Les RansomWares

By Denis JACOPINI

C.A. Nîmes

Les RansomWares

Formation d'une journée

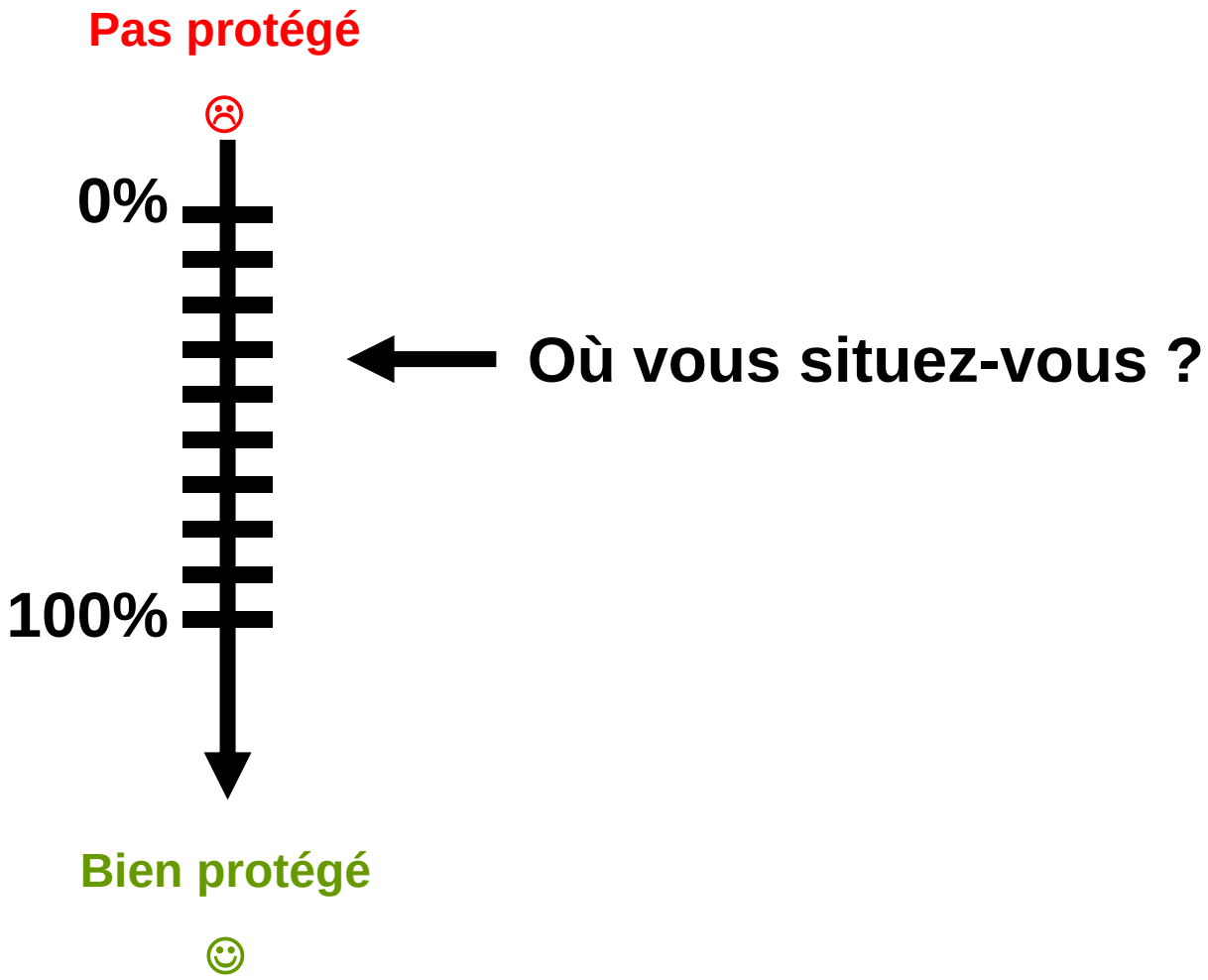
1. **Etat des lieux**
2. **Droits et devoirs**
3. **Bref historique**
4. **Les différentes catégories**
5. **Comment se protéger**
6. **Que faire en cas d'attaque…**

Les RansomWares

<u>On ne verra que le résumé d'une partie</u>

1. **Etat des lieux**
2. **Droits et devoirs**
3. **Bref historique**
4. **Les différentes catégories**
5. **Comment se protéger**
6. **Que faire en cas d'attaque…**

Les RansomWares – Que faire en cas d'attaque



Les RansomWares – Que faire en cas d'attaque

http://itfun.kr/173

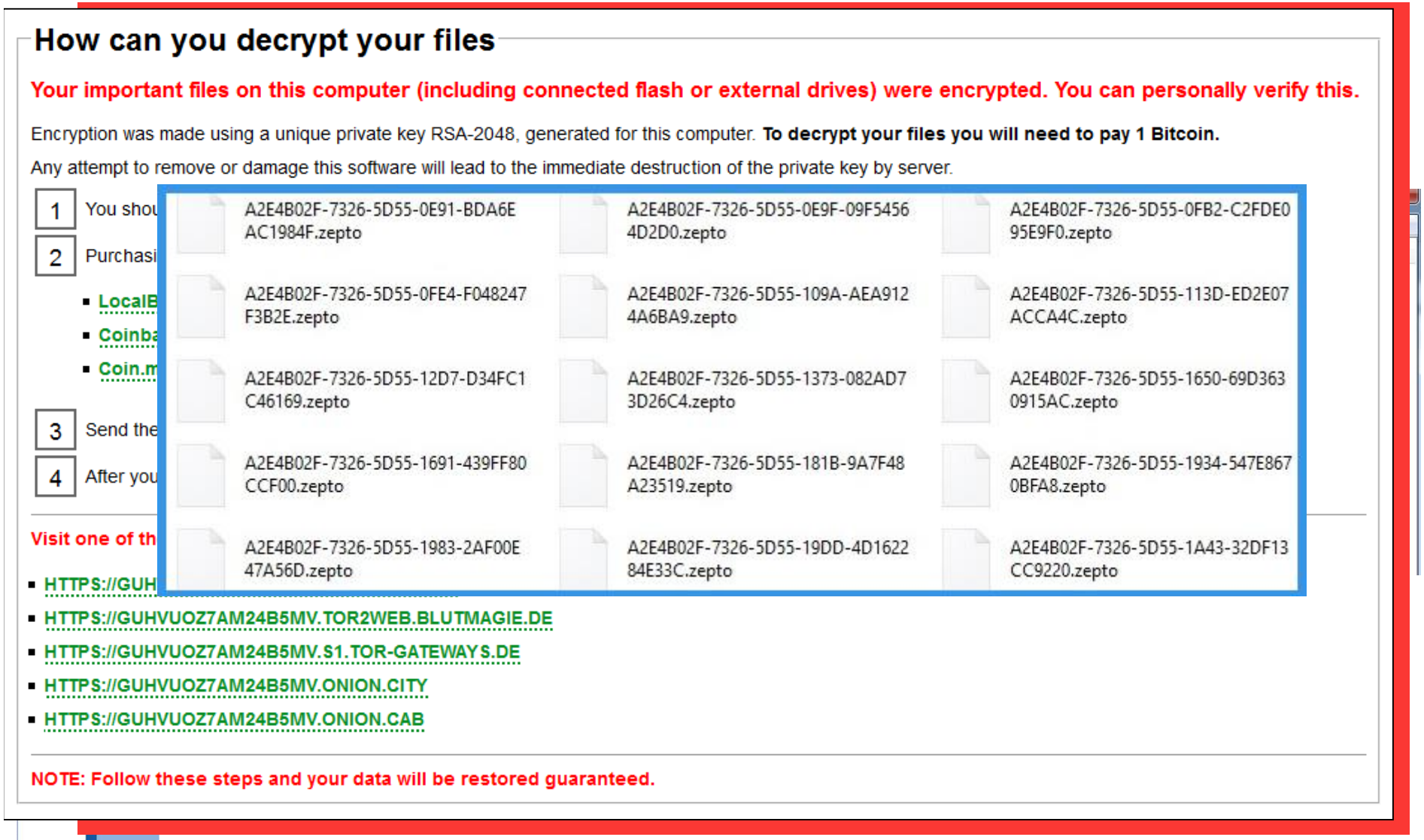

NO MORE RANSOM!
NEED HELP unlocking your digital life without paying your attackers*?
YES
NO
Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

Les RansomWares – Que faire en cas d'attaque

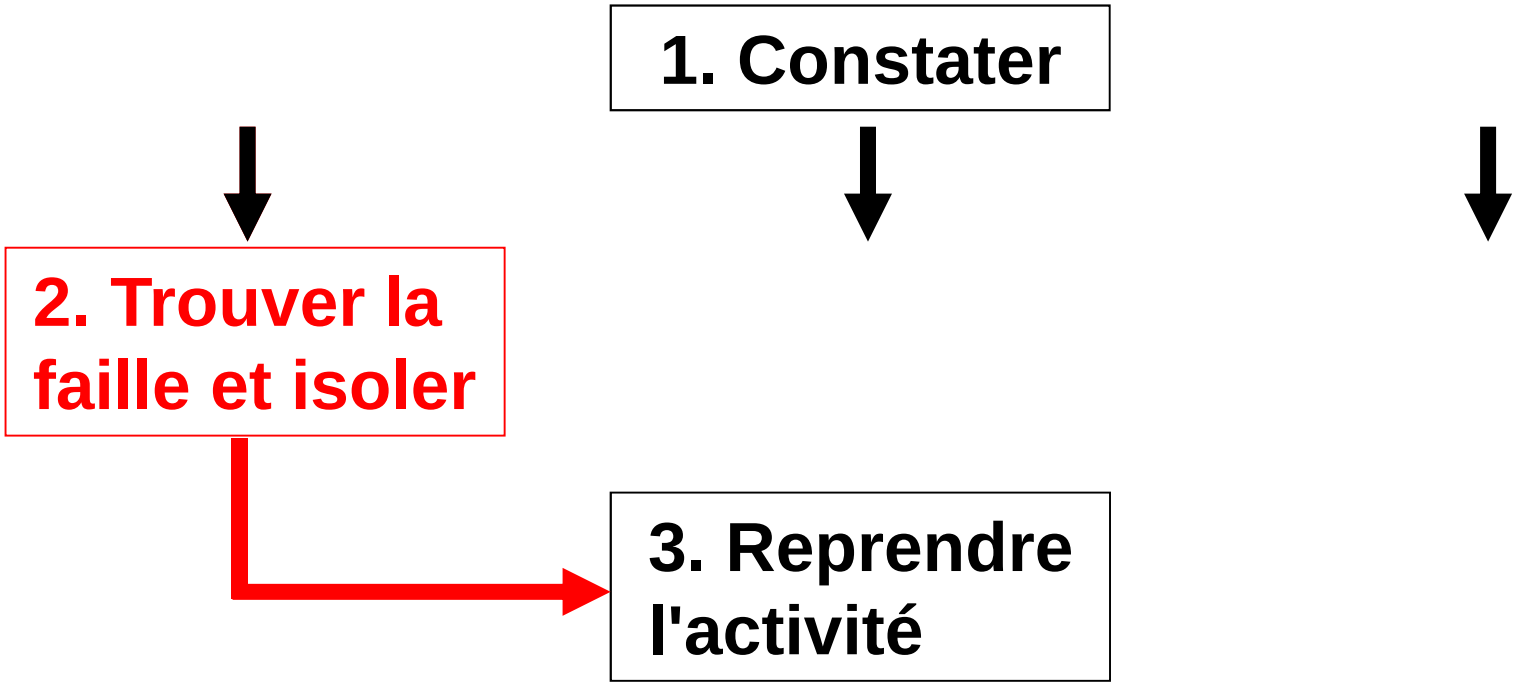
1. Constater

Les RansomWares – Que faire en cas d'attaque

1. Constater



Les RansomWares – Que faire en cas d'attaque

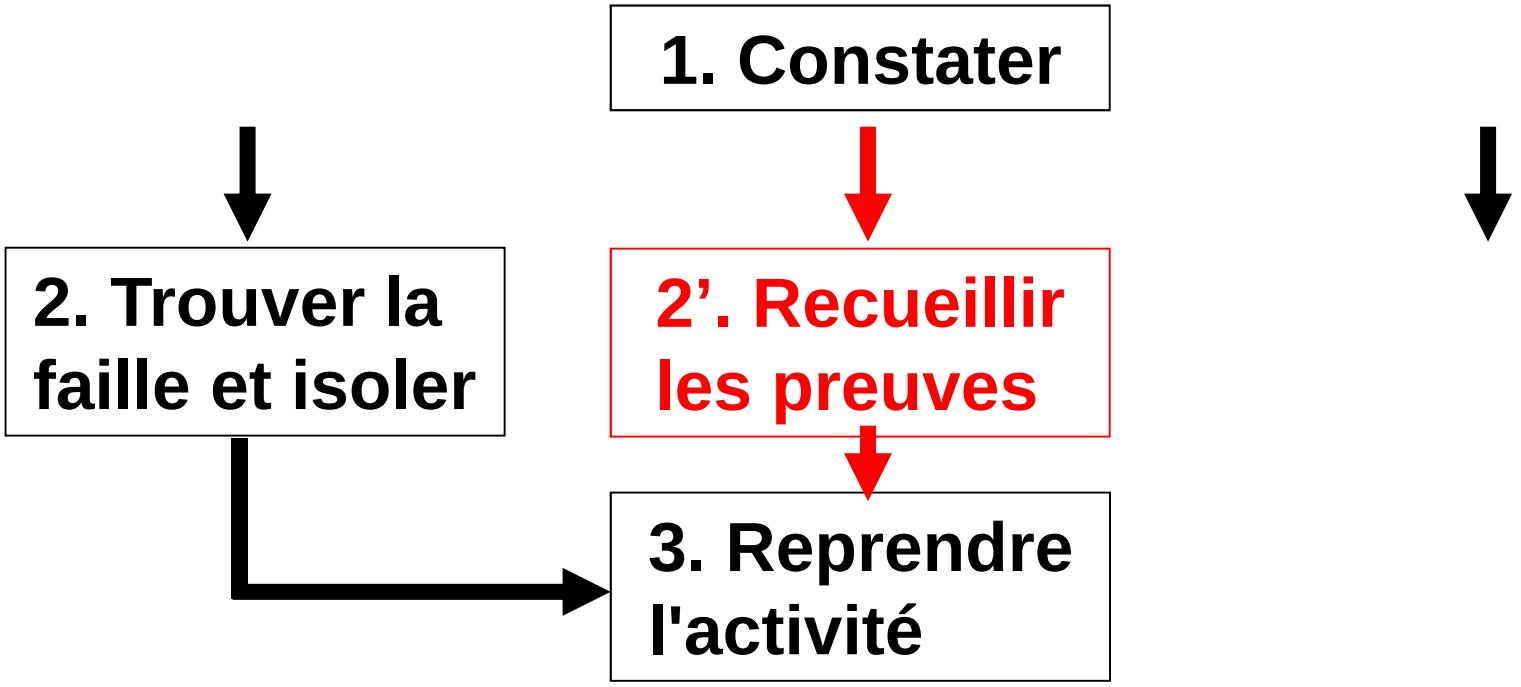


Les RansomWares – Que faire en cas d'attaque

2. Trouver la faille et isoler

- **Provient d'un e-mail (75% des cas) ;**
- **Est cachée dans une page Web (20% des cas) ;**
- **Dans 76% des cas, l'intrusion provient d'une manipulation réalisée par un salarié ;**
- **90% manipulations d'étourderie ;**
- **10% manipulations malveillantes.**

Les RansomWares – Que faire en cas d'attaque



Les RansomWares – Que faire en cas d'attaque

2'. Recueillir les preuves

- Capture d'écran / Photo / Impression ;

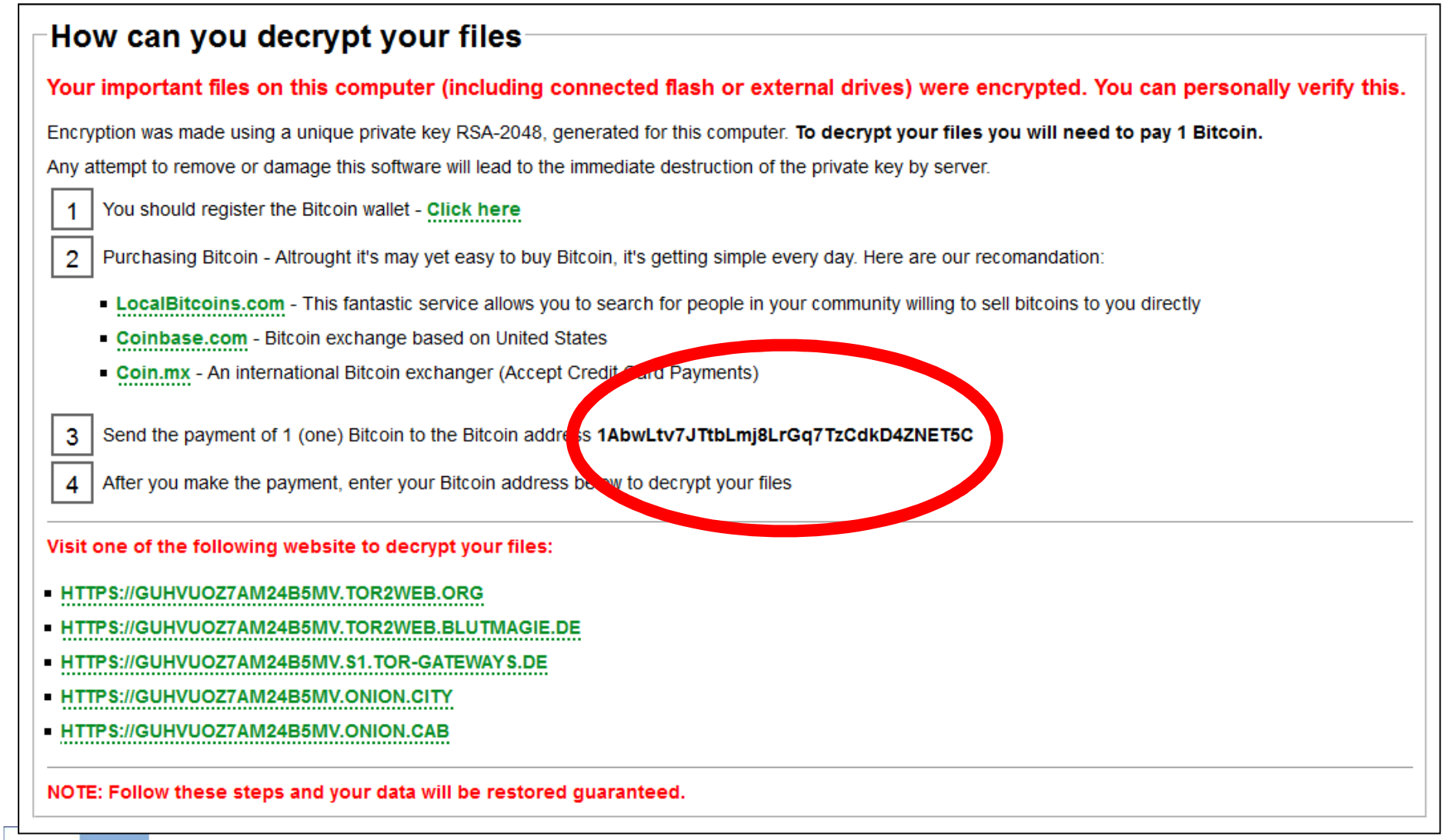
Les RansomWares – Que faire en cas d'attaque

2'. Recueillir les preuves

- **Capture d'écran / Photo / Impression ;**
- **N° du compte Bitcoin ;**

Les RansomWares – Que faire en cas d'attaque

2'. Recueillir les preuves



How can you decrypt your files

Your important files on this computer (including connected flash or external drives) were encrypted. You can personally verify this.

Encryption was made using a unique private key RSA-2048, generated for this computer. **To decrypt your files you will need to pay 1 Bitcoin.**

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

1. You should register the Bitcoin wallet - Click here
2. Purchasing Bitcoin - Altrought it's may yet easy to buy Bitcoin, it's getting simple every day. Here are our recomandation:
   - LocalBitcoins.com - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly
   - Coinbase.com - Bitcoin exchange based on United States
   - Coin.mx - An international Bitcoin exchanger (Accept Credit Card Payments)
3. Send the payment of 1 (one) Bitcoin to the Bitcoin address **1AbwLtv7JTtbLmj8LrGq7TzCdkD4ZNET5C**
4. After you make the payment, enter your Bitcoin address below to decrypt your files

Visit one of the following website to decrypt your files:

- HTTPS://GUHVUOZ7AM24B5MV.TOR2WEB.ORG
- HTTPS://GUHVUOZ7AM24B5MV.TOR2WEB.BLUTMAGIE.DE
- HTTPS://GUHVUOZ7AM24B5MV.S1.TOR-GATEWAYS.DE
- HTTPS://GUHVUOZ7AM24B5MV.ONION.CITY
- HTTPS://GUHVUOZ7AM24B5MV.ONION.CAB

NOTE: Follow these steps and your data will be restored guaranteed.

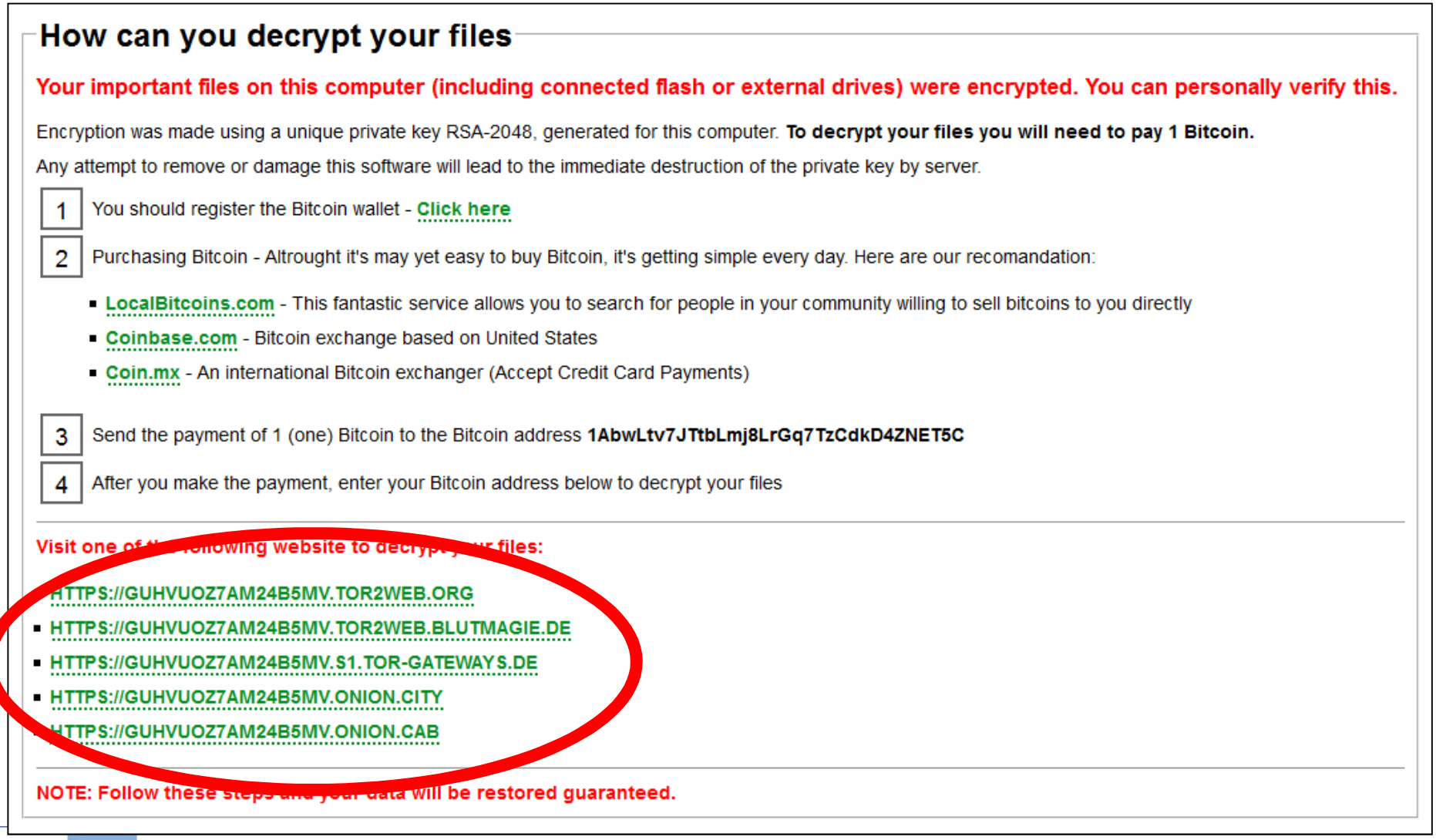
Les RansomWares – Que faire en cas d'attaque

2'. Recueillir les preuves

- **Capture d'écran / Photo / Impression ;**
- **N° du compte Bitcoin ;**
- **Adresse du site .onion ;**

Les RansomWares – Que faire en cas d'attaque

2'. Recueillir les preuves



How can you decrypt your files

Your important files on this computer (including connected flash or external drives) were encrypted. You can personally verify this.

Encryption was made using a unique private key RSA-2048, generated for this computer. **To decrypt your files you will need to pay 1 Bitcoin.**

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

1. You should register the Bitcoin wallet - Click here
2. Purchasing Bitcoin - Altrought it's may yet easy to buy Bitcoin, it's getting simple every day. Here are our recomandation:
   - LocalBitcoins.com - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly
   - Coinbase.com - Bitcoin exchange based on United States
   - Coin.mx - An international Bitcoin exchanger (Accept Credit Card Payments)
3. Send the payment of 1 (one) Bitcoin to the Bitcoin address **1AbwLtv7JTtbLmj8LrGq7TzCdkD4ZNET5C**
4. After you make the payment, enter your Bitcoin address below to decrypt your files

Visit one of the following website to decrypt your files:

- HTTPS://GUHVUOZ7AM24B5MV.TOR2WEB.ORG
- HTTPS://GUHVUOZ7AM24B5MV.TOR2WEB.BLUTMAGIE.DE
- HTTPS://GUHVUOZ7AM24B5MV.S1.TOR-GATEWAYS.DE
- HTTPS://GUHVUOZ7AM24B5MV.ONION.CITY
- HTTPS://GUHVUOZ7AM24B5MV.ONION.CAB

NOTE: Follow these steps and your data will be restored guaranteed.

Les RansomWares – Que faire en cas d'attaque

2'. Recueillir les preuves

- **Capture d'écran / Photo / Impression ;**
- **N° du compte Bitcoin ;**
- **Adresse du site .onion ;**
- **c:\windows\system32\drivers\etc\hosts ;**

Les RansomWares – Que faire en cas d'attaque

2'. Recueillir les preuves

- **Capture d'écran / Photo / Impression ;**
- **N° du compte Bitcoin ;**
- **Adresse du site .onion ;**
- **c:\windows\system32\drivers\etc\hosts ;**
- **Entête du mail ;**

Les RansomWares – Que faire en cas d'attaque

2'. Recueillir les preuves

- **Capture d'écran / Photo / Impression ;**
- **N° du compte Bitcoin ;**
- **Adresse du site .onion ;**
- **c:\windows\system32\drivers\etc\hosts ;**
- **Entête du mail ;**
- **La souche virale sur une clef USB ;**

Les RansomWares – Que faire en cas d'attaque

2'. Recueillir les preuves

- **Capture d'écran / Photo / Impression ;**
- **N° du compte Bitcoin ;**
- **Adresse du site .onion ;**
- **c:\windows\system32\drivers\etc\hosts ;**
- **Entête du mail ;**
- **La souche virale sur une clef USB ;**
- **Journal des connexions du poste ;**

Les RansomWares – Que faire en cas d'attaque

2'. Recueillir les preuves

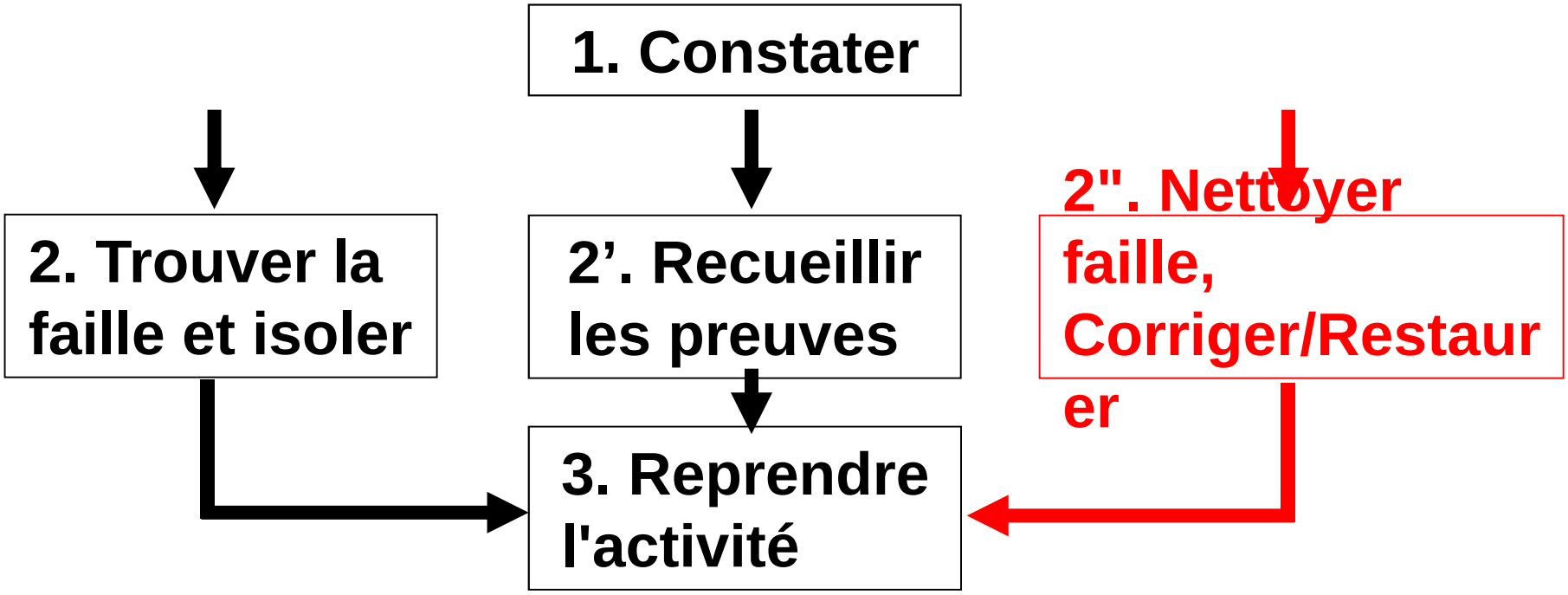
- **Capture d'écran / Photo / Impression ;**
- **N° du compte Bitcoin ;**
- **Adresse du site .onion ;**
- **c:\windows\system32\drivers\etc\hosts ;**
- **Entête du mail ;**
- **La souche virale sur une clef USB ;**
- **Journal des connexions du poste ;**
- **Logs Firewalls, routeurs ;**

Les RansomWares – Que faire en cas d'attaque

2'. Recueillir les preuves

- **Capture d'écran / Photo / Impression ;**
- **N° du compte Bitcoin ;**
- **Adresse du site .onion ;**
- **c:\windows\system32\drivers\etc\hosts ;**
- **Entête du mail ;**
- **La souche virale sur une clef USB ;**
- **Journal des connexions du poste ;**
- **Logs Firewalls, routeurs ;**
- **Copie physique du disque.**

Les RansomWares – Que faire en cas d'attaque



Les RansomWares – Que faire en cas d'attaque

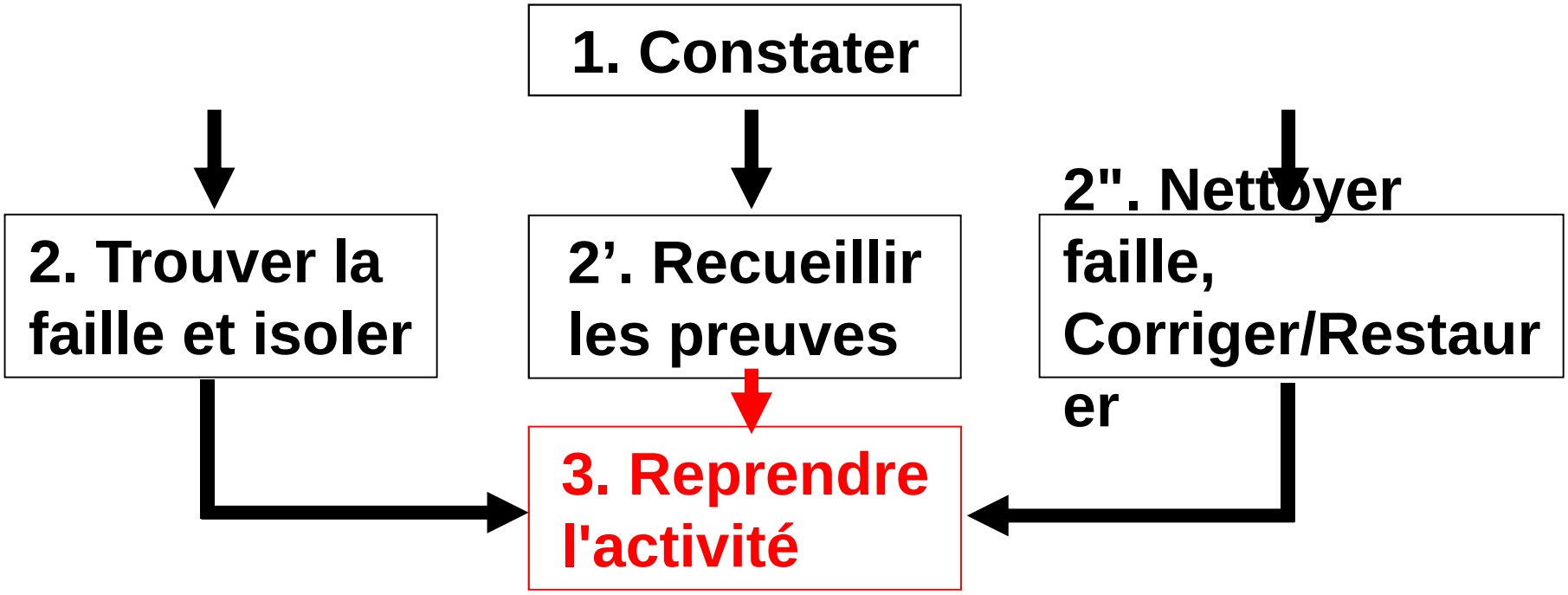
2". Nettoyer et corriger la faille

1. **Modification de la date et de l'heure**
2. **Mise à jour du système d'exploitation**
3. **Mise à jour des navigateurs**
4. **Mise à jour des logiciels**
5. **Outil de nettoyage des fichiers cryptés**
6. **Logiciels de nettoyage des PUP (Potentially Unwanted Programs)**

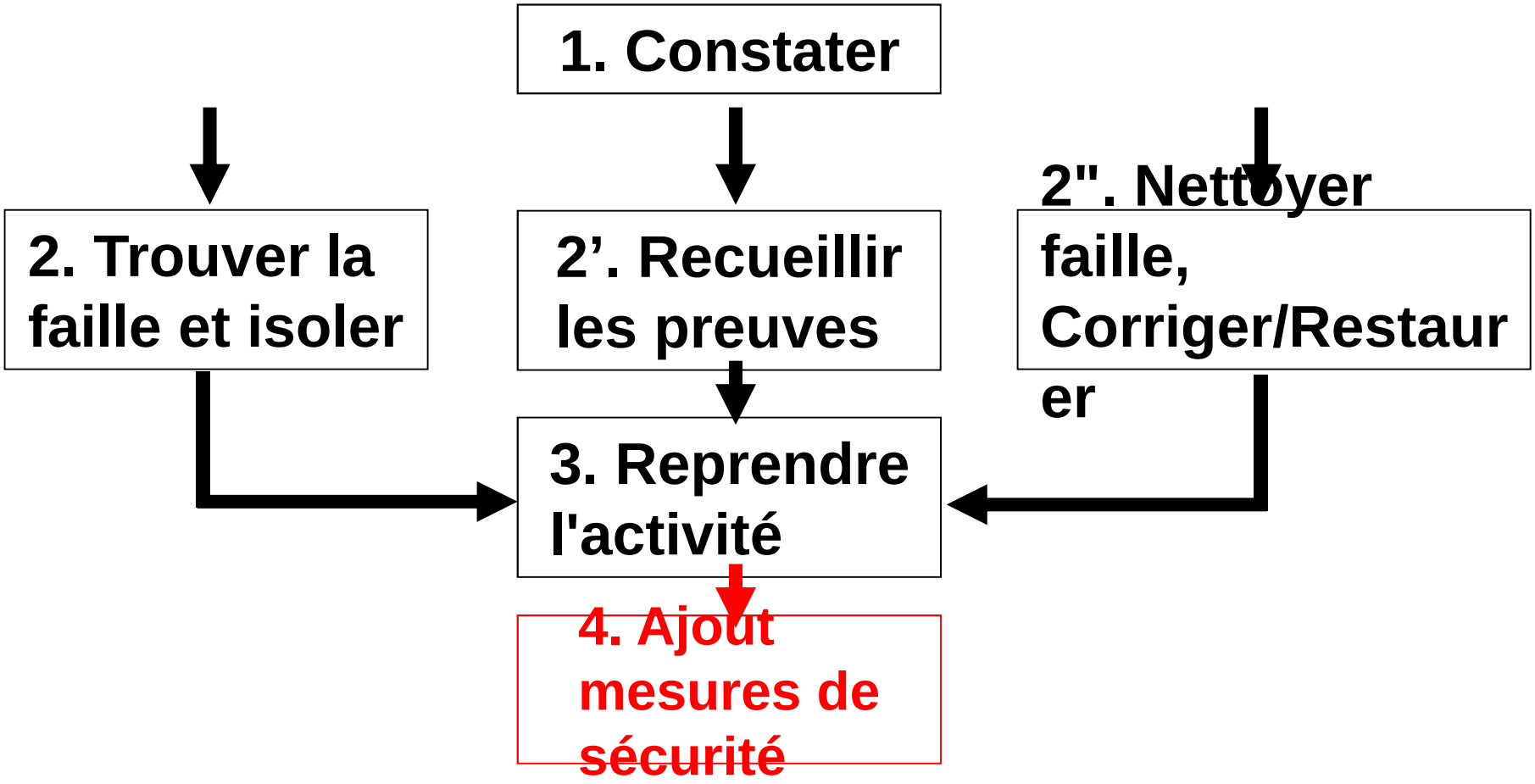
   Malwarebyte Anti-Malware, RogueKiller, ADW Cleaner…
7. **Plugins de Navigateur**

   WOT, Blockulicious…

Les RansomWares – Que faire en cas d'attaque

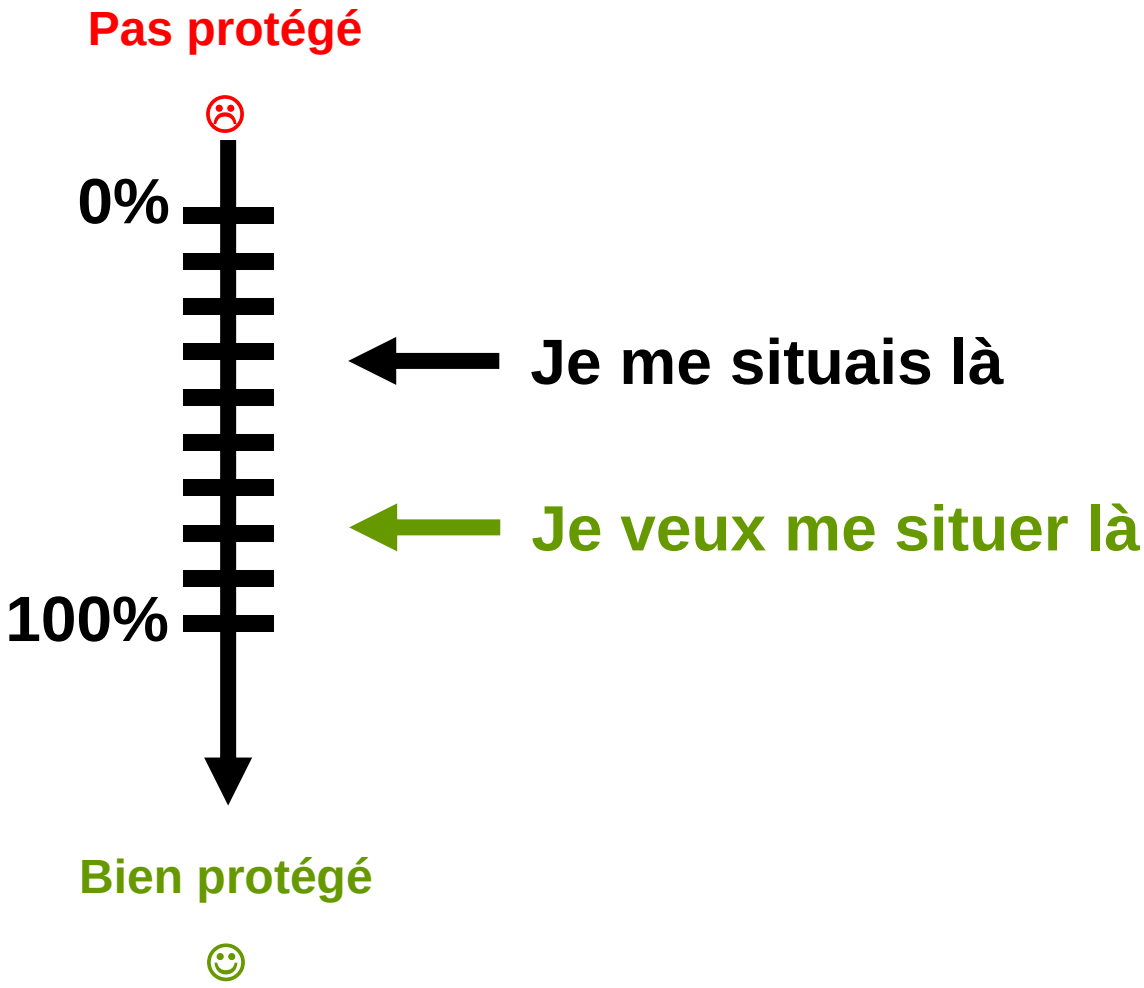


Les RansomWares – Que faire en cas d'attaque



Les RansomWares – Que faire en cas d'attaque

4. Ajout mesures de sécurité



Les RansomWares – Que faire en cas d'attaque

4. Ajout mesures de sécurité

1. Techniques

1.1 Mises à jour OS, Logiciels, Navigateurs + Plugins ;
1.2 Fonction « UAC, User Account Control » activée ;
1.3 Désactiver Remote Desktop Protocol (RDP) ;
1.4 Limiter les droits utilisateur ;
1.5 Mise en place d'une PSSI ;
1.6 Mise en place d'un P.C.A. et d'une P.R.A.
1.7 Outils de détection de Ransomwares (Marmiton / RansomWhere) ;
1.8 Outils de protection de la messagerie (Anti-pub, spam…) ;
1.9 Désactiver Windows Script Host.

2. Juridiques

2.1 Charte informatique
2.2 Assurance

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité

Les RansomWares – Que faire en cas d'attaque

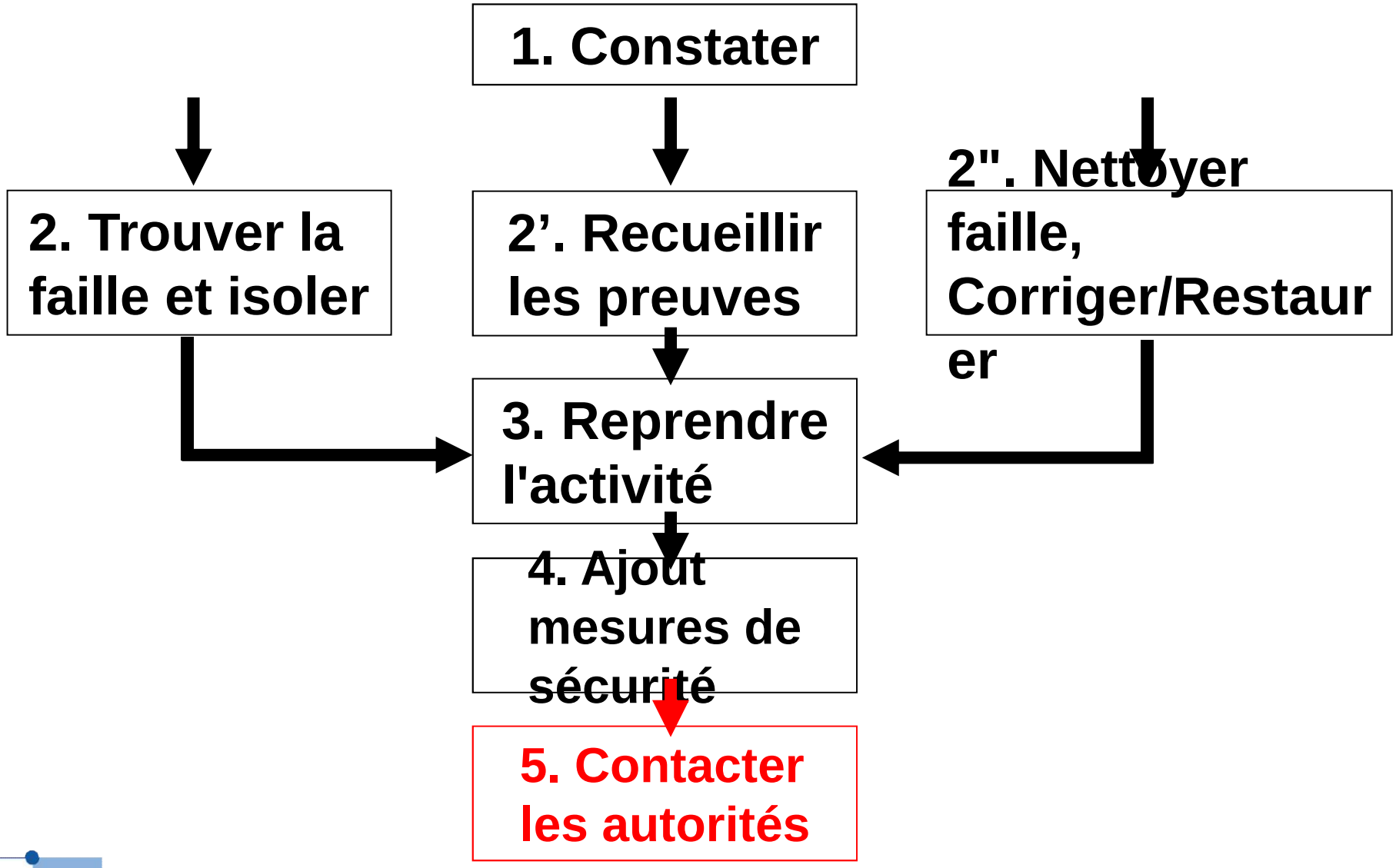
4. Ajout mesures de sécurité

- AlliaCERT est un CERT privé de la société Alliacom ouvert à l'ensemble des entreprises et des institutions ;
- Le CERT-BDF est le CERT de la Banque de France [6] ;
- Le CSIRT BNP Paribas est le CSIRT du Groupe BNP Paribas [7] ;
- Le CERT-Conix est un CERT privé du groupe Conix ouvert à l'ensemble des entreprises et des institutions qui fournit des services de veille et réponse aux incidents de sécurité et est adossé à un service de cyber-surveillance [8] ;
- Le CERT Credit Agricole est le CERT / CSIRT du Groupe Crédit Agricole Il est le premier CERT bancaire à être à la fois accrédité TF-CSIRT et membre du FIRST [9] ;
- Le CERT-CS est le CERT de la société CS Communication & Systèmes ;
- Le CERT CYBERPROTECT est le CSIRT privé de la société Cyberprotect ouvert à l'ensemble des entreprises et des institutions [10] ;
- le CERT-DEVOTEAM (anciennement APOGEE SecWatch) est un CSIRT privé du groupe Devoteam [11] ;
- le CERT-FR (anciennement CERTA appartenant à l'ANSSI/SGDN) est le CERT affecté au secteur de l'administration française [12] ;
- Le CERT-Intrinsec est un CSIRT privé de la société Intrinsec ouvert aux entreprises et institutions [13] ;
- le CERT-IST est le CERT affecté au secteur de l'Industrie, des Services et du Tertiaire (IST). Il a été créé à la fin de l'année 1998 par quatre partenaires : Alcatel, le CNES, ELF et France Télécom [14] ;
- Le CERT La Poste est le CERT interne du Groupe La Poste [15] ;
- le CERT-LEXSI est un CSIRT privé du groupe LEXSI (Laboratoire d'EXpertise en Sécurité de l'Information) ouvert à l'ensemble des entreprises et des institutions [16] ;
- le CERT-Orange-CC est le CERT privé interne du groupe Orange [17] ;
- le CERT-RENATER est le CERT de la communauté des membres du GIP RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche) ;
- Le CERT-SNCF est le CERT privé interne du Groupe SNCF [18] ;
- Le CERT-Société Generale est un CSIRT privé interne du groupe Société Générale. Il est historiquement le premier CERT privé français à avoir été accrédité par le FIRST, en février 2010 [19] ;
- le CERT-Solucom est un CSIRT privé du cabinet Solucom ouvert à l'ensemble des entreprises et des institutions [20] ;
- le CERT Steria est un CERT privé de la société Sopra Steria ouvert à l'ensemble des entreprises et des institutions [21] ;
- le CERT-UBIK est un CSIRT privé de la société Digital Security qui s'intéresse à la sécurité des systèmes d'information et, plus particulièrement, à la sécurité de l'Internet Des Objets [22] ;
- Le CERT-XMCO est un CSIRT ouvert aux entreprises qui fournit des services de veille, de cyber-surveillance et de réponses aux incidents de sécurité (forensic) [23]
- le CERT-AKAOMA est le CSIRT de la société AKAOMA proposant des services de cyber-surveillance et de réponse aux incidents de sécurité à l'ensemble des entreprises et institutions [24]

6. Autres mesures ?

7. Qui fait ça parmi vous ?

Les RansomWares – Que faire en cas d'attaque



Les RansomWares – Que faire en cas d'attaque

5. Contacter les autorités

DÉPOSER PLAINTE

POURQUOI ?

- **Rembourser par l'assurance**
- **Retrouver l'auteur**
- **Créer un antidote ?**
- **Disculper si propagation**

Les RansomWares – Que faire en cas d'attaque

5. Contacter les autorités

DÉPOSER PLAINTE

Infraction :

Atteintes aux Systèmes de Traitement Automatisé de Données (S.T.A.D.)

sanctionnées par les articles L.323-1 et suivants du Code pénal.

Atteintes aux droits de la personne liés aux fichiers ou traitement informatiques (art. 226-16 à 226-24 du Code pénal / Loi 78-17 du 6 janvier 1978 dite « informatique et liberté » modifiée par la loi 2004-801 du 6 aout 2004).

Tribunal de Grande Instance de Paris

POLICE NATIONALE

Gendarmerie nationale

Une force humaine

CNEJITA EXPERTS

Les RansomWares – Que faire en cas d'attaque

5. Contacter les autorités

ORGANES CONCERNÉS

B.E.F.T.I. : Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information
(pour les machines sur Paris ou sur la petite couronne)

122/126, rue du Château des Rentiers - 75 013 Paris.
Standard : 01 55 75 26 19
Email : pppj-befti-gestion@interieur.gouv.fr.

O.C.L.C.T.I.C. : Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication

1 rue des Trois Fontanot
92 000 Nanterre
Standard : 01 49 27 49 27

Les RansomWares – Que faire en cas d'attaque

5. Contacter les autorités

ORGANES CONCERNÉS

C3N : Centre de lutte contre les criminalités numériques.

CERGY-PONTOISE

Téléphone : 01 78 47 36 52

D2A : Division de l'Anticipation et de l'Analyse

11 rue des Saussaies - 75008 Paris

Téléphone : 01 49 27 49 27

Les RansomWares – Que faire en cas d'attaque

5. Contacter les autorités

RÉSEAU D'ENQUÊTEURS

SPÉCIALISÉS EN CYBERCRIMINALITÉ

- **POLICE**

  ICC (Investigateurs en CyberCriminalité)

- **GENDARMERIE**

  N-TECH (enquêteurs Nouvelles Technologies)

Les RansomWares – Que faire en cas d’attaque

5. Contacter les autorités

- **PLATEFORME PHAROS**

  www.internet-signalement.gouv.fr

  Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements

Les RansomWares – Que faire en cas d'attaque

5. C

Les Ran ttaque

5. Contacte s

Pédophilie et pédopornographie

Terrorisme et apologie du terrorisme

Un contenu illicite est publié sur internet

Expression du racisme, de l'antisémitisme et de la xénophobie

Arnaques financières sur Internet

Incitation de la haine raciale, éthnique et religieuse

Un internaute repère un contenu illicite

Un gendarme ou un policier repère un contenu illicite

SIGNALER UN CONTENU

Il le signale à l'hébergeur du site ou au réseau social

L'hébergeur supprime le contenu
il agit en moyenne dans un délais de 24h

IL DEMANDE À L'HÉBERGEUR DE LE SUPPRIMER

ET/OU

PHAROS

Il le signale sur Pharos
https://www.internet-signalement.gouv.fr

Les policiers et gendarmes de l'OCLCTIC* vérifient que le contenu constitue une infraction à la loi française

Si l'infraction est constatée, l'auteur des propos peut faire l'objet d'une enquête sous l'autorité du Procureur de la République

CNEJITA EXPERTS

Les RansomWares – Que faire en cas d'attaque

5. Contacter les autorités

- **PLATEFORME PHAROS**

  www.internet-signalement.gouv.fr

  Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements

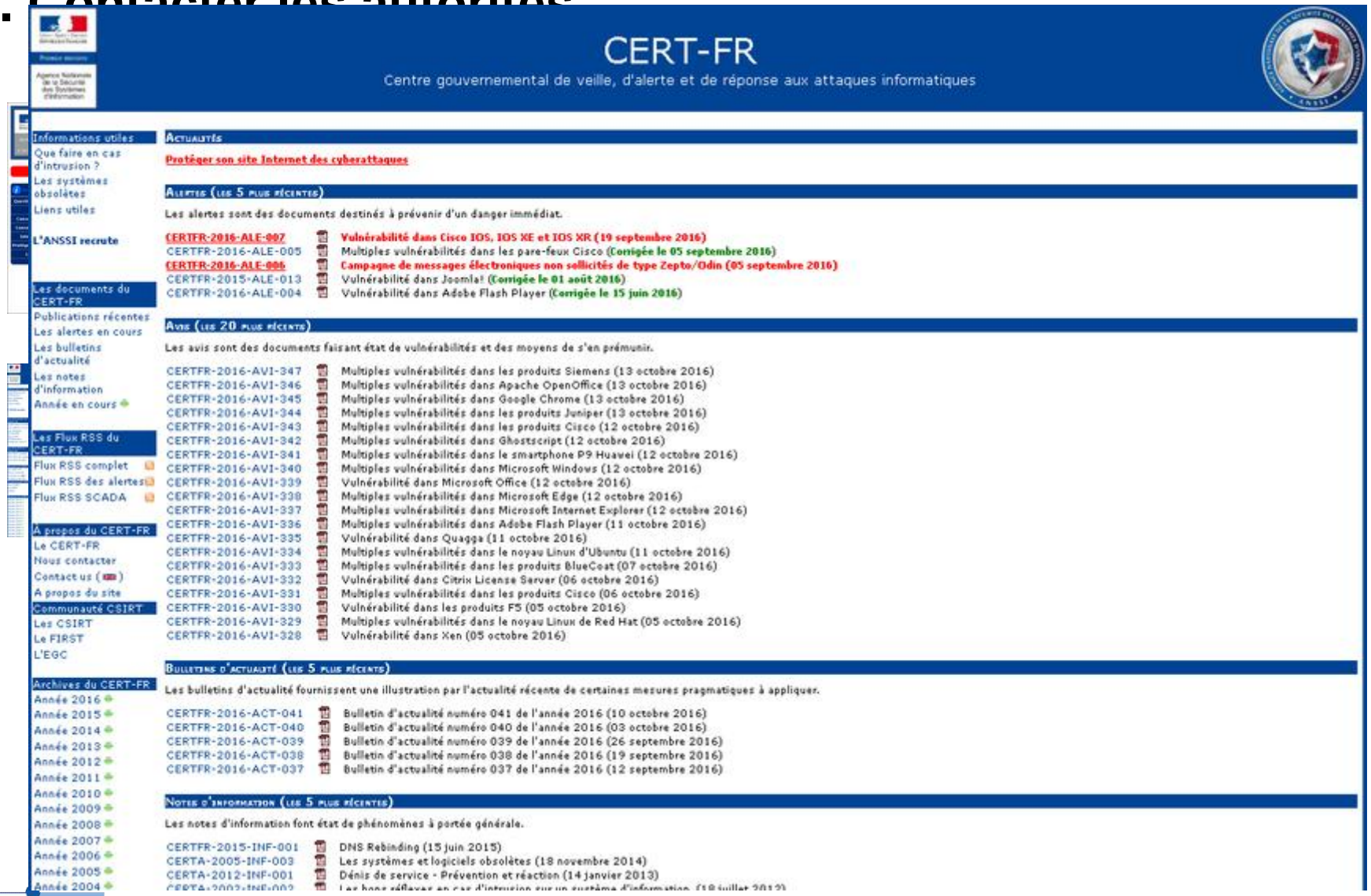
- **CERTA**

  CERT dont dépendent les administrations

  contact@cert.ssi.gouv.fr - téléphone : 01 71 75 84 50

Les RansomWares – Que faire en cas d'attaque

5. Contacter les autorités



CERT-FR

Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

Informations utiles
Que faire en cas d'intrusion ?
Les systèmes obsolètes
Liens utiles

L'ANSSI recrute

Les documents du CERT-FR
Publications récentes
Les alertes en cours
Les bulletins d'actualité
Les notes d'information
Année en cours

Les Flux RSS du CERT-FR
Flux RSS complet
Flux RSS des alertes
Flux RSS SCADA

À propos du CERT-FR
Le CERT-FR
Nous contacter
Contact us ( )
A propos du site

Communauté CSIRT
Les CSIRT
Le FIRST
L'EGC

Archives du CERT-FR
Année 2016
Année 2015
Année 2014
Année 2013
Année 2012
Année 2011
Année 2010
Année 2009
Année 2008
Année 2007
Année 2006
Année 2005
Année 2004

Actualités

Protéger son site Internet des cyberattaques

Alertes (les 5 plus récentes)

Les alertes sont des documents destinés à prévenir d'un danger immédiat.

CERTFR-2016-ALE-007 Vulnérabilité dans Cisco IOS, IOS XE et IOS XR (19 septembre 2016)
CERTFR-2016-ALE-005 Multiples vulnérabilités dans les pare-feux Cisco (Corrigée le 05 septembre 2016)
CERTFR-2016-ALE-006 Campagne de messages électroniques non sollicités de type Zepto/Odin (05 septembre 2016)
CERTFR-2015-ALE-013 Vulnérabilité dans Joomla! (Corrigée le 01 août 2016)
CERTFR-2016-ALE-004 Vulnérabilité dans Adobe Flash Player (Corrigée le 15 juin 2016)

Avis (les 20 plus récents)

Les avis sont des documents faisant état de vulnérabilités et des moyens de s'en prémunir.

CERTFR-2016-AVI-347 Multiples vulnérabilités dans les produits Siemens (13 octobre 2016)
CERTFR-2016-AVI-346 Multiples vulnérabilités dans Apache OpenOffice (13 octobre 2016)
CERTFR-2016-AVI-345 Multiples vulnérabilités dans Google Chrome (13 octobre 2016)
CERTFR-2016-AVI-344 Multiples vulnérabilités dans les produits Juniper (13 octobre 2016)
CERTFR-2016-AVI-343 Multiples vulnérabilités dans les produits Cisco (12 octobre 2016)
CERTFR-2016-AVI-342 Multiples vulnérabilités dans Ghostscript (12 octobre 2016)
CERTFR-2016-AVI-341 Multiples vulnérabilités dans le smartphone P9 Huawei (12 octobre 2016)
CERTFR-2016-AVI-340 Multiples vulnérabilités dans Microsoft Windows (12 octobre 2016)
CERTFR-2016-AVI-339 Vulnérabilité dans Microsoft Office (12 octobre 2016)
CERTFR-2016-AVI-338 Multiples vulnérabilités dans Microsoft Edge (12 octobre 2016)
CERTFR-2016-AVI-337 Multiples vulnérabilités dans Microsoft Internet Explorer (12 octobre 2016)
CERTFR-2016-AVI-336 Multiples vulnérabilités dans Adobe Flash Player (11 octobre 2016)
CERTFR-2016-AVI-335 Vulnérabilité dans Quagga (11 octobre 2016)
CERTFR-2016-AVI-334 Multiples vulnérabilités dans le noyau Linux d'Ubuntu (11 octobre 2016)
CERTFR-2016-AVI-333 Multiples vulnérabilités dans les produits BlueCoat (07 octobre 2016)
CERTFR-2016-AVI-332 Vulnérabilité dans Citrix License Server (06 octobre 2016)
CERTFR-2016-AVI-331 Multiples vulnérabilités dans les produits Cisco (06 octobre 2016)
CERTFR-2016-AVI-330 Vulnérabilité dans les produits F5 (05 octobre 2016)
CERTFR-2016-AVI-329 Multiples vulnérabilités dans le noyau Linux de Red Hat (05 octobre 2016)
CERTFR-2016-AVI-328 Vulnérabilité dans Xen (05 octobre 2016)

Bulletins d'actualité (les 5 plus récents)

Les bulletins d'actualité fournissent une illustration par l'actualité récente de certaines mesures pragmatiques à appliquer.

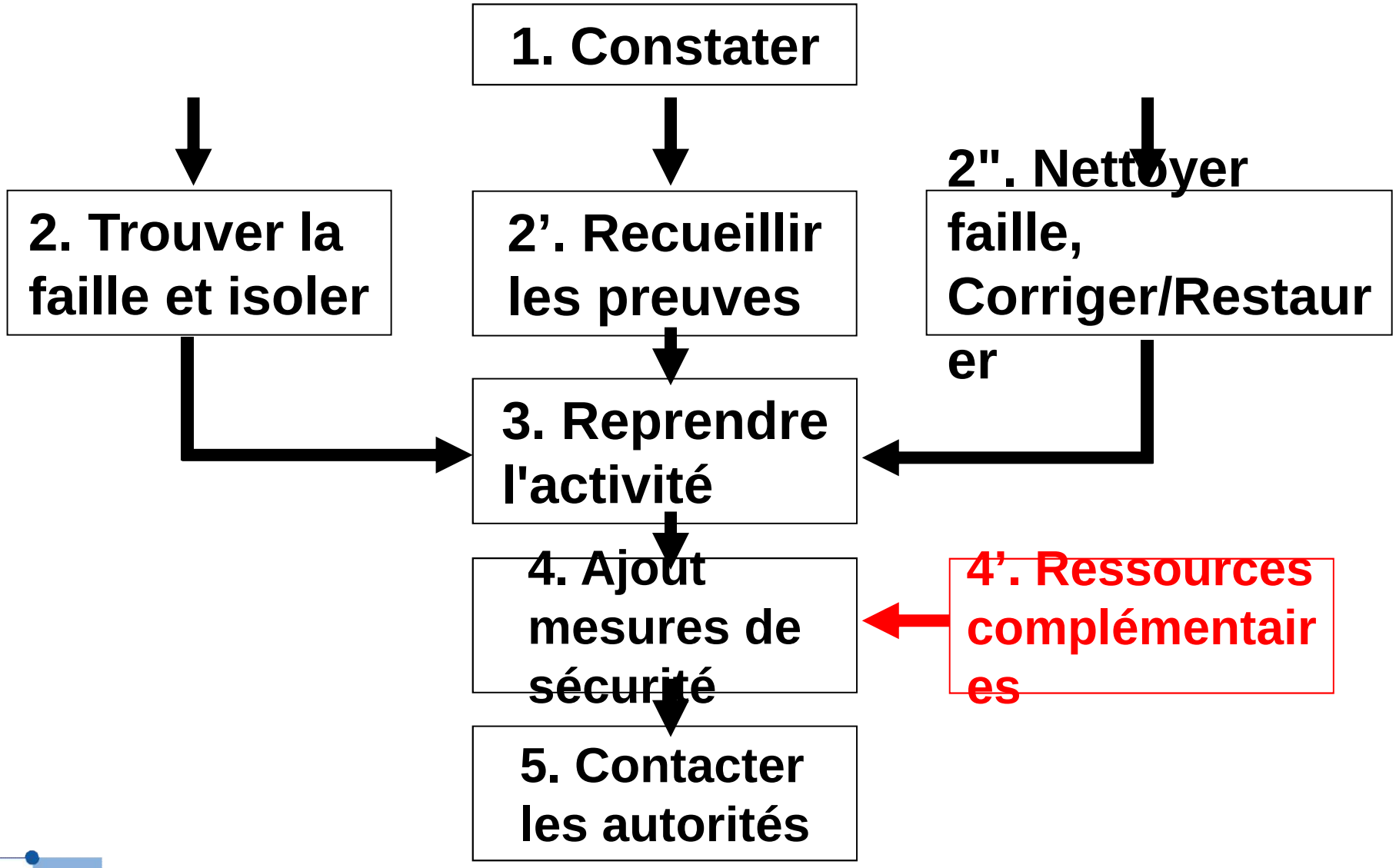
CERTFR-2016-ACT-041 Bulletin d'actualité numéro 041 de l'année 2016 (10 octobre 2016)
CERTFR-2016-ACT-040 Bulletin d'actualité numéro 040 de l'année 2016 (03 octobre 2016)
CERTFR-2016-ACT-039 Bulletin d'actualité numéro 039 de l'année 2016 (26 septembre 2016)
CERTFR-2016-ACT-038 Bulletin d'actualité numéro 038 de l'année 2016 (19 septembre 2016)
CERTFR-2016-ACT-037 Bulletin d'actualité numéro 037 de l'année 2016 (12 septembre 2016)

Notes d'information (les 5 plus récentes)

Les notes d'information font état de phénomènes à portée générale.

CERTFR-2015-INF-001 DNS Rebinding (15 juin 2015)
CERTA-2005-INF-003 Les systèmes et logiciels obsolètes (18 novembre 2014)
CERTA-2012-INF-001 Déni de service - Prévention et réaction (14 janvier 2013)

Les RansomWares – Que faire en cas d'attaque



Les RansomWares – Que faire en cas d'attaque

4'. Ressources complémentaires

- **ANSSI - www.ssi.gouv.fr**

  Agence Nationale de la Sécurité des Systèmes d'Information

  (pour les OIV = Opérateurs d'Importance Vitale)

- **CERT-FR - www.cert.ssi.gouv.fr**

  Computer Emergency Response Team

  Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. Il diffuse les bons réflexes en cas d'intrusion sur un système d'information.

- **FIRST - www.cert.ssi.gouv.fr**

  Forum of Incident Response and Security Teams

  Organisation internationale qui regroupe plus d'une centaine de CERTs

Les RansomWares – Que faire en cas d'attaque

4'. Ressources complémentaires

- **Article 40 du CPP**

  Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs.

Les RansomWares – Que faire en cas d'attaque

4'. Ressources complémentaires

- **Article 47 de la Loi pour une République numérique n° 2016-1321 du 7 octobre 2016**

Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.

« L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée.

« L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le

MERCI POUR VOTRE

ATTENTION !

DES QUESTIONS ?

Denis JACOPINI

d.jacopini@leNetExpert.fr

06 19 71 79 12

LES INTRUSIONS – MODIF ET SUPPRESSION DE DONNÉES

https://a6764.boutique-eset.com/