Global ransomware threat expected to rise with AI, NCSC warns

New assessment focuses on how AI will impact the efficacy of cyber operations and the implications for the cyber threat over the next two years.

- AI is expected to heighten the global ransomware threat, says GCHQ's National Cyber Security Centre
- New report suggests artificial intelligence will almost certainly increase the volume and impact of cyber attacks in the next two years
- NCSC urges organisations and individuals to implement protective measures

Artificial intelligence (AI) is expected to increase the global ransomware threat over the next two years cyber chiefs have warned in a new report published today (Wednesday).

The near-term impact of AI on the cyber threat assessment, published by the National Cyber Security Centre (NCSC), a part of GCHQ, concludes that AI is already being used in malicious cyber activity and will almost certainly increase the volume and impact of cyber attacks – including ransomware – in the near term.

Among other conclusions, the report suggests that by lowering the barrier of entry to novice cyber criminals, hackers-for-hire and hacktivists, AI enables relatively unskilled threat actors to carry out more effective access and information-gathering operations. This enhanced access, combined with the improved targeting of victims afforded by AI, will contribute to the global ransomware threat in the next two years.

Ransomware continues to be the most acute cyber threat facing UK organisations and businesses, with cyber criminals adapting their business models to gain efficiencies and maximise profits.

To tackle this enhanced threat, the Government has invested £2.6 billion under its Cyber Security Strategy to improve the UK's resilience, with the NCSC and private industry already adopting AI's use in enhancing cyber security resilience through improved threat detection and security-by-design.

The Bletchley Declaration, agreed at the UK-hosted AI Safety Summit at Bletchley Park in November, also announced a first-of-its-kind global effort to manage the risks of frontier AI and ensure its safe and responsible development. In the UK, the AI sector already employs 50,000 people and contributes £3.7 billion to the economy, with the government dedicated to ensuring the national economy and jobs market evolve with technology as set out under the Prime Minister's five priorities.

NCSC CEO Lindy Cameron said:

> "We must ensure that we both harness AI technology for its vast potential and manage its risks – including its implications on the cyber threat.
>
> "The emergent use of AI in cyber attacks is evolutionary not revolutionary, meaning that it enhances existing threats like ransomware but does not transform the risk landscape in the near term.
>
> "As the NCSC does all it can to ensure AI systems are secure-by-design, we urge organisations and individuals to follow our ransomware and cyber security hygiene advice to strengthen their defences and boost their resilience to cyber attacks."

Analysis from the NCA suggests that cyber criminals have already started to develop criminal Generative AI (GenAI) and to offer 'GenAI-as-a-service', making improved capability available to anyone willing to pay. Yet, as the NCSC's new report makes clear, the effectiveness of GenAI models will be constrained by both the quantity and quality of data on which they are trained.

The growing commoditisation of AI-enabled capability mirrors warnings from a report jointly published by the two agencies in September 2023 which described the professionalising of the ransomware ecosystem and a shift towards the "ransomware-as-a-service" model.

According to the NCA, it is unlikely that in 2024 another method of cyber crime will replace ransomware due to the financial rewards and its established business model.

James Babbage, Director General for Threats at the National Crime Agency, said:

> "Ransomware continues to be a national security threat. As this report shows, the threat is likely to increase in the coming years due to advancements in AI and the exploitation of this technology by cyber criminals.
>
> "AI services lower barriers to entry, increasing the number of cyber criminals, and will boost their capability by improving the scale, speed and effectiveness of existing attack methods. Fraud and child sexual abuse are also particularly likely to be affected.
>
> "The NCA will continue to protect the public and reduce the serious crime threat to the UK, including by targeting criminal use of GenAI and ensuring we adopt the technology ourselves where safe and effective."

Effective preparation is central to preventing ransomware attacks. Implementing the NCSC's advice, such as the simple protective measures outlined in its ransomware guidance, will help UK organisations to reduce their likelihood of being infected.

Most ransomware incidents typically result from cyber criminals exploiting poor cyber hygiene, rather than sophisticated attack techniques. The NCSC's 10 Steps to Cyber Security and Top tips for staying secure online set out how organisations and individuals respectively can protect themselves in cyberspace.

The *near-term impact of AI on the cyber threat* report outlines further ways in which AI will impact the effectiveness of cyber operations and the cyber threat over the next two years – including social engineering and malware. Read the report in full.

Tackling the challenges of securing future technology is a key priority area for the

NCSC having published its *Guidelines for Secure AI System Development* in November with the endorsement of 17 other countries. CYBERUK 2024, taking place in Birmingham on 13-15 May, will elaborate on these themes with its focus on “Future Tech, Future Threat, Future Ready”. A full programme will be issued in the coming days.

PUBLISHED

24 January 2024

WRITTEN FOR

Large organisations

Cyber security professionals

Small & medium sized organisations

Public sector

NEWS TYPE

General news