

# Microsoft: Iranian Hackers Moved From Recon to Targeting US Critical Infrastructure

A subgroup of Iran-linked advanced persistent threat (APT) actor Mint Sandstorm has started to quickly adopt proof-of-concept (PoC) exploit code targeting vulnerabilities in internet-facing applications, Microsoft warns.

The nation-state group is known as TA453, Ajax Security Team, Charming Kitten, APT35, Magic Hound, NewsBeef, Newscaster, and Phosphorus, and now Mint Sandstorm, per Microsoft's updated threat actor naming taxonomy.

Active since at least 2011, Mint Sandstorm has been observed targeting activists, government entities, journalists, critical infrastructure, and other entities.

According to Microsoft, there are several subgroups operating under Mint Sandstorm, but the overall activity can be associated with the Islamic Revolutionary Guard Corps (IRGC), Iran's military intelligence arm.

One of these subgroups, the tech giant says, has specialized in compromising high-value targets for information theft, and was recently observed quickly adopting PoC code for known vulnerabilities.

Initially focused on performing reconnaissance, the subgroup transitioned to directly targeting critical infrastructure organizations in the United States in 2022, including energy companies, seaports, transit systems, and a major utility and gas company. These attacks were "potentially in support of

retaliatory destructive cyberattacks,” Microsoft said.

Earlier this year, the Mint Sandstorm subgroup was seen adopting PoC exploitation code for N-day vulnerabilities quickly after they were publicly disclosed. Previously, the threat actor took weeks to weaponize exploits for vulnerabilities such as ProxyShell and Log4Shell.

“For example, Mint Sandstorm began exploiting CVE-2022-47966 in Zoho ManageEngine on January 19, 2023, the same day the POC became public. They later exploited CVE-2022-47986 in Aspera Faspex within five days of the POC being made public on February 2, 2023,” Microsoft reports.

The tech giant warns that Mint Sandstorm continues to exploit older vulnerabilities for initial compromise, mostly as part of ‘opportunistic and indiscriminate’ activity, which underlines the need to apply patches for known vulnerabilities in a timely manner.

Following initial compromise, the Mint Sandstorm subgroup deploys a custom PowerShell script for discovery, followed by lateral movement using Impacket, and the deployment of additional tools.

In some attacks, the subgroup uses PowerShell scripts for account enumeration and RDP connections and an SSH tunnel for command-and-control (C&C), to steal the victim’s Active Directory database, compromise user credentials, and access user accounts.

In other attacks, the subgroup created scheduled tasks for persistence, used webhook.site for C&C, and deployed custom malware.

Since 2022, the threat actor has been observed using two custom implants, namely Drokbn (written in .NET, consists of an installer and a backdoor) and Soldier (a multistage .NET backdoor that can fetch additional payloads and uninstall

itself).

In some instances, the subgroup was observed relying on low-volume phishing campaigns to target “individuals affiliated with high-profile think tanks or universities in Israel, North America, or Europe with ties to the security and policy communities” with malicious documents leading to the CharmPower modular backdoor.

“Capabilities observed in intrusions attributed to this Mint Sandstorm subgroup are concerning as they allow operators to conceal C&C communication, persist in a compromised system, and deploy a range of post-compromise tools,” Microsoft concludes.

**Related:** UK Gov Warns of Phishing Attacks Launched by Iranian, Russian Cyberspies

**Related:** Microsoft Dives Into Iranian Ransomware APT Attacks

**Related:** Iranian Cyberspy Group Launching Ransomware Attacks Against US

*Microsoft: Iranian Hackers Moved From Recon to Targeting US Critical Infrastructure*