CYBERCLAN™

Rapport sur les menaces du T2 2026

Introduction

Le paysage des menaces du T2 2026 se caractérise par une évolution vers des attaques plus rapides et plus efficaces reposant sur des accès fondés sur la confiance plutôt que sur l'exécution traditionnelle de maliciels. Les acteurs de menace exploitent de plus en plus l'infrastructure de périphérie et les systèmes d'identité, en tirant parti de services exposés à Internet qui n'ont pas reçu de correctifs, d'identifiants compromis et de l'utilisation abusive de sessions afin d'obtenir un accès et de mener leurs activités en limitant au minimum leur détection.

Parallèlement, les opérations de rançongiciel continuent d'évoluer vers des modèles d'extorsion axés sur les données, qui privilégient l'exfiltration rapide plutôt que le chiffrement. En raison de l'augmentation des risques dans les environnements de développement et les flux de travail automatisés, les acteurs de menace ciblent des systèmes offrant un important effet de levier susceptibles de causer des dommages immédiats et généralisés.

Dans l'ensemble de ces tendances, la principale caractéristique du T2 est la rapidité et la précision : les cybercriminels enchaînent les faiblesses touchant la périphérie, les identités et la visibilité afin de passer de l'accès à l'impact dans des délais de plus en plus courts. Le présent rapport décrit les principales évolutions, les menaces émergentes et les priorités en matière de défense pour faire face à ce paysage en constante évolution.

Pleins feux sur un acteur de menace : The Gentlemen

Aperçu

The Gentlemen est une opération de RaaS (rançongiciel en tant que service) qui a rapidement gagné en importance, au point de devenir l'un des principaux acteurs de menace du paysage mondial des rançongiciels au cours du premier semestre de 2026. Détectée pour la première fois en juillet-août 2025, elle est rapidement passée d'une opération fermée à une plateforme hautement évolutive axée sur les affiliés, prenant ainsi la relève d'opérateurs plus anciens ayant fait l'objet de perturbations.

Au début de 2026, The Gentlemen avait atteint un nombre considérable de victimes et démontré une maturité opérationnelle, confirmant ainsi son statut de menace persistante.

Les principales caractéristiques de The Gentlemen comprennent :

- Rythme opérationnel élevé
- Modèle économique évolutif pour les affiliés
- Capacités avancées de déplacement latéral
- Ciblage multiplateforme

Ce modèle moderne de rançongiciel illustre le passage de campagnes manuelles à des opérations d'extorsion automatisées et très rapides, faisant de The Gentlemen une menace critique que les organisations doivent comprendre et contre laquelle elles doivent se défendre en 2026.

Nombre total de victimes	Victimes en 2026 (à ce jour)	Pays touchés
504	424	75

Vecteurs d'infection connus

- Identifiants compromis
- Exploitation d'applications exposées au public
- Hameçonnage
- Accès au moyen du protocole de bureau à distance (RDP)
- Utilisation abusive des accès RPV

Cinq principaux pays

1. États-Unis
2. Thaïlande
3. Brésil
4. Royaume-Uni
5. France

Cinq principaux secteurs

1. Fabrication
2. Technologie
3. Services aux entreprises
4. Soins de santé
5. Services aux consommateurs

Mise à jour du paysage des menaces

Au T2 2026, le paysage mondial des menaces se caractérise par des volumes d'attaques élevés et des flux de travail optimisés chez les cybercriminels, qui privilégient désormais la compromission rapide, les accès pouvant être déployés à grande échelle et l'extorsion fondée sur les données plutôt que les méthodes traditionnelles. L'écosystème des rançongiciels passe de la fragmentation à la consolidation, un nombre plus restreint de groupes plus compétents étant responsable de la majorité des activités. De plus, les acteurs de menace ciblent de plus en plus les systèmes d'identité, l'infrastructure de périphérie et les environnements de développement, en se concentrant sur des points d'entrée offrant un important effet de levier et sur l'exploitation fondée sur la confiance.

Principales évolutions

Consolidation de l'écosystème et maturité du RaaS : À la suite de la perturbation de grands groupes de

rançongiciels au cours des années précédentes, le T2 montre un net mouvement de reconsolidation autour d'un nombre plus restreint d'opérateurs dominants. Les plateformes modernes de RaaS sont mieux structurées et plus évolutives, attirant des affiliés expérimentés et permettant des opérations constantes à volume élevé.

Passage à des modèles d'extorsion axés sur les données : Les acteurs de menace renoncent de plus en plus au chiffrement au profit de campagnes reposant uniquement sur l'exfiltration de données et l'extorsion. Cette approche réduit la complexité opérationnelle et le risque de détection, tout en maximisant la pression exercée sur les victimes en tirant parti des conséquences réglementaires, juridiques et réputationnelles.

L'infrastructure de périphérie comme principal point d'entrée : Les systèmes exposés à Internet, notamment les équipements RPV, les pare-feu et les services d'accès à distance, demeurent les actifs les plus ciblés. Les acteurs de menace exploitent activement les vulnérabilités et les mauvaises configurations de ces systèmes afin d'accéder aux environnements d'entreprise sans authentification ou au moyen d'identifiants.

Expansion des attaques fondées sur l'identité : Les systèmes d'identité sont devenus une surface d'attaque centrale, les cybercriminels tirant parti des éléments suivants :

- Identifiants volés par des logiciels voleurs d'information
- Détournement de sessions ou de jetons
- Techniques de contournement de l'authentification

Cette évolution permet aux acteurs de menace de contourner les défenses traditionnelles des points de terminaison et d'agir au moyen d'accès légitimes.

Industrialisation de l'accès initial : L'écosystème des courtiers en accès initial (IAB) continue de se développer, fournissant aux groupes de rançongiciels des environnements déjà compromis. Cette banalisation de l'accès permet aux acteurs de menace d'étendre leurs opérations et de réduire le délai avant l'impact, accélérant ainsi les attaques.

Accélération du déroulement des attaques : Les cybercriminels optimisent leurs opérations en vue d'une exécution rapide, de nombreuses attaques passant de l'accès initial au déplacement latéral et à l'impact en quelques heures. L'automatisation, les guides opérationnels réutilisables et les outils banalisés réduisent la dépendance à l'égard des opérations manuelles.

Risque croissant dans les environnements de développement et les chaînes d'approvisionnement logicielles : Les systèmes de développement, les pipelines CI/CD et les écosystèmes logiciels sont de plus en plus ciblés en raison de leur capacité à fournir un accès étendu à l'organisation ainsi qu'aux systèmes en aval. Les acteurs de menace exploitent les flux de travail fondés sur la confiance et les fonctions d'automatisation plutôt que les vulnérabilités traditionnelles.

Résumé

Le paysage des menaces du T2 2026 met en évidence la poursuite de l'évolution vers une cybercriminalité axée sur l'efficacité, dans laquelle les acteurs de menace privilégient :

- La rapidité plutôt que la persistance
- L'accès plutôt que l'exploitation de vulnérabilités
- Les données plutôt que la perturbation

Ces changements redéfinissent la manière dont les organisations doivent aborder la détection et la défense, en mettant davantage l'accent sur la sécurité des identités, la protection de la périphérie et la surveillance des systèmes et des flux de travail présentant un niveau de confiance élevé.

Tendances émergentes en matière de menaces

La surface d'attaque des « environnements de développement »

Au T2 2026, l'attention se porte sur le cycle de vie du développement logiciel, les acteurs de menace ciblant les environnements de travail des développeurs, les environnements de développement intégrés (IDE) et les pipelines CI/CD. Cette évolution s'explique par la valeur de l'accès au code source, aux pipelines de compilation et aux identifiants infonuagiques. Les techniques d'attaque exploitent désormais les scripts post-installation, la configuration des IDE et les interactions avec des dépôts de confiance, permettant une exécution de code fondée sur des flux de travail légitimes qui contourne les défenses classiques.

Utilisation abusive des outils de développement assisté par IA

L'essor des assistants de programmation fondés sur l'IA entraîne de nouveaux risques, puisqu'environ 97 % des équipes de développement utilisent ces outils avec une gouvernance limitée. Les cybercriminels exploitent les intégrations de l'IA avec les plateformes, les jetons d'authentification et les fonctions d'exécution automatisée, facilitant des attaques telles que l'interception OAuth et l'exécution silencieuse de code. Les menaces visant la chaîne d'approvisionnement des outils d'IA indiquent une tendance vers une « exécution fondée sur la confiance », dans laquelle la légitimité prime sur l'exploitation de vulnérabilités.

Passage à des opérations reposant uniquement sur l'extorsion

Les rançongiciels ont évolué vers une extorsion fondée uniquement sur les données, 22 % des incidents de 2026 ne comportant pas de chiffrement. Les acteurs de menace exfiltrent des données sensibles, menacent de les divulguer et contournent les stratégies de reprise, ce qui réduit la complexité et accélère l'exécution.

L'infrastructure de périphérie comme cible principale

Les cybercriminels ciblent de plus en plus les systèmes de périphérie exposés à Internet, comme les RPV et les pare-feu, en exploitant les vulnérabilités d'appareils dont les correctifs ne sont pas à jour. Cette évolution vise à contourner les défenses des points de terminaison et à accéder à des systèmes hautement privilégiés.

L'automatisation et la rapidité comme principaux moteurs des attaques

Les menaces modernes mettent l'accent sur l'automatisation, les acteurs de menace utilisant des outils préétablis pour effectuer rapidement des déplacements latéraux et procéder à une exécution rapide. Les repères avancés en matière de détection témoignent de l'urgence d'intervenir en quelques heures.

Résumé

Les menaces émergentes du T2 2026 illustrent une transition vers l'exploitation de surfaces à forte valeur, notamment les environnements de développement, les outils d'IA et l'infrastructure de périphérie, parallèlement à des modèles d'extorsion axés sur les données. Les cybercriminels privilégient la rapidité, l'exploitation de la confiance et l'automatisation plutôt que la persistance et les vulnérabilités traditionnelles.

Tendances relatives à l'exploitation des vulnérabilités

Principales vulnérabilités activement exploitées

Au T2 2026, un petit nombre de vulnérabilités à fort impact sont exploitées par des opérateurs de rançongiciels et des acteurs de menace opportunistes, touchant particulièrement l'infrastructure de périphérie, les mécanismes d'authentification, les services Web et les plateformes mobiles. On observe une tendance marquée à l'exploitation rapide des vulnérabilités, notamment avant la publication de correctifs et dans des scénarios de jour zéro, les cybercriminels se concentrant sur les faiblesses liées à l'identité et sur l'exposition externe des systèmes.

Vulnérabilités les plus importantes :

CVE-2026-50751 — Contournement de l'authentification des RPV de Check Point (jour zéro)

- Cette vulnérabilité critique permet un accès non autorisé aux RPV d'accès à distance de Check Point utilisant les anciens protocoles IKEv1.
- Une exploitation active a été observée en mai et en juin 2026, notamment en lien avec des affiliés du rançongiciel Qilin.

Principal constat : Les protocoles anciens et les RPV mal configurés présentent un risque élevé d'attaques par rançongiciel.

CVE-2026-0257 — PAN-OS de Palo Alto Networks (GlobalProtect)

- Une faille de gravité élevée permettant le détournement de sessions par le déchiffrement de témoins, contournant ainsi les contrôles d'authentification.
- Ajoutée au catalogue KEV de la CISA en mai 2026 et probablement utilisée par des courtiers en accès initial.

Principal constat : Les vulnérabilités liées aux identités sont de plus en plus exploitées afin de contourner l'AMF.

CVE-2026-49975 — Vulnérabilité de déni de service multifournisseur « HTTP/2 Bomb »

- Vulnérabilité critique de déni de service touchant plusieurs serveurs Web (NGINX, Apache, IIS, etc.) en raison de failles dans le traitement des requêtes HTTP/2.
- Divulguée en juin 2026, elle présente des risques systémiques pour diverses applications.

Principal constat : Les vulnérabilités de protocole touchant plusieurs fournisseurs peuvent entraîner des perturbations à grande échelle.

CVE-2025-48595 — Élévation des privilèges dans le cadriciel Android (Android Framework) (jour zéro)

- Une vulnérabilité locale d'élévation des privilèges sans interaction touchant Android 14 à 16 et permettant d'obtenir des privilèges accrus sur les appareils.
- Ajoutée au catalogue KEV de la CISA en juin 2026, elle cible les parcs d'appareils mobiles d'entreprise.

Principal constat : Les plateformes mobiles constituent souvent des surfaces d'attaque insuffisamment surveillées dans les environnements AVAP (apportez votre appareil personnel).

Campagnes d'exploitation émergentes

Au T2 2026, des campagnes d'exploitation non traditionnelles sont apparues parallèlement aux méthodes classiques fondées sur les CVE. Un exemple notable est la campagne Miasma, également appelée Mini Shai-Hulud, qui cible l'écosystème de développement logiciel en compromettant des dépôts GitHub de confiance, notamment ceux liés à Microsoft Azure.

Principales caractéristiques :

- Comportement de ver à propagation autonome, qui se diffuse dans les dépôts et les environnements de développement
- Exploitation de la confiance accordée au code source ouvert plutôt que de vulnérabilités logicielles traditionnelles
- Incidence sur les flux de travail modernes utilisant des outils de programmation assistée par IA et des environnements de développement intégrés (IDE)

Mécanisme d'exécution :

- Activation de code malveillant lorsqu'un développeur ouvre un dépôt compromis
- Utilisation des éléments suivants :
  - Scripts post-clonage
  - Exécution de dépendances
  - Intégrations d'outils

Impact :

- Facilite l'exécution immédiate de code dans des environnements de confiance
- Compromet les postes de travail des développeurs, les pipelines CI/CD et les chaînes d'approvisionnement logicielles

Principal constat : Cette campagne met en évidence une évolution vers des surfaces d'attaque centrées sur les développeurs, dans lesquelles la confiance et les outils d'automatisation peuvent être exploités afin de permettre des compromissions à grande échelle.

Résumé des principales vulnérabilités

Catégorie	Exemple	Type de risque
Infrastructure de périphérie	CVE-2026-50751	Accès initial (rançongiciel)
Pile Web	HTTP/2 Bomb	Déni de service / perturbation de service
RPV/authentification	CVE-2026-0257	Compromission d'identité
Écosystème de développement	Ver Miasma	Chaîne d'approvisionnement / exécution de code
Mobile	CVE-2025-48595	Élévation des privilèges

Stratégies de défense et recommandations

Les organisations devraient accorder la priorité aux mesures de défense qui réduisent l'exposition de l'infrastructure de périphérie, des systèmes d'identité et des environnements de développement logiciel, car il s'agit des points d'entrée les plus régulièrement exploités ce trimestre.

Renforcement de l'infrastructure de périphérie

Les systèmes exposés à Internet demeurent le point d'entrée présentant le risque le plus élevé et doivent être traités comme des actifs de sécurité critiques.

Mesures prioritaires :

- Appliquer des correctifs d'urgence aux éléments suivants :
  - RPV
  - Pare-feu

    - Plateformes d'accès à distance
    - Passerelles d'authentification
- Désactiver les protocoles anciens ou non sécurisés (p. ex. les configurations RPV obsolètes)
- Restreindre l'accès d'administration aux éléments suivants :
    - Réseaux de confiance
    - Voies d'accès privilégié
- Limiter autant que possible l'exposition directe à Internet

Principal constat : Les appareils de périphérie doivent être gérés comme des actifs de niveau 0 (Tier 0) et non comme une infrastructure courante, en raison de leur rôle dans la compromission initiale.

Renforcement de la sécurité des identités et des accès

Les acteurs de menace s'appuient de plus en plus sur des identifiants valides et le détournement de sessions, faisant de l'identité le nouveau périmètre.

Contrôles recommandés :

- Imposer une AMF résistante à l'hameçonnage (p. ex. FIDO2 lorsque c'est possible)
- Mettre en œuvre et auditer régulièrement les politiques d'accès conditionnel
- Renforcer les contrôles des accès privilégiés (principe du moindre privilège, accès juste-à-temps)
- Surveiller les éléments suivants :
    - Utilisation abusive de jetons ou de sessions
    - Déplacements impossibles
    - Schémas de connexion anormaux
- Éliminer ou réduire le recours aux méthodes d'authentification anciennes

Principal constat : La détection doit porter sur la manière dont les identités sont utilisées, et non uniquement sur la présence éventuelle de maliciels.

Détection de la préparation et de l'exfiltration des données

Avec l'essor de l'extorsion sans chiffrement, la détection précoce des mouvements de données est essentielle.

Principaux éléments à surveiller :

- Schémas inhabituels d'accès aux fichiers, en matière de volume ou de sensibilité
- Création d'archives ou de répertoires de préparation des données
- Téléchargements massifs ou accès en masse aux données
- Modifications apportées aux éléments suivants :
    - Paramètres de partage externe
    - Autorisations d'accès
- Pointes de trafic réseau sortant

Indicateurs contextuels à mettre en corrélation :

- Sessions récentes d'accès à distance
- Activités d'élévation des privilèges
- Anomalies liées aux identités ou connexions suspectes

Principal constat : Les stratégies de détection doivent aller au-delà de l'exécution des rançongiciels afin de repérer les comportements précédant l'exfiltration.

Sécurisation des environnements de développement et des pipelines CI/CD

Les systèmes de développement représentent désormais des surfaces d'attaque à fort impact en raison de leur accès au code, aux identifiants et aux flux de travail de production.

Principaux éléments à sécuriser :

- Dépôts de code source et contrôles d'accès
- Gestion des clés d'API, des jetons et des secrets
- Vérification de la fiabilité des dépendances et des paquets
- Autorisations et politiques d'exécution des pipelines CI/CD

Contrôles recommandés :

- Surveiller les éléments suivants :
  - Modifications non autorisées des dépôts
  - Exécutions suspectes de pipelines
  - Anomalies dans les scripts post-installation ou de compilation
- Imposer les mesures suivantes :
  - Principe du moindre privilège pour l'accès aux pipelines
  - Signature du code et vérification des artéfacts
- Renforcer la gouvernance des éléments suivants :
  - Outils de développement assisté par IA
  - Flux de travail et scripts automatisés

Principal constat : La chaîne de production logicielle doit être considérée comme une infrastructure essentielle, et non comme une simple fonction de développement.

Adaptation des stratégies de détection et d'intervention

Les attaques modernes privilégient la rapidité, les accès légitimes et une exécution discrète, ce qui exige une évolution de l'approche défensive.

Approche recommandée :

- Privilégier la détection comportementale plutôt que les méthodes fondées sur les signatures
- Se concentrer sur les éléments suivants :
  - Indicateurs de déplacement latéral
  - Chaînes d'élévation des privilèges
  - Anomalies d'accès
- Réduire le délai moyen de détection (MTTD) et le délai moyen de confinement (MTTC) grâce aux éléments suivants :
  - Automatisation
  - Alertes en temps réel
- Partir du principe que les acteurs de menace peuvent :
  - Utiliser des outils légitimes
  - Éviter complètement de déployer des maliciels

Principal constat : Les organisations doivent passer de la détection des maliciels à la détection des comportements et au confinement rapide.

Résumé

Les priorités défensives du T2 2026 devraient être axées sur les éléments suivants :

- Renforcer l'infrastructure de périphérie afin de prévenir l'accès initial
- Sécuriser les systèmes d'identité afin d'empêcher l'utilisation abusive d'accès légitimes
- Détecter les activités d'exfiltration de données à un stade précoce

- Protéger les environnements de développement et les pipelines
- Adapter les stratégies de détection à des attaques plus rapides et plus furtives

Principaux constats finaux

Le T2 2026 a renforcé la transition fondamentale observée dans le comportement des cybercriminels : les acteurs de menace privilégient la rapidité, l'efficacité et les accès légitimes plutôt que les méthodes traditionnelles d'intrusion reposant largement sur les maliciels.

L'identité comme surface d'attaque principale

Les systèmes d'identité constituent désormais un point d'entrée principal, et non plus seulement une couche de contrôle.

Tendances observées :

- Utilisation accrue des éléments suivants :
  - Identifiants volés
  - Détournement de sessions
  - Techniques de contournement de l'authentification
- Recours réduit aux éléments suivants :
  - Accès initial fondé sur des maliciels
  - Exploitation des points de terminaison

Conséquence : Les acteurs de menace obtiennent un accès par des voies d'authentification légitimes, contournant souvent entièrement les défenses traditionnelles des points de terminaison.

Mesures efficaces ce trimestre

Les contrôles de sécurité fondamentaux se sont révélés les plus efficaces pour limiter l'impact.

Contrôles à fort impact :

- Hygiène rigoureuse des appareils de périphérie et application rapide des correctifs
- Segmentation du réseau limitant le déplacement latéral
- Renforcement de la gestion des accès privilégiés
- Visibilité accrue sur les éléments suivants :
  - Événements d'authentification
  - Activités d'accès à distance
  - Modifications apportées aux comptes privilégiés

Avantage en matière de détection : Les organisations qui surveillaient les comportements de connexion anormaux et les schémas d'utilisation abusive des identités étaient mieux à même de détecter les menaces avant qu'elles ne s'aggravent.

Changements observés ce trimestre

Plusieurs tendances liées aux menaces ont continué à s'intensifier et à se généraliser :

Principales évolutions :

- Généralisation de l'extorsion axée sur les données
- Ciblage accru des éléments suivants :
  - Environnements de développement
  - Chaînes d'approvisionnement logicielles
- Expansion des voies d'intrusion fondées sur l'identité

Évolution des modes opératoires :

- Les acteurs de menace :
  - Utilisent des identifiants valides plutôt que des codes d'exploitation
  - Tirent parti de sessions actives plutôt que de déployer des maliciels
  - Exploitent des flux de travail de confiance pour effectuer des déplacements latéraux

Conséquence : Les indicateurs traditionnels, comme les maliciels et les codes d'exploitation, ne sont plus nécessaires pour réaliser une compromission à fort impact.

Domaines où le risque augmente

Le risque découle de la combinaison de plusieurs points faibles, et non uniquement de vulnérabilités individuelles.

Facteurs de risque courants :

- Infrastructure de périphérie exposée ou sans correctifs
- Contrôles d'identité faibles ou mal configurés
- Visibilité insuffisante sur les sessions et les jetons
- Capacité limitée à détecter les activités d'exfiltration de données

Lacune critique :

- Les contrôles portent trop souvent uniquement sur les perturbations, sans prévenir ni détecter suffisamment le vol de données.

Conséquence : Le risque découle de plus en plus de l'interaction entre plusieurs lacunes de contrôle plutôt que d'une vulnérabilité unique.

Prochaines mesures à prendre par les organisations

Les efforts de défense devraient désormais viser à limiter la liberté de mouvement des acteurs de menace dans l'environnement.

Principales priorités pour le prochain trimestre :

Renforcer la sécurité des actifs exposés à Internet et en restreindre l'accès	
Renforcer les éléments suivants	• Protection des identités • Contrôle des sessions et des jetons
Améliorer la détection des éléments suivants	• Utilisation abusive des identités • Activités d'exfiltration à un stade précoce
Élargir la surveillance des éléments suivants	• Accès à distance • Comportement des comptes privilégiés
Appliquer des contrôles de sécurité conçus pour les environnements de production aux éléments suivants	• Environnements de développement • Pipelines CI/CD