Key Findings

Banking Trojans represented 25% of all attacks in Q2/Q3, up from 16.7% in Q1. Emotet held its place as the top banking malware in Q2 but disappeared from the scene in Q3, giving the lead to Trickbot. As has been true for at least the last year and a half, fileless Kovter variants account for a steady 10–15% of attacks.

Adware and potentially unwanted programs (PUPs) continue to be the largest group of threats prevented by Morphisec, representing 40% of all attacks. Much of the adware in the wild could just about be categorized as spyware and, as a threat, should not be dismissed based on a potentially damaging impact.

The trend we see is that many strains of adware are being incorporated as part of broader attacks that feature sophisticated, evasive techniques that allow it to penetrate operating systems and bypass static defenses.

Exploit kits, some which hadn't seen updating in years, are back in play, incorporating new Flash, VBScript and Acrobat vulnerabilities.

The top ransomware threat prevented was GandCrab, with Sigma a distant second. With each new release of updated GandCrab ransomware, Morphisec sees a spike in threats prevented, which then levels out as AV and NGAV systems catch up.

All attacks prevented by Morphisec in the second half of the year involved at least one fileless technique, with **approximately 15% of attacks never dropping a malicious executable on disk.**

Coin mining malware remained popular, accounting for 30% of attacks, with RIG-delivered miners the most prevalent type seen by the Morphisec system.