1. List the malware’s significant imports and strings, and its host-based andnetwork-based indicators.

Significant strings:

* \system32\wupdmgrd.exe
* \winup.exe
* <http://www.cmt118cmt118cmt118cmt118.com/updater.exe>
* GetWindowsDirectoryA
* URLDownloadToFileA

Significant imports:

* MSVCRT.dll
* KERNEL32.dll
* urlmon.dll

Host-Based indicator:

* \system32\wupdmgrd.exe
* \winup.exe

Network-Based indicator:

* http://www.cmt118cmt118cmt118cmt118.com/updater.exe

1. Describe how the malware works

The malware serves a malicious purpose on the system. It operates as a downloader which is allowing the attacker to retrieve additional payloads or updates from remote servers. The hardcoded URL “http://www.cmt118cmt118cmt118cmt118.com/update” establishes communication with specific servers, enabling the attacker to modify or extend the malware’s functionalities remotely.

Furthermore, the presence of strings like “\winup.exe” and “\system32\wupdmgrd.exe” suggests that the malware exhibits characteristics of a payload dropper. They indicate an intent to drop and execute malicious files on the system, which is potentially going to enhance the malware’s abilities for a greater attack.

1. Describe the purpose the malware tries to achieve.

The malware's primary purpose is to clandestinely gather comprehensive information about the infected system. By operating as a downloader, it establishes communication with specific servers through the hardcoded URL.

After executing its malicious tasks, the malware exhibits a self-destructive behavior, deleting itself from the system. This meticulous act aims to erase any traces of its presence, further evading detection and forensic analysis.

Downloads info from the local pc and sends it towards something and then deletes itself.