Section 1: Week 3: Avoid or Control Persistent Threats

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

June 21, 2020

North Central University

# Avoid or Control Persistent Threats

Malicious actors, targeted attacks, and advanced persistent threats (APT) each seek to disrupt the confidentiality, integrity, and availability of information systems. These different groups seek out their victims with varying levels of specificity and sophistication (see Table 1). After gaining access through phishing emails, an APT has established a foothold with the NCU Financial (NCU-F) network. The organization needs a strategy to remove the uninvited guest and recover control of the institution.

Table 1: Classifications of Attackers

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Target Selection | Description | Sophistication |
| Generic Malicious Actor (Fischerkeller & Harknett, 2017) | Random Selection | Use automation to attack thousands of systems, exploiting attacker defender economics | Relies on the Law of Large Numbers |
| Targeted Attackers (Alshamrani A, 2019) | Specific / Short Term | Identity specific industries and business artifacts for exploitation | Relies on social engineering and other known vulnerabilities |
| Advanced Persistent Threats (Alshamrani A, 2019) | Specific / Long Term | Seeks prolonged control over a target for months to decades | Well-financed organizations with ‘state-of-the-art’ weapons |