

RESUMO EXECUTIVO

Acronis TRU Cyber Pulse 2026

Principais descobertas e implicações para a segurança

Acronis
Threat Research Unit



Os ciberataques estão evoluindo de formas que aumentam tanto a velocidade quanto o alcance de uma invasão.

Agentes de ameaça estão usando inteligência artificial para automatizar fluxos de trabalho de ataque, explorando identidades roubadas para transitar entre serviços conectados e atacando controles de segurança para reduzir as capacidades de detecção e recuperação.

O relatório inaugural Acronis TRU Cyber Pulse 2026 reúne investigações conduzidas pela Acronis Threat Research Unit (TRU) sobre técnicas de ataque emergentes, atividades de espionagem e cibercrimes. As descobertas revelam um padrão comum: um comprometimento inicial pode proporcionar acesso muito além do dispositivo ou da conta afetada.

Para provedores de serviços gerenciados (MSPs), isso gera riscos específicos. Uma identidade administrativa comprometida, uma ferramenta de gerenciamento remoto ou um serviço compartilhado pode expor diversos ambientes de clientes. Portanto, as organizações devem entender não apenas como os invasores obtêm acesso, mas também até onde esse acesso pode se estender.

Seis descobertas definem o cenário de ameaças analisado neste relatório.

1. Agentes de inteligência artificial estão ampliando a escala dos ciberataques

Agentes de ameaça estão indo além do uso da inteligência artificial em tarefas individuais, como redigir mensagens de phishing ou analisar vulnerabilidades. Alguns estão integrando modelos de linguagem de grande porte a ferramentas de segurança ofensiva e plataformas de mensagens, enquanto usam memória persistente para reter contexto e coordenar operações de ataque mais amplas.

A investigação BOSSAI da Acronis TRU ilustra esse desenvolvimento. Um único operador conectou mais de 10 modelos a estruturas ofensivas e infraestrutura de suporte, permitindo reconhecimento, exploração e gerenciamento de infraestrutura coordenados em alvos de vários países.

Essas descobertas demonstram como sistemas baseados em agentes podem reduzir o esforço manual necessário para conduzir operações complexas.

A adoção de inteligência artificial também introduz novas superfícies de ataque. A TRU identificou mais de 575 habilidades maliciosas do OpenClaw em 13 contas de desenvolvedores. Esses pacotes se passavam por utilitários legítimos enquanto distribuíam 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 redirecionado por meio do MiniMax.

Implicação para a segurança:

As organizações devem tratar os agentes de inteligência artificial e as ferramentas a eles conectadas como sistemas privilegiados. As permissões dos agentes, habilidades externas, credenciais e acesso à rede exigem controles de segurança e monitoramento independentes.

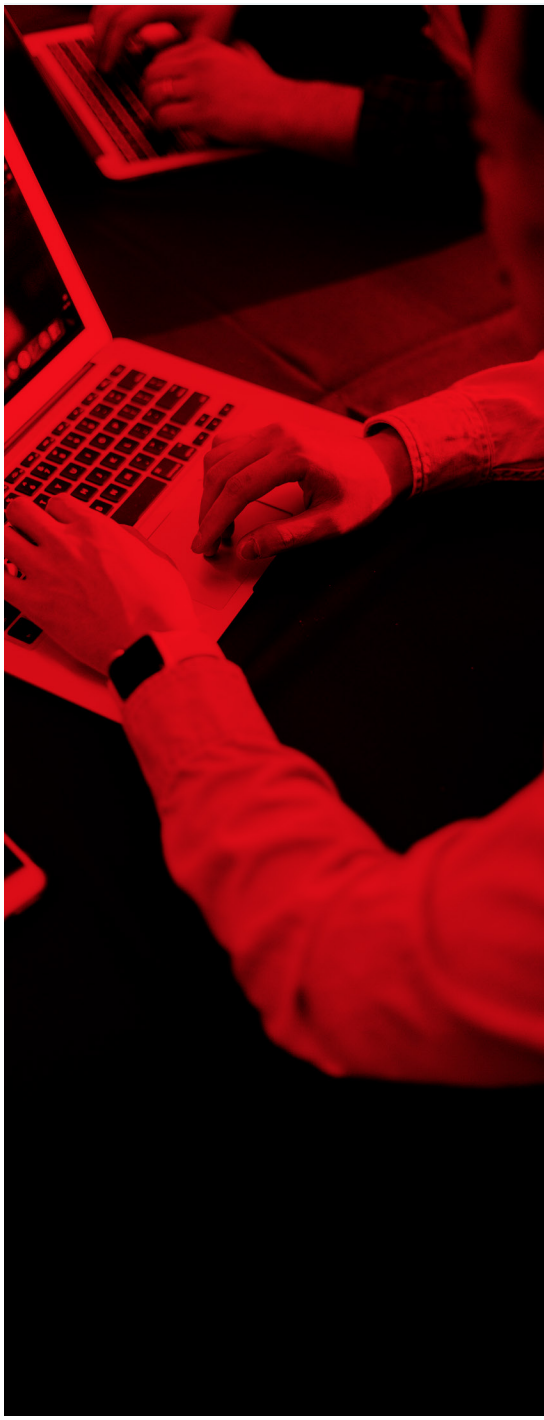
2. Identidades roubadas estão se tornando uma das principais vias para um comprometimento mais amplo

Infostealers e ataques focados em identidade visam cada vez mais credenciais, tokens de autenticação, sessões de navegador e acesso à nuvem.

Os invasores podem usar essas informações para acessar aplicativos e serviços conectados, às vezes sem acionar uma nova solicitação de autenticação multifator. O acesso roubado também pode ser transferido ou vendido a outros agentes de ameaça, incluindo operadores de ransomware e grupos de espionagem.

O risco se estende aos ambientes de desenvolvimento. Investigações recentes identificaram malware voltado a chaves de API de serviços de inteligência artificial, credenciais de repositórios e outros segredos de desenvolvimento. Essas credenciais podem fornecer acesso a sistemas e projetos adicionais.

Para MSPs, identidades privilegiadas são particularmente valiosas porque podem fornecer acesso a vários clientes.



Implicação para a segurança:

Remover malware ou redefinir uma senha não é suficiente. A resposta a incidentes deve incluir a revogação de sessões expostas, a rotação de credenciais, a revisão de alterações na autenticação e a investigação de serviços conectados.

3. Os invasores estão enfraquecendo deliberadamente os controles de segurança e recuperação

Desativar ferramentas de segurança tornou-se uma parte importante das atividades de invasão modernas.

Em abril de 2026, o MITRE ATT&CK apresentou o Defense Impairment (Enfraquecimento de defesas) como uma tática distinta que abrange a interferência deliberada em sistemas defensivos.

Investigações da Acronis TRU sobre operações de ransomware, incluindo Qilin e The Gentlemen, demonstram como os invasores podem encerrar processos de segurança, interferir no monitoramento e interromper mecanismos de recuperação.

Essas atividades podem reduzir a visibilidade dos defensores enquanto os invasores se movimentam pelas redes, roubam informações ou se preparam para criptografar sistemas.

O risco é especialmente significativo quando os invasores obtêm controle de management servers ou de contas administrativas usadas em vários ambientes.



Papel de parede de desktop do ransomware The Gentlemen

Implicação para a segurança:

As organizações devem monitorar de forma independente o estado de funcionamento dos agentes de segurança, as configurações de logs e as tentativas de desativar a proteção. A administração de backups deve permanecer separada da administração rotineira dos sistemas, e os processos de recuperação devem ser testados em cenários que envolvam credenciais ou infraestrutura comprometidas.

4. Serviços e software confiáveis estão sendo explorados para ocultar ataques

Cibercriminosos e operadores de espionagem usam cada vez mais plataformas conhecidas, incluindo GitHub, Telegram e serviços de armazenamento em nuvem, para distribuir malware ou manter comunicação com sistemas comprometidos.

Como esses serviços também oferecem suporte a atividades empresariais legítimas, pode ser difícil distinguir o tráfego malicioso do uso autorizado.

Investigações da Acronis TRU documentaram a distribuição de malware por meio de repositórios do GitHub e o uso de serviços de nuvem confiáveis para comando e controle.

A campanha TamperedChef demonstrou outra fragilidade nos sinais tradicionais de confiança. Os invasores distribuíram aplicativos maliciosos funcionais com certificados válidos de assinatura de código, demonstrando que uma assinatura legítima não comprova que o software é seguro.

Implicação para a segurança:

As organizações devem avaliar a atividade de aplicativos e serviços em seu contexto, em vez de depender apenas da reputação de domínios ou de assinaturas digitais. Downloads inesperados, atividade de API de nuvem e conexões de gerenciamento remoto exigem investigação, mesmo quando envolvem serviços conhecidos.



5. As operações de ransomware estão se adaptando às ações de desarticulação e se expandindo além do Windows

As operações policiais podem interromper a infraestrutura de cibercriminosos, mas as ferramentas e o conhecimento técnico por trás das operações criminosas podem permanecer disponíveis.

Pesquisas da Acronis TRU mostram que afiliados de ransomware, códigos-fonte vazados e técnicas de ataque compartilhadas permitem que operações criminosas se reorganizem e continuem suas atividades sob nomes diferentes.

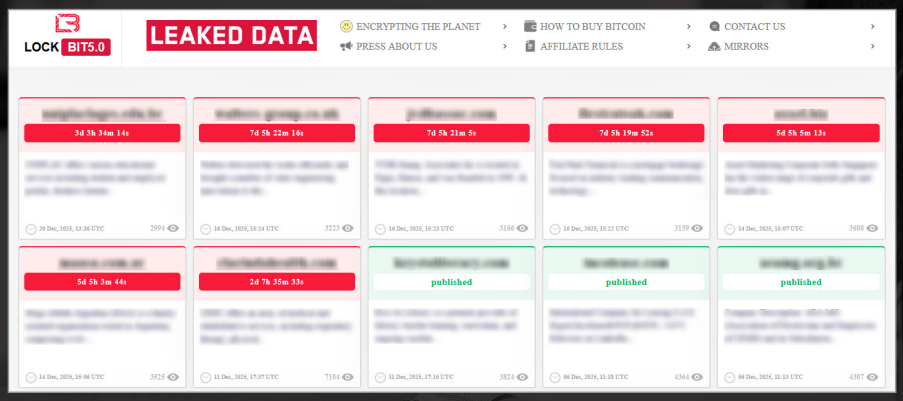
O escopo técnico do ransomware também está se expandindo.

O LockBit 5.0 inclui variantes para Windows, Linux e VMware ESXi. O ransomware INC demonstrou recursos voltados a ambientes Linux e ESXi, enquanto o Qilin usou o Windows Subsystem for Linux para executar um criptografador Linux no Windows.

Ao visar a infraestrutura de virtualização, os invasores podem interromper várias cargas de trabalho e afetar sistemas essenciais para a recuperação dos negócios.

Implicação para a segurança:

As defesas contra ransomware devem abranger hosts Linux, hipervisores e o gerenciamento de máquinas virtuais. As organizações devem monitorar desligamentos inesperados de máquinas virtuais e a exclusão de instantâneos, garantindo ao mesmo tempo que a infraestrutura de recuperação permaneça acessível durante um comprometimento.



Site de vazamento de dados do LockBit 5.0

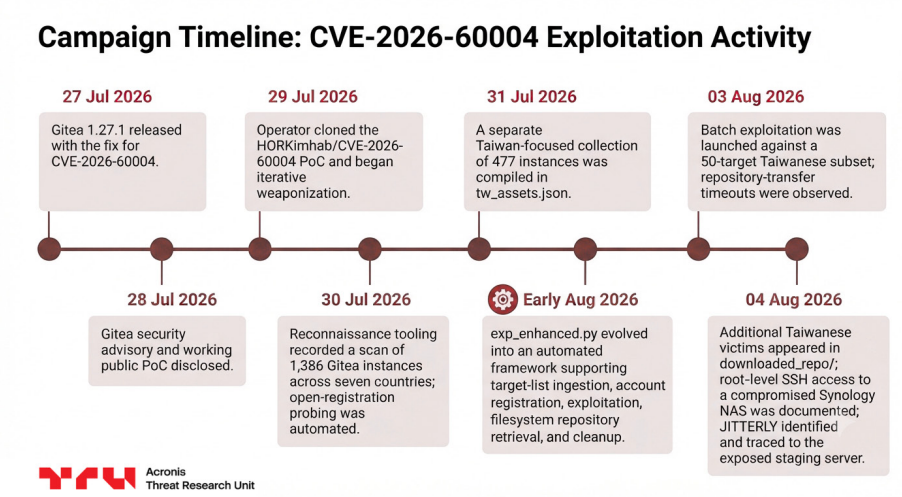
6. A exploração de vulnerabilidades e as relações de confiança estão ampliando o alcance das invasões

Os invasores estão explorando rapidamente vulnerabilidades recém-divulgadas, reduzindo o tempo disponível para que as organizações implantem atualizações de segurança.

Na investigação Red Heron, os invasores adaptaram um exploit disponível publicamente pouco depois da divulgação de uma vulnerabilidade crítica no Gitea. Servidores de desenvolvimento comprometidos expuseram repositórios e credenciais que poderiam dar suporte a outras atividades de invasão.

Investigações sobre espionagem revelaram um padrão relacionado: os agentes de ameaça exploram cada vez mais relacionamentos confiáveis para alcançar alvos indiretamente.

Provedores de TI, ambientes de desenvolvimento e infraestrutura de distribuição de software podem fornecer acesso a organizações que os invasores não conseguem comprometer diretamente ou só o fazem com dificuldade.



Esses ataques têm consequências de grande impacto para MSPs, pois um único serviço ou identidade comprometido pode expor vários clientes.

Implicação para a segurança:

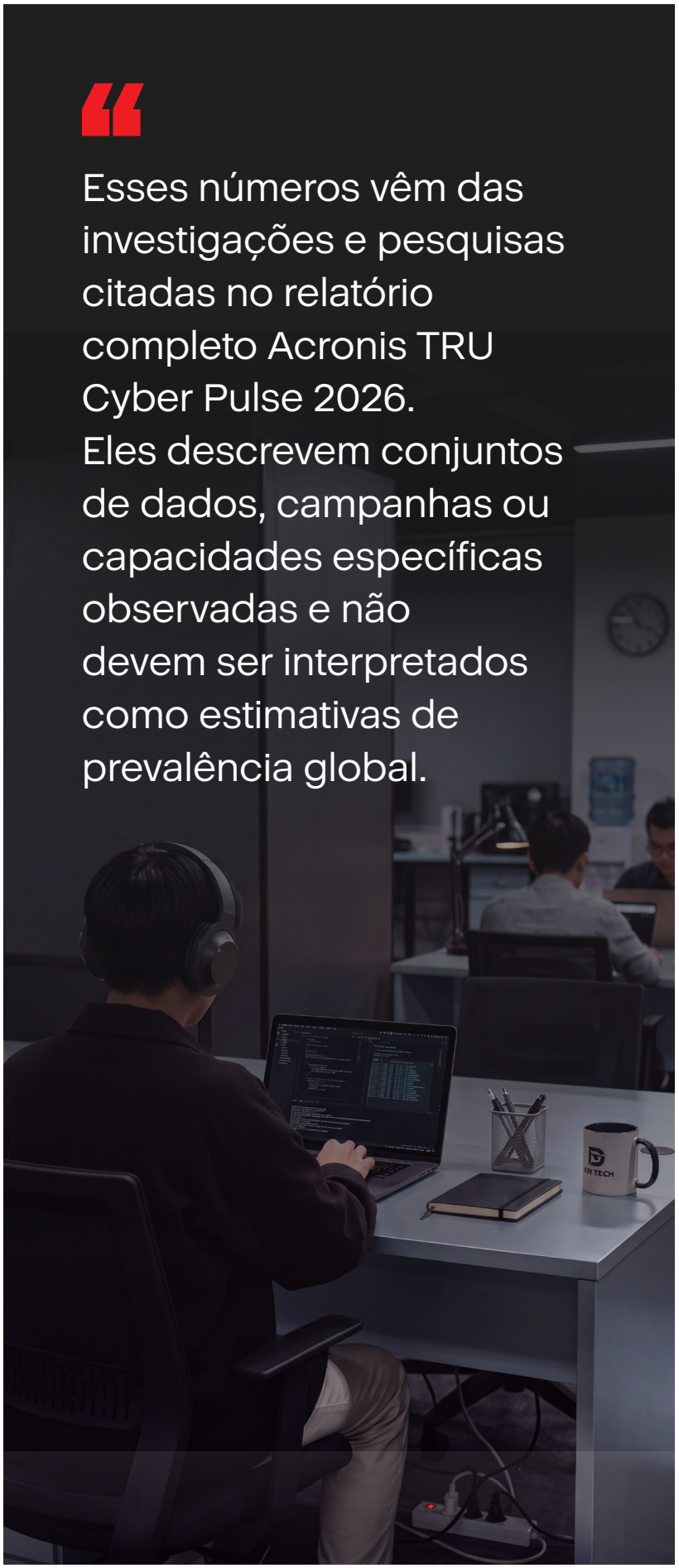
A correção de vulnerabilidades deve considerar o acesso que um sistema fornece, e não apenas a gravidade da vulnerabilidade. Após a exploração, as organizações devem investigar a persistência, as credenciais roubadas e a atividade em ambientes conectados.

Principais descobertas da pesquisa

As descobertas selecionadas a seguir ilustram o escopo da atividade documentada no relatório completo.

Descoberta da pesquisa | Evidência relatada

- **Ataque com uso de inteligência artificial:** o BOSSAI conectou mais de 10 modelos de inteligência artificial a ferramentas ofensivas e infraestrutura de suporte.
- **Ameaças à cadeia de suprimento das inteligências artificiais:** a TRU identificou mais de 575 habilidades maliciosas do OpenClaw em 13 contas de desenvolvedores.
- **Exposição de acesso remoto:** em uma análise de mais de 1,8 milhão de endpoints executando o Acronis RMM, 63,1% tinham pelo menos uma ferramenta adicional de RMM ou acesso remoto instalada.
- **Atrasos na aplicação de patches:** a TRU relatou um tempo mediano de aplicação de patches em aplicativos de terceiros de 5,7 dias no segundo semestre de 2025.
- **Expansão do ransomware:** o LockBit 5.0 inclui variantes voltadas a ambientes Windows, Linux e ESXi.



Prioridades para maior resiliência cibernética



As descobertas apontam cinco prioridades práticas para MSPs e organizações que buscam reduzir o impacto de ciberataques.

1. Limite o alcance de identidades comprometidas. Aplique autenticação resistente a phishing, restrinja o acesso privilegiado e mantenha visibilidade sobre sessões, permissões de aplicativos e conexões de gerenciamento remoto.

2. Priorize vulnerabilidades com base na exposição e no acesso. Acelere a correção de sistemas voltados para a internet e sistemas administrativos, especialmente aqueles que contêm credenciais ou fornecem acesso a outros ambientes. Investigue a persistência e a exposição de credenciais após suspeita de exploração.

3. Detecte tentativas de desativar a proteção. Monitore falhas de agentes de segurança, atividade inesperada de drivers e alterações nas configurações de logs ou proteção. Trate lacunas de visibilidade inexplicadas em sistemas privilegiados como possíveis incidentes de segurança.

4. Proteja a infraestrutura crítica e as capacidades de recuperação. Amplie o monitoramento para ambientes Linux, de virtualização e de backup. Separe as permissões de recuperação da administração rotineira e teste a restauração quando os sistemas normais de gerenciamento estiverem indisponíveis.

5. Estabeleça limites de segurança para agentes de inteligência artificial. Faça o inventário de estruturas de agentes, ferramentas conectadas e habilidades externas. Restrinja as permissões desses agentes, imponha a separação entre ambientes de clientes e exija aprovação independente para ações de alto impacto.

Essas prioridades compartilham um objetivo comum: reduzir o acesso disponível aos invasores, detectar o uso indevido desse acesso e manter a capacidade de recuperar serviços essenciais.

Conclusão:
a resiliência cibernética depende do controle do acesso entre sistemas conectados

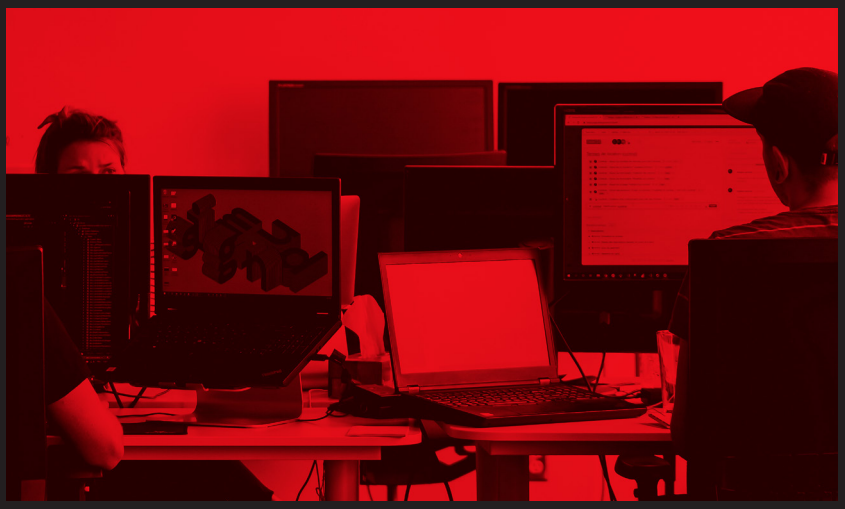
O cenário de ameaças de 2026 é definido não apenas por novas técnicas de ataque, mas também pela capacidade dos agentes de ameaça de explorar conexões entre identidades, serviços e infraestrutura.

Agentes de inteligência artificial podem acelerar fluxos de trabalho de ataque já estabelecidos. Credenciais roubadas podem oferecer acesso em diversos aplicativos de nuvem e ambientes de clientes. Operadores de ransomware podem interferir nos controles de segurança e visar a infraestrutura necessária para a recuperação.

Para MSPs e líderes de TI, o principal desafio é entender o alcance de um comprometimento e contê-lo antes que os invasores possam explorar sistemas adicionais.

Organizações que mantêm visibilidade sobre identidades, endpoints, serviços de nuvem e infraestrutura de recuperação estarão mais bem posicionadas para detectar atividades não autorizadas, conter incidentes e restaurar operações críticas.

Leia o relatório completo Acronis TRU Cyber Pulse 2026 para conferir investigações detalhadas, descobertas técnicas e outras recomendações de segurança.



Sobre esta pesquisa

O relatório Acronis TRU Cyber Pulse 2026 sintetiza investigações de ameaças, análises de malware, pesquisas sobre campanhas e telemetria relevante da Acronis. Ele examina técnicas de ataque emergentes, atividade de ameaças persistentes avançadas e cibercrime, com atenção especial às implicações para MSPs e seus clientes.

Autores



Santiago Pontiroli,
Líder de Pesquisa em Inteligência de Ameaças



Alexander Ivanyuk,
Diretor Sênior de Tecnologia

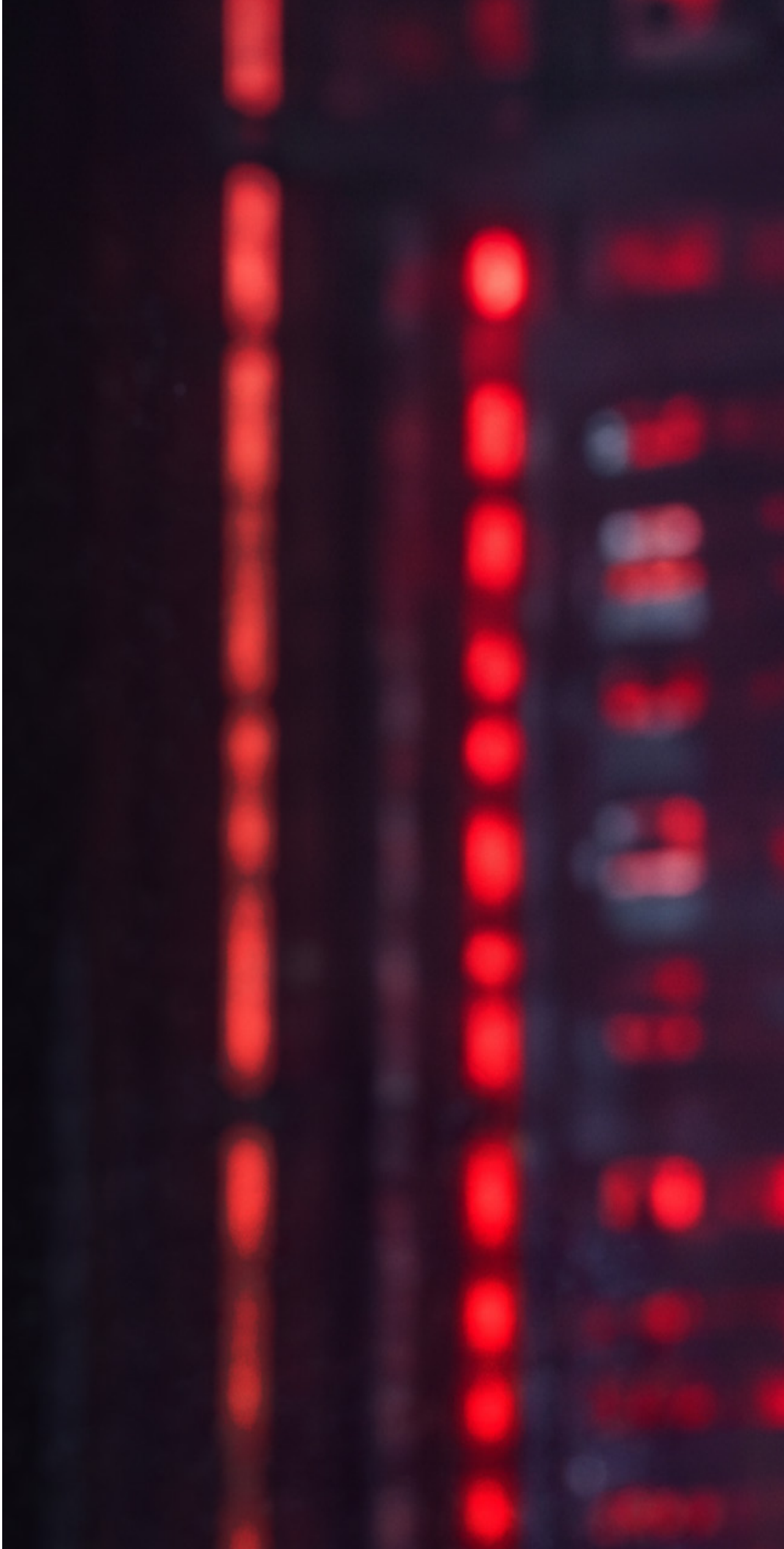


Eliad Kimhy,
Pesquisador Sênior da TRU



Subhajeet Singha,
Pesquisador Sênior da TRU

Acronis
Threat Research Unit



Copyright © 2003-2026 Acronis International GmbH. Todos os direitos reservados. Acronis e o logotipo da Acronis são marcas comerciais da Acronis International GmbH nos Estados Unidos e/ou em outros países. Todas as demais marcas comerciais ou marcas registradas pertencem aos seus respectivos proprietários. Pode haver alterações técnicas e diferenças em relação às ilustrações, bem como erros.

2026