Black Lotus Labs Analysis leads to Detection of New Remote Access Trojan

Michelle Lee
Senior Data Scientist
Lumen Technologies

Lumen's Black Lotus Labs detected a new remote access trojan we're calling ReverseRat. Based on our global telemetry and analysis, we identified that the actor is targeting government and energy organizations in the South and Central Asia regions with operational infrastructure hosted in Pakistan. ReverseRat was deployed in parallel with an open-source RAT called AllaKore to infect machines and achieve persistence. Given the critical nature of the sectors the actor is targeting, we advise security practitioners to learn the actor's current tactics, tools and procedures to better defend their organizations against potential attacks.

The ReverseRat infection chain is noteworthy because of the steps it takes to avoid detection and the critical nature of the targeted entities. The evasion techniques include:

- Use of compromised domains in the same country as the targeted entity to host their malicious files
- Highly targeted victim selection after the initial compromise
- Repurposed open-source code
- In-memory component used during initial access
- Modification of registry keys to covertly maintain persistence on the target device

Based upon Black Lotus Labs and MalBeacon telemetry, we assess that threat actor is very likely operating out of Pakistan. We observed a multi-step infection chain that resulted in the victim downloading two agents; one resided in-memory, while the second was side-loaded, granting threat actor persistence on the infected workstations. The technique documented in the image below was active beginning at least in March 2021 and bi-directional communications with the C2 are, in some instances, still ongoing.