Objet: 🇫🇷/🇬🇧 [Maj] Campagne d’attaque du mode opératoire APT31 ciblant la France

cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-003

S.G.D.S.N

Agence nationale
de la sécurité des
systèmes d'information

Paris, le 21 juillet 2021

N° CERTFR-2021-IOC-003

Affaire suivie par: CERT-FR

le 21 juillet 2021

Indicateurs de compromission du CERT-FR

Gestion du document

Référence	CERTFR-2021-IOC-003
Titre	🇫🇷/🇬🇧 [Maj] Campagne d’attaque du mode opératoire APT31 ciblant la France
Date de la première version	21 juillet 2021
Date de la dernière version	15 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.

🇫🇷 L'ANSSI traite actuellement une vaste campagne de compromission touchant de nombreuses entités françaises. Cette dernière, toujours en cours et particulièrement virulente, est conduite par le mode opératoire APT31 (voir CERTFR-2021-CTI-012 pour plus d'informations).

Les investigations montrent que ce mode opératoire compromet des routeurs pour les utiliser comme relais d'anonymisation, préalablement à la conduite d'actions de reconnaissance et d'attaques. Ainsi, des marqueurs, issus des routeurs compromis par l'attaquant, sont fournis pour permettre de rechercher des compromissions (depuis le début de l'année 2021) et de les mettre en détection.

Toute détection à partir de ces éléments ne constitue pas nécessairement une preuve de compromission et doit être analysée afin de lever le doute.

L'ANSSI rappelle que l'intrusion dans un système d'information est une infraction pénale et pourra mettre en relation toute entité visée dans le cadre de cette campagne avec les services judiciaires compétents.

Merci de faire remonter à l'ANSSI tout incident découvert en lien avec cette campagne à l'adresse suivante : cert-fr.cossi@ssi.gouv.fr.

[Mise à jour] Les routeurs compromis dont sont issus les marqueurs de la présente publication ne sont plus utilisés à ce jour par l'attaquant comme relais d'anonymisation. En revanche, ces marqueurs peuvent toujours servir à des fins de recherches de compromission antérieure, depuis le début de l'année 2021.

🇬🇧 ANSSI is currently handling a large intrusion campaign impacting numerous French entities. Attacks are still ongoing and are led by an intrusion set publicly referred as APT31 (see CERTFR-2021-CTI-013 for more information).

It appears from our investigations that the threat actor uses a network of compromised home routers as operational relay boxes in order to perform stealth reconnaissance as well as attacks. As such, indicators of compromises (IOCs) are shared to help assess possible compromises (searches should start at the beginning of 2021) and used in detection services.

Finding one of the IOCs in logs does not mean the entire system has been compromised and further analysis will be required.

ANSSI encourages recipients to report additional information about any incident linked to this campaign and can be reached at cert-fr.cossi@ssi.gouv.fr

[Update] The infected home routers mentioned in this publication are no longer used by the threat actor. However, the shared IOCs can still be used to assess potential past breaches (from the beginning of 2021 onwards).

TÉLÉCHARGER LES IOCs (CSV)
🇬🇧 DOWNLOAD IOC (CSV)

TÉLÉCHARGER LES IOCs (JSON)
🇬🇧 DOWNLOAD IOC (JSON)

Gestion détaillée du document

le 21 juillet 2021
Version initiale

le 15 décembre 2021
Mise à jour sur l'activité des IOCs