THREAT INTELLIGENCE IN A NUTSHELL:
FROM INTELLIGENCE TO EXPLOITATION

Abdel Sy Fane
Chicago CyberSecurity Meetup – President
Application Security Manager - Allstate
WHAT IS THREAT INTEL (TI)?

- Collecting Information on your adversaries (Threat-Actors)
  - Defining who they are and what they're capable of (Threat Modeling)
    - Hacktivist, APT Groups, Nation States, Hackers (driven by money or chaos)

- Curating the Data (there's tons of data out there!)
  - Contextualize & Visualize Threat Actors
  - Security Intelligence Tools (Gather & Analyze Threats)
WHAT IS THREAT MODELING & WHY IS IT IMPORTANT?
MODELING FOR INTELLIGENCE

- **Know Your Organization**
  - What is your organization’s role in the industry?
- **Know Your Infrastructure**
  - What assets do you need to protect?
- **Know Your Actors**
  - Which bad actor is most likely to come after your assets?
- **Know Your Tools**
  - How are you going to gather threat data & analyze it?
WHAT IS THREAT DATA, INFORMATION & INTELLIGENCE?

- Unusual Network Traffic
- Log-In Red Flags
- Geographical Irregularities
- Web Traffic with Unhuman Behavior
- Anomalies in Privileged User Account Activity
- Other Indicators of Compromise (IOC)
THREAT INTEL, FEEDS & PLATFORMS

• Threat Data Feeds
  • Pros:
    • Good starting point for Threat Intel (Threat Data is knowledge but not power)
    • Tons of OpenSource Feeds (FREE!)
    • Department of Homeland Security’s (DHS) Enhanced Cybersecurity Services (ECS)
      • Knowledge shared among organizations and govt. entities (also FREE!)
  • Cons:
    • Data Feed alone cannot answer any vital questions regarding the threat
    • Data overload
    • Relevant intel can only be extracted by human (time consuming)
• **Human Intelligence (HUMINT)**
  • **Pros:**
    • Collecting Threat Intelligence from human and machine sources
    • Rich in details and located in a searchable DB
    • Contextualized data prevalent to your organization
  • **Cons:**
    • **Time:**
      • Time consuming to collect data from multiple sources
      • Time consuming for human to analyze and correlate the data
      • Time consuming for human to connect the threat to your specific organization/industry
Threat Intelligence Platforms

Pros:
- Help organize threat data feeds (up to thousands of feeds)
  - Centralized feeds you’re subscribed to
- Contextualize and visualize data and correlating/integrating to other security platforms, i.e. SIEMs
- Prioritize what matters and setup alerts

Cons:
- Configure threat data feeds
- Only as good as the data coming in (feeds)
- Can be costly
OpenSource Threat Intelligence

- Write APIs to collect data from publicly available sources
  - Security News
  - Security Blogs
  - Security Forums
  - Security Researches
  - Social Media
    - Twitter – tinfoleak (Github)
- Check out Awesome-Threat-Intelligence (Github)
NOTABLE OPEN SOURCE THREAT INTELLIGENCE RESOURCES

• **vFeed** (Github)

• **MISP** - Malware Information Sharing Platform and Threat Sharing (Github)

• **AlienVault** - provides open access to a global community of threat researchers and security professionals
DEMO

Goals:

• Find a vulnerability reported by vendor (CVE, CWE, CPE, OVAL, CAPEC, CVSS, WASC)
• Find and correlate a vulnerability to a threat data
• Use the threat intelligence to exploit the reported vulnerability
THANK YOU!

The Team:
Abdel Sy Fane
Emily Stamm
Andrea Kim

ChicagoSecurity.Org
Meetup.com/ChicagoSecurity