



Preparing for cyber war

Charles Carmakal^{1,2}

¹Mandiant, ²FireEye

Some threat actors are motivated by money, some want fame and glory, some want competitive intelligence, some want to influence our decisions, and some just want to see the world burn. Threat actors will go to extreme measures to achieve their objectives. The rules of engagement have changed. Over the past two years, we have observed a significant rise in aggressive attacks - extortion, public shaming, destruction, intentional business disruption, and even threats to human safety. This talk will walk through the attacks that are being observed on the front lines by the presenter. We will discuss strategies to prepare and respond to aggressive attacks.

The talk will cover the following topics:

- Overview of the threat actors that have become increasingly disruptive and their motivations.
- Discussion of the tools, tactics, and procedures employed by North Korean, Russian, and Iranian threat actors.
- Case studies of breaches where threat actors extorted, publicly shamed, destroyed, or disrupted business operations or threaten human lives.
- Details of how foreign governments stole and released information to influence public opinion
- Suggestions for preparing for and responding to aggressive threat actors.