Les essentiels de Groupama

QUE FAIRE EN CAS DE CYBER ATTAQUE ?

À distribuer sans modération à tous vos collaborateurs !

Groupama
la vraie vie s'assure ici

LES PRINCIPALES ATTAQUES

Vous trouverez plus loin des fiches décrivant succinctement les principales attaques et les moyens de les traiter :

Écran crypté et demande de rançon
› Rançongiciel ou *Ransomware*

Envoi d'informations aux voleurs
› Hameçonnage ou *Phishing*

Mise hors service de vos sites internet par des requêtes trop nombreuses
› Déni de service ou DDoS

Site Internet modifié ou remplacé
› Défiguration de site

Demande de paiement pour réparer vos problèmes
› Faux support technique

Ces **attaques** sont **visibles** et ont pour but de vous extorquer de l'argent ou de nuire à votre image.
Il existe d'autres types d'attaques quasi « **invisibles** » qui ont pour but de voler vos informations ou de les déformer (emails, propositions commerciales, coordonnées bancaires, brevets, etc.). Elles sont en général identifiables uniquement par des professionnels.

PREMIER RÉFLEXE

APPELEZ DIRECTEMENT LA PLATEFORME GROUPAMA
et bénéficiez d'un accompagnement personnalisé.

RANÇONGICIEL OU *RANSOMWARE*

QU'EST-CE QU'UN RANÇONGICIEL OU *RANSOMWARE* ?

Extorsion d'argent

Vous ne pouvez plus accéder à vos fichiers et on vous demande de payer une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*, en anglais) !

But : réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

Technique : blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.

QUE FAIRE FACE À UN RANÇONGICIEL ?

Comment réagir ?

- Débranchez la machine d'Internet et du réseau local.
- Alertez le support informatique de votre entreprise.
- Ne payez pas la rançon.
- Déposez plainte.
- Identifiez et corrigez l'origine de l'infection.
- Essayez de désinfecter le système et de déchiffrer les fichiers.
- Réinstallez le système et restaurez les données.
- Faites-vous assister par des professionnels.

HAMEÇONNAGE OU *PHISHING*

QU'EST-CE QUE L'HAMEÇONNAGE OU *PHISHING* ?

Vol de données

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (*phishing* en anglais) !

But : voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

Technique : leurre envoyé *via* un faux message, SMS ou appel téléphonique émanant d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites e-commerce…

QUE FAIRE FACE À UN HAMEÇONNAGE ?

Comment réagir ?

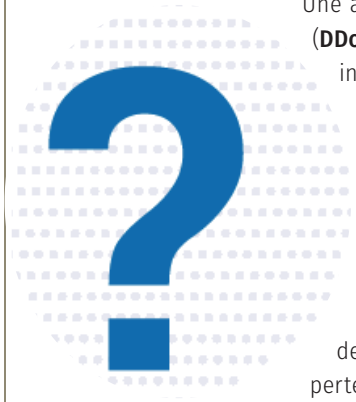
- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique.
- Au moindre doute, contactez directement l'organisme concerné pour confirmer.
- Faites opposition immédiatement (en cas d'arnaque bancaire).
- Changez vos mots de passe divulgués/compromis.
- Déposez plainte.
- Signalez-le sur les sites spécialisés (voir liens utiles).

LIENS UTILES

Signal-spam.fr **Phishing-initiative.fr** **Info Escroqueries : 0 805 805 817 (gratuit)**

DÉNI DE SERVICE OU ATTAQUE DDoS

QU'EST-CE QU'UN DÉNI DE SERVICE OU UNE ATTAQUE DDoS ?



Une attaque en déni de service ou en déni de service distribué (**DDoS** pour *Distributed Denial of Service* en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusquà le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service.

Ce type d'attaque peut être très grave pour l'organisation qui en est victime.

Durant l'attaque, le site ou service n'est plus utilisable, au moins temporairement, ou dfficilement, ce qui peut entraîner des pertes directes de revenus pour les sites marchands et des pertes de productivité.

L'attaque est souvent visible publiquement, voire médiatiquement, et laisse à penser que l'attaquant aurait pu prendre le contrôle du serveur, donc potentiellement accéder à toutes ses données, y compris les plus sensibles (données personnelles, bancaires, commerciales...) : ce qui porte directement atteinte à l'image et donc à la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires...

BUT RECHERCHÉ

Rendre un service indisponible.

Le cybercriminel agit pour des motivations politiques, idéologiques, par goût du challenge, chantage, vengeance, ou pour des raisons économiques (concurrence).

Cette attaque peut être utilisée pour faire diversion par rapport à une autre attaque visant à voler les données sensibles.

QUE FAIRE FACE À UN DÉNI DE SERVICE ?

Filtrez les requêtes de l'attaquant au niveau de votre pare-feu ou de votre hébergeur.

Récupérez les fichiers de journalisation (logs) de votre pare-feu et des serveurs touchés qui seront des éléments d'investigation.

Réalisez une copie complète de la machine attaquée et de sa mémoire.

Évaluez les dégâts causés et les éventuelles informations perdues.

Assurez-vous que l'attaquant n'a pas profité du déni de service pour accéder à des informations sensibles, y compris sur d'autres systèmes. En cas de doute, **changez tous les mots de passe d'accès** aux serveurs touchés ou suspectés de l'être et envisagez leur réinstallation complète à partir de sauvegardes réputées saines.

Faites-vous assister au besoin par des professionnels qualifiés pour la remise en production et la sécurisation des serveurs touchés. Vous trouverez sur **www.cybermalveillance.gouv.fr** des prestataires spécialisés susceptibles de pouvoir vous apporter leur expertise.

L'attaquant peut aussi vous demander une rançon afin de ne pas attaquer : NE PAYEZ PAS ET PORTEZ PLAINTE !

DÉFIGURATION DE SITE

QU'EST-CE QU'UNE DÉFIGURATION DE SITE ?

La défiguration est l'altération par un pirate de l'apparence d'un site Internet, qui peut devenir uniformément noir, blanc ou comporter des messages, des images, des logos ou des vidéos sans rapport avec l'objet initial du site, voire une courte mention comme « owned » ou « hacked ».

La défiguration est le signe visible qu'un site Internet a été attaqué et que l'attaquant en a obtenu les droits lui permettant d'en modifier le contenu.

Durant l'attaque, le site n'est souvent plus utilisable, ce qui peut entraîner des pertes directes de revenus et de productivité.

Par ailleurs, en étant visible publiquement, la défiguration démontre que l'attaquant a pu prendre le contrôle du serveur, et donc, accéder potentiellement à des données sensibles (personnelles, bancaires, commerciales…) : ce qui porte directement atteinte à l'image et à la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires…

QUE FAIRE FACE À UNE DÉFIGURATION DE SITE ?

Si possible, **déconnectez d'Internet** le site concerné (souvent dans les faits, déconnection du serveur).

Récupérez les fichiers de journalisation (logs) de votre pare-feu, serveur mandataire (proxy) et des serveurs touchés qui seront des éléments d'investigation.

Réalisez une copie complète de la machine attaquée et de sa mémoire.

Identifiez les éléments sensibles qui ont pu être copiés ou détruits.

Identifiez le vecteur qui a permis de prendre le contrôle de la machine.

Déposez plainte au commissariat de police ou à la gendarmerie dont vous dépendez et tenez à disposition des enquêteurs tous les éléments de preuves en votre possession.

Lorsque vous aurez repris le contrôle de la machine touchée, **corrigez toutes les vulnérabilités et changez tous les mots de passe** avant de la remettre en ligne.

Faites-vous assister au besoin par des professionnels qualifiés. Vous trouverez sur **www.cybermalveillance.gouv.fr** des prestataires spécialisés susceptibles de pouvoir vous apporter leur expertise.

L'attaquant peut aussi vous demander une rançon afin de ne pas attaquer : NE PAYEZ PAS ET PORTEZ PLAINTE !

FAUX SUPPORT TECHNIQUE

QU'EST-CE QU'UN FAUX SUPPORT TECHNIQUE ?

Escroquerie financière

Votre ordinateur est bloqué et on vous demande de rappeler un support technique ? Vous êtes victime d'une arnaque au faux support !

But : inciter la victime à payer un pseudo-dépannage informatique et/ou à lui faire souscrire des abonnements payants.

Technique : faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement (par écran bloqué, téléphone, SMS, courriel, etc.).

QUE FAIRE FACE À UN FAUX SUPPORT TECHNIQUE ?

Comment réagir ?

- Ne répondez pas.
- Conservez toutes les preuves.
- Redémarrez votre appareil.
- Purgez le cache, supprimez les cookies et réinitialisez les paramètres de votre navigateur.
- Désinstallez tout nouveau programme suspect.
- Faites une analyse antivirus.
- Changez tous vos mots de passe.
- Faites opposition auprès de votre banque si vous avez payé.
- Déposez plainte.

LIENS UTILES

Internet-signalement.gouv.fr **Info Escroqueries : 0 805 805 817 (gratuit)**

PROCÉDURES D'URGENCE ET D'ALERTE - PRÉCAUTIONS

PROCÉDURES D'URGENCE ET D'ALERTE

- **Avoir des outils de détection et d'alerte** ainsi que des personnes disponibles pour traiter les alertes est indispensable.
- **Savoir qui contacter** chez ses prestataires et fournisseurs de sécurité (prévoir une liste de personnes à contacter et des moyens de communication de crise alternatifs).
- Définir des cas précis nécessitant la coupure du réseau, de façon à déporter cette prise de responsabilité sur une **procédure validée** et non une personne qui va forcément hésiter.
- Les **assurances** peuvent aussi servir de « pompiers » et de soutien lorsque les ressources ou compétences internes ne sont pas suffisantes.
- Les **plans de continuité** définis en amont des crises doivent prévoir les moyens de travailler avec des ressources informatiques réduites.
- Disposer d'une **vision claire** de son parc informatique.

QUELQUES PRÉCAUTIONS SIMPLES

- Choisir avec soin ses mots de passe avec **12 caractères de type différent** (majuscules, minuscules, chiffres, caractères spéciaux), n'ayant aucun lien avec vous et ne figurant pas dans le dictionnaire.
- **Mettre à jour** régulièrement vos logiciels.
- Effectuer des **sauvegardes régulières** (a minima hebdomadaires) sur des supports externes indépendants et déconnectés du système d'information et conservés à l'extérieur de l'entreprise ou sur le cloud. Faire régulièrement des tests de restauration pour vérifier l'efficacité des sauvegardes et des plans de secours.
- **Sécuriser l'accès wi-fi** de votre entreprise, privilégier une installation filaire.
- Être aussi **prudent** avec son smartphone ou sa tablette qu'avec son ordinateur.
- Être **prudent** lors de l'utilisation de sa messagerie.

DES QUESTIONS, UN CONSEIL ?

Connectez-vous sur **groupama.fr/contact**
et cliquez sur l'une de ces 4 solutions :

Être appelé

Appeler

Envoyer un mail

Prendre rendez-vous

Coordonnées de votre conseiller

Ce document a vocation à informer le lecteur sur les principales attaques informatiques dont il peut être l'objet et les mesures à prendre en cas de cyber attaque. Le cas échéant, il ne le dispense pas de faire appel à un spécialiste qualifié. De manière générale, aucune responsabilité ne pourra être retenue contre Groupama du fait de l'usage de ce document».

GROUPAMA ASSURANCES MUTUELLES
Caisse Régionale d'Assurances Mutuelles Agricoles
Entreprise régie par le Code des assurances et soumise à l'Autorité de Contrôle Prudentiel et de Résolution - 4, place de Budapest - CS92459 - 75436 Paris Cedex 09

CYBEX ASSISTANCE
SAS au capital de 100 000 €
38 rue de Villiers, 92532 Levallois-Perret Cedex
RCS Nanterre 848 560 694

Document et visuels non contractuels - 03/2020.
Photo et illustrations : © Shutterstock, Cybex. PAO/SP3

Groupama participe à la protection de l'environnement en sélectionnant un imprimeur référencé "Imprim'Vert" ainsi que des papiers issus de forêts gérées durablement.

ÉDITION : MARS 2020

Groupama
la vraie vie s'assure ici