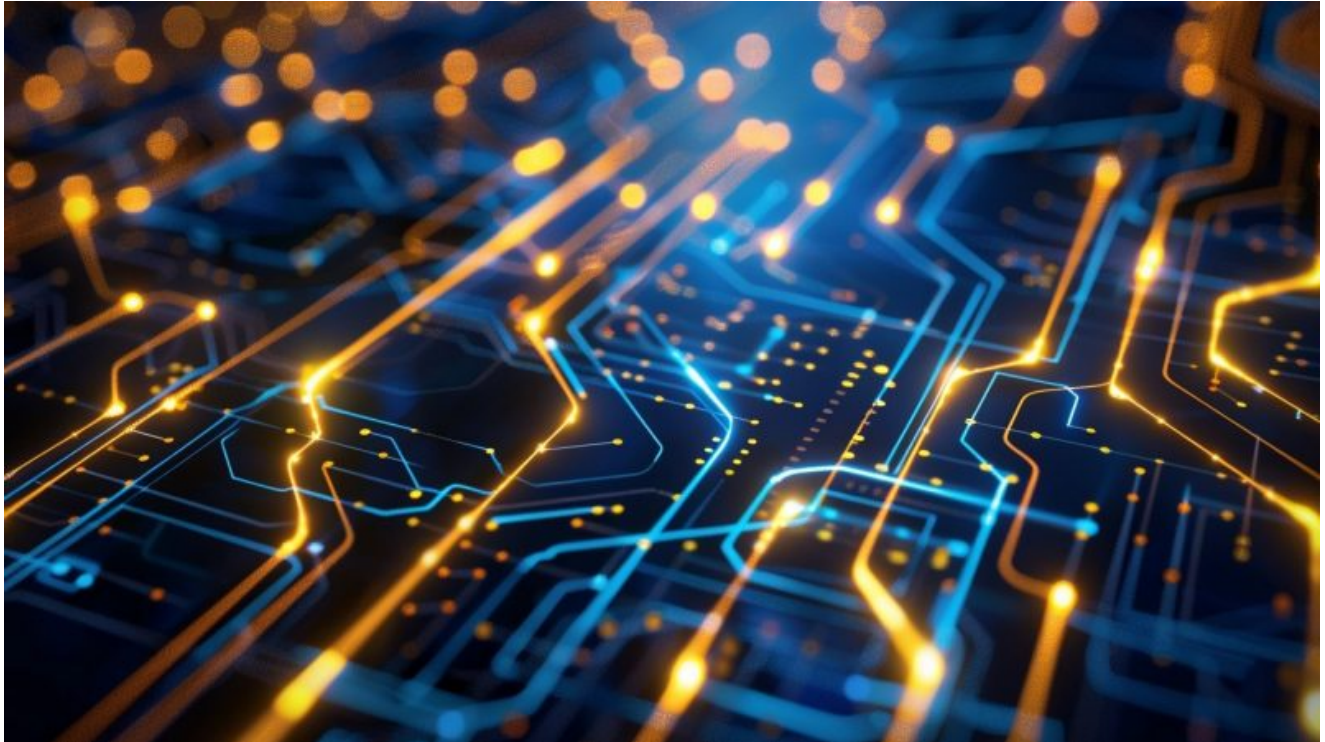


# Russian organizations targeted by backdoor masquerading as secure networking software updates

SL [securelist.com/new-backdoor-mimics-security-software-update/116246/](https://securelist.com/new-backdoor-mimics-security-software-update/116246/)

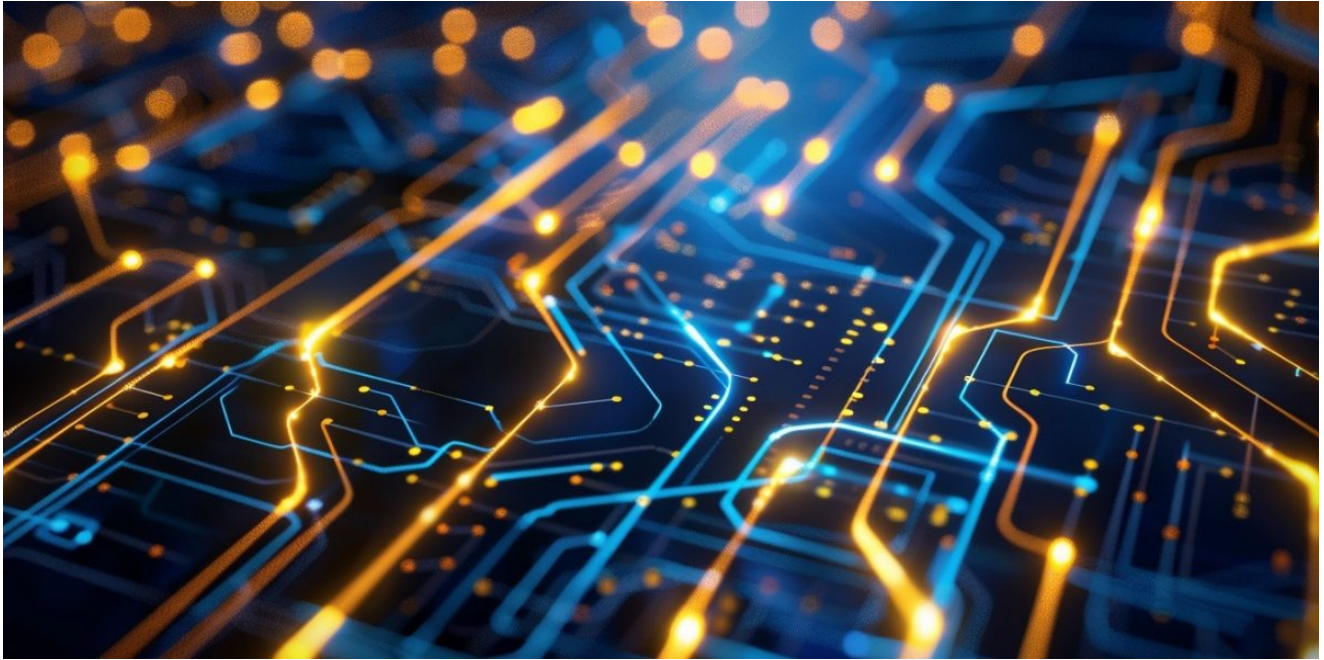


[Incidents](#)


[Incidents](#)

22 Apr 2025

minute read



## Authors

- [Igor Kuznetsov](#)
- [Georgy Kucherin](#)
-  [Alexander Demidov](#)

As we were looking into a cyberincident in April 2025, we uncovered a rather sophisticated backdoor. It targeted various large organizations in Russia, spanning the government, finance, and industrial sectors. While our investigation into the attack associated with the backdoor is still ongoing, we believe it is crucial to share our preliminary findings with the community. This will enable organizations that may be at risk of infection from the backdoor to take swift action to protect themselves from this threat.

## Impersonating a ViPNet update

---

Our investigation revealed that the backdoor targets computers connected to ViPNet networks. ViPNet is a software suite for creating secure networks. We determined that the backdoor was distributed inside LZH archives with a structure typical of updates for the software product in question. These archives contained the following files:

- action.inf: a text file
- lumpdiag.exe: a legitimate executable
- msinfo32.exe: a small malicious executable
- an encrypted file containing the payload (the name varies between archives)

The ViPNet developer confirmed targeted attacks against some of their users and issued security updates and [recommendations for customers \(page in Russian\)](#).

## Malware execution

---

After analyzing the contents of the archive, we found that the action.inf text file contained an action to be executed by the ViPNet update service component (itcsvup64.exe) when processing the archive:

- 1 [ACTION]
- 2 action=extra\_command
- 3 extra\_command=lumpdiag.exe --msconfig

As evident from the file content above, when processing extra\_command, the update service launches lumpdiag.exe with an --msconfig argument. We mentioned earlier that this is a legitimate file. However, it is susceptible to the path substitution technique. This allows attackers to execute the malicious file msinfo32.exe while lumpdiag.exe is running.

## Downloadable payload

---

The msinfo32.exe file is a loader that reads the encrypted payload file. The loader processes the contents of the file to load the backdoor into memory. This backdoor is versatile: it can connect to a C2 server via TCP, allowing the attacker to steal files from infected computers and launch additional malicious components, among other things. Kaspersky solutions detect this threat as HEUR:Trojan.Win32.Loader.gen.

## Multi-layered security is key to preventing sophisticated cyberattacks

---

The complexity of cyberattacks carried out by APT groups has significantly increased over the years. Attackers can target organizations in highly unusual and unexpected ways. To prevent sophisticated targeted attacks, it is essential to employ multi-layered, defense-in-depth security against cyberthreats. This is the type of security architecture implemented in our [Kaspersky NEXT](#) product line, capable of protecting businesses from attacks similar to the one described in this article.

## Indicators of compromise

---

*The full list of indicators of compromise is available to subscribers of our [Kaspersky Threat Intelligence](#) service.*

## Hashes of msinfo32.exe

[018AD336474B9E54E1BD0E9528CA4DB5  
28AC759E6662A4B4BE3E5BA7CFB62204  
77DA0829858178CCFC2C0A5313E327C1  
A5B31B22E41100EB9D0B9A27B9B2D8EF  
E6DB606FA2B7E9D58340DF14F65664B8](#)

## Paths to malicious files

- 1 %TEMP%\update\_tmp\*\update\msinfo32.exe
- 2
- 3 %PROGRAMFILES%\common files\infotecs\update\_tmp\driv\_\*\*\msinfo32.exe
- 4
- 5 %PROGRAMFILESx86%\InfoTeCS\ViPNet  
Coordinator\ccc\update\_tmp\DRIV\_FSA\\*\*\msinfo32.exe

- [Targeted attacks](#)
- [Malware](#)
- [Trojan](#)
- [Backdoor](#)

## Authors

- [Igor Kuznetsov](#)
- [Georgy Kucherin](#)
- **Expert** [Alexander Demidov](#)

Russian organizations targeted by backdoor masquerading as secure networking software updates

---

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

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)

GReAT webinars

13 May 2021, 1:00pm

## [GReAT Ideas. Balalaika Edition](#)

---

26 Feb 2021, 12:00pm

17 Jun 2020, 1:00pm

## [GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots](#)

---

26 Aug 2020, 2:00pm

## [GReAT Ideas. Powered by SAS: threat actors advance on new fronts](#)

---

22 Jul 2020, 2:00pm

## [GReAT Ideas. Powered by SAS: threat hunting and new techniques](#)

---

From the same authors



## [Code highlighting with Cursor AI for \\$500,000](#)

---



[Operation ForumTroll: APT attack with Google Chrome zero-day exploit chain](#)

---



[The GitVenom campaign: cryptocurrency theft using GitHub](#)

---



## [Careto is back: what's new after 10 years of silence?](#)

---



## [Our secret ingredient for reverse engineering](#)

---

Subscribe to our weekly e-mails

The hottest research right in your inbox

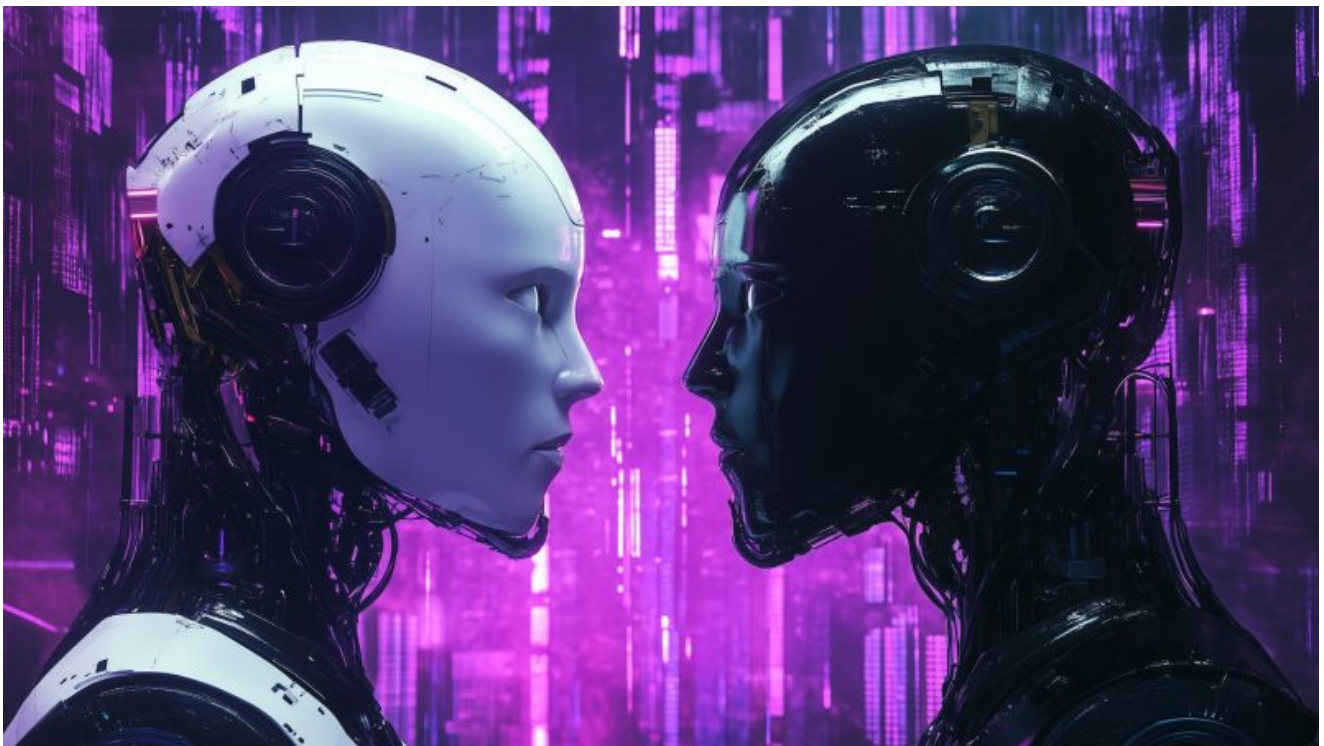
(Required)

In the same category



[The SOC files: Rumble in the jungle or APT41's new target in Africa](#)

---



[How ToddyCat tried to hide behind AV software](#)

---





[XZ backdoor: Hook analysis](#)

---



[Assessing the Y, and How, of the XZ Utils incident](#)

---



## [XZ backdoor story – Initial analysis](#)

---



Reports

### [Sleep with one eye open: how Librarian Ghouls steal data by night](#)

---

According to Kaspersky, Librarian Ghouls APT continues its series of attacks on Russian entities. A detailed analysis of a malicious campaign utilizing RAR archives and BAT scripts.

### [Operation SyncHole: Lazarus APT goes back to the well](#)

---

Kaspersky GReAT experts uncovered a new campaign by Lazarus APT that exploits vulnerabilities in South Korean software products and uses a watering hole approach.

### [IronHusky updates the forgotten MysterySnail RAT to target Russia and Mongolia](#)

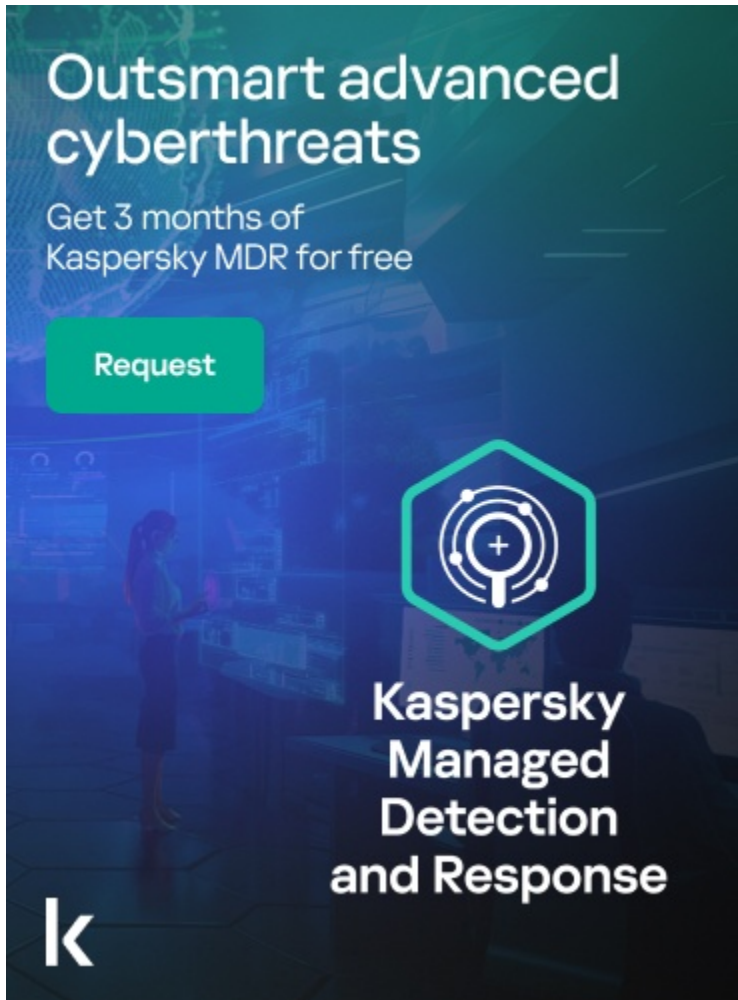
---

MysterySnail RAT attributed to IronHusky APT group hasn't been reported since 2021. Recently, Kaspersky GReAT detected new versions of this implant in government organizations in Mongolia and Russia.

## [GOFFEE continues to attack organizations in Russia](#)

---

Kaspersky researchers analyze GOFFEE's campaign in H2 2024: the updated infection scheme, new PowerModul implant, switch to a binary Mythic agent.

A promotional banner for Kaspersky Managed Detection and Response (MDR). The background is dark blue with a faint image of a person working at a computer. The text is white and green. At the top left, it says "Outsmart advanced cyberthreats". Below that, "Get 3 months of Kaspersky MDR for free". A green button with the word "Request" is positioned below the text. In the center, there is a hexagonal icon containing a stylized circuit or network diagram. Below the icon, the text "Kaspersky Managed Detection and Response" is written in a bold, sans-serif font. In the bottom left corner, there is a large white letter "k" representing the Kaspersky logo.

Outsmart advanced cyberthreats

Get 3 months of Kaspersky MDR for free

Request

Kaspersky Managed Detection and Response

k

Subscribe to our weekly e-mails

The hottest research right in your inbox

(Required)

# Outsmart advanced cyberthreats

Get 3 months of Kaspersky MDR for free

[Request](#)



**Kaspersky  
Managed  
Detection  
and Response**

**kaspersky**

Subscribe to our weekly e-mails

The hottest research right in your inbox

(Required)