BLACK CELL
Protecting critical infrastructures

Overview of Freeze payload creation tool

Overview of Freeze payload creation tool

Freeze is a powerful tool that enables the creation of payloads, which can circumvent EDR security controls and execute shellcode in a stealthy manner. Freeze deploys various techniques to eliminate Userland EDR hooks and execute shellcode in a way that avoids detection by other endpoint monitoring controls.

It's no secret that EDR hooking is a crucial aspect of an adversary's ability to successfully compromise an endpoint security system. Freeze uses a technique to first create a process and then move it into the background. This approach helps keep the process hidden and prevents it from being detected by any EDR product.

Hooking is a method of altering the behaviour of an application to enable EDR tools to monitor the execution flow in a process, gather information for behaviour-based analytics, and detect suspicious and malicious activity. This capability enables more accurate detection rates of post-initial compromise techniques (such as code execution) as well as post-exploitation techniques (such as privilege escalation, lateral movement, or ransomware activity).

To sum up, on Windows, the first DLL that loads is Ntdll.dll. The other DLLs come later, but there is a small delay before the EDR can load and start hooking. Thus, creating a process in a suspended state ensures that no other DLLs are loaded (except for Ntdll.dll), meaning that the syscalls located in Ntdll.dll remain unmodified.

Defending against Freeze and its multiple techniques is not as easy as it may seem at first. Endpoint controls like EDRs may be able to detect that a process is in a suspended state, but suspended processes on their own are common on Windows hosts and are not always reliable indicators of an attack.

One solution to detect concealed processes is anti-malware detection logic. These concealed process detection rules are available in antivirus products or EDR solutions. If you use an SIEM (such as Splunk Enterprise, IBM QRadar or Microsoft Sentinel, all available in Black Cell’s portfolio), you can create alert rules for Freeze and its hidden processes. Since Freeze can generate both .exe and .dll files, it's useful to extend monitoring to both.

It's essential to remember that, from an endpoint security perspective, it's crucial not to focus on a single technique. Instead, the focus should be on the bigger picture of all the different events in the sequence. Adversaries have numerous different ways of circumventing these protections to establish an initial foothold, and focusing solely on

detecting evasion-based or initial foothold techniques creates a narrow focus, resulting in potential detection blind spots.

Sources: [date of access: 15.02.2023]

Optiv (https://www.optiv.com/insights/source-zero/blog/sacrificing-suspended-processes)

Github (https://github.com/optiv/Freeze)

BlackHatEthicalHacking (https://www.blackhatethicalhacking.com/tools/freeze/)