Summary of findings

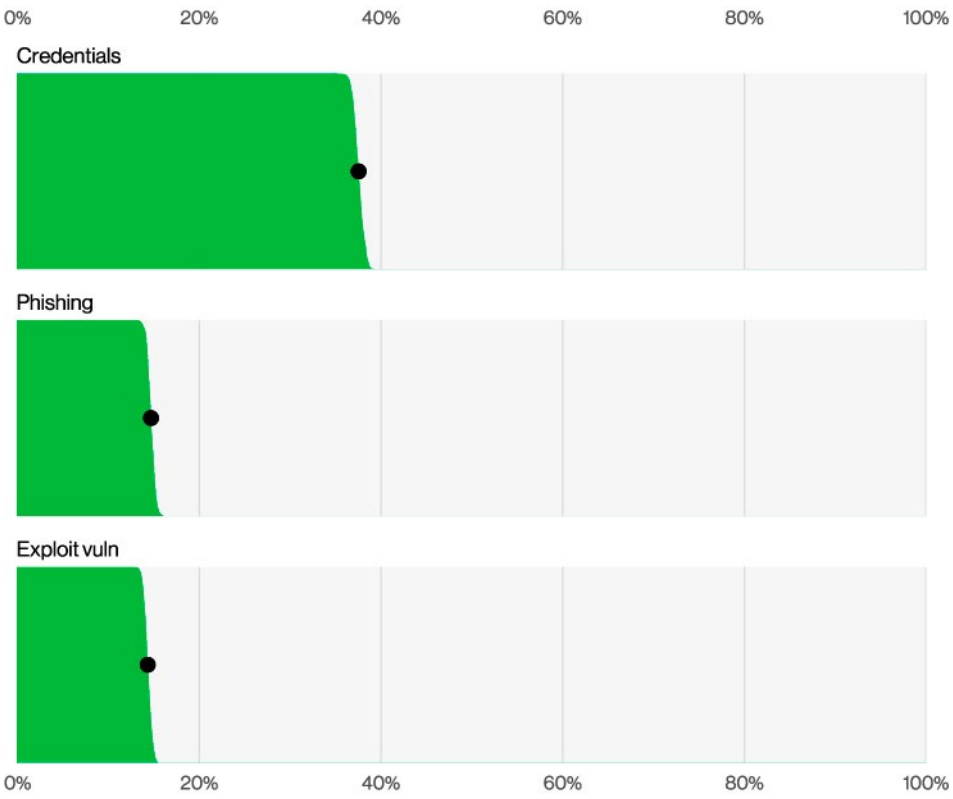

Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

Our ways-in analysis witnessed a substantial growth of attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach when compared to previous years. It almost tripled (180% increase) from last year, which will come as no surprise to anyone who has been following the effect of MOVEit and similar zero-day vulnerabilities. These attacks were primarily leveraged by Ransomware and other Extortion-related threat actors. As one might imagine, the main vector for those initial entry points was Web applications.

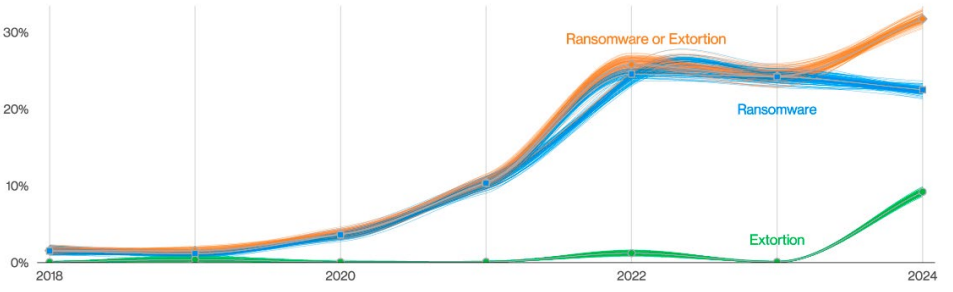

Figure 2. Ransomware and Extortion breaches over time

Roughly one-third of all breaches involved Ransomware or some other Extortion technique. Pure Extortion attacks have risen over the past year and are now a component of 9% of all breaches. The shift of traditional ransomware actors toward these newer techniques resulted in a bit of a decline in Ransomware to 23%. However, when combined, given that they share threat actors, they represent a strong growth to 32% of breaches. Ransomware was a top threat across 92% of industries.