The Best Way to Catch a Thief

Ty Miller

Director, Threat Intelligence

ty.miller@threatintelligence.com

www.threatintelligence.com

Phone: +61 409 713 735

Ty Miller

- Director, Threat Intelligence Pty Ltd
  - Specialist Security Company based in Australia
  - Creator of “Threat Analytics”
  - CREST Australia Tech Lead, Assessor, Board of Directors
- Black Hat
  - “Practical Threat Intelligence” Training
  - “The Shellcode Lab” Training
- Security Researcher
  - Black Hat Reverse DNS Tunneling Shellcode
  - Core Impact “DNS Channel” Shellcode
  - BeEF Bind Shellcode
- Author
  - Hacking Exposed Linux 3rd Edition

What are we doing here?

- Investigate modern security controls and techniques to detect threats, attacks and security breaches

- Discuss areas within these security controls and techniques that often fall short or fail, leaving you exposed, and how to close this gap

The Evolution of Security

- How have threats evolved?
  - How have attacks changed?
  - How has exploitation changed?
  - How have attackers changed?
  - How have backdoors changed?
  - How have hacker targets changed?
- Has your security evolved to detect and protect against these changes?
  - In most cases, probably not … or not enough, as we will see

Threat Detection

- To detect a threat in an effective way, we must:
  - Have a clear model that maps who our threat actors are
  - The intent of these threat actors
  - The types of attacks they are likely to perform
  - The techniques to exfiltrate our data or escape our containment measures
  - What pieces of digital DNA that we need to aggregate, correlate and analyze
  - What analysis we need to do to detect these threats
- We often think that we are finished, but in reality this is just the start

Threat Actor Model

- Who are the key Threat Actors for your organization?

- External
  - Script Kiddies
  - Hacktivists
  - Cyber Criminals
  - State Sponsored Attackers
  - Cyber Terrorists

- Internal
  - Rogue Employees or Contractors

- Partners
  - Managed IT (Security) Providers
  - Offshored Development
  - Building Management

Threat Actor Intent

- What are the Critical Assets and Impacts for your organization?

- Confidentiality
  - Hacktivists leak usernames and passwords ($188 per PII record / avg of $5.4M)
  - Cyber Criminals steal credit card details
  - Cyber Terrorists steal designs for critical infrastructure
  - State Sponsored Attackers steal intellectual property or secret identities
  - Managed IT Provider used as a pivot point into your organization
  - Offshored Development steal intellectual property

Threat Actor Intent

- What are the critical assets and impacts for your organization?

- Integrity
  - Script Kiddies deface eCommerce website leading to loss of revenue
  - Cyber Terrorists inject invalid data into systems to trigger unwanted actions

- Availability
  - Cyber Terrorists perform denial of service attacks on critical infrastructure
    - Loss of power, water, transport, health services, etc
  - Cyber Criminals perform denial of service attacks on financial services
    - Prevent ability to transact for extortion

Threat Actor Attacks

- What are the Threat Scenarios the Threat Actor is likely to carry out?
  - Script kiddy exploits malicious file upload within eCommerce website
  - Hacktivist exploits SQL Injection to dump credit card details
  - Cyber Criminal performs DDoS attacks on financial services for extortion
  - Offshored Development steal and sell source code to critical applications

Threat Actor Attacks

- What are the Threat Scenarios the Threat Actor is likely to carry out?
  - Managed IT Provider compromised to hijack DNS and MITM communications
  - Cyber Terrorist steals designs for critical infrastructure protocols and devices
  - Cyber Terrorist injects data into SCADA systems to stop critical infrastructure
  - State Sponsored Attacker uses client-side exploit to compromise corporate network and escalate privileges to monitor activity

Threat Actor Techniques

- What are the Exfiltration Techniques used to escape your containment measures
  - Reverse TCP Connection
  - HTTP or HTTPS Tunneling
  - DNS Tunneling
  - ICMP Tunneling
  - Social Media Tunneling
    - C&C via Twitter Posts bypasses malicious domain name detection

Threat Actor Techniques

- What are the Exfiltration Techniques used to escape your containment measures
  - Cloud Services (Dropbox, Google Drive, OneDrive, Cloud Email)
  - Web Shell via HTTP or HTTPS
  - SQL Injection via HTTP or HTTPS
  - USB
  - Physical System Boot
  - Offshore Development and Managed IT Providers
    - Well, you basically give it to them with minimal monitoring or control

Threat Actor Indicators

- What Indicators of Compromise (IOCs) do we need to collect?
  - **Threats** – Early IOCs *(Potential Pending Attacks)*
    - Intelligence Gathering
      - Open Source Intelligence (OSINT)
      - Human Intelligence (HUMINT)
      - Internal Intelligence
    - New vulnerability or exploit released for software used on your systems
      - Zero Day exploits don't provide this early indicator
    - Attacks and security breaches for other companies in your industry
      - Requires intelligence sharing across the industry
    - Malicious discussions in online forums towards the company or industry
      - Various languages across multiple countries
    - Compromised partners may indicate pending attack on your organization

Threat Actor Indicators

- What Indicators of Compromise (IOCs) do we need to collect?
  - **Attacks** – Active IOCs
    - Phishing, Spear Phishing or Drive-By Download Attacks
      - Client-side exploit attempts
      - File containing malicious Microsoft Office macro
      - Malicious Java applet
    - Sever-Based Attacks
      - Exploit scan across IP range searching for vulnerable systems
      - Small number of targeted exploit attempts
      - Web Attacks (SQL Injection, Malicious File Upload, Remote File Include, Command Injection)
      - SSL/TLS connections still often bypass detection controls

Threat Actor Indicators

- What Indicators of Compromise (IOCs) do we need to collect?
  - **Breaches** – Post Incident IOCs
    - Unexpected filesystem changes
    - DNS requests to known malicious domains
    - Connections made to know malicious IP addresses
    - Access made to critical data from account that does not typically access it
    - Local Kernel Exploits
    - Process and Thread Creation

Threat Actor Indicators

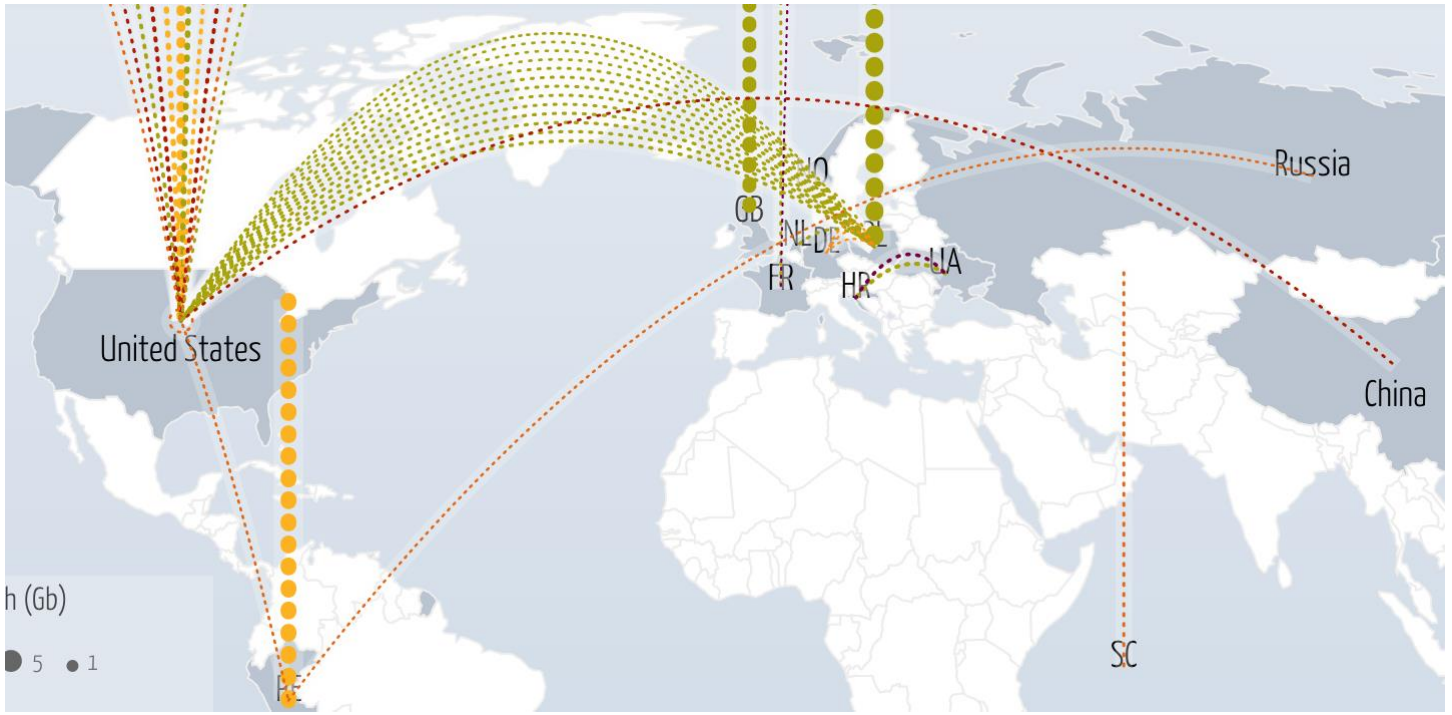
- What Indicators of Compromise (IOCs) do we need to collect?
  - **Breaches** – Post Incident IOCs
    - Process Migration
    - Service Modification or Creation
    - System file accesses searching for insecure file permissions
    - Credential and token dump / theft
    - Logins with local administrator accounts across multiple systems
    - Increased SQL queries and/or outbound data extracted

Threat Actor Analysis

- What Analysis do we need to detect the Threat Actors?
  - Map IOCs to Cyber Threat Intelligence data
  - Provides context to the IOC
    - Who is the Threat Actor?
    - What is the Threat Actor's intent?
    - What attack techniques are likely to be used?
    - What exfiltration techniques are likely to be used?
    - What privilege escalation techniques are likely to be used?

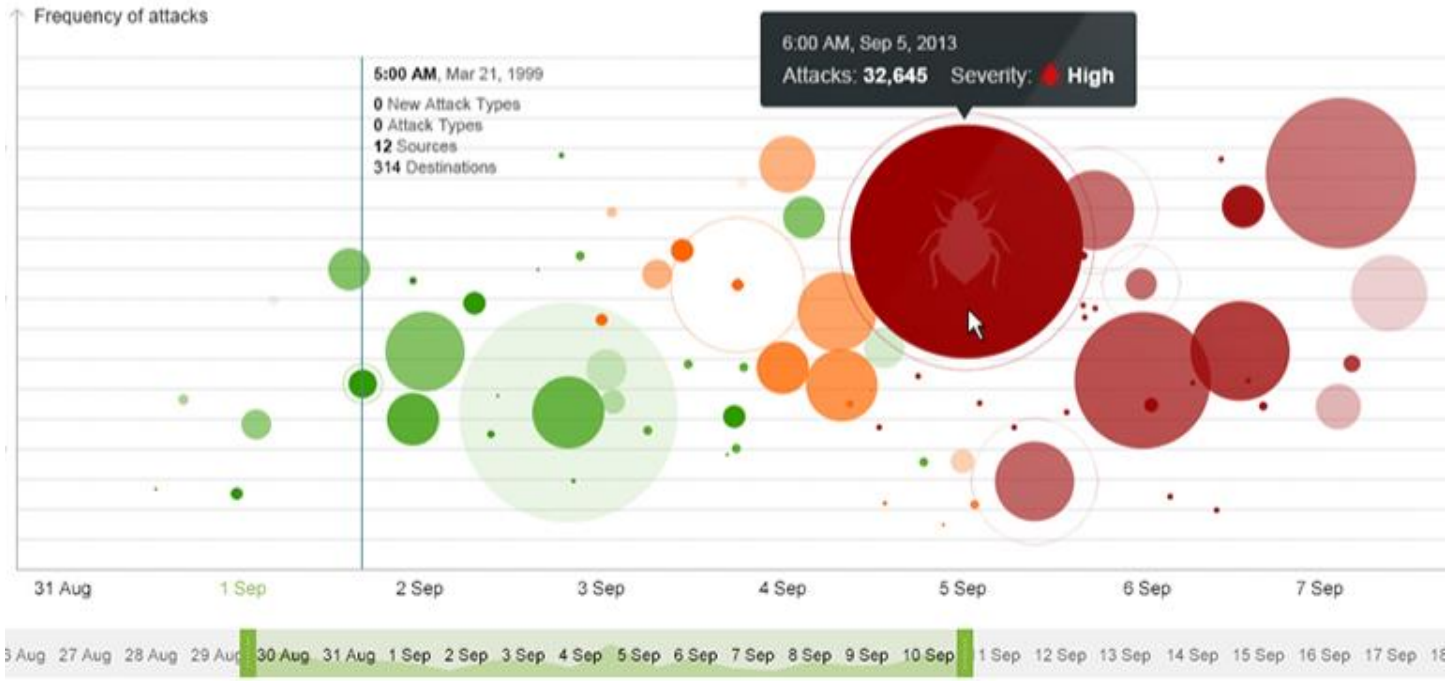
Threat Actor Analysis

- What Analysis do we need to detect the Threat Actors?
  - Data Visualization – Attack Map (Pretty-but-Useless)



Threat Actor Analysis

- What Analysis do we need to detect the Threat Actors?
  - Data Visualization – Attack Severity and Frequency over Time



Threat Detection Fails

- Missing threat detection strategy
- Inability to identify critical assets and impacts
- Out of date understanding of global threats
- Out of date understanding of industry threats
- No definition of who your primary Threat Actors are
- No definition of the various intents that Threat Actors' may have
- Assumption that internal users are all trusted
- A lack of attack knowledge to understand how Threat Actors will break in

Threat Detection Fails

- A lack of knowledge of the techniques to exfiltrate data and communications
- A lack of knowledge of security and detection bypass techniques
- Undefined Indicators of Compromise (IOC) to generate, aggregate and correlate
- Over collection of events that overwhelm Threat Analysts
- Misconfigured or ineffective security implementation / assumption it is working
- A lack of knowledge, skills, budget and resources to analyze and detect a threat
- Preference to dismiss alerts as false-positives, rather than investigate
- Lack of industry Cyber Threat Intelligence information sharing

Questions?

Thank you for attending

ty.miller@threatintelligence.com

www.threatintelligence.com

Phone: +61 409 713 735