Incident Report: DFIR - BumbleBee Round 2

Summary:

This report details a BumbleBee malware intrusion that occurred in May 2022, as documented by the DFIR Report. BumbleBee was used as the initial access vector, and the threat actors employed various tactics, techniques, and procedures (TTPs) to perform reconnaissance, establish persistence, and move laterally within the compromised network.

Attack Details:

The attack began with the execution of BumbleBee malware on the initial compromised system (referred to as the "Beach Head") through a shortcut modification technique. The malware was executed using rundll32.exe, which then used a Windows Management Instrumentation (WMI) call to perform process injection.

From 12:19 UTC to 12:27 UTC, the attackers used a Meterpreter shell to execute commands on the compromised system. Between 12:28 UTC and 12:57 UTC, the attackers performed discovery activities using the Meterpreter sessions, including network share discovery, domain account enumeration, and domain trust discovery.

At 18:26 UTC, a Cobalt Strike beacon was executed on the Beach Head system, initiating further reconnaissance. The attackers used application layer protocols to perform account discovery and then dumped credentials from the LSASS memory using procdump at 18:31 UTC.

Using the stolen credentials, the attackers moved laterally to a server at 18:53 UTC via RDP and installed AnyDesk for remote access. At 19:00 UTC, they created a new domain user account on the server for persistence. The attackers then used AdFind to perform system network configuration discovery at 19:09 UTC and browsed files using AnyDesk at 19:13 UTC.

At 19:17 UTC, the attackers moved laterally to a backup server using RDP. Finally, at 00:14 UTC the following day, they executed a batch script on the backup server for system reconnaissance.