Introduction To Malware & Malware Analysis

It is essential to clarify that this module does not claim to be an all-encompassing or exhaustive program on Malware Analysis. This module provides a robust foundation for SOC analysts, enabling them to confidently tackle key Malware Analysis tasks. The primary focus of the module will be the analysis of malware targeting the Windows Operating System.

Malware Definition

`Malware`, short for malicious software, is a term encompassing various types of software designed to infiltrate, exploit, or damage computer systems, networks, and data.

Although all malware is utilized for malicious intents, the specific objectives of malware can vary among different threat actors. These objectives commonly fall into several categories:

- `Disrupting host system operations`
- `Stealing critical information, including personal and financial data`
- `Gaining unauthorized access to systems`
- `Conducting espionage activities`
- `Sending spam messages`
- `Utilizing the victim's system for Distributed Denial of Service (DDoS) attacks`
- `Implementing ransomware to lock up victim's files on their host and demanding ransom`

Malware Types

In today's fast-paced world of cyber threats, we find ourselves up against a broad spectrum of complex and varied malware forms, which pose a relentless challenge to our cyber defenses. It's paramount for us to grasp the multifaceted nature of malicious software as we endeavor to bolster the security of our systems and networks. Let's peel back the layers of some commonly seen types of malware that we frequently grapple with in our cybersecurity endeavors.

- `Viruses`: These notorious forms of malware are designed to infiltrate and multiply within host files, transitioning from one system to another. They latch onto credible programs, springing into action when the infected files are triggered. Their destructive powers can range from corrupting or altering data to disrupting system functions, and even spreading through networks, inflicting widespread havoc.
- `Worms`: Worms are autonomous malware capable of multiplying across networks without needing human intervention. They exploit network weaknesses to infiltrate systems without permission. Once inside, they can either deliver damaging payloads or keep multiplying to other vulnerable devices. Worms can initiate swift and escalating infections, resulting in enormous disruption and even potential denial of service attacks.
- `Trojans`: Also known as Trojan Horses, these are disguised as genuine software to trick users into running them. Upon entering a system, they craft backdoors, allowing attackers to gain unauthorized control remotely. Trojans can be weaponized to pilfer sensitive data, such as passwords or financial information, and orchestrate other harmful activities on the compromised system.
- `Ransomware`: This malicious type of malware encrypts files on the target's system, making them unreachable. Attackers then demand a ransom in return for the decryption key, effectively holding the victim's data to ransom. The impacts of ransomware attacks can debilitate organizations and individuals alike, leading to severe financial and reputational harm.

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

- `Spyware`: This type of malware stealthily gathers sensitive data and user activities without their consent. It can track online browsing habits, record keystrokes, and capture login credentials, posing a severe risk to privacy and security. The pilfered data is often sent to remote servers for harmful purposes.
- `Adware`: Though not as destructive, adware can still be an annoyance and a security threat. It shows uninvited and invasive advertisements on infected systems, often resulting in a poor user experience. Adware may also track user behavior and collect data for targeted advertising.
- `Botnets`: These are networks of compromised devices, often referred to as bots or zombies, controlled by a central command-and-control (C2) server. Botnets can be exploited for a variety of harmful activities, including launching DDoS attacks, spreading spam, or disseminating other malware.
- `Rootkits`: These are stealthy forms of malware designed to gain unauthorized access and control over the fundamental components (the "root") of an operating system. They alter system functions to conceal their presence, making them extremely challenging to spot and eliminate. Attackers can utilize rootkits to maintain prolonged access and dodge security protocols.
- `Backdoors/RATs (Remote Access Trojans)`: Backdoors and RATs are crafted to offer unauthorized access and control over compromised systems from remote locations. Attackers can leverage them to retain prolonged control, extract data, or instigate additional attacks.
- `Droppers`: These are a kind of malware used to transport and install extra malicious payloads onto infected systems. They serve as a conduit for other malware, ensuring the covert installation and execution of more sophisticated threats.
- `Information Stealers`: These are tailored to target and extract sensitive data, like login credentials, personal information, or intellectual property, for harmful purposes. This includes identity theft or selling the data on the dark web.

These examples barely scratch the surface of the types of malware we confront in today's threat landscape. It's essential to remember that cybercriminals consistently refine their strategies, techniques, and malware variants to avoid detection and exploit new vulnerabilities.

Malware Samples

When it comes to enhancing our cybersecurity defenses and understanding the threats that exist, sometimes we have to dive into the dark corners of the cyber world. This means getting our hands on actual malware samples, be it for research, analysis, or educational purposes. However, it's crucial to emphasize that dealing with real malware samples should be done in a safe and controlled environment to prevent accidental infections and potential harm. Here are some resources, both free and paid, where we can find such samples.

- VirusShare: An excellent resource for malware researchers, VirusShare houses a vast collection of malware samples. They currently have over 30 million samples in their repository, all of which are freely available to the public.
- Hybrid Analysis: This website allows us to submit files for malware analysis. However, they also have a public feed of their analyses, where malware samples are often shared.
- TheZoo: A GitHub repository that contains a collection of live malware for analysis and education. The repository also contains additional information about each sample, such as its family and the type of activities it performs.
- Malware-Traffic-Analysis.net: This website provides traffic analysis exercises that can be extremely beneficial for people trying to learn about malware traffic patterns. They often provide pcap files of actual malware traffic, which can be quite informative.
- VirusTotal: VirusTotal inspects items with over 70 antivirus scanners and URL/domain blocklisting services, in addition to a myriad of tools to extract signals from the studied content. Any user can select a file from their computer using their browser and send it to VirusTotal. VirusTotal offers a number of file submission methods, including the primary public web interface, desktop uploaders, browser extensions and a programmatic

API.

- ANY.RUN: An interactive online sandbox for malware analysis. The service allows researchers to analyze malware behavior by running samples in a controlled environment. While it offers both free and paid tiers, even the free version provides access to public submissions, which can include various malware samples.
- Contagio Malware Dump: Contagio Dump is a collection of malware samples, threat reports, and related resources curated by a malware researcher named Mila. The site provides direct, anonymized access to an extensive range of malware samples, including various types of trojans, worms, ransomware, and exploits. It's frequently used by security researchers and analysts to study malware behavior and develop mitigation techniques.
- VX Underground: VX-Underground is one of the largest collections of malware source code, articles, and papers on the internet. It aims to collect, preserve, and share all kinds of materials related to malware, exploit, and hacking culture. This resource is valuable to security researchers and enthusiasts who want to study malware construction and behavior from a more technical and code-centric perspective.

Malware/Evidence Acquisition

When it comes to gathering evidence during a digital forensics investigation or incident response, having the right tools to perform disk imaging and memory acquisition is crucial. Let's discuss some free solutions we can use to collect the necessary data for our investigations.

Disk Imaging Solutions

- FTK Imager: Developed by AccessData (now acquired by Exterro), FTK Imager is one of the most widely used disk imaging tools in the cybersecurity field. It allows us to create perfect copies (or images) of computer disks for analysis, preserving the integrity of the evidence. It also lets us view and analyze the contents of data storage devices without altering the data.
- OSFClone: A free, open-source utility designed for the task of creating and cloning forensic disk images. It's easy to use and supports a wide variety of file systems.
- DD and DCFLDD: Both are command-line utilities available on Unix-based systems (including Linux and MacOS). DD is a versatile tool included in most Unix-based systems by default, while DCFLDD is an enhanced version of DD with features specifically useful for forensics, such as hashing.

Memory Acquisition Solutions

- DumpIt: A simplistic utility that generates a physical memory dump of Windows and Linux machines. On Windows, it concatenates 32-bit and 64-bit system physical memory into a single output file, making it extremely easy to use.
- MemDump: MemDump is a free, straightforward command-line utility that enables us to capture the contents of a system's RAM. It’s quite beneficial in forensics investigations or when analyzing a system for malicious activity. Its simplicity and ease of use make it a popular choice for memory acquisition.
- Belkasoft RAM Capturer: This is another powerful tool we can use for memory acquisition, provided free of charge by Belkasoft. It can capture the RAM of a running Windows computer, even if there's active anti-debugging or anti-dumping protection. This makes it a highly effective tool for extracting as much data as possible during a live forensics investigation.
- Magnet RAM Capture: Developed by Magnet Forensics, this tool provides a free and simple way to capture the volatile memory of a system.
- LiME (Linux Memory Extractor): LiME is a Loadable Kernel Module (LKM) which allows the acquisition of volatile memory. LiME is unique in that it's designed to be transparent to the target system, evading many common anti-forensic measures.

Other Evidence Acquisition Solutions

- KAPE (Kroll Artifact Parser and Extractor): KAPE is a triage program designed to help in collecting and parsing artifacts in a quick and effective manner. It focuses on targeted collection, reducing the volume of collected data and the time required for analysis. KAPE is free for use and is an essential tool in our digital forensics toolkit.
- Velociraptor: Velociraptor is a versatile tool designed for host-based incident response and digital forensics. It allows for quick, targeted data collection across a wide number of machines. Velociraptor employs Velocidex Query Language (VQL), a powerful tool to collect and manipulate artifacts. The open-source nature of Velociraptor makes it a valuable free tool in our arsenal.

Malware Analysis Definition, Purpose, & Common Activities

The process of comprehending the behavior and inner workings of malware is known as `Malware Analysis`, a crucial aspect of cybersecurity that aids in understanding the threat posed by malicious software and devising effective countermeasures.

In our pursuit of Malware Analysis, we delve into the malware's code, structure, and functionality to gain profound insights into its purpose, propagation methods, and potential impact on targeted systems. By answering pertinent questions, such as the type of malware (e.g., spybot, keylogger, ransomware), its intended behavior on endpoints, the aftermath of its execution (including generated artifacts on the network or endpoint and possible connections to Command and Control (C2) servers), the extent of damage it can inflict, its attribution to specific threat groups, and crafting detection rules based on the analysis to detect the malware across the entire network, we can devise robust defense mechanisms against these threats.

Malware analysis serves several pivotal `purposes`, such as:

- `Detection and Classification`: Through analyzing malware, we can identify and categorize different types of threats based on their unique characteristics, signatures, or patterns. This enables us to develop detection rules and empowers security professionals to gain a comprehensive understanding of the nature of the malware they encounter.
- `Reverse Engineering`: Malware analysis often involves the intricate process of reverse engineering the malware's code to discern its underlying operations and employed techniques. This can unveil concealed functionalities, encryption methods, details about the command-and-control infrastructure, and techniques used for obfuscation and evasion.
- `Behavioral Analysis`: By meticulously studying the behavior of malware during execution, we gain insights into its actions, such as modifications to the file system, network communications, changes to the system registry, and attempts to exploit vulnerabilities. This analysis provides invaluable information about the impact of the malware on infected systems and assists in devising potential countermeasures.
- `Threat Intelligence`: Through malware analysis, threat researchers can amass critical intelligence about attackers, their tactics, techniques, and procedures (TTPs), and the malware's origins. This valuable intelligence can be shared with the wider security community to enhance detection, prevention, and response capabilities.

The `techniques` employed in malware analysis encompass a wide array of methods and tools, including:

- `Static Analysis`: This approach involves scrutinizing the malware's code without executing it, examining the file structure, identifying strings, searching for known signatures, and studying metadata to gain preliminary insights into the malware's characteristics.
- `Dynamic Analysis`: Dynamic analysis entails executing the malware within a controlled environment, such as a sandbox or virtual machine, to observe its behavior and capture its runtime activities. This includes monitoring network traffic, system calls, file system modifications, and other interactions.

- `Code Analysis`: Code analysis (includes reverse engineering) and involves disassembling or decompiling the malware's code to understand its logic, functions, algorithms, and employed techniques. This helps in identifying concealed functionalities, exploitation methods, encryption methods, details about the command-and-control infrastructure, and techniques used for obfuscation and evasion. Inferentially, code analysis can also help in uncovering potential Indicators of Compromise (IOCs).
- `Memory Analysis`: Analyzing the malware's interactions with system memory helps in identifying injected code, hooks, or other runtime manipulations. This can be instrumental in detecting rootkits, analyzing anti-analysis techniques, or identifying malicious payloads.
- `Malware Unpacking`: This technique refers to the process of extracting and isolating the hidden malicious code within a piece of malware that uses packing techniques to evade detection. Packers are used by malware authors to compress, encrypt, or obfuscate their malicious code, making it harder for antivirus software and other security tools to identify the threat. Unpacking involves reverse-engineering these packing techniques to reveal the original, unobfuscated code for further analysis. This can allow researchers to understand the malware's functionality, behavior, and potential impact.

In today's ever-evolving threat landscape, the usage of malware analysis plays a pivotal role in our cybersecurity defense strategies. As cyber threats become increasingly sophisticated, we must continually enhance our capabilities to identify, analyze, and mitigate the risks posed by malicious software.

Through malware analysis, we gain invaluable insights into the nature of the threats we face. Understanding the malware's specific attributes allows us to tailor our response tactics accordingly, addressing each threat with precision.