Expéditeur	Objet	Destinataire(s)
RSSI	Cybersécurité Covid-19	Personnels UGA
Date		
19/03/2020		

Table des matières

1. Contexte et menaces

Une crise sanitaire importante affecte l'Europe contraignant les Etats à prendre des mesures exceptionnelles. Dans ce cadre, il est demandé de favoriser le télétravail lorsque cela est possible. Ce mode inhabituel pour certains, peut être source de déstabilisation et de désorganisation rendant cette période propice à des actes malveillants y compris sur nos systèmes informatiques.

Dans ce contexte, le risque d'une cyberattaque est très élevé, l'actualité l'illustre :

- Une cyberattaque a affecté ce weekend la métropole de Marseille et les villes qui la composent. Le système d'information a été fortement impacté. [1]
- Des attaquants profitent de l'actualité pour générer des escroqueries ou des actes malveillants. Par exemple une application pour téléphone portable pour suivre la propagation du Covid-19 est en fait un moyen de déployer un rançongiciel (ransomware) sur l'ordinateur ou le smartphone utilisé [2]
- Des escrocs ont mis en ligne plusieurs sites promettant une attestation de déplacement sans limite sur le territoire Français durant le confinement général lié au Coronavirus. [3]. Ces sites outre le fait qu'ils peuvent vous faire payer, vont récupérer vos données personnelles comme par exemple votre signature
- Au niveau de l'UGA des usagers ont été confrontés à des tentatives d'escroqueries au support informatique. Un message s'affichant sur l'ordinateur pour indiquer qu'un problème de sécurité a été détecté et qu'il convient de contacter un numéro de téléphone. Il ne faut surtout pas appeler le numéro !

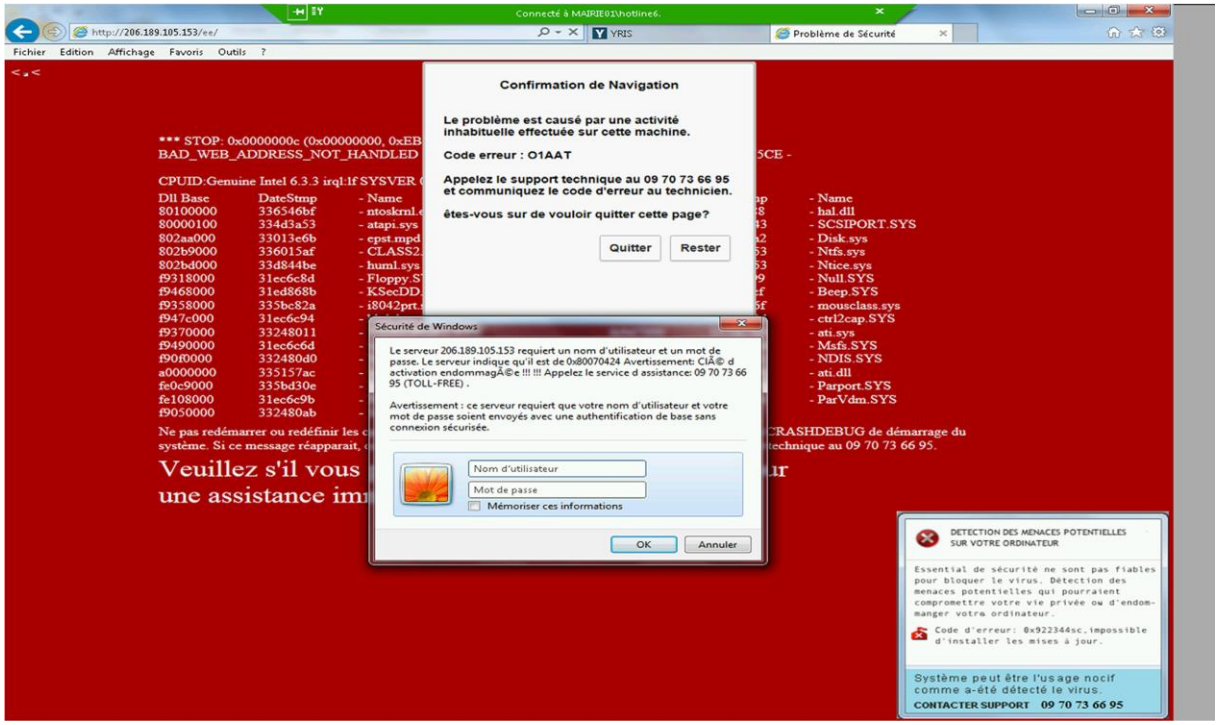

Figure 1 : Capture d'écran d'une escroquerie au support

- De plus, de nombreuses tentatives d'hameçonnage (phishing) au webmail ou à la boite aux lettres saturée sont constatés

2. Points de vigilance

Lorsque vous êtes en situation de nomadisme numérique, vous n'êtes plus protégés par les dispositifs de sécurité mis en œuvre par la DGDSI de l'UGA. **Vous devez donc être encore plus vigilant qu'à l'accoutumée**.

Vous pouvez notamment être confrontés aux situations suivantes :

- des messages invitant à se connecter sur des espaces partagés en ligne qui sont frauduleux, glissés au milieu du foisonnement d'espaces partagés légitimes ;
- des courriels malveillants semblant venir du Ministère de la Santé et autres autorités ;
- des courriels malveillants usurpant l'identité de l'établissement ;
- des fausses demandes RH liées à l'organisation du travail à domicile ;
- des applications et sites malveillants supposés donner des renseignements sur la crise et les bons réflexes ;
- des faux appels téléphoniques de help desk ;
- une propagation de rumeurs, idées reçues et fausses informations.

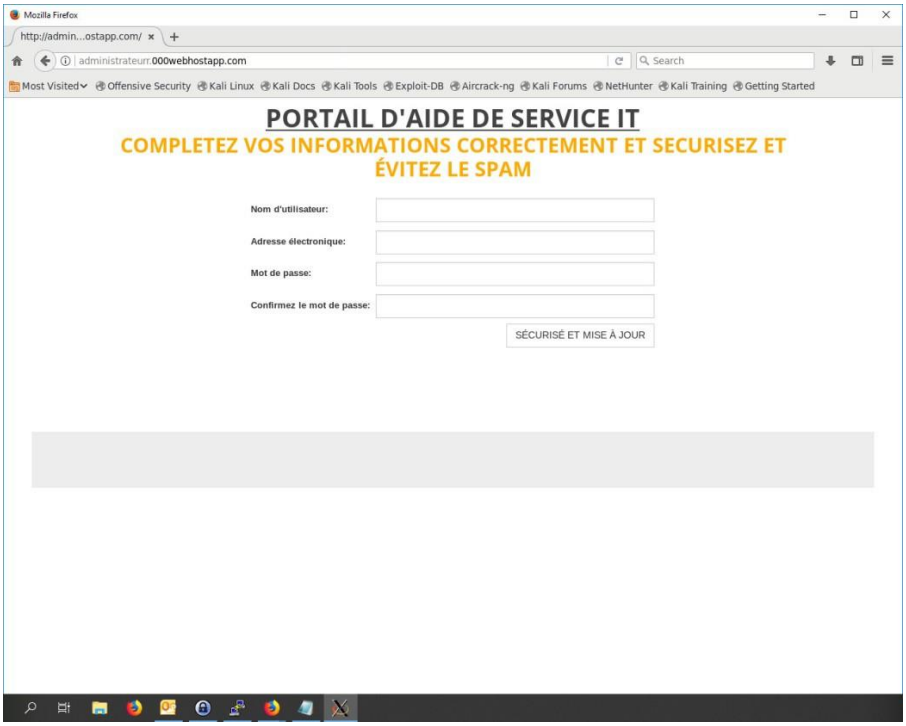

Figure 2: Capture d'écran d'un portail d'hameçonnage (phising)

Vous devez adopter une posture de vigilance renforcée.

- **A la réception d'un courriel, vous devez :**
  1. Regarder l'expéditeur et son adresse,
     les messages officiels de l'UGA ne peuvent provenir que du domaine @univ-grenoble-alpes.fr
  2. Regarder la date et l'heure d'expédition qui doit correspondre avec une période d'activité normale
  3. Regarder l'objet du message : par exemple « message du service informatique »
  4. Regarder le contenu du message d'une part si le message comporte un lien ou une pièce jointe et d'autre part si une pression psychologique est présente (vous devez effectuer cette action avant telle date…).
  5. Etre attentifs à tout élément vous paraissant suspect
  6. Si un message semble provenir d'un (d'une) collègue mais avec une adresse privée (gmail, free, orange…), recontactez-le (la) sur son adresse institutionnelle pour vérification et demandez-lui un renvoi avec son adresse professionnelle

- **Lors de la navigation sur Internet, vous devez :**
  1. Limiter votre navigation aux sites institutionnels ou de confiance
  2. Ne pas utiliser les espaces de stockage en ligne gratuits type Dropbox ou Wetransfer car cela va augmenter le risque d'être leurré par des courriels de type hameçonnage.
  3. Être vigilants lorsque vous recevez des invitations à vous connecter à des espaces de partage ou de visioconférence

- **Lors de sollicitations téléphoniques notamment pour du support informatique, vous devez :**
  1. Vérifier que vous êtes bien en présence du service help de l'UGA - par exemple, ils connaissent le numéro de votre ticket de demande d'aide

- **De manière générale à votre domicile vous devez :**
  1. Protéger le matériel de l'UGA contre le vol en ne le laissant pas accessibles à des tiers
  2. Ne pas connecter de périphériques USB personnels (tolérance pour un ensemble écran, clavier souris uniquement)

  Si vous utilisez un ordinateur personnel assurez-vous de :
  1. Disposer d'une version de système d'exploitation maintenu et à jour (ex : des connexions depuis des postes exécutants Windows 7, 8 ou Vista sont interdits)
  2. Disposer d'un antivirus à jour et opérationnel.

3. Contacts Cybersécurité

Notre capacité à faire face à la situation et réagir de façon efficace face à une cyber-attaque implique une participation active de chacun(e) d'entre nous.

En cas de doute ou de problèmes simples, du type « Est-ce un hameçonnage (phishing) ? », contactez l'assistance par courriel à l'adresse **help@univ-grenoble-alpes.fr**

S'il s'agit d'un problème plus grave pouvant mettre en cause le système d'information de l'UGA, déconnectez l'ordinateur de l'utilisation du réseau (câble et/ou wifi), et à partir d'un autre appareil (PC secondaire, smartphone…) contactez **dgdsi-securite@univ-grenoble-alpes.fr** par messagerie, et en dernier ressort, ou urgence absolue, appelez le RSSI de l'UGA au 04 57 42 13 19.

Vous trouverez également des informations sur :

- le site cybermalveillance.fr avec une page spécifique concernant l'actualité Covid-19 et menaces associées.
  https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/coronavirus- covid-19-vigilance-cybersecurite
- Le site officiel d'information sur le Covid-19 https://www.gouvernement.fr/info-coronavirus
- Le site officiel de l'Agence Nationale de Sécurité des Systèmes d'Information et notamment le guide d'hygiène numérique qu'il convient plus que jamais de respecter
  https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

4. Références bibliographique

[1] J. Saint-Marc, «Marseille : « Les dégâts sont assez lourds » après une attaque informatique contre la mairie et la métropole,» 17 Mars 2020. [En ligne]. Available: https://www.20minutes.fr/societe/2741875-20200317-marseille-degats-assez-lourds- apres-attaque-informatique-contre-mairie-metropole. [Accès le 18 Mars 2020].

[2] BGR.In, «Coronavirus Tracker app on Android is a malicious ransomware; security researchers explain how to unlock affected devices,» 18 Mars 2020. [En ligne]. Available: https://www.bgr.in/news/coronavirus-

tracker-app-on-android-is-a-malicious-ransomware- security-researchers-explain-how-to-unlock-affected-devices-881163/. [Accès le 18 Mars 2020].
[3] D. Bancal, «Non, l'attestation de déplacement dérogatoire ne coûte pas 5, 10 ou 100€,» 17 Mars 2020. [En ligne]. Available: https://www.zataz.com/non-lattestation-de-deplacement-derogatoire-ne-coute-pas-5-10-ou-100e/. [Accès le 18 Mars 2020]