Cyberattacks enabled disinformation in Lithuania

Reference: Memo [1904151-1] – Version: 1.0
Keywords: hacking, disinformation, social media, defence
Sources: publicly available information

Key Points

- The Lithuanian Ministry of Defence was targeted by a disinformation campaign.
- The dissemination of disinformation was likely enabled and facilitated by cyberattacks.

Summary

On April 11, Lithuanian media reported that the Lithuanian Ministrer of Defence (MoD), M. Karoblis, had been targeted by a disinformation campaign. A fake report claimed that Mr. Karoblis 'accepted a bribe of USD 586,000 euros [sic] and this was allegedly revealed by the MoD sanctioned audit'.

The fake report was sent to several email addresses (individuals working in the Lithuanian Parliament, Government office, President's office) from a sender masquerading as a MoD employee.

The fake news was also inserted as an article into three media websites: 'Kas vyksta Kaune', a regional media outlet, 'Baltic Times', a Riga-based English language news website, and "OpEdNews" a US-based progressive/liberal news, antiwar activism, and opinion website founded by Rob Kall in 2003. Contrary to the first two websites, the third one has a track record in spreading fake news. Experts pointed out that both 'Kas vyksta Kaune' and 'Baltic Times' had been targeted by cyberattacks in 2018.

Comments

In this campaign, the dissemination of disinformation was likely enabled and facilitated by cyberattacks.

It is plausible that the targeted email campaign was preceded by preliminary reconnaissance and information-gathering activities (possibly via intrusion) to find the email addresses of the recipients and to masquerade the sender's address in the MoD. This tactic (collect recipient's email addresses from a non-public address book, lure recipients by spoofing the email address of a partner) is often used to deliver malware to a targeted audience.

While the public dissemination of fake news mostly leverage social media platforms, in this case illegitimate articles were posted on traditional news websites. To do this, attackers likely compromised two news websites ('Kas vyksta Kaune', 'Baltic Times') with no known track record in wilful disinformation actions in order to plant the article. It is worth mentioning that, in January, another Lithuanian news portal 'tv3' had already been hacked for disinformation purposes.

News websites are frequently scanned for vulnerabilities by malicious actors. A successful compromise can be used for different purposes:

- Enable denials of service or defacements to disseminate politically motivated hacktivists messages.
- Turn websites into watering holes, to infect the computers of visitors for espionage purposes.
- Plant a fabricated, yet credible, article with a spoofed signature of a known author, as part of a disinformation campaign.