AUTOMATING THREAT DETECTION & RESPONSE
TY MILLER

CEO, Threat Intelligence Pty Ltd
Evolve Security Automation

Black Hat Asia Review Board

CREST ANZ Board of Directors

Security Researcher, Presenter and Trainer

• Black Hat Training
• Black Hat Training
• Black Hat Training
• Black Hat Presentation
• Black Hat Presentation
• Black Hat Webcast
• Black Hat Webcast
• Hack In The Box Training
• Ruxcon Presentation
• Ruxcon Presentation
• Core Impact
• Co-Author
• Presentation
• Presentation
• Presentation
• Presentation

The Shellcode Lab
Practical Threat Intelligence
The Security Automation Lab
Reverse DNS Tunnelling Shellcode
The Active Directory Botnet
The Best Way to Catch a Thief
Intelligent Security Automation
Practical Threat Intelligence
The Active Directory Botnet
BeEF Bind Shellcode
DNS Channel Payload
Hacking Exposed Linux 3rd Edition
Machine Learning and Modern Malware Mitigations
Modern Threat Detection and Prevention
Securing Your Startup to Secure Big Brands
Can your application be breached?

... and many more
WHAT ARE WE DOING HERE?

• The state of the industry and why automating incident response is so important

• Why the average cost of a major security breach is so high

• How to automate threat detection and response to reduce the cost of a security breach
WHAT IS THE PROBLEM?

• We surveyed 120 Black Hat students across our Black Hat USA and Europe training courses …

• “Not a single security professional in the training had the in-depth knowledge or skills to effectively carry out an incident response investigation from end-to-end to contain a breach of their organization”

• This reflects closely on the current state of the IT security industry
In 2018, according to the UN, $800 billion - $2 trillion is laundered annually, mainly through crypto-currencies with an increase via in-game purchases.

In 2009, revenues from cyber-crime exceeded drug trafficking as the most lucrative illegal global business, estimated at profits of over $1 Trillion annually.
ATTACKERS VS. DEFENDERS

THREAT ACTORS
- Highly skilled
- Fully resourced
- Well funded
- Highly motivated

SECURITY TEAMS
- Limited skills
- Limited resources
- Limited budgets
- Limited motivation
WAR STORY

• Two threat actors aggressively infiltrating company

• Not detected by security team – limited skills, resources and budgets

• Hundreds of different backdoors found

• Redesign and implementation of security architecture to assume backdoored systems

• Overall breach cost estimated at $15M
SECURITY BREACH IMPACT

- Average total cost of a data breach in 2019:
  - Australia $2.13M
  - ASEAN $2.62M
  - Europe $4.33M
  - USA $8.19M

- How do we go from a user clicking a malicious link to suffering $8M in losses?
  - Investigation Costs
  - Loss of Revenue
  - Compliance Fines
  - Knock-on Costs
  - Increased Security Controls

- Cost of a breach is 95% higher in companies not using security automation
  - Average breach containment is 279 days

* IBM Cost of a Data Breach Report 2019
How do we automate this process (as much as possible) to reduce time to containment, and therefore, reduce breach costs?
AUTOMATED INCIDENT DETECTION

Cyber Threat Intelligence – OSINT Examples:

• Ransomware and C2 Intelligence
  http://osint.bambenekconsulting.com/feeds/c2-ipmasterlist.txt
  http://osint.bambenekconsulting.com/feeds/c2-dommasterlist.txt
  http://list.iblocklist.com/?list=xdcrpxkpcfqiaybcssw

• Spam and Phishing Intelligence
  https://www.spamhaus.org/drop/drop.txt
  https://www.spamhaus.org/drop/edrop.txt
  https://www.spamhaus.org/drop/dropv6.txt

• TOR and Open Proxy Intelligence
  https://check.torproject.org/exit-addresses
  http://spys.me/proxy.txt
  http://list.iblocklist.com/?list=xaebmixwuiogbyprb

• Attacks and Brute-Force Intelligence
  http://list.iblocklist.com/?list=qhizqtxnzctvvajwag

• DDoS Intelligence
  https://www.badips.com/get/list/ddos/

Integrate with NextGen FW, DNS Sinkhole, Threat Intel Gateway, SIEM

* IBM Cost of a Data Breach Report 2019
AUTOMATED INCIDENT DETECTION

- NextGen Firewalls / IPS / Proxy Content Filter / HoneyPots / Honey Tokens
  - Anomalous internal network traffic

- Endpoint Security Software
  - Malware Detection
  - Exploit Detection
  - Privilege Escalation / Credential Dump / Process Migration
  - Persistence / Service Creation / Account Creation

- File Integrity Software / Application Whitelisting
  - Unexpected filesystem changes

- SIEM
  - Anomalous system access (eg, local admin logins)
  - Security log analysis
  - Outbound data exfiltration
  - Aggregation of all of the above

* IBM Cost of a Data Breach Report 2019
What evidence needs to be collected for a security breach?

- Memory dump
- Disk image
- Running processes
- Network connections
- Registry hive
- Latest changed files
- User account list
- Local host file
- DNS Cache

- Swap files
- Hibernation files
- Startup scripts
- System and security logs
- Kernel and program hooks
- Web server modules list
- Driver list
- Network traffic
AUTOMATED EVIDENCE COLLECTION

What tools can be used for automating evidence collection?

- Memory dump
  - https://github.com/google/rekall/tree/master/tools/windows/winpmem
  - https://github.com/NateBrune/fmem + dd

- Disk Image / Swap Files / Hibernation Files / Locked Files / Master File Table
  - https://ad-zip.s3.amazonaws.com/FTKImager.3.1.1_win32.zip
  - https://github.com/jschicht/RawCopy
  - dd

- Built-in Operating System Tools
  - Running processes
  - Network connections
  - Registry hive
  - User account list
  - Local host file
  - Latest changed files
  - Startup scripts
  - System and security logs
  - Kernel and program hooks
  - Web server modules list
  - Driver list
  - Network traffic
What incident response analysis needs to be performed?

- Rootkit detection
- Malware detection
- Code injection detection
- Extract processes and drivers
- Command history extraction
- Hidden or deleted files
- Rogue processes
- Rogue network connections
- Rogue DNS requests
- Malicious registry entries
- Malware/Sandbox analysis on files
- Vulnerability and exploit identification
- Newly created user accounts
- Newly created or backdoored services
- Modified local host file
- Newly created or modified startup scripts
- Log file analysis typically for authentication or crash identification
- Rogue kernel and program hooks
- Rogue web server modules list
- Rogue driver list
- Network traffic analysis
- Intelligence IOC search
- Event timeline
What tools can be used for automating evidence analysis?

- Memory Analysis
  - Volatility  [https://www.volatilityfoundation.org/releases](https://www.volatilityfoundation.org/releases)
  - Rekall  [https://github.com/google/rekall/](https://github.com/google/rekall/)

- Malware and Bootkit detection
- Rogue and hidden processes, DLLs, drivers and services
- Rogue kernel and program hooks
- Code injection detection
- Command history extraction
- Extract network connections and sockets
- Malicious registry entries
- Master File Table analysis
- Timeline creation
What tools can be used for automating evidence analysis?

- Cyber Threat Intelligence
  - Map network connections to known bad IPs
  - Map DNS requests to known bad domains
  - Search file system for known bad IOCs
    
    https://github.com/Yara-Rules/rules
    yara command line tool

- Malware/Sandbox Analysis on executables / files
  - Anti-Virus / Endpoint Security Software
  - VirusTotal API

- Network traffic analysis
  - tcpdump / wireshark command line tools
    
    https://github.com/MITRECND/yaraprocessor
    https://github.com/MITRECND/chopshop
AUTOMATED RESPONSE ACTIONS

Incident response actions can be performed:

- Raise ticket to notify IR team of the breach
- Feed bad IP addresses in firewall block lists
- Feed bad domains / URLs in Proxy block lists
- Feed malicious domains into DNS sinkholes
- Feed malicious IPs and domains into IPS
- Send events to a SIEM
- Disable compromised / malicious accounts
- Terminate auto-scaled cloud system
- Terminate processes
- Quarantine malicious files
- Share threat intelligence data with peers
- Yara scans across internal machines
- Shut down victim hosts to contain the breach
How do we centrally manage automated incident response?

- **Open Source IT Automation Software**
  
  **Ansible**
  
  [https://github.com/ansible/ansible](https://github.com/ansible/ansible)
  
  Develop Ansible playbooks to automate your incident response
  
  **Pro:**
  
  - No required investment in commercial software
  - Good for non-existent or small budgets

  **Con:**
  
  - Requires a lot of time to develop, test and maintain
  - Requires human security resources, skills and experience

- **Commercial Security Automation Platforms**
  
  **Pro:**
  
  - Minimal time to implement for fast security capabilities
  - Minimal human security resources, skills or experience

  **Con:**
  
  - Requires budget for commercial software or platform
THANK YOU FOR ATTENDING

TY MILLER
CEO, THREAT INTELLIGENCE

ty.miller@threatintelligence.com
https://www.threatintelligence.com
https://evolve.threatintelligence.com