

ZERO DAY VIRUSES TOXICITY AND WAYS TO COMBAT THEM

Definition

0-day is a term for unresolved vulnerabilities, as well as malware against which no defense mechanisms have yet been developed.

The term itself means that the developers had 0 days to fix the defect: a vulnerability or attack becomes publicly known until the software manufacturer releases bug fixes (that is, the vulnerability can potentially be exploited on running copies of the application without the ability to protect against it).

Vulnerability detection

At the moment, many virus writers are focusing their efforts on finding unknown vulnerabilities in software. This is due to the high efficiency of vulnerability exploitation, which, in turn, is associated with two facts - the high prevalence of vulnerable software (it is such software that is usually attacked) and a certain time interval between the discovery of the vulnerability by the software company and the release of the corresponding update for bug fixes. To detect vulnerabilities, virus writers use various techniques, for example:

1. Disassembly of program code and subsequent search for errors directly in the software code;
2. Reverse engineering and subsequent search for errors in software algorithms;
3. Fuzz testing is a kind of stress test for software, the essence of which is the processing by software of a large amount of information containing deliberately incorrect parameters;
4. Creation of malicious code.

After a vulnerability is discovered in the software, the process of developing malicious code begins that uses the discovered vulnerability to infect individual computers or computer networks.

As of 2017, the most famous malware exploiting the 0day vulnerability in software is the WannaCry network ransomware worm, which was discovered in May 2017. WannaCry used the EternalBlue exploit in the SMB (Server Message Block) vulnerability on Windows operating systems. Upon a successful attempt to infiltrate a computer, WannaCry installs the DoublePulsar backdoor for further manipulation and action. Also, the equally well-known Stuxnet worm exploited a previously unknown vulnerability of Windows operating systems related to the shortcut

processing algorithm. It should be noted that, in addition to the 0day vulnerability, Stuxnet exploited three more previously known vulnerabilities.

In addition to creating malicious programs that exploit 0 day vulnerabilities in software, virus writers are actively working on creating malicious programs that are not detected by antivirus scanners and monitors. These malicious programs also fall under the definition of the term 0day.

The lack of detection by antivirus programs is achieved due to the use of technologies such as obfuscation, encryption of program code, etc. by virus writers.

Protection

Due to the use of special technologies, 0day threats cannot be detected by classic anti-virus technologies. It is for this reason that products that rely on classic antivirus technologies perform poorly in dynamic antivirus tests.

According to antivirus companies, proactive antivirus technologies must be used to provide effective protection against 0day malware and vulnerabilities. Due to the specifics of proactive protection technologies, they are able to provide protection against both known threats and 0day threats equally effectively. However, it should be noted that the effectiveness of proactive protection is not absolute, and a significant proportion of 0day threats can harm victims of cybercriminals. At the moment, there is no independent confirmation of these statements.