

Cybersécurité et propriété intellectuelle

AMAN VLADIMIR

Analyste Sécurité des Systèmes d'Information

ISO 27001 Lead Implementer



AGENDA

- Introduction
- Enjeux de la protection de la propriété intellectuelle
- Panorama des menaces de SSI
- Protéger la propriété intellectuelles: des solutions?
- Cybersécurité: les réponses de l'ARTCI
- Conclusion

Introduction

Contexte

- Avec la vulgarisation du web 2.0 couplée à l'apparition du haut débit et la pénétration du large bande, la dernière décennie a été marquée par une forte accélération de l'innovation technologique, des échanges en ligne et partant des cybermenaces.
- Ces mutations de l'écosystème Internet favorisent l'émergence de nouveaux marchés de contenus pour les personnes physiques et morales portant ces innovations technologiques.
- Cependant de nouvelles menaces liées aux droits des propriétaires de créations originales se multiplient et posent par ricochet la problématique du frein de la croissance de l'économie numérique
- Dans un tel contexte, cybersécurité et protection des droits de propriété intellectuelle se retrouvent corrélativement liés
- En effet, les réseaux P2P, newsgroup, torrents, streaming, autres services du web 2.0, sont des sujets de préoccupation de plus en plus croissants.

Introduction

Définitions: « cybersécurité »



Selon la recommandation de l'UIT–T X.1205

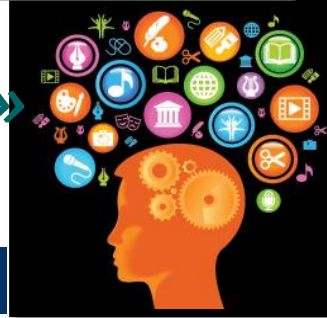
« On entend par cybersécurité l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. [...] »

Les objectifs généraux en matière de sécurité sont les suivants :

- **Disponibilité;**
- **Intégrité**, qui peut englober l'**authenticité** et la **non-répudiation**;
- **Confidentialité.»**

Introduction

Définitions: « propriété intellectuelle »



Aux termes de l'article 2 de la Convention dite de Stockholm du 14 juillet 1967 créant l'organisation mondiale de la propriété intellectuelle (OMPI).

On entend par propriété intellectuelle « les droits relatifs : aux œuvres littéraires, artistiques et scientifiques; aux interprétations des artistes-interprètes et aux exécutions des artistes exécutants, aux phonogrammes et aux émissions de radiodiffusion ; aux inventions dans tous les domaines de l'activité humaine ; aux découvertes scientifiques, aux dessins et modèles industriels ; aux marques de fabrique, de commerce et de service, ainsi qu'aux noms commerciaux et dénominations commerciales; à la protection de la concurrence déloyale et de tous les autres droits afférents à l'activité intellectuelle dans les domaines industriel, scientifique, littéraire et artistique »

Enjeux de la protection de la propriété intellectuelle

Quelques faits

- Le piratage numérique représentait quelque 75 milliards USD en 2008, chiffre qui devrait atteindre 215 milliards USD d'ici à 2015 (*Frontier Economics*)
- 2 millions de téléchargements illégaux de la série « Lost » en 2010
- Entre 17 et 40 milliards USD en 2008, valeurs commerciales globales du piratage de données musicales (*Frontier Economics pour la Chambre de commerce internationale*)
- **24 583** utilisateurs de BitTorrent, principalement localisés aux Etats-Unis, auraient illégalement téléchargé le film «Démineurs», (*Voltage Pictures*)
- **50%** des ménages ont déjà téléchargé illicitement des œuvres cinématographiques, pour un préjudice de 1 milliard USD (*Conseil Coréen du Film*)

• Source: UIT

Enjeux de la protection de la propriété intellectuelle

Quelques faits

- De janvier à juin 2011, les violations de droits d'auteur en ligne ont concerné **31 000 titres**, diffusés sur plus de **80 000** pages web (**Publisher Association**)
- **7,5 millions** de notifications de retrait à l'intention de sites de partage P2P coupables de distribution illégale de logiciels en 2009.
- Le piratage représente près de **40%** du marché mondial (**Business Software alliance**)
- **2696** plaintes pour cybersquattage concernant 4370 noms de domaine et 57 pays auprès du Centre d'arbitrage et de médiation de l'OMPI
- **20 000** plaintes ont été déposées à l'OMPI concernant **35 000** noms de domaine (depuis 1999)
- 8 milliards de francs CFA, préjudice du piratage informatique en Côte d'Ivoire (**Microsoft Côte d'Ivoire**)

Enjeux de la protection de la propriété intellectuelle

- Assurer le progrès technique et social



- Assurer la confiance numérique



- Promouvoir l'innovation



Panorama des menaces de SSI

Quelques chiffres en Côte d'Ivoire

	2009	2010	2011	2012	2013
Phishing		38	29	134	79
Defacement de site web		101	55	6	38
Déni de service		104	47		
Botnet		55	10	347	309
Web-based attack		46	15		
XSS			12	62	108
SPAM				221	83
Scan				1020	
Malware infection				203	242
Vol de données					25
Fraude à la SIMBOX					6
Total		344	168	1993	890

Panorama des menaces de SSI

Ransomware ou rançongiciels

- Logiciels malveillants
- Cryptage de l'ensemble des données se trouvant sur la machine infectée
- Paiement d'une rançon réclamé contre le décryptage des données et le **retour à la normal**.
- Objectifs:
 - Gain financier



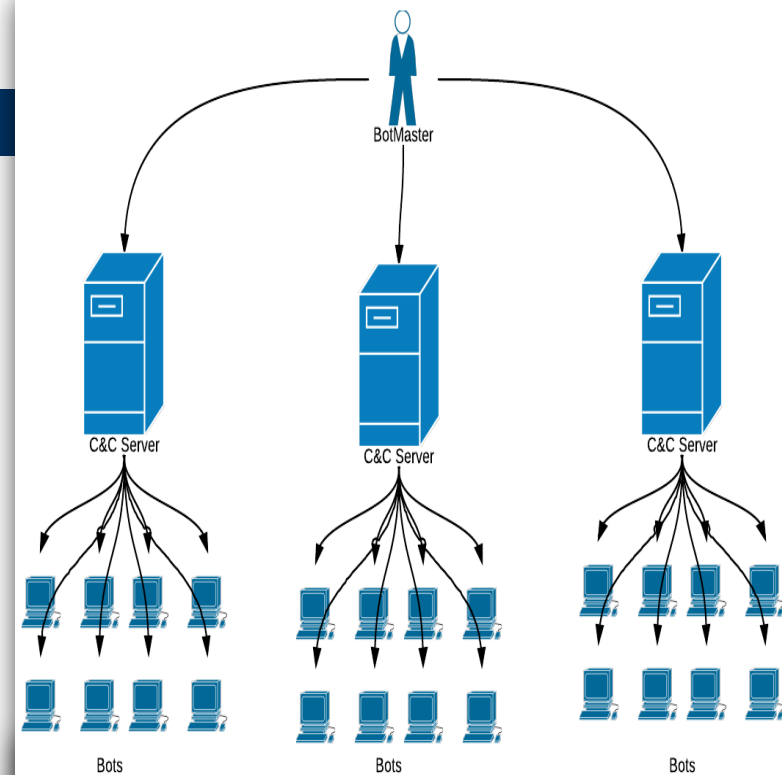
Panorama des menaces de SSI

Botnets

- Réseaux de machines zombies (bot)
- Contrôlés par des serveurs C&C qui sont contrôlés à distance
- Attaques informatiques massives (DDoS, spam, etc.) contre d'autres systèmes d'informations.

- **Objectifs:**

- Chantage
- Location ou vente
- Vol et revente d'informations
- Distribution d'adware et de malware, Spam



Panorama des menaces de SSI

Phishing, Spear Phishing

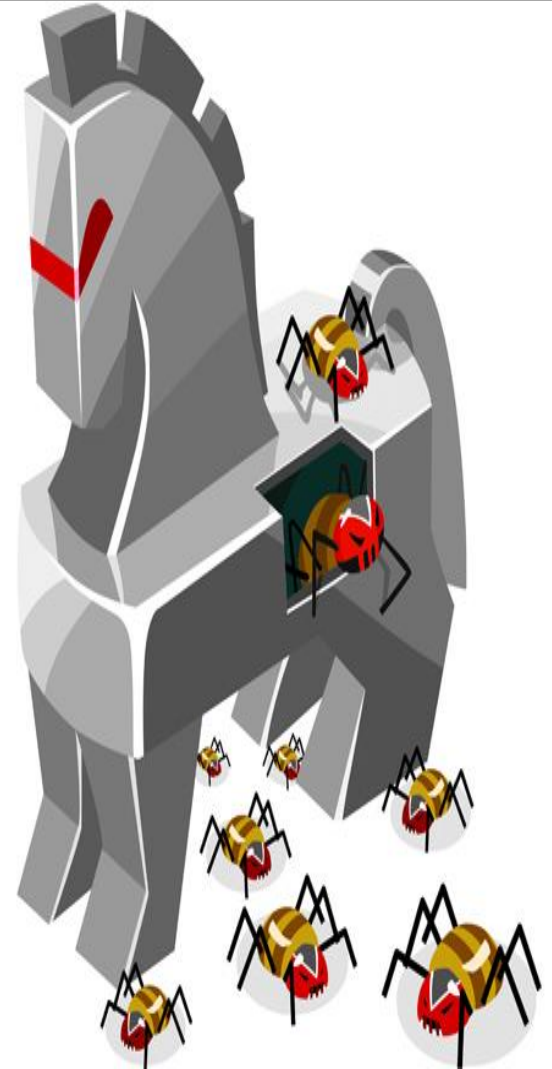
- Technique dite de l'hameçonnage
 - Usurpation de l'identité d'une personne physique ou morale dans le but de soutirer des informations personnelles ou sensibles à sa victime.
 - Le spear phishing est une variante de phishing qui est ciblée et très précise.
- Objectifs:
 - Obtenir de l'information sensible
 - Accéder à des systèmes d'information en vue de réaliser des actions malveillantes plus graves



Panorama des menaces de SSI

Chevaux de Troie, RAT

- Logiciels malveillants de prise de contrôle à distance;
- Apparence inoffensive contenant une charge virale importante
- **Objectifs:**
 - Intrusion dans les systèmes d'information
 - Vol de données
 - Espionnage
 - Etc.



Panorama des menaces de SSI

0-Day

- Les failles dont l'existence n'est pas rendue publique
- même pas du fabricant du produit impacté dans la majorité des cas;
- Aucun patch de sécurité disponible;
- Porte grande ouverte dans le système d'information



Panorama des menaces de SSI

APT (Advanced Persistent Threat)

- Menaces persistantes avancées
- L'attaquant va **s'introduire** dans un système, étudier les mécanismes **de défense internes**, **copier** l'information, **exfiltrer** les données.
- Rester indétectable sur une longue période
- **Objectifs:**
 - Espionnage
 - Vol d'informations

Advanced Persistent Threat (APT): The Uninvited Guest

How attackers remain in your network harvesting information and avoiding detection over time

1. INCURSION

Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

2. DISCOVERY

Once in, the attackers stay "low and slow" to avoid detection. They then map the organization's defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

3. CAPTURE

Attackers access unprotected systems and capture information over an extended period. They may also install malware to secretly acquire data or disrupt operations.

4. EXFILTRATION

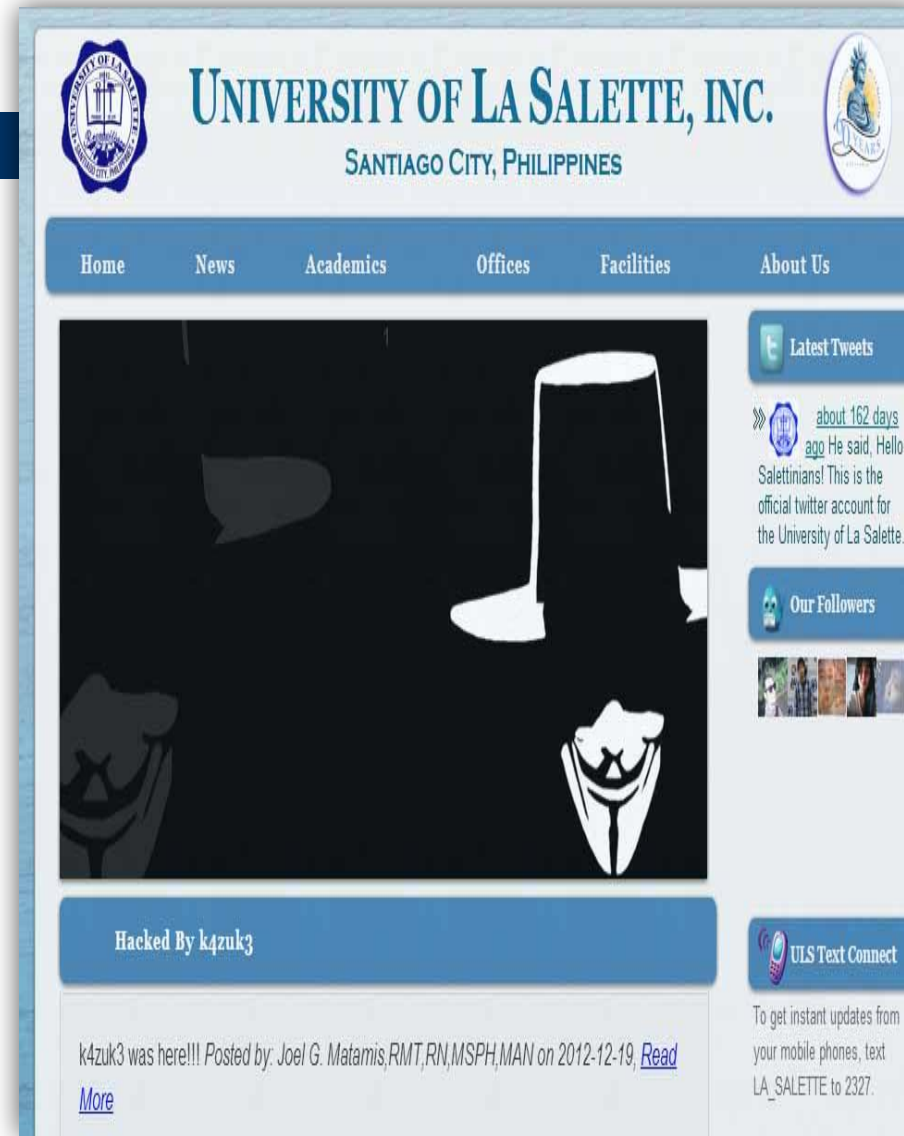
Captured information is sent back to attack team's home base for analysis and further exploitation fraud—or worse.



Panorama des menaces de SSI

Website defacement

- Intrusion dans le site
 - Exploitant une vulnérabilité
 - Remplacement de la page « index »
 - Publication de contenus propagandistes, injurieux, dégradant, etc.
-
- **Objectifs:**
 - Sabotage
 - Atteinte à l'image d'une marque, d'une personne



Panorama des menaces de SSI

Cybersquatting



Est une pratique qui consiste à enregistrer un nom de domaine désignant une marque ou une entreprise dans le but de nuire à cette dernière ou d'en tirer un profit illicitement.

- **Objectifs:**

- Capter du trafic internet naturel destiné initialement à la société lésée
- Générer des revenus publicitaires via des pages de liens sponsorisées appelées « **page parking** »
- Revendre le nom de domaine au plus offrant
- Commercialiser des produits similaires et / ou concurrents à la marque détournée
- Détourner des mails à destination de l'entreprise (« mailsquatting »)

Protéger la propriété intellectuelle

Les solutions technologiques

- Pas de solution technologique unique pour protéger la propriété intellectuelle
- La sécurité organisationnelle, ainsi que « **I'HOMME** » sont à mettre au cœur des stratégies de sécurité
- Il faut mettre en place des stratégies intégrées dès la conception du contenu pour:
 - Identifier la propriété et la source :
 - Protéger en assurant la sécurité, l'intégrité et la traçabilité
 - Prévenir les fuites de données

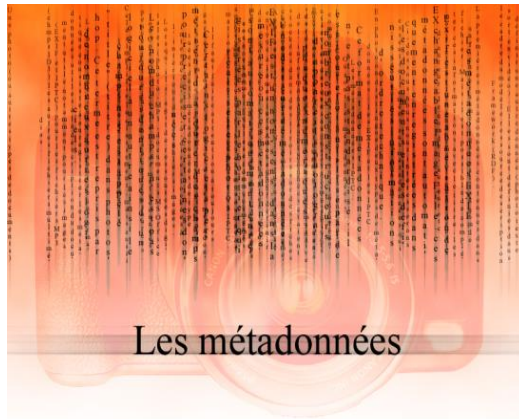


Protéger la propriété intellectuelle

Les solutions technologiques

- **Identifier la propriété et la source**

- **Les métadonnées**



- **Le watermarking**



- **Les empreintes numériques**



Protéger la propriété intellectuelle

Les solutions technologiques

- **Protéger en assurant la sécurité, l'intégrité et la traçabilité:**

- **Streaming protégé**



- **Digital Right Management (DRM)**



Protéger la propriété intellectuelle

Les solutions organisationnelles

- **Prévenir les fuites de données**

- Mettre en place un SMSI (ISO 2700x)
- Intégrer la composante sécurité dès la création des contenus
- Se doter d'équipes de sécurité (CSIRT)
- Investir dans la formation et spécialisation d'experts en sécurité de l'information
- Etablir des liens de coopération étroits avec le CERT National (**CI-CERT**) ou des réseaux de CERTs sectoriels

Le cadre juridique

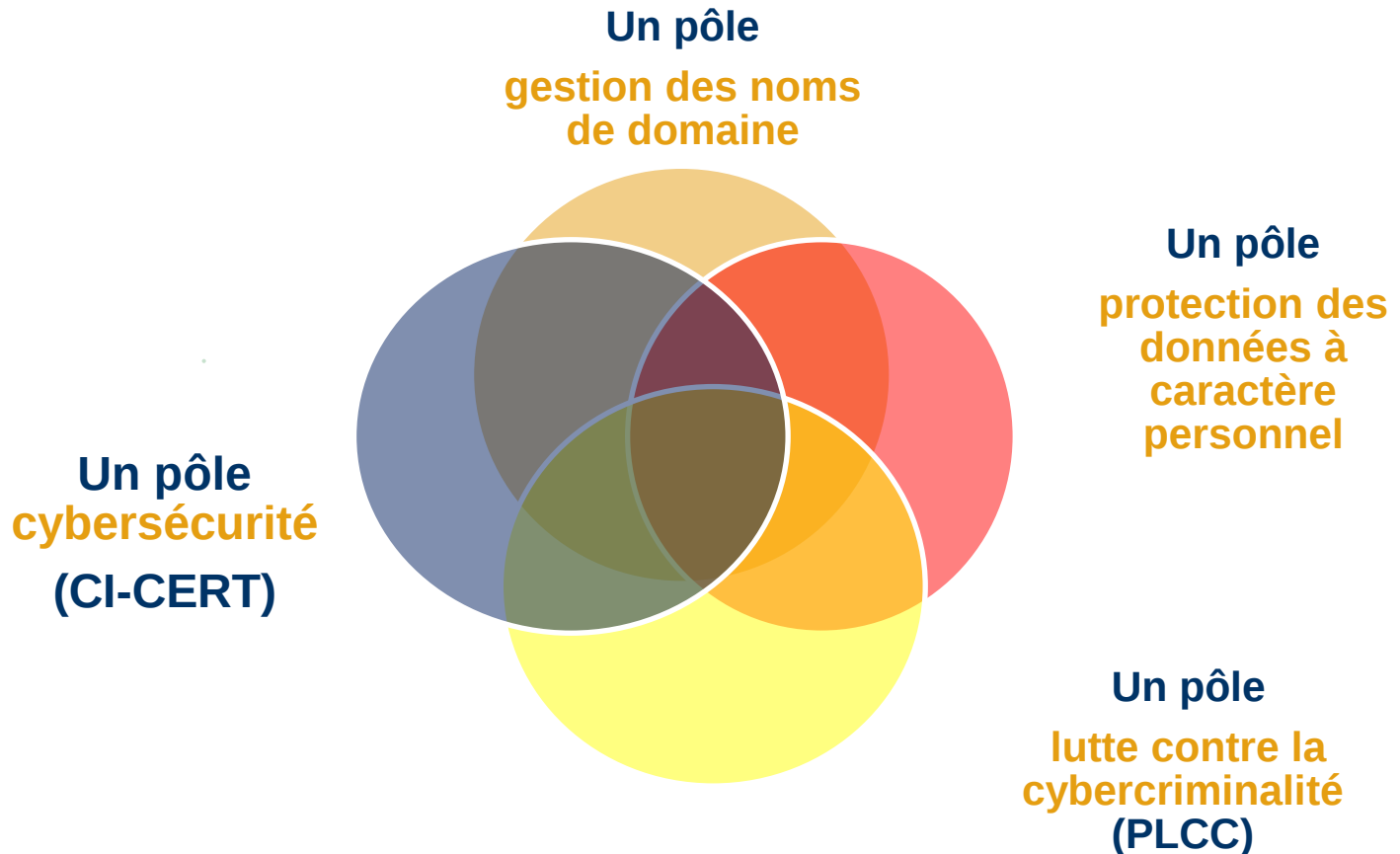
Au plan juridique



- Loi N°2013-450 → **DCP**
- Loi N°2013-451 → **Cybercriminalité**
- Loi N°2013-546 → **Transactions électroniques**

Cybersécurité: les réponses de l'ARTCI

Au plan stratégique: 4 axes



Cybersécurité: les réponses de l'ARTCI

Projet: « Cybersécurité et sécurité des Réseaux et SI »



Etat des lieux de la Cybersécurité et la sécurité des réseaux en Côte d'Ivoire



Mise en place d'un référentiel pour l'accréditation de prestataires d'audit de sécurité des entreprises en vue de la certification



Infrastructures pour la lutte contre la cybercriminalité



Plan de continuité national des SI et réseaux nationaux



Stratégie nationale de Cybersécurité



Sécurité des infrastructures critiques nationales



Renforcement de la communication sur la Cybersécurité en Côte d'Ivoire

Conclusion

- La croissance de l'économie numérique nationale nécessite la mise en place d'un environnement propice à la créativité, l'innovation et qui favorise la compétitivité et la concurrence, le tout en exploitant le potentiel de transformation des technologies numériques;
- Les menaces SSI se multiplient et gagnent en complexité avec le développement de l'interconnexion et la dépendance aux TIC. Il faut accepter de vivre dans un environnement numérique substantiellement vulnérable et dans lequel la sécurité y est relativement fragile.
- Protéger la P.I réside dans la mise en œuvre judicieuse de moyens technologiques (DRM, streaming protégé, Watermarking, etc.) et de mesures organisationnelles (SMSI selon ISO27k1, Formation, Coopération avec les CERT, etc.).
- Dans sa mission de sécurisation de l'environnement numérique Ivoirien, l'ARTCI entend mettre un focus particulier sur la protection de la P.I, par la réalisation des sous-projets: *Mise en place d'un référentiel pour l'accréditation de prestataires d'audit de sécurité des entreprises en vue de la certification et mise en place d'Infrastructures pour la lutte contre la cybercriminalité*

Je vous remercie!!!

- Références bibliographiques

- <https://itunews.itu.int/fr/1707-Les-droits-de-propriete-intellectuelle-dans-leconomie-numerique-daujourdhui.note.aspx>
- http://www.indicare.org/tiki-download_file.php?fileId=196