Threat Hunting Strategies

Brian Olliff

Defensive Engineering Instructor

Key Concepts

+ **Preparation and background**

+ **Threat hunting methods**

+ **Hypothesis creation**

MAJOR TOPICS

- Attackers and malware
- Threat hunting preparation
- Hypotheses
- Data Analysis

LEARNING OUTCOMES

- Understand different attacker groups and their motivations
- Understand various ways attackers can enter organization’s systems
- Be able to explain threat hunting hypothesis and how to form one
- Understand different types of threat hunts, and different hypothesis types for each

PREREQUISITES

- Understanding of basic cybersecurity topics
- Understanding of what threat hunting is, and why it’s important
- Knowledge of threat hunting terminology (IOC, TTP, etc)

Let’s Get Started!

Threat Hunting Strategies

+ Explanation of various methods & strategies for performing threat hunt
+ Start with background of attackers, their motivations, and attacks

Attackers & Motivations

Threat Actors

- External - no account or authorization on network/system
  - Unskilled attacker -> well-funded nation states
- Internal - has been granted some level of authorization
  - Employees, vendors, business partners, etc
- All attackers have some sort of motivation & intent
  - Financial, political, curiosity, etc
  - Data theft, vandalism, etc
- Various levels of skill, funding, and resources
  - Unskilled using “commodity” malware and tools
  - Custom zero-day exploits, with government funding

Nation-state Actors

- Threat actor supported by resources of host country
  - Military, government, financial, etc
- Separated from host government/country
  - Unofficial support
  - Pose as “hacktivists” or independent groups, other countries
  - Provides plausible deniability to government
- Frequently attack using APTs
  - Advanced Persistent Threat
- Motivations
  - Espionage, financial, cyber “warfare”, disinformation, other political

APTs

- Highly sophisticated and capable of extended attacks
- Advanced
  - Extensive skills & resources, capable of complex attacks
- Persistent
  - Able to remain on network long-term without detection
- Often sponsored by nation-states (officially or unofficially)
- Often target high value organizations
  - Government agencies, critical infrastructure, political campaigns, etc
  - Smaller organizations as part of supply chain attack
- Motivations similar to nation-states

Organized Crime

- Not necessarily tied to specific country
- Very similar to typical organized crime syndicates
  - Cyber attacks vs physical attacks
- May span multiple regions, jurisdictions
  - Complicates prosecution
- Common goals are financial profit
  - Carried out through financial fraud and extortion
  - Data exfiltration
    - especially PII/PHI & IP

Hacktivists

- Groups of threat actors motivated by political and social causes
  - Anonymous, WikiLeaks
- Common goals/motivations
  - Data theft with intention to release
  - Defacement of public sites
  - DoS (denial of service) attacks
- Often target political and financial groups
  - May also target media organizations and other companies
  - Targets depend solely on groups' goals

Others

- Unskilled attackers
  - Threat actors who may have minimal skills and knowledge
  - Normally use commonly available tools and malware
  - May not understand tools or tactics they are using
  - Often have no specific target or goals
    - Gaining attention, proving their skills & abilities
- Insider threats
  - Intentional
  - Unintentional
  - Shadow IT

Threat Vectors

Threat (Attack) Vector

- Path that an attacker takes to gain unauthorized access

- Common attack vectors
  - Removable storage
  - Software/hardware vulnerabilities
  - Unsupported or out-of-date systems
  - Images and malicious files
  - Open ports
  - Supply chain

Removable Storage

- USB thumb drives, portable HDs, memory cards, (less frequently) CDs
- Attackers can conceal malware on removable media
  - Run automatically when inserted
  - Run when application on drive launched
- USB drop attack
  - Attackers place removable media around specific locations
  - Relies on users picking up drive and inserting out of curiosity
- Attacks may run automatically, may require user action
  - If action required, social engineering to trick user

Malicious Files

- One of most common methods for spreading malware
- Malware can be embedded in legitimate files
  - Weaponized applications
  - Macros in Word documents & PDF files
  - Steganography
    - Concealing information within other messages
    - Commonly used with image files
- Frequently combined with other vectors to deliver files
  - Email delivery
  - Removable storage

Messaging-Based Vectors

- Email
  - One of most common attack vectors
  - Phishing emails, malicious attachments and links in message body
- SMS
  - Frequently used to bypass MFA restrictions
  - Can also compromise mobile devices
    - Attackers send malicious links/files via SMS
- Instant Messaging
  - Similar to SMS, but available on more systems
  - Typically more secure than SMS, but can still contain vulnerabilities
- Social engineering is common thread among message vectors

Vulnerable & Unsupported Systems

- Attackers frequently look for and exploit vulnerabilities
  - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source - NIST
- Vulnerabilities are very common in all systems
  - Software & hardware
  - Zero-day - new vulnerability that is being exploited, no fix yet
- Unsupported systems
  - Not actively maintained or supported by vendor/manufacturer
  - Commonly do not receive security updates
  - Contain multiple vulnerabilities and outdated security measures

Advanced Malware

Malware

- Software that does something bad, from user perspective
  - Malicious software
- Various classifications of malware
  - Virus, worms
  - Trojans
  - Ransomware
  - Potentially unwanted programs (PUPs)
  - Adware/spyware
  - Remote access trojan (RAT)
  - Rootkits
  - Logic bombs

Ransomware

- Malware that attempts to extort victim for money to recover data
  - Most will encrypt and only provide decryption after payment
    - Crypto-ransomware
  - Some is only threatening, without blocking access
- Will prominently display notice(s) demanding payment or other action
- Encryption-based can only be remediated by restoring data
  - Possibly by paying ransom - but almost never recommended
    - Sometimes illegal
- Demand payment via various methods, often cryptocurrency

Remote Access

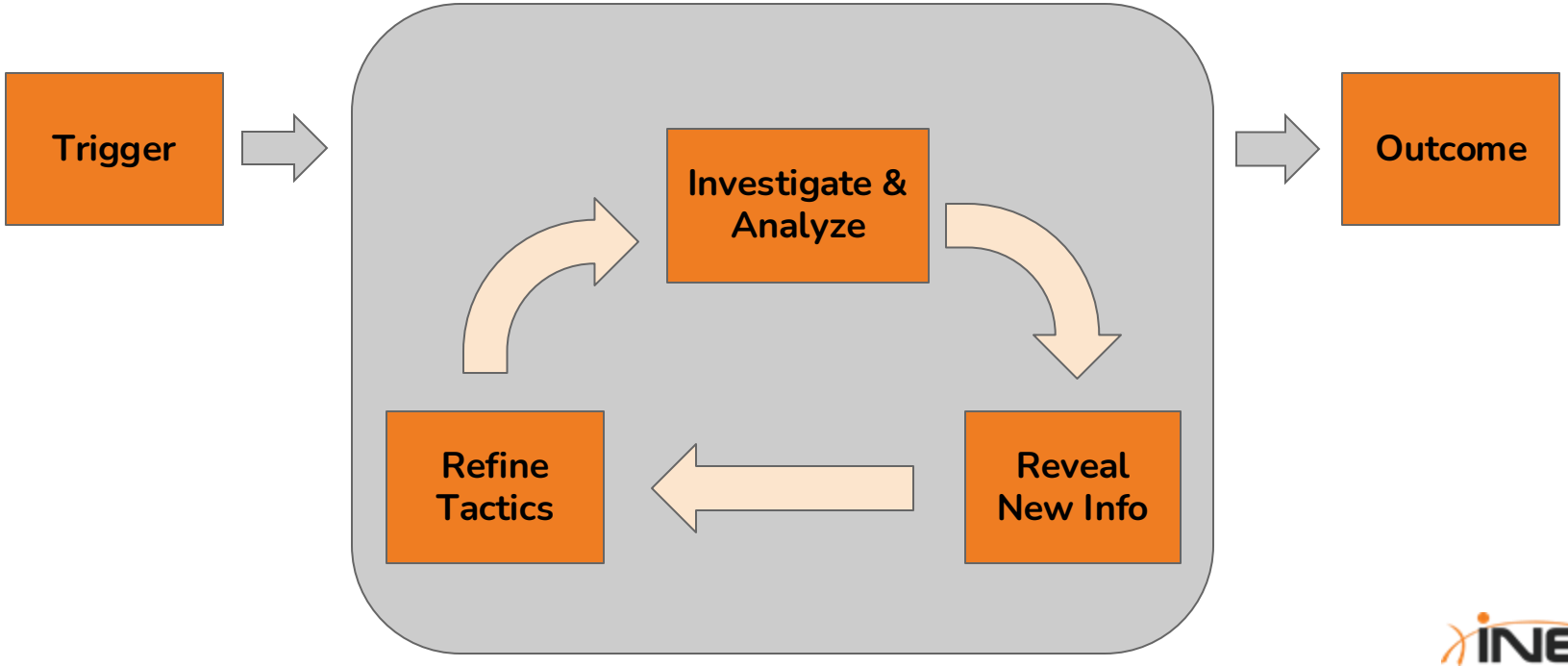
- RAT - Remote Access Trojan
  - Remote Administration Tool
  - Provides attacker with backdoor access to system
- Command & Control
  - Attacker controlled infrastructure that compromised systems connect to
  - C&C or C2
  - Often use disguised DNS or HTTPS traffic to hide usage

Advanced Malware

- Rootkit
  - Malware that can run as unrestricted system processes
  - Can compromise critical system files and be difficult to detect
    - High level of access results in effective masking, difficult discovery
    - Often erases logs to hide evidence of infection
  - Modern OSes have mechanisms to help prevent
- Logic bomb
  - Malware designed to not run immediately
  - Can wait for predetermined date/time or specific event before executing
  - Not necessarily typical malware
    - Disgruntled system admin leaving a scripted trap

Prepare to Hunt

Threat Hunting



Prepare Information & Data

- Access to necessary intelligence sources
  - Paid (or free) feeds/services
  - Open source intelligence (OSINT)
  - Internal reports
- MITRE ATT&CK Framework
- TTPs of potential attackers
- IOC sources
  - Specific data after hypothesis formed and scope defined
- Appropriate log data/access
  - Ideally configured well before hunt
- Availability of all determines hunting capabilities

MITRE ATT&CK Matrix

https://attack.mitre.org

Technique

Phishing

Sub-techniques (4)

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., Email Hiding Rules).[1][2] Another way to accomplish this is by forging or spoofing[3] the identity of the sender which can be used to fool both the human recipient as well as automated security tools,[4] or by including the intended target as a party to an existing email thread that includes malicious files or links (i.e., "thread hijacking").[5]

Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,[6][7] or install adversary-accessible remote management tools onto their computer (i.e., User Execution).[8]

ID: T1566

Sub-techniques: T1566.001, T1566.002, T1566.003, T1566.004

Tactic: Initial Access

Platforms: Identity Provider, Linux, Office Suite, SaaS, Windows, macOS

Contributors: Liora Itkin; Liran Ravich, CardinalOps; Ohad Zaidenberg, @ohad_mz; Philip Winther; Scott Cook, Capital One

Version: 2.6

Created: 02 March 2020

Last Modified: 07 October 2024

Version Permalink

Logging

- Required logging must be in place long before hunting
  - Minimum of timeframe that hunt will possibly cover
- Specific log sources depend on organization
  - Authentication/authorization systems
  - Endpoints (with Sysmon)
    - File modification (creation, deletion, changes)
    - Registry modifications
    - Process creation
  - IPS/IDS/Firewall
- All stored in centralized location for ease of searching

Forming a Hypothesis

Hypothesis

- Threat hunts start with hypothesis
  - Assumption about malicious activity occurring
  - Can be tested
  - “Threat actors have created scheduled tasks to execute code”
  - “An endpoint has communicated with <malicious IP>”

- Identifies specific behavior/activity to hunt for
- Requires understanding of attack technique
- Indicates which data and sources used to detect threat
- Can be very specific or more vague

Hypothesis

1. Determine tactic/technique or IOC
    a. Review intelligence & other sources (MITRE ATT&CK)
2. Identify associated procedure(s)
    a. MITRE ATT&CK as one source
    b. Additional research recommended
        i. Prerequisites, other requirements, outcome of success, etc
3. Determine logs/data required for hunt
    a. Where do artifacts exist on systems?
        i. Files, registry, memory, network traffic, processes, etc
4. Set scope of hunt
    a. Systems involved, duration of hunt

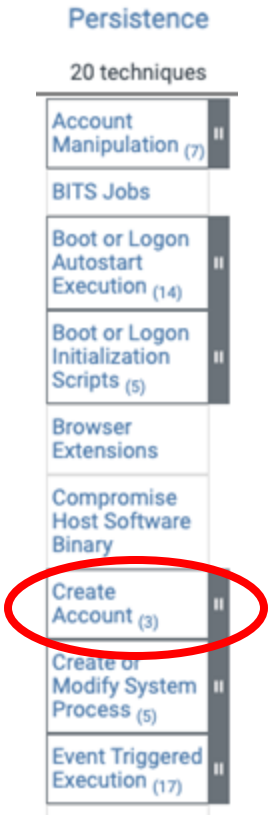
Structured Hunt Hypothesis

Structured Hunt

- Hypothesis based off attacker's methods
- Relies heavily on TTPs
  - MITRE ATT&CK Matrix
- Hunt based on possible symptoms of that type of attack

Hypothesis Building

- Tactic - Persistence
  - “Adversary is trying to maintain their foothold”
- Technique - Create Account
  - Used to maintain access to system
  - Can establish secondary access without needing persistence remote tools



Hypothesis

“Attackers have created administrative accounts on endpoints to maintain their access on the network”

Hunting Options

- Examine logs from in-scope workstations for evidence of any new account creation
- Check Active Directory for new accounts created during hunt time frame
- Examine any network devices in-scope

- Many accounts may be found - most may be legitimate
  - Analysis of accounts required (who created, why, when, etc)
  - If suspicious or malicious accounts found
    - Coordinate with IR team
    - Continue hunt to determine origin and effects of accounts

Unstructured Hunt Hypothesis

Unstructured Hunt

- Hypothesis based on IOCs
- Sources
  - Intelligence reports
  - IR/SOC information
  - Security controls
  - Previous threat hunt

Hypothesis Building

- Intelligence report from vendor shows attacker is targeting organizations in same industry
- IPs
  - 123.45.67.89
  - 86.75.30.9
- SHA256 hashes of malicious executables
  - badfile1.exe - 56e84483194d38026c76785faa2800d2c1e556f8609676e3c83ea454a1a26e24
  - badfile2.exe - 55d008cbeaa2a78097d7973c5820bd8d427088387a4b2ca7dd75b09fdb879f2b

Hypothesis

“Attackers have compromised the network, executing files with the attached file names/hashes and are communicating with C2 infrastructure at attached IP addresses”

Hunting Options

- Examine logs for in-scope systems for evidence of
  - Presence or execution of files matching
    - badfile1.exe
    - badfile2.exe
    - 56e84483194d38026c76785faa2800d2c1e556f8609676e3c83ea454a1a26e24
    - 55d008cbeaa2a78097d7973c5820bd8d427088387a4b2ca7dd75b09fdb879f2b
  - Network communication to or from
    - 123.45.67.89
    - 86.75.30.9
- If any found, excellent indication of threat
  - Coordinate with IR team
  - Continue hunt

Situational Hunt Hypothesis

Situational Hunt

- Hypothesis based on specific risk or threat
- Often starts with assessment of network (or individual system)

Hypothesis Building

- Risk assessment shows that customer-facing web server farm is at high risk of attack
  - Commonly exploited software
  - Well-known site with large amounts of traffic
  - Significant financial and reputational impact from breach or downtime

- Research software to determine vulnerabilities/common exploits
- Use organization's baselines to identify "normal"
  - Geo location of IPs for customers
  - Common user-agent strings
  - Normally accessed files on web server

Hypothesis

“Attackers are targeting the customer ordering portal in an attempt to compromise and steal customer and organization data”

Hunting Options

- Based on research, examine logs for evidence of common exploits
  - HTTP access logs
  - WAF logs
- Verify that IPs accessing public server are in line with normal activity
  - Ensure no/minimal traffic from locations with no customers, or known adversarial countries
- Compare logged activity with documented baseline activity
  - Normal user-agent strings for browsers
  - Look for attempts to access “non-standard” files on web server

Data Analysis

Data Review

- Review available logs and data
  - Ensure required sources are available
  - Ensure available time frame is sufficient
- Ensure “normal” baselines are known
  - Running processes
  - User logins (where, who, when, type, etc)
  - Network connections
  - Services/scheduled tasks
  - Permitted/approved software

Data Analysis

- Normally performed on SIEM
  - Splunk, ELK Stack, etc
- Analysis requires multiple steps
  - Searching, aggregating, filtering
  - Steps are different depending on hunt
- Searching
  - Entering query to attempt to find answers to questions
  - First searches often require “fine tuning”
    - Change time frame, exclude IPs, filter out user, etc
  - Continuous process, always adjusting

Aggregation

- Grouping values within same fields together
- Normally sorted by most common or least common
- Useful for providing different perspective

Process name	Occurrences
Svchost.exe	13
Winword.exe	9
Calc.exe	1

Data Analysis

- Search results further expanded to match exact needs
- Example: Searching for executed PowerShell commands
  - Simple search results in command name
  - Expanded information can include
    - Full command executed
    - User who executed command
    - Which host
    - How many times command was run
- Analysis process is very situational

Threat Hunting Strategies - Summary

Key Concepts - Recap

+ **Preparation and background**

+ **Threat hunting methods**

+ **Hypothesis creation**

Learning Outcomes Recap

- Understand different attacker groups and their motivations
- Understand various ways attackers can enter organization’s systems
- Be able to explain threat hunting hypothesis and how to form one
- Understand different types of threat hunts, and different hypothesis types for each

Next Steps

- Continue with Threat Hunting learning path
- Revisit courses or videos about threat actors and their motivations
- Practice navigating and using MITRE ATT&CK Matrix
- Practice creating hypotheses for different types of hunts and scenarios

Thank you!

Threat Hunting Strategies

+ Background of attackers, motivations & attacks
+ Hypothesis creation for different types of hunts
+ Thank you for your time!

EXPERTS AT MAKING YOU AN EXPERT