UID: U01155118

Equation Group (G0020) - MITRE ATT&CK

Equation Group is an advanced and sophisticated threat actor often described as one of the most technically capable cyber espionage groups known till date. As per the Kaspersky Lab, the group has been active since at least 2001 with more than 60 actors. Public research, such as those from Symantec, Kaspersky Lab has noted their use of firmware-level malware that can override firmware data on hard drives, control PLCs, and is capable of physically destroying hardware itself.

Techniques Used (as per MITRE ATT&CK)

- Pre-OS Boot (T1542)

  As per Kaspersky Lab, the group is known to have the capability to overwrite the firmware on hard drives from some manufacturers. This leads their malware to persist on a very low level that most likely evades any detection.
- Execution Guardrails (T1480)

  The group has been observed utilizing environmental keying in payload delivery. This ensured execution occurs only on target systems, which led to complicated analysis and research done by many defenders and researchers.
- Hide Artifacts (T1564)

  Use of encrypted virtual file systems stored in the Windows Registry has many times been reported to be used by the group. This makes the threat data unrecognizable and unreadable for analysts to figure out more about the threat and its operating processes.
- Peripheral Device Discovery (T1120)

  Use of tools with the functionality to search for specific information about the attached hard drive that could be used to identify and overwrite the firmware, has been done by the group. Also, searching and identifying PLC units and their peripherals has been specifically implemented as tailored payload to target specific hardwares. The threat overall allowed to map environments and also led for lateral movement by spreading even into isolated systems.

Even though there is almost no information on *Initial Access* and *Command & Control* techniques for the group on MITRE ATT&CK, many sources indicate that the initial access is done mostly via USBs and commanding & controlling is done by recognizing the specifically targeted system with predefined parameters, automated routines but not limited to internet access whenever possible. For persistence, use and modification of hard drive’s firmware and residing along with it, have been reported to be done by the group. This level of sophistication and their in-depth technical capabilities has made the group wear the crown of *the most sophisticated cyber espionage group.*

References:

- Equation, Group G0020 | MITRE ATT&CK®
- Equation Group - Wikipedia