nccgroup

Aug 31, 2021 15:50 BST

NCC Group reveals threefold increase in targeted ransomware attacks in 2021

Analysis from NCC Group's Research Intelligence and Fusion Team (RIFT) has highlighted the growing threat of ransomware around the world.

The number of ransomware attacks analysed by the team has increased by 288% between January-March 2021 and April-June 2021, with organisations continuing to face waves of digital extortion in the form of targeted ransomware.

22% of ransomware data leaks analysed between April and June were attributed to Conti ransomware, which often uses email phishing to remote

into a network via an employee's device. This was closely followed by Avaddon ransomware, which was linked to 17% of ransomware data leaks. While the victims of this ransomware strain have faced data encryption, the threat of data leaks, and the wider risk of distributed denial of service (DDoS) attacks disrupting operations, the strain is now believed to be inactive.

One significant trend identified by NCC Group is the prevalent issue of ransomware gangs threatening to leak the stolen sensitive data of non-paying victims to damage organisational reputation. This additional pressure to force a pay out is known as "double extortion", which is an increasing tactic used by threat actors.

This issue is affecting organisations around the world, with 49% of victims with known locations in the last three months based in the United States, followed by 7% in France and 4% in Germany. One notable example is the Colonial Pipeline ransomware attack in June, carried out by affiliates of the DarkSide ransomware. The attack resulted in the shutdown of oil supplies and fuel shortages across the United States.

Christo Butcher, global lead for threat intelligence at NCC Group, said:

"Over the years, ransomware has become a significant threat to organisations and governments alike. We've seen targets range from IT companies and suppliers to financial institutions and critical national infrastructure providers, with ransomware-as-a-service increasingly being sold by ransomware gangs in a subscription model.

"It's therefore crucial for organisations to be proactive about their resilience. This should include proactive remediation of security issues, and operating a least-privilege model, which means that if a user's account is compromised, the attacker will only be able to access and/or destroy a limited amount of information."

Notes to editors

Figures based on incidents analysed and dealt with by NCC Group's Research Intelligence and Fusion Team throughout 2021.

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