2023 CYBER THREATS FOR THE INDUSTRIAL SECTOR

Part 1

ROOT LEVEL RESOURCES

Key trends

- The number of attacks on industrial sector companies in 2022 increased by 19% (295 incidents detected).
- The APT41 group, sponsored by China, keeps attacking the technology and manufacturing sectors. The group is attributed with the CuckooBees campaign, which has been secretly spying on businesses in North America, Europe, and Asia since 2019.
- Even isolated air gap networks do not provide complete protection from pro-state hackers. For example, the Chinese tool Daxin operated successfully on these networks, remaining undetected for more than 10 years.
- Tropic Trooper (another Chinese group) used the xPack Trojan to attack a Taiwanese manufacturing organization and remained in the company's network for 175 days.

Cybercrime groups attacking the industrial sector

ROOT LEVEL RESOURCES

295

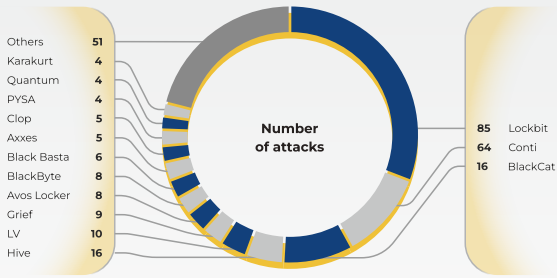
In 2022, **295 encryption group attacks** on industrial companies were detected.

This is **19%** more than in 2021

The largest number of accesses came from companies in the United States (31%), Germany (11%), and Italy (9%)

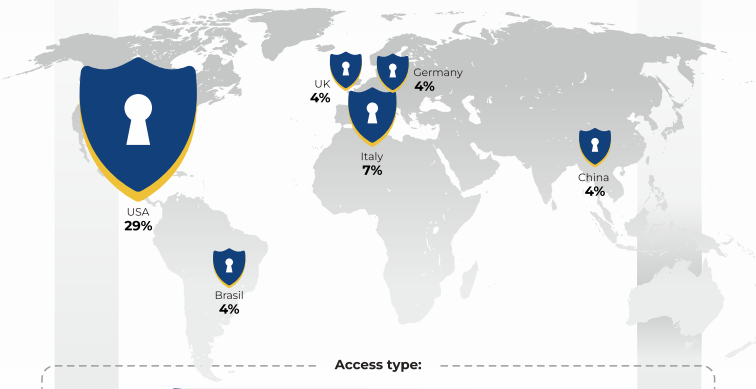
The geography of attacks is as follows:

The most active groups involved in attacks on industrial companies in 2022 were Lockbit (29%), Conti (22%) and BlackCat (5%), Hive (5%):

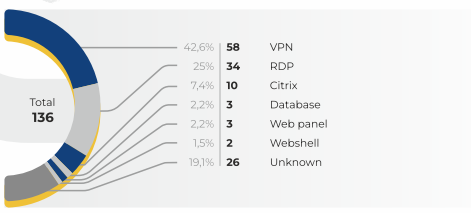


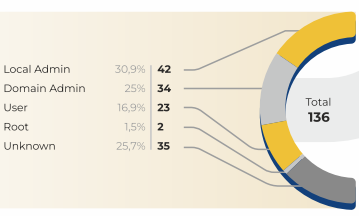
After analyzing the 2022 access broker market in the industry, experts found **136** accesses to industrial companies put up for sale by cybercriminals. This is **33%** more than in 2021.

Most acceses:



Access type:





Brokers who most often sold accesses to industrial companies:

Novelli

15 RDP accesses, 9 of which are from Latin America.

Almost all of the accesses include local or domain administrator privileges

orangecake

15 accesses, most of which are VPNs.

More than half of the accesses are in Europe

Nei

7 VPN accesses during September and December 2021 worldwide.

5 of them with local administrator privileges