‘MuddyWater’ spies suspected in attacks against Middle East governments, telecoms

By Sean Lyngaas

Published: 2020-10-21 · Archived: 2026-04-05 22:49:31 UTC

One of the most prolific cyber-espionage groups linked to Iran has used old tricks — and perhaps a new hacking tool — in dozens of attempts to breach government and telecommunications operators in the Middle East in recent months, security researchers said Wednesday.

The hacking attempts have hit organizations in Iraq, Kuwait, Turkey and the United Arab Emirates, according to researchers at security provider Symantec. Iran has strategic interests in all of those countries. And the attackers appear to be trying to smuggle key data from the organizations they managed to breach.

It’s a reminder that while other hacking teams associated with Tehran have gained notoriety for disruptive, data-wiping attacks against Middle East organizations, the group known as MuddyWater, or Seedworm, is better known for its relentless spying efforts.

“These actors are extremely focused in what they’re doing,” said Vikram Thakur, technical director at Symantec, a division of semiconductor and software maker Broadcom. “They’re not using zero days. They’re just looking for commonly available methods along with their custom malware to get into these environments, exfiltrate whatever they want and then move on.”

Researchers from Symantec and other security companies are investigating a new hacking tool they suspect MuddyWater has been using in the compromises. Known as PowGoop, the malicious code can install other programs capable of siphoning data off of networks.

“It could be a subgroup within [MuddyWater] which has been tasked differently” from the rest of the group, Thakur said of the PowGoop tool.

While Symantec said it had “medium confidence” that MuddyWater was behind PowGoop, there were other signs that the group has been developing new tools.

“MuddyWater has been very active in the last year, both in its prolific operations and constant development of tools,” said Saher Naumaan, senior threat intelligence analyst at BAE Systems. “One significant evolution is the group’s advancements in malware, which over the years has shifted away from solely scripting-based tooling, such as PowerShell, to .NET and now to custom C++ payloads, as seen with Backdoor.Mori,” added Naumaan, who closely tracks hackers associated with Iran.

MuddyWater’s recent activity is in keeping with its reputation for prolific hacking campaigns. From September to December 2018, for example, the group compromised 131 victims in 30 organizations all over the map, from Russia to Saudi Arabia to North America, Symantec said in previous research.

MuddyWater has so far avoided the extra scrutiny that comes from public U.S. indictments. It was not among the alleged Iranian hackers who were indicted last month by U.S. grand juries. And while security companies continue to expose MuddyWater's tools, the group shows no signs of letting up.
