

Objet: Malicious activities linked to the Nobelium intrusion set

Paris, le 19 juin 2024

Gestion du document


Référence	CERTFR-2024-CTI-006
Titre	 Malicious activities linked to the Nobelium intrusion set
Date de la première version	19 juin 2024
Date de la dernière version	19 juin 2024
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.

Several cyberattacks against French diplomatic entities can be linked to the Nobelium intrusion set. Nobelium is an intrusion set active since at least October 2020, used against high-value targets, most likely for espionage purposes. Western diplomatic entities, such as embassies and Ministries of Foreign Affairs, account for the majority of known victims of Nobelium. However, several IT companies have also reported that they have been targeted by Nobelium's operators in late 2023 and 2024.

This document is based upon elements collected by ANSSI, elements shared by its national partners (known as C4 members), and publicly available reports. It exposes phishing campaigns linked to Nobelium against French public and diplomatic entities aiming to exfiltrate strategic intelligence. It also recapitulates attacks publicly attributed to Nobelium against international IT companies through which Nobelium's operators potentially seek to strengthen their offensive capabilities.

The Nobelium intrusion set has been publicly linked to the Russian SVR by different sources. Nobelium's activities against government and diplomatic entities represent a national security concern and endanger French and European diplomatic interests.

Indicators of compromise are available in structured formats on the page [CERTFR-2024-IOC-001](#).

[DOWNLOAD THE REPORT](#)

Gestion détaillée du document

le 19 juin 2024

Version initiale

