KASPERSKY lab

Zero-day, Exploit and Targeted Attack (ZETA) Shield Technology

Targeted attacks on key employees at companies, or even on ordinary home users, are today among the most serious threats facing corporate networks. These attacks are different: they involve teams of well-trained cybercriminals, able and willing to spend significant amounts of time and money on thorough preparation.

As a rule, targeted attacks take advantage of vulnerabilities or flaws in the code of popular applications that have not as yet been discovered, known as 'zero-day' vulnerabilities. In fact, a large proportion of the time cybercriminals spend preparing attacks is devoted to searching for such vulnerabilities. Once a vulnerability has been identified, the programmers take over and create dedicated program code, called an exploit, that uses the vulnerability to take control of the victim's computer, plant malware on it and perform other tasks. These exploits are generally hard to detect using run-of-the-mill antivirus software, including both reactive and proactive methods. In the case of a targeted attack, the situation is even more complicated. Since relatively few computers are attacked, there is no infection outbreak that could normally be used to help identify malware early on using statistical methods. Unfortunately, it is not always possible to obtain an exploit sample quickly from one source, such as an infected computer.

One example of zero-day vulnerabilities being exploited in the corporate sector was an attack on several industrial companies carried out by unknown perpetrators. The cybercriminals gathered the email addresses of about 20 employees and sent them emails with malicious PDF files attached. If a recipient opened the file using Adobe Reader, the exploit embedded in the document downloaded a Sykipot family Trojan and installed it on the computer. The exploit targeted a vulnerability in Adobe Reader which had been unknown before the incident in question and which was closed soon after.

Although zero-day vulnerabilities are often used in targeted attacks, employees who do not have access to any valuable data, as well as ordinary users, also need protection against this type of threat. Exploits are not just tools that cybercriminals can use for targeted attacks against an organization; they can also be used for mass-infections of computers to steal or destroy data.

Home Users

Home users can be compromised too. In fact, they are more vulnerable to targeted attacks because they usually rely on one of the various Internet Security solutions available on the market that are not equipped with high-end tools for detecting unknown threats. Meanwhile cybercriminals often use zero-day vulnerabilities in popular applications to infect PCs with Trojans and viruses in order to steal money from online banking accounts or sensitive personal data.

Since cybercriminals devote considerable effort to finding new ways of infecting user machines, including the development of new exploits capable of avoiding detection by traditional antivirus technologies, it is impossible to protect a home computer or employee workstation without sophisticated proactive technologies. The only effective solution for companies in this situation is to deploy multi-tier protection in order to block malicious objects on employee workstations as well as the local corporate network, and in email and network

traffic. Home users are advised to find an Internet Security solution that can proactively detect zero-day vulnerabilities.

ZETA Shield technology

The ZETA Shield technology developed by Kaspersky Lab is designed to counteract targeted attacks. It scans the data stream for code fragments characteristic of exploits built into legitimate files. This can be executable code in the body of an office document or an attempt to call commands that are not typically used by the file type in question. The technology includes numerous parsers, i.e., modules that apply different mechanisms to analyze code depending on each file's actual contents and on the context.

ZETA Shield works with data streams instead of individual files. It means conducting more in-depth analysis of incoming data, identifying non-standard elements and the connections between them, which may be indirect indicators of potential threats. This is an important feature that distinguishes ZETA Shield from analysis methods used in traditional file antivirus solutions, which sees the objects being analyzed broken up into components to be studied separately.

ZETA Shield technology uses updatable heuristic rules to provide targets for analysis, define scanning rules and calculate results using effective mathematical methods. Technology updates are created by a dedicated group of Kaspersky Lab analysts which studies various techniques used by exploits to spread and penetrate victim machines. This enables ZETA Shield to provide a rapid response to current threats and ensure a higher level of protection. It is also important to mention that ZETA Shield constantly communicates with the Kaspersky Security Network cloud service. This service gathers the latest data about new threats and makes it available to Kaspersky Lab customers. Each time ZETA Shield anonymously sends any new piece of information about suspicious file or code, heuristic rules developed by Kaspersky Lab analysts become more specific and sophisticated. The more data Kaspersky Security Network gathers about threats, the stronger Kaspersky Lab protection becomes.

Advantages

By using antivirus products that feature the ZETA Shield technology, a company or a home user can significantly lower the cybercriminals' chances of conducting a successful targeted attack, keep computers from being infected with malware and hence prevent leaks of sensitive data and damage to the IT infrastructure. The main advantages of the technology are:

- A high level of protection. ZETA Shield detects and blocks targeted attack attempts against a company or a home computer. The technology can also interact with other Kaspersky Lab security solutions, providing maximum protection.
- Multistreaming. The technology can process numerous data streams at the same time and easily adapts to existing corporate infrastructure and available hardware resources.
- Feedback. Interaction with the Kaspersky Security Network cloud service enables ZETA Shield to respond to new threats quicker.

In the process of developing the technology, emphasis was placed on the ability to cope with a heavy workload. ZETA Shield can effectively track and block malicious objects in email or network traffic. This is the main feature that distinguishes the technology from other proactive methods of protection used in Endpoint Security and Internet Security solutions that process relatively small volumes of data on employee workstations or home PCs.

Availability

ZETA Shield technology is currently included in Kaspersky Security for Linux Mail Server, a solution designed to protect corporate mail traffic. The technology works in synergy with other systems that analyze mail traffic and filter spam, offering businesses enhanced protection against targeted attacks. The technology is also available in the latest versions of Kaspersky Lab's consumer products: Kaspersky Anti-Virus, Kaspersky Internet Security and Kaspersky Internet Security – Multi-Device. ZETA Shield will also be incorporated into other corporate and consumer products to be released by Kaspersky Lab in the near future.