

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

SL [securelist.com/operation-forumtroll/115989/](https://securelist.com/operation-forumtroll/115989/)



[APT reports](#)



[APT reports](#)

25 Mar 2025

minute read



## Authors

-  Igor Kuznetsov
-  Boris Larin

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.

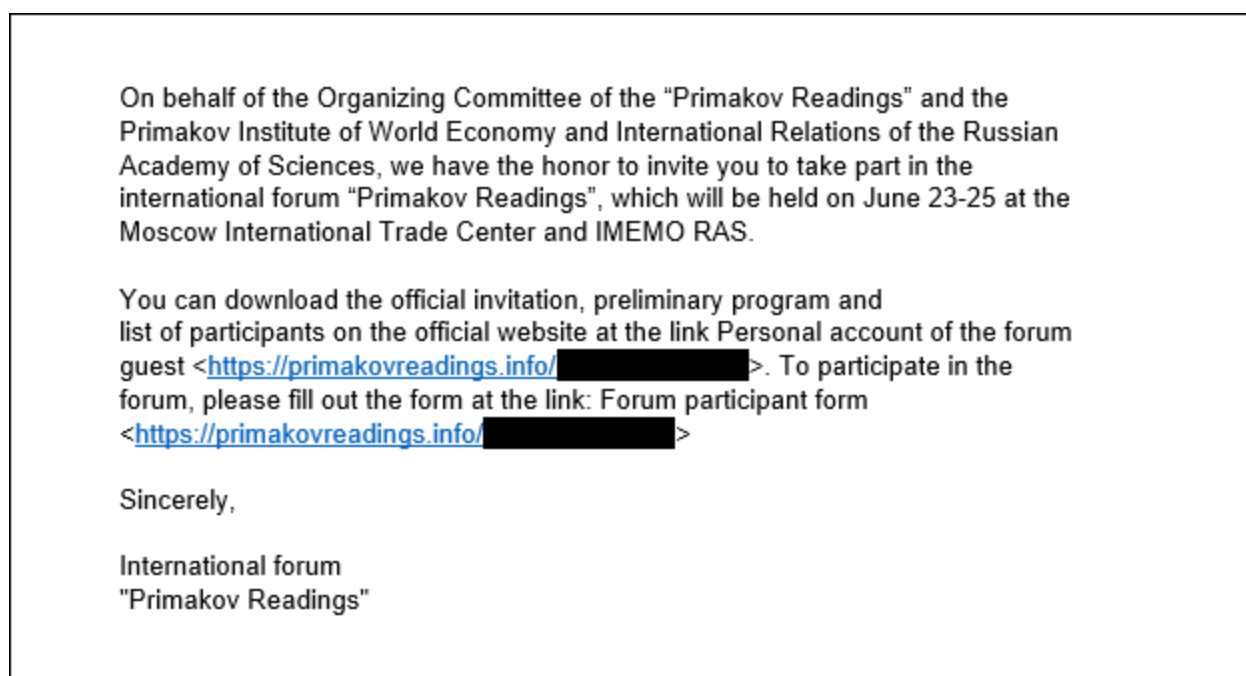
All malicious links were personalized and had a very short lifespan. However, Kaspersky's exploit detection and protection technologies successfully identified the zero-day exploit that was used to escape Google Chrome's sandbox. We quickly analyzed the exploit code, reverse-engineered its logic, and 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.



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](#)

- [APT](#)
- [ForumTroll](#)
- [Google Chrome](#)
- [Targeted attacks](#)
- [Vulnerabilities](#)
- [Vulnerabilities and exploits](#)
- [Zero-day vulnerabilities](#)

Authors

-  [Igor Kuznetsov](#)
-  [Boris Larin](#)

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

---

Your email address will not be published. Required fields are marked \*

GReAT webinars

13 May 2021, 1:00pm

### **GReAT Ideas. Balalaika Edition**

---

26 Feb 2021, 12:00pm

17 Jun 2020, 1:00pm

26 Aug 2020, 2:00pm



22 Jul 2020, 2:00pm

## **GReAT Ideas. Powered by SAS: threat hunting and new techniques**

---

From the same authors



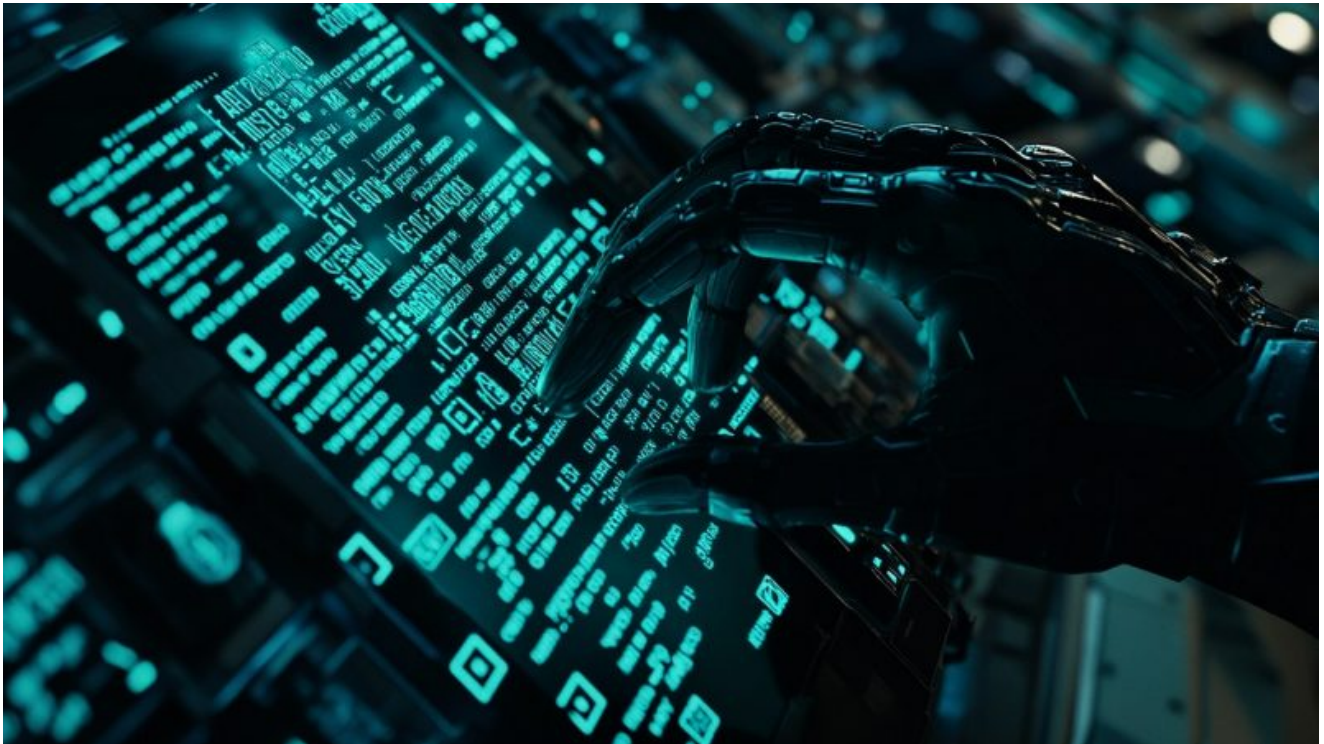
## **Advanced threat predictions for 2025**

---



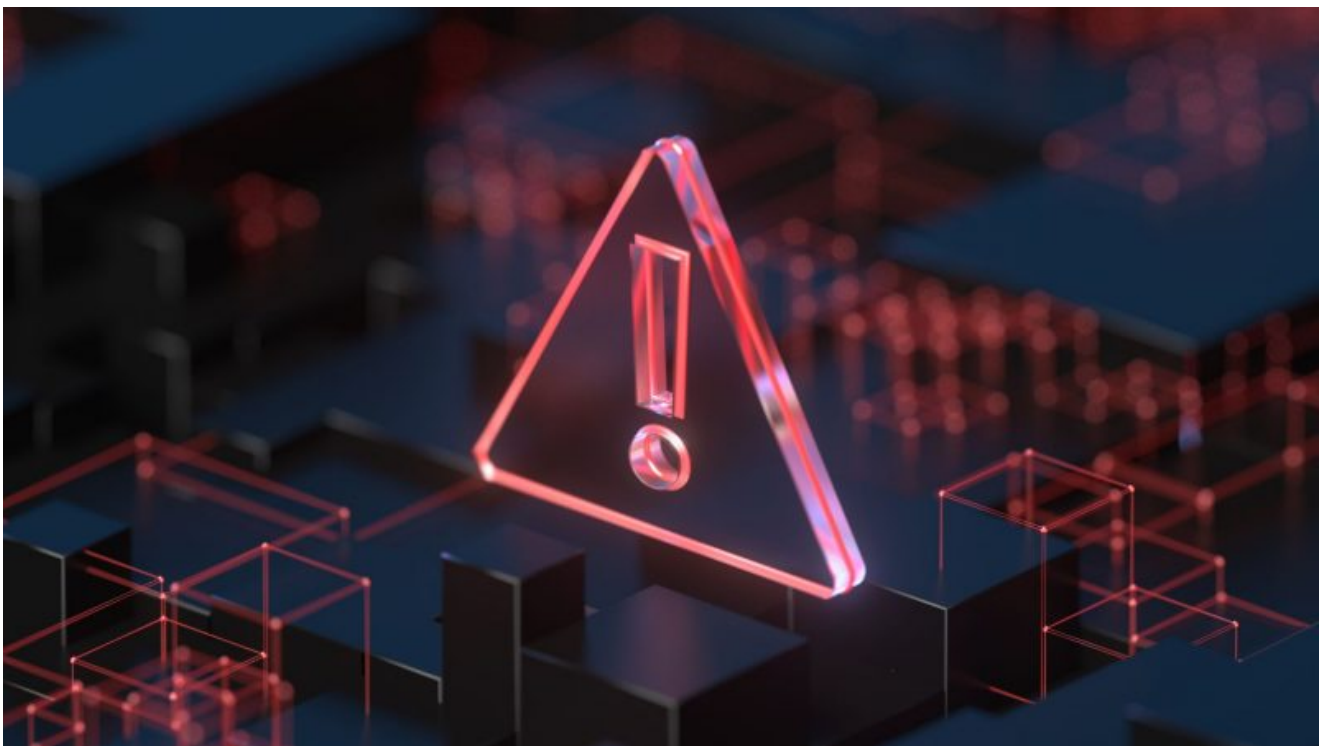
## The Crypto Game of Lazarus APT: Investors vs. Zero-days

---



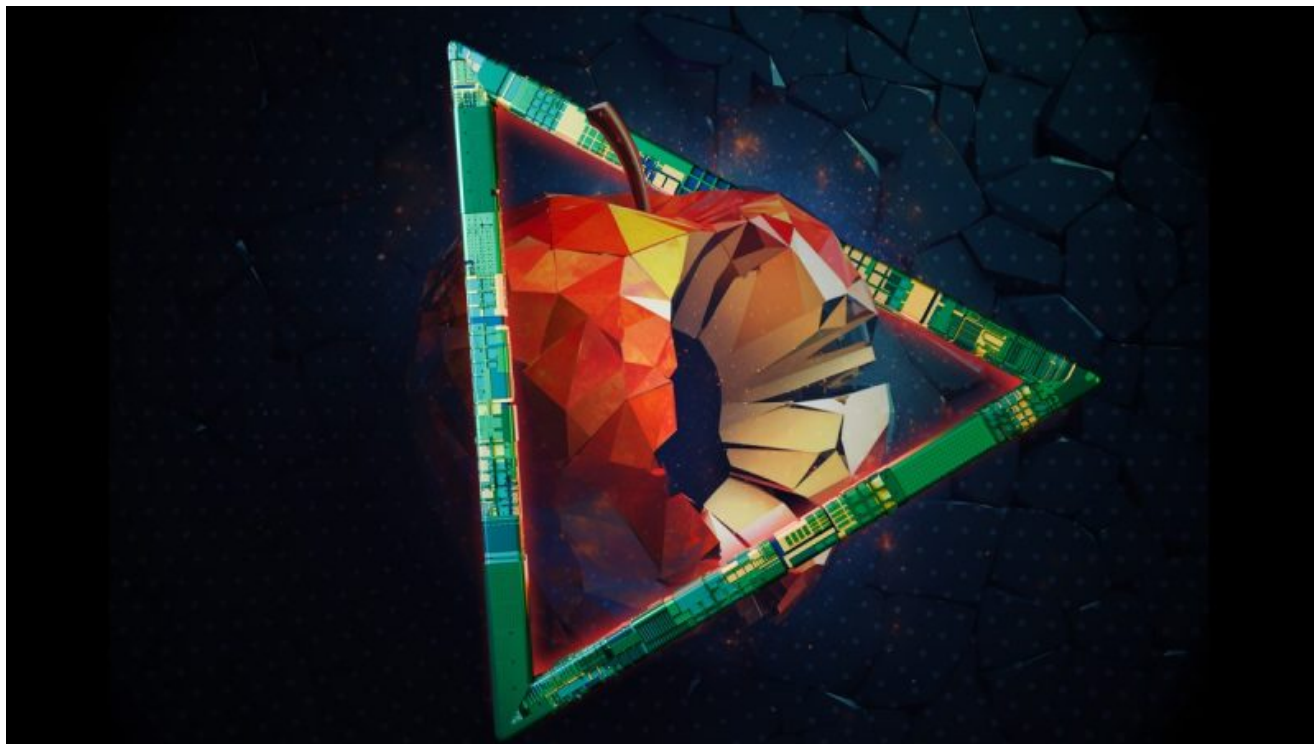
## SAS CTF and the many ways to persist a kernel shellcode on Windows 7

---



## QakBot attacks with Windows zero-day (CVE-2024-30051)

---



## **Operation Triangulation: The last (hardware) mystery.**

---

Subscribe to our weekly e-mails

The hottest research right in your inbox

**(Required)**

In the same category





**SideWinder targets the maritime and nuclear sectors with an updated toolset**

---



**EAGERBEE, with updated and novel components, targets the Middle East**

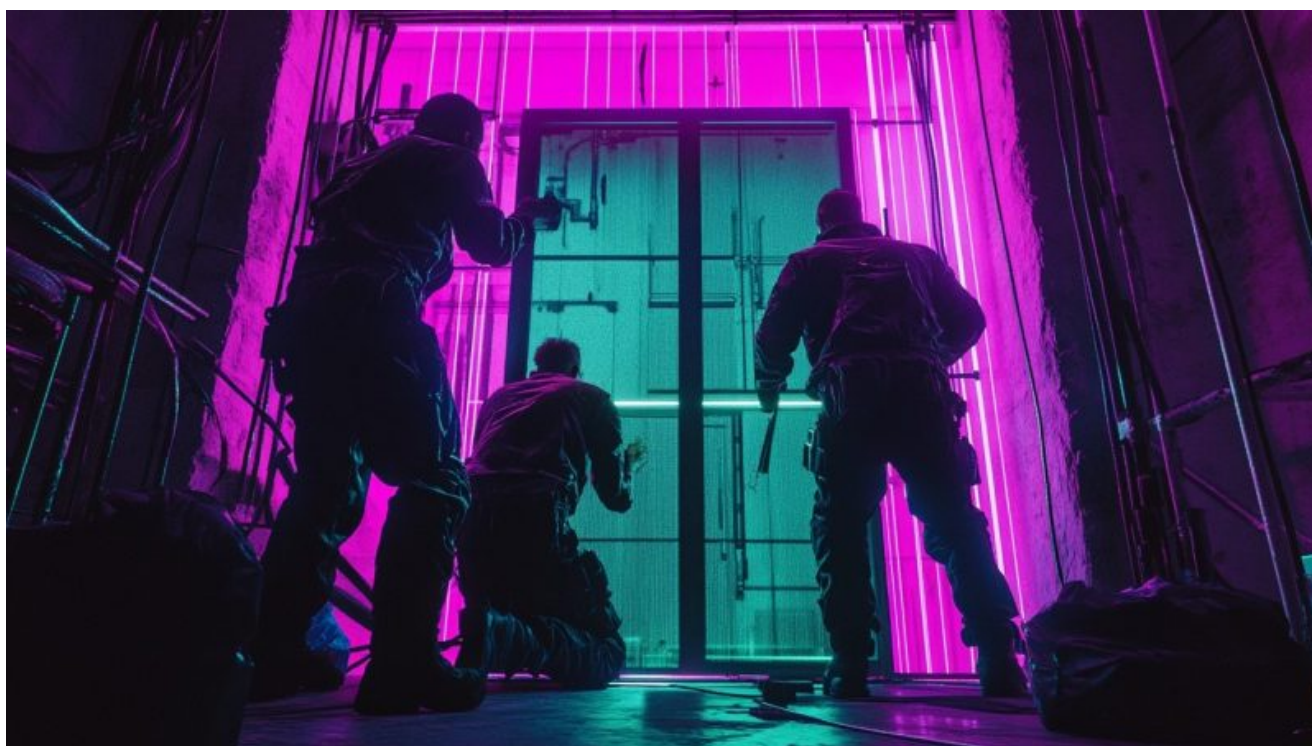
---





### BellaCPP: Discovering a new BellaCiao variant written in C++

---



### Lazarus group evolves its infection chain with old and new malware

---



**Careto is back: what's new after 10 years of silence?**

---



## Reports

Kaspersky GReAT experts discovered a complex APT attack on Russian organizations dubbed Operation ForumTroll, which exploits zero-day vulnerabilities in Google Chrome.

### **SideWinder targets the maritime and nuclear sectors with an updated toolset**

In this article, we discuss the tools and TTPs used in the SideWinder APT's attacks in H2 2024, as well as shifts in its targets, such as an increase in attacks against the maritime and logistics sectors.

### **EAGERBEE, with updated and novel components, targets the Middle East**

Kaspersky researchers analyze EAGERBEE backdoor modules, revealing a possible connection to the CoughingDown APT actor.

### **BellaCPP: Discovering a new BellaCiao variant written in C++**

While investigating an incident involving the BellaCiao .NET malware, Kaspersky researchers discovered a C++ version they dubbed "BellaCPP".



APR 8, 15:00 CET

WEBINAR

# What your security stack isn't catching

How to identify hidden threats

**Nikita Nazarov**

Head of Threat Exploration

**Alexander Rumyantsev**

Senior Product Manager

**Sergey Zarovny**

Product Launch Manager

k



Subscribe to our weekly e-mails

The hottest research right in your inbox

(Required)

APRIL 8, 15:00 CET

WEBINAR

# What your security stack isn't catching

How to identify hidden threats

**Nikita Nazarov**

Head of Threat Exploration

**Alexander Rumyantsev**

Senior Product Manager

**Sergey Zarovny**

Product Launch Manager

**kaspersky**



Subscribe to our weekly e-mails

The hottest research right in your inbox

(Required)