt a range of methods, including:

- Luring users onto a purpose-built malicious website or legitimate one that has been compromised and infected with malicious code. Some criminals target legitimate sites popular with particular types of users, such as developers in large enterprises – so-called watering hole attacks.
- Duping users into downloading or opening a specially crafted, seemingly legitimate document, such as a PDF, Office document or even a harmless-looking image.
- Removable storage devices such as USB drives carrying exploit-using malware are easily smuggled into the enterprise – several studies in recent years have found that end users who found USB sticks in the company parking lot invariably plugged them into their computer, especially if they were enterprise branded.[2]

Typically, targeted attacks begin with a user opening a specially crafted malicious email attachment that looks legitimate at first sight.

2 Bruce Schneier, "Yet Another 'People Plug in Strange USB Sticks' Story," Schneier on Security, https://www.schneier.com/blog/archives/2011/06/yet_another_peo.html

For further information on exploits delivered via removable media, visit: http://www.securelist.com/en/blog/208187475/Another_usb_media_infection

3. POPULARITY MAKES YOU VULNERABLE – THE MOST ATTACKED SOFTWARE

Almost every program is vulnerable to bugs, some of which enable the unauthorized execution of malicious code. Given that the average user has about 72 programs installed on his or her machine,[3] that's a lot of vulnerability in the enterprise. But the reality is that criminals tend to stick to the most popular applications because this guarantees a large number of potential victims; after all, to be successful, you only need one person to click...

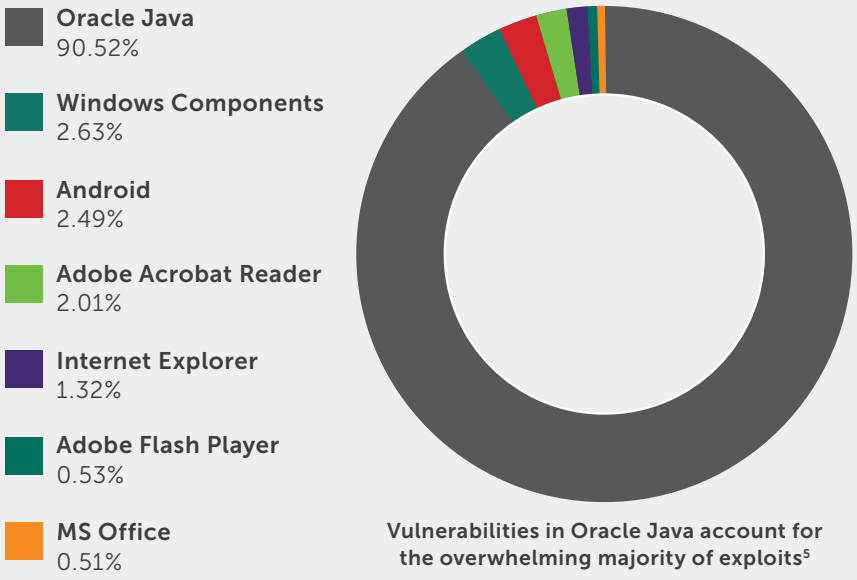
"Of the Kaspersky Lab users participating in our cloud-based Kaspersky Security Network intelligence and threat detection system, 6.3 percent are still using Windows XP."

Kaspersky Lab research shows the software most targeted by exploits is Oracle Java, which accounted for 90.52 percent of all detected attempts to exploit vulnerabilities in 2013. These vulnerabilities are exploited by drive-by attacks using the Internet, and new Java exploits are now present in lots of exploit packs.[4]

The second most popular vulnerability target is the Windows components category, including vulnerable Windows OS files other than Internet Explorer and Microsoft Office, which Kaspersky assigned to a separate category. Most of the attacks in this components category target a vulnerability discovered in win 32k.sys-CVE-2011-3402 – first used in the famous Duqu exploit.

3 Secunia Vulnerability Review 2013.

4. Kaspersky Lab Report: Java Under Attack – The Evolution of Exploits in 2012-2013, Securelist, October 30, 2013, http://www.securelist.com/en/analysis/204792310/Kaspersky_Lab_Report_Java_under_attack_the_evolution_of_exploits_in_2012_2013.



Vulnerabilities in Oracle Java account for the overwhelming majority of exploits[5]

Over time, the list of targeted software may change; for example, Microsoft Office was the number one target for attack in 2010. As Microsoft transitions Windows XP and Office 2003 toward end of life from April 2014, security updates and patches will no longer be developed for this software, leaving some organizations exposed to serious weakness that criminals are no doubt already eyeing up. Of the Kaspersky Lab users participating in our cloud-based Kaspersky Security Network intelligence and threat detection system, 6.3 percent are still using Windows XP.

5 http://www.securelist.com/en/images/vlill/stat_ksb_2013_04.png

4. GENERAL MEANS OF PROTECTION FROM EXPLOITS

Kaspersky Lab's solutions employ several methods of blocking exploits. For example, special signatures are added for exploit-using malware that enable malicious file detection (such as an email attachment) even before the file is opened. Proactive protection and other technologies enable detection and blocking of malware once a vulnerable file is opened. Finally, Vulnerability Scanning enables the easy detection of vulnerable software on any endpoint – and can work in concert with Patch Management and other Systems Management features to automatically apply updates or prevent unpatched software from loading.

"Even if relatively few threats escape the traditional security layers, the potential for massive damage that even one exploit slipping through the net could cause makes it vital to introduce an additional layer of security to the enterprise."

Of course, performing regular updates of Windows system components and other installed software is the best way to avoid most exploits.

In some cases, however, everyday protection techniques may not be effective. This is especially true of zero-day vulnerabilities – undetected or newly discovered software flaws. Under these circumstances, it's difficult for security vendors to recognize exploits targeting zero-day vulnerabilities through signature-based methods. Complex exploits may also use a variety of techniques to bypass or overcome proactive protection technologies. Even if relatively few threats escape the traditional security layers, the potential for massive damage that even one exploit slipping through the net could cause makes it vital to introduce an additional layer of security to the enterprise. That's where Automatic Exploit Prevention comes in.

5. AUTOMATIC EXPLOIT PREVENTION: HOW IT WORKS

Automatic Exploit Prevention technology specifically targets malware that exploits software vulnerabilities to gain a toehold on enterprise endpoints and networks. Even if a user downloads or opens a malicious file, AEP technology will prevent the malware from executing.

Kaspersky developed AEP through in-depth analysis of the behaviour and features of the most widespread exploits. This means our technology can discern exploit-characteristic behaviour patterns and block them from completion.

During the development process, Kaspersky's R&D teams gained insight into the most frequently targeted enterprise software and applications, tailoring the AEP technology accordingly. AEP now features in Kaspersky Lab's Antivirus and Internet Security solutions, where it works alongside our standard System Watcher module to deliver an additional layer of security that includes the following capabilities:

CONTROL OF POTENTIALLY VULNERABLE APPLICATIONS

AEP technology gives specific focus to the most frequently targeted applications, such as Adobe Reader, Internet Explorer and Microsoft Office. Any attempt these programs make to launch unusual executable files or code will trigger additional security checks. Sometimes, these actions will be legitimate – for example, Adobe Reader may launch an executable file to check for updates. But certain characteristics of the executable file, along with any associated actions, may be indicative of malicious activity and therefore worthy of additional examination.

MONITOR PRE-LAUNCH ACTIVITIES

How an application launches or code executes – and what happens just before it does so – can reveal a lot about it. Certain kinds of behaviour strongly indicate malicious activity; AEP technology can track this activity and detect the source of the attempt to launch the code. The source may originate with the software itself – but it could also be the result of an exploit. Data on the most typical exploit behaviours can help detect this kind of activity, even when a zero-day vulnerability is being used. This means AEP doesn't need to know the precise nature of the vulnerability being exploited to understand that malicious activity is taking place.

TRACKING THE ORIGIN OF CODE

Certain types of exploit, particularly those used in drive-by downloads (i.e., exploits launched through a malicious web page), need to fetch their payload from another website before executing it. AEP can trace the origin of such files, identify the exact browser that initiated the download and retrieve the remote web address for the files.

"Kaspersky's methodology of checking and tracking, along with in-depth and ongoing research into the most popular enterprise applications, makes the risk of false positives very low. It's possible to run this feature in interactive mode, if preferred. "

In addition, for certain kinds of programs, AEP can distinguish between files created with the user's consent and unauthorized new files. When an attempt is made to launch suspicious code, this information can help identify an exploit and block it.

PREVENT EXPLOITS FROM ACCESSING THEIR CHOSEN VULNERABILITY

AEP can use a technique called Forced Address Space Layout Randomization with some programs and software modules, preventing exploits from finding the specific vulnerability or code they need to execute.

Address space layout randomization (ASLR) technology has been included in Microsoft's Windows operating system since Vista but not all programs support this default feature. Kaspersky's AEP technology extends the functionality of ASLR to programs that don't support this default version – blocking certain exploit types by preventing them from determining the location of the code they need to operate for example, in memory. Repeated efforts to locate the required code are more likely to result in the application crashing than they are in the malicious code executing.

Where to Find AEP

Automatic Exploit Prevention technology is available as part of Kaspersky Endpoint Security for Business. It's activated by default, but can be turned off separately or along with the entire System Watcher module (which tracks program activity across the system), if desired.

By default, AEP blocks the launch of any suspicious code; Kaspersky's methodology of checking and tracking, along with in-depth and ongoing research into the most popular enterprise applications, makes the risk of false positives very low. It's possible to run this feature in interactive mode, if preferred.

6. THE BENEFITS TO ENTERPRISE IT SECURITY

Automatic Exploit Prevention significantly reduces the risk of infection from widespread malware, or more targeted attacks using exploits – even when a zero-day vulnerability is used. During Kaspersky Lab's extensive internal testing, research and development processes, AEP successfully blocked exploits targeting widely used vulnerabilities in Adobe Flash Player, QuickTime Player, Adobe Reader, Java and other programs.

Kaspersky Lab's approach to IT security has always been based on providing multiple layers of protection, along with the effective use of threat intelligence to anticipate the nature of as-yet-unknown threats. Automatic Exploit Prevention blocks both known and unknown exploits from executing. In doing so, it complements Kaspersky's other technologies, such as antivirus and anti-spam filters, by providing a safety net to catch more complex or sophisticated code that can sometimes bypass traditional IT security technologies.

Kaspersky never stops anticipating and preventing IT security threats – reducing enterprise risk today and in the increasingly complex future.

About Kaspersky

Organizations need intelligent security technologies to protect their data – and they also need intuitive and uncomplicated IT efficiency tools. Kaspersky Lab's 2,500 employees are driven to meet those needs for the 300 million plus systems they protect – and the 50,000 new systems a day that are added to their number.

Kaspersky Systems Management is a component of Kaspersky Endpoint Security for Business. Combining award-winning anti-malware, IT policy enforcement tools, centralized management and cloud-assisted protection, Kaspersky's business security products are the right choice for your organization.

Talk to your security reseller about how Kaspersky can bring secure configuration to your networks, the devices that run on them – and more!

kaspersky.com/business

SEE IT. CONTROL IT. PROTECT IT.

With Kaspersky Lab, now you can.

Twitter.com/
Kaspersky

Facebook.com/
Kaspersky

Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

KASPERSKY lab