Written by Marco Attard
28 May 2020

According to Trend Micro research, trust has eroded among criminal interactions, leading to a switch to e-commerce platforms and communications via Discord, both to increase user anonymisation.

"This report highlights the threat intelligence we collect and analyze from global cybercriminal networks that enables us to alert, prepare and protect our corporate customers and partners," the company says. "This research helps us inform businesses early about emerging threats, such as Deepfake ransomware, AI bots, Access-as-a-Service and highly targeted SIM-swapping. A layered, risk-based response is vital for mitigating the risk posed by these and other increasingly popular threats."

The report claims law enforcement efforts are leaving an impact on the cybercrime underground. Global police entities have taken down a number of forums, and the remaining forums are currently experiencing persistent DDoS attacks and log-in problems, impacting their usefulness. Meanwhile the loss of trust has lead to the creation of DarkNet Trust, a website created to verify vendors and increase user anonymity. Other underground markets are launching new security measures, including direct buyer-to-vendor payments, multi-signatures for cryptocurrency transactions, encrypted messaging and a ban on JavaScript.

Interestingly, commoditisation has driven down the prices of many items. For example, crypting services are down from $1000 to just $20 per month, while generic botnets costs have dropped from $200 to $5 daily. The pricing for other items, such as ransomware, Remote Access Trojans (RATs), online account credentials and spam services remain stable, indicating continued demand. Other services, such as IoT botnets, see high demands, and new undetected malware

variants sell for as much as $5000. Also popular are fake news and cyber-propaganda services, with voter databases selling for hundreds of dollars and accounts for games such as Fortnite.

Trend Micro points out the emergence of markets for things such as deepfake services for sextortion or photo verification bypassing, as well as AI-based gambling bots to predict dice roll patterns and crack complex Roblox CAPTCHA. The price to access Fortune 500 companies can reach up to $10000, with services including access to read and write privileges, while wearable device accounts allowing cybercriminals to run warranty scams by requesting replacement devices are in demand.

Underground marketplace trends will probably shift further in the months following the global Covid-19 pandemic, as attack opportunities will always continue to evolve. Trend Micro suggests companies adopt a multi-layered defense strategy to protect against the latest threats and mitigate corporate security risk.

Go Trend Micro Research Finds Trust Lacking Within the Cybercriminal Underground