NOTE DE SECURITE

Objet	Informations sur le groupe Qilin (alias Agenda), ransomware vendu en service (RaaS)
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-NDS-018
TLP	**GREEN**

Résumé

Qilin (alias Agenda) est un ransomware vendu en service (RaaS) à des affiliés, actif depuis 2022 et parmi les plus prolifiques en 2026. Il pratique la double extorsion : vol des données puis chiffrement.
En octobre 2026, Palo Alto a confirmé que Qilin exploite la faille CVE-2026-0257 (VPN GlobalProtect) pour contourner le MFA et entrer dans les réseaux. Les attaquants visent ensuite la virtualisation (vCenter, ESXi) et les sauvegardes (Veeam).
Qilin reste le groupe de ransomware le plus actif en 2026. Les chiffres varient selon les sources, car ils reposent sur les revendications publiées sur son site de fuite.

Liste des Indicateurs de compromission (IoC) relatifs au ransomware Qilin, à examiner : cf fichier joint

Risque de sécurité

- Arrêt de l'activité : chiffrement des serveurs, des postes et des machines virtuelles
- Fuite de données : publication des données volées si la rançon n'est pas payée
- Perte des sauvegardes : Veeam est ciblé pour empêcher toute restauration
- Vol d'identifiants : comptes VPN, administrateurs et domaine compromis
- Contournement de la sécurité : MFA contourné, EDR désactivé par pilote vulnérable (BYOD)

Systèmes cibles

- Palo Alto PAN-OS / GlobalProtect / Prisma Access : CVE-2026-0257 (contournement d'authentification VPN)
- Veeam Backup & Replication : CVE-2023-27532 et vol d'identifiants
- VMware ESXi / vCenter : CVE-2024-37085 et chiffreur dédié ESXi
- VPN et RDP exposés : Identifiants volés ou achetés
- Outils d'accès distant (ScreenConnect, AnyDesk, Atera) : pour la persistance

Recommandations

1. **Appliquer les correctifs : PAN-OS (CVE-2026-0257), Veeam, ESXi**
2. Rechercher les IoC (hash, IP, domaines) dans les logs des 90 derniers jours
3. Bloquer les IoC: hash sur l'EDR, IP sur le pare-feu (entrée et sortie), domaines sur DNS et proxy
4. Vérifier les connexions VPN suspectes et changer les mots de passe VPN et admin
5. Activer un MFA résistant au phishing sur VPN et accès d'administration
6. Supprimer les outils d'accès distant non autorisés
7. Isoler Veeam, vCenter et ESXi sur un réseau d'administration dédié
8. Garder une sauvegarde hors ligne ou immuable et tester la restauration
9. Sensibiliser les utilisateurs aux faux CAPTCHA (« collez cette commande »)
10. En cas de détection : prendre les premières de sécurité idoines et informer la DCSSI (CNOC)

ANNEXE 1 : Mode Opératoire

1. **Accès initial** : faille VPN (CVE-2026-0257), identifiants volés ou achetés, phishing par faux CAPTCHA.
2. **Persistance** : installation d'outils d'accès distant (ScreenConnect, AnyDesk, Atera).
3. **Vol d'identifiants** : extraction de la base Active Directory, parfois depuis le disque virtuel du contrôleur de domaine.
4. **Mouvement latéral** : RDP, SMB et PsExec vers les serveurs, puis vCenter et ESXi.
5. **Contournement** : désactivation de l'EDR par pilote vulnérable (BYOVD), effacement des journaux Windows.
6. **Exfiltration** : copie des données vers le cloud (Rclone vers MEGA).

Impact : suppression des clichés et sauvegardes, puis chiffrement des postes, serveurs et VM.

ANNEXE 2 : MAPPING MITRE ATT&CK

Tactique	Technique	ID
Accès initial	Exploitation d'application exposée	T1190
	Comptes valides	T1078
	Services distants externes (VPN)	T1133
Exécution	Exécution par l'utilisateur (faux CAPTCHA)	T1204
	PowerShell	T1059.001
Persistance	Logiciel d'accès à distance	T1219
Élévation de privilèges	Exploitation (pilote vulnérable)	T1068
Évasion	Désactivation des outils de sécurité	T1562.001
	Effacement des journaux Windows	T1070.001
Accès aux identifiants	Extraction NTDS	T1003.003
Mouvement latéral	RDP / partages SMB	T1021.001 / T1021.002
Exfiltration	Exfiltration vers stockage cloud	T1567.002
Impact	Arrêt de services / VM	T1489
	Inhibition de la restauration	T1490
	Chiffrement des données	T1486