Identifying and Removing Malicious Artifacts

There are a number of different actions we can take when working to identify and remove malicious artifacts, but alternatively, there are some easy 'quick wins' to completely remediate the incident or infection immediately. In this lesson we will cover the following:

- **What are malicious artifacts?**
- **Identifying artifacts.**
- **Removing artifacts.**

WHAT ARE MALICIOUS ARTIFACTS?

The term 'malicious artifact' is used to describe some object with malicious purposes, such as a piece of malicious software (malware) that is installed on a system, a running process, a scheduled task, a registry entry, a text file generated by a keylogger, etc. We need to ensure that we remove all malicious artifacts during the incident response process, because if we miss something, the attackers may still have some degree of control over the system. If they're using a backdoor to allow for remote access and we miss it, even if the system is patched and hardened, they have a direct route in.

IDENTIFYING ARTIFACTS

This is often a case of experience in dealing with incidents, being able to identify what items should and shouldn't be on a system. However, there are some places we can look to see if anything looks suspicious, such as active network connections, user accounts, file downloads, running processes, scheduled tasks, and registry entries.

There are some manual checks we can conduct to try and identify suspicious activity, allowing us to find and remove artifacts. Some examples include:

- Check for suspicious or unknown processes running in the system. For Windows systems, Sysinternals Process Explorer is a very powerful task manager that can show processes that try to mask themselves as ordinary system processes.
- To determine the source of suspicious network connections, the netstat utility and Sysinternals' Process Monitor are an excellent combination to help track down malware that is attempting to "call home" or attempting to spread.
- Another tool from Sysinternals, the Rootkit Revealer, is very useful in detecting Rootkits or malware that uses advanced techniques in order to mask its presence on a system.

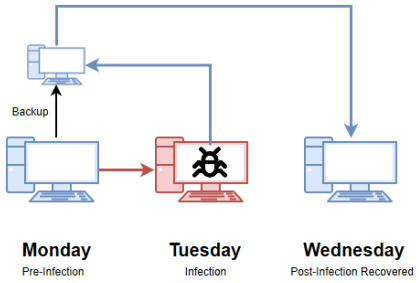
REMOVING ARTIFACTS

Below are different methods we can use to remove malicious artifacts that we have identified during the incident response process

response process.

Reimaging Affected Systems

One of the easiest ways to completely recover a system from any kind of infection is to reimage it from a backup. In the below diagram, we've demonstrated how incident responders can remove **all** malicious artifacts in one go, ensuring the system is completely clean, provided there is a backup before the infection occurs. The downside with this method is that all data after the pre-infection backup was taken will be lost.



Anti-Malware Solutions

We can scan affected systems with a high-grade Antivirus solution, preferably a Next-Generation Antivirus solution, to ensure that malicious artifacts are identified and removed from the system. This may not always be a good solution, in the event of a malware infection, if the antivirus didn't detect the malware to start with it may struggle to find associated malicious artifacts. Next-Generation AV might be more useful here, as it doesn't take the same approach of traditional antivirus methods that are often beaten by knowledgeable attackers, but what's the difference? It goes beyond known file-based malware signatures and heuristics and can utilize predictive analytics powered by machine learning and artificial intelligence to detect file-less malware that hides in memory, and respond to new threats that would normally go undetected. In all cases we should ensure the endpoint solution is enabled, properly configured, and has the latest updates and signatures to increase the chance of successful detection. In the case of an advanced malware infection, it is likely better to proceed with the re-imaging method of removing artifacts.

Bootable Tools

Some antimalware vendors offer tools or versions of their products that don't require installation and can be run from a CD or USB drive in order to prevent them from being affected by malware residing on the system. For example:

- McAfee provides the stand-alone Stinger Malware removal tool and Microsoft has the Malicious Software Removal Tool, for detecting and removing specific malware.
- Avira offers the "Avira Rescue System", designed to be booted and run from a CD or USB drive.

Previous Topic
Mark Complete
Next Topic
Back to Lesson