# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:42:33 UTC

## APT group: WildCard

| | |
|---|---|
| Names | WildCard *(Intezer)* |
| Country | [Unknown] |
| Motivation | Information theft and espionage |
| First seen | 2021 |
| Description | (Intezer) Our research team has identified a new APT group, dubbed “WildCard,” initially detected through its use of the SysJoker malware, which targeted Israel’s educational sector in 2021. WildCard has since expanded its reach, creating sophisticated malware variants disguised as legitimate software, and a recently developed malware called ‘RustDown,’ written in Rust for potential operational advantages. Connections to Operation Electric Powder indicate WildCard’s advanced capabilities with a focus on critical sectors within Israel. While we’ve begun to understand WildCard’s tactics and methods, their precise identity is still enigmatic, demanding deeper analysis and collaboration within the infosec community. |
| Observed | Sectors: Education, Industrial.<br>Countries: Israel. |
| Tools used | RustDown, SysJoker. |
| Information | <https://intezer.com/blog/research/wildcard-evolution-of-sysjoker-cyber-threat/><br><https://research.checkpoint.com/2023/israel-hamas-war-spotlight-shaking-the-rust-off-sysjoker/> |

Last change to this card: 30 November 2023

Download this actor card in PDF or JSON format

---