Cyber-espionage group Cloud Atlas targets Russian companies with war-related phishing attacks

By Daryna Antoniuk

Published: 2023-12-21 · Archived: 2026-04-05 17:27:25 UTC

The hacker group known as Cloud Atlas targeted a Russian agro-industrial enterprise and a state-owned research company in a new espionage campaign, researchers have found.

Cloud Atlas is a state-backed threat actor, active since at least 2014, that mostly attacks organizations in Russia, Belarus, Azerbaijan, Turkey, and Slovenia.

In its new campaign, the hackers sent their victims phishing emails with malicious attachments — the tactic they were seen using in previous attacks, according to the Russian cybersecurity firm F.A.C.C.T., an offshoot of the Singapore-based cybersecurity firm Group IB.

The researchers said that two attacks they detected were successfully blocked. In the report released earlier this week, F.A.C.C.T. published examples of two phishing letters discovered while analyzing the attacks.

The first email offered to send postcards to soldiers fighting in the war in Ukraine and their family members. Both the report and the malicious emails referred to the war as “SVO” (special military operation), a term used by the Kremlin to describe its invasion of Ukraine. The second email was related to changes in the law regarding military reserves.

Both letters were sent from email addresses registered on popular Russian email services — yandex.ru and mail.ru.

The emails contained malicious attachments that, once opened, uploaded files with an exploit for the vulnerability known as CVE-2017-11882. This is a vulnerability in Microsoft Office that was fixed back in 2017 but is still actively exploited.

Successful exploitation of this bug allows attackers to execute arbitrary code with the privileges of the user who opened the malicious file. Thus, if the victim has administrator rights, the attacker will be able to take full control of their system — install programs, view, modify, or destroy data, and even create new accounts, said researchers at Moscow-based Kaspersky.

Last December, researchers at Check Point published a report saying that Cloud Atlas ramped up activities targeting “high profile victims” in Russia, Belarus, Transnistria (a pro-Kremlin breakaway region of Moldova), and Russian-annexed territories of Ukraine, including Crimea, Luhansk, and Donetsk.

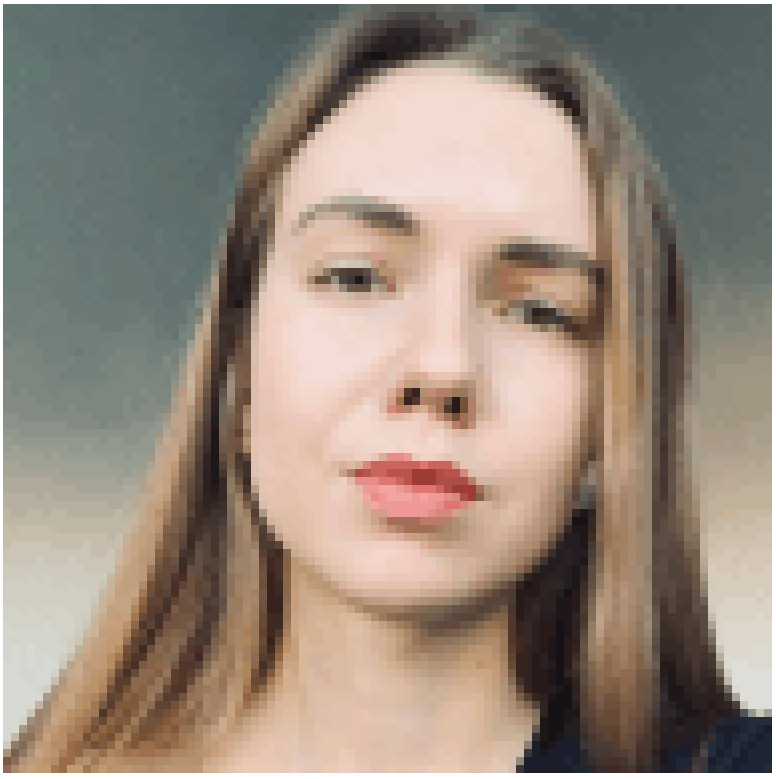
Cloud Atlas focuses on espionage and theft of confidential information, but it isn’t clear what country sponsors the group.

The hackers typically use phishing emails with malicious attachments to gain initial access to a victim's computer. These documents are carefully crafted to mimic government statements, media articles, business proposals, or advertisements, researchers said.

The attackers closely control who can access their malicious attachments by whitelisting the targets. To collect the IP information of the victims, Cloud Atlas first sent them reconnaissance documents, which do not contain any malicious files aside from fingerprinting the victim, according to Check Point.

No previous article

No new articles



Daryna Antoniuk

is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.
