Kaspersky Lab uncovers third Windows zero day exploit in three months

Kaspersky Lab technologies have automatically detected a new exploited vulnerability in the Microsoft Windows OS kernel, the third consecutive zero-day exploit to be discovered in three months.

Kaspersky Lab technologies have automatically detected a new exploited vulnerability in the Microsoft Windows OS kernel, the third consecutive zero-day exploit to be discovered in three months. The latest exploited vulnerability (CVE-2018-8611) was found in malware targeting a small number of victims in the Middle East and Asia. Because the vulnerability exists in the kernel mode module of the operating system, the exploit is particularly dangerous and can be used to bypass built-in exploit mitigation mechanisms in modern web browsers, including Chrome and Edge. The vulnerability has been reported to Microsoft, which has released a patch.

Zero-day vulnerabilities are previously unknown, and therefore unpatched, software bugs that attackers can exploit to gain access to victim systems and devices. They are immensely valuable to threat actors, and difficult to detect.
All three exploits were detected by Kaspersky Lab's Automatic Exploit Prevention technology, embedded in most of the company's products. Like the previous two exploited vulnerabilities (CVE-2018-8589 and CVE-2018-8453), patched by Microsoft in October and November respectively, the latest exploit was found used in-the-wild targeting victims in the Middle East and Africa. The exploit for CVE-2018-8589 was called "Alice" by the malware writers, who also referred to the latest exploit as "Jasmine". Kaspersky Lab researchers believe that the new vulnerability has been exploited by multiple threat actors, including a new advanced persistent threat (APT) called Sandcat.

"The detection of three kernel mode zero-days within a few months is evidence that our products use the best technologies, which are capable of detecting such sophisticated threats. For organizations, it is important to understand that to protect their perimeter they should use a combined solution, like endpoint protection with an advanced threat detection platform," – said Anton Ivanov, a security expert at Kaspersky Lab.

Kaspersky Lab recommend taking the following security measures:
• Install Microsoft's patch for the new vulnerability.
• Make sure you update all software used in your organization on a regular basis, and whenever a new security patch is released. Security products with Vulnerability Assessment and Patch Management capabilities may help to automate these processes.
• Choose a proven security solution such as Kaspersky Endpoint Security that is equipped with behavior-based detection capabilities for effective protection against known and unknown threats, including exploits.
• Use advanced security tools like Kaspersky Anti Targeted Attack Platform (KATA) if your company requires highly sophisticated protection.
• Make sure your security team has access to the most recent cyber threat intelligence. Private reports on the latest developments in the threat landscape are available to customers of Kaspersky Intelligence Reporting. For further details, contact: intelreports@kaspersky.com.
• Last, but not least, ensure your staff is trained in the basics of cybersecurity hygiene.

For further details on the new exploit see the report on Securelist.

Zero-day in Windows Kernel Transaction Manager (CVE-2018-8611)