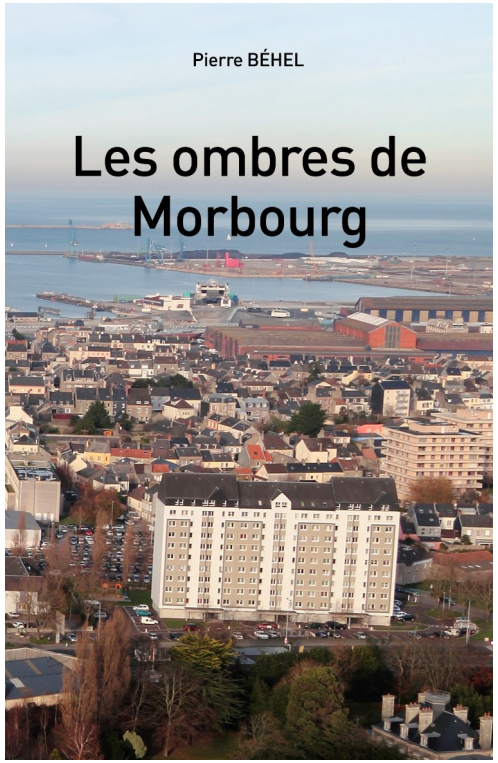
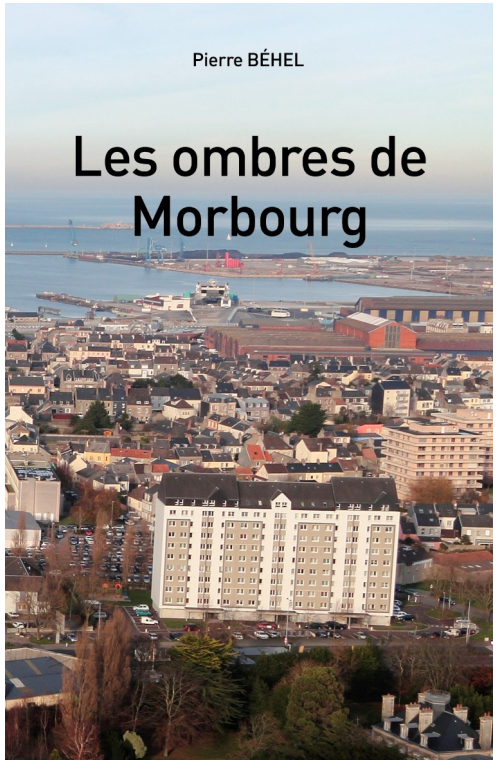
Le cybercrime à Morbourg



Au travers des récits du cycle de Morbourg, réunis dans *Les Ombres de Morbourg*, voyons des techniques et des méthodes des cybercriminels réels et comment s'en protéger.

Morbourg

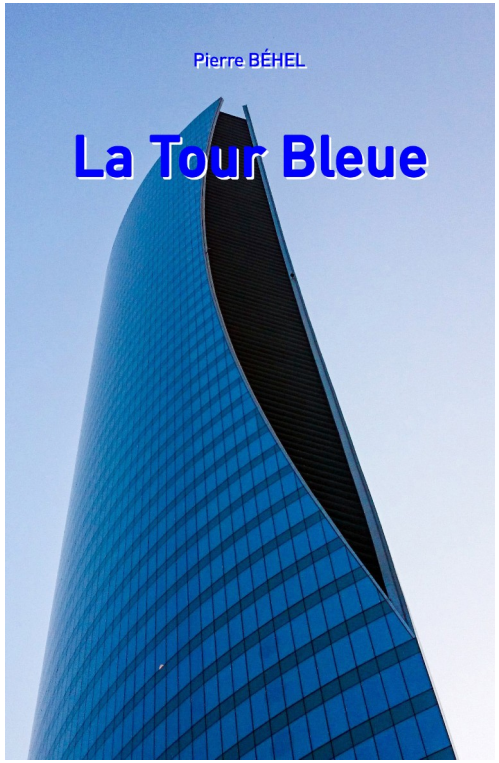


La ville de Morbourg a connu des jours meilleurs. Un paquebot, jadis fierté de la ville, y rouille à quai. Des jeunes filles veulent fuir et parfois disparaissent. Des notables se perdent et parfois meurent. Entre Carole Nède, la policière, et Mélissa Madeleine, l'éternelle adolescente, se noue une étrange histoire qui se décline en quatre actes.

Les Ombres de Morbourg réunit les histoires parues séparément sous les titres de *Notre Fierté*, *L'Ombre des Etoiles*, *L'Ombre du Jeu* et *La Tour Bleue*.

Infecter sa victime

La clé USB infectée



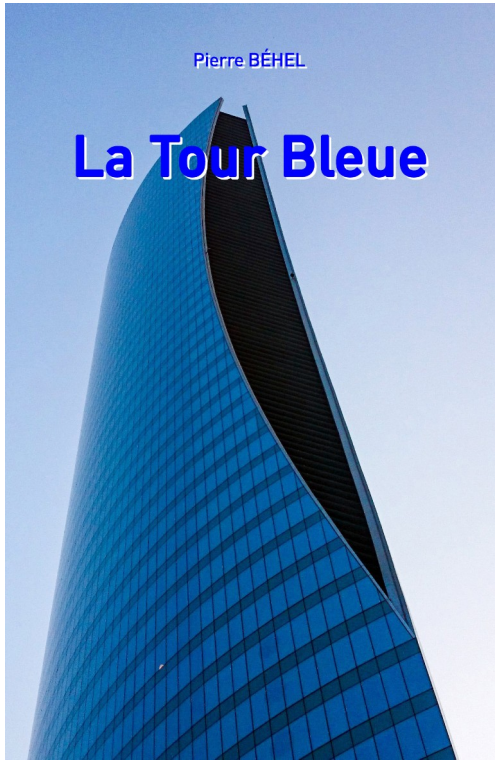
Grand classique, faire parvenir une clé USB possédant un fichier et/ou son secteur d'amorce contaminés par un virus reste efficace dans beaucoup de cas. Jadis, c'était une disquette…

C'est ainsi que le premier pirate infecte sa victime dans *La Tour Bleue*.

Mécanisme : miser sur la curiosité (qu'est-ce qu'il y a sur la clé USB?) voire une certaine confiance pour que la victime utilise le support infecté.

Mesures correctives : éduquer les utilisateurs (répandre des clés USB dans un parking...), installer des stations de « tests de clés », un bon anti-virus qui analyse les supports introduits.

Le hameçonnage (ou phishing)



Autre grand classique, faire parvenir un e-mail comprenant un logiciel malveillant. Pour éviter d'être détecté, le logiciel malveillant peut être dans un conteneur zip joint au mail.

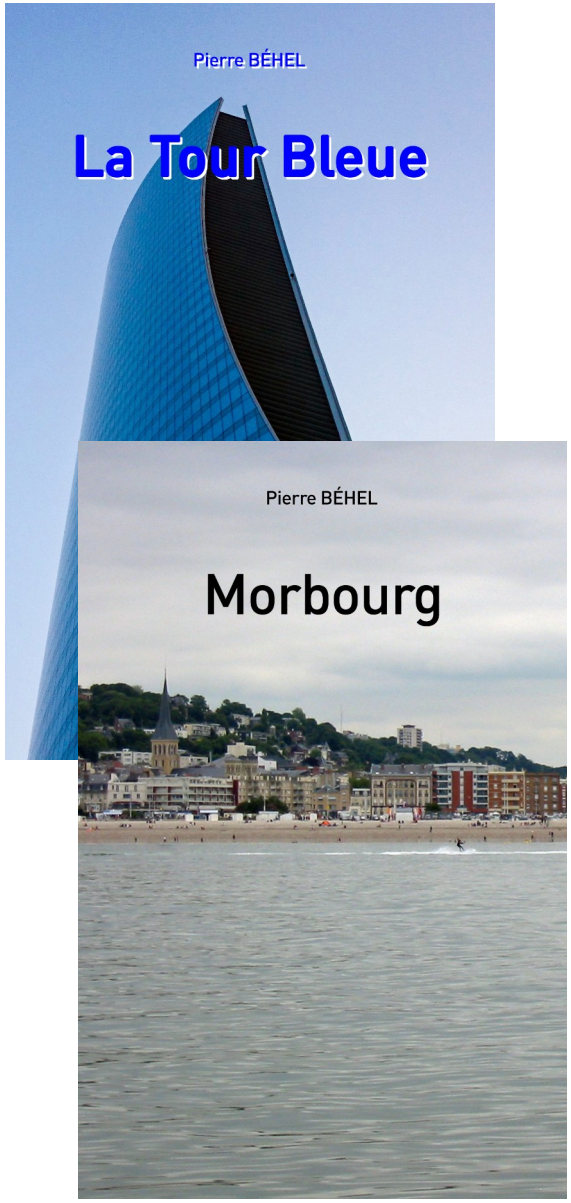
C'est ainsi que le deuxième pirate infecte sa victime dans *La Tour Bleue*.

Mécanisme : miser sur la curiosité (qu'est-ce qu'il y a dans la pièce jointe ou via le lien ?) voire une certaine confiance pour que la victime déclenche l'action nécessaire pour être infectée. Un phishing très personnalisé et bien construit peut être redoutable (principe de l'**ingénierie sociale**).

Mesures correctives : éduquer les utilisateurs, installer des anti-virus/anti-spams sur les serveurs de mails.

Variante : le phishing peut viser à faire saisir un couple identifiant/mot de passe sur un faux-site (de banque par exemple). Les pirates récupèrent alors ce couple et s'en servent (usurpation d'identité).

La faille de sécurité

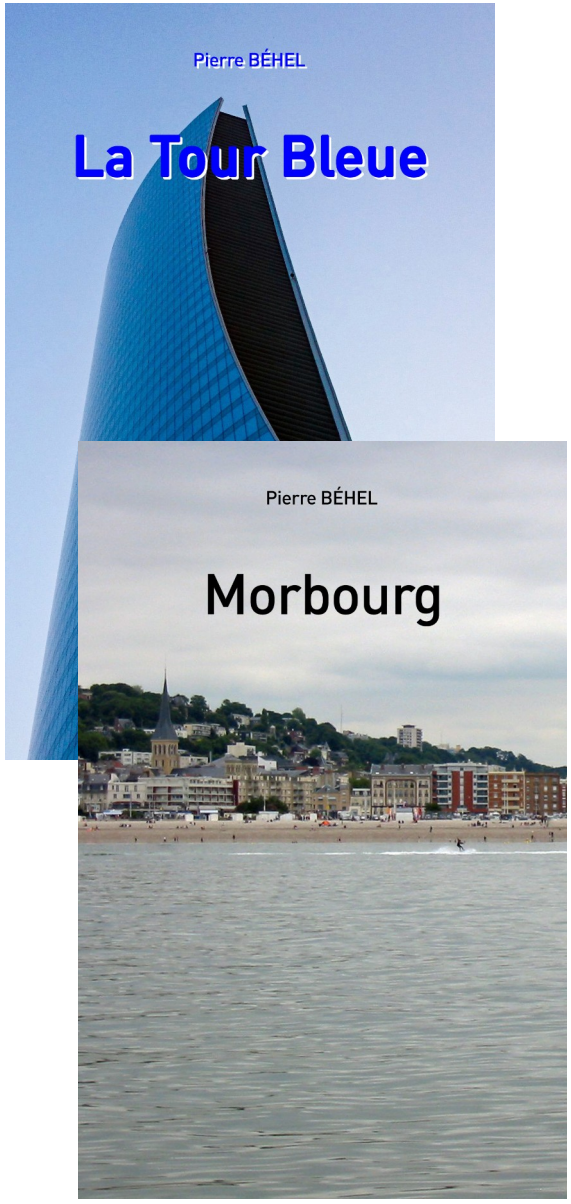


Cette fois, l'utilisateur est moins en cause… Son terminal comporte une faille plus ou moins documentée (éventuellement dite « zéro day ») utilisée par le pirate pour y introduire son logiciel malveillant ou mener diverses actions.

Cette technique est utilisée plusieurs fois dans le cycle de Morbourg, notamment dans *La Tour Bleue*. A chaque fois, ce sont les smartphones des victimes qui sont visés.

Mécanisme : tester les failles possibles jusqu'à en trouver une.

Mesures correctives : veiller à disposer de terminaux et de logiciels bien à jour (mises à jour dites « de sécurité »), surveiller le trafic de données suspect (mode de détection par l'un des pirates dans *La Tour Bleue*), faire faire des tests d'intrusion par des spécialistes white hats (« gentils pirates »).



Le rebond

La cible finale du pirate n'est pas forcément directement accessible. Il va donc utiliser un ou plusieurs intermédiaires moins protégés comme bases afin de mener une attaque « de l'intérieur » ou à partir d'une « zone de confiance ».

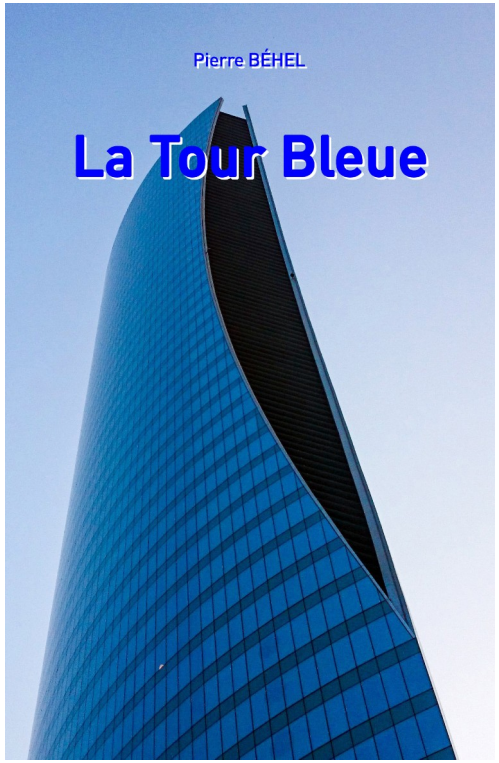
Cette technique est utilisée plusieurs fois dans Morbourg et dans *La Tour Bleue*.
1er exemple : utilisation d'une faille bluetooth pour pénétrer un smartphone qui va envoyer un message piégé à un second smartphone, propriété d'un malade équipé d'un pacemaker qui sera attaqué par bluetooth.
2ème exemple : infection d'un PC pour infecter une imprimante multifonction.
3ème exemple : infection d'un smartphone pour infecter un véhicule connecté.

Mécanisme : trouver un chemin avec des fragilités.

Mesures correctives : veiller à disposer de terminaux et de logiciels bien à jour (mises à jour dites « de sécurité ») et un système sans faille exploitable.

La sécurité globale d'un système est celle de son « maillon le plus faible ».

La fausse alerte

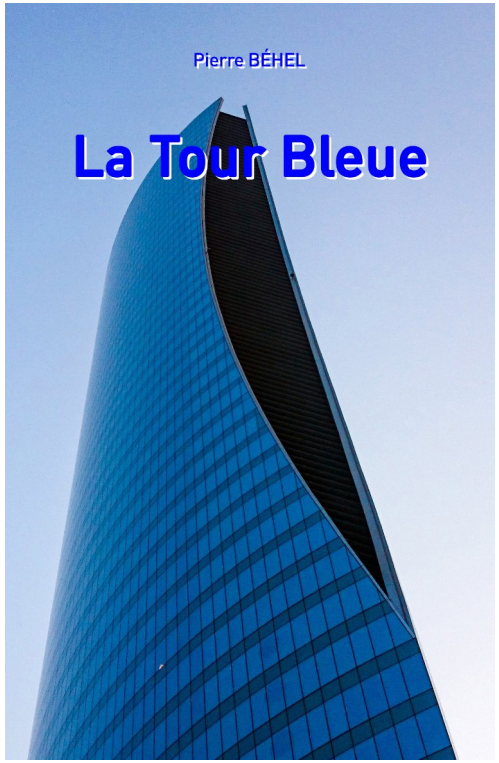


Si un mécanisme de protection constitue un blocage, le mieux est encore de pousser son propriétaire à le désactiver.

Dans *La Tour Bleue*, la méthode est utilisée pour pousser la victime à désactiver une alarme en déclenchant de fausses alertes.

Pour faire quoi ?

Extorquer de l'argent

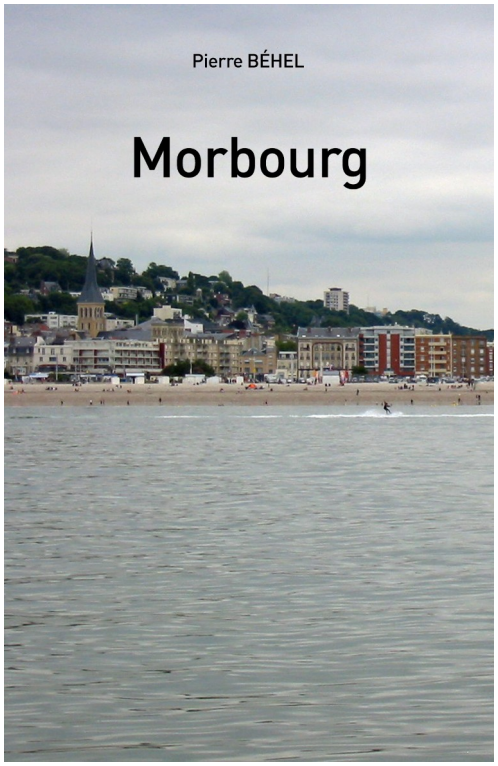


Dans la saga de *Morbourg*, les pirates ne sont pas aussi vulgaires… Mais le premier pirate de *La Tour Bleue* est un habitué du procédé (on en entend juste parler).

L'objectif final du pirate est le plus souvent de retirer un bénéfice financier direct...

Exemples :
1) Vol de données de connexion à un site bancaire => capacité à effectuer des virements vers un compte contrôlé par le pirate.
2) Ransomware : chiffrement de données dans le seul but d'obtenir une rançon en échange de la clé pour déchiffrer les données.

Détruire / rendre inopérant

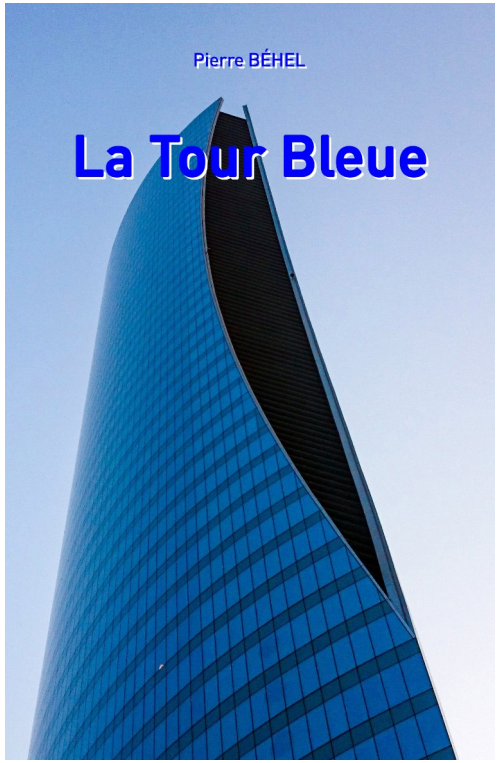


Dans *Morbourg*, l'objectif final du piratage est de commettre un meurtre en détruisant/reprogrammant un pacemaker.
Des attaques de type NotPetya visent à détruire des appareils industriels.
Eventuellement, la menace de destruction peut être un moyen d'obtenir une rançon (principe du ransomware).

Mécanisme : prise de contrôle partielle ou totale des systèmes permettant la destruction.

Mesures correctives : veiller à disposer de systèmes de secours ou de sauvegardes de données isolées ou de capacités à réinitialiser aisément des outils.

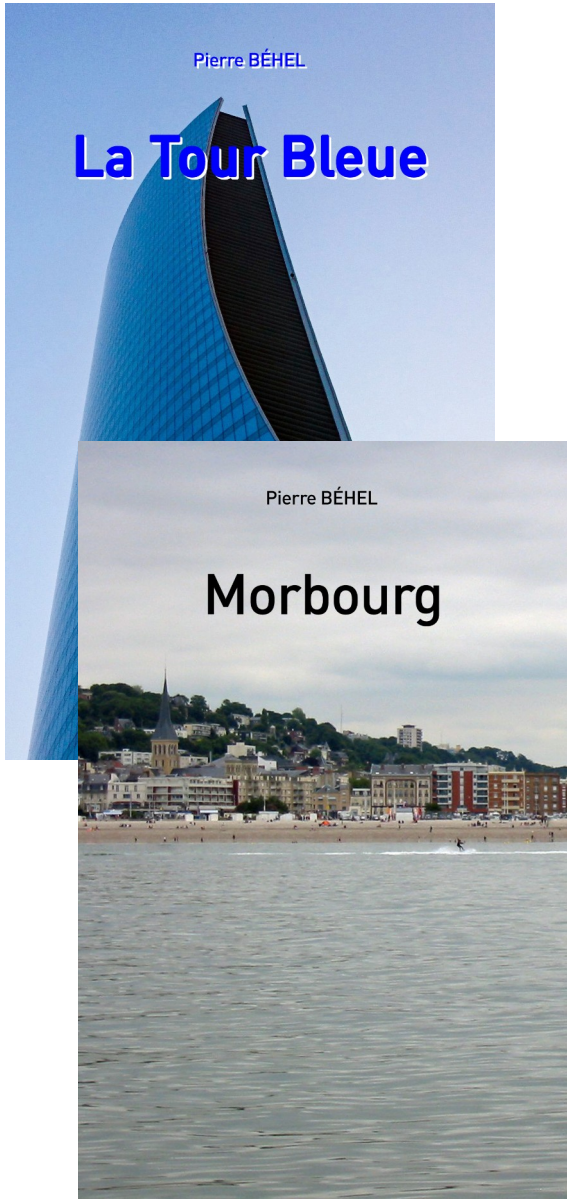
Prendre le contrôle



Lorsque le pirate prend le contrôle d'un véhicule connecté avec des fonctions d'auto-pilote (ces véhicules « qui se garent seuls » existent déjà !), il peut faire faire une manœuvre au dit véhicule.

Dans *La Tour Bleue*, la méthode est utilisée pour commettre un meurtre en envoyant un véhicule par delà des barrières et le faire chuter du haut d'une falaise.

Voler des données



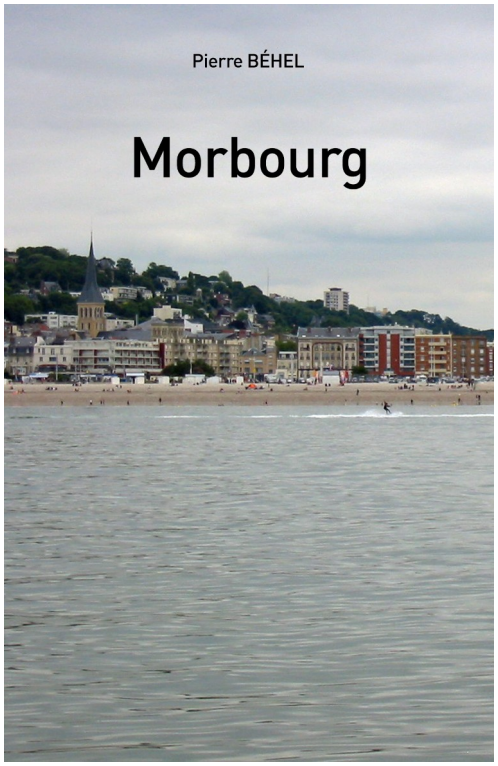
Dans *Morbourg* : l'infection du smartphone visait à repérer la cible (vol de données de géolocalisation) dans le but de prouver son implication dans un réseau criminel.

Dans *La Tour Bleue*, il s'agit de voler des données sensibles transitant via une imprimante multifonction dans le cadre d'une attaque boursière.

Mesures correctives :
1) stocker les données uniquement chiffrées. Récupérées, les données sont inexploitables.
2) Tracer et analyser tous les flux de données afin de repérer les flux suspects (analyse de logs avec outils d'intelligence artificielle, SIEM).
3) Bloquer les sorties de données via des terminaux ou des supports amovibles (usage d'un logiciel de DLP).

Qui sont les pirates ?

Un employé (ou ex-)

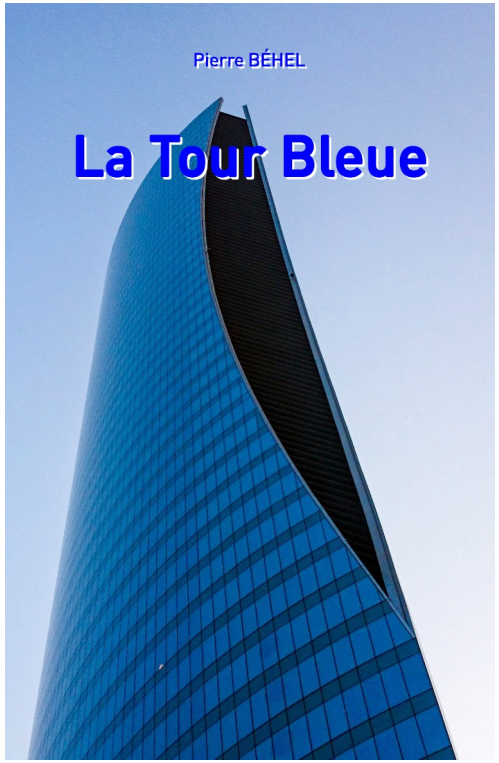


Dans *Morbourg*, le pirate veut se venger du patron de son ancienne entreprise.

La menace interne reste la plus négligée.

Précautions :
1) Veiller à couper ses accès au système d'information dès le départ d'un employé.
2) Surveiller les « utilisateurs à pouvoir » (exemple : Wallix Bastion)
3) DLP, analyse de logs...

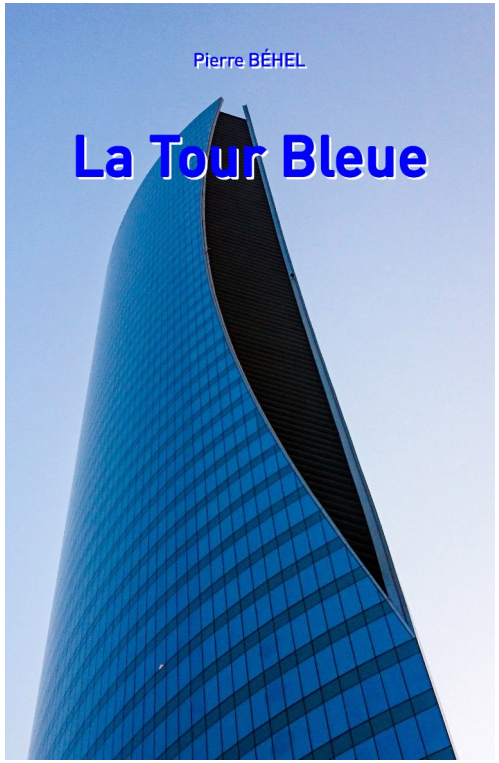
Un voyou « de base »



Le cybercrime est actuellement très hiérarchisé et divers rôles apparaissent :
1) Fabricants d'outils => CaaS (Crime as a Service)
2) Commanditaires d'attaques
3) Exécutants pour le compte des commanditaires et utilisant les outils CaaS.

Et :
4) Petits voyous de base, « script-kiddies », utilisant des outils CaaS pour mener des opérations limitées en solitaire comme le premier pirate dans *La Tour Bleue*.

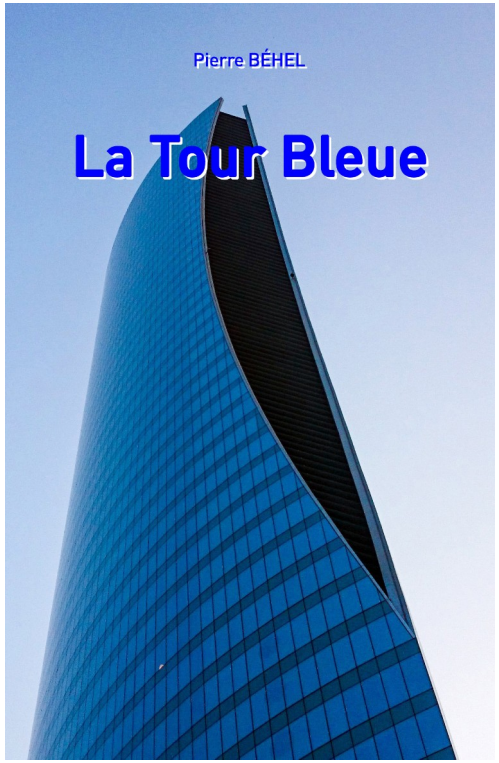
Un mercenaire



Le cybercrime est actuellement très hiérarchisé et divers rôles apparaissent :
1) Fabricants d'outils => CaaS (Crime as a Service)
2) Commanditaires d'attaques
3) Exécutants pour le compte des commanditaires et utilisant les outils CaaS.

Dans *La Tour Bleue*, le 2ème pirate est un mercenaire de type « exécutant » qui est par ailleurs expert en cybersécurité et fabriquant ses propres outils dans une certaine mesure.

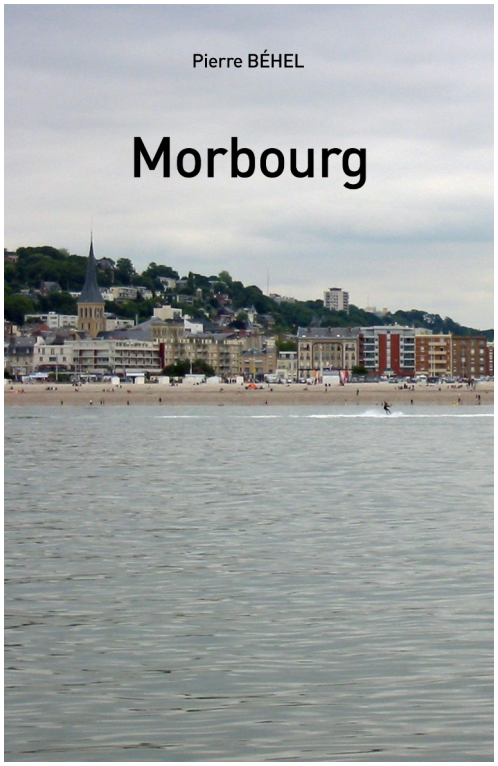
Un créateur d'exploit



Le défi technique peut être une motivation suffisante pour un pirate.

Dans *La Tour Bleue*, le 2ème pirate comme la « gentille pirate » agissent beaucoup par défi (et se défient l'un l'autre).

Un activiste



Dans *Morbourg*, le pirate veut dénoncer les actions du patron de son ancienne entreprise.

L'argent ou la vengeance ne sont pas les seuls mobiles…

Précaution : être irréprochable.

Questions ?

Autres cas...

Dans la sage *Les Ombres de Morbourg*, les pirates sont des gens aux moyens limités et aux objectifs précis.

Il existe des opérations qui relèvent des opérations spéciales menées par des Etats ou des groupements de pirates mercenaires.

Certaines attaques vont bien au-delà de ce qui a été expliqué ici.

L'opération Sunburst visant l'éditeur Solarwinds est un bon exemple.

Mais c'est une autre histoire...