Operation ForumTroll: APT attack with Google Chrome zero-day exploit chain

By Igor Kuznetsov

Published: 2025-03-25 · Archived: 2026-04-05 13:26:19 UTC

APT reports

APT reports

25 Mar 2025

2 minute read

In mid-March 2025, Kaspersky technologies detected a wave of infections by previously unknown and highly sophisticated malware. In all cases, infection occurred immediately after the victim clicked on a link in a phishing email, and the attackers' website was opened using the Google Chrome web browser. No further action was required to become infected.

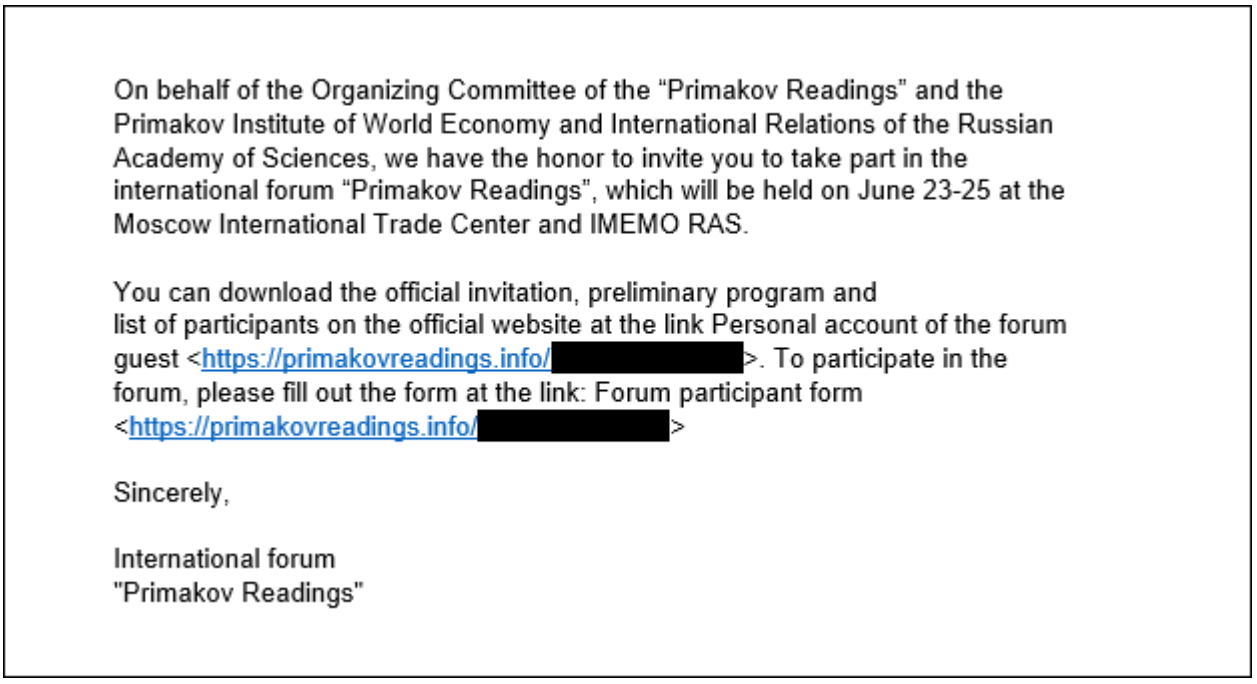
All malicious links were personalized and had a very short lifespan. However, Kaspersky's exploit detection and protection technologies successfully identified the zero-day exploit that was used to escape Google Chrome's sandbox. We quickly analyzed the exploit code, reverse-engineered its logic, and confirmed that it was based on a zero-day vulnerability affecting the latest version of Google Chrome. We then reported the vulnerability to the Google security team. Our detailed report enabled the developers to quickly address the issue, and on March 25, 2025, Google released an update fixing the vulnerability and thanked us for discovering this attack.

> [TBD][405143032] High CVE-2025-2783: Incorrect handle provided in unspecified circumstances in Mojo on Windows. Reported by Boris Larin (@oct0xor) and Igor Kuznetsov (@2igosha) of Kaspersky on 2025-03-20

Acknowledgement for finding CVE-2025-2783 (excerpt from security fixes included into Chrome 134.0.6998.177/.178)

We have discovered and reported dozens of zero-day exploits actively used in attacks, but this particular exploit is certainly one of the most interesting we've encountered. The vulnerability CVE-2025-2783 really left us scratching our heads, as, without doing anything obviously malicious or forbidden, it allowed the attackers to bypass Google Chrome's sandbox protection as if it didn't even exist. The cause of this was a logical error at the intersection of Google Chrome's sandbox and the Windows operating system. We plan to publish the technical details of this vulnerability once the majority of users have installed the updated version of the browser that fixes it.

Our research is still ongoing, but judging by the functionality of the sophisticated malware used in the attack, it seems the attackers' goal was espionage. The malicious emails contained invitations allegedly from the organizers of a scientific and expert forum, "Primakov Readings", targeting media outlets, educational institutions and government organizations in Russia. Based on the content of the emails, we dubbed the campaign Operation ForumTroll.



On behalf of the Organizing Committee of the "Primakov Readings" and the Primakov Institute of World Economy and International Relations of the Russian Academy of Sciences, we have the honor to invite you to take part in the international forum "Primakov Readings", which will be held on June 23-25 at the Moscow International Trade Center and IMEMO RAS.

You can download the official invitation, preliminary program and list of participants on the official website at the link Personal account of the forum guest <https://primakovreadings.info/[redacted]>. To participate in the forum, please fill out the form at the link: Forum participant form <https://primakovreadings.info/[redacted]>

Sincerely,

International forum
"Primakov Readings"

Example of a malicious email used in this campaign (translated from Russian)

At the time of writing, there's no exploit active at the malicious link – it just redirects visitors to the official website of "Primakov Readings". However, we strongly advise against clicking on any potentially malicious links.

The exploit we discovered was designed to run in conjunction with an additional exploit that enables remote code execution. Unfortunately, we were unable to obtain this second exploit, as in this particular case it would have required waiting for a new wave of attacks and exposing users to the risk of infection. Fortunately, patching the vulnerability used to escape the sandbox effectively blocks the entire attack chain.

All the attack artifacts analyzed so far indicate high sophistication of the attackers, allowing us to confidently conclude that a state-sponsored APT group is behind this attack.

We plan to publish a detailed report with technical details about the zero-day exploit, the sophisticated malware, and the attackers' techniques.

Kaspersky products detect the exploits and malware used in this attack with the following verdicts:

- Exploit.Win32.Generic
- Trojan.Win64.Agent
- Trojan.Win64.Convagent.gen
- PDM:Exploit.Win32.Generic
- PDM:Trojan.Win32.Generic

- UDS:DangerousObject.Multi.Generic

Indicators of Compromise

primakovreadings[.]info

Latest Posts

Latest Webinars

Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
