Hackers use new malware to breach air-gapped devices in Eastern Europe

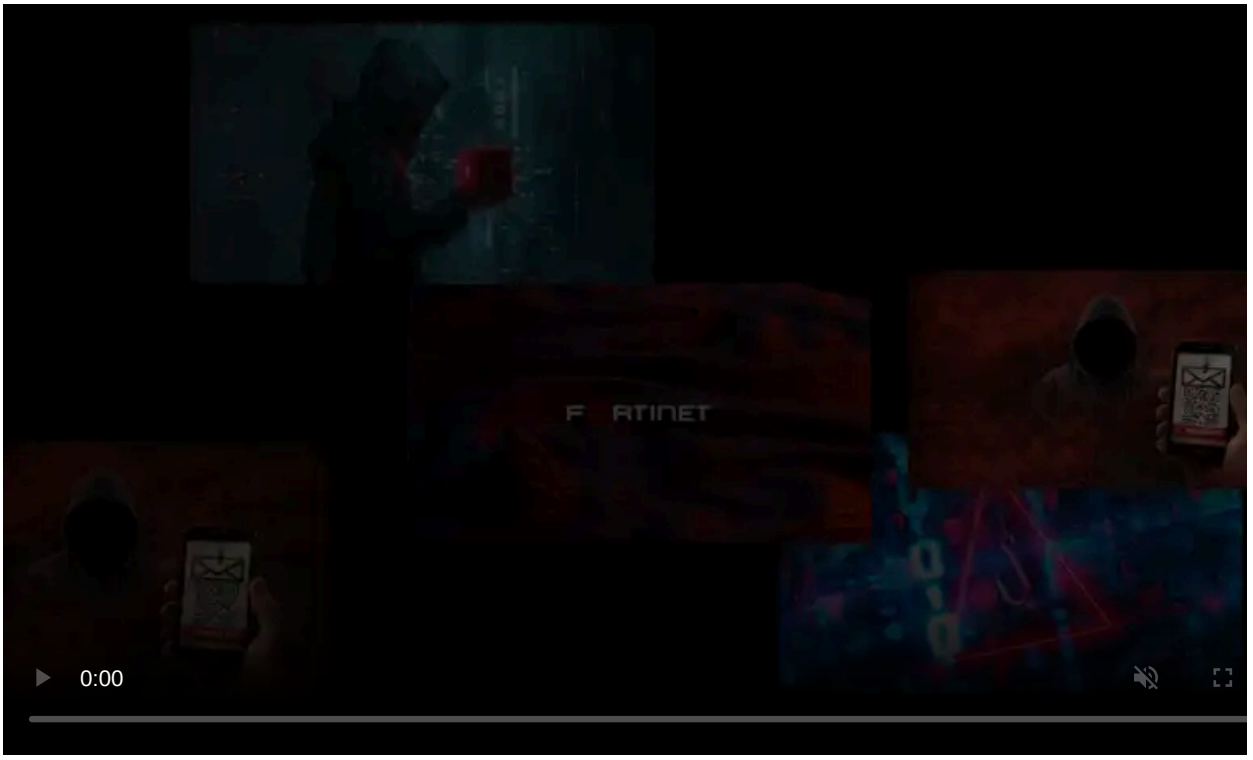
By Bill Toulas

Published: 2023-08-01 · Archived: 2026-04-05 22:48:20 UTC

Chinese state-sponsored hackers have been targeting industrial organizations with new malware that can steal data from air-gapped systems.

Air-gapped systems typically fulfill critical roles and are isolated from the enterprise network and the public internet either physically or through software and network devices.

Researchers at cybersecurity company Kaspersky discovered the new malware and attributed it to the cyber-espionage group APT31, a.k.a. Zirconium.


F RTINET
0:00

According to the findings, the hackers used at least 15 distinct implants in attacks in Eastern Europe, each for a distinct stage of the operation, as well as their signature 'FourteenHi' malware family.

Multi-stage attacks

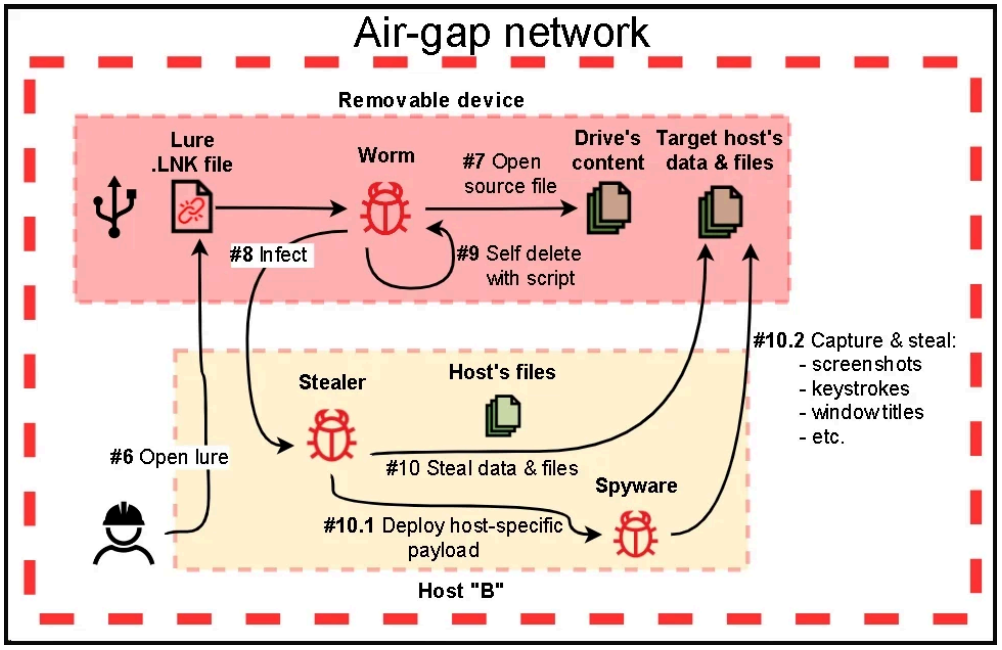
Kaspesky says that the attacks started in April last year and involved three separate stages. The implants in the initial-phase established persistence and remote access to the compromised systems and collected data useful for reconnaissance.

In the second stage, APT31 drops more specialized malware that can steal data from isolated (air-gapped) systems using USB propagation.

Finally, in the third stage of the attack, the hackers use implants that can upload the collected data to their command and control (C2) servers.

The malware that targets isolated systems consists of four modules described below.

1. **First module**: Profiles removable drives connected to the system, collects files, captures screenshots and window titles, and drops additional payloads on the infected device.
2. **Second module**: Infects removable drives by copying a legitimate McAfee executable which is vulnerable to DLL hijacking, and a malicious DLL payload onto the root directory of the device, and sets them as "hidden." The tool also creates a lure LNK file that triggers the infection if the victim launches it.
3. **Third module**: Executes a batch script to collect data from the device and save the output to the "$RECYCLE.BIN" folder, from where the first module will collect it.
4. **Fourth module**: Variant of the first module seen in some attacks, acts as a payload dropper, keylogger, screenshot-capturing tool, and file stealer.



Infection route for air-gapped systems *(Kaspersky)*

In May 2022, Kaspersky noticed an additional implant used in the APT31 attacks, designed to collect local files from breached systems.

That implant decrypts and injects its payload into the memory of a legitimate process to evade malware detection, then sleeps for 10 minutes and eventually copies all files that match the file type extensions defined in its configuration.

The stolen files are archived using WinRAR (if not available, the malware exits) and then stored in temporary local folders created by the malware under "C:\ProgramData\NetWorks\." Ultimately, the archives are exfiltrated to Dropbox.

Kaspersky underlines that the attacks were stealthy and listed the following tactics, techniques, and procedures (TTPs): DLL order hijacking to load malicious payloads into memory and hide payloads in encrypted form in separate binary data files.

The company provides a technical report that includes additional data such as malware hashes, a full set of indicators of compromise, and details about the activity of the malware from start to finish.

Air-gapped systems are an attractive target for APT groups, who typically turn to USB drives to deliver malware and exfiltrate data from the isolated environment.

Source: https://www.bleepingcomputer.com/news/security/hackers-use-new-malware-to-breach-air-gapped-devices-in-eastern-europe/