

SINTESI RIEPILOGATIVA

Acronis TRU Cyber Pulse 2026

Principali conclusioni e impatto sulla sicurezza

Acronis
Threat Research Unit



Gli attacchi informatici si evolvono aumentando sia la velocità sia la portata delle intrusioni.

Gli autori delle minacce utilizzano agenti AI per automatizzare i flussi di attacco, sfruttano identità sottratte per spostarsi tra i servizi connessi e colpiscono i controlli di sicurezza per ridurre le capacità di rilevamento e ripristino.

Il primo report Acronis TRU Cyber Pulse 2026 raccoglie le indagini condotte dalla Acronis Threat Research Unit (TRU) sulle tecniche di attacco emergenti, sulle attività di spionaggio e sulla criminalità informatica. Ne emerge uno schema ricorrente: una compromissione iniziale può dare accesso a risorse che vanno ben oltre il dispositivo o l'account colpito.

Per i managed service provider (MSP), ciò comporta rischi specifici: la compromissione di un'identità amministrativa, di uno strumento di gestione remota o di un servizio condiviso può esporre più ambienti cliente. Alle organizzazioni quindi non basta capire come gli attaccanti riescono ad accedere, ma devono sapere anche fino a che punto questi possono spingersi.

Il quadro delle minacce analizzato in questo report si può riassumere in sei risultati.

1. Gli agenti AI ampliano la portata degli attacchi informatici

Gli autori delle minacce non si limitano più a utilizzare l'AI per singole attività come la scrittura di messaggi di phishing o l'analisi delle vulnerabilità. Alcuni combinano modelli linguistici di grandi dimensioni con strumenti di sicurezza informatica offensiva e piattaforme di messaggistica, usando al contempo una memoria persistente per mantenere il contesto e coordinare operazioni di attacco più ampie.

L'indagine di Acronis TRU su BOSSAI illustra questa evoluzione. Un singolo operatore ha collegato più di 10 modelli a framework di attacco e infrastrutture di supporto, riuscendo a coordinare attività di ricognizione, sfruttamento delle vulnerabilità e gestione dell'infrastruttura su obiettivi in più paesi.

Il caso dimostra come i sistemi agentici possano ridurre l'intervento manuale necessario per condurre operazioni complesse.

L'adozione dell'AI introduce anche nuove superfici di attacco. TRU ha identificato più di 575 skill OpenClaw malevole, pubblicate da 13 account di sviluppatori: pacchetti che si spacciavano per strumenti legittimi e al tempo stesso distribuivano 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 reindirizzato tramite MiniMax.

Impatto sulla sicurezza

Le organizzazioni devono considerare gli agenti AI e gli strumenti a essi collegati come sistemi con privilegi. Le autorizzazioni degli agenti, le skill esterne, le credenziali e l'accesso alla rete necessitano di controlli di sicurezza e monitoraggio indipendenti.

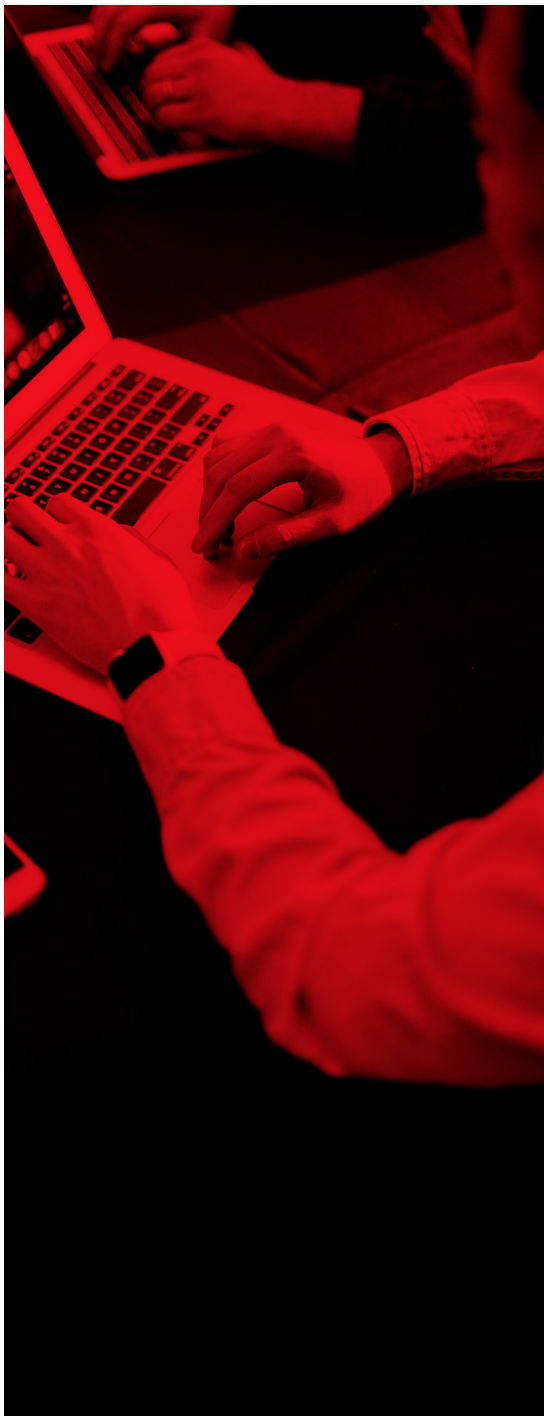
2. Le identità sottratte diventano la via primaria verso compromissioni più estese

Sempre più spesso, gli infostealer e gli attacchi incentrati sull'identità prendono di mira credenziali, token di autenticazione, sessioni del browser e accessi al cloud.

Con queste informazioni, gli attaccanti possono accedere ad applicazioni e servizi connessi, talvolta senza attivare una nuova richiesta di autenticazione a più fattori. Gli accessi sottratti possono anche essere trasferiti o venduti ad altri autori delle minacce, tra cui operatori ransomware e gruppi di spionaggio.

Il rischio riguarda anche gli ambienti di sviluppo. Indagini recenti hanno identificato malware che puntano a informazioni quali le chiavi API di servizi AI, le credenziali dei repository e altri dati riservati usati nello sviluppo. Queste informazioni possono consentire l'accesso ad altri sistemi e progetti.

Per gli MSP, le identità con privilegi hanno un valore particolarmente elevato perché possono dare accesso a più clienti.



Impatto sulla sicurezza

Rimuovere il malware o reimpostare una password non basta. L'incident response deve prevedere la revoca delle sessioni esposte, la rotazione delle credenziali, la revisione delle modifiche all'autenticazione e l'indagine sui servizi connessi.

3. Gli attaccanti indeboliscono deliberatamente i controlli di sicurezza e di ripristino

La disabilitazione degli strumenti di sicurezza è ormai una componente importante delle intrusioni moderne.

Ad aprile 2026, MITRE ATT&CK ha introdotto la Compromissione delle difese come tattica distinta che comprende l'interferenza deliberata con i sistemi difensivi.

Le indagini di Acronis TRU sulle operazioni ransomware, incluse Qilin e The Gentlemen, dimostrano come gli attaccanti possano interrompere i processi di sicurezza, interferire con il monitoraggio e compromettere i meccanismi di ripristino.

Queste attività possono ridurre la visibilità dei difensori mentre gli attaccanti si muovono nelle reti, sottraggono informazioni o si preparano a crittografare i sistemi.

Il rischio è particolarmente elevato quando gli attaccanti assumono il controllo dei server di gestione o di account amministrativi utilizzati in più ambienti.



Sfondo del desktop di The Gentlemen

Impatto sulla sicurezza

Le organizzazioni dovrebbero monitorare in modo indipendente l'integrità degli agenti di sicurezza, le modifiche alle impostazioni di registrazione e i tentativi di disabilitare la protezione. L'amministrazione dei backup deve rimanere separata da quella ordinaria dei sistemi e i processi di ripristino devono essere testati in scenari che coinvolgono credenziali o infrastrutture compromesse.

4. Servizi e software affidabili vengono sfruttati per nascondere gli attacchi

Criminali informatici e operatori di spionaggio usano sempre più spesso piattaforme note, come GitHub, Telegram e servizi di cloud storage, per distribuire malware o comunicare con sistemi compromessi.

Poiché questi servizi supportano anche attività aziendali legittime, distinguere il traffico malevolo dall'uso autorizzato può risultare difficile.

Le indagini di Acronis TRU hanno documentato la distribuzione di malware tramite repository GitHub e l'uso di servizi cloud affidabili per le attività di comando e controllo.

La campagna TamperedChef ha evidenziato un altro punto debole dei segnali di affidabilità tradizionali: gli attaccanti hanno distribuito applicazioni malevole funzionanti dotate di certificati validi per la firma del codice, dimostrando che una firma legittima non prova che un software sia sicuro.

Impatto sulla sicurezza

Le organizzazioni dovrebbero valutare le attività delle applicazioni e dei servizi nel contesto, anziché basarsi esclusivamente sulla reputazione del dominio o sulle firme digitali. Download imprevisti, attività delle API cloud e connessioni di gestione remota richiedono un'indagine anche quando interessano servizi noti.



5. Le operazioni ransomware si adattano alle azioni di contrasto e si estendono oltre Windows

Le operazioni delle forze dell'ordine possono mettere fuori uso le infrastrutture dei criminali informatici, ma i loro strumenti e competenze restano spesso disponibili.

La ricerca di Acronis TRU mostra che affiliati a gruppi ransomware, codice sorgente pubblicato e tecniche di attacco condivise consentono ai criminali di riorganizzarsi e proseguire l'attività con nomi diversi.

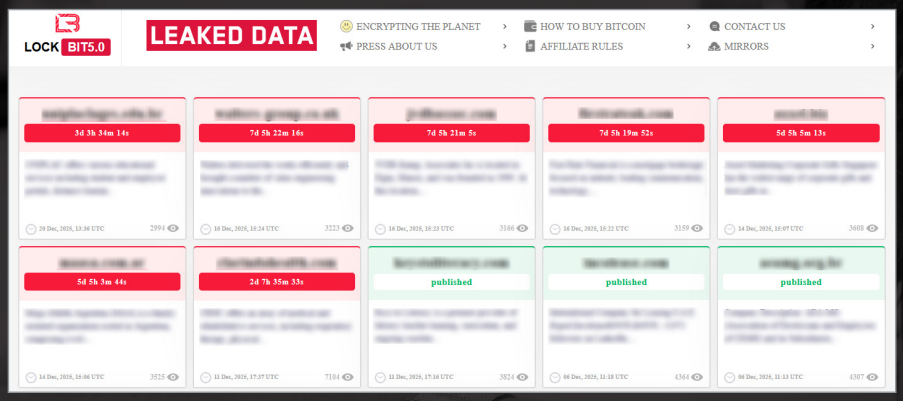
Si amplia anche l'ambito tecnico del ransomware:

LockBit 5.0 include varianti per Windows, Linux e VMware ESXi. Il ransomware INC ha dimostrato di poter colpire gli ambienti Linux ed ESXi, mentre Qilin ha utilizzato Windows Subsystem for Linux per eseguire un crittografatore Linux su Windows.

Puntando all'infrastruttura di virtualizzazione, gli attaccanti possono bloccare più workload e danneggiare sistemi essenziali per il ripristino aziendale.

Impatto sulla sicurezza

Le difese contro il ransomware devono coprire host Linux, hypervisor e gestione delle macchine virtuali. Le organizzazioni dovrebbero monitorare gli arresti imprevisti delle macchine virtuali e le eliminazioni di snapshot, assicurando che l'infrastruttura di ripristino rimanga accessibile anche durante una compromissione.



Il sito di LockBit 5.0 per la pubblicazione dei dati sottratti

6. Lo sfruttamento delle vulnerabilità e le relazioni di fiducia ampliano la portata delle intrusioni

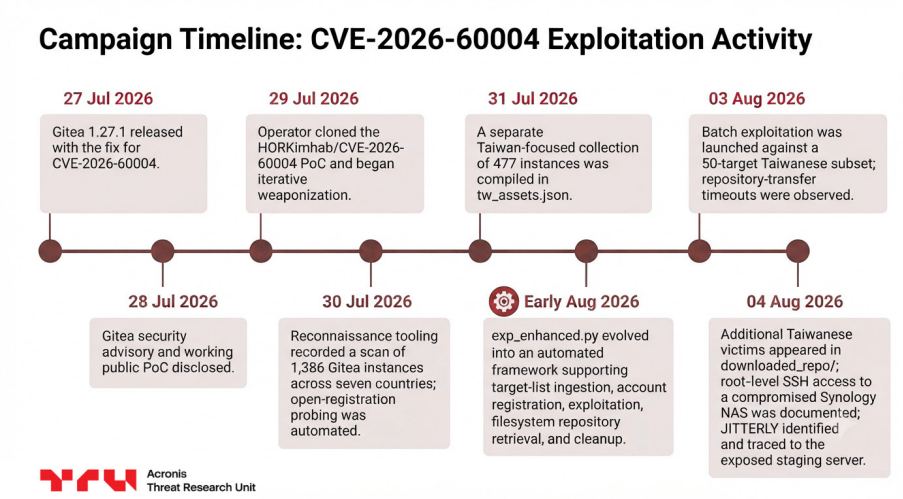
Le vulnerabilità appena divulgate vengono sfruttate con rapidità dagli attaccanti e alle organizzazioni resta sempre meno tempo per applicare gli aggiornamenti di sicurezza.

Nell'indagine Red Heron, gli attaccanti hanno adattato un exploit pubblico poco dopo la divulgazione di una vulnerabilità critica di Gitea. I server di sviluppo compromessi hanno esposto repository e credenziali che potevano favorire ulteriori intrusioni.

Le indagini sullo spionaggio hanno rivelato uno schema correlato: gli autori delle minacce sfruttano sempre più spesso le relazioni di fiducia per raggiungere gli obiettivi in modo indiretto.

I provider IT, gli ambienti di sviluppo e l'infrastruttura di distribuzione del software possono fornire l'accesso a organizzazioni che gli attaccanti non riescono a compromettere direttamente con facilità.

Questi attacchi hanno particolare rilievo per gli MSP, poiché un singolo servizio o un'unica identità compromessi possono esporre più clienti.



Impatto sulla sicurezza

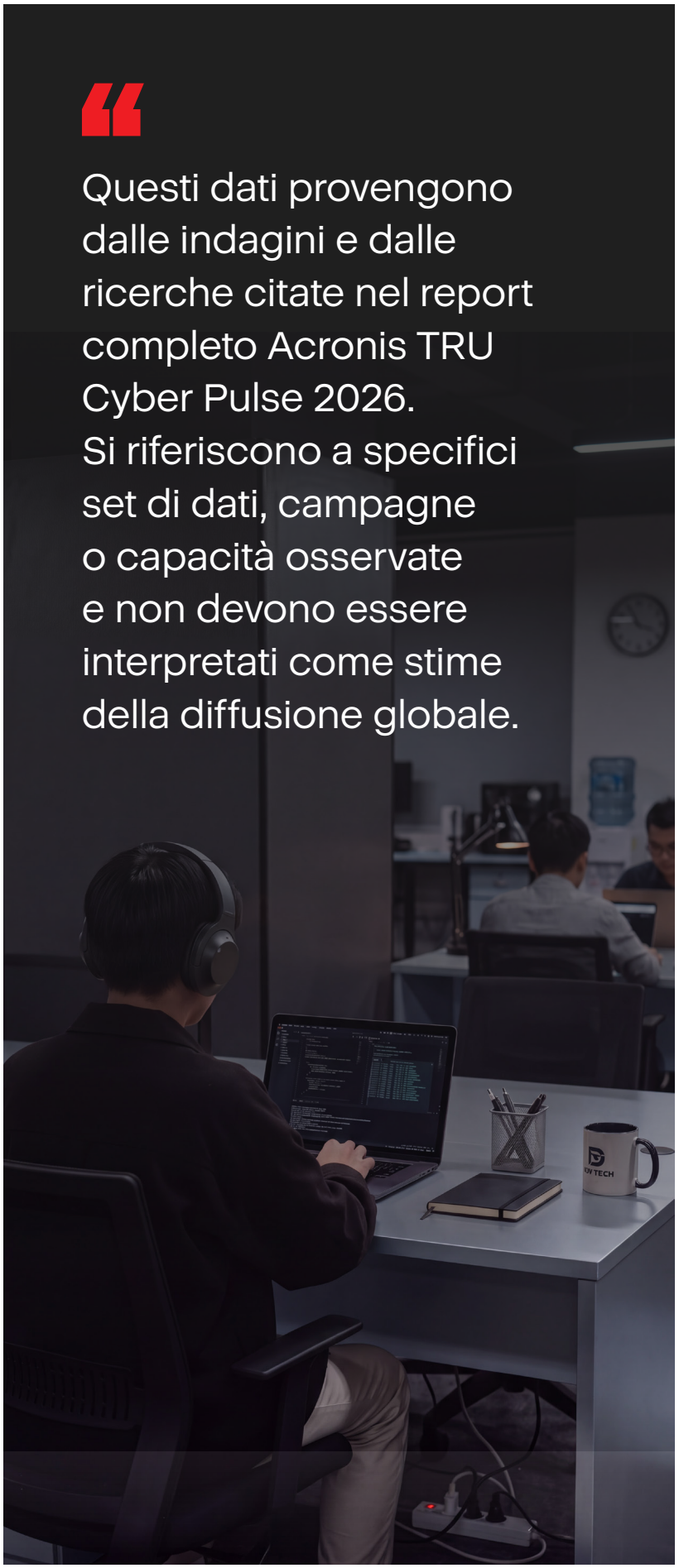
Le azioni correttive devono tenere conto delle possibilità di accesso fornite da un sistema e non solo della gravità delle vulnerabilità. Dopo un exploit, le organizzazioni devono indagare sulla persistenza, sulle credenziali sottratte e sulle attività negli ambienti connessi.

I risultati della ricerca in sintesi

I risultati selezionati di seguito illustrano la portata delle attività documentate nel report completo.

Risultato della ricerca | Riscontri riportati

- **Attacco potenziato dall'AI:** BOSSAI ha collegato più di 10 modelli di AI a strumenti di sicurezza informatica offensiva e a infrastrutture di supporto.
- **Minacce alla supply chain dell'AI:** TRU ha identificato più di 575 skill OpenClaw malevole, pubblicate da 13 account di sviluppatori.
- **Esposizione dell'accesso remoto:** in un'analisi condotta su oltre 1,8 milioni di endpoint che eseguivano Acronis RMM, è risultato che nel 63,1% dei casi era stato installato almeno un altro strumento RMM o di accesso remoto.
- **Ritardi nell'applicazione delle patch:** nel secondo semestre del 2025, TRU ha rilevato un tempo mediano di 5,7 giorni per il patching delle applicazioni di terze parti.
- **Espansione del ransomware:** LockBit 5.0 include varianti specifiche per ambienti Windows, Linux ed ESXi.



Le priorità per rafforzare la resilienza digitale



Dai risultati emergono cinque priorità pratiche per gli MSP e le organizzazioni che intendono ridurre l'impatto degli attacchi informatici.

1. Limitare la portata delle identità compromesse. Adottare forme di autenticazione resistente al phishing, limitare gli accessi con privilegi e mantenere la visibilità su sessioni, autorizzazioni delle applicazioni e connessioni di gestione remota.

2. Dare priorità alle vulnerabilità in base a esposizione e accesso. Accelerare la correzione delle vulnerabilità su sistemi esposti a Internet e amministrativi, in particolare su quelli che contengono credenziali o forniscono accesso ad altri ambienti. Dopo un sospetto exploit, indagare sulla persistenza e sull'esposizione delle credenziali.

3. Rilevare i tentativi di disabilitare la protezione. Monitorare i malfunzionamenti degli agenti di sicurezza, le attività impreviste dei driver e le modifiche alle impostazioni di registrazione o protezione. Considerare le lacune di visibilità inspiegate sui sistemi con privilegi come potenziali incidenti di sicurezza.

4. Proteggere l'infrastruttura critica e le capacità di ripristino. Estendere il monitoraggio agli ambienti Linux, di virtualizzazione e di backup. Separare le autorizzazioni di ripristino dall'amministrazione ordinaria e testare il ripristino quando i sistemi di gestione abituali non sono disponibili.

5. Definire limiti di sicurezza per gli agenti AI. Creare un inventario dei framework degli agenti, degli strumenti connessi e delle skill esterne. Limitarne le autorizzazioni, applicare la separazione tra gli ambienti dei clienti e richiedere un'approvazione indipendente per le azioni ad alto impatto.

Queste priorità condividono un obiettivo: ridurre l'accesso a disposizione degli attaccanti, rilevarne l'uso improprio e mantenere la capacità di ripristinare i servizi essenziali.

Conclusione: la resilienza digitale dipende dal controllo degli accessi connessi

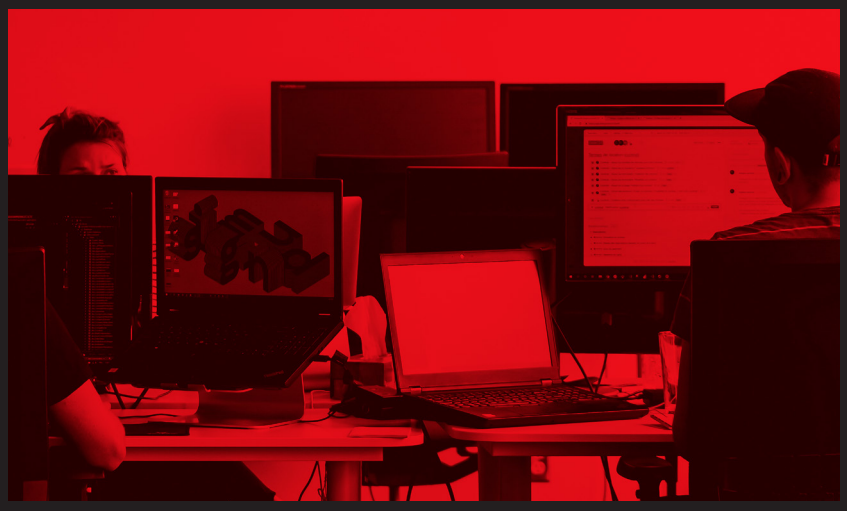
Il panorama delle minacce del 2026 si caratterizza non solo per le nuove tecniche di attacco, ma anche per la capacità degli autori delle minacce di sfruttare le connessioni tra identità, servizi e infrastrutture.

Gli agenti AI possono accelerare flussi di attacco già consolidati. Le credenziali sottratte possono dare accesso ad applicazioni cloud e ambienti dei clienti. Gli operatori ransomware possono interferire con i controlli di sicurezza e colpire l'infrastruttura necessaria al ripristino.

Per gli MSP e i responsabili IT, la sfida centrale è capire la portata di una compromissione e contenerla prima che gli attaccanti possano sfruttare altri sistemi.

Le organizzazioni che mantengono visibilità su identità, endpoint, servizi cloud e infrastruttura di ripristino saranno più preparate a rilevare le attività non autorizzate, contenere gli incidenti e ripristinare le attività critiche.

Leggi il report completo Acronis TRU Cyber Pulse 2026 per approfondire indagini, risultati tecnici e ulteriori raccomandazioni di sicurezza.



Informazioni sulla ricerca

Il report Acronis TRU Cyber Pulse 2026 sintetizza indagini sulle minacce, analisi di malware, ricerche sulle campagne e dati di telemetria Acronis rilevanti. Esamina le tecniche di attacco emergenti, le attività delle minacce persistenti avanzate e la criminalità informatica, con particolare attenzione alle implicazioni per gli MSP e i loro clienti.

Autori



Santiago Pontiroli,
Threat Intelligence Research Lead



Alexander Ivanyuk,
Senior Director, Technology

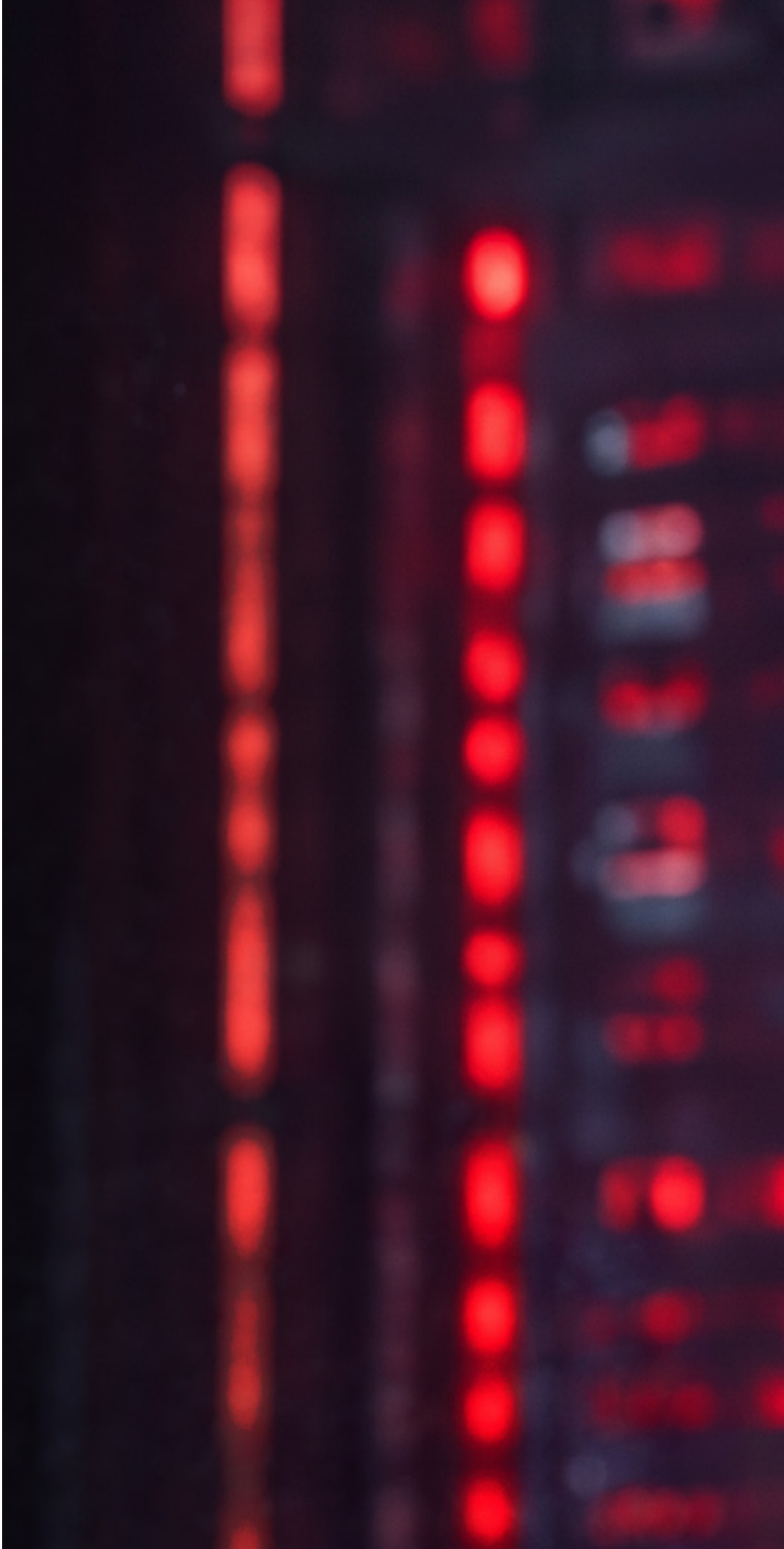


Eliad Kimhy,
Senior TRU Researcher



Subhajeet Singha,
Senior TRU Researcher

Acronis
Threat Research Unit



Copyright © 2003–2026 Acronis International GmbH. Tutti i diritti riservati. Acronis e il logo Acronis sono marchi registrati di Acronis International GmbH negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi o marchi registrati sono proprietà dei rispettivi proprietari. Soggetto a modifiche tecniche. Le immagini potrebbero non corrispondere al prodotto reale. Si declina qualsiasi responsabilità per possibili errori.

2026