INTELLIGENT SECURITY AUTOMATION
INTRODUCTION

Ty Miller

• Managing Director
• Threat Intelligence Pty Ltd
  https://www.threatintelligence.com
  https://evolve.threatintelligence.com

• CREST Australia New Zealand
  • Board of Directors
  • Technical Team Lead
  • Assessor

• Black Hat Asia Review Board

Security Researcher, Presenter and Trainer

• Black Hat Training
• Black Hat Training
• Black Hat Training
• Black Hat Presentation
• Black Hat Presentation
• Black Hat Webcast
• Hack In The Box Training
• Ruxcon Presentation
• Ruxcon Presentation
• Core Impact
• Co-Author
• 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
Practical Threat Intelligence
The Active Directory Botnet
BeEF Bind Shellcode
DNS Channel Payload
Hacking Exposed Linux 3rd Edition
Machine Learning and Modern Malware
Modern Threat Detection and Prevention
Securing Your Startup to Secure Big Brands
Can your application be breached?

… and many more
OVERVIEW

Key Takeaways

• Understand the driver behind Security Automation and why it is so important

• Learn how to utilize Security Automation to maximize your security skills, resources and budgets

• How to streamline your operational security process through automated intelligence correlation and contextual awareness
WHY SECURITY AUTOMATION?
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.

$1T

$2T
## Attacker Motivations

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Variety</th>
<th>Vector</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use of stolen creds</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(hacking)</td>
<td>ESP: 27, FIG: 6, FIN: 598</td>
<td></td>
</tr>
<tr>
<td><strong>Use of backdoor/C2</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(hacking)</td>
<td>ESP: 121, FIG: 557</td>
<td></td>
</tr>
<tr>
<td><strong>Theft</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(physical)</td>
<td>ESP: 39</td>
<td>FIG: 27</td>
</tr>
<tr>
<td><strong>Tampering</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(physical)</td>
<td>ESP: 21</td>
<td>FIG: 21</td>
</tr>
<tr>
<td><strong>SQLi</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(hacking)</td>
<td>ESP: 14</td>
<td>FIG: 14</td>
</tr>
<tr>
<td><strong>Spyware/Keylogger</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(malware)</td>
<td>ESP: 38, FIG: 557</td>
<td>FIN: 557</td>
</tr>
<tr>
<td><strong>Skimmer</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(physical)</td>
<td>ESP: 60</td>
<td>FIG: 60</td>
</tr>
<tr>
<td><strong>Ransomware</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(malware)</td>
<td>ESP: 14</td>
<td>FIG: 14</td>
</tr>
<tr>
<td><strong>Ram scraper</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(malware)</td>
<td>ESP: 191</td>
<td>FIG: 191</td>
</tr>
<tr>
<td><strong>Privilege abuse</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(misuse)</td>
<td>ESP: 17, FIG: 37, FIN: 74</td>
<td>FIN: 74</td>
</tr>
<tr>
<td><strong>Pretexting</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(social)</td>
<td>ESP: 39</td>
<td>FIG: 39</td>
</tr>
<tr>
<td><strong>Possession abuse</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(misuse)</td>
<td>ESP: 6, FIG: 9, FIN: 29</td>
<td>FIN: 29</td>
</tr>
<tr>
<td><strong>Phishing</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(social)</td>
<td>ESP: 163, FIG: 490</td>
<td>FIN: 490</td>
</tr>
</tbody>
</table>

| **Website**                 |         |        |
| (social)                    | ESP: 19 | FIG: 19 |
| **Web drive-by**            |         |        |
| (malware)                   | ESP: 26 | FIG: 26 |
| **Web application**         |         |        |
| (hacking)                   | ESP: 5, FIG: 23, FIN: 507 | FIN: 507 |
| **Victim work area**        |         |        |
| (physical)                  | ESP: 16 | FIG: 16 |
| **Victim public area**      |         |        |
| (physical)                  | ESP: 39 | FIG: 39 |
| **Victim grounds**          |         |        |
| (physical)                  | ESP: 31 | FIG: 31 |
| **Remote access**           |         |        |
| (misuse)                    | ESP: 7, FIG: 7, FIN: 7 | FIN: 7 |
| **Public facility**         |         |        |
| (physical)                  | ESP: 6 | FIG: 6 |
| **Physical access**         |         |        |
| (misuse)                    | ESP: 8, FIG: 11, FIN: 34 | FIN: 34 |
| **Phone**                   |         |        |
| (social)                    | ESP: 5 | FIG: 5 |
| **Personal vehicle**        |         |        |
| (physical)                  | ESP: 7 | FIG: 7 |
| **Partner facility**        |         |        |
| (physical)                  | ESP: 5 | FIG: 5 |
| **Partner**                 |         |        |
| (hacking)                   | ESP: 108 | FIG: 108 |
| **LAN access**              |         |        |
| (misuse)                    | ESP: 19, FIG: 31, FIN: 68 | FIN: 68 |

Limited Security Budgets
• Security is an expense
• This means security budgets will always be limited

Limited Security Skills
• No offence intended! Our industry has a very real security skills shortage
• Risk Managers, Security Managers and Security Officers have a wide range of security skills
• Often gaps in deep technical expertise, such as in-depth incident analysis and bypass techniques

Limited Security Resources
• Limited security budgets result in under-resourced security teams
• This means security teams focus on BAU or fight fires
• No time to implement strategic security, fix security flaws, threat hunt, or perform breach response
THREATS VS. DEFENDERS

- Threat Actors:
  - Highly skilled
  - Fully resourced
  - Well funded
  - Highly motivated

- Security Teams:
  - Limited skills
  - Limited resources
  - Limited budgets
  - Limited motivation
SECURITY AUTOMATION AND INTELLIGENCE
SECURITY AUTOMATION

• What areas of security are prime for automation and orchestration?
  
  • Automated Cyber Threat Intelligence
  • Orchestrated Security Infrastructure
  • Automated Incident Response
  • Automated Penetration Testing
AUTOMATED INTELLIGENCE

- Automated Intelligence Collection
- Automated Intelligence Transformation
- Automated Intelligence Aggregation
- Automated Intelligence Analysis
- Automated Intelligence Sharing
EXTERNAL INTELLIGENCE

• External Intelligence Sources

A wide range of intelligence sources exist that can be used to:

- Gain an insight into threats
- Prevent attacks
- Detect security breaches
- Identify risky systems
- Identify risky employees
- Gain an insight into industry-based threats

- Malware Feeds
- Botnet Feeds
- TOR Feeds
- Phishing Feeds
- Scanner Feeds
- Spam Feeds
- Social Media Data
- Online Dump Sites
- Offline Password Dumps
- Defacement Archives
- Dark Web
- Vulnerability Feeds
- Exploit Feeds
- Intelligence Sharing
INTERNAL INTELLIGENCE

- **Internal Intelligence Sources**

  Massive amounts of intelligence data exists within your organization that can be used to:

  - Identify security incidents
  - Provide context to threat activity
  - Generate internal intelligence feeds
  - Detect malicious network traffic
  - Detect anomalous traffic
  - Detect security breaches
  - Identify risky systems
  - Identify risky employees
  - Identify compromised accounts
  - Generate industry-based threat data
How to automate the collection and analysis of intelligence data

- Collect relevant intelligence data for your strategic purpose
- Transform intelligence data into a normalized format removing irrelevant data and formatting
- Aggregate intelligence data into central data storage, such as a file or database
- Analyse the intelligence data potentially by correlating it with other data or intelligence sources
- Make a security decision based on the intelligence data and action it to prevent threats or contain breaches, or share the intelligence
• Orchestrated Security Infrastructure
• Automated Intelligence Integration
• Automated Incident Detection
INTELLIGENCE INTEGRATED SECURITY INFRASTRUCTURE

• DNS Sinkhole
  • Utilize intelligence feeds to detect malicious domains and IP addresses being requested by internal systems to automatically identify security breaches.

• Syslog Collector
  • Utilize intelligence feeds to map internal syslog entries, such as proxy logs, to automatically identify security breaches.

• Block List Server
  • Utilize intelligence feeds to be served up by a block list server and pulled directly into firewalls and web application firewalls for automated protection.
DNS SINKHOLE

Common Security Breach Flow
• Security Breach occurs
• Implant embedded into the system
• DNS lookup for Command and Control
• Connection to Command and Control
• Attacker remotely accesses the system

DNS Sinkhole Flow
• Security Breach occurs
• Implant embedded into the system
• DNS lookup for Command and Control
• Sinkhole blocks identified malicious domains

Intelligence Collector → Intelligence Transformer → Intelligence Aggregator → Intelligence Analyzer → Automated Incident Response

Download malicious domains

Infected System → Corporate DNS Server → DNS Sinkhole → Command and Control

INTELLIGENT SYSLOG COLLECTOR

- Central log collection for evidence preservation and trust protection
- Long-term storage for compliance requirements
- Automated intelligence-integration for log analysis for automated breach detection
- Trigger security automation and incident response from logging events
INTELLIGENCE BLOCKLIST SERVER

• Cyber threat intelligence data collected and made available via a web interface
• Security devices, such as firewalls and WAFs, automatically download the intelligence data
• Malicious IP addresses, URLs or domain names are automatically blocked
AUTOMATED INCIDENT RESPONSE

Automated Incident Response

- Automated Evidence Collection
- Automated Evidence Analysis
- Automated Incident Response Actions
AUTOMATED INCIDENT RESPONSE

End-to-End Automated Incident Response Activities

- System is breached / Incident occurs
- Internal and external incident detection techniques used to automatically detect the security incident
- Automated evidence collection triggered to capture the security incident data from the victim system
- Collected evidence is then automatically analysed to identify various indicators of compromise and determine whether a breach has occurred
- Automated incident response actions are then triggered for compromised systems and accounts, customised for each business need
AUTOMATED PENETRATION TESTS

- Automated Reconnaissance
- Automated External Infrastructure Penetration Testing
- Automated Internal Infrastructure Penetration Testing
- Automated DevOps Application Security Testing
AUTOMATED DEVOPS APPLICATION SECURITY TESTING

- What is Automated DevOps Application Security Testing?

  - Developer commits new code
  - CI/CD pipeline detects new code
  - Runs automated functional tests
  - CI/CD pipeline runs automated application vulnerability scanner
  - Import results into CI/CD pipeline
  - CI/CD pipeline stops vulnerable code going into production

Code Repository → CI/CD Pipeline → DevOps Security Testing → CI/CD Pipeline → Staging / Production
SECURITY AUTOMATION
BUSINESS BENEFITS

• Repeatable and automated specialist security capabilities to immediately enhance your organization’s skills and capabilities

• Streamlines your security operations by automating security tasks, allowing security resources to focus on business-specific strategic security activities

• Security budgets are maximized by reducing the need for additional security resources, combined with subscription or usage-based billing
THANK YOU FOR ATTENDING

TY MILLER
MANAGING DIRECTOR

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