Objet: 🇬🇧 Phishing campaigns by the Nobelium intrusion set

cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-011/

S.G.D.S.N

Agence nationale
de la sécurité des
systèmes d'information

Paris, le 06 décembre 2021

N° CERTFR-2021-CTI-011

Affaire suivie par: CERT-FR

le 06 décembre 2021

Rapport Menaces et Incidents du CERT-FR

Gestion du document

Référence	CERTFR-2021-CTI-011
Titre	🇬🇧 Phishing campaigns by the Nobelium intrusion set
Date de la première version	06 décembre 2021
Date de la dernière version	06 décembre 2021
Source(s)	
Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

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