

# **Veille Technologique : Le ransomware**

## Table des matières

<b>1. Introduction</b>	<b>3</b>
1.1. Objectif de la veille	3
1.2. Objectifs spécifiques de la veille ransomware	3
<b>2. Attaque par ransomware</b>	<b>4</b>
2.1 Vecteurs d'attaque courants	4
2.2 Évolution des modes opératoires	4
2.3. Cycle d'une attaque par ransomware	4
2.4. Conséquences d'une attaque ransomware	6
<b>3. Périmètre de la veille technologique</b>	<b>6</b>
3.1 Thématiques principales surveillées	6
3.2 Sources d'information surveillées	7
3.3 Typologie des organisations ciblées	8
3.4 Cadre temporel et fréquence	8
<b>4. Méthodologie de veille</b>	<b>8</b>
4.1 Veille active ( Méthode Pull )	8
4.2 Veille passive ( Méthode Push )	12
<b>5. Analyse et sélection des informations pertinentes</b>	<b>15</b>
5.1 Objectifs du traitement	15
5.2 Critères de sélection des informations	15
5.3 Nettoyage et filtrage	16
5.4 Classement et synthèse	16
5.5 Cas spécifique : veille sur Akira et ENDGAME	17
<b>6. Traitement et analyse des informations recueillies</b>	<b>17</b>
6.1 Analyse approfondie et formulation des recommandations	17
6.2 Étude de cas : Ransomware Akira	17
6.2.1 Contexte	17
6.2.2 Vecteurs d'infection identifiés	18
6.2.3 Zoom sur la CVE-2024-40766 – SonicWall	18
6.2.4 Analyse et sélection des informations pertinentes	20
6.2.4.1 Identification des vecteurs d'attaque critiques	21
6.2.4.2 Évaluation de la criticité et de l'impact	21
6.2.5 Conséquences opérationnelles et économiques des attaques Akira	22
6.2.6 Appui des recommandations par les sources expertes	23
6.2.7 Recommandations de sécurité	23
6.2.7.1 Qualification et investigation	23
6.2.7.2 Remédiation	24
6.2.7.3 Durcissement de la sécurité	24
6.2.7.4 Supervision renforcée	24
6.2.7.5 Recommandations renforcées ( Prévention et défense contre Akira )	25
<b>7. Sources officielles</b>	<b>26</b>

# 1. Introduction

Dans un contexte numérique en constante évolution, la cybersécurité s'impose comme un enjeu stratégique pour les organisations publiques et privées. L'augmentation continue des cybermenaces (ransomwares, attaques de la supply chain, APT, exfiltration de données), couplée à un durcissement du cadre réglementaire (RGPD, NIS2, DORA, LPM), nécessite une veille technologique rigoureuse, proactive et structurée.

Ce travail de veille permet non seulement d'anticiper les nouvelles menaces, mais aussi d'adapter les politiques de sécurité, de renforcer les capacités de détection et de réaction, et de garantir la conformité réglementaire.

## 1.1. Objectif de la veille

Dans le cadre de mon activité, j'ai orienté ma veille technologique sur une menace prioritaire : le ransomware. Ce type de malware constitue aujourd'hui une menace majeure pour les systèmes d'information, de par :

- Sa capacité à chiffrer et rendre indisponibles des données critiques,
- Son impact économique (coût des rançons, pertes d'exploitation),
- Les risques juridiques liés à la fuite de données personnelles (sanctions CNIL, atteinte à la réputation),
- Sa sophistication croissante (double extorsion, exfiltration, automatisation des charges utiles).

## 1.2. Objectifs spécifiques de la veille ransomware

Cette veille m'a permis de répondre à plusieurs objectifs opérationnels :

- Identifier et suivre les groupes cybercriminels actifs (ex. : LockBit, BlackCat, Cl0p) et leurs modes opératoires (TTP – Tactiques, Techniques et Procédures),
- Analyser les campagnes d'attaque récentes ciblant des entreprises de secteurs critiques (santé, énergie, administration),
- Cartographier les vulnérabilités exploitées (CVE récentes, zero-days, détournement d'outils légitimes),
- Étudier les techniques de propagation (phishing, RDP, exploitation de VPN non patchés),
- Rechercher les meilleures pratiques en matière de protection, durcissement, détection et réponse à incident,
- Suivre les évolutions réglementaires imposant des obligations de notification, de prévention ou de chiffrement (ex. : NIS2, RGPD, LPM).

## 2. Attaque par ransomware

Les attaques par ransomware (ou rançongiciel) figurent aujourd'hui parmi les menaces les plus graves et les plus fréquentes auxquelles sont confrontées les organisations. Ce type d'attaque consiste à chiffrer les données d'un système d'information ou à en bloquer l'accès, en échange d'une rançon, souvent payée en cryptomonnaie. Dans les cas les plus complexes, les attaquants menacent également de divulguer publiquement les données volées.

### 2.1 Vecteurs d'attaque courants

Les rançongiciels utilisent généralement les vecteurs suivants pour pénétrer les systèmes d'information :

- **Phishing** : campagnes d'emails piégés contenant des pièces jointes malveillantes ou des liens vers des serveurs de commande.
- **Exploitation de vulnérabilités** : faille logicielle critique non corrigée (ex. : CVE non patchée dans un service exposé).
- **Accès RDP non sécurisé** : protocoles RDP exposés sur Internet sans authentification forte (MFA), souvent brute forcés.

### 2.2 Évolution des modes opératoires

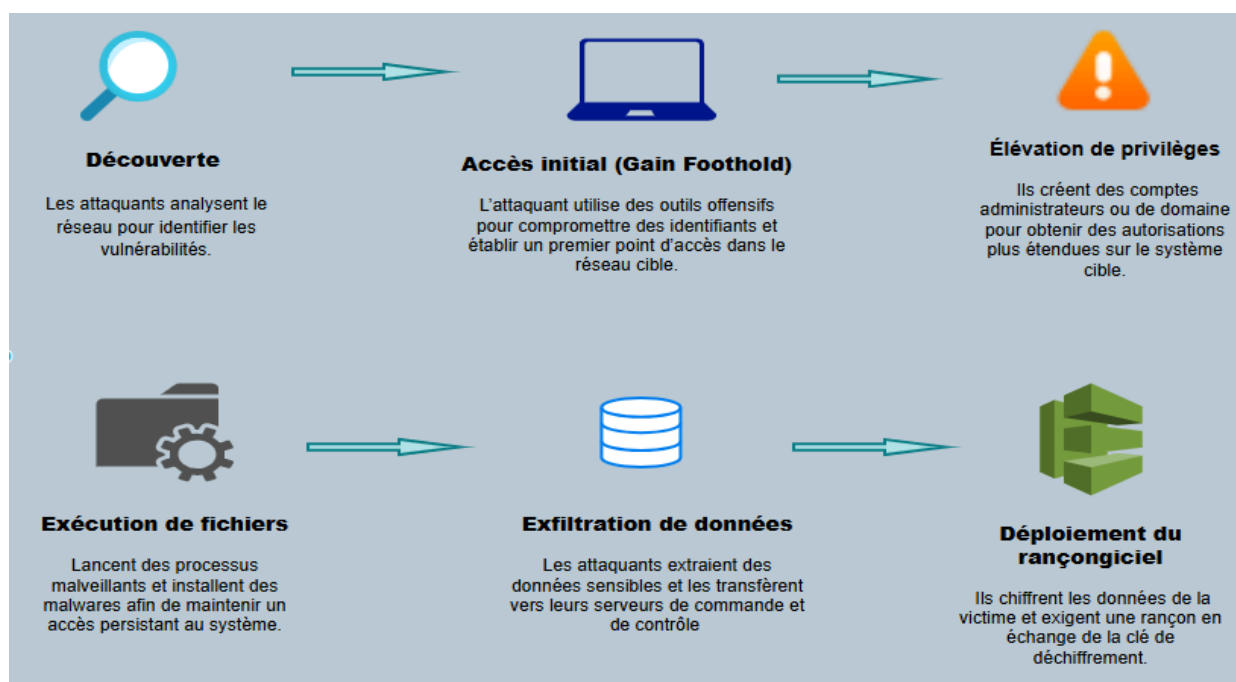
Les cybercriminels ont professionnalisé leurs pratiques selon un modèle industriel, avec notamment :

- **Ransomware-as-a-Service (RaaS)** : des groupes développent des outils malveillants qu'ils louent à des affiliés via des portails dédiés (ex. : LockBit, Akira, BlackCat).
- **Double extorsion** : les données sont d'abord exfiltrées, puis chiffrées. Le paiement est exigé pour éviter leur publication.
- **Triple extorsion** : la pression s'étend aux clients, partenaires ou aux médias, pour accentuer l'impact.

Ces attaques ont un impact critique sur les entreprises, avec des conséquences souvent multidimensionnelles : interruption d'activité, pertes financières, atteinte à la réputation, et obligations réglementaires (notamment RGPD).

### 2.3. Cycle d'une attaque par ransomware

Voici un schéma typique du déroulement d'une attaque par ransomware :



### Étapes d'une attaque ransomware :

Phase	Description
<b>1. Reconnaissance</b>	Scan automatisé d'IP publiques, recherche de failles exposées, récolte d'informations via OSINT ou ingénierie sociale.
<b>2. Intrusion initiale</b>	Phishing, exploitation d'une CVE, utilisation d'identifiants faibles ou fuites sur le dark web.
<b>3. Mouvement latéral et élévation de privilèges</b>	Utilisation d'outils légitimes (ex : PSEXEC, Cobalt Strike) pour explorer le réseau et élever les privilèges (ex : Kerberoasting, exploitation Active Directory).
<b>4. Exfiltration des données</b>	Les fichiers sensibles sont exfiltrés vers des serveurs externes (souvent via FTP ou Tor).
<b>5. Déploiement du ransomware</b>	Chiffrement des fichiers, désactivation ou suppression des sauvegardes.
<b>6. Demande de rançon</b>	Affichage d'une note de rançon (souvent personnalisée), avec des instructions de paiement.
<b>7. Menace de publication</b>	Si le paiement est refusé, les données sont publiées sur un site de "data leak" contrôlé par les attaquants.

## 2.4. Conséquences d'une attaque ransomware

Les impacts d'une attaque réussie sont à la fois techniques, opérationnels, juridiques et financiers :

Type de conséquence	Détails
<b>Technique</b>	- Données inaccessibles - SI à l'arrêt, corruption de sauvegardes
<b>Opérationnelle</b>	- Interruption d'activité - Pertes de revenus - Retards logistiques
<b>Réputationnelle</b>	- Perte de confiance des clients - Partenaires et usagers
<b>Juridique</b>	- Obligation de notification (CNIL, clients) - Risque de sanction RGPD
<b>Financière</b>	- Coût de la rançon (souvent refusée) - Frais de remédiation - Audit - Communication de crise
<b>Assurantielle</b>	- Clauses de non-couverture si MFA - sauvegardes ou patching absents

Face à la sophistication croissante de ces menaces et à leur fréquence, il est indispensable de maintenir une veille ciblée sur les groupes actifs, leurs outils, les vulnérabilités exploitées et les contre-mesures disponibles. Cela permet de :

- Anticiper les modes opératoires émergents,
- Adapter les stratégies de défense (durcissement, détection, segmentation réseau),
- Garantir la résilience de l'organisation en cas d'incident.

## 3. Périmètre de la veille technologique

Pour assurer une veille pertinente, exploitable et alignée avec les enjeux opérationnels, j'ai défini un périmètre de veille structuré autour des attaques par ransomware. Ce périmètre couvre à la fois les aspects techniques, organisationnels et réglementaires de la menace.

### 3.1 Thématiques principales surveillées

La veille s'est articulée autour des axes suivants :

- ★ **Typologies de ransomwares :**

- Locker, Wiper, Double extorsion, Triple extorsion
- Ransomware-as-a-Service (RaaS)

★ **Groupe cybercriminels actifs :**

- Lockbit, Clop, Akira, BlackCat (ALPHV), etc.

★ **Vulnérabilités critiques exploitées :**

- Vulnérabilités avec un score CVSS  $\geq 8$ , exploitées dans des campagnes récentes.

★ **Tactiques, techniques et procédures (TTPs) :**

- Référencement dans la base MITRE ATT&CK (initial access, lateral movement, exfiltration, impact).

★ **Solutions de cybersécurité :**

- Outils de détection (EDR/XDR), de prévention (durcissement, MFA, segmentation), et de réponse (SOAR, plans de reprise).

★ **Évolutions réglementaires :**

- RGPD (notification des violations),
- Directive NIS2,
- Obligations de déclaration à la CNIL,
- Positionnement de l'ANSSI sur les rançons et la remédiation.

## 3.2 Sources d'information surveillées

La veille s'est appuyée sur un panel de sources qualifiées, diversifiées et actualisées :

Catégorie	Sources principales
Portails officiels	CERT-FR, ANSSI, CISA (US), ENISA, base CVE/NVD
Presse spécialisée	The Hacker News, BleepingComputer, ThreatPost
Rapports de fournisseurs	Microsoft Threat Intelligence, Palo Alto Unit42, CrowdStrike, SentinelOne
Réseaux sociaux techniques	Comptes X (ex-Twitter) et LinkedIn d'experts en cybersécurité
Clubs professionnels	Clusif, Club 27001, Club EBIOS, Cercle des RSSI

### 3.3 Typologie des organisations ciblées

Cette veille a été pensée pour être utile aux structures potentiellement exposées à ce type de menace, en particulier :

- Entreprises de taille intermédiaire à grande (ETI, grandes entreprises)
- Collectivités territoriales
- Établissements publics de santé (notamment visés depuis 2020)
- Fournisseurs de services numériques (ESN, MSP, infogéreurs)

### 3.4 Cadre temporel et fréquence

Paramètre	Détail
Période de veille	Du 29 juillet au 08 août
Fréquence	Hebdomadaire (veille pull) + quotidienne (veille push via flux RSS, newsletters, alertes CVE)

Ce cadrage méthodologique m'a permis de maintenir une veille stratégique et opérationnelle, directement exploitable pour renforcer la détection, la prévention et la réponse face aux attaques par ransomware. Il assure également une couverture transversale, alliant vision technique, analyse des menaces, exigences réglementaires et positionnement sectoriel.

## 4. Méthodologie de veille

Afin de garantir une veille cybersécurité rigoureuse, actualisée et centrée sur les menaces liées aux ransomwares, j'ai adopté une double approche méthodologique combinant :

- une veille active (méthode pull), basée sur des recherches manuelles ciblées,
- une veille passive (méthode push), reposant sur la réception automatisée d'informations en temps réel.

Cette approche hybride m'a permis de concilier profondeur d'analyse stratégique et réactivité face aux alertes critiques, en assurant une couverture équilibrée des actualités techniques, des campagnes malveillantes en cours, et des évolutions réglementaires.

### 4.1 Veille active ( Méthode Pull )

La veille active consiste à rechercher et croiser manuellement les informations, selon une fréquence hebdomadaire, en s'appuyant sur des sources spécialisées, officielles et validées.

**Objectifs :**



- Suivre les vulnérabilités critiques exploitées par les ransomwares (ex. CVE avec CVSS  $\geq 8$ ),
- Identifier les nouveaux groupes cybercriminels actifs et leurs TTPs,
- Comprendre les modes opératoires et les tendances techniques émergentes,
- Analyser les mesures de détection et de prévention proposées par les éditeurs et organismes de référence.

#### Sources principales mobilisées :

Type de source	Exemples
Bases de vulnérabilités	CVE, NVD (NIST)
Organismes officiels	CERT-FR, ANSSI, CISA, ENISA
Référentiels techniques	MITRE ATT&CK, bulletins de sécurité Microsoft, Palo Alto, CrowdStrike
Presse spécialisée	The Hacker News, BleepingComputer
Clubs professionnels	CLUSIF, CLUSIR, Club EBIOS, Club 27001

#### Démarche :

- Utilisation de moteurs de recherche (Google, DuckDuckGo) pour des requêtes précises :  
site:cisa.gov ransomware cve 2024, site:bleepingcomputer.com lockbit, etc.
- Croisement des sources pour validation (priorité aux informations recoupées par des entités gouvernementales ou fournisseurs reconnus).
- Recherche systématique des techniques associées via le référentiel MITRE ATTACK.

#### Exemple :

À partir d'une alerte CISA sur une vulnérabilité critique exploitée par Clop, j'ai vérifié son existence dans le NVD (score CVSS), puis j'ai identifié la TTP associée dans MITRE ATT&CK, ce qui a permis d'établir un lien entre la faille technique et le vecteur d'attaque observé sur le terrain.

Lors de cette veille active, je me suis principalement concentré sur les informations les plus récentes, en privilégiant les actualités, vulnérabilités et incidents publiés au cours des dernières semaines, afin d'assurer une vision à jour des menaces émergentes.

## LATEST RANSOMWARE NEWS



### SonicWall firewall devices hit in surge of Akira ransomware attacks

SonicWall firewall devices have been increasingly targeted since late July in a surge of Akira ransomware attacks, potentially exploiting a previously unknown security vulnerability, according to cybersecurity company Arctic Wolf.

SERGIU GATLAN AUGUST 01, 2025 01:28 PM 2



### Inside a Real Clickfix Attack: How This Social Engineering Hack Unfolds

ClickFix abuses clipboards. FileFix hijacks File Explorer. Both social engineering attacks start in the browser—and end in malware. See how Keep Aware stops these stealthy attacks before they break out of the browser in a run down of a real attack.

KEEP AWARE JULY 31, 2025 10:05 AM 0

Je souhaitais vérifier la véracité des données. Pour cela, j'ai décidé de me concentrer tout particulièrement sur les informations validées par des organismes gouvernementaux tels que la CISA.



## America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

[Topics](#) [Spotlight](#) [Resources & Tools](#) [News & Events](#) [Careers](#) [About](#)

[Home](#) / [News & Events](#) / [Cybersecurity Advisories](#) / [Alert](#) / CISA and Partners Release Advisory on Akira Ransomware

### ALERT

# CISA and Partners Release Advisory on Akira Ransomware

J'ai également vérifié la situation en France, en m'appuyant sur les publications du CERT-FR.



## RAPPORT MENACES ET INCIDENTS DU CERT-FR

Objet: Opération ENDGAME

### GESTION DU DOCUMENT

Référence	CERTFR-2024-CTI-004
Titre	Opération ENDGAME
Date de la première version	30 mai 2024
Date de la dernière version	30 mai 2024
Source(s)	



JSON

## BULLETIN D'ALERTE DU CERT-FR

Objet: Vulnérabilité dans SonicWall

### GESTION DU DOCUMENT

Référence	CERTFR-2024-ALE-011
Titre	Vulnérabilité dans SonicWall
Date de la première version	10 septembre 2024
Date de la dernière version	21 novembre 2024
Source(s)	Bulletin de sécurité SonicWall SNWLID-2024-0015 du 22 août

A l'aide de ces informations, j'ai recherché sur MITRE Attack les techniques d'attaques utilisées.



## 4.2 Veille passive ( Méthode Push )

En complément de la méthode Pull (veille active), j'ai mis en œuvre une veille passive basée sur la réception automatisée de contenus spécialisés. Cette approche m'a permis de suivre en temps réel l'évolution des menaces, des vulnérabilités et des exigences réglementaires, sans sollicitation manuelle systématique.

Objectifs de la veille passive

Cette démarche avait pour finalité de :

- Suivre l'évolution des menaces techniques (ransomwares, failles critiques, supply chain),
- Recevoir rapidement les alertes de sécurité (CVE majeures, campagnes actives, IoC),
- Anticiper les évolutions réglementaires et normatives (NIS2, RGPD, etc.).

a) Veille technologique ( Menaces et vulnérabilités )

**Outils et canaux mobilisés**

- **Flux RSS** via Feedly : agrégation de sources de référence telles que :
  - CERT-FR
  - CISA
  - The Hacker News
  - BleepingComputer
- **Newsletters spécialisées** :
  - SANS Newsbites
  - Rapid7 Threat Intelligence
  - ThreatPost

- DarkReading
- **Alertes ciblées :**
  - Filtrage des CVE selon le score CVSS, la date de publication et la criticité
- **Réseaux sociaux techniques :**
  - Suivi de comptes experts sur X (ex-Twitter) et LinkedIn : chercheurs, CERTs, éditeurs (Microsoft, Palo Alto, etc.), RSSI

## Résultats

Cette veille m'a permis de détecter rapidement :

- Les failles critiques exploitées par les groupes de ransomware,
- Les campagnes malveillantes en cours,
- Les tactiques techniques émergentes (ex : usage d'outils comme Cobalt Strike ou AnyDesk dans certaines intrusions).

## b) Veille réglementaire (Conformité et normes)

### Axes surveillés

La veille réglementaire a porté sur les cadres suivants :

- Directive NIS2 (et sa transposition nationale),
- RGPD,
- Cybersecurity Act,
- RGS (Référentiel Général de Sécurité),
- eIDAS 2.0 (identité numérique et services de confiance).

### Canaux utilisés

- Newsletters officielles : CNIL, ANSSI, ENISA, CERT-FR
- Alertes Google personnalisées sur des requêtes précises :
  - *transposition NIS2 France*
  - *cybersécurité eIDAS 2.0*
  - *obligation RGPD cybersécurité*
- Veille sociale via LinkedIn et X : publications d'avocats, juristes, RSSI, consultants cyber

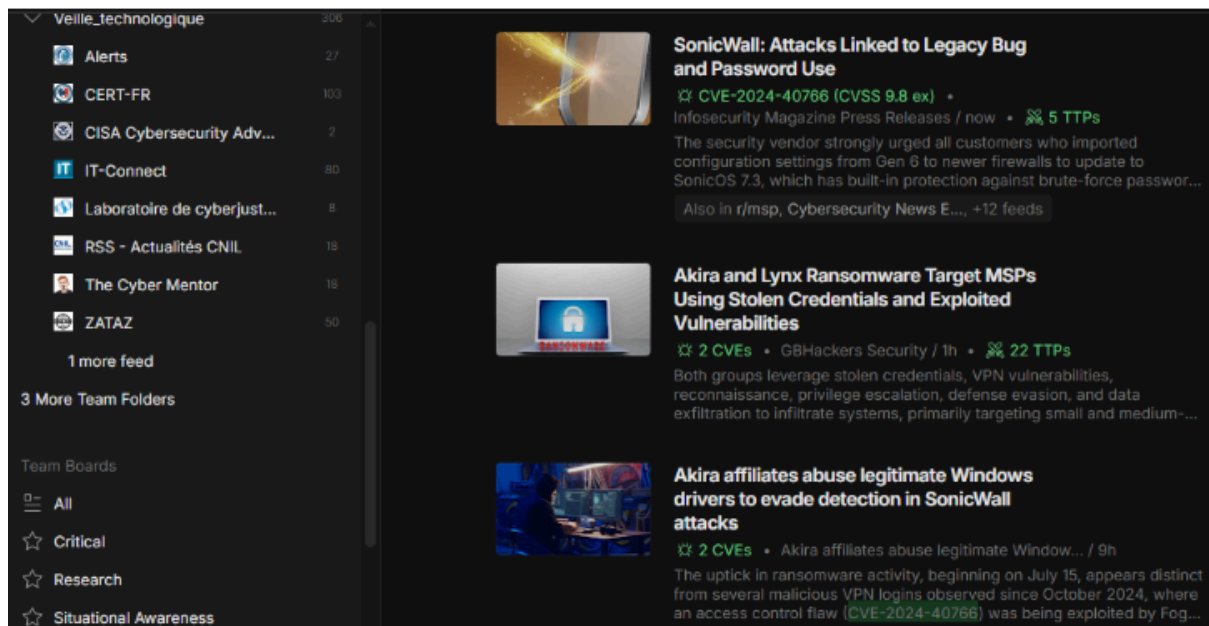
### Utilité

Cette veille a facilité l'identification :

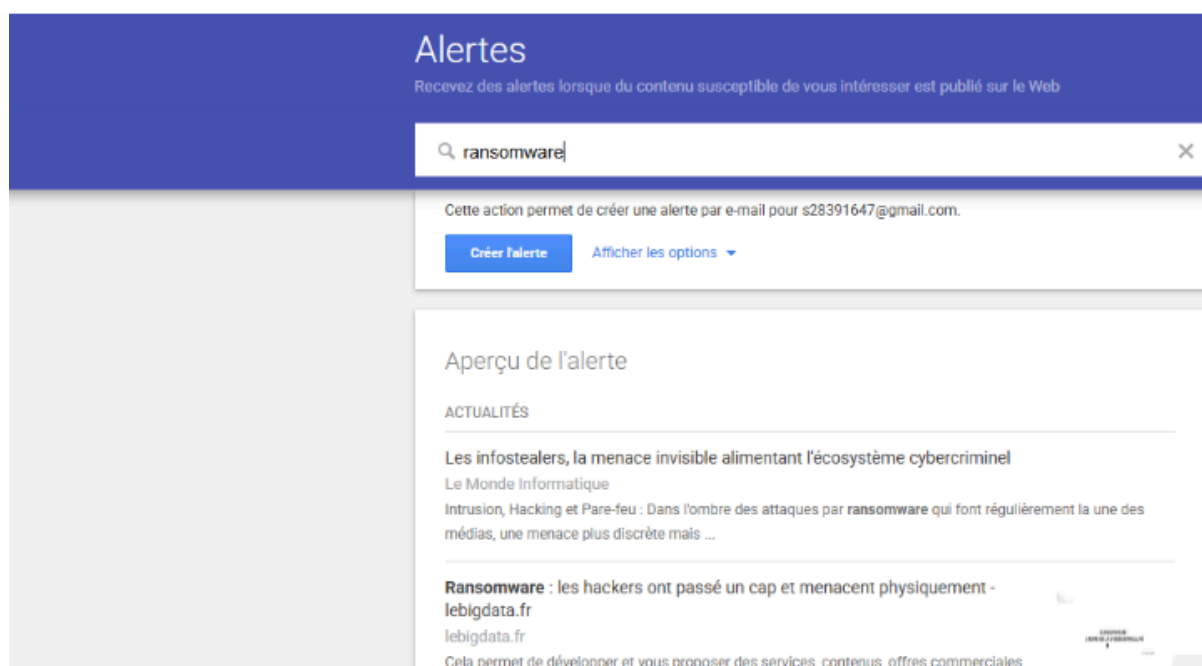
- Des dates clés (entrée en vigueur de NIS2, directives CNIL),

- Des recommandations pratiques (exigences de MFA, obligations de notification, etc.),
- Des risques juridiques en cas de non-conformité (notamment dans les contextes de ransomware impliquant des fuites de données).

Ci-dessous, mon flux RSS Feedly, configuré pour recevoir automatiquement les alertes concernant les vulnérabilités critiques, comme les CVE récents, les bulletins d'incident en cours et les rapports techniques.



Une alerte Google a également été mise en place afin d'être notifié en temps réel des nouvelles publications liées aux vulnérabilités critiques, aux CVE, ou aux incidents de cybersécurité.



La méthode Push m'a offert une couverture en continu des menaces et des exigences, une capacité d'adaptation rapide face aux évolutions techniques et réglementaires, un gain de temps considérable, en évitant des recherches manuelles répétitives.

## 5. Analyse et sélection des informations pertinentes

Une fois les données collectées via les approches Push et Pull, j'ai appliqué un processus de traitement structuré visant à :

- Identifier les informations fiables et utiles,
- Éliminer les contenus redondants, non vérifiés ou hors périmètre,
- Retenir uniquement les données opérationnellement exploitables.

### 5.1 Objectifs du traitement

Ce traitement avait pour but :

- De garantir la qualité des informations intégrées dans la veille,
- D'assurer leur pertinence contextuelle (technologique, réglementaire ou sectorielle),
- De faciliter leur exploitation opérationnelle.

### 5.2 Critères de sélection des informations

J'ai défini une grille d'évaluation pour filtrer les contenus :

Critère	Description
<b>Pertinence</b>	Lien direct avec les axes définis : ransomware, vulnérabilités critiques, évolutions réglementaires
<b>Fiabilité</b>	Source reconnue et vérifiée : CERT-FR, CISA, ANSSI, éditeurs de cybersécurité, etc.
<b>Actualité</b>	Donnée récente et toujours valide au moment de la consultation
<b>Impact</b>	Niveau de criticité ou d'exposition associé (secteurs ciblés, CVSS $\geq$ 8, etc.)
<b>Actionnabilité</b>	Possibilité de déclencher une mesure concrète : alerte, patch, durcissement, communication interne

## 5.3 Nettoyage et filtrage

Face au volume important d'informations, notamment via la méthode Push (réseaux sociaux, newsletters automatisées), j'ai appliqué un processus de nettoyage rigoureux :

- Suppression des doublons : contenus relayés plusieurs fois sur différentes plateformes,
- Élimination des données hors périmètre : ex. ransomwares ciblant des régions non pertinentes ou failles obsolètes,
- Exclusion des sources non vérifiées : blogs non sourcés, forums anonymes.

Pour assurer la fiabilité :

- J'ai systématiquement recoupé les informations avec au moins deux sources fiables,
- Les données ont été validées par des publications officielles (CERT-FR, CISA, ENISA, etc.),
- Les éléments ont été mis en contexte pour être applicables à un environnement organisationnel réaliste.

## 5.4 Classement et synthèse

Les données retenues ont été structurées pour faciliter leur exploitation :

- Classement par thématique : ransomware, vulnérabilité, outil offensif, réglementation...
- Hiérarchisation par niveau de priorité : faible, modérée, élevée



- Formats produits :
  - Fiches de veille synthétiques
  - Notes d'analyse
  - Bulletins hebdomadaires (résumant l'évolution des menaces)

## 5.5 Cas spécifique : veille sur Akira et ENDGAME

Dans le cadre de la veille orientée sur les menaces liées à Akira ransomware et à l'opération ENDGAME, j'ai :

- Prioriser les publications issues de CERT-FR, CISA, The DFIR Report,
- Écarté les contenus issus de blogs personnels ou de forums sans fondement technique,
- Retenu en priorité les rapports intégrant :
  - Une analyse MITRE ATTACK,
  - Une cartographie des vecteurs d'infection,
  - Des recommandations opérationnelles (isolement de postes, règles EDR, indicateurs de compromission, etc.)

Cette méthodologie m'a permis d'optimiser le temps de traitement des informations, de réduire la surcharge cognitive liée à l'abondance de données, de produire des synthèses pertinentes, contextualisées et directement exploitables.

## 6. Traitement et analyse des informations recueillies

### 6.1 Analyse approfondie et formulation des recommandations

L'analyse a porté sur l'évaluation de l'impact, l'identification des vecteurs d'attaque et la compréhension du comportement des attaquants à travers le prisme du framework MITRE ATTACK. Pour chaque menace identifiée, des actions concrètes ont été formulées : renforcement de la supervision, mesures de confinement, durcissement des accès, bonnes pratiques d'hygiène informatique, etc.

### 6.2 Étude de cas : Ransomware Akira

#### 6.2.1 Contexte

En mai 2024, l'opération ENDGAME a permis le démantèlement de plusieurs infrastructures cybercriminelles, utilisées notamment pour la diffusion de rançongiciels. Parmi ceux identifiés, le ransomware Akira s'est révélé particulièrement actif et destructeur.

Akira est souvent déployé via des loaders malveillants comme BumbleBee, IcedID, Pikabot, SmokeLoader et SystemBC, qui servent à établir un premier point d'accès avant l'exécution de charges secondaires.

Depuis son apparition en mars 2023, Akira a affecté plus de 300 organisations à travers le monde, avec des cibles de grande envergure telles que Nissan, Hitachi ou encore l'Université Stanford.

D'après le FBI, le groupe Akira aurait extorqué plus de 42 millions de dollars à plus de 250 victimes.

Plus récemment, en juillet 2024, une intensification des attaques ciblant les dispositifs SonicWall a été observée, notamment par l'exploitation de la vulnérabilité CVE-2024-40766, facilitant la propagation du ransomware Akira via les services SSL VPN.

### Description technique du ransomware Akira

Caractéristique	Description
Type	Rançongiciel (ransomware)
Mode de propagation	Charge finale exécutée après compromission initiale par un loader (BumbleBee, IcedID, etc.), via phishing ou vulnérabilités réseau
Fonctionnalités	Chiffrement des fichiers avec demande de rançon ; utilisée en phase finale d'attaque pour maximiser les dommages

### 6.2.2 Vecteurs d'infection identifiés

- Campagnes de phishing ciblé : e-mails malveillants contenant pièces jointes ou liens infectés ;
- Loaders malveillants : exploitation d'infections initiales par BumbleBee, IcedID, Pikabot, etc. ;
- Tunnels chiffrés : usage de SystemBC pour établir des canaux de communication furtifs ;
- Exploitation de la faille CVE-2024-40766 dans les appliances SonicWall, via le service SSL VPN ;
- Publicités malveillantes et spam comme méthode d'amorçage de la chaîne d'infection.

### 6.2.3 Zoom sur la CVE-2024-40766 – SonicWall

# CVE-2024-40766 Detail

## Description

An improper access control vulnerability has been identified in the SonicWall SonicOS management access, potentially leading to unauthorized resource access and in specific conditions, causing the firewall to crash. This issue affects SonicWall Firewall Gen 5 and Gen 6 devices, as well as Gen 7 devices running SonicOS 7.0.1-5035 and older versions.

Metrics


CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

*NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.*

**CVSS 3.x Severity and Vector Strings:**

**NIST: NVD**

**Base Score:**  
9.8 CRITICAL

**Vector:**  
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**ADP: CISA-ADP**

**Base Score:**  
9.3 CRITICAL

**Vector:**  
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:L

- **Score CVSS** : 9.8 / 10 (critique)
- **Produit affecté** : SonicOS (versions < 7.0.1-5035), générations 5, 6 et 7 de pare-feux SonicWall
- **Nature de la faille** :
  - Permet un accès non autorisé via SSL VPN
  - Risques : déni de service, contournement des politiques de sécurité, atteinte à la confidentialité
- **Exploitation active** : confirmée depuis juillet 2024, notamment pour faciliter le déploiement d’Akira
- **Recommandations émises par SonicWall et CERT-FR** :
  - Application immédiate des correctifs de sécurité
  - Activation de l’authentification multifacteur (MFA) pour tous les accès VPN
  - Renforcement de la supervision des logs d’accès et du trafic réseau

### MITRE ATT&CK – Tactiques et techniques observées

Phase ATT&CK	Technique associée
Initial Access	Spearphishing (T1566.001), Exploitation (T1190)
Execution	Loader via malspam ou tunnel SystemBC (T1204)
Persistence	Création de nouveaux comptes, Scheduled Tasks

<b>Privilege Escalation</b>	Abuse of legitimate tools, credential dumping
<b>Defense Evasion</b>	Disabling security tools, use of encrypted tunnels
<b>Impact</b>	File encryption (T1486), Data exfiltration (T1041)

<b>Phase</b>	<b>Description</b>	<b>Exemples concrets</b>
<b>Initial Access</b>	Comment l'attaquant entre dans le système.	<ul style="list-style-type: none"> <li>- Email piégé avec pièce jointe malveillante (spearphishing)</li> <li>- Exploitation d'une faille SonicWall</li> </ul>
<b>Execution</b>	Comment il exécute son code malveillant.	<ul style="list-style-type: none"> <li>- Le malware est lancé après que l'utilisateur clique sur un fichier</li> <li>- Usage de SystemBC (tunnel malveillant)</li> </ul>
<b>Persistence</b>	Comment il reste dans le système après redémarrage.	<ul style="list-style-type: none"> <li>- Création d'un compte admin caché</li> <li>- Ajout d'une tâche planifiée pour relancer le malware</li> </ul>
<b>Privilege Escalation</b>	Comment il obtient plus de droits.	<ul style="list-style-type: none"> <li>- Vol de mots de passe admin</li> <li>- Exploitation de failles pour devenir Administrateur</li> </ul>
<b>Defense Evasion</b>	Comment il évite d'être détecté.	<ul style="list-style-type: none"> <li>- Désactivation de l'antivirus</li> <li>- Chiffrement du trafic malveillant</li> </ul>
<b>Impact</b>	Les actions finales de l'attaque.	<ul style="list-style-type: none"> <li>- Chiffrement des fichiers (ransomware)</li> <li>- Vol et fuite de données</li> </ul>

## 6.2.4 Analyse et sélection des informations pertinentes

L'analyse approfondie des données collectées sur le ransomware Akira et les attaques ciblant les dispositifs SonicWall permet de tirer plusieurs enseignements clés, tant sur les modes opératoires des attaquants que sur les leviers de défense prioritaires.

#### 6.2.4.1 Identification des vecteurs d'attaque critiques

Deux vecteurs principaux ressortent des rapports techniques et bulletins d'alerte :

- Exploitation de vulnérabilités non corrigées, notamment la CVE-2024-40766, touchant les équipements SonicWall. Cette faille critique permet un accès non authentifié via SSL VPN, facilitant une compromission initiale rapide, sans besoin d'identifiants valides.
- Utilisation de loaders malveillants tels que BumbleBee, IcedID, Pikabot, souvent déployés via phishing ou campagnes de spam. Ces outils établissent un point d'accès persistant dans le système avant le déclenchement du ransomware.

Ces deux vecteurs imposent une double priorité en matière de défense :

1. Application rapide des correctifs de sécurité sur les équipements critiques.
2. Renforcement de la sensibilisation et du filtrage contre les attaques par phishing.

#### 6.2.4.2 Évaluation de la criticité et de l'impact

La CVE-2024-40766 présente un score CVSS de 9.8/10, indiquant une vulnérabilité critique :

- Permet un accès non autorisé, une élévation de privilèges et le contournement des politiques de sécurité.
- Affecte un parc important de dispositifs SonicWall (générations 5, 6 et 7), souvent déployés dans des infrastructures sensibles.

Le lien établi entre cette vulnérabilité et la propagation du ransomware Akira démontre que l'absence de patches expose les organisations à des conséquences graves :

- **compromission totale de l'infrastructure,**
- **interruption d'activité,**
- **exfiltration de données,**
- **et exigence de rançon.**

L'analyse a permis de :

- Mettre en lumière les techniques d'accès initial les plus exploitées.
- Hiérarchiser les menaces en fonction de leur criticité technique et impact opérationnel.
- Appuyer des recommandations concrètes pour la prévention et la supervision ciblée.

L'évolution rapide d'Akira et sa capacité à exploiter des failles zero-day comme celle affectant SonicWall soulignent l'urgence d'adopter une stratégie de cybersécurité défensive, multi-couches et résiliente. La simple détection ne suffit plus : seule une préparation active, une remédiation rapide et une posture de sécurité globale permettent de réduire l'impact de ces menaces à fort potentiel destructif.

## 6.2.5 Conséquences opérationnelles et économiques des attaques Akira

Les attaques du groupe Akira, notamment celles récentes exploitant la vulnérabilité CVE-2024-40766 des pare-feux SonicWall, ont des répercussions graves sur les organisations ciblées, tant sur le plan opérationnel que financier.

### Impacts opérationnels

#### 1. Interruption des activités :

Le chiffrement des systèmes par Akira entraîne une paralysie complète ou partielle des services informatiques, empêchant l'accès aux applications métier critiques, aux bases de données et aux services de communication internes. Certaines entreprises ont connu des arrêts de production de plusieurs jours, voire semaines.

#### 2. Compromission de données :

Akira applique une stratégie de double extorsion, en exfiltrant les données sensibles avant de les chiffrer. Ces données peuvent ensuite être divulguées publiquement sur les sites de fuite (leak sites) si la rançon n'est pas payée. Cela représente un risque juridique et réputationnel important (RGPD, confidentialité des données clients, etc.).

#### 3. Mobilisation de ressources internes :

La réponse à une attaque de ce type nécessite une mobilisation urgente des équipes IT, sécurité, juridique et communication. Dans certains cas, une assistance externe spécialisée est requise, retardant d'autant plus le retour à la normale.

### Impacts économiques

#### 1. Paiement des rançons :

Selon le FBI, le groupe Akira a collecté plus de 42 millions de dollars auprès de plus de 250 victimes entre 2023 et avril 2024. Bien que déconseillé par les autorités, le paiement de rançon reste une réalité pour certaines entreprises souhaitant récupérer leurs données plus rapidement.

#### 2. Coût de remédiation :

Même en l'absence de paiement, les coûts liés à la récupération (remise en service, reconfiguration, changement d'infrastructure, etc.) peuvent atteindre plusieurs centaines de milliers d'euros. À cela s'ajoutent les frais d'enquête, d'analyse forensic et de durcissement post-incident.

#### 3. Pertes d'exploitation :

Les interruptions de service peuvent engendrer des pertes de chiffre d'affaires directes (ex. : sites e-commerce inaccessibles, arrêt d'usines), des pénalités contractuelles, et une détérioration de la relation client.

#### 4. Atteinte à la réputation :

Être listé sur un leak site ou faire l'objet d'un article dans la presse spécialisée (ex. BleepingComputer, The Record) peut durablement affecter la réputation d'une entreprise, entraînant une perte de confiance de la part des clients, partenaires et investisseurs.

### Secteurs particulièrement visés

Akira cible des organisations de tous secteurs, mais plusieurs cas récents ont touché :

- Le secteur industriel (ex. Nissan Océanie) ;
- L'enseignement supérieur (ex. Université de Stanford) ;
- Les infrastructures IT critiques, notamment celles utilisant des équipements SonicWall.

Cela démontre une stratégie opportuniste, appuyée par une bonne connaissance des failles techniques exploitables.

## 6.2.6 Appui des recommandations par les sources expertes

Les recommandations formulées dans cette étude rejoignent celles émises par SonicWall, CERT-FR et Arctic Wolf, confirmant leur pertinence et leur urgence :

- **Application immédiate des correctifs de sécurité** pour la vulnérabilité CVE-2024-40766.
- **Activation de l'authentification multifactorielle (MFA)** pour les accès VPN.
- **Surveillance des journaux d'accès VPN** et des comportements suspects.
- **Isolation rapide** des systèmes compromis.
- **Sensibilisation des utilisateurs** face aux campagnes de phishing et aux vecteurs de loaders malveillants.

## 6.2.7 Recommandations de sécurité

À la suite de l'analyse de la menace Akira et de l'exploitation active de la CVE-2024-40766, les recommandations suivantes ont été formulées. Elles sont organisées selon les étapes classiques de gestion d'incident : qualification, remédiation, durcissement, et supervision.

### 6.2.7.1 Qualification et investigation

- **Identifier précisément l'équipement compromis** (poste utilisateur, serveur, équipement matériel dédié).
- **Analyser l'activité durant la période d'infection présumée** (horodatage des connexions, journaux d'accès).
- **Recenser les accès, comptes, secrets et permissions associés**, notamment au sein de l'annuaire Active Directory.
- **Rechercher des signes de compromission latérale** sur l'ensemble du système d'information, avec un focus sur les comptes à privilèges.
- **Analyser les logs VPN SonicWall** afin de détecter d'éventuels accès malveillants via l'exploitation de la CVE-2024-40766.

### 6.2.7.2 Remédiation

- **Isoler immédiatement** tout équipement suspect ou compromis pour éviter la propagation.
- **Conserver les éléments techniques utiles à une enquête judiciaire** (si dépôt de plainte envisagé).
- **Réinstaller ou remplacer les machines compromises** en évitant toute restauration non vérifiée.
- **Appliquer en urgence les correctifs de sécurité SonicWall**, notamment pour les versions vulnérables.
- **Changer tous les mots de passe et secrets associés aux comptes affectés.**
- **Désactiver temporairement les services SSL VPN vulnérables**, jusqu'à mise à jour complète.
- **Activer l'authentification multifacteur (MFA)** pour tous les accès distants, en particulier VPN.

### 6.2.7.3 Durcissement de la sécurité

- **Bloquer l'exécution de fichiers dans les répertoires inscriptibles par les utilisateurs** (ex. AppData, Downloads).
- **Restreindre les privilèges administrateurs locaux** aux seuls cas nécessaires, avec traçabilité.
- **Segmenter les communications inter-postes** à l'aide de règles de pare-feu local ou de Private VLAN.
- **Déployer LAPS (Local Administrator Password Solution)** pour gérer automatiquement les mots de passe locaux.
- **Renforcer le filtrage des flux e-mail et web** (contrôle des pièces jointes, des URL, sandboxing).
- **Bloquer les connexions VPN depuis des plages IP douteuses**, notamment celles de VPS publics.

### 6.2.7.4 Supervision renforcée

- **Détecter toute exécution anormale** à partir de chemins utilisateurs non standards (T1086 – PowerShell, T1059 – Command Shell).
- **Activer une surveillance proactive des alertes EDR et antivirus**, avec seuils d'alerte adaptés.
- **Garantir une couverture complète des postes et serveurs avec un EDR/antivirus à jour.**
- **Surveiller activement les connexions VPN SonicWall** (horaires inhabituels, géolocalisation anormale, volumes de données).
- **Mettre en place une corrélation des logs réseau, systèmes et EDR**, pour détecter les enchaînements d'attaques (kill chain).

Ces recommandations visent à couvrir l'ensemble du cycle de vie de l'attaque : de la détection initiale jusqu'au durcissement post-incident. Elles s'inscrivent dans une logique de défense en profondeur, combinant techniques de prévention, détection et réponse à incident.



### 6.2.7.5 Recommandations renforcées ( Prévention et défense contre Akira )

Face à la sophistication croissante des attaques Akira et l'exploitation active de vulnérabilités critiques comme CVE-2024-40766 (SonicWall), il est essentiel d'adopter une posture de sécurité proactive, axée sur l'anticipation, la résilience, et la détection rapide.

#### 1. Renforcement des accès à distance (SSL VPN / SonicWall)

- Appliquer immédiatement les correctifs fournis par SonicWall, en particulier sur les appliances Gen 5, 6 et 7 vulnérables.
- Désactiver temporairement les services SSL VPN en attente de correctif si l'organisation le permet.
- Mettre en place l'authentification multifacteur (MFA) pour tous les accès VPN.
- Filtrer les connexions VPN provenant de services d'hébergement (VPS, datacenters, etc.), souvent utilisés par les attaquants.

#### 2. Hygiène des identifiants et supervision des connexions

- Changer immédiatement tous les mots de passe utilisateurs SSL VPN, surtout s'ils sont stockés localement.
- Activer une journalisation détaillée des connexions distantes (horaires, IP, durée).
- Mettre en place des alertes sur tentatives de connexion anormales ou massives (brute force, credential stuffing).
- Superviser les comptes inactifs ou rarement utilisés, souvent ciblés dans les campagnes Akira.

#### 3. Protection contre les loaders malveillants (BumbleBee, IcedID, Pikabot...)

- Bloquer l'exécution de fichiers dans les répertoires utilisateur temporaires (%AppData%, %Temp%, etc.).
- Renforcer la sécurité des postes avec des EDR/antivirus à jour et capables de détecter des comportements anormaux (commandes PowerShell, beaconing réseau, etc.).
- Sensibiliser les utilisateurs aux phishing ciblés et malwares véhiculés par email.

#### 4. Segmentation et surveillance du réseau

- Mettre en œuvre une segmentation forte (zones de confiance, pare-feux internes, PVLAN) pour limiter la latéralisation post-infection.
- Bloquer les protocoles non nécessaires (SMBv1, RDP en clair...).
- Déployer une détection de compromission basée sur les comportements MITRE ATTACK : Akira est souvent associé aux techniques T1059 (Command Shell), T1021 (Remote Services), T1566 (Phishing), etc.

#### 5. Plans de réponse et continuité

- Élaborer ou réviser un plan de réponse aux incidents (PRI) incluant les rançongiciels.
- Maintenir des sauvegardes hors ligne, testées et vérifiées, déconnectées du SI principal.
- Organiser des exercices de simulation d'attaque ransomware (tabletop ou technique) pour tester les réflexes des équipes.

## 7. Sources officielles

CERT-FR – Alerte sur SonicWall (CVE-2024-40766)

<https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-011/>

CISA – Alerte conjointe sur Akira ransomware (avril 2024)

<https://www.cisa.gov/news-events/alerts/2024/04/18/cisa-and-partners-release-advisory-akira-ransomware>

CVE-2024-40766 – Improper Access Control dans SonicWall SonicOS

<https://www.cve.org/CVERecord?id=CVE-2024-40766>

### Analyses techniques / rapports de sécurité

Arctic Wolf Labs – Rapport sur la campagne Akira via SonicWall VPN

<https://www.bleepingcomputer.com/news/security/surge-of-akira-ransomware-attacks-hits-sonicwall-firewall-devices/>

Bulletin de sécurité SonicWall SNWLID-2024-0015

<https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015>

Cadres de référence et documentation technique

MITRE ATTACK – Akira ransomware (ID : S1129)

<https://attack.mitre.org/software/S1129/>

### Sources spécifiques à Akira et SonicWall

CERT-FR – Alerte CERTFR-2024-ALE-011

<https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-011/>

SonicWall – Bulletin de sécurité SNWLID-2024-0015

<https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015>

CVE-2024-40766 – Improper Access Control dans SonicOS

<https://www.cve.org/CVERecord?id=CVE-2024-40766>

NVD – National Vulnerability Database (fiche CVE-2024-40766)

<https://nvd.nist.gov/vuln/detail/CVE-2024-40766>

CISA – Alerte sur Akira ransomware (avril 2024)

<https://www.cisa.gov/news-events/alerts/2024/04/18/cisa-and-partners-release-advisory-akira-ransomware>

MITRE ATT&CK – Akira ransomware (S1129)

<https://attack.mitre.org/software/S1129/>

Arctic Wolf Labs et Campagne VPN contre SonicWall

<https://www.bleepingcomputer.com/news/security/surge-of-akira-ransomware-attacks-hits-sonicwall-firewall-devices/>

### Veille générale et outils de référence

#### Bases de données de vulnérabilités

CVE – Common Vulnerabilities and Exposures

<https://cve.mitre.org/>

NVD – National Vulnerability Database

<https://nvd.nist.gov/>

### **Sites officiels de cybersécurité**

CERT-FR – France

<https://www.cert.ssi.gouv.fr/>

CISA – États-Unis

<https://www.cisa.gov/>

ANSSI – Agence Nationale de la Sécurité des Systèmes d'Information (France)

<https://www.ssi.gouv.fr/>

NIST Cybersecurity Framework – États-Unis

<https://www.nist.gov/cyberframework>

ENISA – Europe

<https://www.enisa.europa.eu/>

### **Médias spécialisés**

The Hacker News

<https://thehackernews.com/>

BleepingComputer – Dossiers ransomware

<https://www.bleepingcomputer.com/tag/ransomware/>

### **Rapports et publications techniques**

MITRE ATT&CK Framework

<https://attack.mitre.org/>

CISA Publications & Advisories

<https://www.cisa.gov/publications-library>

ENISA Reports

<https://www.enisa.europa.eu/publications>

### **Blogs et rapports de fournisseurs de cybersécurité**

Microsoft Security Blog

<https://www.microsoft.com/security/blog/>

Palo Alto Networks – Unit 42 Threat Intelligence

<https://unit42.paloaltonetworks.com/>

CrowdStrike – Intelligence Reports

<https://www.crowdstrike.com/resources/reports/>

### **Réseaux professionnels & communautés cyber**

Club EBIOS – Analyse de risque

<https://club-ebios.fr/>

CLUSIF – Club de la Sécurité de l'Information Français

<https://clusif.fr/>

CLUSIR – Réseaux régionaux de sécurité

<https://clusir.org/>

Club 27001 – Groupe ISO/IEC 27001  
<https://club27001.fr/>

