Iran's MuddyWater Hacker Group Using New Malware in Worldwide Cyber Attacks

By The Hacker News

Published: 2022-02-25 · Archived: 2026-04-05 12:54:39 UTC

Cybersecurity agencies from the U.K. and the U.S. have laid bare a new malware used by the Iranian government-sponsored advanced persistent threat (APT) group in attacks targeting government and commercial networks worldwide.

"MuddyWater actors are positioned both to provide stolen data and accesses to the Iranian government and to share these with other malicious cyber actors," the agencies said.

The joint advisory comes courtesy of the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Cyber Command Cyber National Mission Force (CNMF), and the U.K.'s National Cyber Security Centre (NCSC).

The cyberespionage actor was outed this year as conducting malicious operations as part of Iran's Ministry of Intelligence and Security (MOIS) targeting a wide range of government and private-sector organizations, including telecommunications, defense, local government, and oil and natural gas sectors, in Asia, Africa, Europe, and North America.

MuddyWater is also tracked by the wider cybersecurity community under the names Earth Vetala, MERCURY, Static Kitten, Seedworm, and TEMP.Zagros, with the group known for cyber offensives in support of MOIS objectives since roughly 2018.

Besides exploiting publicly reported vulnerabilities, the hacking collective has been historically observed employing open-source tools to gain access to sensitive data, deploy ransomware, and achieve persistence on victim networks.

A follow-on investigation by Cisco Talos late last month also uncovered a previously undocumented malware campaign aimed at Turkish private organizations and governmental institutions with the goal of deploying a PowerShell-based backdoor.

The new activities unmasked by the intelligence authorities are no different in that they make use of obfuscated PowerShell scripts to conceal the most damaging parts of the attacks, including command-and-control (C2) functions.

The intrusions are facilitated via a spear-phishing campaign that attempts to coax its targets into downloading suspicious ZIP archives that either contain an Excel file with a malicious macro that communicates with the actor's C2 server or a PDF file that drops a malicious payload to the infected system.

"Additionally, the group uses multiple malware sets — including PowGoop, Small Sieve, Canopy/Starwhale, Mori, and POWERSTATS — for loading malware, backdoor access, persistence, and exfiltration," FBI, CISA, CNMF, and NCSC said.

While PowGoop functions as a loader responsible for downloading second-stage PowerShell scripts, Small Sieve is described as a Python-based implant used for maintaining a foothold in the network by leveraging the Telegram API for C2 communications to evade detection.

Other key pieces of malware are Canopy, a Windows Script File (.WSF) used to collect and transmit system metadata to an adversary-controlled IP address, and two backdoors called Mori and POWERSTATS that are used to run commands received from the C2 and maintain persistent access.

Rounding up the arsenal of tools employed by MuddyWater is a survey script to enumerate and transmit information about victim computers back to the remote C2 server. Also deployed is a newly identified PowerShell backdoor that's used to execute commands received from the attacker.

To create barriers for potential attacks, the agencies are recommending organizations to use multi-factor authentication wherever applicable, limit the use of administrator privileges, implement phishing protections, and prioritize patching known exploited vulnerabilities.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
