

Rapport menaces et incidents - CERT-FR

Archived: 2026-04-05 17:36:47 UTC

Une gestion de version détaillée se trouve à la fin de ce document.

Version française: 

ANSSI has observed a number of phishing campaigns directed against French entities since February 2021. Technical indicators correspond to activities associated with the Nobelium intrusion set. These campaigns have succeeded in compromising email accounts belonging to French organisations, and then using these to send weaponised emails to foreign institutions. Moreover, French public organisations have also been recipients of spoofed emails sent from supposedly compromised foreign institutions. Overlaps have been identified in the tactics, techniques & procedures (TTP) between the phishing campaigns monitored by ANSSI and the SOLARWINDS supply chain attack in 2020.

This report lays out the technical information related to the phishing campaigns, beginning with details as to the nature of the malicious activities observed, the TTPs and the attack infrastructure. Recommendations and indicators of compromise are available at the end of the document.

Indicators of compromise are available in structured formats on the page [CERTFR-2021-IOC-005](#).

[DOWNLOAD THE REPORT](#)

Gestion détaillée du document

le 06 décembre 2021

Version initiale

Source: <https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-011/>