New Linux Backdoor Attacking Linux Users Via Installation Packages

Date: 01st June 2024 | Severity: High

Summary

The North Korean hacker group Kimsuki has been using a new Linux malware called Gomir that is a version of the GoBear backdoor delivered via trojanized software installers.

Attack Vectors

The Springtail group launched a campaign delivering the new Troll Stealer malware, a Go-based information stealer with overlapping code from previous Springtail malware like GoBear or BetaSeed backdoors. Troll Stealer was distributed via Trojanized software installers, including those for TrustPKI, NX_PRNMAN from SGA Solutions, and Wizvera VeraPort, which was previously compromised in 2020.

Targeting government agencies by copying GPKI data, the campaign exploited legitimate websites requiring a login. GoBear was also spread, masquerading as a Korean transport org's app installer with a stolen cert. Symantec noticed Linux.Gomir, a Linux version of Springtail's GoBear Windows backdoor, which shares much code similarity.

When installed, it communicates over HTTP POST with its C&C server, sending an infection ID after hashing the hostname and the username and receiving Base64-encoded commands. Gomir employs custom encryption to decode received commands, with this ensuring that the system can support 17 GoBear-like operations.

This campaign reveals North Korean groups' inclination toward software supply chain vectors such as Trojanized installers, fake apps, and compromised update channels. Springtail carefully chooses popular software among desired South Korean audiences to Trojanize them on third-party websites where they must be installed. The group's developing tactics exhibit a sophisticated and targeted approach to cyber espionage operations.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hashes	• 30584f13c0a9d0c86562c803de350432d5a0607a06b24481ad4d92cdf7288213 • 7bd723b5e4f7b3c645ac04e763dfc913060eaf6e136eecc4ee0653ad2056f3a0 • d7f3ecd8939ae8b170b641448ff12ade2163baad05ca6595547f8794b5ad013b • 36ea1b317b46c55ed01dd860131a7f6a216de71958520d7d558711e13693c9dc • 8e45daace21f135b54c515dbd5cf6e0bd28ae2515b9d724ad2d01a4bf10f93bd • 6c2a8e2bbe4ebf1fb6967a34211281959484032af1d620cbab390e89f739c339 • 47d084e54d15d5d313f09f5b5fcdea0c9273dcddd9a564e154e222343f697822 • 8a80b6bd452547650b3e61b2cc301d525de139a740aac9b0da2150ffac986be4 • 380ec7396cc67cf1134f8e8cda906b67c70aa5c818273b1db758f0757b955d81 • ff945b3565f63cef7bb214a93c623688759ee2805a8c574f00237660b1c4d3fd • cc7a123d08a3558370a32427c8a5d15a4be98fb1b754349d1e0e48f0f4cb6bfc • 8898b6b3e2b7551edcceffbef2557b99bdf4d99533411cc90390eeb278d11ac8 • ecab00f86a6c3adb5f4d5b16da56e16f8e742adfb82235c505d3976c06c74e20 • d05c50067bd88dae4389e96d7e88b589027f75427104fdb46f8608bbcf89edb4
IP	• 216.189.159[.]34

Recommendation

- Keep computers, devices, and applications updated and patched.
- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Prioritize remediating known exploited vulnerabilities.
- Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- Regularly patch and update software and applications to their latest version and conduct regular vulnerability assessments.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis

Reference Link

- https://gbhackers.com/linux-backdoor-attack-installation-packages/