

Cyber threat bulletin: Agentic artificial intelligence is accelerating cyber attacks



Communications Security
Establishment Canada

Canadian Centre
for Cyber Security

Centre de la sécurité des
télécommunications Canada

Centre canadien
pour la cybersécurité

Canada

Table of contents

Overview	2
A sign of what is changing	2
Why the Cyber Centre is warning Canadians	3
What organizations should do	4
Preparing critical infrastructure.....	4
Reporting cyber incidents	6
Useful resources.....	6



Overview

A long-anticipated change in cyber security is beginning to take shape.

Artificial intelligence (AI) has already made it easier to find weaknesses, develop malicious code and attack many organizations at once. These are more powerful versions of familiar cyber threats. Agentic AI goes further by linking separate stages of an attack and carrying them out with less human direction.

Recent malicious cyber activities conducted by Storm-0940 exemplify this trend, pointing to a fundamental evolution of malign techniques which can be employed by a range of different threat actors. The actor used an agentic AI framework to carry out and coordinate several stages of a cyber attack.¹ It could search for targets, test ways into systems, explore compromised networks and seek greater access. It could do this rapidly, repeatedly and across many organizations.

The most important development is not the identity of one threat actor or the details of one campaign. It is the emergence of a reusable framework that can help conduct cyber operations on an industrial scale.

Cyber attacks are not yet fully autonomous. Humans still choose the targets, set the objectives and oversee the operation. However, more of the work between those decisions can now be delegated to machines. This gives defenders less time to detect and stop an attack.

A sign of what is changing

Storm-0940 used an agentic AI framework known as ARTEX against hundreds of organizations. In some cases, the activity moved from selecting a target to gaining privileged access to cloud systems in less than three hours.²

¹ Agentic AI refers to AI systems that can plan and carry out a series of tasks with limited human direction. ARTEX is one example of a broader shift toward AI systems that can plan and execute multiple stages of a cyber attack. Several publicly available frameworks support automated security testing, and threat actors have also abused general-purpose AI agents to conduct cyber operations. These systems differ in capability and degree of autonomy, but the trend extends beyond one tool or campaign: more of an attack can be delegated to machines, increasing its speed and scale and reducing the time available for defenders to respond.

² Microsoft Security Research and Microsoft Threat Intelligence. [AI-Driven, Large-Scale Nation-State Campaign Using ARTEX Enables Supply Chain Compromise](#). Microsoft Security Blog. October 21, 2026.



The framework helped identify targets, test passwords and explore compromised systems. None of these techniques are new. What is new is the ability to link them together, automate them and repeat them across many targets.

Storm-0940 offers an early view of how AI is reshaping cyber operations. Weakly protected accounts, excessive access, exposed systems, unpatched software and gaps in monitoring remain common ways into an organization. Agentic AI can help threat actors find and exploit these weaknesses more quickly and on a much larger scale.

Why the Cyber Centre is warning Canadians

The Canadian Centre for Cyber Security (Cyber Centre) has warned for some time that AI is lowering barriers to malicious cyber activity and increasing the speed, scale and sophistication of cyber threats.³ The activities made public this week gives that warning new urgency.

As automated agents become more capable, organizations may face attacks that move across several systems at once. Machines can act faster than many existing processes and policies were designed to handle. Decisions that once allowed time for discussion may soon have to be made within minutes.

This is especially important for critical infrastructure. An incident involving a cloud provider, supplier, identity system or operational technology can spread beyond the organization first compromised. It can disrupt essential services and cause physical and economic harm across sectors. This makes it a risk to Canada's national and economic security.

The Cyber Centre is prioritizing the security and resilience of Canada's most important digital systems, both within the Government of Canada and across critical infrastructure. We are also helping critical infrastructure owners and operators prepare to continue essential services during a serious cyber incident.

For now, much of this activity is widespread and noisy enough to be detected by sophisticated cyber defenders. We assess that AI-enabled cyber activity will likely become more targeted, less visible and harder to detect as the technology improves.

³ Canadian Centre for Cyber Security. [National Cyber Threat Assessment 2025-2026](#). Government of Canada. September 20, 2024; Canadian Centre for Cyber Security. [Five Eyes Cyber Security Agencies Statement on the AI Shift in Cyber Risk: Why Leaders Must Act Now](#). June 22, 2026.



What organizations should do

Agentic AI does not make established cyber security practices obsolete. It makes them more important.

The Cyber Centre has long warned that Canadians and Canadian organizations face greater risk when basic cyber security practices are not consistently applied.⁴

Organizations should:

- require phishing-resistant multi-factor authentication for administrators, remote access and other important accounts
- limit the access given to users, applications and service accounts
- review access granted to third-party and shared cloud applications
- patch Internet-facing systems promptly and remove services that are no longer needed
- retain security logs and monitor for unusual sign-ins, new credentials and unexpected changes in access
- decide in advance who can isolate an account, application, network or service
- practice responding to incidents that unfold within hours rather than days
- separate important systems and maintain tested offline or protected backups

These measures reduce an attacker's options. AI increases the consequences of weak controls and slow decisions, but the fundamentals of good cyber security remain effective.

Preparing critical infrastructure

Prevention alone is not enough. Critical infrastructure owners and operators must prepare for the possibility that important systems, suppliers or communications will become unavailable or cannot be trusted.

⁴ Canadian Centre for Cyber Security. [Top 10 IT Security Actions](#). January 13, 2021; Canadian Centre for Cyber Security. [Top Measures to Enhance Cyber Security for Small and Medium Organizations \(ITSAP10.035\)](#). February 2024.



Through the [Critical Infrastructure Resilience and Escalated Threat Navigation \(CIREN\) initiative](#)⁵, the Cyber Centre is helping organizations prepare for serious and prolonged cyber disruption while continuing to provide essential services to Canadians.

CIREN focuses on three practical capabilities:

- isolating critical systems
- operating essential services independently during a wider disruption
- rebuilding affected systems from trusted offline sources

Critical infrastructure owners and operators should:

- identify the minimum functions needed to protect life and safety and continue essential services
- establish clear, pre-authorized procedures for isolating critical systems and external connections
- test safe manual or alternative ways of operating
- determine which services can be reduced or paused during a crisis
- understand their dependence on telecommunications, cloud services, utilities, suppliers and specialized personnel
- maintain trusted offline copies of essential software, configurations, instructions and recovery material
- test how information technology and operational technology systems will be restored and checked before they are reconnected

The objective is not to maintain normal operations under every condition. It is to protect life and safety, limit wider harm and continue providing those minimal viable services that Canadians depend on while operating within a reduced capacity.

⁵ Canadian Centre for Cyber Security. [Critical Infrastructure Resilience and Escalated Threat Navigation \(CIREN\) initiative](#). September 18, 2026.

Reporting cyber incidents

Organizations that experience suspicious or malicious cyber activity should report it to the Cyber Centre via [our online portal](#). Victims of cybercrime should also report the incident to local police and the [Canadian Anti-Fraud Centre](#), as appropriate.

For follow-up questions or issues, contact the Canadian Centre for Cyber Security at contact@cyber.gc.ca.

Useful resources

Refer to the following online resources for more information and for advice and guidance.

- [National Cyber Threat Assessment 2025–2026 –Canadian Centre for Cyber Security](#)
- [Five Eyes Cyber Security Agencies Statement on the AI Shift in Cyber Risk: Why Leaders Must Act Now –Canadian Centre for Cyber Security](#)
- [Frontier Artificial Intelligence \(ITSAP.10.050\) –Canadian Centre for Cyber Security](#)
- [Top 10 Artificial Intelligence Security Actions: A Primer \(ITSAP.10.049\) –Canadian Centre for Cyber Security](#)
- [Critical Infrastructure Resilience and Escalated Threat Navigation Initiative –Canadian Centre for Cyber Security](#)
- [Top 10 IT Security Actions to Protect Internet-Connected Networks and Information \(ITSM.10.089\) –Canadian Centre for Cyber Security](#)
- [Foundational Cyber Security Actions for Small Organizations \(ITSAP.10.300\) –Canadian Centre for Cyber Security](#)
- [Cyber Security Readiness Goals: Securing Our Most Critical Systems –Canadian Centre for Cyber Security](#)

