Recorded Future

Archived: 2026-04-05 22:42:58 UTC

Threat Activity Group RedFoxtrot Linked to Chinese Military Targets Bordering Asian Countries

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Insikt Research Report

Using a combination of large-scale, automated network traffic analytics and expert analysis, Recorded Future’s Insikt Group has identified ties between a suspected Chinese state-sponsored threat activity group tracked as RedFoxtrot and the Chinese military intelligence apparatus, People's Liberation Army (PLA) Unit 69010, located in Ürümqi, Xinjiang.

The cyber activity of the PLA has largely been a black box for the intelligence community since its 2015 organizational restructuring. Since then, public reporting has largely concentrated on groups linked to China's Ministry of State Security. This breakthrough report changes that, providing a rare glimpse into PLA cyber espionage operations.

Details revealed in this Insikt Group report include:

- A rare glimpse into PLA Unit 69010 cyber espionage operations and links that tie activity back to specific individuals.
- Specifics on network intrusions targeting aerospace and defense, government, telecommunications, mining, and research organizations in bordering Asian countries.
- Details into PLA operational infrastructure that has employed both bespoke and publicly available malware families commonly used by Chinese cyber espionage groups.

Ready to get started? Sign up now!

Recommended Content

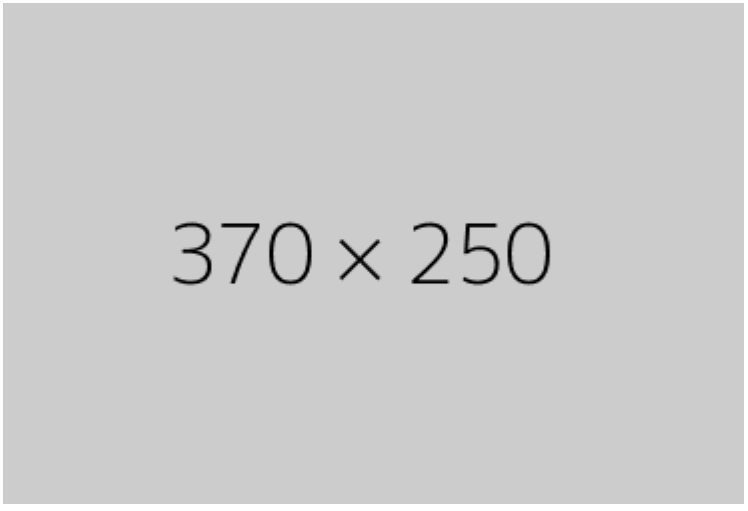
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Ut Enim Minima

Sed ut perspiciatis unde omnis iste natus error sit voluptatem!

Sed ut perspiciatis

Sed ut perspiciatis unde omnis iste natus error sit voluptatem!



Error sit voluptatem!

Sed ut perspiciatis unde omnis iste natus error sit voluptatem!

Consectetur adipiscing elit...

Lorem C.

"Et harum quidem rerum facilis est et expedita distinctio!"

Ipsem T.

"Et harum quidem rerum facilis est et expedita distinctio!"

Aoeren T.

"Et harum quidem rerum facilis est et expedita distinctio!"

Source: https://go.recordedfuture.com/redfoxtrot-insikt-report