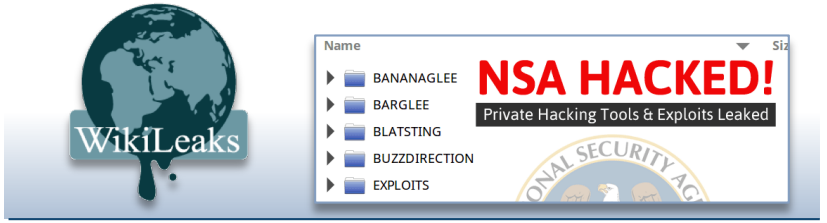
Agence Nationale de la Sécurité des Systèmes d'Information - ANSSI

Patrice Bigeard – Délégué Ile de France

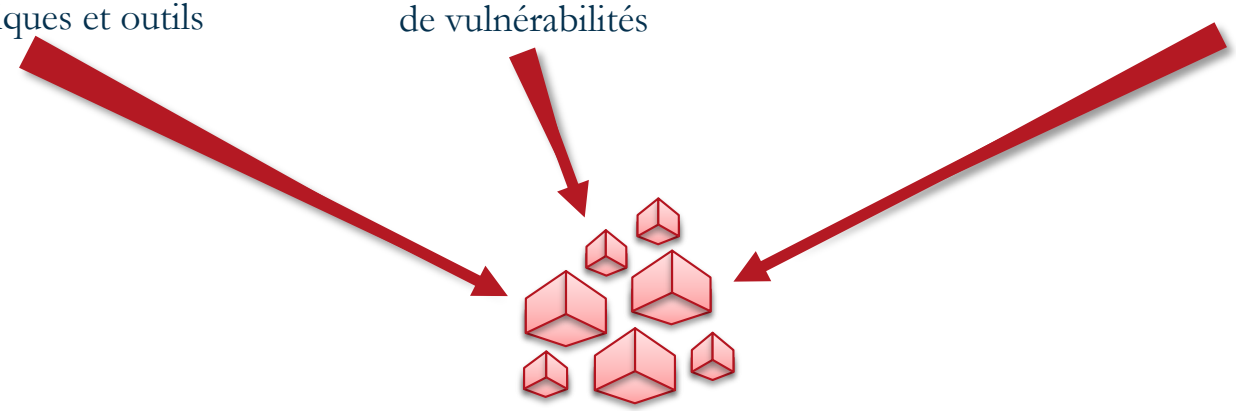
Prolifération de codes d'attaque

Publications de rapports sur techniques et outils

Découvertes et publications de vulnérabilités



Divulgations de codes très sophistiqués

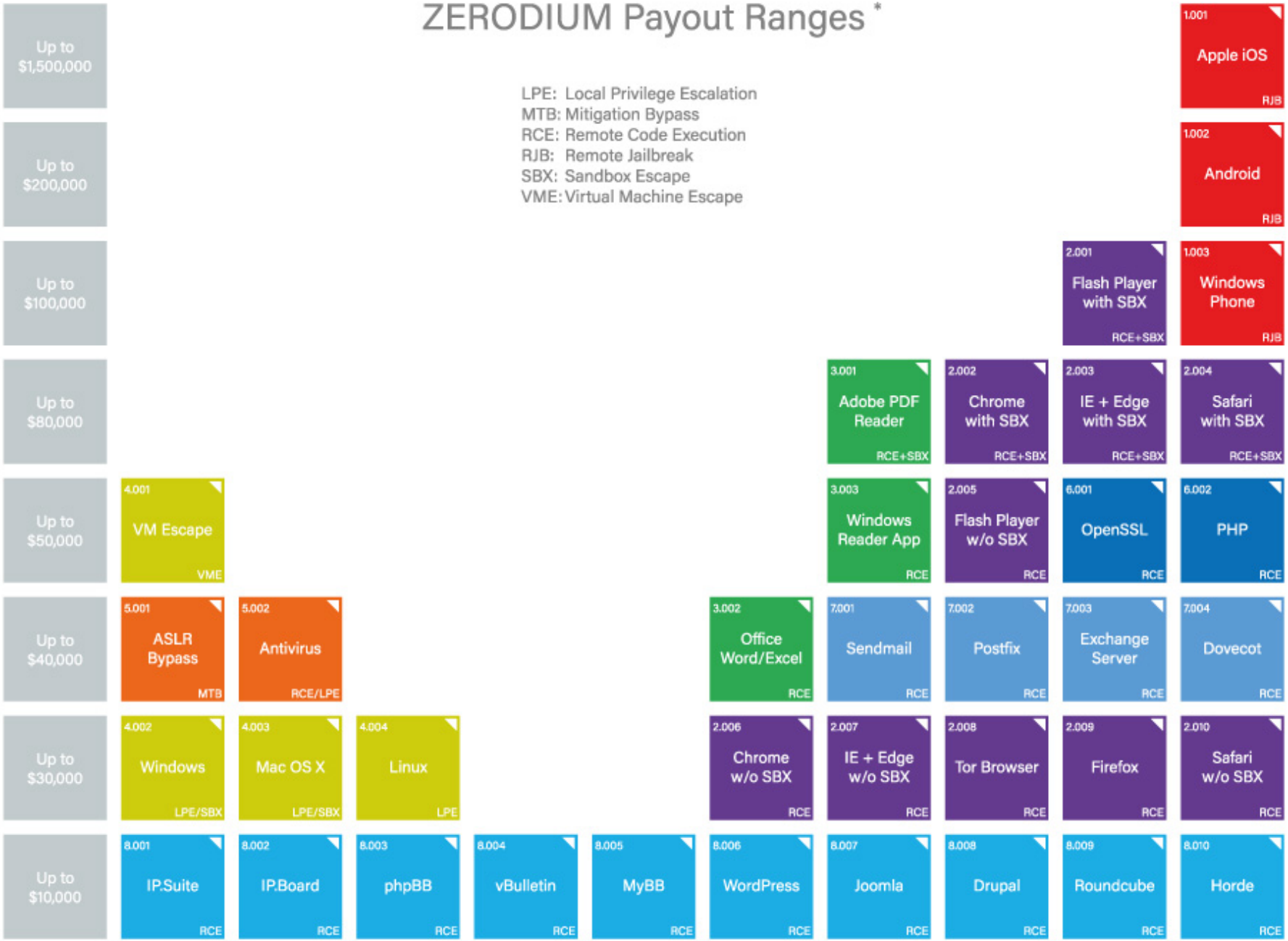


Somme de codes et techniques réutilisables

Aujourd'hui, les attaquants vont plus vite à réaliser de nouveaux codes d'exploitation que les défenseurs à mettre à jour leur système d'information

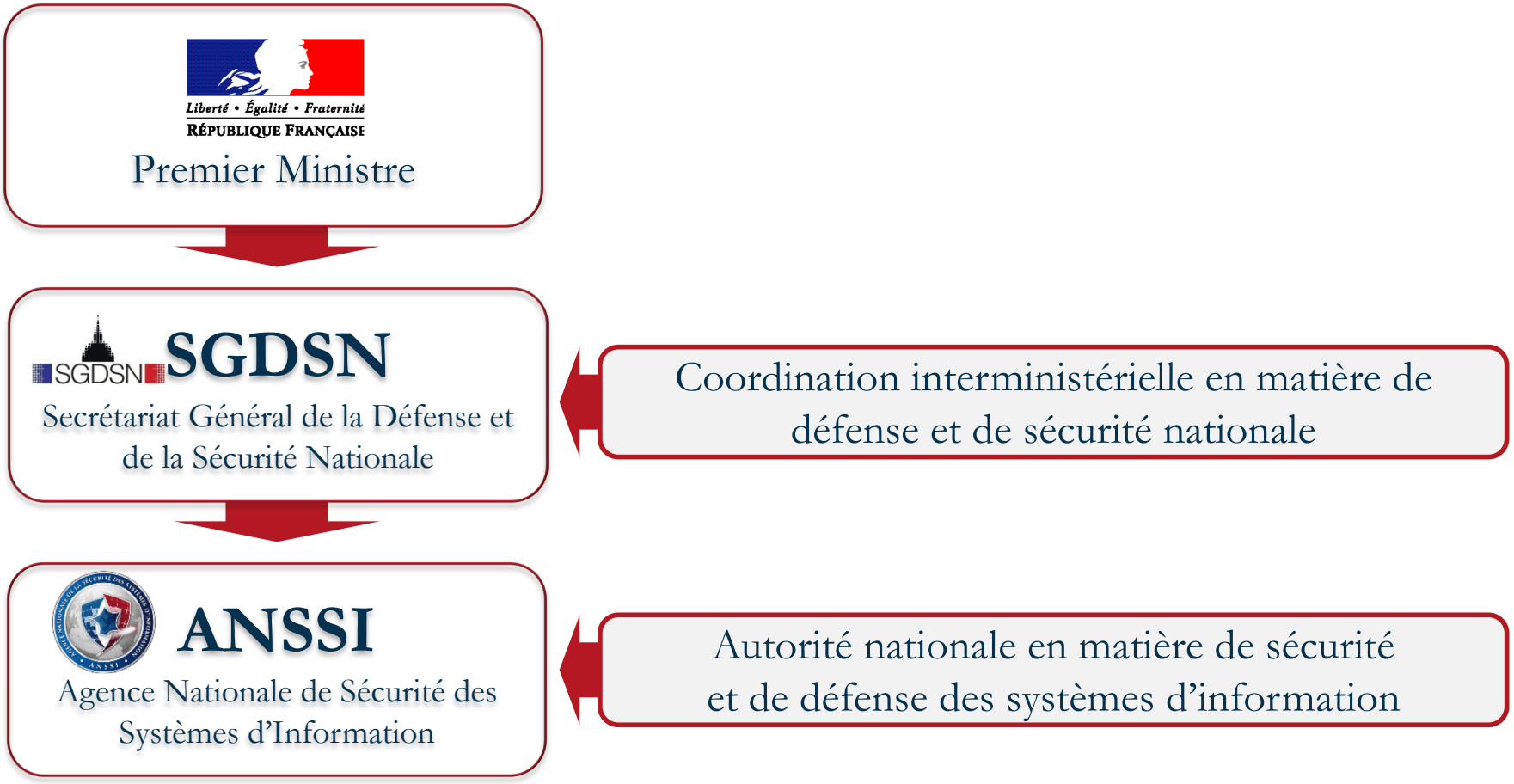
ZERODIUM Payout Ranges *

LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape



** All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.*

Positionnement de l'ANSSI



Créée le 7 juillet 2009 par le décret n°2009-934, l'ANSSI est un **service à compétence nationale.**

Agence Nationale de Sécurité des Systèmes d'Information

SDAG
Sous Direction Affaires Générales

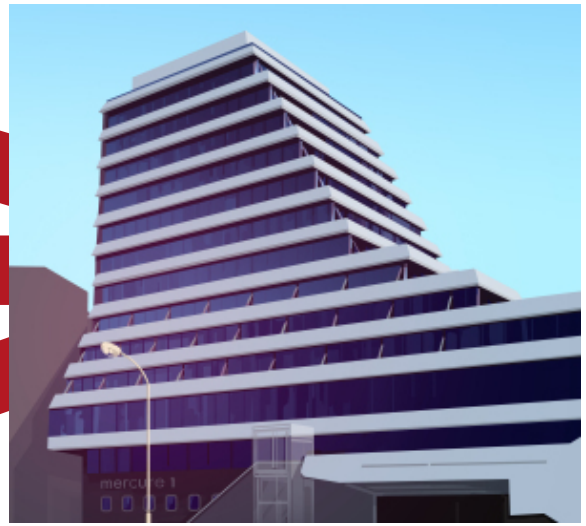
RELEC
Relations Extérieures et Coordination

SDE
Sous Direction Expertise

SIS
Systèmes d'Information Sécurisés

COSSI
Centre Opérationnel de la SSI

Hôtel National des Invalides (75007)



Tour Mercure, 31 quai de Grenelle (75015)

Deux principaux domaines de compétences

-> Autorité de sécurité (prévention)

-> Autorité de défense (réaction)

~~-> Renseignement~~

~~-> Actions offensives~~

Autorité de sécurité (prévention)

- Recherche et expertise technique
- Conseil et assistance
- **Formation et sensibilisation**
- Audits, inspections et contrôles SSI
- Élaboration de textes règlementaires (règles de sécurité LPM)
- Planification et exercices
- Gestion de clés cryptographiques
- Conception, maîtrise d'ouvrage et mise en œuvre des moyens de communication sécurisés pour l' État
- **Labellisation de produits et de services de confiance**
- Contribution au développement de produits gouvernementaux
- Contribution au développement de produits et de services commerciaux de confiance
- Prendre part aux négociations internationales et être en lien avec les partenaires étrangers

Autorité de défense (réaction)

- Veille, analyse et évaluation de la menace
- Détection des attaques informatiques
- Réponse aux attaques informatiques
- Surveillance en temps réel des infrastructures critiques

Dans le cas d'une crise majeure contre les SI de l'État ou des OIV
et dans le cadre des orientations fixées par le Premier ministre, l'ANSSI :

- Décide des mesures de protection à faire appliquer
- Coordonne l'action du gouvernement contre la crise
- Met en œuvre la réponse à la crise

EN CAS D'INCIDENT

Sur Internet, nul n'est à l'abri d'une action malveillante ou de messages non sollicités.

Les éléments suivants vous aideront à avoir les bons réflexes et à contacter les bons correspondants.

VOUS ÊTES UN OPÉRATEUR D'IMPORTANCE VITALE ?

Retrouvez le formulaire de déclaration d'incident à adresser à l'ANSSI dans la rubrique « cybersécurité des OIV »

SOUPÇON D'ATTAQUE INFORMATIQUE ?

Consultez la note d'information *Les bons réflexes en cas d'intrusion sur un système d'information* sur le site du CERT-FR

VOUS RECEVEZ DES MESSAGES NON SOLLICITÉS ?

Utilisez Signal-Spam

VOUS SOUHAITEZ SIGNALER UN CONTENU ILLICITE ?

Utilisez le portail officiel de signalements de contenus illicites

VOUS SOUHAITEZ DÉPOSER PLAINTE EN CAS DE CYBERCRIMINALITÉ ?

La cybercriminalité est le terme employé pour désigner l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunication ou ciblant ces mêmes réseaux. Cette tentative de définition recouvre deux réalités :

EN CAS D'INCIDENT

SOUS-DIRECTION DE LUTTE CONTRE LA CYBERCRIMINALITÉ (SDLC)

France – Particuliers & PME

BRIGADE D'ENQUÊTE SUR LES FRAUDES AUX TECHNOLOGIES DE L'INFORMATION (BEFTI)

Paris et petite couronne – Particuliers & PME

CENTRE DE LUTTE CONTRE LES CRIMINALITÉS NUMÉRIQUES (C3N) DU SERVICE CENTRAL DU RENSEIGNEMENT CRIMINEL (SCRC) DE LA GENDARMERIE NATIONALE

France – Particuliers & organismes

DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE (DGSI)

France – État, secteurs protégés, OIV

Guide d'hygiène informatique

42 règles de sécurité

Guide des bonnes pratiques de l'informatique

12 règles de sécurité

Focus sur le secteur de l'Education

Sur une période de 3 ans (2015-2017), **1200 incidents** signalés au CERT-FR (académies, universités, lycées, collèges)

- 620 liés à des défigurations
- 330 liés à des vulnérabilités
- 200 liés à des indisponibilités (sans compromission)
- **40** liés à des tentatives d'attaques ou compromissions avérées

Focus sur le secteur de l'Education
Cas d'un ERP « Education » (Avril 2018)

1. Un groupe d'écoles d'ingénieurs fait l'acquisition d'un ERP spécialisé dans la gestion d'application universitaires (catalogue des cours, gestion de scolarité, RH, etc.)

2. Un test d'intrusion réalisé avant le déploiement de cette application révèle:
   1. Vulnérabilités sur la page d'authentification
   2. Vulnérabilités sur l'applicatif (injection de codes, messages révélateurs sur le S.I.)

3. Lors des tests, l'exploitation de ces vulnérabilités a permis l'exposition de l'intégralité de la base de données de l'ERP

4. Le prestataire des tests a recommandé à son client de demander à l'éditeur un ensemble de correctifs et d'informer l'ANSSI

Tendances

- Le **nombre global d'attaques** informatiques **augmente**

- Les motivations des attaquants demeurent les mêmes

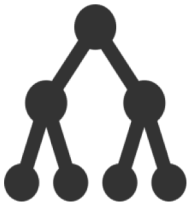
- Les **cibles sont changeantes**, les technologies et usages aussi :

  Les mobiles/tablettes

  Usages pro et perso : moins de frontières

  Le cloud plus ou moins maitrisé

- **Augmentation** des surfaces d'attaques



- L' **Internet des Objets (IoT)** complique les choses (botnets) …

Se préparer à des attaques plus nombreuses et d'impact croissant …

… Et donc anticiper.

Pourquoi les attaques réussissent-elles trop souvent ?

- **Sensibilisation et maturité insuffisante des utilisateurs**
- **Systèmes et applications pas à jour dont sites Web**
- **Politique de gestion des mots de passe insuffisante**
- **Pas de séparation des usages (utilisateur/administrateur) et des réseaux**
- Laxisme dans la gestion des droits d'accès
- Absence de surveillance des SI
- Cloisonnement insuffisant des systèmes (propagation latérale)
- Absence de restrictions (périphériques…)
- Nomadisme / télétravail incontrôlés

Votre élève Martin

Votre élève Willy

L'hydrolienne immergée au large d'Ouessant victime de pirates informatiques

Des pirates informatiques ont perturbé en octobre le contrôle de l'hydrolienne immergée au large d'Ouessant (Finistère), la seule actuellement à être raccordée à un réseau électrique en France. La production d'électricité a été interrompu pendant deux semaines.

AFP | Publié le 17/03/2016 | 19:07, mis à jour le 17/03/2016 | 19:13

© Sabella Hydrolienne Sabella D10 avant son immersion

Source : http://www.zdnet.fr/actualites/quand-un-ransomware-paralyse-un-hopital-americain-39832906.htm

Quand un ransomware paralyse un hôpital américain

Sécurité : *Un hôpital de Los Angeles a vu son système informatique touché par un ransomware, qui a progressivement bloqué la majorité de ses fonctions administratives pendant une semaine. Les attaquants réclameraient la coquette somme de 3,6 millions de dollars pour déverrouiller l'accès aux données chiffrées.*

Par Louis Adam | Mercredi 17 Février 2016

Suivre @zdnetfr

La France n'est pas la seule à voir ses infrastructures infectées par les ransomwares. Aux États Unis, le Hollywood Medical Presbyterian Center a été victime d'une attaque similaire à celle relayée dans la presse au ministère des Transports en début d'année.

Le système informatique de l'hôpital a été infecté par des cyberattaquants ayant recours à un malware de type ransomware (ou rançongiciel) : celui-ci chiffre les données contenues sur la machine et les rend inaccessibles à l'utilisateur, qui se voit contraint de verser une rançon afin d'espérer récupérer l'accès à ses fichiers. Sans système de sauvegarde fonctionnel, la situation peut rapidement devenir critique et cela semble être le cas de cet hôpital, dont les services administratifs se retrouvent paralysés depuis une semaine comme le relatent les médias locaux

Contre les rançongiciels

Sensibilisez, formez, éduquez l'utilisateur. N'ouvrez pas les messages dont la provenance ou la forme est douteuse. Ne vous fiez pas aux apparences. Apprenez à distinguer des emails piégés.

Effectuez des **sauvegardes** régulièrement. Ne laissez pas votre périphérique de sauvegarde banché en continue sur votre installation. Sortez physiquement la sauvegarde de votre réseau et placez là en lieu sûr. Testez vos sauvegardes.

Les rançongiciels utilisent les vulnérabilités des applications pour se propager. Il faut donc impérativement **mettre à jour** ses principaux outils et désactiver les macros exécutables des solutions « Office ».

Ne travaillez pas en tant qu' « administrateur » de votre poste. Une fois que celui-ci a été configuré, créer un **compte utilisateur** et n'utiliser que celui-ci. Cette règle empêchera l'escroc d'avoir tous les privilèges sur votre machine.

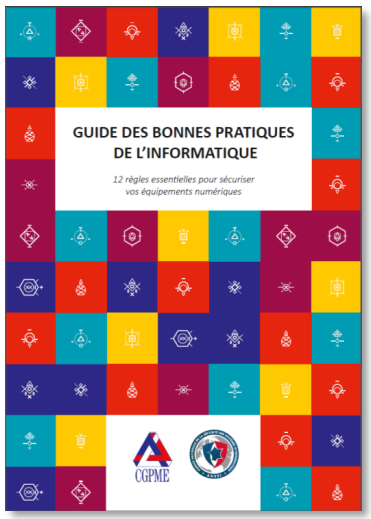
Les solutions …

Réponses :

> Technique

> Organisationnel / règle

> **Humain**



www.ssi.gouv.fr

Panorama des menaces

TABLE DES MATIERES

Présentation SecNum*académie*

- Cours **gratuit** en ligne sous forme de MOOC
- Modules de sensibilisation à la sécurité des systèmes d'information à destination des utilisateurs en milieu professionnel
- Avril 2018: 62 000 inscrits

Objectifs :

- Permettre à tous d'être initiés à la cybersécurité
- Approfondir leurs connaissances
- Pouvoir agir sur la protection de leurs systèmes

www.secnumacademie.gouv.fr