Threat Hunting Scenario

1. Threat Hunting Hypothesis

Web Proxy- find consistent HTTP beaconing behaviour which may indicate malware C2

Hunt Scenario Description

Malware C2 frequently establish regular request intervals ("beacons") to maintain communication with the attacker's infrastructure. Suspicious patterns can be hunted using different techniques which includes

- Dynamically generated domain analysis,
- Threat intelligence comparison
- Domain rarity analysis
- User agent analysis.

This hunting needs to be based on either on IP address or the account name having count of distinct patterns.

2. Threat Hunting Hypothesis

- Web Proxy/ DNS – Hunt for malware by investigating the User-Agent strings
- HTTP proxy data: list of known-bad URL's (optional) mass counting, string compare, tokenization, outlier detection

Hunt Scenario Description

- Detect and flag abnormally short or long strings in URL's
- Detect and flag known adverse user agents.
- Create a behaviour profile for user agent length and flag abnormally short or long user agents and rare user agents.

3. Threat Hunting Hypothesis

DNS / Web Proxyhunt for common behaviour of HTTP-based attacks

Hunt Scenario Description

- Create a behaviour profile for followed requests from same source or from an entity to rare URL's.
- Increase in numbers of request could indicate potential to generate a working exploit for a supposed vulnerability or position to use a web shell embedded in the web content directory
- Investigate URI resources that has vulnerability (from vulnerability scans and penetration testing report) in the front end or back-end application
- Perform outlier analysis on behaviour profiled length of URL's / Domains and show violations on unusual short or long user agents.

4. Threat Hunting Hypothesis

- DNS / Web Proxy hunt for the incoming POST requests that have no referrer.
- Then identify the number of posts.
- Multiple command execution through http requests in a very short amount of time can indicate suspicious web traffic and this hypothesis will lead to a propagated adversarial effect.

Hunt Scenario Description

- Log Source: Webserver logs
- Request Method: POST
- Referrer: None
- Count > 20
- Event Difference Time: 30 Min
- In this hunt scenario bytes in or bytes out will not be consistent in size.
- Communication will be observed from single or multiple IP address. This will lead to establish and maintain communication to command and control.

5. Threat Hunting Hypothesis

- Web Proxy / DNS / HTTP – Detect potential interaction to command-and-control centre.
- Activity of outgoing traffic events that contains information about domains visited by internal clients, such as DNS query or HTTP proxy logs.
- Threat hunter also need a list of dynamic DNS provider domain names.

Hunt Scenario Description

- DNS or Web Proxy events can contain information about unique hosts and dynamic DNS.
- Segregate the event traces that contain domains hosted on dynamic DNS providers. Provide violation information on domains requested by very few users/IP/Systems.
- Passive hunt on list or feed of known dynamic DNS (DDNS) domains to query against data.

6. Threat Hunting Hypothesis

Web shell hunting is a hypothesis in which detection actions are taken by adversary when a web shell is initially placed on a web server. Windows security event logs (4688 / 592 events), Endpoint detection and response, HIPS or other host monitoring tools provides detailed information on process creation.

Hunt Scenario Description

- On system level check the webserver process, also check if this process are generated from PHP or asp.net function like eval(), exec(), shell_exec(),bind(), etc.
- Perform parallel monitoring for web directory for traces of new file addition and/or file modification, for example using notify(apache), Filesystem Watcher(IIS).
- Monitor all parameter which are passed through or attached to media files (e.g /media/security0morel.jpg?id=ls)
- Hunt for commands executed on system like cmd.exe, powershell.exe or rare process executed.
- Hunt for supplementary files uploaded or exfiltrated from system with extension like .exe, .rar, .7z, .zip, .tar,. bz2

7. Threat Hunting Hypothesis

- System level suspicious binary execution. To hunt for any suspicious binary execution, investigate 4688 events of windows.
- Hunting lateral movement with explicit login credentials.

Hunt Scenario Description

- Analysis for windows security events – (4688/592 events). A web shell/malicious binary is placed on an endpoint system, the command which will be executed need to tie back to account. Finding the webserver process and a child process of webserver will be indication of compromise.
- If same child process is found on other system of enterprise posture, then it is a serious indicator of lateral movement.
- Hunt for eventid's 4728, 4732, 4756 for same user added to privileged group. Privileged escalation occurs once the attacker completely gets access and control over account/system/ within the environment.

8. Threat Hunting Hypothesis

System level authentication based lateral movements. Not all of these events are enabled by default, so you may need to work with your system admin team on audit policy.

Hunt Scenario Description

Transactions of abnormal event from the below mentioned category within the same user context in a short span indicates potentially malicious behaviour.

- Successful Logon (Eventid 4624) primarily look for Logon Type 3,10,2,11
- Increase in Failed Logon (Eventid 4625)
- Kerberos Authentication (Eventid 4768)
- Increase in Kerberos Service Ticket (Eventid 4776)
- Increase in Assignment of Administrator Rights (Eventid 4672)
- Increase in Multiple user Account currently disabled (Eventid 4725)
- Increase in Multiple User Account deleted (Eventid 4726)
- Increase in Account lockout (Eventid 4740)

9. Threat Hunting Hypothesis

Hunting Lateral Movement with probable privilege escalation attempts.

Hunt Scenario Description

- Perform deep analysis on rare process executed on system event ID 4688. Look across parent process and child process if are executed on system.
- Analysis for event ID 4728 and 4756 in domain controller logs on same system by same user.
- Detect account which was added to group for 4732 on both the domain controller and workstation.
- Escalating privileges of a non-privileged account to a privileged group is a routine method for threat actors to clinch more access to a compromised system or domain.

10. Threat Hunting Hypothesis

Hunting lateral movement with exploring of remote shares – detect instances of psexec service (remote command execution) on Windows systems by examining event logs involving access control to remote shares.

Hunt Scenario Description

- Preliminary analysis starting with event ID 4663, event ID 5140
- Based on the analysis direction perform investigation for event ID 5145. Which indicates, a network shared object was checked to see whether client can be granted desired access.
- Exclude all logs which contains IPC$ and the service is PSEXECSVC-*.

- Pay attention to 5145 events for access to the ADMIN$ share for tool/file copies and execution events.

11. Threat Hunting Hypothesis

Hunting remote desktop connections -monitor abnormal incoming RDP requests

Hunt Scenario Description

- Hunt for event ID 4624 for login type 10 and 4778.
- Investigate abnormal RDP connection to systems which are internet facing or which is "High Value Assets".
- Also perform reverse analysis on RDP connection by checking for rare account authenticated.

12. Threat Hunting Hypothesis

Endpoint detection and response or antivirus – Execution of binary from users APP Data directory

Hunt Scenario Description

Requires profiling of user's activity and add multiple filter condition to eliminate false positive.
Example – C:\Users*\AppData\Local\Temp*.exe

13. Threat Hunting Hypothesis

Endpoint detection and response or antivirus – process execution without parent process or services

Hunt Scenario Description

Svchost.exe launching without services.exe being its parent process

14. Threat Hunting Hypothesis

Endpoint detection and response or antivirus – scheduled jobs to perform known malicious behaviour

Hunt Scenario Description

Program jobs (at.exe) and hunt command line entries for adding or modifying registry keys, perform processes execution, fetch or send executable.

15. Threat Hunting Hypothesis

Endpoint detection and response or antivirus notification for executable on web or application server

Hunt Scenario Description

1. Once adversary is in your enterprise they establish and persists connection with command-and-control center.
2. It is advisable to create profile of executable at system level by excluding file extension: .jsp, .war, .asp, .aspx, .php, .cmf (or as custom as required)

16. Threat Hunting Hypothesis

Endpoint detection and response or antivirus – process execution from rare directory locations.

Hunt Scenario Description

Processes execution from rare path:

- %windows\fonts,
- %windows\help,
- %windows\wbem,
- %windows\addins,
- %windows\debut,
- %windows\system32\tasks

Familiar web shell filenames, adversaries running under a system directory (%WINDOWS%, %RECYCLER%) or other unusual locations (the web root).

Hunt in 4688 events with commands like net.exe, ipconfig.exe, whoami.exe, nbstats.exe