Equation Group | Stuxnet Campaign

Equation Group (G0020), believed to be a partnership group formed by Israeli and the US government, is often described as one of the most advanced cyber espionage groups ever discovered. Even though the MITRE ATT&CK framework does not explicitly list Stuxnet under Equation Group, extensive research by security firms (Kaspersky and Symantec) strongly suggests that Equation Group was directly involved in its development or operation. Stuxnet is considered the world's first digital weapon that causes physical destruction besides spying.

Stuxnet – The Campaign

Stuxnet (S0603) is a very sophisticated program that was believed to have utilized multiple programming languages, frameworks and approaches to target Iran's Natanz uranium enrichment facility. Its mission was to sabotage centrifuges used to refine uranium. Stuxnet would first record the machinery data for up to 30 days, and during actual attack, it would replay those logs just like in sci-fi movies, avoiding detection and causing delays for the experts to figure out the actual cause and effect of what's going on.

Tools, Techniques, and Procedures (TTPs)

- **Initial Access and Propagation**
  Stuxnet spread into isolated (air-gapped) environments via infected USB devices while using four separate Windows zero-day vulnerabilities. It is worth mentioning that finding out even a single zero-day vulnerability is considered a very good luck/finding.
- **Execution and Defense Evasion**
  It has been reported to have used stolen yet legitimate digital driver certificates from Realtek and JMicron vendors. This made itself a trustworthy program in Windows environment.
  Also, with the use of encryption and virtual file system, Stuxnet concealed its malicious files and processes, evading antivirus detection.
- **Persistence**
  Installing itself as kernel/firmware-level drivers and reloading even after system reboots was the key approach to persist in the system. This allowed itself to maintain presence across infected machines.
- **Impact**
  The primary target of the Stuxnet was Simens Step 7 PLCs that were used in the target facility. Findings by Kaspersky Lab suggests that the code consisted of string variable that hold value like Stuxnet, WCC, Step 7, etc that led to identification of the intentions of the Stuxnet.
  The sole purpose of it being to destroy physical centrifuges, Stuxnet injected malicious logic into PLCs causing centrifuges to spin too fast or too slow. The irony of the situation is that the defenders of the facility had wrong reading in

their system log as it would replay stale spoofed logs to hide its concurrent attacks.

Outcomes

Approximately 1,000 centrifuges at Natanz were damaged, setting back Iran's nuclear program by months or even years. It demonstrated that cyber operations could leap from the digital to the physical world. Stuxnet indeed changed the digital security perception globally, leading many nations and similar groups to advance both the offensive and defensive cyber capabilities.

While MITRE ATT&CK only records a handful of Equation Group techniques (firmware implants, environmental keying, peripheral device discovery), several explicit research leads Equation Group's tools and infrastructure to the same factors that produced Stuxnet. The technical similarities, sophistication levels, code similarities, and operational behavior support the correlation of Stuxnet to the Equation Group.

References

- Equation Group - Wikipedia
- Stuxnet - Wikipedia
- The World's First Cyber Weapon Attack on a Nuclear Plant | Vice News