RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

COMPRENDRE LES RISQUES

LES RANÇONGICIELS Pro

Une attaque de type rançongiciel, ou *ransomware* en anglais, consiste à compromettre un équipement ou un système d'information pour en bloquer l'accès, en chiffrer et/ou en copier les données en réclamant une rançon à la victime pour les rendre à nouveau accessibles et/ou ne pas les rendre publiques.

Ce type d'attaque est généralement consécutif à une intrusion suite à l'exploitation de failles de sécurité ou d'une sécurisation insuffisante des systèmes exposés sur Internet (NAS, RDP, VPN…), ou encore par la compromission d'un compte ou d'une machine du système d'information suite à un hameçonnage (*phishing*) ou l'infection par un programme malveillant (virus).

BUT RECHERCHÉ

Extorquer de l'argent à la victime en échange de la promesse (pas toujours tenue) de lui restituer l'accès aux équipements ou aux données chiffrées et/ou de la non-divulgation de ses données dérobées.

Durant l'attaque, les cybercriminels cherchent souvent à détruire les sauvegardes de la victime pour l'empêcher de restaurer ses données.

Les attaques sont généralement déclenchées durant une période de moindre activité de la victime (la nuit, le week-end…) pour maximiser les chances qu'elles ne puissent pas être détectées rapidement et interrompues.

Les attaquants peuvent mettre en œuvre d'autres moyens de pression sur la victime : revendication publique de l'attaque, attaque en déni de service (DDoS) contre son site Internet…

Une attaque par rançongiciel peut conduire à paralyser complètement l'activité de l'organisation qui en est victime.

FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS QUALIFIÉS

Vous trouverez sur www.cybermalveillance.gouv.fr des professionnels en cybersécurité susceptibles de pouvoir vous apporter leur assistance technique tant sur la sécurisation de votre système d'information qu'en cas d'incident.

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

MESURES PRÉVENTIVES

Réalisez des sauvegardes régulières de vos données en gardant des **copies déconnectées**.

Appliquez de manière régulière et systématique les mises à jour de sécurité des logiciels de tous vos équipements.

Utilisez une solution de protection contre les programmes et comportements malveillants (antivirus, EDR…) sur l'ensemble de vos postes de travail et serveurs.

Utilisez un pare-feu pour protéger les accès extérieurs à votre réseau informatique interne.

Sécurisez les accès distants à votre réseau informatique interne en utilisant un **VPN** et systématisez l'emploi d'une **double authentification**.

Limitez les droits des utilisateurs selon le « principe de moindre privilège » pour accéder aux données et applications.

L'administration des systèmes doit se faire depuis des **postes ou comptes dédiés sans accès autorisé à Internet**.

Utilisez des mots de passe suffisamment longs, complexes et différents pour chaque service.

Activez la double authentification sur tous vos services et applications hébergés sur Internet (SaaS) qui peuvent contenir des données critiques de votre organisation.

N'installez pas d'application ou de programme « piratés » ou dont l'origine ou la réputation sont douteuses car ils peuvent souvent être piégés.

Sensibilisez l'ensemble de vos collaborateurs aux risques et **rappelez régulièrement les consignes de sécurité**.

Avancé **Supervisez la sécurité de votre système d'information** afin d'identifier toute activité anormale.

Avancé **Renforcez la sécurité de vos interconnexions à Internet** avec des dispositifs complémentaires (proxy, WAF…).

Avancé **Segmentez votre réseau informatique** en différentes zones (utilisateurs, administrateurs, serveurs…) avec des dispositifs de filtrage entre ces zones (VLAN, DMZ, pare-feu…).

COMPRENDRE LES RISQUES

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

SI VOUS ÊTES VICTIME

COUPEZ LES CONNEXIONS À INTERNET du réseau attaqué.

DÉCONNECTEZ LES MACHINES TOUCHÉES du réseau informatique.

DÉBRANCHEZ VOS SAUVEGARDES DU RÉSEAU si elles y sont connectées.

N'ÉTEIGNEZ PAS LES MACHINES TOUCHÉES au risque de détruire des éléments d'investigation. Privilégiez une mise en veille prolongée si le chiffrement est en cours.

NE DÉMARREZ PAS LES MACHINES ÉTEINTES pour éviter qu'elles ne soient à leur tour compromises.

ALERTEZ IMMÉDIATEMENT VOTRE SERVICE OU PRESTATAIRE INFORMATIQUE si vous en disposez.

PILOTEZ LA CRISE :

- **Constituez une équipe de gestion de crise** avec les différents acteurs concernés.
- **Tenez un registre** des évènements et actions réalisées.
- **Gérez votre communication** avec le juste niveau de transparence.
- **Mettez en œuvre des solutions** de secours (PCA-PRA...).

NE PAYEZ PAS LA RANÇON réclamée car vous n'êtes pas certain que les cybercriminels tiendront parole et vous financeriez leur activité.

CONSERVEZ OU FAITES CONSERVER LES PREUVES par un professionnel (journaux, copies ou disques des matériels touchés...) qui seront des éléments d'investigation.

DÉPOSEZ PLAINTE avant la réinstallation des équipements touchés (et dans les 72 heures si vous disposez d'une assurance « cyber »).

DÉCLAREZ LE SINISTRE AUPRÈS DE VOTRE ASSUREUR qui peut vous dédommager, voire vous apporter une assistance selon votre niveau de couverture.

NOTIFIEZ L'INCIDENT À LA CNIL dans les 72 heures si des données personnelles ont pu être consultées, modifiées ou détruites par les cybercriminels.

IDENTIFIEZ L'ORIGINE DE L'ATTAQUE et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

IDENTIFIEZ LES ACTIVITÉS DE L'ATTAQUANT au sein de votre système informatique.

ÉVALUEZ ET VÉRIFIEZ L'ÉTENDUE DE L'INTRUSION à d'autres équipements de votre système informatique. Identifiez les informations perdues ou compromises.

RÉALISEZ UNE ANALYSE ANTIVIRALE COMPLÈTE (scan) des équipements touchés.

RECHERCHEZ SI UNE SOLUTION DE DÉCHIFFREMENT EXISTE. Le site No More Ransom propose des solutions qui peuvent fonctionner dans certains cas.

RÉINSTALLEZ LES SYSTÈMES TOUCHÉS puis restaurez les données depuis une sauvegarde antérieure à l'attaque réputée saine.

CHANGEZ TOUS LES MOTS DE PASSE d'accès aux équipements et systèmes qui ont pu être compromis.

METTEZ À JOUR L'ENSEMBLE DE VOS LOGICIELS et équipements après leur réinstallation et avant de les remettre en service.

FAITES UNE REMISE EN SERVICE PROGRESSIVE ET CONTRÔLÉE en surveillant son fonctionnement pour pouvoir détecter toute nouvelle attaque.

COMPRENDRE LES RISQUES

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

Atteinte à un système de traitement automatisé de données (STAD) : article 323-1 du code pénal.

Extorsion de fonds : article 312-1 du code pénal.

Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite : article 226-18 du code pénal.

En savoir plus sur les rançongiciels :

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

V260204