

Trade Crypto with Confidence

Valid Network's crypto security insights help you protect the value of your digital assets
Valid Network

Open

TUESDAY, FEBRUARY 15, 2022

ABOUT US

ADVISORY BOARD

CAREERS

WRITE FOR CISO MAG

EDITORIAL CALENDAR

LOGIN

> >



EC-Council

CISO MAG
IS EVOLVING

As a response to our community and to ensure timely and relevant content, CISO Mag's digital edition will be replaced with the new EC-Council Cybersecurity Exchange. Stay tuned for new, free online content, coming soon via Cybersecurity Exchange!

CISO MAG

MAGAZINE >

NEWS >

FEATURES >

PODCASTS

GET FEATURED >

VIDEOS >

WEBINARS

EVENTS >

>

EC-COUNCIL
UNIVERSITY
ACCREDITED, FLEXIBLE, ONLINE

CISO
The Security Suite 2022

Security lapses aren't just technical failures, they could be management failures too.

Learn the leadership skills from Seasoned CISOs and join the C-Suite executives.

EC-Council

Get certified today



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

NEWS THREATS

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 CISO MAG - October 28, 2021

SHARE



Facebook



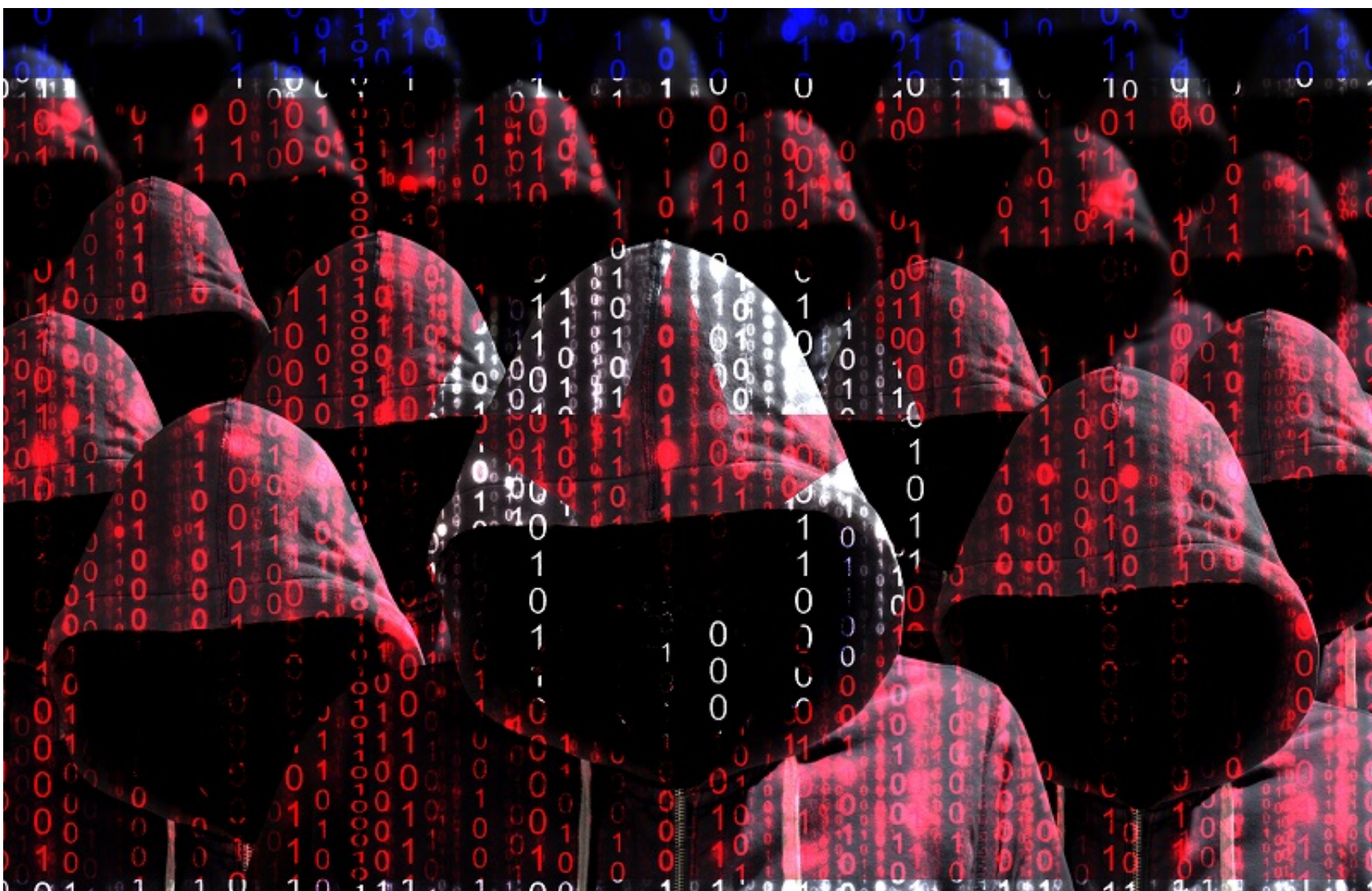
Twitter



Google Plus



Pinterest



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 TangoDaiwo, 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

SHARE



Facebook



Twitter



Google Plus



Pinterest

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

CISO MAG

https://cismag.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?



EVEN MORE NEWS

CISO MAG is the handbook for Chief Information Security Officer (CISO)s, CXOs, and every stakeholder of safe internet.

Contact us: cismag@eccouncil.org

> >

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

POPULAR CATEGORY

News	2554
Threats	1657
Features	594
Partnerships	215
Governance	191
Startups	161
Interviews	121

How to Update Web Browsers for Secure Browsing

How to Update Web Browsers for Secure Browsing

How to Update Web Browsers for Secure Browsing

How to Update Web Browsers for Secure Browsing

We Care

Ensuring that you get the best experience is our only purpose for using cookies. If you wish to continue, please accept. You are welcome to provide a controlled consent by visiting the cookie settings. For any further queries or information, please see our [privacy policy](#).

Do not sell my personal information.

Cookie Settings

Accept