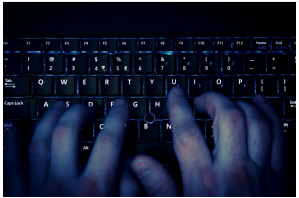

Threat Actors ● March 27, 2019 ● Cyware News

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, Cybersecop 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 For this, the Lazarus group leverages a vulnerability - CVE-2018-20250 - in outdated WinRAR file-archiving software.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
Ursnif trojan's latest campaign affects several organiz ...
Malware and Vulnerabilities

READ NEXT
Over 110,000 Australians affected by cyberattack on Fac ...
Breaches and Incidents