Threat Based Defence – Alonso Jose da Silva II
Objectives

What we will discuss

- Threat-based defence: principles and function
- Running a threat intelligence cycle
- Case study - financial services fraud

About Tempest

- Cyber security consulting and services provider with 14 years of experience, 100+ security engineers
- Working with large corporations in financial services, telecoms and media & broadcasting
- Extensive experience in penetration testing, risk assessments, 24/7/365 security monitoring and cyber threat intelligence operations
Limitations in the ‘fortress mentality’ approach to cybersecurity

- No more fixed perimeters
- Increasing attack surface
- Thriving underground marketplaces
- End-users targeted as a means to an end
Intelligence-driven security, also known as threat-based defence, is a risk management strategy that addresses the threat component of risk, incorporating analysis of adversaries, their capabilities, objectives, doctrine and limitations.

- Shift towards breach response and containment: deny attackers from acting on their core objectives
- Understanding the adversary’s behaviour, tactics, techniques and procedures
- Going beyond the corporate perimeter: understanding the supply chain of the underground economy

Reference: Intelligence-Driven CND informed by analysis of adversary campaigns and intrusion kill chains
Lockheed Martin, USA, 2010
Helping business leaders understand the cyber threat scenario

The threat component of risk can be broken down into:

- **Intent**: what the attacker is after, usually defined by your industry
- **Opportunity**: knowledge of the attack space, position (insider x outsider) and timing
- **Capabilities**: ability to successfully attack you, defined by skill level and resources
Cyber threat intelligence is based on acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities.

The threat intelligence cycle is the backbone of this approach:

- Continuous process, blending human skill and technology
- Collecting information, producing intelligence and integrating the result into decision-making and network defence

Reference: Cyber Intelligence Tradecraft Survey, 2013
Software Engineering Institute - Carnegie Mellon University

Reference: Towards an Intelligence-Driven Information Security Risk Management Process for Organisations
24th Australasian Conference on Information Systems
1. Direction

- Identifying customer needs
- Alignment with business requirements and industry threat scenario
- Guides planning, priorities and resource allocation
- Key issues
  - Direction cannot be outsourced
  - Requires leaders with communication skills and understanding of business culture
  - Finding the ‘right way in’ by leveraging existing security processes
2. Collection

- Collect and compile raw data for later analysis
- Establishing sources
  - Internal
  - External
  - OSINT / TECHINT / HUMINT
- Key issues
  - Breadth versus depth of collection
  - Technology for automation and scale
  - Leveraging service providers with established presence and collection capabilities
3. Analysis

- Build intelligence by analysing raw data
- Identifying and extrapolating patterns, meanings and sequences
  - TTPs: tactics, techniques and procedures
  - Assessing adversary capabilities and intent
  - Levels: Strategic / Tactical / Operational
- Key issues
  - Developing an analytical mindset
  - Specialized service providers with technical and analytical skillsets can accelerate results
4. Dissemination

- Distribution of intelligence product
  - Periodic industry/trend analysis;
  - Daily / Weekly situation reports and alerts
  - Actionable technical threat information feeds
- Key issues
  - Calibrating format to enhance decision-making
  - Integration into network defences
Case study: Financial Services, payment systems fraud

- Financial services industry in Brazil
  - #1 country in the world for banking malware \[1\]
  - Dynamic and hostile cyber threat scenario
  - Extensive underground economy

- Tempest works with clients to:
  - Monitor the cybercrime scene 24/7/365
  - Leverage deep presence to provide early warning of attacks and identify new types of fraud (HUMINT)
  - Analyse methods and tools, develop protections (TECHINT)
Case study: Financial Services, payment systems fraud

1: Through our cybercrime monitoring, we identified a threat actor selling devices for frauding Chip-and-PIN credit card terminals

2: Engaged with the threat actor, and obtained video evidence

Reference: Kaspersky report, 2012
Case study: Financial Services, payment systems fraud

1: Through our cybercrime monitoring, we identified a threat actor selling devices for frauding Chip-and-PIN credit card terminals

2: Engaged with the threat actor, and obtained video evidence

(Collection)

3: Reproduced the attack in our lab, by building our own devices

Reference: Kaspersky report, 2012
Case study: Financial Services, payment systems fraud
1: Through our cybercrime monitoring, we identified a threat actor selling devices for frauding Chip-and-PIN credit card terminals

2: Engaged with the threat actor, and obtained video evidence (Collection)

3: Reproduced the attack in our lab, by building our own devices (Analysis)

4: Understanding of the method, and how to defend client

5: Provided the threat profile and technical solution to client, who avoided millions in losses. (Dissemination)
Questions?

Alonso Jose da Silva II
Tempest Security Intelligence
alonso.silva@tempestsi.com