Cybersecurity at MIT Sloan

Cybersecurity at MIT Sloan

Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, $(IC)^3$

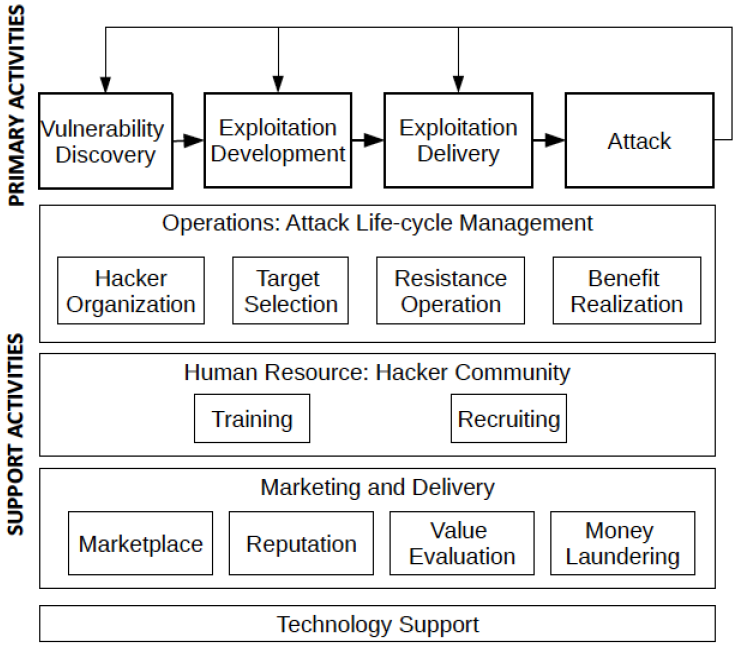
Understanding the Cyber Attack Business

Cybersecurity at MIT Sloan brings thought leaders from industry, academia and government together with MIT faculty, researchers and students to address strategy, management, governance and organization of cybersecurity of critical infrastructure using an interdisciplinary approach.

Where there is commerce, there is the risk for cybercrime. It is estimated that the cost of cybercrime will grow to $6 trillion by the end of 2021.

The Cyber Crime Business Follows a Value Chain

Nearly one third of companies are affected by cybercrime. Unfortunately, the rate of cyber crime innovation outpaces the rate of cyber defense innovation: the bad guys are 'badder' faster. Most cyber attack research focuses on how attackers gain access to systems, but the problem is much larger. Cyber crime is big business. Attackers cooperate, working to maximize profits and minimize risk of arrest. Through the dark web, an attacker can tinker together services to create an attack without understanding the technical execution behind the attack. Such "cybercrime as a service" puts cybercriminal tools in the hands of new threat actors, and helps hide attackers from authorities. This project uses a value chain model to examine the cybercrime ecosystem. The framework describes subsystems and support activities that help reduce cost and increase benefit. This paper identifies twenty-four key activities that can be offered "as a service," including Botnet, exploit kits, and money laundering. More than theoretical, such services are actively used, as demonstrated in the recent attacks on the Ukraine power grid. Understanding the value chain can inspire ways of breaking down that chain, such as targeting control-points, or assigning defense responsibilities to encourage collaboration.



The Cybercriminal Value Chain Model

View this research paper:
http://bit.ly/mitic3darkwebbusiness

IMPACT: This paper provides insight on cyber attacks using a value chain framework. Viewing cyber attacks as "as a service" business processes will help develop more effective defenses against the cybercrime business.

Cybersecurity at MIT Sloan welcomes funding from sponsors for general support of the consortium research, and from organizations interested in specific research topics. All members and sponsors receive invitations to consortium events and activities, and access to consortium research, websites, and newsletters. For more information, visit https://ic3.mit.edu .