VEILLE TECHNOLOGIQUE

Cybersécurité et Ransomwares

■ Menaces • Actualités • Solutions • Prévention

Formation	BTS SIO Option SISR - 2ème année
Thème	Cybersécurité et Ransomwares
Période	2024 - 2025
Objectif	Comprendre les menaces et solutions de protection

SOMMAIRE

1. INTRODUCTION : POURQUOI CETTE VEILLE ?

1.1 Contexte

En tant que futur technicien réseau et système, la **cybersécurité** est au cœur de mon métier. Les ransomwares (rançongiciels) représentent aujourd'hui la **menace n°1** pour les entreprises et les organisations.

Cette veille technologique me permet de :

- Comprendre les **menaces actuelles** et leur évolution
- Connaître les **techniques d'attaque** pour mieux s'en protéger
- Identifier les **solutions de protection** à mettre en place
- Rester informé des **actualités** du secteur

1.2 Pertinence pour le BTS SIO SISR

Cette veille s'inscrit directement dans les compétences du référentiel BTS SIO option SISR : administration des systèmes, sécurisation des infrastructures, gestion des incidents et continuité de service.

2. QU'EST-CE QU'UN RANSOMWARE ?

2.1 Définition

Un **ransomware** (ou rançongiciel) est un logiciel malveillant qui **chiffre les données** d'une victime et exige le paiement d'une **rançon** pour fournir la clé de déchiffrement.

2.2 Fonctionnement

1. **Infection** : Le malware pénètre le système (phishing, faille, RDP...)
2. **Propagation** : Il se répand sur le réseau interne
3. **Chiffrement** : Les fichiers sont chiffrés et inaccessibles
4. **Rançon** : Une demande de paiement (souvent en Bitcoin) est affichée
5. **Double extorsion** : Menace de publication des données volées

2.3 Modèle économique : RaaS

Les groupes criminels proposent du **Ransomware-as-a-Service (RaaS)** : ils fournissent l'outil à des "affiliés" qui mènent les attaques, en échange d'un pourcentage des rançons (généralement 20-30%).

3. LES PRINCIPAUX GROUPES DE RANSOMWARE

Groupe	Origine	Spécificité	Victimes notables
LockBit	Russie	Le plus actif (27% des attaques en France)	Hôpitaux, Thales, Boeing
BlackCat/ALPHV	Russie	Double extorsion systématique	Entreprises tech
Cl0p	Russie/Ukraine	Attaques supply chain (MOVEit)	Centaines d'entreprises
RansomHub	International	Nouveau groupe en forte croissance	PME/ETI
8Base	International	Cible les PME	Entreprises françaises
Black Basta	Russie	Affiliés ex-Conti	Industrie, santé

3.1 Focus sur LockBit

LockBit est considéré comme le groupe de ransomware **le plus prolifique et dangereux au monde** selon Europol. Depuis 2020, il a réalisé plus de **2 500 attaques** et extorqué plus d'**1 milliard de dollars**.

En France, LockBit est responsable de **27% des demandes de rançon** et a notamment attaqué l'hôpital de Corbeil-Essonnes (2022) et l'hôpital de Cannes (2024).

4. CHIFFRES CLÉS 2024-2025

4.1 En France

- **74% des organisations françaises ciblées par un ransomware en 2024 (Sophos)**
- **La France = pays avec le plus fort taux d'attaques ransomware en 2024**
- **144 compromissions par ransomware signalées à l'ANSSI en 2024**
- **4 386 événements de sécurité traités par l'ANSSI (+15% vs 2023)**
- **PME et ETI = 61,7% des victimes**

4.2 Dans le monde

- **75% des brèches "intrusion système" liées aux ransomwares (Verizon 2025)**
- **24% des organisations touchées par un ransomware en 2025 (+5,4% vs 2024)**
- **60% des brèches impliquent le facteur humain (phishing, erreurs)**
- **Coût moyen d'une attaque : > 500 000 € (hors rançon)**

4.3 Secteurs les plus touchés

Secteur	% d'attaques	Raison
Santé / Hôpitaux	11,4%	Données sensibles, systèmes critiques
Collectivités	10%	Budgets limités, SI vieillissants
PME / ETI	36,2%	Moins de ressources cyber
Industrie	15%	OT/IT convergence, supply chain

5. ACTUALITÉS MARQUANTES EN FRANCE (2024)

5.1 Hôpital d'Armentières (Février 2024)

Dans la nuit du 10 au 11 février 2024, le centre hospitalier d'Armentières (Nord) a été victime d'une attaque ransomware par le groupe **Blackout**. Les urgences ont été fermées pendant 24h et **950 000 données patients** ont été publiées après refus de payer la rançon.

5.2 Hôpital de Cannes (Avril 2024)

Le 16 avril 2024, l'hôpital Simone-Veil de Cannes a été attaqué par **LockBit**. L'établissement a refusé de payer et **61 Go de données** (patients, personnel) ont été publiés sur le dark web. Les opérations non urgentes ont été reportées pendant plusieurs jours.

5.3 CHU de Nantes (Janvier 2024)

Le CHU de Nantes a été victime d'une cyberattaque bloquant Internet, les emails et l'accès externe (Doctolib). L'établissement, préparé, a réussi à contenir l'attaque et préserver le système de soins.

5.4 Autres victimes notables

- **Auchan** : fuite de données de centaines de milliers de clients fidélité
- **Norauto** : cyberattaque avec vol de données clients
- **Schneider Electric** : attaqué par le groupe Hellcat

6. L'OPÉRATION CRONOS CONTRE LOCKBIT

6.1 Une opération internationale historique

Le **20 février 2024**, une coalition de 11 pays (France, USA, UK, Allemagne, Pays-Bas, Australie, Canada, Japon, Suisse, Suède, Finlande) coordonnée par Europol et la NCA britannique a mené l'**Opération Cronos** contre LockBit.

6.2 Résultats de l'opération

- **34 serveurs** saisis dans plusieurs pays
- **200+ comptes crypto** gelés
- **1 000+ clés de déchiffrement** récupérées
- **14 000 comptes** utilisés pour les opérations fermés
- Site vitrine LockBit pris en contrôle par les forces de l'ordre
- Deux suspects arrêtés (Pologne, Ukraine)
- Identité du leader **Dmitry Khoroshev** (alias LockBitSupp) révélée

6.3 Participation française

La **Gendarmerie nationale** (Unité Nationale Cyber - C3N) a joué un rôle clé dans cette opération, enquêtant depuis 2020. Un développeur présumé a été arrêté en France.

6.4 Et après ?

Malgré le démantèlement, LockBit a **relancé ses activités** quelques jours plus tard avec un nouveau site. En 2025, **LockBit 5.0** est apparu avec des capacités renforcées. La lutte continue.

7. MÉTHODES D'ATTAQUE

7.1 Vecteurs d'intrusion principaux

Méthode	% des attaques	Description
Exploitation de vulnérabilités	32%	Failles non corrigées (VPN, pare-feu, serveurs)
Phishing / Hameçonnage	29%	Emails piégés avec pièces jointes ou liens malveillants
Identifiants compromis	23%	Mots de passe volés ou faibles (RDP exposé)
Attaques supply chain	10%	Compromission d'un fournisseur (ex: MOVEit)

7.2 La double extorsion

Les attaquants ne se contentent plus de chiffrer : ils **volent les données** avant de chiffrer, puis menacent de les publier si la rançon n'est pas payée. En 2024, **47% des victimes** ont reçu des menaces de signalement aux autorités.

7.3 Nouvelles tendances 2025

- **IA générative** : phishing plus réaliste, code malveillant auto-généré
- **Ciblage des équipements de bordure** : VPN, pare-feu, passerelles
- **Ransomware multiplateformes** : Windows, Linux, ESXi (virtualisation)

8. SOLUTIONS DE PROTECTION

8.1 Mesures techniques

- **Sauvegardes 3-2-1** : 3 copies, 2 supports différents, 1 hors-site (immuables)
- **Mises à jour** : Patcher rapidement les vulnérabilités (VPN, serveurs...)
- **Segmentation réseau** : Isoler les systèmes critiques (VLANs)
- **MFA** : Authentification multi-facteurs sur tous les accès
- **EDR/XDR** : Solutions de détection et réponse aux menaces
- **Filtrage email** : Anti-spam, anti-phishing, sandboxing

8.2 Mesures organisationnelles

- **Sensibilisation** : Former les utilisateurs au phishing
- **Plan de réponse aux incidents** : Procédures documentées
- **Tests de restauration** : Vérifier que les sauvegardes fonctionnent
- **Assurance cyber** : Couvrir les coûts d'une attaque
- **Veille sécurité** : Suivre les alertes ANSSI/CERT

8.3 En cas d'attaque : NE PAS PAYER

L'ANSSI et les autorités recommandent de **ne jamais payer la rançon** : cela finance les criminels et ne garantit pas la récupération des données. En France, les hôpitaux publics ne paient jamais.

9. MES SOURCES DE VEILLE

9.1 Sites officiels

Source	URL	Type
ANSSI	cyber.gouv.fr	Alertes, recommandations
CERT-FR	cert.ssi.gouv.fr	Bulletins de sécurité
Cybermalveillance.gouv.fr	cybermalveillance.gouv.fr	Assistance, prévention
ENISA	enisa.europa.eu	Rapports européens

9.2 Médias spécialisés

- **LeMagIT** (lemagit.fr) - Actualités cybersécurité France
- **Zataz** (zataz.com) - Actualités cybercriminalité
- **SOS Ransomware** (sosransomware.com) - Statistiques et analyses
- **Bleeping Computer** (bleepingcomputer.com) - Actualités mondiales

9.3 Outils de veille

- **Feedly** : Agrégateur de flux RSS
- **Google Alerts** : Alertes sur mots-clés
- **Twitter/X** : Comptes @ABORLA, @ANSSI, @CERT_FR
- **LinkedIn** : Publications experts cybersécurité

10. LIEN AVEC LE BTS SIO SISR

10.1 Compétences mobilisées

Bloc	Compétence	Application
B1	Gérer le patrimoine informatique	Inventaire, sauvegardes, mises à jour
B2	Répondre aux incidents	Détection, réponse aux cyberattaques
B3	Développer la présence en ligne	Sécurisation des services exposés
B3	Mettre à disposition un service	Continuité de service, PRA/PCA

10.2 Application dans mes projets

Cette veille m'a permis de mieux comprendre l'importance de :

- La **segmentation réseau** (VLANs) pour limiter la propagation
- Les **sauvegardes régulières** et leur test de restauration
- La **mise à jour des systèmes** (Apache, Windows Server...)
- Le **monitoring** avec des outils comme Nagios, Wazuh, Snort
- La **sensibilisation des utilisateurs** au phishing

10.3 Conclusion

Les ransomwares représentent une menace majeure et en constante évolution. Cette veille technologique m'a permis de comprendre les enjeux, les techniques d'attaque et les solutions de protection. En tant que futur administrateur système et réseau, je suis maintenant mieux armé pour **sécuriser les infrastructures** et **répondre aux incidents**.