Recent Trends in Ransomware – A Summary

2022 has already been another unique year in the cyber market, especially reflected with the changes in the threats of ransomware, which has seen a drop in volume and change in approach.

Since the outbreak of the Russian/Ukrainian conflict in early March, there has been a substantial downward shift in the volume of ransom events and the attack vector that Threat Actors (TAs) have been targeting, with a dramatic shift from targeting 'standard' or 'normal' organisations and a refocus on infrastructure, which has been heavily targeted. Consequentially there has been a drop in ransomware attacks that fall into the traditional insurance environment.

The Colonial Pipeline attack could be argued was the first direct ransomware attack on US infrastructure, brought an intense focus from law enforcement. This particular incident garnered the attention of the worlds law enforcement, bringing a focus onto TAs and their activities. There is a lot of intelligence that some TAs are 'going to ground' until the attention is drawn elsewhere.

The dissolution of Conti as a TA group has also had a significant impact on the volume of ransomware events. In recent years, Conti were by far the most active and aggressive TA on a consistent basis. Their implosion following their announcement to aligning to Russia and the TrickBot leaks effectively led Conti to become sanctioned.

This year may also be the year where underwriting changes applied in previous years begins to bear fruit. The increase in pricing has drawn the attention of organisations to review and improve their IT posture and cyber security, combined with tighter underwriting controls, could be argued have also been a factor in reducing the volume of ransomware events affecting insureds.

However, TAs haven't disappeared, but have pivoted with their tactics. Arete has seen a large uplift in business email compromise / wire transfer fraud claims, as TAs move to a different approach, which is perhaps a lower profile attack.

In terms of the ransom events that have been occurring, there is a far greater proportion of exfiltration only events. In our experience these events are normally quicker to execute for an adversary, and in terms of claim settlement, tend to be at a far lower costs and generally take less time. The intelligence we have gained here is that those TAs are looking to get in and out as fast as possible to ensure that they keep their profiles as low as possible, to reduce their exposure.

In a general, 2021 is a year like no other in cyber, but we say that each and every year! What we are seeing at the moment is a continuation of the general trending down of ransoms being paid against organisations either choosing to not pay or are now better prepared and able to restore instead. The fight against ransomware definitely isn't over and will likely never be, but it does feel like it's a rare moment of where the 'good guys' are on top.