

RESUMEN EJECUTIVO

Acronis TRU Cyber Pulse 2026

Hallazgos clave e implicaciones para la seguridad

Acronis
Threat Research Unit

Resumen ejecutivo



Los ciberataques evolucionan de formas que aumentan tanto la velocidad como el alcance de una intrusión.

Los ciberdelincuentes utilizan agentes de IA para automatizar los flujos de trabajo de los ataques, aprovechan identidades robadas para desplazarse entre servicios conectados y atacan los controles de seguridad para reducir las capacidades de detección y recuperación.

El informe inaugural "Acronis TRU Cyber Pulse 2026" reúne las investigaciones realizadas por la Unidad de investigación de amenazas de Acronis (TRU) sobre técnicas de ataque emergentes, actividades de espionaje y ciberdelincuencia. Los hallazgos revelan un patrón común: una vulneración inicial puede proporcionar acceso mucho más allá del dispositivo o la cuenta afectados.

Para los proveedores de servicios gestionados (MSP), esto genera riesgos particulares. La vulneración de una identidad administrativa, una herramienta de administración remota o un servicio compartido puede exponer los entornos de varios clientes. Por lo tanto, las organizaciones no solo deben comprender cómo obtienen acceso los atacantes, sino también hasta dónde puede llegar ese acceso.

En total, son seis hallazgos los que definen el panorama de amenazas analizado en este informe.

1. Los agentes de IA amplían el alcance de los ciberataques

Los ciberdelincuentes están exprimiendo las capacidades de la IA para mucho más que simples tareas individuales, como redactar mensajes de phishing o analizar vulnerabilidades. Algunos integran modelos de lenguaje de gran tamaño (LLM) con herramientas de seguridad ofensiva y plataformas de mensajería, al tiempo que emplean memoria persistente para conservar el contexto y coordinar operaciones de ataque de mayor alcance.

La investigación sobre BOSSAI de Acronis TRU ilustra esta evolución. Un único operador conectó más de 10 modelos a marcos de trabajo ofensivos e infraestructuras de apoyo, lo que permitió coordinar tareas de reconocimiento, aprovechamiento de vulnerabilidades y administración de infraestructuras contra objetivos ubicados en varios países.

Estos hallazgos demuestran cómo los sistemas agentivos pueden reducir el esfuerzo manual necesario para llevar a cabo operaciones complejas.

La adopción de la IA también introduce nuevas superficies de ataque. TRU identificó más de 575 habilidades maliciosas de OpenClaw distribuidas en 13 cuentas de desarrollador. Estos paquetes suplantaban utilidades legítimas mientras distribuían malware.

```
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 redirigido a través de MiniMax.

Implicación de seguridad:

Las organizaciones deben tratar los agentes de IA y las herramientas conectadas a ellos como sistemas con privilegios elevados. Los permisos de los agentes, las habilidades externas, las credenciales y el acceso a la red requieren controles de seguridad y una supervisión independientes.

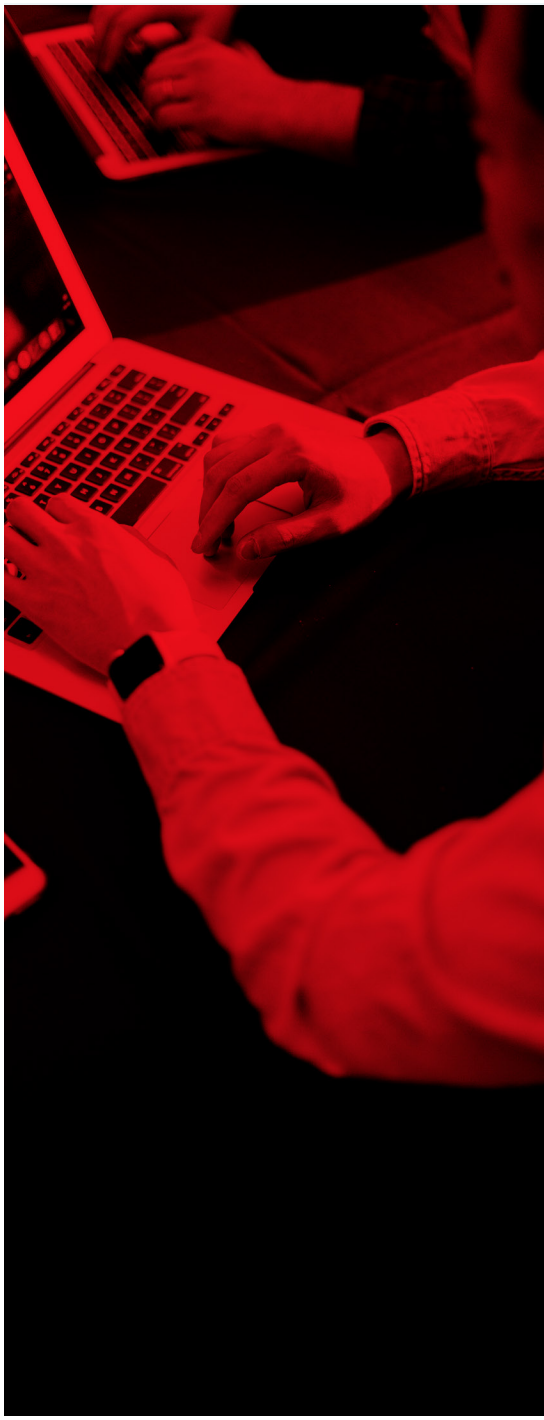
2. El robo de identidades: una de las principales vías para ampliar el alcance de las vulneraciones

Los programas de robo de información (infostealers) y los ataques centrados en las identidades tienen cada vez más en el punto de mira las credenciales, los tokens de autenticación, las sesiones de navegador y los accesos a la nube.

Los atacantes pueden utilizar esta información para acceder a aplicaciones y servicios conectados, en ocasiones sin activar una nueva solicitud de autenticación multifactor. El acceso comprometido también puede transferirse o venderse a otros ciberdelincuentes, incluidos operadores de ransomware y grupos de espionaje.

El riesgo también se extiende a los entornos de desarrollo. Investigaciones recientes identificaron malware dirigido a claves de API de servicios de IA, credenciales de repositorios y otros secretos de desarrollo. Estas credenciales pueden dar acceso a sistemas y proyectos adicionales.

Para los MSP, las identidades con privilegios elevados son especialmente valiosas, ya que pueden proporcionar acceso a varios clientes.



Implicación de seguridad:

No basta con eliminar el malware o restablecer una contraseña. La respuesta ante incidentes debe incluir la revocación de sesiones expuestas, la rotación de credenciales, la revisión de los cambios en la autenticación y la investigación de los servicios conectados.

3. Los atacantes debilitan deliberadamente los controles de seguridad y recuperación

Desactivar herramientas de seguridad se ha convertido en un componente importante de las intrusiones modernas.

En abril de 2026, MITRE ATT&CK incorporó el concepto de "deterioro de las defensas" como una táctica diferenciada que engloba las interferencias deliberadas en los sistemas defensivos.

Las investigaciones de Acronis TRU sobre operaciones de ransomware, incluidas las de Qilin y The Gentlemen, demuestran cómo los atacantes pueden finalizar procesos de seguridad, interferir en la supervisión e interrumpir los mecanismos de recuperación.

Estas actividades pueden reducir la visibilidad de los defensores mientras los atacantes se desplazan por las redes, sustraen información o se preparan para cifrar sistemas.

El riesgo es especialmente significativo cuando los atacantes obtienen el control de servidores de administración o de cuentas administrativas utilizadas en varios entornos.



Fondo de pantalla de The Gentlemen

Implicación de seguridad:

Las organizaciones deben supervisar de forma independiente el estado de los agentes de seguridad, los cambios en los registros y los intentos de desactivar la protección. La administración de las copias de seguridad debe mantenerse separada de la administración rutinaria de los sistemas, y los procesos de recuperación deben ponerse a prueba frente a escenarios que impliquen credenciales o infraestructuras comprometidas.

4. Los ataques se ocultan tras servicios y software de confianza

Los ciberdelincuentes y los operadores de espionaje utilizan cada vez más plataformas conocidas, como GitHub, Telegram y servicios de almacenamiento en la nube, para distribuir malware o mantener comunicaciones con sistemas comprometidos.

Dado que estos servicios también respaldan actividades empresariales legítimas, puede resultar difícil distinguir el tráfico malicioso del uso autorizado.

Las investigaciones de Acronis TRU documentaron la distribución de malware a través de repositorios de GitHub y el uso de servicios en la nube de confianza para actividades de mando y control.

La campaña TamperedChef demostró otra limitación de los indicadores de confianza tradicionales. Los atacantes distribuyeron aplicaciones maliciosas plenamente funcionales con certificados válidos para la firma de código, lo que demuestra que una firma legítima no garantiza que el software sea seguro.

Implicación de seguridad:

Las organizaciones deben evaluar la actividad de las aplicaciones y los servicios en su contexto, en lugar de basarse únicamente en la reputación de los dominios o en las firmas digitales. Las descargas inesperadas, la actividad de las API en la nube y las conexiones de administración remota requieren una investigación, incluso cuando implican servicios conocidos.



5. Las operaciones de ransomware se adaptan a las interrupciones y se expanden más allá de Windows

Las operaciones de las fuerzas de seguridad pueden interrumpir la infraestructura de los ciberdelincuentes, pero las herramientas y los conocimientos que sustentan esas operaciones pueden seguir estando disponibles.

Las investigaciones de Acronis TRU muestran que los afiliados de ransomware, el código fuente filtrado y las técnicas de ataque compartidas permiten a las operaciones delictivas reorganizarse y continuar su actividad con otros nombres.

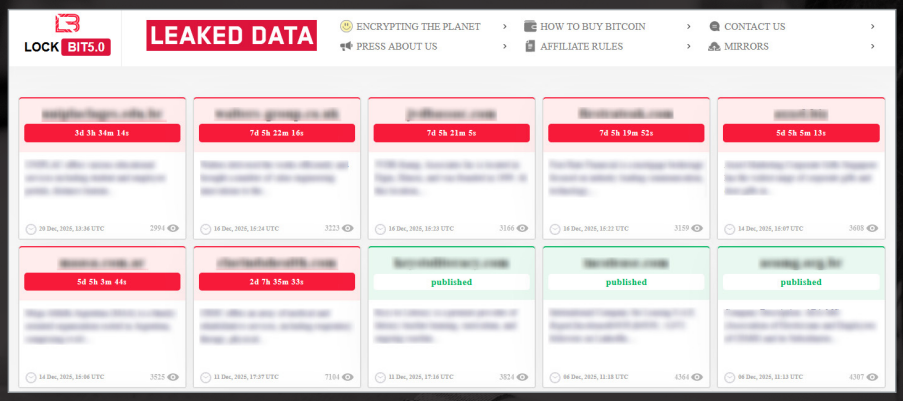
El alcance técnico del ransomware también se está ampliando.

LockBit 5.0 incluye variantes para Windows, Linux y VMware ESXi. El ransomware INC ha demostrado capacidades dirigidas a entornos Linux y ESXi, mientras que Qilin ha utilizado el Subsistema de Windows para Linux (WSL) para ejecutar un cifrador de Linux en Windows.

Al dirigirse contra infraestructuras de virtualización, los atacantes pueden interrumpir múltiples cargas de trabajo y afectar a sistemas esenciales para recuperar la actividad empresarial.

Implicación de seguridad:

Las defensas contra el ransomware deben abarcar los hosts Linux, los hipervisores y la gestión de máquinas virtuales. Las organizaciones deben supervisar los apagados inesperados de máquinas virtuales y la eliminación de instantáneas, así como garantizar que la infraestructura de recuperación siga siendo accesible durante una intrusión.



Sitio de filtración de datos de LockBit 5.0

6. El aprovechamiento de vulnerabilidades y las relaciones de confianza amplían el alcance de las intrusiones

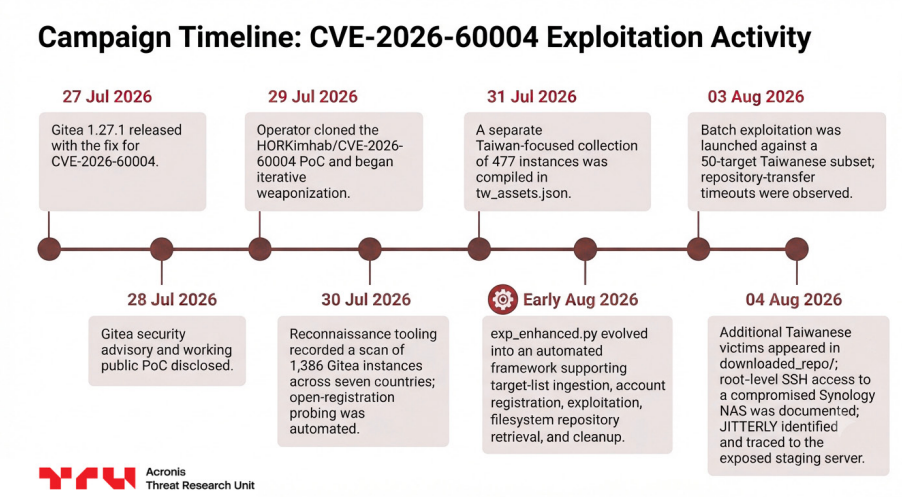
Los atacantes aprovechan las vulnerabilidades recién divulgadas con rapidez, lo que reduce el tiempo disponible para que las organizaciones desplieguen actualizaciones de seguridad.

En una investigación de Red Heron, los atacantes adaptaron un exploit disponible públicamente poco después de que se divulgara una vulnerabilidad crítica de Gitea. Los servidores de desarrollo comprometidos expusieron repositorios y credenciales que podían favorecer actividades de intrusión adicionales.

Las investigaciones relacionadas con actividades de espionaje revelaron un patrón similar: los ciberdelincuentes aprovechan cada vez más las relaciones de confianza para acceder indirectamente a sus objetivos.

Los proveedores de servicios de TI, los entornos de desarrollo y las infraestructuras de distribución de software pueden proporcionar acceso a organizaciones que los atacantes no pueden comprometer fácilmente de forma directa.

Estos ataques tienen consecuencias especialmente significativas para los MSP, ya que un único servicio o identidad comprometidos pueden exponer a varios clientes.



Implicación de seguridad:

La corrección de vulnerabilidades debe tener en cuenta el acceso que proporciona un sistema, y no únicamente la gravedad de la vulnerabilidad. Tras un aprovechamiento exitoso, las organizaciones deben investigar los mecanismos de persistencia, las credenciales robadas y la actividad en los entornos conectados.

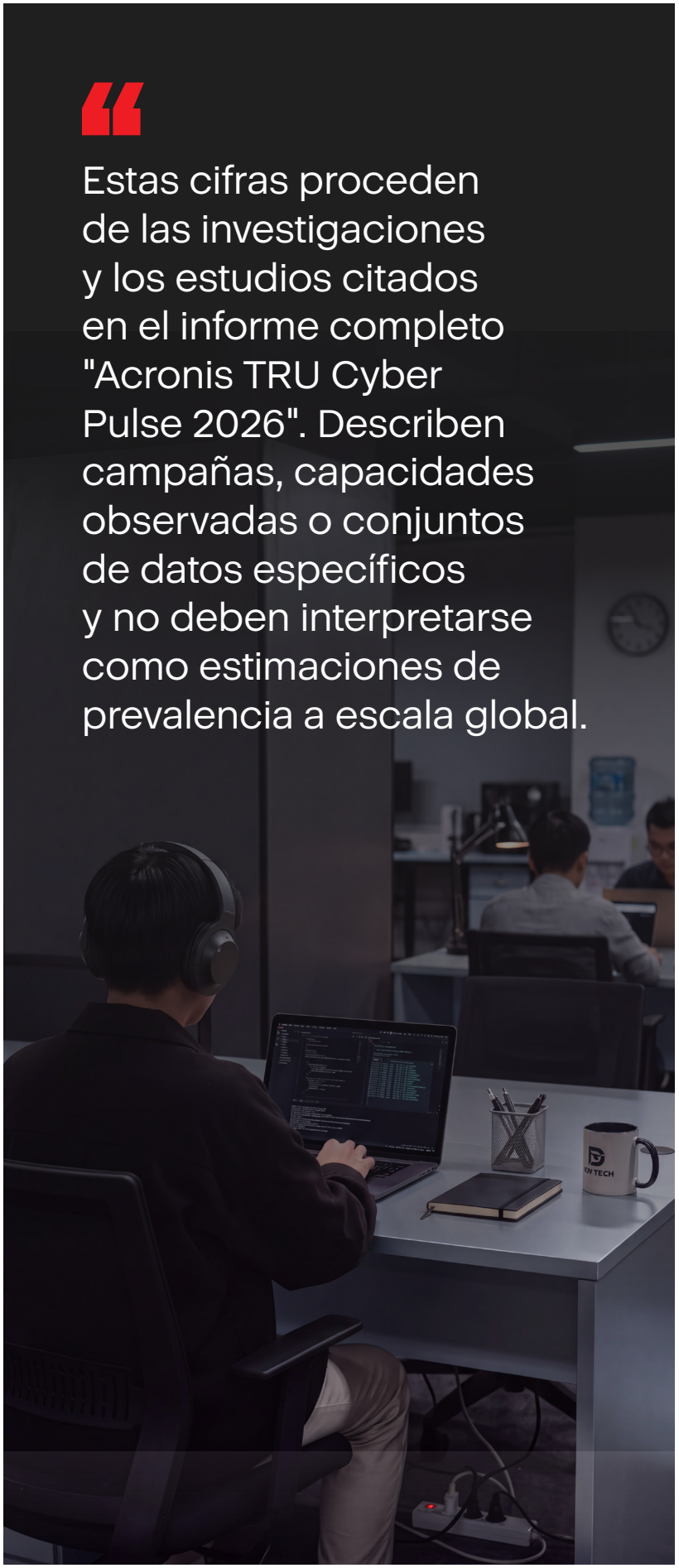
Resumen de los principales hallazgos de la investigación

Los siguientes hallazgos seleccionados ilustran el alcance de la actividad documentada en el informe completo.

Hallazgos de la investigación | Evidencias notificadas

- **Ataque habilitado por IA:** BOSSAI conectó más de 10 modelos de IA a herramientas ofensivas e infraestructuras de apoyo.
- **Amenazas para la cadena de suministro de IA:** TRU identificó más de 575 habilidades maliciosas de OpenClaw distribuidas en 13 cuentas de desarrollador.
- **Exposición derivada del acceso remoto:** en un análisis de más de 1,8 millones de endpoints que ejecutaban Acronis RMM, el 63,1 % tenía instalada al menos una herramienta adicional de RMM o acceso remoto.
- **Retrasos en la aplicación de parches:** TRU informó de una mediana de 5,7 días para aplicar parches en aplicaciones de terceros durante la segunda mitad de 2025.
- **Expansión del ransomware:** LockBit 5.0 incluye variantes dirigidas a entornos Windows, Linux y ESXi.

> Estas cifras proceden de las investigaciones y los estudios citados en el informe completo "Acronis TRU Cyber Pulse 2026". Describen campañas, capacidades observadas o conjuntos de datos específicos y no deben interpretarse como estimaciones de prevalencia a escala global.



Prioridades para reforzar la ciberresiliencia



Los hallazgos apuntan a cinco prioridades prácticas para los MSP y las organizaciones que desean reducir el impacto de los ciberataques.

1. Limitar el alcance de las identidades comprometidas. Aplique métodos de autenticación resistente al phishing, restrinja el acceso con privilegios elevados y mantenga visibilidad sobre las sesiones, los permisos de las aplicaciones y las conexiones de administración remota.

2. Priorizar las vulnerabilidades en función de la exposición y el acceso. Acelere la corrección de los sistemas expuestos a internet y de los sistemas administrativos, sobre todo aquellos que contienen credenciales o proporcionan acceso a otros entornos. Investigue los mecanismos de persistencia y la exposición de credenciales tras cualquier sospecha de vulneración.

3. Detectar los intentos de desactivar la protección. Supervise el estado de los agentes de seguridad en busca de posibles fallos, la actividad inesperada de los controladores y los cambios en la configuración de los registros o de la protección. Considere cualquier brecha de visibilidad injustificada en sistemas con privilegios elevados como un posible incidente de seguridad.

4. Proteger las infraestructuras críticas y las capacidades de recuperación. Amplíe la supervisión a los entornos Linux, de virtualización y de copias de seguridad. Mantenga los permisos de recuperación separados de la administración rutinaria y ponga a prueba la restauración cuando los sistemas de administración habituales no estén disponibles.

5. Establecer límites de seguridad para los agentes de IA. Elabore un inventario de los marcos de trabajo de agentes, las herramientas conectadas y las habilidades externas. Restrinja sus permisos, garantice la separación entre los entornos de clientes y exija una aprobación independiente para las acciones de alto impacto.

Estas prioridades comparten un objetivo común: reducir el acceso disponible para los atacantes, detectar su uso indebido y mantener la capacidad de recuperar los servicios esenciales.

Conclusión: la ciberresiliencia depende del control de los acceso conectados

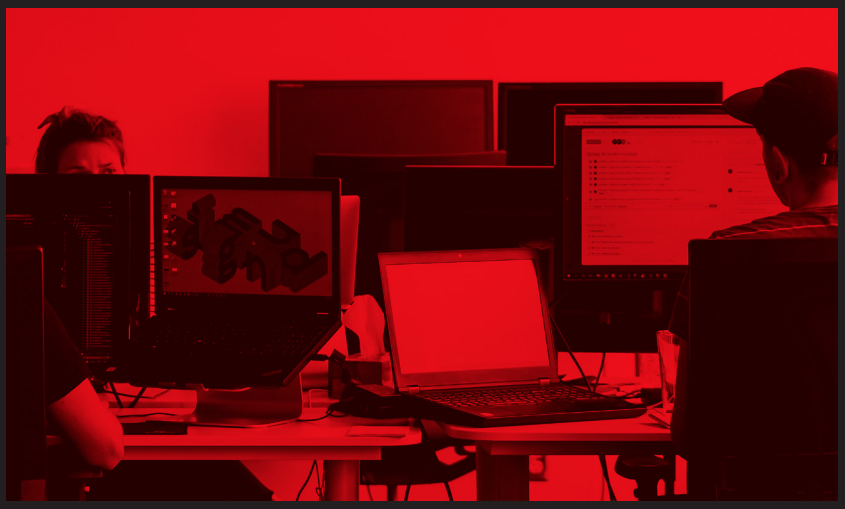
El panorama de amenazas de 2026 no se define únicamente por las nuevas técnicas de ataque, sino también por la capacidad de los ciberdelincuentes para aprovechar las conexiones entre identidades, servicios e infraestructuras.

Los agentes de IA pueden acelerar los flujos de trabajo de ataque ya establecidos. Las credenciales robadas pueden proporcionar acceso a aplicaciones en la nube y entornos de clientes. Los operadores de ransomware pueden interferir en los controles de seguridad y atacar la infraestructura necesaria para la recuperación.

Para los MSP y los responsables de TI, el principal desafío consiste en comprender el alcance de una intrusión y contenerla antes de que los atacantes puedan sacar provecho de sistemas adicionales.

Las organizaciones que mantengan visibilidad sobre las identidades, los endpoints, los servicios en la nube y la infraestructura de recuperación estarán mejor preparadas para detectar actividades no autorizadas, contener incidentes y restaurar operaciones críticas.

Consulte el informe completo Acronis TRU Cyber Pulse 2026 para acceder a investigaciones detalladas, hallazgos técnicos y recomendaciones de seguridad adicionales.



Acerca de esta investigación

El informe "Acronis TRU Cyber Pulse 2026" reúne investigaciones sobre amenazas, análisis de malware, estudios de campañas y datos de telemetría relevantes de Acronis. En él se examinan técnicas de ataque emergentes, actividad de amenazas persistentes avanzadas (APT) y ciberdelincuencia, con especial atención a sus implicaciones para los MSP y sus clientes.

Autores



Santiago Pontiroli,
responsable de investigación de inteligencia sobre amenazas



Alexander Ivanyuk,
director sénior de Tecnología

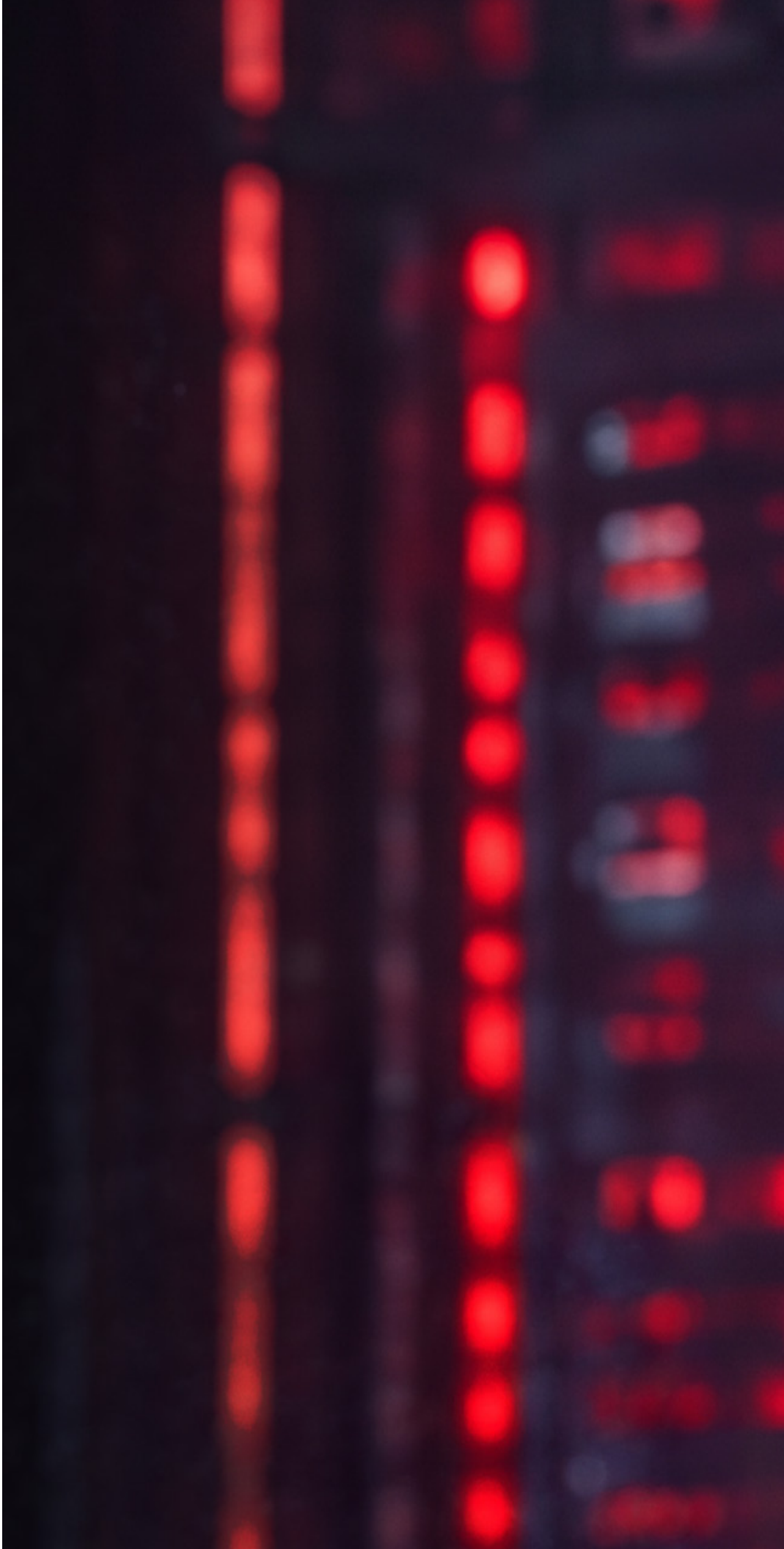


Eliad Kimhy,
investigador sénior de TRU



Subhajeet Singha,
investigador sénior de TRU

Acronis
Threat Research Unit



Copyright © 2003-2026 Acronis International GmbH. Reservados todos los derechos. Acronis y el logotipo de Acronis son marcas comerciales de Acronis International GmbH en Estados Unidos y otros países. Todas las demás marcas comerciales o marcas registradas son propiedad de sus respectivos dueños. Nos reservamos el derecho a que haya cambios técnicos y diferencias con respecto a las ilustraciones; declinamos la responsabilidad por cualquier error.

2026