

NCC Group Monthly Threat Pulse – Review of July 2026

Archived: 2026-09-04 02:00:25 UTC

Ransomware reaches 2026 high in July, up by 22%

- Ransomware volume rose 22% month-on-month, with 894 cases recorded in July
- Industrials remain top target as sector takes over a quarter (28%) of attacks
- Western regions are still most targeted with North America experiencing 41%, and Europe 29%, of all attacks
- Threat group, The Gentlemen, conducted 15% of all attacks

[Read the report](#)

August 2026 - Ransomware levels peaked in July, reaching the highest volume since the start of the year and up 22% since June 2026.

The rise in volume is reported in NCC Group's monthly Threat Intelligence Report for July, which recorded a year-to-date high of 894 cases of ransomware activity for the month. This is only 19% lower than the current monthly record, which is 1,099 attacks in February 2025.

North America and Europe remain prime regional targets

In line with recent trends, North America and Europe have continued to be the most targeted regions for ransomware activity. Almost three quarters (70%) of ransomware attacks occurred across the two continents - 41% in North America and 29% in Europe.

New ransomware group emerges, but threat remains uncertain

The new ransomware group CRPxO has claimed responsibility for 36 victims in July. However, NCC Group warns that its credibility is not yet guaranteed, with inconsistent evidence that it is behind the attacks. This is a common tactic of new ransomware groups – they make false claims about their activity levels to create an exaggerated sense of threat.

In July, prominent threat group The Gentlemen continued to assert its dominance across the global landscape, responsible for 15% of all attacks.

AI advancements accelerate attacks

The rise of ransomware activity in July was driven in part by advancements in AI. JADEPUFFER, the first known fully autonomous end-to-end AI-driven agent, demonstrated its ability to infiltrate systems and conduct attacks without human instruction. As competition in AI continues to intensify, similar future attacks could become more common, raising concerns that future increases in attack volume may be driven less by new tactics and more by the proliferation of autonomous agents.

AI agents capable of operating without human intervention can adapt and execute an attack from initial compromise through to extortion. So far, these attacks appear to have been motivated less by financial gain and more by demonstrating what the technology can achieve. Now that the concept has been proven, further development could enable cyber criminals to conduct attacks with greater speed and scale.

Matt Hull, Vice President of Cyber Intelligence and Response at NCC Group said:

“AI is changing the speed and scale of cyber attacks. It’s allowing attackers to automate more of what they do, operate at greater scale and create increasingly convincing phishing, social engineering and other malicious content. That can make threats harder for both organisations and individuals to identify.

For organisations, the response doesn’t need to be complicated. Getting the fundamentals right remains incredibly important: strong identity and access controls, good vulnerability management, visibility across your environment and the ability to detect and respond quickly when something goes wrong.

There’s also a human element. As AI-generated content becomes more convincing, employees need to understand what threats look like, know when something doesn’t feel right and have a simple way to report it.

AI is equally valuable for defenders, helping security teams process information faster and identify potentially malicious activity. The challenge is making sure we use that technology effectively while maintaining the human judgement needed to understand what represents a genuine threat.”

Speaker biography

Matt Hull is Vice President of Cyber Intelligence and Response at NCC Group, leading the global Cyber Response and Intelligence (CRI) capability.

A former Detective Constable specialising in cybercrime, Matt brings deep operational experience across investigation, response, and intelligence-led operations. He leads multidisciplinary teams supporting organisations through complex incidents, advanced threat activity, and the development of mature detection and response capabilities.

Matt is recognised across the industry for his authenticity and clear communication, speaking at major conferences and featuring in media including BBC News, the Financial Times and Channel 4’s Hunted. He also serves as Chair of the Threat Intelligence Focus Group and sits on the CREST International Council.

Source: <https://www.nccgroup.com/newsroom/ncc-group-monthly-threat-pulse-review-of-july-2026/>