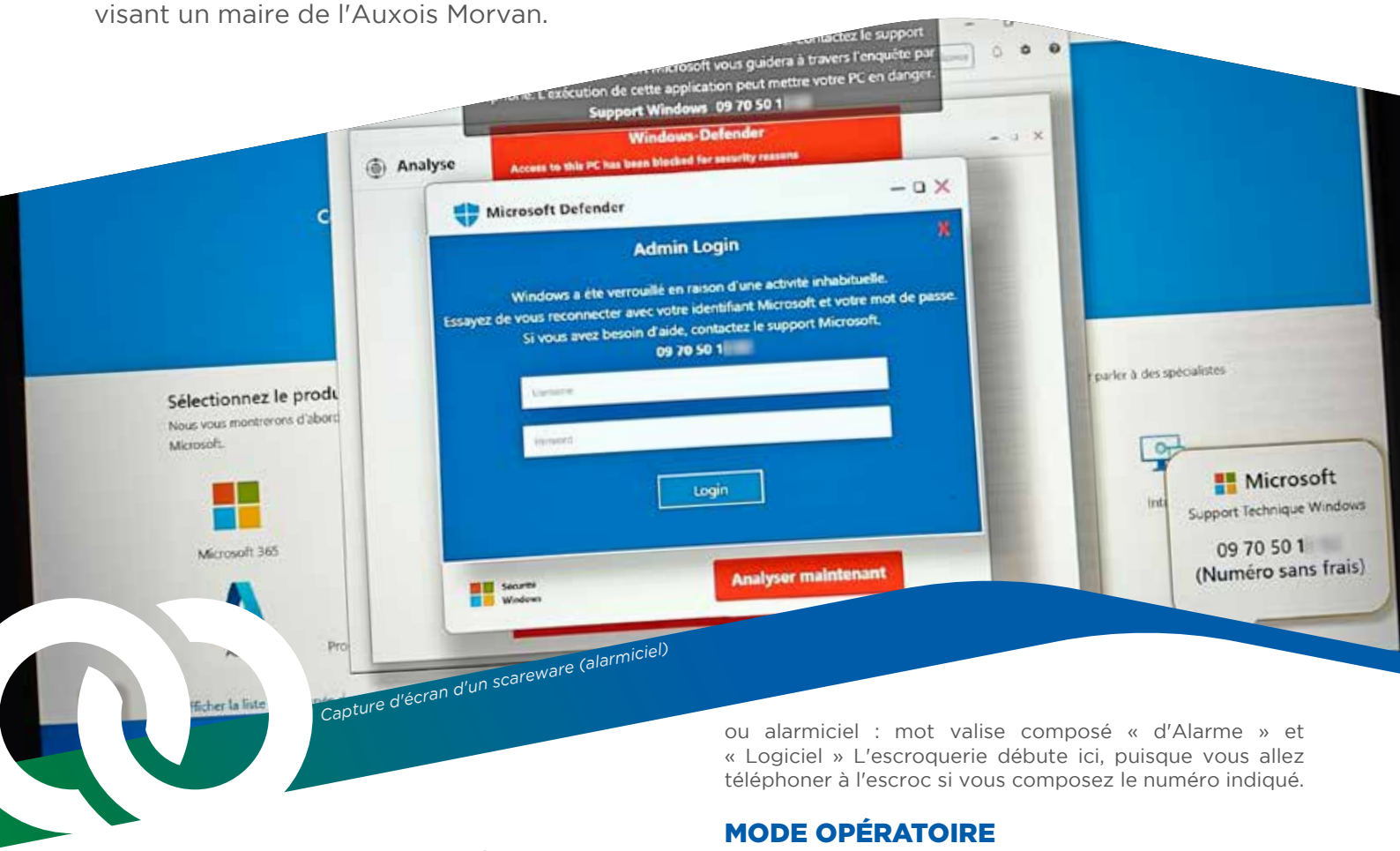
Retour d'expérience
FAUX SUPPORT TECHNIQUE

La Mission numérique du PETR du Pays Auxois Morvan, conjointement avec Cybergogne, vous propose ce retour d'expérience partagé suite à une escroquerie au faux support technique visant un maire de l'Auxois Morvan.



Capture d'écran d'un scareware (alarmiciel)

L'escroquerie au faux support technique est une arnaque visant à convaincre la victime d'effectuer des actions solutionnant un problème de sécurité informatique. Dans les faits, cette escroquerie s'appuie sur le manque de connaissances informatiques de la cible et sur la capacité de l'escroc à convaincre son interlocuteur.
Pour contrer de futures tentatives, passons en revue les signaux d'alerte, découvrons les réflexes à adopter et identifions les contacts à solliciter.

L'ESCROQUERIE EN ELLE-MÊME

En surfant sur le web, vous accédez à une page bloquant la navigation : cette page a l'apparence du système d'exploitation Windows ou de celui d'Apple. Au centre de cette page apparaît une fenêtre surgissante qui vous invite à appeler le support technique, au prétexte que votre ordinateur est infecté. C'est un « scareware » ou alarmiciel : mot valise composé « d'Alarme » et « Logiciel » L'escroquerie débute ici, puisque vous allez téléphoner à l'escroc si vous composez le numéro indiqué.

MODE OPÉRATOIRE

Au bout du fil, l'escroc va vous convaincre :

- **d'installer un logiciel de prise de contrôle à distance** (pour vous dépanner prétend-il) ;
- de lui **transmettre différents codes** : mot de passe de l'ordinateur, de la messagerie etc.
- d'**installer une « solution » payante** pour désinfecter votre ordinateur ;
- de **verser des fonds** pour vérifier que son intervention a correctement solutionné le « problème » ;

Même s'il se montre rassurant, l'escroc sera pressant, voire intimidant, il mettra l'accent sur l'urgence à débloquer la situation ; il insistera également sur le risque de perte de données ou de fonds si vous ne suivez pas ses directives.

Au fil des échanges, il utilisera un vocabulaire technique poussé visant à vous convaincre de son niveau d'expertise.

RÉFLEXES À ADOPTER

Lorsque vous arrivez sur la page d'un faux support technique et si celle-ci vous bloque, vous pouvez :

- Essayer de forcer la fermeture de la page, avec le raccourci clavier ALT+F4 sur PC ou CMD+Q sur Mac ;
- Basculer sur une autre fenêtre avec le raccourci clavier ALT+Tabulation (CMD+Tabulation sur Mac) ;

- Forcer la fermeture du navigateur avec le raccourci CTRL+MAJ+ECHAP (Gestionnaire des tâches) ou (CMD+ALT+Esc sur Mac).

Si l'escroc se réclame d'une société connue, trouvez un prétexte pour **raccrocher et appeler directement la société** via un numéro différent de la prise de contact que vous avez initiée.

De plus, les outils de prise de contrôle à distance sont souvent disponibles en téléchargement sur le site web des prestataires. L'escroc peut vous inciter à télécharger des outils de prise de contrôle à distance connus mais détournés de leur finalité : ScreenConnect, AnyDesk, TeamViewer...

En cas de doute, évitez d'installer le logiciel de prise de contrôle à distance transmis par votre interlocuteur et passez par le site web officiel de la société.

Ne transmettez pas de codes, mots de passe, etc. Les services d'assistance ont :
- soit un accès métier à vos données (ils n'ont pas besoin du code d'accès) ;
- soit n'ont pas le moyen de lire vos données pour raisons réglementaires (RGPD). Une réinitialisation des accès est alors nécessaire. Si vous êtes face à un escroc, il vous demandera le mot de passe nouvellement créé, sous prétexte de sécurisation.

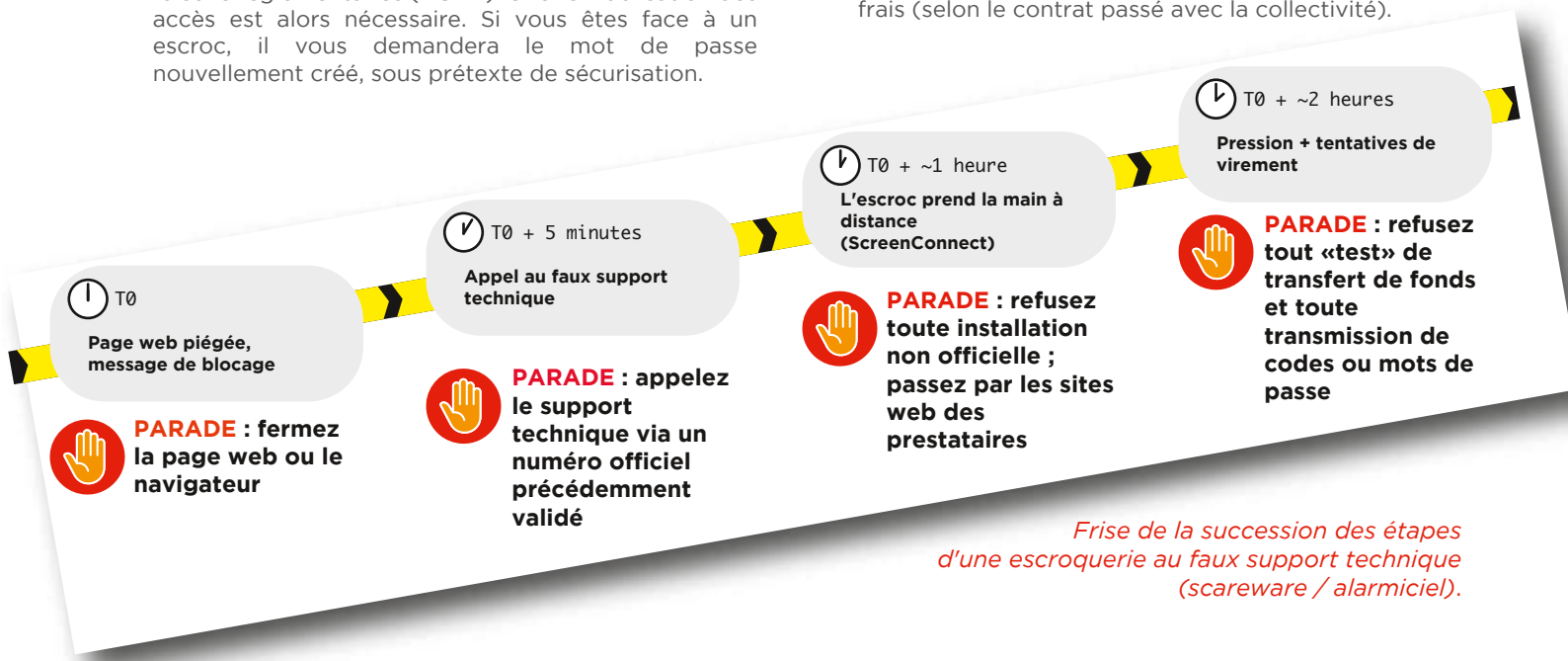
LE DÉPÔT DE PLAINTE

Si l'escroc arrive à ses fins, vous devrez porter plainte. Les collectivités peuvent porter directement plainte à la Gendarmerie ou au commissariat : il faudra alors fournir des justificatifs (captures d'écran, impressions, photos).

Des informations plus poussées peuvent être nécessaires : en-têtes techniques des courriels, journaux de connexion, relevés divers.

À cette étape, l'accompagnement d'un professionnel sera indispensable : le Centre de Réponse à Incident Cyber de Bourgogne-Franche-Comté, le CSIRT-BFC propose une liste d'entreprises spécialisées disponible à l'adresse : https://www.csirt-bfc.fr/cyber-en-bfc/

Dès la découverte de la supercherie, il est primordial voire obligatoire d'informer différents interlocuteurs :
1. Le Service de Gestion Comptable (SGC) pour qu'il tente de bloquer les fonds ;
2. Le Centre de Réponse à Incident Cyber (CSIRT) pour qu'il épaule la collectivité, voire la mette en relation avec un prestataire spécialisé ;
3. L'assurance qui pourra prendre en charge d'éventuels frais (selon le contrat passé avec la collectivité).



Frise de la succession des étapes d'une escroquerie au faux support technique (scareware / alarmiciel).

À chaque étape, une solution bloquant l'attaque est proposée : c'est avant tout la méconnaissance des outils numériques et la peur de mal faire qui permet à l'escroc d'avoir un ascendant sur la victime. La participation à des séances de formation permet d'informer et de former aux risques les agents territoriaux et les élus.

Ce retour d'expérience a été rédigé d'après l'analyse post-mortem fournie par Cybergogne.

CYBERGOGNE
La sécurité en toute transparence

CYBERGOGNE
Solutions de cybersécurité adaptées aux petites collectivités et aux TPE/PME en Bourgogne
• Diagnostic / plan d'actions / durcissement • Sensibilisation (agents & élus)
• Appui en cas d'incident (en lien avec l'écosystème régional)

CONTACT (pour ce retour d'expérience)
Michel Ract-Mugnerot – Architecte Cloud & Sécurité
Tél. : **+33 6 15 28 14 35 -** Web : **https://www.cybergogne.fr**
Adresse : 3, place de l'Église - 21210 Saint-Martin-de-la-Mer (France)

CSIRT BOURGOGNE-FRANCHE-COMTÉ

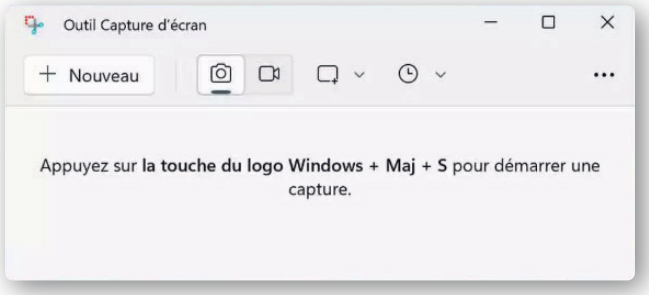
En cas d'attaque, contactez le Centre de Réponse à Incident Cyber : CSIRT BFC au 0 970 609 909

Retour d'expérience
FICHE RÉFLEXES

La Mission numérique du PETR du Pays Auxois Morvan, conjointement avec Cybergogne, vous propose cette fiche réflexes. Vous retrouverez différentes aides et solutions pour savoir comment réagir face à une cybermenace.

Quelles preuves conserver ?

1) **Captures d'écrans, photographies de l'écran** : ciblez l'écran dans son intégralité, pas seulement une partie ou la fenêtre en cours ;
2) **Enregistrements audio** : certains téléphones portables permettant d'enregistrer les conversations ;
3) **Historique des connexions internet** : les navigateurs conservent la succession des pages visitées ;
4) **Historique des appels téléphoniques** : numéros, temps de conversation, dates ;
5) **D'autres éléments peuvent servir de preuves** : il faudra alors solliciter un professionnel pour les identifier et les exploiter.



Le RGPD en 6 lignes

1) Ne collectez que les **informations strictement nécessaires** (cela réduit les impacts des fuites de données) ;
2) **Soyez transparent** : les personnes concernées doivent être informées ;
3) Les personnes doivent **pouvoir exercer facilement leur droit** de consultation ou d'accès, de rectification ou de suppression des données qui les concernent ;
4) Définissez des **durées de conservation réalistes**, puis détruisez, anonymisez ou archivez les données collectées, selon les obligations légales ;
5) Anticipez les risques et **sécurisez les données** ;
6) Suivez attentivement votre mise en conformité en **réexaminant régulièrement** les éléments ci-dessus.

Qui contacter en cas de compromission ?

Selon la nature de la compromission, vous devrez contacter différents organismes. Les propositions ci-dessous correspondent aux contacts à solliciter dans la majorité des cas. Avant tout incident, élaborez, à tête reposée, votre liste de **contacts vérifiés** : sous la pression d'une cybermenace, vous pourrez vous appuyer sur ce document.

1) Notez le jour et l'heure où vous avez constaté la compromission ;
2) Contactez votre prestataire ou référent informatique si vous en avez un ;
3) Alertez le Centre de Réponse à Incident Cyber au 0 970 609 909 suivi du choix 1 ;
4) Alertez également la Gendarmerie ;
5) Alertez la Trésorerie ou votre Banque, s'il y a une suspicion de transferts de fonds ;
6) Déposez plainte ;
7) Dans les 72 heures (voir point 1), vous devrez :
   A. déclarer le sinistre à votre assureur ;
   B. notifier la CNIL si des données à caractère personnel ont pu être consultées, modifiées ou détruites.
8) Informez les contacts qui peuvent être impactés par la compromission : il peut s'agir d'administrés, de fournisseurs, de partenaires ou de toute personne dont la sécurité est compromise par l'incident.

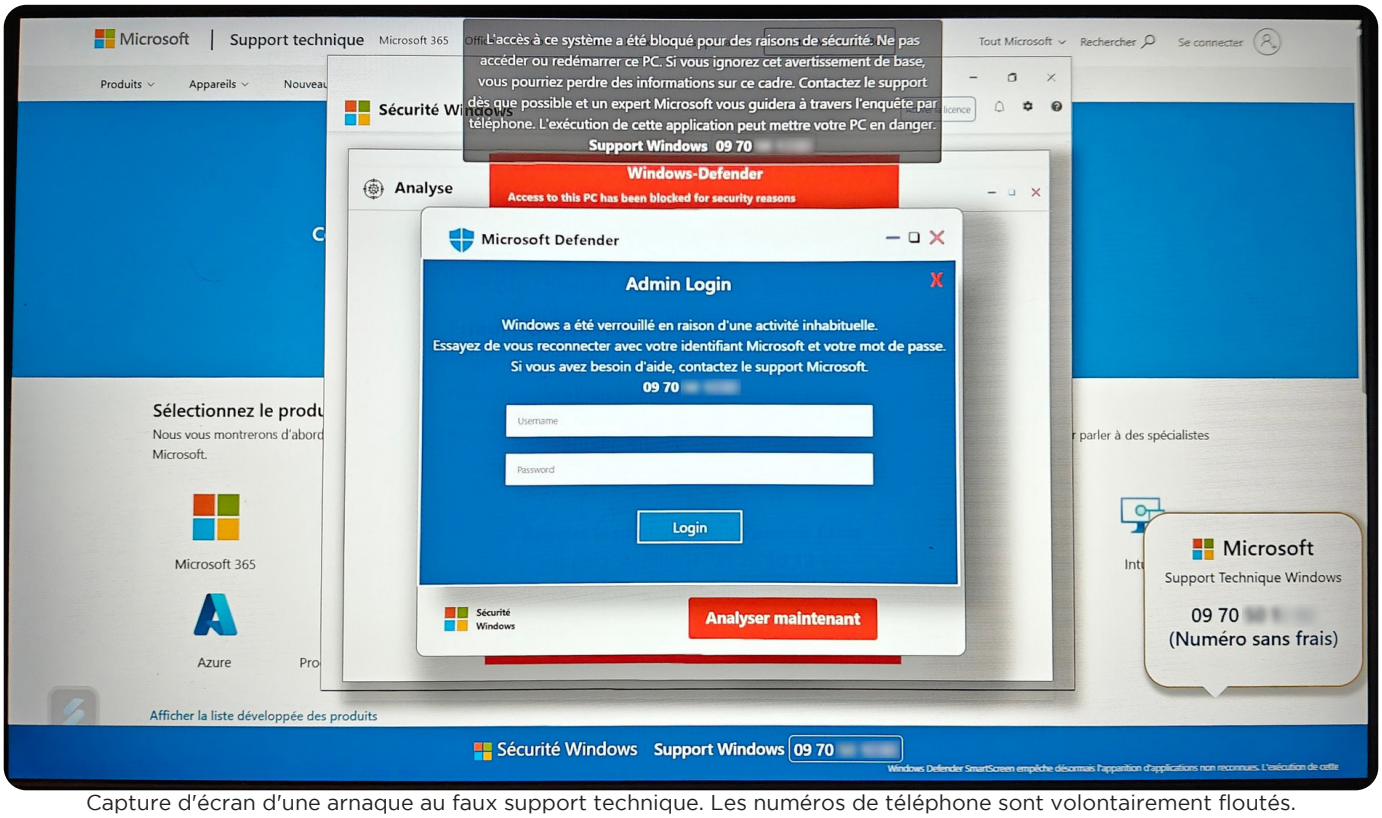
URGENCE :
isolez la machine incrimée du réseau

Dès la compromission constatée, débranchez l'équipement concerné du réseau. Débranchez la prise réseau (RJ-45) et vérifiez que l'appareil n'a pas basculé en Wi-Fi.
Évitez de l'éteindre, branchez-le sur secteur s'il s'agit d'un équipement portable.

Exemple de « scareware » - arnaque au faux support technique

Urgence et menace
Le message occupe tout l'écran prétendant que l'ordinateur est bloqué.
Objectif : provoquer la panique, forcer à agir dans l'urgence

Usurpation de l'identité visuelle de Microsoft Windows
Les icones, textes et couleurs simulent un message de l'ordinateur, invitant à appeler un numéro.
Ce n'est pas le canal officiel : c'est l'arnaque



Capture d'écran d'une arnaque au faux support technique. Les numéros de téléphone sont volontairement floutés.

Vol d'accès et prise de contrôle
Faux écran de connexion administrateur : l'attaquant force la victime à transmettre son identifiant et mot de passe pour obtenir les droits sur la machine (accès à la messagerie, outils métiers etc.)

Réflexe immédiat (élus, agents)
- Conserver une capture d'écran et noter l'heure ;
- Fermer la page (raccourci clavier ALT+F4) ;
- Contacter un référent ou un prestataire informatique ;
- Ne pas appeler le numéro affiché par les escrocs !

CYBERGOGNE
La sécurité en toute transparence

En cas d'attaque, contactez le centre de réponse à incident cyber :
CSIRT BFC au 0 970 609 909

CYBERGOGNE
Solutions de cybersécurité adaptées aux petites collectivités et aux TPE/PME en Bourgogne
• Diagnostic / plan d'actions / durcissement
• Sensibilisation (agents & élus)
• Appui en cas d'incident (en lien avec l'écosystème régional)

CONTACT (pour ce retour d'expérience)
Michel Ract-Mugnerot – Architecte Cloud & Sécurité
Tél. : **+33 6 15 28 14 35**
Web : **https://www.cybergogne.fr**
Adresse : 3, place de l'Église
21210 Saint-Martin-de-la-Mer (France)

CSIRT
BOURGOGNE-FRANCHE-COMTÉ