Handling Vast Amounts of Threat Intel via Automation

Justin Swisher,
Security Strategy Manager
jswisher@anomali.com
Agenda

• Threat Intelligence Automation
  • Intelligence management
  • Intelligence deployment
  • Intelligence integration

• Adversary Simulation
  • Beyond IOCs
  • External and Internal intelligence
  • Example
  • Automation
Threat Intelligence Management

- Massive amount of IOCs across numerous data feeds
- Duplication between sources
- Aggregation of all these feeds into a central location
- Enriching indicators for better context
- Human analysis, verification, and tagging

THREAT OVERLOAD

78% say threat intelligence critical for achieving strong security posture

70% of organizations say they’re swamped by cyberthreat data

source: www.anomali.com/ponemon
• How to get IOCs into your detection/blocking systems?
• What IOCs do you want to actually deploy?
• Automate the deployment of IOCs via a defined tagging library
  • Leverage tagging
    • FW-BL
    • IDS/IPS
    • SIEM
    • HIPS
• Automate the contextualization of alerts
• Human analysts are still critical for judgement calls
  • Automation adds speed and context
• Automate ticket creation and population
• Leverage Tags

Tags

- high-priority-threat ✗
- identified-threat ✗
- SOC-ALERT ✗
• Once you’ve automated the tactical intelligence (IOCs), you can progress to operational intelligence
• Combine external intelligence with internal intelligence
  • Identify adversaries targeting your industry
  • Align their capabilities with your internal systems
• Research adversary behaviors during attacks
  • Threat sharing
  • Incident response
Automation of Adversary TTPs

• Red Team and Blue Team Collaboration
  • Threat Intelligence outlines adversary TTPs and typical progression
  • Pen Testers emulate these actions
    • Preferably NOT in production systems

• After manual tests and verification, automate using tool of choice

• Numerous Open Source Tools
  • Metta (https://github.com/uber-common/metta)
  • Caldera (https://github.com/mitre/caldera)
  • Atomic Red Team (https://github.com/redcanaryco/atomic-red-team)
• FIN7 – “financially motivated threat group that has primarily targeted the retail and hospitality sectors, often using point-of-sale malware”

• TTPs
  • Persistence using registry Run and Run Once keys
  • Command line obfuscation
  • Mshta used to download and execute malicious scripts

• MITRE ATT&CK™
  • Tactic – Defense Evasion, Execution
  • Technique – Mshta
  • ID – T1170

https://attack.mitre.org/wiki/Group/G0046
https://attack.mitre.org/wiki/Technique/T1170
Adversary Simulation - Example

• Metta YAML action file example below
  • Thanks to Chris Gates and Red Canary - awesome work by these folks

```yaml
enabled: true
meta:
  author: jswhiser
  created: 2018-08-02
  decorations:
    - Purple Team
  description: FIN7 TTP Test Example
  mitre_link: https://attack.mitre.org/wiki/Group/G0046
  mitre_attack_phases:
    - Defense Evasion
    - Execution
  mitre_attack_techniques:
    - MSHTA (T1170)
    - Registry Run Keys (T1068)
  purple_actions:
    2: cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\Windows\System32\calc.exe"
```
Summary

• Start small – automate the simple intelligence tasks firsts
• Focus on IOCs in the beginning – easy to manage, deploy, and integrate
  • But don’t stop there!
• Mature into TTP research and adversary simulation
• Lastly – automate what you can and recognize that sometimes you still need a plain old human