Seqrite, a specialist provider of endpoint security, network security, enterprise mobility management and data protection solutions, highlighted the growing security threat that enterprises face in an increasingly digital-first world with the launch of the Seqrite Threat Report H2 2018. In its latest report, Seqrite mapped threat detections to provide comprehensive insights into the global threat landscape and detailed analysis of various attack vectors adopted by cybercriminals. Seqrite is the enterprise arm of Quick Heal Technologies, one of the leading providers of IT Security solutions to consumers, businesses and Government.

During the period, Seqrite detected close to 50 million threats targeting enterprises– translating to around 186 detections every minute. These detections included known and unknown threats such as cryptojacking, ransomware, trojans, exploits, worms, infectors, potentially unwanted applications (PUAs), and adware.

Newer threats become more prominent, as older threats evolve

Researchers at Seqrite detected more than 15,000 cryptojacking hits a day on average, totalling to more than 2.76 million detections. This further underlined the long-term shift in cybercriminal preferences towards ease of deployment and instant return on investment, as has been previously reported by Seqrite.

But to think that traditional attacks such as ransomware are dead would be imprudent. With more than 2,000 detections on a daily basis, ransomware remained one of the most persistent threats deployed by cybercriminals. Ransomware attacks have also evolved with time to become more sophisticated and targeted, leveraging multiple attack vectors to sneak past enterprise defences.

GandCrab, for instance, has evolved five times since it was first detected in January 2018, demonstrating why ransomware remain the most worrisome threat for organisations. There was also a sharp increase in the number of fileless malware, underlining the importance of robust, multi-layered defense that is rightly deployed and configured.

Multiple industries at risk

Somewhat unsurprisingly, the IT/ITeS industry was highlighted as the most targeted sector in the Seqrite Threat Report H2 2018, accounting for 27.83 per cent of the total malware detections during the reporting period. Professional services followed close on its heels with a detection share of 24.43 per cent, while manufacturing (17.70 per cent) and education (11.08 per cent) were also identified as at-risk industries.

Advanced Persistent Threats likely to be made available as-a-Service

In early 2018, Quick Heal Security Labs had predicted that RaaS (Ransomware as a Service) will become the new pillar of MaaS (Malware as a Service). This prediction came true, as RaaS developers started selling entire attack packages along with the intrusion mechanism for a lucrative cut. Seqrite expects this evolution to lead to the possibility of an as-a-Service model for Advanced Persistent Threats (APTs).

Malware authors will leverage generic loopholes in data-intensive sectors such as healthcare, BFSI, and cloud services to sell well-organized APT attack vectors to prospective threat actors. There is also the possibility of APTs being deployed against specific nation-states, large organizations, government agencies, law enforcement systems etc.

Speaking on the findings in the latest Seqrite threat report, Sanjay Katkar, Joint Managing Director and Chief Technology Officer, Quick Heal Technologies Limited said, “The growing scale, speed, and sophistication of cyber-attacks underlines just how critical it is for enterprises to keep up with the developments within the global cybersecurity domain. The Seqrite Threat Report H2 2018 is aimed at identifying the latest enterprise security trends and emerging threats that affect the business ecosystem. The insights available in this report analyse various attack methodologies and tactics adopted by cybercriminals with the objective to empower organisations with an in-depth understanding of the level of threat that they are exposed to, and the measures they can take to defend themselves against advanced threats.”

Based on Seqrite telemetry data, the Seqrite H2 2018 Threat Report has been compiled by Quick Heal Security Labs, the R&D division of Quick Heal Technologies. Quick Heal Security labs is dedicated to arm enterprises and consumers with cutting-edge security threat research and cyber intelligence, and analyses data fetched from enterprise networks and endpoints across the globe to deliver enhanced protection to clients against existing and future cyber threats.