Applying the Diamond Model for Threat Intelligence to the Star Wars' Battle of Yavin

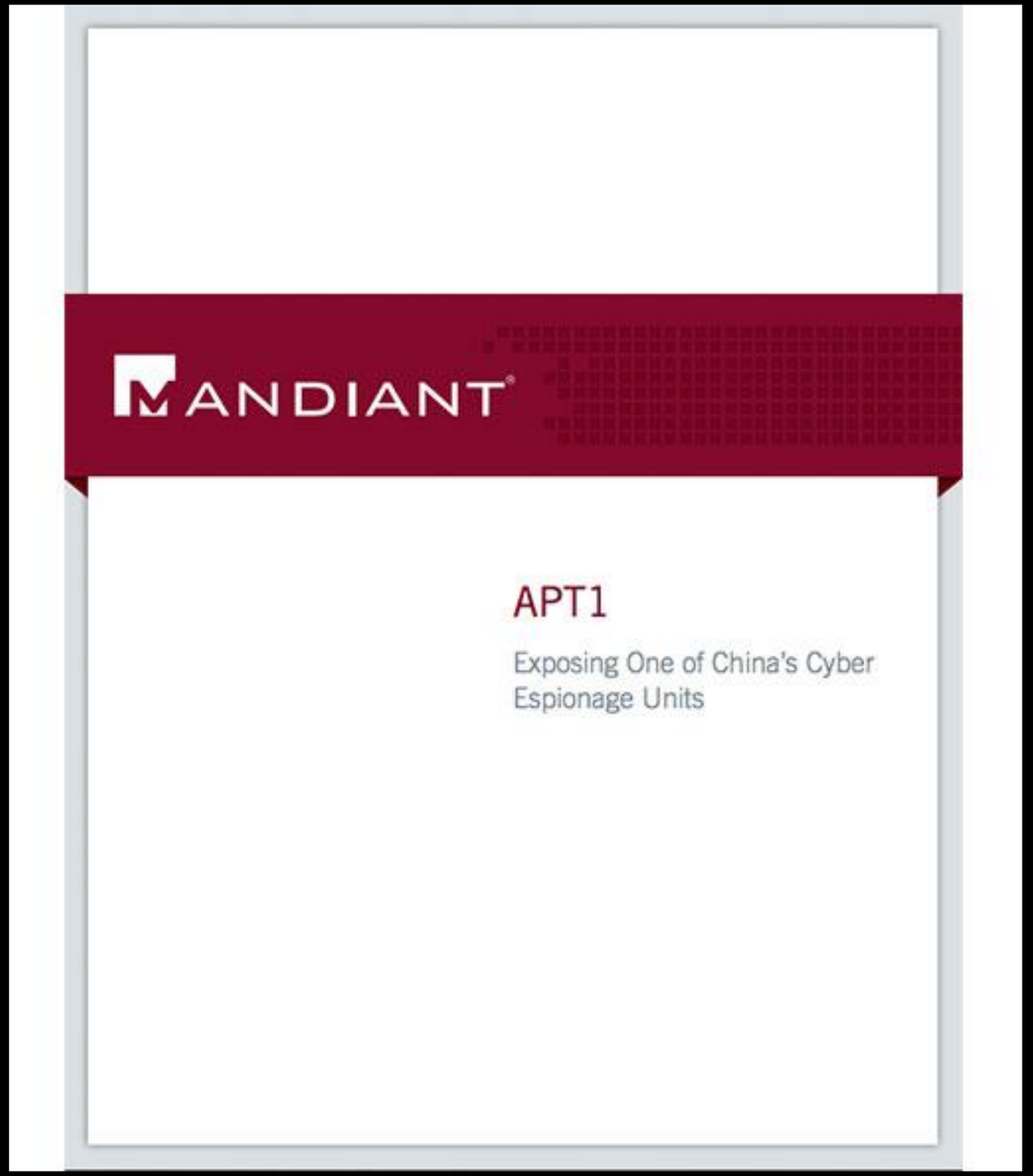
ADVANCED PERSISTENT THREATS

Identification and Attribution

Quincy Taylor
Aaron Anderson

An Advanced Persistent Threat is a group that is not purely financially motivated, but tries to obtain data that can be used strategically or politically. This usually excludes a petty criminal background. Instead, it is assumed that the group either belongs to a government organization or acts on its behalf furthering a strategic intent.

APT1: Dawn of the APT



https://www.youtube.com/watch?v=mYaTCvA2VLQ

Kaspersky labs	CrowdStrike	FireEye	Symantec
Unknown	CommentPanda	APT1	CommentCrew
MSUpdater	PutterPanda	APT2	Junebug
Unknown	GothicPanda	APT3	Buckeye
Sykipot	Maverick/SamuraiPanda	APT4	Hornet
Sofacy	FancyBear	APT28	Sofacy
Turla	VenomousBear	Snake	Epic/Waterbug
Newscaster	CharmingKitten	Newsbeef	Unknown
CloudAtlas	Unknown	Unknown	Inception
RedOctober	Unknown	Unknown	Rocra
Project Sauron	Unknown	Unknown	Strider


АКВЕДУК

Kahoot

APT #1:

Asia:

- Stripes
- Pakistan, South Asia, and China focused
- Aerospace corporations
- Financial Services, Government, Media, and Telecommunications
- Hangover

Viceroy Tiger

APT #2:

Europe:

- Large mammal
- The GRU
- Destructive track record
- Particularly focused on Ukraine
- Sandworm

Voodoo Bear

APT #3:

Southeast Asia:

- Canid species
- Website defacements, spear-phising, DDOS, and data theft
- Android malware
- Army
- Electronic Army

Deadeye Jackal