Pain Pyramid Explained

Tactics, techniques, and procedures (TTPs) [under the behavior tab]

Collection: This is about gathering valuable information or data from a computer system or network. It could be things like important documents, user details, system settings, or any data that hackers find useful.

Command and Control: This is when hackers set up secret communication lines between their computers and the ones they've hacked. It includes techniques such as using command-and-control (C2) servers, remote access tools (RATs), or communication protocols to send and receive commands.

Credential Access: This involves obtaining valid credentials, such as usernames and passwords, to gain unauthorized access to systems or accounts. Attackers may use various techniques like phishing, password spraying, credential dumping, or brute-force attacks to acquire credentials.

Discovery: This involves finding out more about the computer network they've hacked into. They look for things like how the network is set up, what software it's running, who the users are, and any weaknesses they can exploit. Attackers perform discovery to understand the target's infrastructure and identify potential attack vectors.

Defense Evasion: This category includes techniques used by attackers to avoid detection by security tools and evade security measures. Examples of defense evasion techniques include using obfuscation, encryption, anti-analysis techniques, and fileless malware to hide malicious activities and payloads from detection mechanisms.

Privilege Escalation: Privilege Escalation refers to the process of gaining higher levels of access or permissions than originally intended. Attackers may exploit vulnerabilities, misconfigurations, or weak security controls to escalate privileges from standard user accounts to administrative or root-level access, allowing them to carry out more extensive and damaging actions.

Execution: Execution involves the launching or execution of malicious code, scripts, or commands on a compromised system. Attackers use various techniques to execute malicious payloads, such as exploiting vulnerabilities, using social engineering tactics, injecting code into legitimate processes, or using malicious macros in documents.

Tools [in the Collection section under the Behavior tab]

Input Capture: This refers to techniques used by attackers to capture user input, such as keystrokes or mouse clicks. While it's not a standalone tool, it can be part of malware or malicious scripts designed to capture sensitive information.

Virtualization/Sandbox Evasion: This category includes techniques and tools used by attackers to detect and evade virtualized environments or sandboxes, which are isolated environments used for analyzing suspicious files or activities. Examples include detecting virtualized drivers or services and modifying behavior to avoid detection.

Network/host artifacts [in the Network Communication section under the Behavior tab]

HTTP Requests: These are requests sent over the Hypertext Transfer Protocol (HTTP), which is commonly used for web browsing. HTTP requests include actions such as fetching web pages, submitting forms, downloading files, and interacting with web services. Monitoring HTTP requests can help detect suspicious or malicious activities, such as accessing malicious websites, downloading malware, or sending sensitive data over unencrypted connections.

DNS Resolutions: DNS (Domain Name System) resolutions involve translating domain names (e.g., www.example.com) into IP addresses (e.g., 192.168.1.1) that computers can understand. DNS resolutions are crucial for accessing websites, services, and other resources on the internet. Monitoring DNS resolutions can reveal potentially malicious domain names, suspicious IP addresses, DNS hijacking attempts, or communication with known malicious domains.

IP Traffic: IP (Internet Protocol) traffic refers to the data packets exchanged between devices on a network. It includes all communication activities, such as sending/receiving emails, browsing websites, downloading files, and accessing network services. Analyzing IP traffic can uncover anomalies, unauthorized connections, suspicious data transfers, or indicators of compromise (IoCs) related to malware infections or malicious activities.

JA3 Digests: JA3 is a fingerprinting method used to identify SSL/TLS (Secure Sockets Layer/Transport Layer Security) client applications based on their specific SSL/TLS handshake parameters. JA3 digests represent unique identifiers derived from the cryptographic properties of SSL/TLS connections, including cipher suites, TLS versions, extensions, and other handshake details. Monitoring JA3 digests can help detect malicious SSL/TLS traffic, identify SSL/TLS-based attacks, or pinpoint unusual SSL/TLS configurations.

Memory Pattern Domains: Memory pattern domains refer to domain names extracted from memory artifacts during malware analysis or forensic investigations. Malware often uses domain names for command-and-control (C2) communication, data exfiltration, or downloading additional payloads. Identifying memory pattern domains can reveal C2 infrastructure, malicious domains, or communication channels used by malware.

Memory Pattern URLs: Similar to memory pattern domains, memory pattern URLs are URLs extracted from memory artifacts during malware analysis or forensic examinations. Malware may use URLs to fetch malicious files, download payloads, or interact with malicious websites. Analyzing memory pattern URLs can uncover malicious URLs, phishing links, compromised websites, or indicators of malicious activities.

Memory Pattern IPs: Memory pattern IPs are IP addresses extracted from memory artifacts during malware analysis or digital forensics. Malware may communicate with C2 servers, download payloads, or establish connections to malicious IP addresses. Monitoring memory pattern IPs can reveal malicious IP addresses, suspicious network connections, or indicators of network-based attacks.

Domain names [in the Contacted URLs section under the Relations tab]
org.misecure.com is reported as a malicious contacted domain.

Date (2024-03-12): This is the date when the URL was accessed or scanned.

Detections (10): This indicates that out of the 93 total scans conducted, 10 detections were made related to this URL. Detections typically refer to instances where security tools or services identified something suspicious or potentially malicious about the URL.

Total Scans (93): This represents the total number of times the URL was scanned or checked by security tools or services.

Status (-): The dash "-" in the status column suggests that the scanning or detection result is inconclusive or unavailable. It could mean that the URL's status or reputation is not definitively classified as either safe or malicious based on the available information.

URL (http://org.misecure.com/index.html): This is the specific URL that was accessed or scanned. It points to a web page named "index.html" hosted on the "org.misecure.com" domain.

IP addresses [in Contacted IP addresses section under the relations tab]
207.148.109.242 is listed as one of many IP addresses under the Relations tab in the VirusTotal report. This IP address is also associated with the org.misecure.com domain as listed in the DNS Resolutions section under the Behavior tab from the Zenbox sandbox report.Just click on **org.misecure.com** to see the associated IP address.

Hash values [Details tab in the Basic properties section of the virus report]
MD5 (Message Digest Algorithm 5):

- MD5 produces a 128-bit hash value often used to check file integrity, but it's considered weak for security due to possible collisions.

SHA-1 (Secure Hash Algorithm 1):

- SHA-1 creates a 160-bit hash value for data integrity verification, but it's also vulnerable to collision attacks.

SHA-256 (Secure Hash Algorithm 256-bit):
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

- SHA-256 generates a strong 256-bit hash for secure verification and is resistant to collision attacks, making it widely used in security.

Vhash:

- Vhash is a unique hash value used internally by VirusTotal to identify different file variants during analysis.

Authentihash:

- Authentihash is a hash value used by security tools like VirusTotal for file authentication and integrity verification.

Imphash (Import Hash):

- Imphash identifies malware variants based on their code imports, aiding in malware analysis and threat identification.