How a Diverse Ecosystem Creates Resilience in the Cybercrimal Underground

Andrei Barysevich[1]
[1]*Recorded Future*

The common misperception of cybercriminals as "larger than life," incredibly clever, well-off, and unreachable by law enforcement has created a romanticized perception of cybercrime, luring a steady supply of ambitious recruits into various restricted and illicit online communities.
In this research, I introduce the architects of the first major Russian-speaking underground community, who single-handedly created a framework of cybercriminal collaboration.

We will explore the evolution of the dark-web from inefficient peer-to-peer “enterprises” in its early days, to a highly specialized, robust economy it is today with diverse, niche supporting infrastructure. We will visit some prominent fraud marketplaces and the various platforms and tools available to criminals.

As a culmination, I will dissect the entire cycle of operations of a notorious hacking group known as Carbanak/Fin7, the shadowy group responsible for a long streak of sophisticated payment card breaches of prominent corporations including Hilton, Omni Hotels, Chipotle, and Trump Hotels. We will review the distribution mechanism of compromised payment data, provide real-time statistics on daily sale volume, and outline staggering profit levels, rivaled only by money earned by the Colombian drug smugglers and Ukrainian firearm vendors.