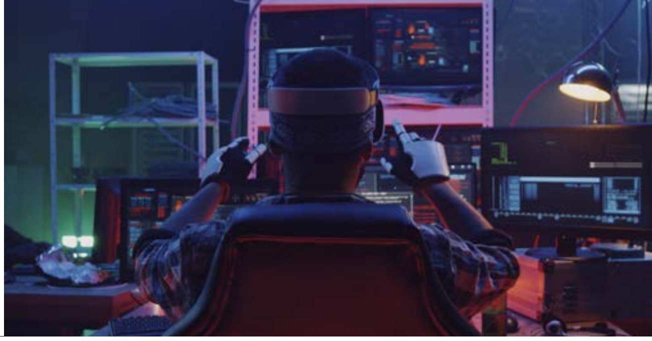
The Near and Far Future of Ransomware Business Models

By Feike Hacquebord, Stephen Hilt, and David Sancho



Ransomware groups are expected to undergo changes, triggered by a number of factors in the security landscape and the ransomware "business." These small changes ("evolutions") will naturally occur borne of competition with other cybercriminal players, while bigger deviations ("revolutions") will likely increase to adapt to the changing environment, threat actors' income yields, and attack objectives. Our research paper, "**The Near and Far Future of Ransomware Business Models**," discusses this at breadth based on documented incidents, changing legislation, and shifts in the geopolitical and economic scene, among other components.

Key talking points

- When pushed, ransomware actors are expected to change to other criminal business models that monetize initial access, such as short and distort (stocks fraud), business email compromise (BEC), and cryptocurrency theft.
- Defending against initial access brokers and arresting them is key in the fight against ransomware.
- Sanctions, cloud adoption, and hardening networks will trigger ransomware actors to evolve but not revolutionize their business model.
- Ransomware actors are expected to evolve with more automation, better operational security (OpSec), and adding new cloud targets and internet of things (IoT) platforms. Linux ransomware will continue to grow.
- Cryptocurrency crime is expected to grow significantly, and ransomware actors are expected to have their share in crypto crime sooner or later.

Insights and Conclusions

Historically, these shifts in ransomware groups and their respective business models are triggered by the escalatory cycle of reacting and adjusting to previous incidents. Specific changes adopted by legitimate organizations, politics, and economies also drive these illicit groups to adapt, scale, monetize, and execute their business models at faster rates than we realize. Sanctions target yesterday's problems of ransomware, but do not solve today's problems. Nonetheless, by keeping in mind that ransomware groups and their respective tactics constantly change, a concerted effort from security practitioners and law enforcement to keep these threats and groups at bay will have to be backed by a continuous stream of preparing, studying, and strategizing their defenses.

Read the full paper at **research.trendmicro.com/FutureofRansomware** for more details on the changing trends in ransomware and how to defend your systems.

TREND MICRO™ | research