aDvens

SECURITY FOR THE DIGITAL AGE

BULLETIN D'INFORMATIONS CYBER

Suivi de la crise sanitaire COVID-19
Edition N°02 – 30.03.2020

INTRODUCTION

En cette période perturbée par la crise liée au virus COVID-19, la sécurité est un challenge majeur pour ne pas ajouter une crise Cyber à la crise sanitaire en cours.

La menace évolue à la hausse compte-tenu de cette actualité, et des mesures adoptées par chacun pour poursuivre son activité.

Advens vous propose ce bulletin d'information pour faire le point sur les points d'attention à avoir en tête.

EN SYNTHÈSE

SOC & SECURITY-AS-SERVICE FACTORY

Retour à une activité d'alerte conforme aux standards habituels

Point d'attention : baisse du trafic Web derrière le proxy de nos clients (configuration « remote » ou contournement par les utilisateurs ?)

SOURCES EXTERNES

La résistance contre les cyber-attaquants s'organise : COVID-19 CTI League !

Toujours et encore de fausses applications de suivi du virus

RECOMMANDATIONS

Rappeler les bonnes pratiques aux utilisateurs

Renforcer la surveillance et se doter d'une capacité de réaction

Vérifier que les protections sont actives à distances et qu'elles ne peuvent pas être désactivées !

ÉVOLUTIONS DE LA MENACE : VISION DE LA SECURITY-AS-A-SERVICE FACTORY

ACTIVITÉS DE LA SECURITY-AS-A-SERVICE FACTORY

Semaine 13 : retour à la normale mais tendance à surveiller concernant le surf Web

Activité globale du SOC

- Retour à la normale après une semaine 12 marquée par un pic d'activité malveillante

Vigilance à conserver sur les failles humaines

- Menace liée au phishing toujours présente
- Risque accru par les utilisateurs qui installent par curiosité des applications de suivi de la pandémie

Point d'attention : surf Web

- Analyse des logs proxy de nos clients : forte baisse de l'activité de surf sur le Web

FOCUS : ÉVOLUTION DU TRAFIC LIÉ AU SURF WEB

L'analyse des logs proxy de nos clients montre une forte baisse de l'activité de surf sur le Web.

Deux cas de figurent sont envisageables selon les organisations

- Option 1 : évolution de la configuration Proxy en cas d'accès distant et passage sur une instance Cloud du proxy

  Quid de la maitrise des logs dans ce cas de figure ?

- Option 2 : désactivation du Proxy par les utilisateurs en capacité de le faire (admin local ou autre)

  Risque accru sur la sécurité des postes et in fine de toute l'organisation

ÉVOLUTIONS DE LA MENACE : VISION DES SOURCES EXTERNES

LA RÉSISTANCE S'ORGANISE…

La communauté Cyber se prépare pour défendre et réagir face aux risques d'attaque et en particulier face aux risques sur les structures de santé.

COVID-19 CTI League

- Un collectif de cyber super-héros s'est monté, à l'initiative de quelques experts du monde de la CTI (ClearSky, Microsoft, Okta…) pour tenter de neutraliser les attaquants qui exploiteraient la pandémie… en espérant qu'ils ne soient pas victimes de leur succès suite au battage médiatique sur cette nouveauté !

Initiatives en France

- CESIN
  https://www.cesin.fr/actu-coronavirus-et-cybersecurite.html
  + Contenu pour les membres du club (nous contacter pour adhérer)
- Cybermalveillance
  https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail

… MAIS LA MENACE EST TOUJOURS TRÈS FORTE !

Toujours et encore des malwares ou des menaces liées au COVID

Des structures de soin déjà attaquées

- **L'AP-HP victime d'un déni de service** aux impacts vite limités
  https://www.lesechos.fr/tech-medias/hightech/laphp-victimes-dune-cyberattaque-1188022

Des anciennes menaces remise au gout du jour…

- **Malwares et applications vérolées** : le virus fait peur, les utilisateurs testent différentes applications ou des sites d'information et/ou de suivi de la propagation
  https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

- **Distribution de clés USB vérolées** : on profite de la présence des utilisateurs à la maison !
  https://www.bleepingcomputer.com/news/security/fbi-hackers-sending-malicious-usb-drives-and-teddy-bears-via-usps/

… MAIS LA MENACE EST TOUJOURS TRÈS FORTE !

Toujours et encore des malwares ou des menaces liées au COVID

Et des nouvelles problématiques à adresser ?

Quid des attaques qui viseraient à modifier les données utilisées par les soignants et les administrations ?

- ➔ Les données sont cruciales pour analyser l'évolution de la pandémie et prendre des décisions structurantes pour protéger les populations.
- ➔ L'IA sera utilisée de plus en plus pour assister la médecine et la recherche.
- ➔ Les données doivent donc être protégées plus que jamais !

https://www.belfercenter.org/publication/weaponizing-digital-health-intelligence (Source @Bortzmeyer)

Une bonne nouvelle malgré tout ? Certains attaquants ont déclaré qu'ils ne toucheraient pas aux hôpitaux – d'autres ont rappelé qu'ils n'y touchent jamais !

https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/

RECOMMANDATIONS

NOS PRÉCONISATIONS

Back to basic ? Ca marche aussi à la maison !

Pour les utilisateurs à distance

- Ne pas désactiver les protections et les mesures de sécurité (proxy par exemple)
- Ne pas se faire piéger par les campagnes de phishing et ne pas donner d'informations sensibles après un clic sur un mail douteux
- Ne pas mélanger les usages « pro » et « perso » et rester vigilants sur les usages domestiques

Pour les équipes sécurité

- S'assurer que les utilisateurs ne peuvent pas désactiver les protections de sécurité
- Renforcer la vigilance et les moyens en matière de détection
  - Revue renforcée des logs et des outils de supervision
  - Passage des derniers patchs en retard (cf. alerte récente sur la faille SMB)
  - Activer les logs sur les composants qui n'en produiraient pas encore
- Envisager le scénario d'une attaque réussie et revalider les processus de réaction
- Intégrer les infrastructures d'accès distant dans le périmètre du SOC le cas échéant
- Accélérer les projets de déploiement d'EDR

advens.fr

SECURITY FOR THE DIGITAL AGE

Paris +33 1 84 16 30 25
Lille +33 3 20 68 41 81
Lyon +33 4 28 29 08 29
Bordeaux +33 5 35 54 82 84