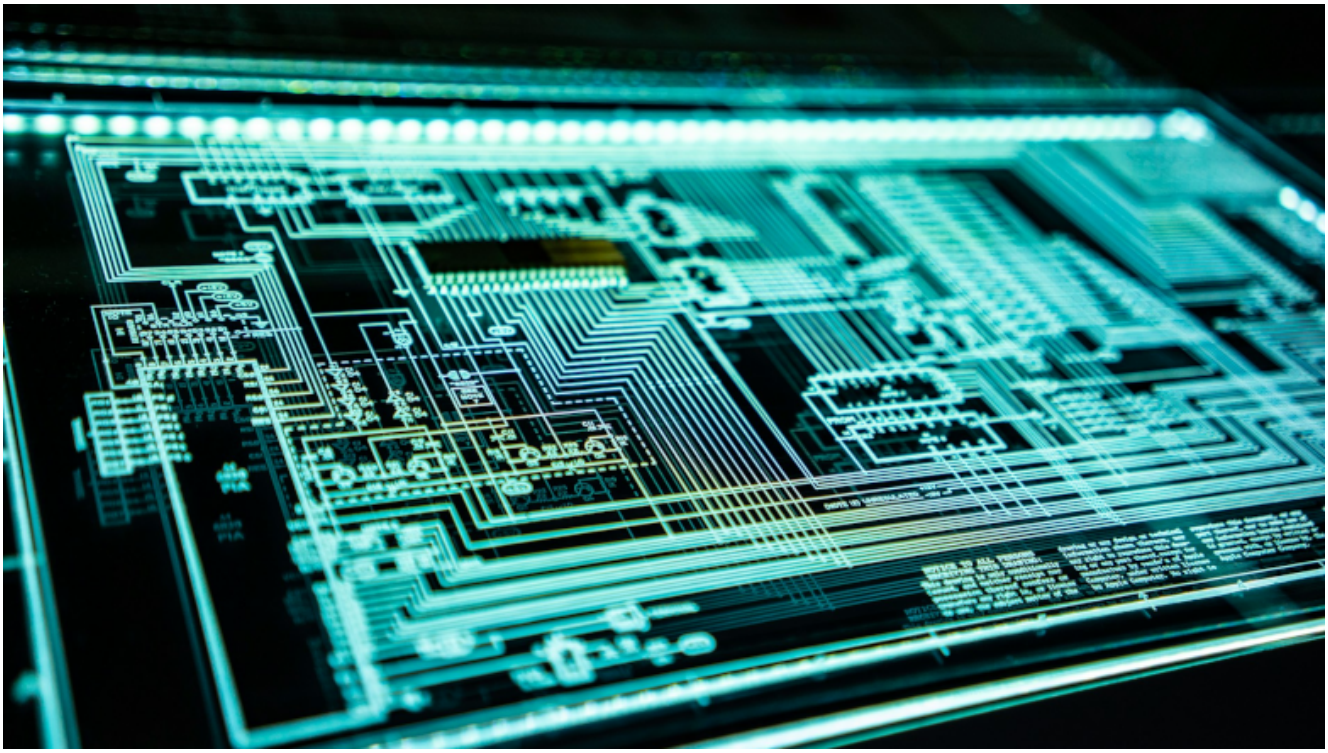
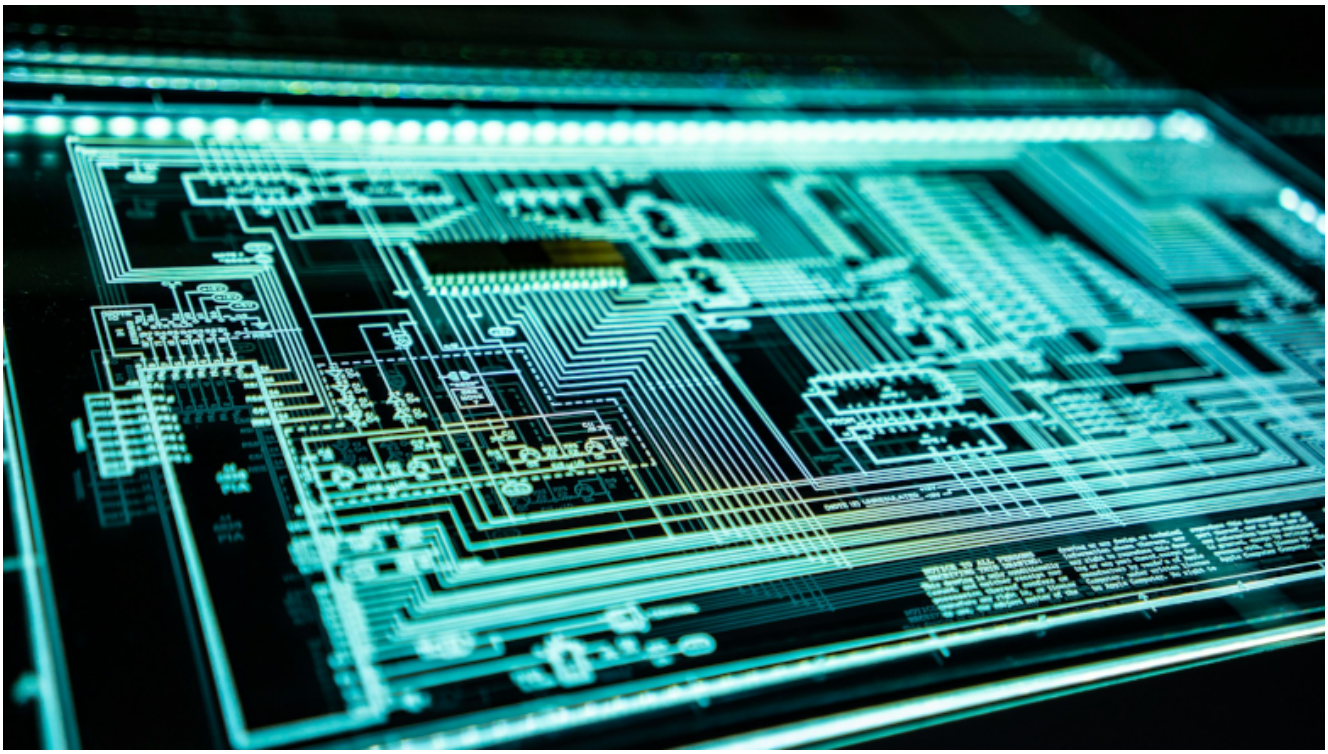
Cyber security threats are predominantly as-a-service attacks





A recent report by Darktrace reveals the key threats

businesses have faced in the past sixmonths. The report emphasizes the prevalence of as-a-service attacks, as a majority of malicious actors use Malware-as-a-Service (MaaS) and Ransomware-as-a-Service (Raas) to carry out attacks. These tools provide resources to attackers, such as pre-made malware or phishing templates. The report noted that following the dismantling of ransomware group Hive, new threats such as ScamClub and AsyncRAT emerged.

The most widespread tools used by such attackers were malware loaders, which made up 77% of investigated threats. This was followed by cryptominers at 52%, botnets at 39%, information-stealing malware at 36% and proxy botnets at 15%.

The report also discusses a rise in sophisticated phishing tactics. The report showed 10.4 million phishing emails between September and December of 2023. One such tactic includes Microsoft Teams phishing attempts, in which attackers pose as a victim’s co-worker and lure them in to clicking a malicious link.

Another noted trend is the increase in multi-functioning malware, allowing attackers to cast a wide net and inflict maximum damage. As attackers shift toward the latest methods to bypass modern security measures, security teams must continue to adapt and innovate.

Read the full report here.

https://www.securitymagazine.com/articles/100390-cyber-security-threats-are-predominantly-as-a-service-attacks