Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:37:42 UTC

Description(Kaspersky) So what does PlusDLL control? It turns out that the target functionality is implemented in different files. Each file provides a specific remote control feature and is downloaded from the attackers' server every time the system starts up. These files are not saved on disk or in the registry but are loaded directly into the memory.

At the very start of the operation, after launching the driver, PlusDLL collects information about the infected system. A unique identifier for the infected computer is generated based on information about the hard drive and the network adapter's MAC address, e.g., TKVFP-XZTTL-KXFWH-RBJLF-FXWJR. The attackers are interested primarily in the computer's name, the program which loaded the malicious library, as well as information about remote desktop sessions (session name, client name, user name and session time). All of this data is collected in a buffer, which is then compressed and sent to the attackers' control center.

In reply to this initial message from the bot, the control center sends the list of available plugins. Plugins are DLL libraries that provide specific remote control functions. Upon receiving the list of plugins, the bot downloads them, allocates them in the memory and passes control to these libraries.

Also see HighNoon, which seems to be a variant of Winnti.
