Cracking down on crypto addresses just one part of a much bigger problem, says ProLion

Efforts to curtail the continuous onslaught of ransomware attacks should focus on prevention rather than payment.

As the frequency and severity of ransomware attacks shows no sign of easing, sanctioning crypto exchanges will do little to address the growing problem. This is according to ProLion, a best-in-class proactive ransomware and data protection solution provider for ONTAP centralised file services.

The US treasury last week announced sanctions on the SUEX crypto exchange that it asserts has facilitated ransomware transactions totalling $13 million. It believes around 40 per cent of SUEX's transactions are linked to illicit actors, while the company has aided the laundering of funds from more than eight ransomware variants. The newly announced sanctions block US citizens and companies from transacting with the group.

While cracking down on crypto exchanges that allow these transactions is an essential part of the process, without further action it will only make these payments less secure rather than stopping them. Especially at a time when according to a report from Kaspersky, over half of victims resort to paying the ransom.

Steve Arlin, VP Sales, UK, Americas & APAC, ProLion believes that merely disrupting the work of cyber criminals isn't enough to have a lasting impacting. "While this is a positive first step, it should be followed by real action to tackle the effects of ransomware and its criminals rather than further criminalising payment," he said.

"A successful ransomware attack in its simplest form can be split into two parts, a security breach of followed by a payment. Addressing the second part of this process is somewhat misguided, just like it is impossible to stop attacks from occurring, it is essentially impossible to stop payment completely. Attackers will always find an avenue that makes it possible to obtain the ransom.

"Instead, action should be taken to limit the damage that attacks can have before payment is even considered. In doing so, both parts of the problem are tackled in one. This means businesses and legislators need to be proactive rather than reactive in their approach. Focusing on actively monitoring your network to counter opportunist threats," he continued.

Proactive ransomware solutions work by protecting Central File Services whether in the local data centre, NAS or in the Cloud, allowing the possibility to deal with attack long before it becomes a transaction on a crypto exchange.

“The focus of action from government should be on prevention of the damage an attack can cause by encouraging the implementation of better security measures.”

“The best course of action is to bolster your defences with several layers of protection with several mitigations at each layer. This gives victims the chance to detect attacks and stop them before they have long-lasting and damaging effects,” said Arlin.

Notes to editors

About ProLion
ProLion GmbH is a developer of ransomware protection and data integrity software solutions for any ONTAP centralised file services 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