CSO

NEWS

Russian military attacked, possibly by Chinese cyber group

Members of the Russian military have been receiving well-crafted phishing emails since mid-summer

By Maria Korolov | Follow

CSO | Sep 17, 2015 12:47 PM PT

Members of the Russian military have been receiving well-crafted phishing emails since mid-summer from attackers that use Chinese-language tools and Chinese command-and-control installations, according to a report released yesterday.

The campaign also targets Russian telecom firms and, as collateral damage, has hit Russian-speaking financial analysts who cover the telecom space for global financial firms, according to Sunnyvale, Calif.-based security vendor Proofpoint, Inc.

In the past, the same group of attackers has been reportedly targeting military installations in Central Asia.

MORE ON CSO: How to spot a phishing email

"Actor attribution is always tricky, but there is significant use of Chinese-language build tools and command-and-control goes back to host sites in Chinese-influenced areas," said Kevin Epstein, the company's vice president of the threat operations center.

Occam's Razon would mean that the Chinese are the most likely actors, he said, but there's always the possibility that some other group entirely is deliberately trying to cast blame on the Chinese.

In addition, the attack could be government sponsored, or it could be a financially-motivated group planning to sell the military intelligence it gathers.

"There is a world market for classified data of any time," said Epstein. "There are documented cases in the past where private hackers hacked into various institutions and then sold the data to nation states. The lines are increasingly blurred in the world of cybersecurity."

The attack starts with a well-written Russian-language email that seems to come from someone else in the targeted military division or an analyst section from the same group of the military, he said.

It comes with an attached document, a Microsoft Word file with a published article about the history of military testing in Russia.

"It's a decoy document," said Epstein. "You double-click on it, you open it, you read it, you think, 'Ah, that was kind of interesting.' Then you close it and you don't think about it again. But when it closes, it activates a macro, and the macro triggers a secondary file to take action, which is to download a third file, which is the nasty stuff."

That's when the malware takes over the computer and everything the user has access to, the attackers now have access to.

"Any anti-virus program wouldn't see a virus in the document because there's no virus in the document," he said. "And the trigger on closing is a common anti-sandboxing technique because most sandboxes check for triggering when documents are opened, not when they are closed."

According to Epstein, Russian-language speakers on his staff say that the email is very convincing, and if they didn't know to watch out for it -- or hadn't had enough coffee -- they might well have clicked on it.

"This looks like something a colleague might well send you as a reference, and there is nothing there to trigger suspicion," he said.

Maria Korolov — *Contributing Writer*

Insider: How a good CSO confronts inevitable bad news ›

View 3 Comments

10 Super Cars Every Man Wants

Carophile

How Do Pro Golfers Swing So Fast?

Revolution Golf

Reducing Infant Mortality With 'Kangaroo Care'

Financial Times

Fast & Comprehensive Hotel Price Comparison

Hotel Bargains

The Most Exciting MMORPG You've Ever Played. Don't miss this!

Sparta Online Game

The 5 best hidden features in iOS 9

Phishing attacks targeting government agencies linked to Hacking Team breach

Attackers go on malware-free diet

Easy To Pick Up, But Hard To Put Down. Dive In To The World of Nords!

Nords Online Game