AYI NEDJIMI Consultants

Livre Blanc Détaillé : Guide Pratique Cybersecurite

Catégorie : Livres Blancs Lecture : 9 min Publié le : 07/12/2025 Auteur : Ayi NEDJIMI

Un guide complet et détaillé pour 2025 pour comprendre le fonctionnement des attaques par ransomware en suivant le framework MITRE ATT&CK, et pour.

Livre Blanc

Ransomware : Anatomie d'une Attaque et Stratégies de Défense (Édition 2025)

Les ransomwares ne sont plus de simples malwares, mais des opérations cybercriminelles complexes, menées par des groupes organisés (les "affiliés") utilisant des plateformes "Ransomware-as-a-Service" (RaaS). Comprendre leur cycle de vie, souvent modélisé par le framework MITRE ATT&CK, est la première étape pour construire une défense en profondeur. Un guide complet et détaillé pour 2025 pour comprendre le fonctionnement des attaques par ransomware en suivant le framework MITRE ATT&CK, et pour. Ce guide technique sur livre blanc anatomie attaque ransomware s'appuie sur des retours d'expérience terrain et des méthodologies éprouvées en environnement de production. Nous abordons notamment : ransomware : anatomie d'une attaque et stratégies de défense (édition 2025), chapitre 1 : qu'est-ce qu'un ransomware en 2025 ? et chapitre 2 : les groupes les plus actifs (tendances 2024-2025). Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

Comment mesurez-vous concrètement l'efficacité de votre programme de sécurité ?

Chapitre 1 : Qu'est-ce qu'un Ransomware en 2025 ?

Un ransomware, ou rançongiciel, est un logiciel malveillant qui prend en otage les données d'une victime. Historiquement, cela se limitait au chiffrement des fichiers, les rendant inaccessibles jusqu'au paiement d'une rançon. Aujourd'hui, le modèle a évolué vers une **multi-extorsion** :

1. **Exfiltration de données :** Avant de chiffrer, les attaquants volent des copies de vos données les plus sensibles.
2. **Chiffrement :** Ils chiffrent ensuite vos systèmes pour paralyser vos opérations.
3. **Menace de publication :** Si vous refusez de payer (par exemple, parce que vous avez des sauvegardes), ils menacent de publier les données volées sur leur site vitrine sur le dark web.
4. **Attaques DDoS :** Certains groupes ajoutent une couche de pression en menant des attaques par déni de service (DDoS) contre votre infrastructure exposée sur Internet.

Le modèle économique : Ransomware-as-a-Service (RaaS)

La prolifération des ransomwares est due au modèle RaaS. Il fonctionne comme un logiciel en franchise :

- **Les Opérateurs :** Un groupe de développeurs experts crée et maintient le ransomware, le site de paiement, et le site de fuite de données.
- **Les Affiliés :** Des groupes d'attaquants "louent" l'infrastructure du RaaS. Ce sont eux qui mènent les attaques pour obtenir l'accès initial et déployer le ransomware. Les profits de la rançon sont ensuite partagés, généralement 70-80% pour l'affilié et 20-30% pour l'opérateur.

Ce modèle a abaissé la barrière à l'entrée, permettant à des acteurs moins qualifiés de mener des attaques critiques.

Chapitre 2 : Les Groupes les Plus Actifs (Tendances 2024-2025)

Le paysage des ransomwares est en constante évolution, avec des groupes qui apparaissent et disparaissent. Cependant, quelques acteurs majeurs dominent la scène.

Part de marché estimée des attaques par ransomware (2024-2025)

LockBit 3.0
35%
ALPHV/BlackCat
25%
Cl0p
18%
Play
12%
Autres
10%

Description des principaux variants

- **LockBit 3.0 :** Le groupe le plus prolifique. Connu pour son ransomware rapide et efficace, et pour son programme de "bug bounty" qui récompense les chercheurs trouvant des failles dans leur propre logiciel. Ils utilisent souvent des identifiants valides achetés pour l'accès initial.
- **ALPHV/BlackCat :** Le premier ransomware majeur écrit en Rust, ce qui le rend plus difficile à analyser. Ils sont connus pour leurs tactiques de triple extorsion et pour la publication de données volées de manière très organisée et consultable.
- **Cl0p :** Spécialistes de l'exploitation de vulnérabilités zero-day à grande échelle. Ils sont responsables des vagues d'attaques massives contre les serveurs Accellion FTA, GoAnywhere MFT et MOVEit Transfer, touchant des milliers d'entreprises en une seule campagne.
- **Play :** Ce groupe utilise des techniques avancées pour contourner les défenses, comme l'exploitation de failles dans les VPN (ex: Fortinet) et l'utilisation d'outils comme AdFind pour la reconnaissance interne. Ils sont connus pour ne pas utiliser de site de fuite public, préférant la négociation privée.

Element	Description	Priorite
Prevention	Mesures proactives de reduction de la surface d'attaque	Haute
Detection	Surveillance et alerting en temps reel	Haute
Reponse	Procedures d'incident response et remediation	Critique
Recovery	Plan de reprise et continuite d'activite	Moyenne

Notre avis d'expert
Nos retours d'expérience montrent que les organisations qui investissent dans la lecture et l'application de référentiels méthodologiques structurés réduisent leur temps de réponse aux incidents de 40% en moyenne. La connaissance formalisée est un avantage compétitif sous-estimé.

Phase 1 : Accès Initial (Initial Access)

Comment les attaquants entrent-ils ? Plusieurs tactiques dominent : Pour approfondir, consultez Sécurité LLM Adversarial : Attaques, Défenses et Bonnes.

- **Phishing (T1566) :** L'envoi d'e-mails avec une pièce jointe malveillante (ex: un document Word avec une macro, un fichier ISO ou LNK) ou un lien vers une fausse page de connexion reste la méthode N°1. La formation des utilisateurs est essentielle, mais pas suffisante.
- **Exploitation de services publics (T1190) :** Des services exposés sur Internet et non patchés (VPN SSL comme Citrix ou Fortinet, Microsoft Exchange, serveurs RDP) sont des portes d'entrée de choix. Une gestion rigoureuse des patchs est vitale.
- **Identifiants valides (T1078) :** Achat d'identifiants sur le dark web ou compromission via des attaques de type "password spraying" contre des comptes sans MFA. L'authentification multifacteur (MFA) est la défense la plus efficace ici.

Phase 2 : La chaîne de compromission interne

Une fois à l'intérieur, l'attaquant n'est qu'un simple utilisateur. Son but est de devenir administrateur du domaine. Cette phase, appelée "dwell time", peut durer des jours, voire des semaines. C'est votre meilleure fenêtre pour le détecter.

1. **Exécution & Persistance (T1059, T1547) :** L'attaquant exécute des scripts (PowerShell) pour télécharger d'autres outils et établit une persistance (tâche planifiée, service) pour survivre à un redémarrage.
2. **Désactivation des défenses (T1562) :** Il tente de désactiver ou de contourner les solutions de sécurité comme les antivirus ou les EDR via des scripts ou en abusant des fonctionnalités de désinstallation.
3. **Reconnaissance & Découverte (T1087, T1018) :** Il utilise des outils comme AdFind ou PowerView pour cartographier l'Active Directory, identifier les comptes à privilèges, les serveurs de fichiers et, surtout, les serveurs de sauvegarde.
4. **Mouvement latéral (T1550) :** Il se déplace de machine en machine en utilisant des techniques comme Pass-the-Hash ou en exploitant des mots de passe d'administrateurs locaux identiques (d'où l'importance de LAPS).
5. **Escalade de privilèges :** Il utilise des techniques d'audit d'Active Directory (Kerberoasting, etc.) pour trouver des chemins de compromission et obtenir le contrôle d'un compte administrateur du domaine.

La majorité des attaques par ransomware aboutissent à une compromission totale de l'Active Directory. La sécurité de l'AD est donc la clé de voûte de la défense anti-ransomware.

Seriez-vous capable de détecter un attaquant sur votre réseau ?
Un pentest interne simule exactement ce scénario. Il permet de tester votre segmentation réseau, l'efficacité de vos outils de détection (EDR, SIEM) et la résilience de votre Active Directory face à un attaquant déterminé.

Tester ma défense interne

Cas concret
L'ANSSI a publié en 2023 son guide de recommandations pour l'administration sécurisée des SI, mettant à jour les principes de Tiering et de bastionnement. Ce document de référence pour les organisations françaises rappelle que les fondamentaux de l'hygiène informatique restent les mesures les plus efficaces.

Bonus : Analyse de WannaCry avec Ghidra

Présentation de Ghidra

Ghidra est un framework de reverse engineering (décompilation) développé par la NSA et rendu public en 2019. C'est un outil extrêmement puissant qui permet aux analystes de transformer un code binaire (un `.exe` ou un `.dll`) en un code source lisible (proche du C). Cela permet de comprendre la logique interne d'un malware : comment il se propage, ce qu'il chiffre, comment il communique avec son serveur de commande et de contrôle (C2).

Analyse du "Kill Switch" de WannaCry

WannaCry est célèbre pour avoir inclus un "kill switch" : avant de s'exécuter, il tentait de contacter un nom de domaine qui n'existait pas. Si la connexion réussissait (parce qu'un chercheur avait enregistré le domaine), le malware s'arrêtait. Voici à quoi ressemble la fonction décompilée dans Ghidra : Pour approfondir, consultez Livre Blanc Détaillé :.

```
void check_kill_switch(void) {
  // Tente d'ouvrir une connexion internet
  HINTERNET hInternet = InternetOpenW(L"WannaCry", 1, NULL, NULL, 0);

  if (hInternet != NULL) {
    // Tente de se connecter au domaine du kill switch
    HINTERNET hConnect = InternetOpenUrlW(hInternet,
                                          L"http://
www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com",
                                          NULL, 0, 0x84000000, 0);

    // Si la connexion réussit (le domaine existe et répond)
    if (hConnect != NULL) {
      InternetCloseHandle(hConnect);
      InternetCloseHandle(hInternet);
      // Le malware s'arrête ici et se termine
      exit(0);
    }
    InternetCloseHandle(hInternet);
  }
  // Si la connexion échoue (le domaine n'existe pas), le malware continue son exécution
  // ... Lancement de la routine de chiffrement ...
}
```

Cette analyse simple montre comment la décompilation permet de comprendre une logique cruciale du malware. L'attaquant pensait probablement utiliser ce domaine pour des tests, sans imaginer qu'il deviendrait son talon d'Achille.

Analyse de la routine de chiffrement

En analysant plus loin, on peut trouver la fonction qui scanne les fichiers de la victime. Ghidra révèle une logique qui parcourt les disques durs et recherche des fichiers avec des extensions spécifiques. WannaCry ciblait plus de 150 types de fichiers, incluant les documents Office, les images, les vidéos et les archives.

```
void encrypt_files_on_drive(char* drive_path) {
  // Liste des extensions ciblées
  char* target_extensions[] = { ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".jpg",
".zip", ... };

  // Parcours récursif des dossiers du disque
  // ... (code de parcours de fichiers) ...

  // Pour chaque fichier trouvé
  //   Vérifier si son extension est dans la liste target_extensions
  //   Si oui:
  //     Générer une clé de chiffrement AES pour ce fichier
  //     Chiffrer le contenu du fichier avec AES
  //     Chiffrer la clé AES avec la clé publique RSA du malware
  //     Ajouter la clé AES chiffrée à la fin du fichier
  //     Renommer le fichier en ajoutant l'extension .WCRY
}
```

Cette structure est typique des ransomwares modernes : un chiffrement symétrique rapide (AES) pour chaque fichier, et un chiffrement asymétrique (RSA) pour protéger les clés AES. Seul l'attaquant, avec sa clé privée RSA, peut déchiffrer les clés AES et donc les fichiers.

Phase 3 : L'Impact

Une fois administrateur du domaine, l'attaquant passe à la phase finale.

Double Extorsion : Exfiltration de données (T1567)

Avant de chiffrer, les groupes modernes comme LockBit ou Cl0p pratiquent la "double extorsion". Ils identifient vos données les plus sensibles (données financières, R&D, informations personnelles...) et les exfiltrent vers leurs serveurs, souvent via des outils légitimes comme Rclone ou Mega. Ils peuvent ainsi vous menacer de les publier sur leur site vitrine si vous ne payez pas la rançon, même si vous parvenez à restaurer vos sauvegardes. Pour approfondir, consultez Livre Blanc Détaillé :.

Chiffrement et destruction des sauvegardes (T1486, T1490)

Enfin, ils déploient le ransomware sur l'ensemble du réseau, généralement via une GPO ou des outils de déploiement comme PsExec. Le malware chiffre les serveurs et postes de travail (T1486). Une de ses premières actions est de supprimer les sauvegardes locales et les clichés instantanés de volume (via `vssadmin.exe delete shadows /all /quiet` - T1490) pour empêcher une restauration facile.

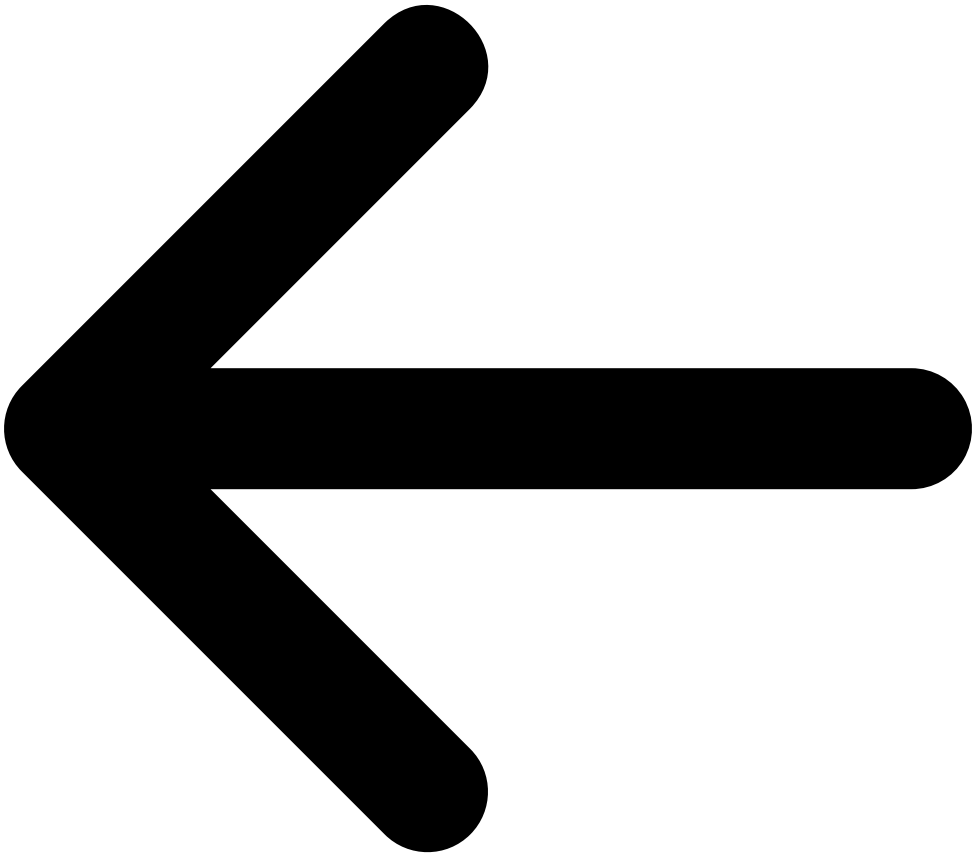
Comment se défendre ? Une stratégie de résilience

Aucune défense n'est parfaite. L'objectif est de construire une résilience multi-couches pour prévenir, détecter, répondre et récupérer.

1. **Prévention :** MFA partout, gestion des patchs agressive, filtrage email avancé, formation continue des utilisateurs, blocage des macros Office provenant d'Internet.
2. **Hardening :** Mettre en œuvre LAPS, le modèle de Tiering pour l'AD, Credential Guard, et des politiques de sécurité strictes pour PowerShell.
3. **Détection :** Déployer un EDR sur tous les endpoints, surveiller activement les logs AD et réseau avec un SIEM pour détecter les signaux faibles du "dwell time". Détecter l'utilisation d'outils comme Mimikatz ou la désactivation de services de sécurité.
4. **Réponse :** Avoir un plan de réponse à incident prêt et testé. Qui appeler ? Comment isoler le réseau ? Comment communiquer en interne et en externe ?
5. **Récupération : La règle d'or 3-2-1-1-0 des sauvegardes.** Avoir au moins **3** copies de vos données, sur **2** supports différents, dont **1** est hors-site, **1** est hors-ligne/immuable (non modifiable ou effaçable, par exemple avec S3 Object Lock), et avec **0** erreur après des tests de restauration réguliers.

Vous avez terminé votre parcours

Vous avez maintenant une vue d'ensemble des principales menaces modernes. Continuez à explorer nos ressources pour approfondir vos connaissances.



Retour à la liste des livres blancs

Ressources open source associées : Pour approfondir, consultez ISO 27001:2022 - Guide Complet de Certification et Mise en Conformité.

- ransomware-playbooks-fr — Dataset playbooks ransomware (HuggingFace)
- incident-response-playbooks — Dataset playbooks réponse à incident (HuggingFace)

Questions frequentes

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, mettre en place des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

Quelles sont les bonnes pratiques recommandees par les experts ?

Les experts recommandent une approche basee sur les risques, incluant l'evaluation reguliere de la posture de securite, la mise en place de controles techniques et organisationnels, la formation continue des equipes et l'adoption des referentiels de securite reconnus comme ceux du NIST, de l'ANSSI et de l'OWASP.

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

Conclusion

Cet article a couvert les aspects essentiels de Chapitre 1 : Qu'est-ce qu'un Ransomware en 2025 ?, Chapitre 2 : Les Groupes les Plus Actifs (Tendances 2024-2025), Phase 1 : Accès Initial (Initial Access). La mise en pratique de ces recommandations permet de renforcer significativement la posture de securite de votre organisation.

Sources et références : ANSSI · CERT-FR

Outils et Ressources Anti-Ransomware

Decouvrez nos outils open source et modeles d'IA developpes pour les professionnels de la cybersecurite :

Outil / Ressource	Description	Lien
YaraMemoryScanner	Scanner memoire YARA pour la detection de ransomware en temps reel	Voir sur GitHub
SysmonEventCorrelator	Correlateur Sysmon pour identifier les chaines d''attaque ransomware	Voir sur GitHub
VSSIntegrityWatcher	Surveillant d''integrite VSS pour detecter la suppression de shadow copies	Voir sur GitHub
AmcacheForensics	Analyse forensique Amcache pour tracer l''execution des binaires malveillants	Voir sur GitHub
ThreatIntel-GPT	Agent IA de threat intelligence pour l''analyse des indicateurs de compromission	Voir sur GitHub

Tous ces outils sont disponibles en open source sur notre profil GitHub et nos modeles d'IA sur notre espace HuggingFace. N'hesitez pas a contribuer et a signaler les issues.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr