Russian cyberspies targeted the Slovak government for months

By Catalin Cimpanu

Published: 2022-12-13 · Archived: 2026-04-05 23:46:07 UTC

A Russian cyber-espionage group linked to one of Russia's intelligence forces has targeted the Slovak government for months, Slovak security firms ESET and IstroSec said this week.

The attacks were attributed to a group known as the Dukes, Nobelium, or APT29, which cyber-security agencies from the US and other countries formally linked to the Russian Foreign Intelligence Service, also known as the SVR, earlier this year after its attack on software company SolarWinds.

ESET and IstroSec said SVR hackers recently orchestrated several spear-phishing campaigns between February and July 2021 that targeted Slovak officials.

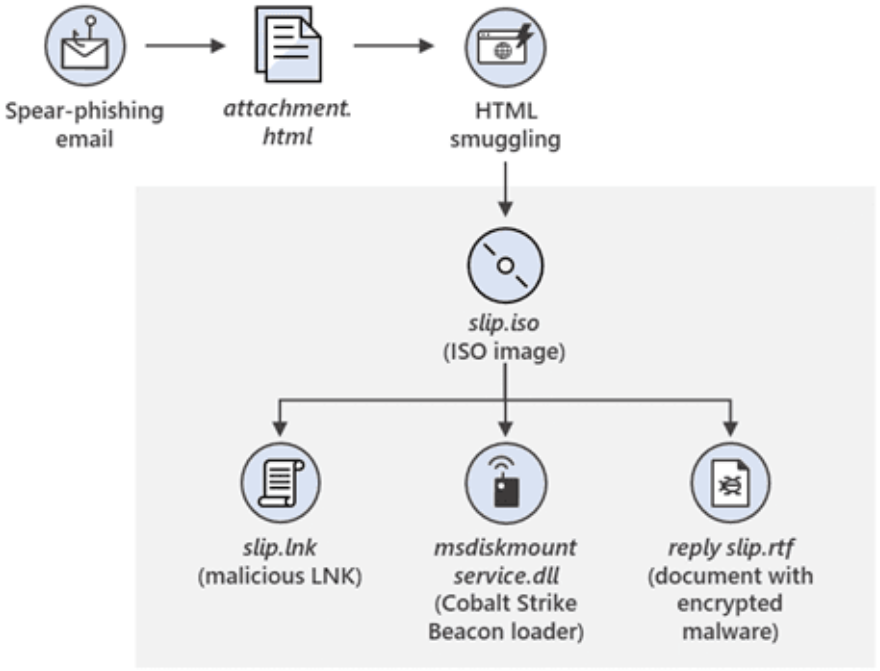
SVR operators sent emails to Slovak diplomats posing as the Slovak National Security Authority (NBU). The documents, usually an ISO image file, would download and install a Cobalt Strike backdoor on infected systems.

In a recent talk at the Def Con security conference this year, IstroSec researchers described how they found the SVR command-and-control servers used in these attacks.

The IstroSec team said that some of the SVR C&C servers also hosted documents that appeared to have been aimed at Czech government officials as well.

ESET confirmed the attacks earlier today and said that they've also tracked the group's recent campaign, which targeted diplomats in more than 13 European countries.

According to ESET, all the attacks appeared to follow the same tactic (email-> ISO disk image -> LNK shortcut file -> Cobalt Strike backdoor), a tactic that was also described in two reports earlier this year from Volexity and Microsoft. In some of these attacks, the Russian espionage group also relied on a Safari iOS zero-day to infect diplomats who read their emails on their iPhones.



Source: https://therecord.media/russian-cyberspies-targeted-slovak-government-for-months/