OWPA(OPSWAT WEB TRAFFIC SECURITY PROTECTION ASSOCIATE) NOTES

Dangers of web traffic

Risks posed by internet connection even with modern cybersecurity where hackers go into many vectors to trick and making to do dangerous actions

Due to Iot devices growing in use and deployment businesses increasingly interact with and rely on the internet connections to support migration to cloud servers

Hackers create attack vectors to trick people into tracking dangerous actions that bypass secure systems

Vulnerabilities and the internet

Vulnerabilities are the primary threat vector that allows hackers to bypass and install malware

Users visiting websites are subjected to device fingerprinting and other sniffing tools that find vulnerabilities by checking installed application versions

Many users disable or put off important security updates creating an opportunity for hackers to exploit unpatched systems

known vulnerabilities CVE's and unknown vulnerabilities zero day vulnerabilities

Hackers trick users into visiting malicious websites through phishing attacks:
Malverstisements.
pharming efforts to make a user trick and visit fake pages.
DNS poisoning .

DNSSEC is a cryptographic based DNS system that protects against DNS poisoning

Drive by Download :

If a hacker successfully directs a user to their site and has sniffed out a vulnerability on the endpoint One of the most dangerous actions they can perform is the successful deployment of a drive by download in this scenario a vulnerability is taken advantage of to automatically download and install malicious code onto device

A common playload from drive by download comes from rootkits a rootkit primary purpose is to conceal itself or other forms of malware from operating system rootkit name derives from root-level access it takes over broad permissions to change files and settings

rootkits come in many forms a common method of achieving low-level access on a device is to disuse and install the rootkit as a driver on the device as system because drivers has access to kernel operations which resides below the antivirus actions on a device making the rootkit itself appear as if it is part of the OS

some rootkits can be installed on motherboards firmware or boot sector of a hard drive completely reformatting a device won't purge the infection.

Securing Web Traffic

Websites consist of many objects that can be analyzed for malware

Network scanning infrastructure like DLP data loss protection tools and real time malware scanning tech and static scans enhance network security

Running file downloads that could pose a threat through content disarm and reconstruction (CDR) ensures that they will be delivered to end users they will be delivered to end users in a known safe state

IP reputation

Ip reputation vendors

ip reputation source vendors examine and rate a website looking for common security threat flags such as botnet infections phishing attacks and other types of malware intrusions

websites scores are based on the availability of downloads file or code association with malicious internet objects current association with malicious internet objects current association with malicious internet objects hosting location and its presence on any allow/block list

This security practice that many enterprise network tools are taking advantage of the integration with established IP reputation source vendors is best for security needs

Ip reputation sources typically come from an original equipment manufacturer (OEM) integration tools already scanning internet traffic and if potentially malicious site is blocked to protect the end user in order to establish the databases necessary to associate IPs with potential threats websites are usually given a score that is based on a variety of factors derived by the IP reputation vendor

These include but are not limited to :
The availability of downloads files or code

Association with malicious internet objects
Hosting location
Presence on any allow/block lists

By integrating a service that automatically checks ip reputations we greatly increase our protection.

Endpoint internet best practices

Daily use : By operating our end systems daily with Non-admin User account or only user accounts or without a admin privileged account we can stop the impact of malware
System update : Longer the vulnerability in the system the longer is the risk
System cleaning : The more programs installed to our system the larger is the attack surface and more the potential vulnerabilities additionally
Downloading free tools in the internet can also include bundleware or opt-out inclusions
Read URL's : Read hyperlinks before clicking many hackers spoof hyperlinks to **legitimate sites** . A commonly seen tactic is to show hyperlink text actually navigates to an entirely different website
hovering a hyperlink before clicking many hackers however take a step ahead to fool people through an IDN homograph attack this is where a hacker creates a site that looks close to the intended targeted link at a quick glance like google.com
Examine Popups: Hackers mask dangerous hyperlinks in security notification popups taking users to malicious resources when clicked
verify popups with system security panel
Use Ad Blockers: Some popups are designed to populate the screen right as users take an action on another part of the website
Run an Ad Blocked to prevent popup attack

Integration Of Security

Proxy

Introducing secure process of our internet traffic with leveraging the proxies that facilitate many enterprise network operations To better understand there are two kinds of proxies that facilitate many enterprise network operations.

Forward proxy :

A forward proxy server sits in front of a client network and hides it from external servers if a client was to reach out to an internet hosted server the server wouldn't know any information about the client device connecting to it just the information of the proxy which is typically configured to secure against endpoint sniffing tools

Reverse proxy :

As the name suggests a reverse proxy server sits in front of a server network and hides it from external clients these are used to secure and hide web services which may run on multiple hosts from the clients connecting to them
some reverse proxies act as high availability and load balancing tools sending traffic to servers that have either more available bandwidth or are currently under lighter loads pure load balances don't allow for many of the security features that reverse proxies provide and therefore most load balancing today is done through reverse proxies.

Both forward and reverse proxies provide wide range of benefits :
Traffic scanning services
firewall features
data compression
off-loading ssl encryption known as ssl acceleration
caching - as long as the site data caching takes place after the network traffic security scans and cache retention time is less than our antimalware definition updates it can safely be used to quickly provide content to end users

```
Request->scan->cache
```