Microsoft: Iranian Gov Hackers Caught in Azure Wiper Attacks

Iranian advanced persistent threat (APT) actors MuddyWater and DEV-1084 have been observed launching destructive cyberattacks disguised as ransomware, Microsoft warns.

Also tracked as Mercury, Seedworm, and Static Kitten, and known to be launching espionage campaigns against targets in the Middle East since at least 2017, MuddyWater was officially linked by the U.S. government to Iran's Ministry of Intelligence and Security.

DEV-1084, which claims to be a financially motivated cybercriminal group operating under the DarkBit persona, is connected to MuddyWater, if not a subgroup of the APT, Microsoft says (the tech giant uses the DEV designation for emerging, developing, or unknown clusters of activity).

According to Microsoft, DEV-1084 was seen using an IP address and a VPN provider historically associated with MuddyWater, using tools previously used by the APT, and using a domain believed to be controlled by MuddyWater.

"Microsoft assesses that Mercury gains access to the targets through remote exploitation of an unpatched internet-facing device. Mercury then handed off access to DEV-1084. It is not currently clear if DEV-1084 operates independently of Mercury and works with other Iranian actors or if DEV-1084 is an 'effects based' sub-team of Mercury that only surfaces when Mercury operators are instructed to carry out a destructive attack," the tech giant notes.

Following initial compromise, the adversary deploys web shells, creates administrative user accounts, installs legitimate tools for remote access (including eHorus, Ligolo, and RPort), installs a PowerShell script backdoor, and steals credentials.

After establishing persistence, the threat actor performs reconnaissance and lateral movement, using remote scheduled tasks to launch the backdoor, Windows Management Instrumentation (WMI) to execute commands, and remote services to run PowerShell commands.

The attackers were also caught abusing compromised Azure Active Directory (Azure AD) accounts that had 'global administrator' privileges to perform destructive actions, "deleting within a few hours server farms, virtual machines, storage accounts, and virtual networks. We assess that the attacker's goal was to cause data loss and a denial of service (DoS) of the target's services", Microsoft said.

The adversary was observed performing new actions weeks or even months after completing one of the steps. In some cases, the hackers were seen deploying tunneling tools such as Ligolo and OpenSSH to hide command-and-control (C&C) communication.

Microsoft also observed the attackers using high-privileged credentials and domain controller access to carry out on-premises destructive operations and prepare for large-scale encryption.

Using Group Policy Objects (GPO), the threat actor deployed the DarkBit ransomware in the Netlogon shares of several domain controllers and registered a scheduled task to launch the payload.

Using the compromised accounts, the adversary obtained credentials for other privileged accounts, which were abused for other malicious activities, including adding certificates to the OAuth application and attempting to dump mailboxes

and/or search for sensitive data.

Related: Iranian Hackers Deliver New ‘Fantasy’ Wiper via Supply Chain Attack

Related: US, Allies Link Iranian Government Agency to Ransomware Attacks

Related: Microsoft Dives Into Iranian Ransomware APT Attacks

Microsoft: Iranian Gov Hackers Caught in Azure Wiper Attacks