Extremely dangerous zero-day vulnerability on Chrome: Users update now!

Immediately after clicking on the phishing link in the email, the user's system is immediately compromised.

Security firm Kaspersky has just discovered a new wave of malware infections. After clicking on a phishing link in an email, the user's system is immediately compromised, even if the person does not perform any further actions.

Through analysis, Kaspersky confirmed that the attack was exploiting a previously undiscovered vulnerability in the latest version of Chrome at that time. The Kaspersky team immediately alerted Google's security team. As a result, a security patch for this vulnerability was released on March 25, 2025.

Zero-day vulnerabilities are extremely dangerous. (Illustration)

Kaspersky dubbed the campaign 'Operation ForumTroll', as the attackers sent emails inviting victims to the 'Primakov Readings' forum. The main targets included media outlets, educational institutions, and government agencies in Russia. To make matters worse, the malicious links were only available for a short period of time to avoid detection. And in most cases, the links redirected to the legitimate Primakov Readings website to hide their tracks after the scam was complete.

"This vulnerability is particularly dangerous compared to dozens of zero-day vulnerabilities we have discovered over the years. Attackers exploit this vulnerability to bypass Chrome's sandbox protection mechanism without

performing any explicit actions, as if the browser's security system almost does not exist," said Boris Larin, head of security research at Kaspersky's GReAT.

"Given the level of sophistication, this attack method is likely developed by highly skilled and resourceful cybercriminal groups. We recommend that all users update Google Chrome and other Chromium-based browsers to the latest version to avoid the risk of attack," Larin warned.

Previously, Kaspersky's GReAT team also discovered another zero-day vulnerability in Chrome (CVE-2024-4947). This vulnerability was exploited by the APT group Lazarus in a cryptocurrency theft campaign. At that time, Kaspersky researchers discovered a 'type confusion' bug in Chrome's V8 JavaScript engine, allowing hackers to bypass security mechanisms through a fake cryptocurrency website.

Kaspersky security experts recommend that Internet users always update their operating systems and web browsers - especially Google Chrome - to avoid cybercriminals attacking through new security vulnerabilities.