Tech firms are in the firing line as the top targets for cyber criminals are revealed

Attacks on technology organisations increased by 29.8% in Q3 of 2021.

The latest report published by security firm Digital Shadows has revealed that as expected, the most common target of ransomware attacks continues to be the industrial goods and services sector, playing victim to a total of 111 attacks. Compared with the previous quarter however, the results represented a 42% decrease as attackers turned their attention to tech organisations.

The results illustrate the continued need for businesses to be well equipped to counteract the onslaught of cyber security attacks. This is according to ProLion, a best-in-class proactive ransomware and data protection solution provider.

The research from the data loss detectors was carried out by monitoring 35 data-leak sites each day. In total, 61 tech businesses had their data posted on a data leak site throughout the third quarter of 2021, increasing by almost a third on the previous quarter.

The report also notes that attacks are down 13% from Q2, but this is likely a result of the closure of various data leak sites, including those attributed to prominent gangs like Avaddon, Happy Blog and DarkSide.

In total in Q3, 571 different victims were named on the sites, although the researchers also noted that some ransomware groups operate without the need for data leak sites, such as Ryuk. The closure of several of this type of site might in turn warn some gangs off this tactic, especially given that REvil reported in October that it had led to their servers being compromised.

Steve Arlin, VP Sales, UK, Americas & APAC at ProLion, said: “We know from some of the higher profile attacks this year and last that the industrial goods and services sector has long been a popular target of attacks. Perhaps the most high-profile attack being that on Colonial Pipeline. Just recently in September, BlackMatter attacked agriculture supply-chain New Cooperative, locking computers and severely disrupting the management of their supply chains.

“It’s interesting to see a shift in focus towards tech organisations, but this isn’t unexpected. Companies such as these will often work with masses of data, and it puts you in a very vulnerable position when these databases are breached,” said Arlin.

“The threat of that data ending up on one of these sites adds another level of pressure to an attack, with the associated challenge of reputational risk and the threat of information regulators and associated GDPR fines.

“While the statistics clearly represent that a distinct group of businesses are regularly being targeted, ultimately the results of the research are not surprising nor new. Criminals are frequently disrupting supply chains and accessing large databases full of sensitive information.”

“If you haven’t already, get your defences in order before your data and your customers’ data finds itself in the report for the next quarter,” said Arlin.

Notes to editors

About ProLion

ProLion GmbH is a developer of ransomware protection and data integrity software solutions for any ONTAP focused storage environment and high-availability solutions for SAP and MetroCluster environments.

Founded in Austria, ProLion’s best-of-breed CryptoSpike solution eliminates system downtime and data loss risk ensures that an organisations’ data remains secure, compliant, manageable and accessible.

www.prolion.com