North Korean hackers target Russian diplomats using New Year greetings

By Catalin Cimpanu

Published: 2023-01-09 · Archived: 2026-04-06 00:59:39 UTC

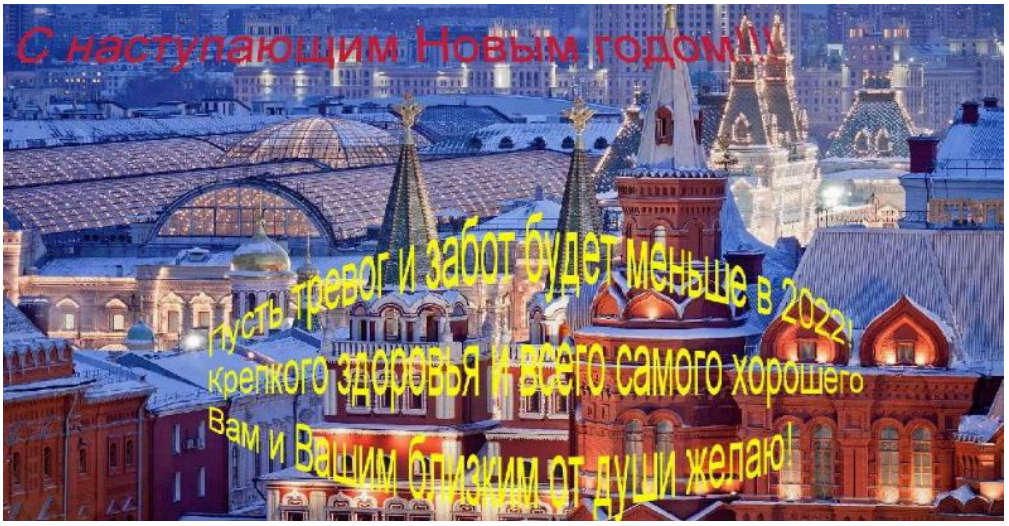
A North Korean cyber-espionage group has targeted Russian embassy diplomats over the winter holidays with emails carrying New Year greetings in the hopes of infecting them with malware.

The attacks have been linked to a threat actor known as Konni, and have been taking place since at least December 20, cybersecurity firm Cluster25 said in a report published on Monday.

"[T]hese emails used the New Year Eve 2022 festivity as decoy theme," Cluster25 researchers said.

"Contrary to its past actions, the North Korean APT group this time did not use malicious documents as attachments; instead, they attached a .zip file type named 'поздравление.zip', which means 'congratulation' in Russian, containing an embedded executable representing the first stage of the infection."

According to Cluster25, the ZIP files contained a Windows screensaver (.scr) file that, when executed, installed a screensaver with Russian holiday greetings, but also the Konni remote access trojan (RAT), the malware after which the group was named, and which granted the attacker full control over the infected systems.

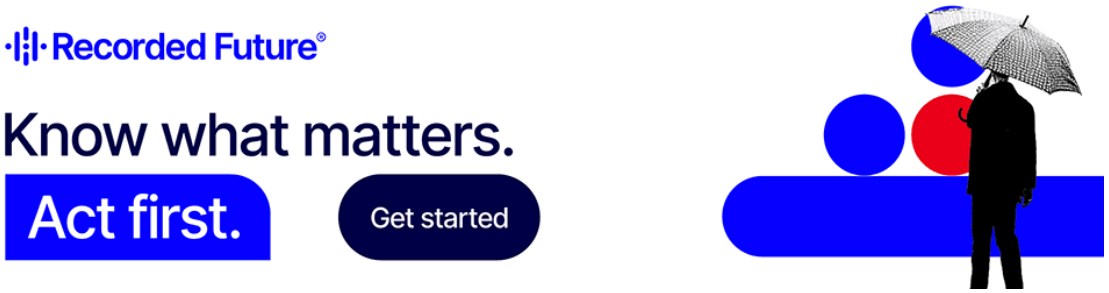


Cluster25 said it only detected emails sent to the Russian Embassy in Indonesia but the attack most likely targeted other embassies as well.

To look as authentic as possible, Cluster25 said the emails were also spoofed using a @mid.ru account as the sender to pretend that the email came from the Russian Embassy in Serbia.

The security firm said they've been tracking recent Konni attacks targeting Russian diplomats since at least August 2021, as part of a series of attacks first detected and detailed by Malwarebytes last year.

All in all, attacks using Windows screensaver files have been heavily abused by malware operations in the early 2000s and might look too simplistic to work, but the reality is that non-technical users still fall for this technique, as it was the case last year with NFT creators.



Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.

Source: https://therecord.media/north-korean-hackers-attack-russian-diplomats-using-new-year-greetings/