NCC Group Monthly Threat Pulse November 2021. Illustrated wireframe cityscape in futuristic style. Royalty-free stock vector ID: 1335323081.

Dec 21, 2021 13:21 GMT

NCC Group Monthly Threat Pulse – November 2021

- 1.9% increase in ransomware attacks compared to October
- 50% increase in organisations targeted by PYSA ransomware, with a 400% rise in government sector victims
- North America and Europe continued to be the most targeted regions in November, with 154 and 96 victims respectively

NCC Group's Strategic Threat Intelligence team has identified PYSA and Lockbit as the threat actors dominating the ransomware landscape in November. Since August this year, Conti and Lockbit have been the top threat

groups, but in November, PYSA, also known as Mespinoza, overtook Conti with an increase of 50%. Meanwhile, the prevalence of Conti decreased by 9.1%.

PYSA is a malware capable of exfiltrating data and encrypting users' critical files and data, which typically targets large or high-value finance, government and healthcare organisations.

Both North America and Europe continue to be the most targeted regions in November, with 154 and 96 victims respectively. In North America, organisations in the US experienced 140 of these attacks, while Canada experienced 14.

In Europe, the top targeted countries included the UK and France, with Italy and Germany sharing third place. Each of these countries experienced 32, 14, and 11 attacks respectively in November.

The industrials sector continued to be the most targeted sector in November. Meanwhile,automotive, housing, entertainment, and retail businesses overtook technology this month, with attacks targeting the sector decreasing by 38.1%.

Spotlight on the Everest ransomware group

Over the last year, NCC Group has seen threat actors emerge and adopt new tactics to achieve their aims. The Russian-speaking Everest Group is a perfect example of this, and are taking hack and leak campaigns a step further.

In November, the group offered paid access to the IT infrastructure of their victims, as well as threatening to release stolen data if the victim refused to pay a ransom. This included data related to the Argentine Government, Peru's Ministry of Economy and Finance, and the Brazilian Police.

While selling ransomware-as-a-service has seen a surge in popularity over the last year, this is a rare instance of a group forgoing a request for a ransom and offering access to IT infrastructure – but we may see copycat attacks in 2022 and beyond.

While this report focuses on November activity, NCC Group's Strategic Threat

Intelligence team have also been closely monitoring exploitation of the Log4Shell vulnerability, disclosed in December. For more information and up-to-date advice, take a look at our dedicated recommendations and resources page.

Keep up to date with our latest insights
Never miss a threat intelligence update - sign up to receive our monthly insights into the emerging advances in threat landscape.

Plus, sign up for our next quarterly Threat Monitor webinar here.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750