Payoff demands triple from ransomware groups as the scale of the financial impact exposed

Stolen funds increase 179 percent to $326,264 in the first half of 2021 and this will only increase according to ProLion

The recent report published by Coalition, a cybersecurity insurance provider, which found that payoff demands from ransomware groups has tripled year-on-year, illustrates the continued challenge organizations face as they grapple with on-going cyber security attacks. This is according to ProLion, a best-in-class active ransomware and data protection solution for ONTAP storage.

The insurance provider researched its 50,000 North American policyholders and identified in its H1 2021 Cyber Insurance Claims Report that during the first half of 2021 the average ransom demand roughly tripled to $1.2 million per claim up from $450,000 in the same period a year ago.

Steve Arlin, VP Sales, UK, Americas & APAC, ProLion, stated: “This Report follows on from other detailed analysis coming out of the insurance market such as the recently published Hiscox Report that not only illustrates the sheer scale of ransomware-as-a-service today as opposed to a year ago and the clear financial impact.

“This report not only highlights a tripling of demands year-on-year but that the average funds stolen leapt a staggering 179% from $116,842 in H1 2020 to $326,264 in H1 2021. This is a significant increase and only serves to encourage bad faith actors.”

Once a company’s IT systems have been breached by ransomware, it is immediately left open to the loss of mission critical systems which could be fatal. But then the threat of data leaks adds another level of pressure with the associated challenge of reputational risk and the threat of information regulators and associated GDPR fines.

One undeniable reason why you should care more than ever about Ransomware is the removal of barriers to entry. With the introduction of Ransomware-as-a-Service (RaaS), many more criminals can now operate, and now it’s not only large organizations that fall victim, but also SMEs, local government, and councils, and even sports teams, resulting in massive business disruption, reduced revenue, and disenfranchised customers.

“The call to action is simple – be proactive. We have seen with the Covid-19 response that most people would not wait till they are infected with a virus before doing something about it. These figures present a truly frightening picture – cybercrime is ballooning and as we are seeing time and again, ransomware is fast becoming a serious threat to us all. This is no longer an issue of a database being held to ransom, entire supply chains are now threated as the bad actors are targeting mission critical infrastructure,” concluded 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 organizations’ data remains secure, compliant, manageable, and accessible.

www.prolion.com