

[Threat Actors](#) • [March 27, 2019](#) • [Cyware News](#)

Lazarus hacking group expand their attack horizon by targeting an Israeli defense company

- The campaign is carried out with an intention to steal military and commercial secrets.
- The Israeli defense company discovered the campaign on March 7, 2019.

The infamous Lazarus threat actor group has been found targeting an Israeli defense company, according to new research outlined by a cybersecurity firm ClearSky. The campaign is carried out with an intention to steal military and commercial secrets.

What's the matter • According to ClearSky, the unnamed company manufactures products used in the military and aerospace industries. It is believed that the hackers could have been after commercial secrets or traditional espionage.

"We cannot be sure what the objective of the attackers [was]. [It] could be industrial/commercial espionage but could be military espionage, for example," said Eyal Sela, head of threat intelligence at ClearSky, [Cyberscoop reported](#).

When was it discovered • The Israeli defense company discovered the campaign on March 7, 2019 after an employee received an email in broken Hebrew from a colleague whose account was likely breached.

Researchers believe that the hackers had implanted the malicious Rising Sun backdoor malware to launch the attack. For this, the Lazarus group leverages a vulnerability - CVE-2018-20250 - in outdated WinRAR file-archiving software. The analysis of the source code shows that the malware is capable of bypassing email-filtering protections.

[Rising Sun](#) [Cyberespionage Actor](#) [Lazarus Apt Group](#) [commercial secrets](#) [Cyberespionage Campaigns](#)[READ PREVIOUS](#)[Unsubtrogen's latest campaign affects several organiza ...](#)[Malware and Vulnerabilities](#)[READ NEXT](#)[Over 110,000 Australians affected by cyberattack on Fac ...](#)[Breaches and Incidents](#)

CATEGORIES

Expert Blogs and Opinion
Innovation and Research
The Hacker Tools
Incident Response, Learnings
Malware and Vulnerabilities
Breaches and Incidents
Laws, Policy, Regulations
Strategy and Planning

[News and Updates, Hacker News:](#)
[Stream](#)

Mobile Security
Govt., Critical Infrastructure
Security Culture
Identity Theft, Fraud, Scams
Trends, Reports, Analysis
New Cyber Technologies
Major Events
Cyber Glossary

Write to us at:
community@cyware.com

Threat Actors
Security Products & Services
Threat Intel & Info Sharing
Emerging Threats
Geopolitical, Terrorism
Internet of Things
Computer, Internet Security
Social Media Threats

Follow us on:
[f](#) [t](#) [in](#)

Security Tips and Advice
Companies to Watch
Interesting Tweets
Marketplace
Did You Know?
Physical Security

EVENTS

Conference
Webinar
Summit
Course
Other
Symposium
Seminar
Talk

Visit Us
[Cyware Labs, 5400 Broadway, New York, NY 10018](#)