

RÉSUMÉ

Acronis TRU Cyber Pulse 2026

Principales conclusions et implications en matière de sécurité

Acronis
Threat Research Unit



Les cyberattaques évoluent, augmentant à la fois la vitesse et la portée des intrusions.

Les acteurs malveillants utilisent des agents IA pour automatiser les processus d'attaque, exploitent des identités volées pour passer d'un service connecté à un autre et ciblent les mécanismes de sécurité afin de réduire les capacités de détection et de reprise.

Le premier rapport Acronis TRU Cyber Pulse 2026 rassemble les résultats des investigations menées par l'Acronis Threat Research Unit (TRU) sur les nouvelles techniques d'attaque, les activités d'espionnage et la cybercriminalité. Les conclusions révèlent une tendance commune : une compromission initiale peut donner accès à bien plus que l'appareil ou le compte touché.

Pour les fournisseurs de services managés (MSP), cela représente des risques particuliers. La compromission d'une identité disposant de privilèges d'administration, d'un outil de gestion à distance ou d'un service partagé peut exposer les environnements de plusieurs clients. Les organisations doivent donc comprendre non seulement comment les cybercriminels obtiennent un accès, mais aussi jusqu'où cet accès peut s'étendre.

Six conclusions permettent de définir le paysage des menaces étudié dans ce rapport.

1. Les agents IA décuplent l'ampleur des cyberattaques

Les acteurs malveillants ne se limitent plus à utiliser l'IA pour des tâches ponctuelles, comme la rédaction de messages de phishing ou l'analyse de vulnérabilités. Certains combinent des modèles d'IA avec des outils de sécurité offensive et des plateformes de messagerie. Grâce à une mémoire persistante, ces systèmes conservent le contexte et peuvent coordonner des attaques plus complexes.

L'enquête BOSSAI menée par l'Acronis TRU illustre cette évolution. Un seul opérateur a connecté plus de 10 modèles à des frameworks de sécurité offensive et à une infrastructure de soutien, permettant de coordonner la reconnaissance, l'exploitation des vulnérabilités et la gestion de l'infrastructure sur des cibles situées dans plusieurs pays.

Ces résultats montrent comment les systèmes agentiques peuvent réduire les efforts manuels nécessaires à la conduite d'opérations complexes.

L'adoption de l'IA crée également de nouvelles surfaces d'attaque. La TRU a identifié plus de 575 compétences malveillantes OpenClaw réparties sur 13 comptes de développeurs. Ces packages se faisaient passer pour des utilitaires légitimes tout en diffusant des malwares.

```
export ANTHROPIC_SMALL_FAST_MODEL="MiniMax-M3"
export ANTHROPIC_DEFAULT_SONNET_MODEL="MiniMax-M3"
export ANTHROPIC_DEFAULT_OPUS_MODEL="MiniMax-M3"
export ANTHROPIC_DEFAULT_HAIKU_MODEL="MiniMax-M3"
claude
export ANTHROPIC_BASE_URL="https://api.minimaxi.com/anthropic"
export ANTHROPIC_AUTH_TOKEN="sk-cp-[redacted]"
export API_TIMEOUT_MS="3000000"
export CLAUDE_CODE_DISABLE_NONESSENTIAL_TRAFFIC=1
export ANTHROPIC_MODEL="MiniMax-M3"
export ANTHROPIC_SMALL_FAST_MODEL="MiniMax-M3"
export ANTHROPIC_DEFAULT_SONNET_MODEL="MiniMax-M3"
export ANTHROPIC_DEFAULT_OPUS_MODEL="MiniMax-M3"
export ANTHROPIC_DEFAULT_HAIKU_MODEL="MiniMax-M3"
claude --model MiniMax-M3
export ANTHROPIC_BASE_URL="https://api.minimaxi.com/anthropic"
```

Claude Code redirigé via MiniMax.

Implications en matière de sécurité :

Les organisations doivent considérer les agents IA et les outils auxquels ils sont connectés comme des systèmes à privilèges. Les autorisations accordées aux agents, les extensions externes, les identifiants et les accès réseau doivent faire l'objet de mesures de sécurité et d'une surveillance spécifiques.

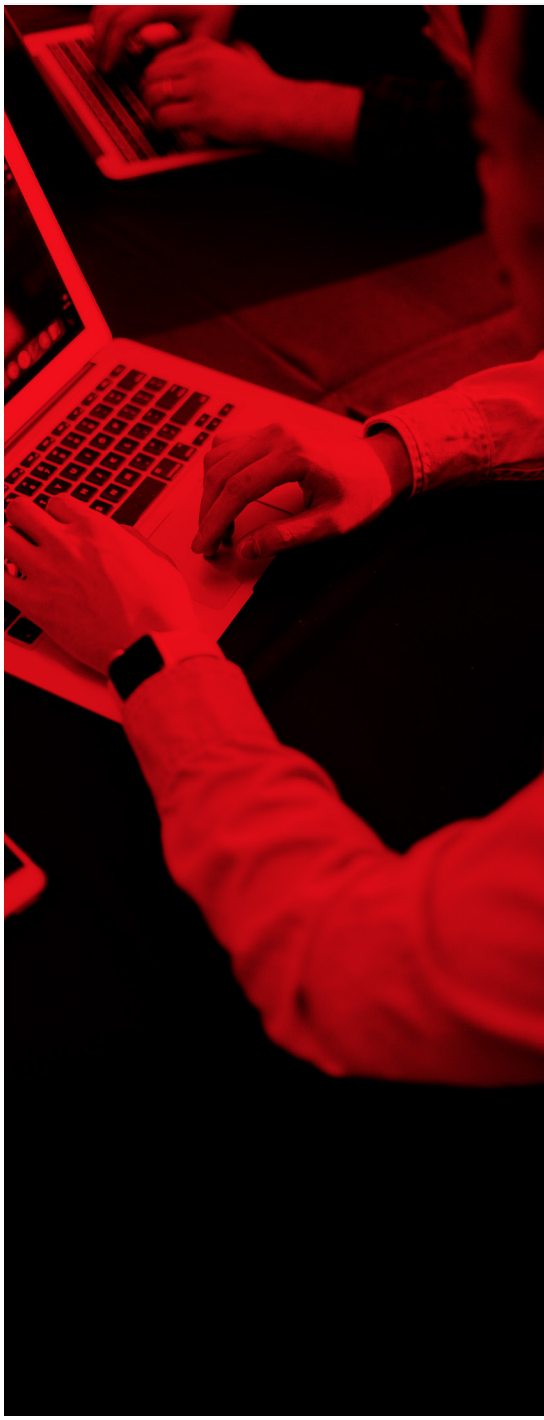
2. Les identités dérobées deviennent un vecteur majeur de compromission à grande échelle

Les infostealers et les attaques ciblant les identités visent de plus en plus les identifiants de connexion, les jetons d'authentification, les sessions de navigateur et les accès aux services cloud.

Les attaquants peuvent exploiter ces informations pour accéder à des applications et services connectés, parfois sans déclencher de nouvelle demande d'authentification multifacteur (MFA). Les accès volés peuvent également être transférés ou vendus à d'autres acteurs malveillants, notamment des gangs de ransomware et des groupes d'espionnage.

Les environnements de développement sont eux aussi exposés. Des investigations récentes ont mis en évidence des malwares ciblant les clés API de services IA, les identifiants d'accès aux dépôts de code et d'autres secrets utilisés dans le développement. Ces identifiants peuvent donner accès à d'autres systèmes et projets.

Pour les MSP, les identités disposant de privilèges élevés sont particulièrement recherchées, car elles peuvent donner accès aux environnements de plusieurs clients.



Implications en matière de sécurité :

La suppression des malwares ou la réinitialisation d'un mot de passe ne suffit pas. L'intervention sur incidents doit également prévoir la révocation des sessions exposées, le renouvellement des identifiants, la vérification des modifications apportées aux paramètres d'authentification et l'investigation des services connectés.

3. Les cybercriminels ciblent délibérément les mécanismes de sécurité et de restauration

La désactivation des outils de sécurité est devenue une étape importante des attaques informatiques modernes.

En avril 2026, MITRE ATT&CK a introduit la tactique Defense Impairment (altération des défenses) comme catégorie à part entière, afin de regrouper les actions visant à perturber délibérément les systèmes de défense.

Les investigations de l'Acronis TRU sur des opérations de ransomware, notamment celles de Qilin et The Gentlemen, montrent comment les cybercriminels peuvent arrêter des processus de sécurité, perturber la surveillance et neutraliser les mécanismes de restauration.

Ces actions peuvent réduire la visibilité des équipes de sécurité pendant que les cybercriminels se déplacent dans les réseaux, dérobent des informations ou préparent le chiffrement des systèmes.

Le risque est particulièrement élevé lorsque les cybercriminels prennent le contrôle de serveurs de gestion ou de comptes administrateurs utilisés dans plusieurs environnements.



Fond d'écran The Gentlemen

Implications en matière de sécurité :

Les organisations doivent surveiller de manière indépendante l'état de fonctionnement des agents de sécurité, les modifications apportées aux journaux d'activité ainsi que toute tentative de désactivation des protections. L'administration des sauvegardes doit être distincte de l'administration courante des systèmes. Enfin, les procédures de restauration doivent être testées dans des scénarios où les identifiants ou l'infrastructure ont été compromis.

4. Les services et logiciels de confiance sont détournés pour dissimuler les attaques

Les cybercriminels et les acteurs de l'espionnage utilisent de plus en plus des plateformes connues, comme GitHub, Telegram et des services de stockage cloud, pour diffuser des malwares ou communiquer avec des systèmes compromis.

Comme ces services sont également utilisés dans le cadre d'activités professionnelles légitimes, il peut être difficile de distinguer le trafic malveillant du trafic autorisé.

Les investigations de l'Acronis TRU ont mis en évidence la diffusion de malwares via des dépôts GitHub ainsi que l'utilisation de services cloud de confiance pour assurer les communications de commande et de contrôle.

La campagne TamperedChef a révélé une autre limite des mécanismes de confiance traditionnels. Les cybercriminels ont diffusé des applications malveillantes fonctionnelles dotées de certificats de signature de code valides. Cet exemple montre qu'une signature numérique valide ne garantit pas qu'un logiciel est sûr.

Implications en matière de sécurité :

Les organisations doivent évaluer les activités des applications et des services en tenant compte de leur contexte, plutôt que de se fier uniquement à la réputation des domaines ou aux signatures numériques. Tout téléchargement inattendu, toute activité inhabituelle via une API cloud ou toute connexion à distance à des fins de gestion doit faire l'objet d'une investigation, même lorsque ces activités impliquent des services connus.



5. Les opérations de ransomware s'adaptent aux perturbations et s'étendent au-delà de Windows

Les opérations menées par les forces de l'ordre peuvent perturber les infrastructures des cybercriminels, mais les outils et les compétences nécessaires à ces opérations peuvent rester disponibles.

Les recherches de l'Acronis TRU montrent que les cybercriminels affiliés à des groupes de ransomware, les codes sources divulgués et le partage de techniques d'attaque permettent aux groupes criminels de se réorganiser et de poursuivre leurs activités sous d'autres noms.

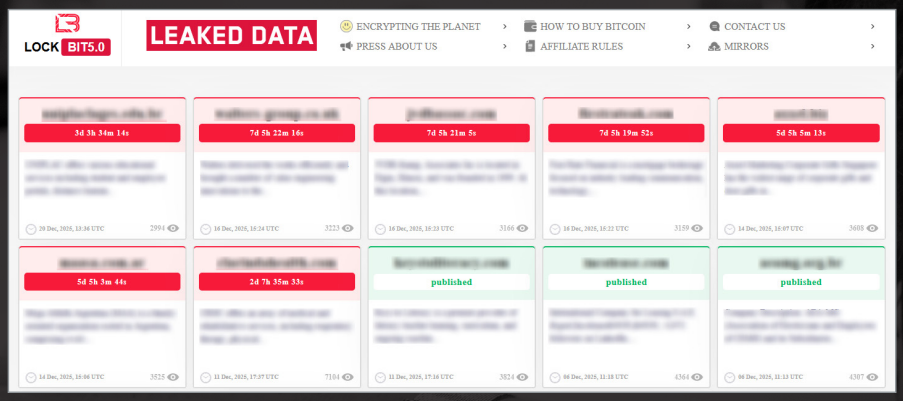
Les attaques par ransomware ciblent désormais un éventail plus large de systèmes.

LockBit 5.0 existe en plusieurs variantes compatibles avec Windows, Linux et VMware ESXi. Le ransomware INC a démontré sa capacité à cibler les environnements Linux et ESXi, tandis que Qilin a utilisé le sous-système Windows pour Linux (WSL) afin d'exécuter un programme de chiffrement Linux sous Windows.

En ciblant les infrastructures de virtualisation, les cybercriminels peuvent perturber plusieurs workloads à la fois et affecter des systèmes essentiels à la reprise d'activité des entreprises.

Implications en matière de sécurité :

Les mesures de protection contre les ransomwares doivent couvrir les hôtes Linux, les hyperviseurs et les outils de gestion des machines virtuelles. Les organisations doivent surveiller toute extinction inattendue de machines virtuelles et toute suppression de snapshots. Elles doivent également veiller à ce que l'infrastructure de restauration reste accessible en cas de compromission.



Site de divulgation de données de LockBit 5.0

6. L'exploitation des vulnérabilités et des relations de confiance étendent la portée des intrusions

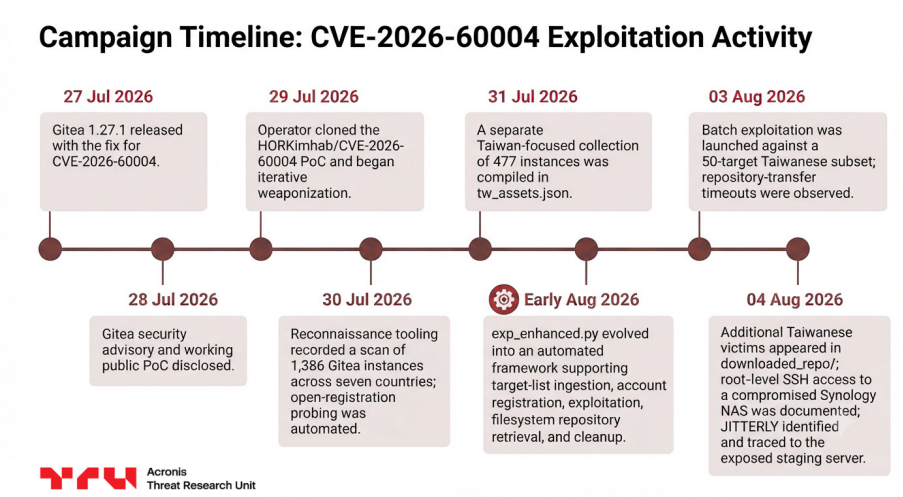
Les cybercriminels exploitent rapidement les vulnérabilités dès leur divulgation publique, réduisant ainsi le délai dont disposent les organisations pour déployer les correctifs de sécurité.

Dans le cadre de l'enquête Red Heron, les cybercriminels ont adapté un exploit disponible publiquement peu après la divulgation d'une vulnérabilité critique de Gitea. La compromission de serveurs de développement a exposé des dépôts de code et des identifiants susceptibles de faciliter d'autres intrusions.

Les investigations sur les activités d'espionnage ont révélé une tendance similaire : les acteurs malveillants exploitent de plus en plus les relations de confiance pour atteindre indirectement leurs cibles.

Les fournisseurs de services informatiques, les environnements de développement et les infrastructures de distribution logicielle peuvent servir de points d'accès à des organisations qu'il serait plus difficile de compromettre directement.

Ces attaques sont particulièrement lourdes de conséquences pour les MSP, car la compromission d'un seul service ou d'une seule identité peut exposer les environnements de plusieurs clients.



Implications en matière de sécurité :

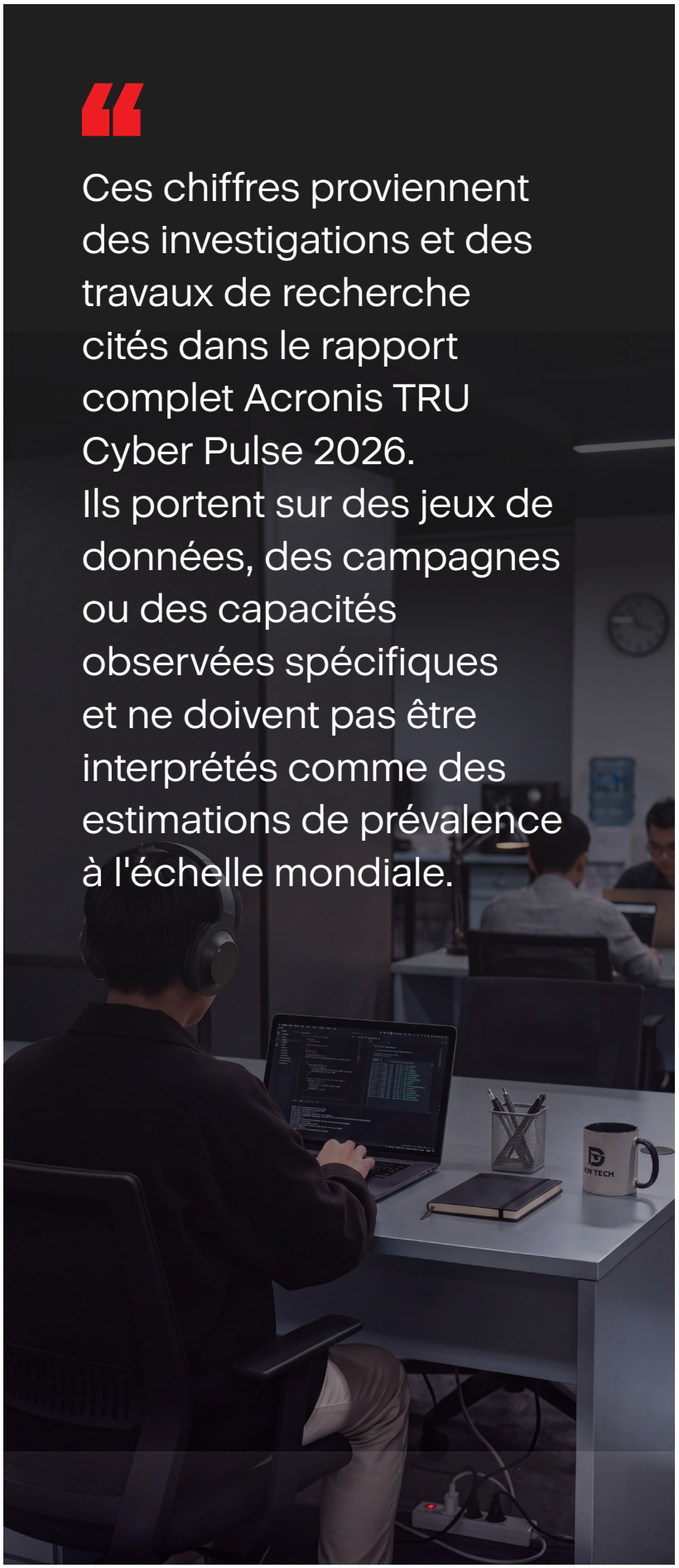
La gestion des vulnérabilités doit tenir compte du niveau d'accès qu'un système peut offrir, et pas uniquement de la gravité de la vulnérabilité. Après l'exploitation d'une vulnérabilité, les organisations doivent rechercher toute trace de maintien de l'accès, vérifier si des identifiants ont été volés et examiner les activités menées dans les environnements connectés.

Principaux résultats de l'étude

Les résultats présentés ci-dessous illustrent l'ampleur des activités documentées dans le rapport complet.

Résultat de l'étude | Éléments rapportés

- **Attaques assistées par l'IA :** BOSSAI a connecté plus de 10 modèles d'IA à des outils de sécurité offensive et à une infrastructure de soutien.
- **Menaces sur la chaîne d'approvisionnement de l'IA :** la TRU a identifié plus de 575 compétences malveillantes OpenClaw réparties sur 13 comptes de développeurs.
- **Exposition aux accès à distance :** sur plus de 1,8 million de terminaux équipés d'Acronis RMM analysés, 63,1 % disposaient d'au moins un autre outil RMM ou d'accès à distance.
- **Retards dans l'application des correctifs :** la TRU a relevé un délai médian de 5,7 jours pour l'application des correctifs aux applications tierces au second semestre 2025.
- **Extension des attaques par ransomware :** LockBit 5.0 comprend des variantes ciblant les environnements Windows, Linux et ESXi.



> Ces chiffres proviennent des investigations et des travaux de recherche cités dans le rapport complet Acronis TRU Cyber Pulse 2026. Ils portent sur des jeux de données, des campagnes ou des capacités observées spécifiques et ne doivent pas être interprétés comme des estimations de prévalence à l'échelle mondiale.

Priorités pour renforcer la cyberrésilience



Les résultats de l'étude mettent en évidence cinq priorités concrètes pour les MSP et les organisations qui souhaitent limiter l'impact des cyberattaques.

1. Limiter la portée des compromissions d'identités. Mettre en place une authentification résistante au phishing, restreindre les accès à privilèges et assurer une visibilité sur les sessions, les autorisations des applications et les connexions de gestion à distance.

2. Hiérarchiser les vulnérabilités en fonction de leur exposition et des accès qu'elles permettent. Accélérer la correction des vulnérabilités affectant les systèmes exposés à Internet et les systèmes d'administration, en particulier ceux qui contiennent des identifiants ou permettent d'accéder à d'autres environnements. En cas de suspicion d'exploitation, rechercher toute trace de maintien de l'accès et vérifier si des identifiants ont été exposés.

3. Détecter les tentatives de désactivation des protections. Surveiller les défaillances des agents de sécurité, toute activité inhabituelle des pilotes ainsi que les modifications des paramètres de journalisation ou de protection. Toute perte de visibilité inexpliquée sur des systèmes à privilèges doit être considérée comme un incident de sécurité potentiel.

4. Protéger les infrastructures critiques et les capacités de restauration. Étendre la surveillance aux environnements Linux, aux infrastructures de virtualisation et aux environnements de sauvegarde. Séparer les droits d'accès nécessaires à la reprise d'activité de ceux liés à l'administration courante et tester la restauration lorsque les systèmes de gestion habituels sont indisponibles.

5. Définir des règles de sécurité pour les agents IA. Recenser les frameworks d'agents, les outils connectés et les extensions externes. Restreindre leurs autorisations, garantir l'isolation des environnements clients et exiger une validation indépendante pour toute action ayant un impact important.

Ces priorités poursuivent un même objectif : réduire les possibilités d'accès des cybercriminels, détecter toute utilisation malveillante de ces accès et préserver la capacité à rétablir les services essentiels.

Conclusion : la cyberrésilience repose sur la maîtrise des accès interconnectés

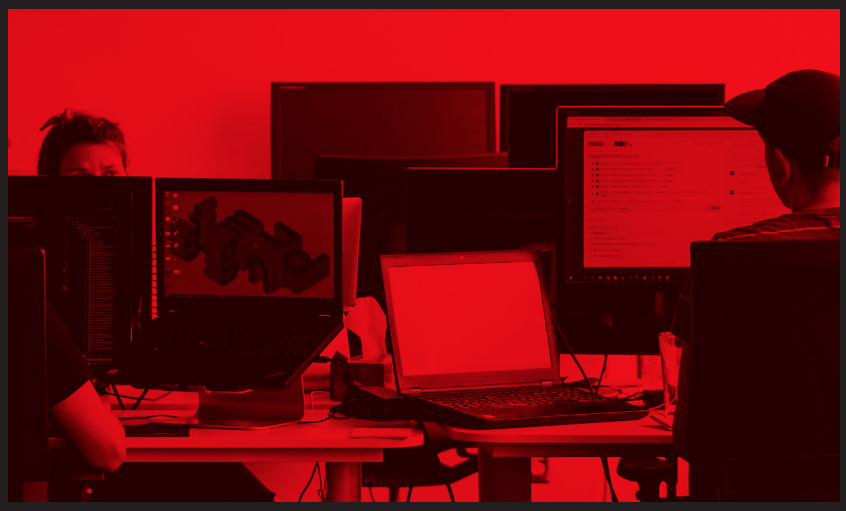
Le paysage des menaces en 2026 se caractérise non seulement par l'émergence de nouvelles techniques d'attaque, mais aussi par la capacité des acteurs malveillants à exploiter les connexions entre les identités, les services et les infrastructures.

Les agents IA peuvent accélérer les processus d'attaque existants. Les identifiants dérobés peuvent donner accès à plusieurs applications cloud et environnements clients. Les opérateurs de ransomware peuvent neutraliser les mécanismes de sécurité et cibler les infrastructures nécessaires à la restauration.

Pour les MSP et les responsables informatiques, le principal défi consiste à comprendre l'étendue d'une compromission et à la contenir avant que les cybercriminels ne puissent accéder à d'autres systèmes.

Les organisations qui disposent d'une visibilité sur les identités, les terminaux, les services cloud et les infrastructures de reprise seront mieux à même de détecter les activités non autorisées, de contenir les incidents et de rétablir les opérations essentielles.

Découvrez le rapport complet Acronis TRU Cyber Pulse 2026 pour consulter les investigations détaillées, les conclusions techniques et des recommandations de sécurité supplémentaires.



À propos de cette étude

Le rapport Acronis TRU Cyber Pulse 2026 rassemble les résultats d'investigations sur les menaces, d'analyses de malware, d'études de campagnes d'attaque et de données de télémétrie pertinentes issues des solutions Acronis. Il examine les nouvelles techniques d'attaque, les menaces persistantes avancées (APT) et la cybercriminalité, en accordant une attention particulière aux conséquences pour les MSP et leurs clients.

Auteurs



Santiago Pontiroli,
responsable de la recherche en cyberveille



Alexander Ivanyuk,
directeur senior des technologies

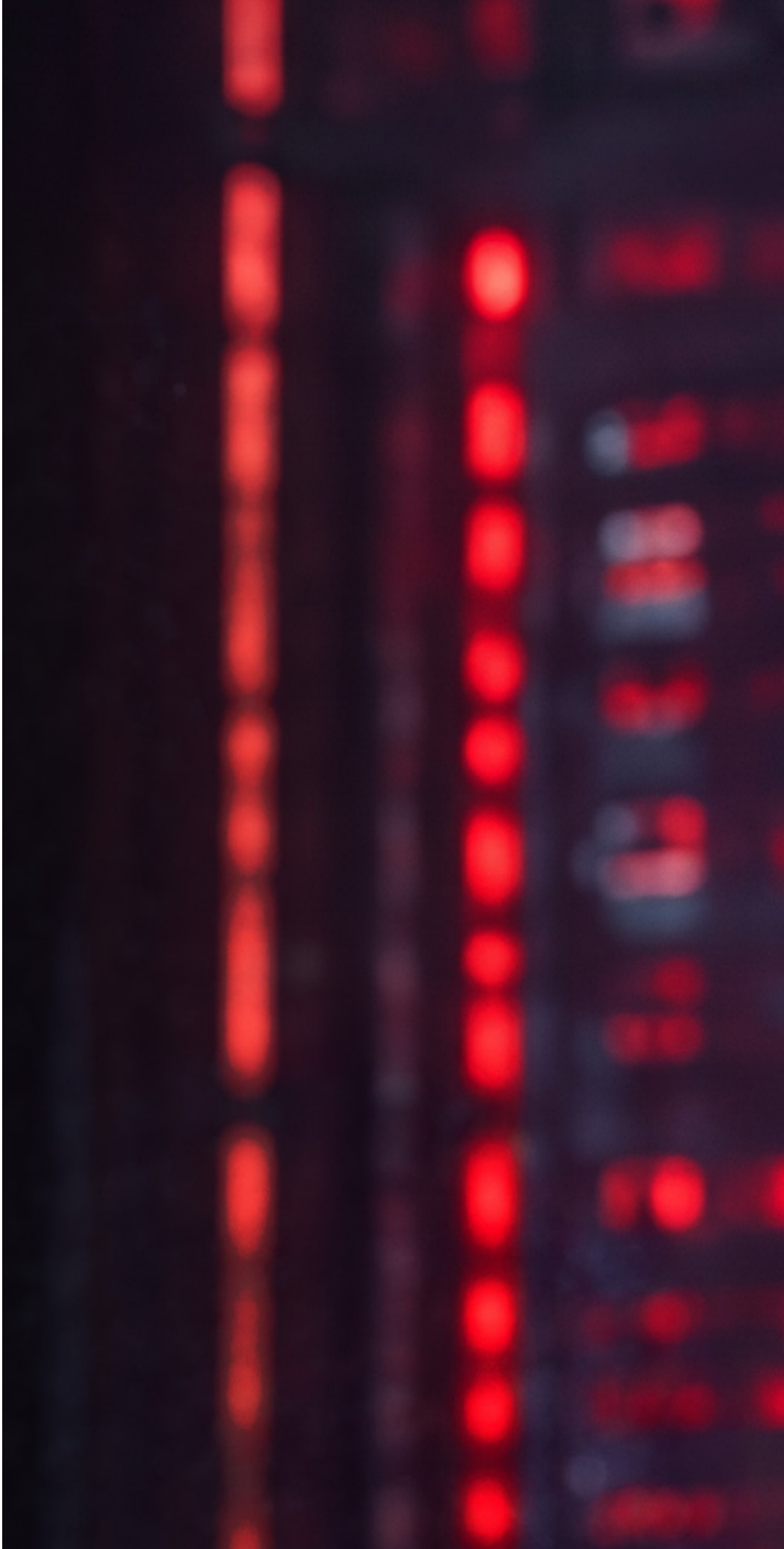


Eliad Kimhy,
chercheur senior au sein de l'Acronis TRU



Subhajeet Singha,
chercheur senior au sein de l'Acronis TRU

Acronis
Threat Research Unit



Copyright © 2003-2026 Acronis International GmbH. Tous droits réservés. Acronis et le logo Acronis sont des marques commerciales d'Acronis International GmbH aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales, déposées ou non, sont la propriété de leurs détenteurs respectifs. Sous réserve d'erreurs, de modifications techniques et de différences par rapport aux illustrations.

2026