Iranian APT group 'MuddyWater' Adds Exploits to Their Arsenal – ClearSky Cyber Security

Published: 2019-06-06 · Archived: 2026-05-01 03:08:29 UTC

In recent months, there has been considerable unrest in the Iranian cybersphere. Highly sensitive data about Iranian APT groups were leaked, exposing abilities, strategies, and attack tools. The main medium for this leak was a telegram channel.

The first leak uncovered attack frameworks and web shells of APT-34 (Known as OilRig group). This was followed by another leak that that exposed previously unknown details (such as compromised C2 servers) regarding the operation of MuddyWater. Further, it detailed the modus operandi of RANA – a cyber division of the Iranian Ministry of Intelligence (MOIS).

However, Clearsky's Threat Intelligence team investigation indicates that MuddyWater's activities were unaffected. This report will reveal the group's latest exploit usage and TTPs.

Read the full report: Iranian APT group 'MuddyWater' Adds Exploits to Their Arsenal

Clearsky has detected a new and advanced attack vector used by MuddyWater to target governmental entities and the telecommunication sector. Notably, the TTP includes decoy documents exploiting CVE-2017-0199 as the first stage of the attack. This is followed by the second stage of the attack – communication with the hacked C2 servers and downloading a file infected with the macros.

Malicious document propagated by MuddyWater impersonating the Iraqi government

MuddyWater (aka SeedWorm/Temp.Zagros) is a high-profile Advanced Persistent Threat (APT) actor sponsored by Iran. The group was first observed in 2017, and since has operated multiple global espionage campaigns. With that in mind, their most significant operations mainly focus on Middle Eastern and Middle Asian nations.

The group targets a wide gamut of sectors, including governmental, military, telecommunication, and academia. In the past months, Clearsky had monitored and detected malicious files of each one of these TTPs – decoy Microsoft software with embedded Macros; and documents exploiting vulnerability CVE-2017-0199. **This is the first time MuddyWater has used these two vectors in conjunction**.

By analyzing the Rana documents, it appears that the MOIS attack teams are divided into two branches, each with different purposes.

The first is the espionage team that specializes in hacking systems, while the other is the social engineering team that compromises assets via social engineering and spear-phishing methods. Clearsky assessment is that MuddyWater is likely the latter group.

Indicators of compromise are available for subscribers of the ClearSky threat intelligence service in MISP event 1583.
