

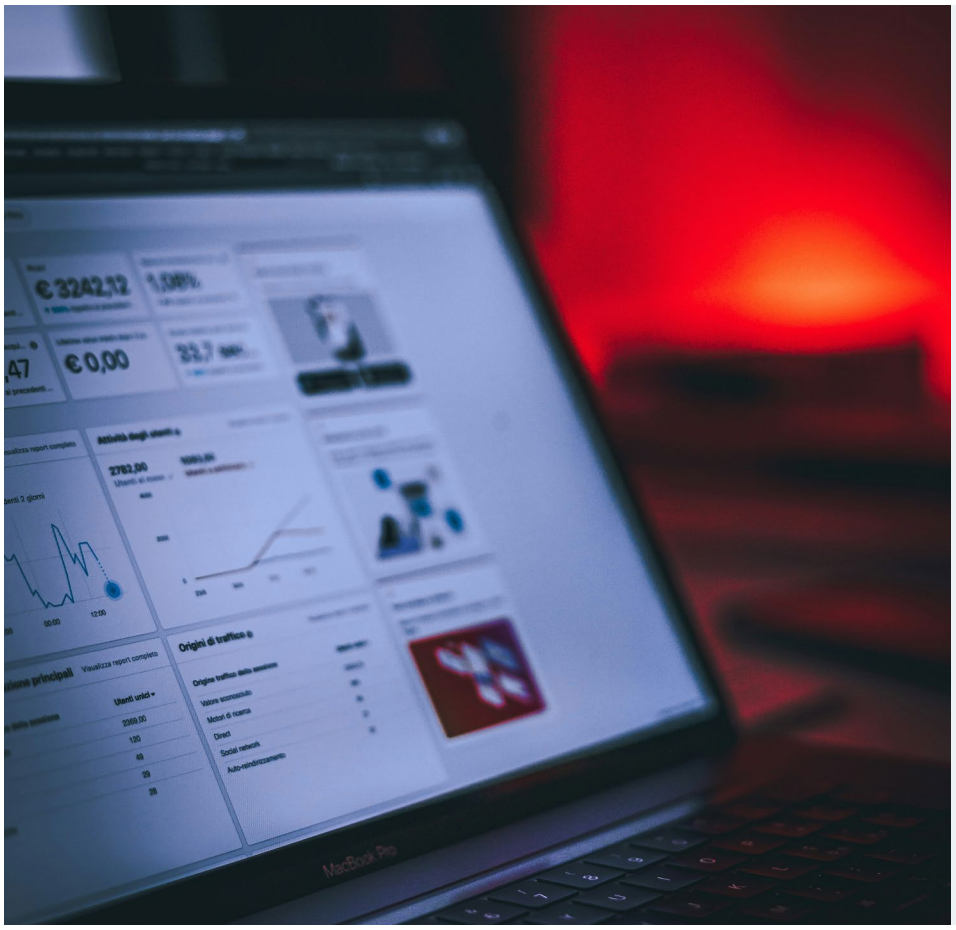
EXECUTIVE SUMMARY

Acronis TRU Cyber Pulse 2026

Key findings and security implications

Acronis
Threat Research Unit

Executive overview



Cyberattacks are evolving in ways that increase both the speed and reach of an intrusion.

Threat actors are using AI agents to automate attack workflows, exploiting stolen identities to move between connected services and targeting security controls to reduce detection and recovery capabilities.

The inaugural Acronis TRU Cyber Pulse 2026 report brings together investigations conducted by the Acronis Threat Research Unit (TRU) into emerging attack techniques, espionage activity and cybercrime. The findings reveal a common pattern: An initial compromise can provide access far beyond the affected device or account.

For managed service providers (MSPs), this creates particular risks. A compromised administrative identity, remote management tool or shared service can expose multiple client environments. Organizations must therefore understand not only how attackers gain access, but also how far that access can extend.

Six findings define the threat landscape examined in this report.

1. AI agents are expanding the scale of cyberattacks

Threat actors are moving beyond using AI for individual tasks, such as writing phishing messages or analyzing vulnerabilities. Some are integrating large language models with offensive security tools and messaging platforms, while using persistent memory to retain context and coordinate broader attack operations.

The Acronis TRU BOSSAI investigation illustrates this development. A single operator connected more than 10 models to offensive frameworks and supporting infrastructure, enabling coordinated reconnaissance, exploitation and infrastructure management across targets in several countries.

These findings demonstrate how agentic systems can reduce the manual effort required to conduct complex operations.

AI adoption also introduces new attack surfaces. TRU identified more than 575 malicious OpenClaw skills across 13 developer accounts. These packages impersonated legitimate utilities while delivering 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 redirected through MiniMax.

Security implication:

Organizations must treat AI agents and their connected tools as privileged systems. Agent permissions, external skills, credentials and network access require independent security controls and monitoring.

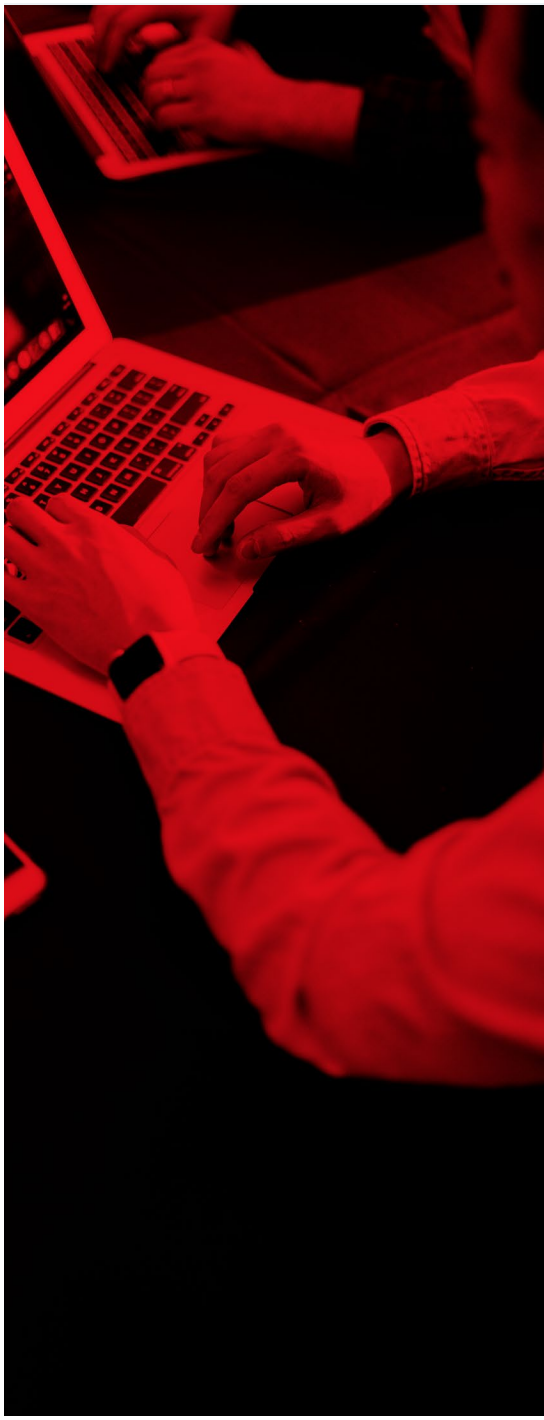
2. Stolen identities are becoming a primary route to wider compromise

Infostealers and identity-focused attacks increasingly target credentials, authentication tokens, browser sessions and cloud access.

Attackers can use this information to access connected applications and services, sometimes without triggering a new multifactor authentication challenge. Stolen access may also be transferred or sold to other threat actors, including ransomware operators and espionage groups.

The risk extends to developer environments. Recent investigations identified malware targeting AI service API keys, repository credentials and other development secrets. These credentials can provide access to additional systems and projects.

For MSPs, privileged identities are particularly valuable because they may provide access to multiple clients.



Security implication:

Removing malware or resetting a password is not sufficient. Incident response must include revoking exposed sessions, rotating credentials, reviewing authentication changes and investigating connected services.

3. Attackers are deliberately weakening security and recovery controls

Disabling security tools has become an important part of modern intrusion activity.

In April 2026, MITRE ATT&CK introduced Defense Impairment as a distinct tactic covering deliberate interference with defensive systems.

Acronis TRU investigations into ransomware operations, including Qilin and The Gentlemen, demonstrate how attackers can terminate security processes, interfere with monitoring and disrupt recovery mechanisms.

These activities can reduce defenders' visibility while attackers move through networks, steal information or prepare to encrypt systems.

The risk is especially significant when attackers gain control of management servers or administrative accounts used across multiple environments.



The Gentlemen desktop wallpaper

Security implication:

Organizations should independently monitor security agent health, logging changes and attempts to disable protection. Backup administration must remain separate from routine system administration, and recovery processes must be tested against scenarios involving compromised credentials or infrastructure.

4. Trusted services and software are being exploited to conceal attacks

Cybercriminals and espionage operators increasingly use familiar platforms, including GitHub, Telegram and cloud storage services, to distribute malware or maintain communication with compromised systems.

Because these services also support legitimate business activity, malicious traffic can be difficult to distinguish from authorized use.

Acronis TRU investigations documented malware distribution through GitHub repositories and the use of trusted cloud services for command and control.

The TamperedChef campaign demonstrated another weakness in traditional trust signals. Attackers distributed functional malicious applications carrying valid code-signing certificates, illustrating that a legitimate signature does not establish that software is safe.

Security implication:

Organizations should evaluate application and service activity in context rather than relying solely on domain reputation or digital signatures. Unexpected downloads, cloud API activity and remote management connections require investigation even when they involve familiar services.



5. Ransomware operations are adapting to disruption and expanding beyond Windows

Law enforcement operations can disrupt cybercriminal infrastructure, but the tools and expertise behind those operations may remain available.

Acronis TRU research shows that ransomware affiliates, leaked source code and shared attack techniques enable criminal operations to reorganize and continue activity under different names.

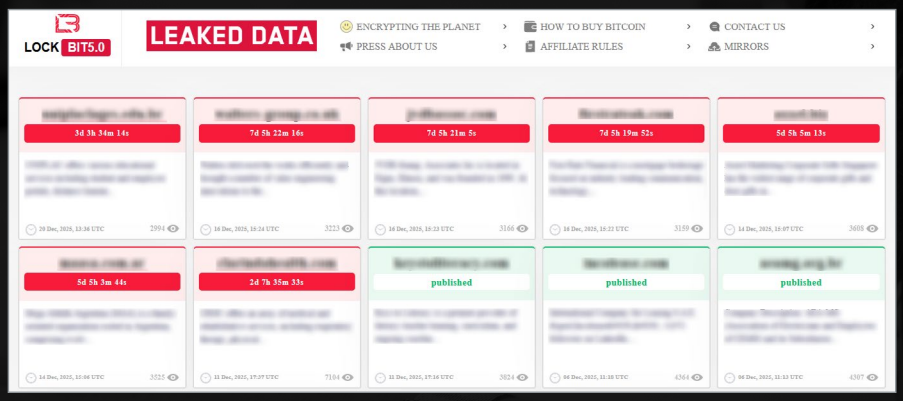
The technical scope of ransomware is also expanding.

LockBit 5.0 includes Windows, Linux and VMware ESXi variants. INC ransomware has demonstrated capabilities targeting Linux and ESXi environments, while Qilin has used Windows Subsystem for Linux to execute a Linux encryptor on Windows.

By targeting virtualization infrastructure, attackers can disrupt multiple workloads and affect systems essential to business recovery.

Security implication:

Ransomware defenses must cover Linux hosts, hypervisors and virtual machine management. Organizations should monitor unexpected virtual machine shutdowns and snapshot deletion, while ensuring recovery infrastructure remains accessible during a compromise.



Lockbit 5.0 data leak site

6. Vulnerability exploitation and trusted relationships are increasing the reach of intrusions

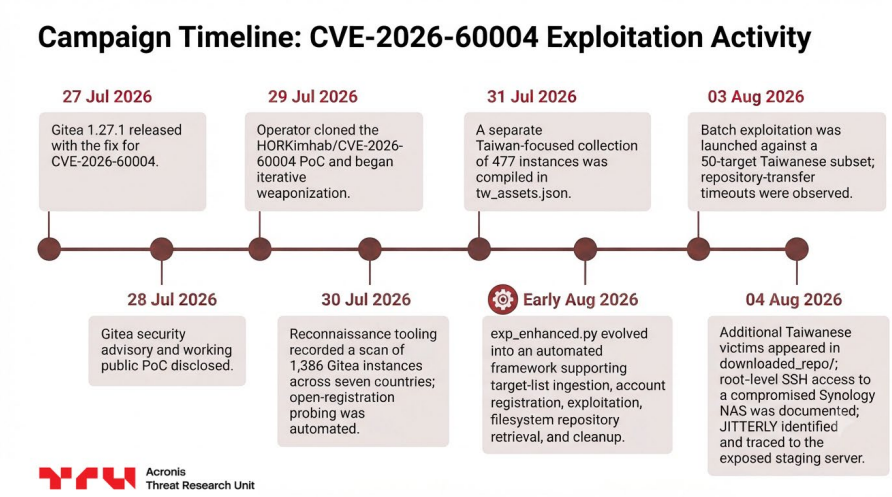
Attackers are exploiting newly disclosed vulnerabilities quickly, reducing the time available for organizations to deploy security updates.

In the Red Heron investigation, attackers adapted a publicly available exploit shortly after the disclosure of a critical Gitea vulnerability. Compromised development servers exposed repositories and credentials that could support further intrusion activity.

Espionage investigations revealed a related pattern: Threat actors increasingly exploit trusted relationships to reach targets indirectly.

IT providers, development environments and software distribution infrastructure can provide access to organizations that attackers cannot easily compromise directly.

These attacks are especially consequential for MSPs because a single compromised service or identity may expose multiple clients.



Security implication:

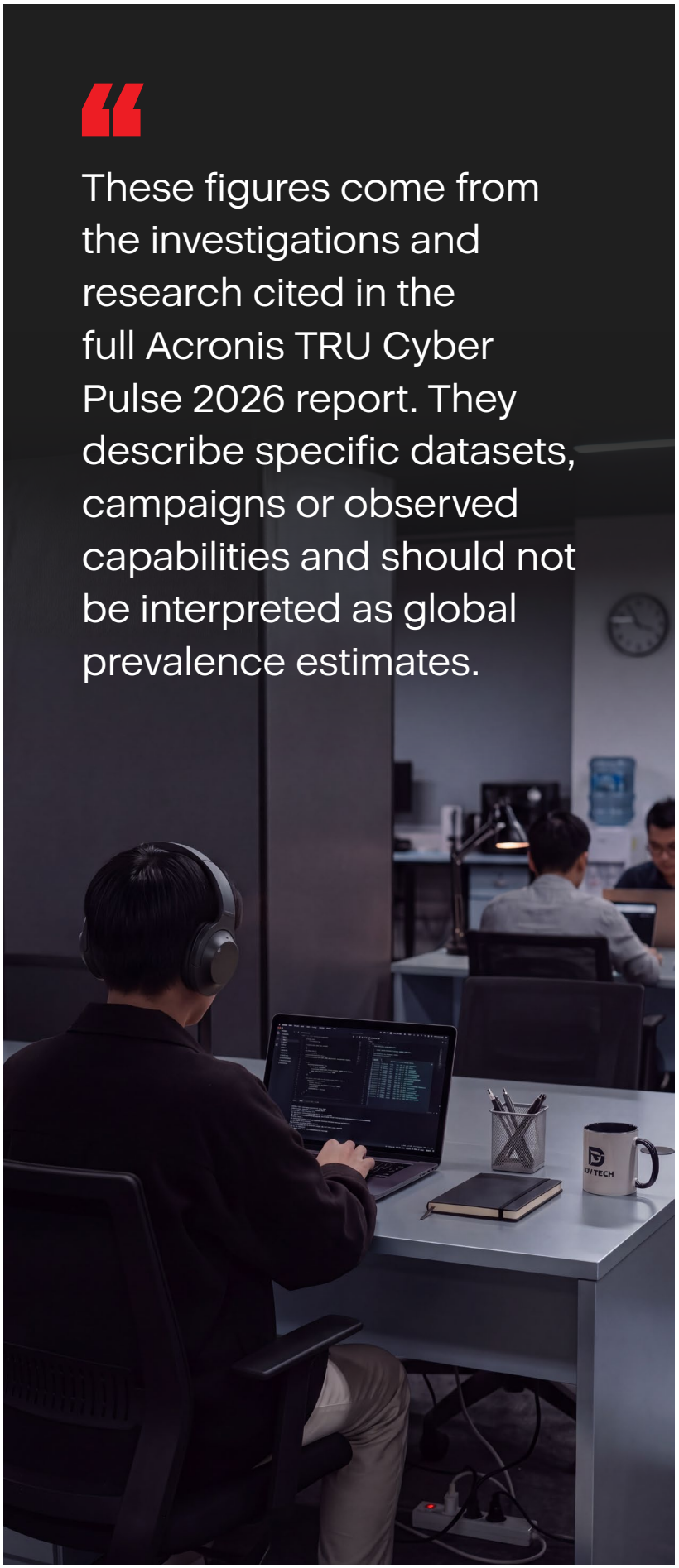
Vulnerability remediation must consider the access a system provides, not only the severity of the vulnerability. Following exploitation, organizations must investigate persistence, stolen credentials and activity across connected environments.

Research findings at a glance

The following selected findings illustrate the scope of the activity documented in the full report.

Research finding | Reported evidence

- **AI-enabled attack:** BOSSAI connected more than 10 AI models to offensive tools and supporting infrastructure.
- **AI supply chain threats:** TRU identified more than 575 malicious OpenClaw skills across 13 developer accounts.
- **Remote access exposure:** In an analysis of more than 1.8 million endpoints running Acronis RMM, 63.1% had at least one additional RMM or remote-access tool installed.
- **Patching delays:** TRU reported a median third-party application patching time of 5.7 days in the second half of 2025.
- **Ransomware expansion:** LockBit 5.0 includes variants targeting Windows, Linux and ESXi environments.



Priorities for stronger cyber resilience



The findings point to five practical priorities for MSPs and organizations seeking to reduce the impact of cyberattacks.

1. Limit the reach of compromised identities. Apply phishing-resistant authentication, restrict privileged access and maintain visibility into sessions, application permissions and remote management connections.

2. Prioritize vulnerabilities based on exposure and access. Accelerate remediation of internet-facing and administrative systems, particularly those containing credentials or providing access to other environments. Investigate persistence and credential exposure after suspected exploitation.

3. Detect attempts to disable protection. Monitor security agent failures, unexpected driver activity and changes to logging or protection settings. Treat unexplained visibility gaps on privileged systems as potential security incidents.

4. Protect critical infrastructure and recovery capabilities. Extend monitoring to Linux, virtualization and backup environments. Separate recovery permissions from routine administration and test restoration when normal management systems are unavailable.

5. Establish security boundaries for AI agents. Inventory agent frameworks, connected tools and external skills. Restrict their permissions, enforce separation between client environments and require independent approval for high-impact actions.

These priorities share a common objective: Reduce the access available to attackers, detect its misuse and maintain the ability to recover essential services.

Conclusion: Cyber resilience depends on controlling connected access

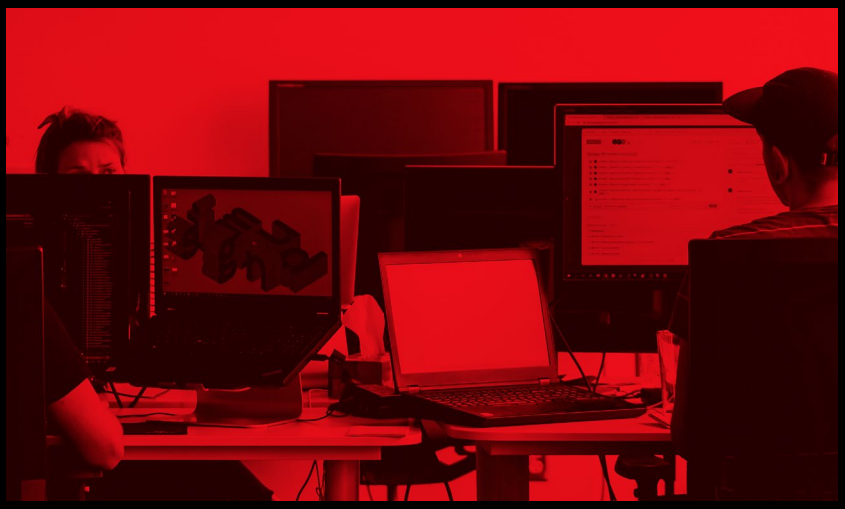
The 2026 threat landscape is defined not only by new attack techniques, but also by the ability of threat actors to exploit connections between identities, services and infrastructure.

AI agents can accelerate established attack workflows. Stolen credentials can provide access across cloud applications and client environments. Ransomware operators can interfere with security controls and target the infrastructure needed for recovery.

For MSPs and IT leaders, the central challenge is understanding the reach of a compromise and containing it before attackers can exploit additional systems.

Organizations that maintain visibility across identities, endpoints, cloud services and recovery infrastructure will be better positioned to detect unauthorized activity, contain incidents and restore critical operations.

Explore the full Acronis TRU Cyber Pulse 2026 report for detailed investigations, technical findings and additional security recommendations.



About this research

The Acronis TRU Cyber Pulse 2026 report synthesizes threat investigations, malware analysis, campaign research and relevant Acronis telemetry. It examines emerging attack techniques, advanced persistent threat activity and cybercrime, with particular attention to implications for MSPs and their clients.

Authors



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. All rights reserved. Acronis and the Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and differences from the illustrations are reserved; errors are excepted.

2026