NCC Group Monthly Threat Pulse – Review of July 2024

22 August 2024

Press Release Threat Intelligence

The Holiday period sees significant increase in ransomware activity across July.

- Total ransomware cases in July were 20% higher than the previous month, with 395 attacks compared to 331
- Threat actor RansomHub dominates the threat landscape with 11% of attacks.
- Industrials continues to climb as most targeted sector, accounting for 34% of attacks.
- North America and Europe combined accounted for 77% of all cases.

August 2024 – In July 2024, global levels of ransomware attacks increased month-on-month (331 to 395) but decreased year-on-year (502 to 395), according to NCC Group's July Threat Pulse.

This month-on-month increase could be attributed to the holiday period kicking in across many parts of the world, during which time threat actors may seek to exploit the decrease in employee presence at work, including in IT security and support departments.

RansomHub dominates the threat landscape

RansomHub emerged as the most active threat actor this month with 43 attacks, up from 27 in June. This accounted for 11% of all activity for the month and reflects a continued hold on the threat landscape by the group.

LockBit 3.0 secured second position with 37 attacks; this figure is incomparable to the high numbers observed prior to their takedown.

Akira came in third with 29 attacks followed by Hunters with 25, Play with 20, and Meow with 16.

Oceania faces noticeable surge in global attacks

North America remained the most targeted region, representing 56% of total global attacks (220). Europe followed with 21% of attacks (83), a slight decrease from 90 in June.

Oceania faced a notable surge, with attacks doubling from 10 in June to 22 in July, now 6% of the global total.

South America reported a 29% increase or from 14 to 18 ransomware incidents, while Africa saw an increase from 4 to 10 incidents. There is expected to be a continued rise in attacks within these continents as threat actors continue to exploit the lower levels of cyber security infrastructure and readiness within these regions.

Attack levels continue to soar for Industrials

The Industrials sector remains the primary target for cyber attacks, representing 34% (125) of all incidents in July. This ongoing focus on the sector highlights the persistent interest of threat actors in compromising critical national infrastructure (CNI).

Given the essential nature of the services provided by this sector, attackers capitalise on the sector's need to remain operational. The increasing integration of Operational Technology (OT) within IT systems has also expanded the attack surface, offering more potential entry points for ransomware attacks.

The Consumer Cyclicals sector experienced the second-highest number of attacks (48), with Hotels and Entertainment services identified as the most frequently targeted.

As it is the summer period, the data suggests that ransomware actors are strategically timing their attacks to coincide with peak holiday periods in some regions to maximise disruption and pressure organisations into payment. So, businesses in this sector should prioritise reinforcing their ransomware defences.

With 44 attacks recorded, the Healthcare sector closely followed in terms of incidents. In the UK, the mid-July warning from the NHS chief executive reinforced the sector's vulnerability, following the ransomware incidents in June. This serves as a stark reminder of the tangible, long-lasting impacts that ransomware attacks can have on healthcare services, emphasising the critical need for robust cyber security measures in this sector.

A significant portion of ransomware activity in July was driven by the exploitation of a critical VMware ESXi vulnerability. This allowed attackers to gain full administrative privileges, enabling them to steal sensitive data and encrypt virtual machines. The attacks stress the importance of active patching to mitigate against ransomware across sectors.

Ian Usher, Deputy Head of Threat Intelligence at NCC Group, said:

"July 2024 has been a stark reminder that the cyber security landscape is as turbulent as ever, marked by a surge in ransomware attacks and the spread of misinformation. The Industrials, Consumer Cyclicals, and Technology sectors have borne the brunt of these attacks, with groups like RansomHub and LockBit 3.0 leading the charge.

“The rise in sophisticated techniques, such as the use of information stealer malware in their pre-attack phase, highlights that cybercriminals are not standing still. As these threats evolve, so must our defences. It's crucial that we leverage the latest technologies and maintain robust, intelligence-driven security measures to stay ahead, or risk falling behind in this ever-escalating battle.”

Download Report