North Korea's Lazarus Group Targets IT Supply Chains with MATA Malware

Security experts from Kaspersky uncovered two latest supply-chain attack campaigns from the North Korean hacking group, Lazarus, targeting multiple downstream companies.

By **CISOMAG** - October 28, 2021

Lazarus, a notorious advanced persistent threat (APT) group that needs no introduction in the cyberthreat landscape, strikes again with improved malware variants. The North Korea-backed group is better known for its state-sponsored cyberespionage and attacks extended across the globe. Cybersecurity experts identified the two latest supply-chain attack campaigns from the Lazarus group targeting multiple downstream companies.

According to the Q3 2021 APT Trends report from Kaspersky, the attackers behind the Lazarus group used **MATA malware** along with **Blindingcan** and **Copperhedge** backdoors to attack the defense sector, a software solutions vendor based in Latvia, and a think tank located in South Korea.

Old Malware in a New Campaign

Previously, the Lazarus group leveraged MATA malware to target various e-commerce and IT firms in India, South Korea, Poland, Germany, Turkey, and Japan to distribute ransomware and steal sensitive information.

But in its latest campaign, MATA was used for cyberespionage activities. The threat actors reportedly leveraged a Trojanized version of the malware to execute a multi-staged infection chain beginning with a downloader that deploys additional malware from compromised C2 servers.

MATA possesses several components like loader, orchestrator, and plugins to infect Windows, Linux, and macOS operating systems.

"We were able to acquire several MATA components, including plugins. The MATA malware discovered in this campaign has evolved compared to previous versions and uses a legitimate, stolen certificate to sign some of its components. Through this research, we discovered a stronger connection between MATA and the Lazarus group, including the fact that the downloader malware fetching MATA malware showed ties to TangoDaiwbo, which we had previously attributed to the Lazarus group," Kaspersky said.

Lazarus Turns to Supply Chain Attacks

The latest malware campaigns from the Lazarus Group represent the group's growing interest in leveraging trusted IT supply chain vendors as a gateway to corporate networks. The attackers obtained access to a South Korean security software vendor's network to exploit the corporate software and a Latvia-based IT asset-monitoring product vendor by deploying Blindingcan and Copperhedge backdoors. Earlier, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) had issued security alerts 1 & 2 — warning about the two malware backdoors.

Supply chain attacks are certainly not new to the security landscape. Several destructive supply chain attacks like SolarWinds and Kaseya caused severe damage to the critical infrastructures and triggered additional threats worldwide.

TAGS CYBERATTACKS CYBERSECURITY KASPERSKY LATVIA LAZARUS LAZARUS GROUP NORTH KOREA NORTH KOREAN ATTACKS SUPPLY CHAIN ATTACKS

Previous article
Why Businesses Should Be Invested in Digital Identity in 2021

Next article
Empowering Your Team to Fight Cybercrime: What You Need to Know

CISOMAG
https://cisomag.eccouncil.org/

RELATED ARTICLES MORE FROM AUTHOR

News
FBI Issues a Lookout for SIM Swapping Attacks

News
How Remote Work Increase Digital Anxiety

News
Ransomware: To Pay or Not to Pay?

MOST POPULAR

45% companies don't have cybersecurity leader: Study
CISOMAG - December 11, 2017

Nearly half of companies have suffered a data breach in the past year: Survey
November 15, 2017

Mobile messaging apps new hideout of Dark Web activities: Study
October 27, 2017

NSA hacking code lifted from a personal computer in U.S.: Kaspersky
October 30, 2017

Instagram data breach! 49 million users' sensitive data exposed online
May 23, 2019

RECENT POSTS

FBI Issues a Lookout for SIM Swapping Attacks
February 15, 2022

How Remote Work Increase Digital Anxiety
February 9, 2022

How to Update Web Browsers for Secure Browsing
February 8, 2022

We'll See More Data Exfiltration and Data Leak Threats
February 7, 2022

A Beginner's Guide to Forensics as a Service (FaaS)
February 4, 2022