URGENT - DANGER – URGENT

Sécurité économique territoriale
Auvergne - Rhône-Alpes

RANÇONGICIEL : NOUVELLE ATTAQUE MONDIALE

Depuis le 27 juin 2017, un nouveau rançongiciel dénommé « PETRWAP » frappe la France et de nombreux autres pays.

Comme ce fut déjà le cas pour Wannacry en mai 2017, les ordinateurs travaillant sous environnement Windows* sont impactés. *Le mode de propagation** *(mails avec pièces jointes piégées, mises à jours de logiciels piégées, ...)* ***est pour l'heure inconnu.

De source média, plus de 2000 entreprises et institutions auraient été recensées à travers le monde, mais ce bilan risque de s'alourdir.

COMMENT MINIMISER LES RISQUES ?

♦ D'***effectuer des sauvegardes quotidiennes*** et ***multiples. Faire des tests de restauration*** pour s'assurer de leur viabilité. (Si vous optez pour une sauvegarde en local (*Disque dur, clé USB, …*), ne connecter le support que le temps de l'opération).

♦ De ***mettre impérativement à jour*** les systèmes d'exploitation logiciels et applications.

♦ D'***installer des solutions de sécurité*** (*anti-virus, firewall, antispams, ...*) et de les ***maintenir à jour***.

♦ De ***ne pas ouvrir les pièces jointes ou liens*** contenus dans des courriels dont l'identité de l'expéditeur est incertaine ou inconnue. (***Attention*** : *les attaquants peuvent imiter les adresses de vos correspondants habituels*). Porter également une attention particulière aux mises à jour, lesquelles peuvent être piégées.

♦ De ***restreindre l'autorisation des macros*** dans les suites bureautiques et de ***désactiver le moteur Javascript*** des lecteurs PDF.

♦ D'***attribuer des comptes*** « ***utilisateur*** » adaptés aux besoins de chaque salarié et non pas des droits « ***administrateur*** ».

♦ De ***sensibiliser régulièrement*** l'ensemble des salariés aux problématiques de sécurité informatique.

QUE FAIRE EN CAS D'INFECTION ?

♦ ***Isoler immédiatement l'ordinateur compromis en le déconnectant du réseau*** *(arrêt du Wi-Fi, câble Ethernet débranché ; but : bloquer la propagation du chiffrement et la destruction des dossiers partagés)*.

♦ ***Alerter rapidement*** le responsable informatique ou la société de maintenance. Vérifier l'intégralité du réseau, d'autres machines ayant pu être infectées. ***Désinfecter*** les postes et ***restaurer*** les données.

♦ ***Communiquer immédiatement*** sur l'attaque auprès de l'ensemble des utilisateurs.

♦ ***Déposer plainte*** auprès du service de police ou de gendarmerie territorialement compétent.

Si possible, vous munir des renseignements suivants :

Mode de transmission de l'infection (*mail avec pièce jointe, lien internet,...*) ; Nom du ransomware et extension des fichiers chiffrés ; Adresse de paiement de la rançon en bitcoins et adresses URL apparaissant ; Adresse ".onion" du site de téléchargement du déchiffreur

♦ ***Prévenir votre assurance*** pour éventuellement mettre en route la procédure d'indemnisation (contrat "***perte d'exploitation***" et/ou "***risques cyber***").

Lettre électronique **N° 19** éditée par la région de gendarmerie de Rhône-Alpes – 36 bd de l'Ouest – 69580 Sathonay-Camp : 04.37.85.21.15
Rédaction : Cellule Intelligence Économique régionale.

ATTENTION

♦ ***Dans ce cas précis, le paiement de la rançon est à proscrire*****,** l'adresse mail associée ayant été désactivée par un fournisseur d'accès.

A noter : Payer la rançon encourage la poursuite et le développement de cette activité délictuelle et ne garantit en rien le déchiffrement des données. Il peut en outre compromettre l'intégrité d'une machine, voire du réseau de l'entreprise, si le téléchargement de la clef s'accompagne de l'installation d'un RAT (*logiciel de prise de contrôle à distance d'un ordinateur*).

♦ Des escrocs se font parfois passer pour des entreprises spécialisées dans la sécurité informatique. Ceux-ci proposent, moyennant finances, de déchiffrer les données « ***sans payer la rançon*** ». En réalité, ils la payent discrètement, en prenant une marge, et acquièrent ainsi la confiance de la victime leur permettant de procéder ultérieurement à d'autres méfaits.

POUR ALLER PLUS LOIN

Bulletin d'alerte du CERT N° CERTFR – 2017 – ALE – 012

http://www.cert.ssi.gouv.fr/site/CERTFR-2017-ALE-012/index.html

SECNUMACDEMIE : Formation gratuite en ligne sur la sécurité informatique de l'ANSSI

https://www.secnumacademie.gouv.fr/

Sites d'information sur les attaques par ransomwares

http://stopransomware.fr

https://www.nomoreransom.org/

Infographie « *cybersécurité, toutes les entreprises sont concernées* »

http://www.bpifrance.fr/A-la-une/Actualites/Cybersecurite-toutes-les-entreprises-sont-concernees-30829

Et retrouvez tous nos messages d'attention sur le site d'Espace Numérique Entreprises

http://www.ene.fr/informer/ressources-documentaires1/fiches-alertes-gendarmerie.html