Malware

What is it

Malware alerts detect potentially malicious code on a host system. These alerts can be triggered based on indicators of compromise (IOC) such as a known bad file name or they can be triggered by the behavior of executed code.

Attacker Behavior

Attackers will craft malicious code the can be executed on a target system to achieve an objective. This code can be a standalone program or embedded in other legitimate software. Common malware types include: ransomware, keyloggers, botnet software, and credential sealers

Important Context

What is the affected system?

What malware variant was detected?

How was the malware detected (network signature or host signature)

Did anti-virus take an action?

Triage Runbook

	Do This	What to look for	Where to look	Takeaways
1	Identify what system the malware was reported on	Look for the systems primary operating system, it's owner, it's primary function, and if is has data classification or priority categorization.	Often the alert details will include the name of the system where the potential malware was found. Take this name and find additional details in the CMDB (asset inventory)	Understanding what a system is and how it is used, can help you determine the priority of a potential infection as well as what false positive scenarios could apply
2	Figure out what type of malware was reported	Often times, alerts will include details on what the malware may be trying to do.	Look in the alert details, or search logs for the anti virus (AV) system that reported the alert. You can often web search for additional context on the identified malware variant.	Understanding potential malware intent will help you decided if it's actually malicious or could have a valid purpose Malware detected by network signatures may not show up in AV logs
3	Figure out if an Anti-Virus action taken?	In many cases AV will try to take an action to prevent malware from running. Check AV logs to see if any AV actions such as a clean or quarantine were taken.	Look in anti-virus logs for the specified host. **NOTE**: Many organizations have multiple AV tools on systems. You need to check logs for them all because only one of these tools is likely to took an action.	Many organization don't take further action on malware blocked or cleaned by AV. Though these tools are imperfect. Always consult your Incident response plan for appropriate action.
4	Look if similar hosts are reporting similar alerts	It is very interesting to know if many other systems are reporting similar activity.	Search of the alert or malware signature in AV logs to see any other systems are reporting similar/same activity	Many systems reporting the same activity can indicate the alert is flagging legitimate software installed by IT, OR a wide spread infection. The former is

Cyber Alert Triage Runbook

	Do This	What to look for	Where to look	Takeaways
5	Check if the host has new or changed behavior.	Identify changes to the host data, configuration or new or changed network communications.	Identify any recent rare system events in the host event log. These logs are either collected centrally in a SIEM, can be search via an EDR tool, or need to be downloaded off the hosts log file	Most malwares will need to establish a communication channel to external attacker Command and Control infrastructure.

Common False Positive Scenarios

Anti-Virus identified blocked and cleaned a potential malware infection
Many organizations will consider this a false positive, since the remediation is complete. Consult your IR plan.

Legitimate IT software is flagged as malicious
IT organization sometimes add software that behave in similar ways to malware and can be flagged by AV tools.

Anti-Virus incorrectly flagged custom script files that is non-malicious
Custom scripts files are often non-signed by a trusted source which can cause AV to be more likely to flag as malicious.

Tools, such as remote desktop applications will be flagged as potential unwanted software
Attackers and system owners use tools that can have legitimate or malicious uses. These can be flagged even when used for a legitimate business purpose.

What to do next

If No Threat Found

- If malware was found but cleaned by AV, in might be useful to perform forensic analysis to confirm the malware is fully removed. Many malwares will try to hide and will be reloaded after being cleaned by scheduled task or from modified system registry keys.
- If the alert was a false positive, consider whitelisting the reported file to prevent future false positives. Be careful to not be too broad when whitelisting known good files, so you don't include unintended files

If Potential Threat Identified

FOLLOW YOUR IR PLAN
Some potential actions can include:

- Perform forensic analysis on to figure out how the malware arrived and what it did to the host.
- Isolate the host and eradicate the malware. Many times wiping the host is most effective.
- Capture and record IOCs (email addresses, domain names, etc.)
- Monitor the host system for reinfection