OFSA(OPSWAT FILE SECURITY ASSOCIATE) NOTES

COMMON MALWARE TERMS

HACKERS use specific types of malware for specific purposes, there are millions of malware programs in circulation they create or modify malware for specific circumstances

Virus
Keylogger
Worm
Trojan
Ransomware
Botnet
Spyware
RootKit
Malvertisement

Zero Day Threats
They are unknown software vulnerabilities , They are dangerous because victims cannot see them coming and are not created by hackers then the vulnerability is discovered and patched
Hacker targets include IP, Personally identifiable information PII , Financial data and to disrupt services
There are Wide variety of Hacker types with motivations varying that includes :
Black Hat , Blue hat, green hat , Red hat, script kiddies, Hacktivist and Whistleblowers

Analysis Techniques

Static analysis:

Av scanning is known as static analysis
Av definitions are called signatures
Traditional AV software is much like a dictionary of AV definitions
AV software must be regularly updated and properly configured
AV software houses definitions for malware samples , The use of AV definitions usually called signatures within the AV industry answer questions for malware without doing anything to potentially dangerous file This is known as static analysis allowing a quick inexpensive assessment.
But like dictionaries we have various dictionaries disagree or have discrepancies with word

definitions Av companies will often have their own discrepancies
When a real malware is missed because your AV vendor has a slightly different definition for a malware sample or not updated
Anti virus software is not entirely a set-it-and-forget-it software it must be updated

Heuristic Analysis:

An flaw with static analysis practices where hackers can bypass traditional signatures matching software by making slight alterations to their malware. In Today's circumstances of thousands of malware programs being released daily analysis and updates from AV companies to update their definitions is becoming less and less effective . Av companies introduced a technique known as heuristic analysis to aid detecting polymorphic malware designed to evade traditional signature-based detection systems
It works as decompiling the file or program and inspecting the source code it has its own database matching decompiled source code of known malware to look for matching elements
Heuristic scanning is not a infallible nor is perfect scanning a portion of composition of a file is observed for malware match, the risk of a false positive is significantly increased.

Dynamic analysis :

Modern cybersecurity tools like sandbox analysis allow us to detonate malware in much the same way Sample programs and files are loaded into isolated and secured virtual environments where malware can run, but not harm any outside system the malware sample is our landmine and sandbox our heavily armored fail this running malware in isolated environment is known as dynamic analysis
Sandboxing is a safe way to detonate and analyze the malware and it requires that each file must be scanned individually
But to not contaminate the results each file must be scanned on an individual basis which can be a bottleneck security systems when dealing with large quantities of files
Knowing when and under what circumstances to use a sandbox is paramount to making this a truly effective technology.

IN-Line Scanning and other methods

The best place to implement malware scanning solutions is to work directly in-line with processes A well deployed malware solution should only be noticed once a detection has been made and not hinder the systems it has been integrated with
It can be deployed at various layers of segmentation within an internal network
The types of malware techniques we deploy are heavily dependent on the type of data we expect and volume other techniques hand-off approach

Multi scanning - Combining with multiple AV engines may result in more precession

Vulnerability detection tools - CVE common vulnerabilities exposures or CVE list and all the vulnerabilities has a score based on industry standard called common vulnerability scoring system or CVSS it is scored on basis of exploit susceptibility and impact it would have done

Dynamic analysis - Sandboxing each activities is analyzed and monitored and finally scored the lower the score is the lower is the risk
if score for a file is 5% then it is clean
if it is 85% must be quarantined and in any case the confidence score and exam of observed activities can be used for forensic analysis threat assessment and other research

DLP - Data loss most data loss solutions focus on detecting and blocking mechanisms of financial or personally identifiable information If software identifies patterns that look like social security numbers credit cards and similar private information it suppresses sensitive information with automatic document redaction metadata removal or watermark addition

CDR- Content Disarm and Reconstruction employs a similar process To continue the analogy in cybersecurity it just eliminates the contaminants which are potential threat vector in files and then reconstructs all the remaining pieces back to safe and fully functional file we can even further go to deep CDR and its recursive approach
Only supported file types can be perform CDR

Importantly CDR & Deep CDR are not intended as detection tools It is OPSWAT solution to address any class of malware that we can consider an unknown threat its success is not measured by giving you detailed diagnostics of the contaminants left behind in the process

BIG Data Analysis - Analyzing the data and creating information through the data patterns and using as intelligence is important when taking action to protect the technologies.

In-Line Integration Techniques :

OOTB :
Out-of-the-box security solutions include preconfigured tools and appliances
Vendors provide strong technical partnerships with customers to provide seamless integrations

Standardized Protocols:
Protocols like http and smtp are two standardized protocols for web trafficking and email transfer like these in cyber security to offloads these cyber tasks we had ICAP (Internet content adaption protocol) which is again a standardized, lightweight protocol and evaluates network throughput and this protocol is seamless integration.

API
Application Programming interface is a programmatic interface that allows software systems to communicate with each other software systems

They only expose necessary information actions and specified parts of a system thus preventing exposure of interworking of software code from connecting systems
For many systems they have a list of available calls that can be requested security systems can use API to send and receive all kinds of information and can be used to integrate with other solutions built in house by programmatic connection

Webhook
In Dynamic analysis of sandbox solution that sends a retroactively a detection notification the information sends to additional security systems for an administrator notifications in form of webhook they send data over http and https trigger events
Web hooks are not only used as explicitly for retroactive actions and can easily be used as a real-time communication method they function as an excellent method to trigger reactive detection response event procedures.

PITFALLS :
Increased security can often come with cost of increased complexity and the more moving pieces there are the higher the likelihood of a potential failure it is imperative when any new solutions are introduced to a secure environments proper testing and validation is completed before moving to a production environment
High availability, scaling, and contingency plans are important when architecting a security solutions or stack
With proper analysis and planning we can run a secure environment with excellent uptime