MuddyWater targets Middle Eastern and Asian countries in phishing attacks - TechRepublic

By Brian Stone

Published: 2022-03-10 · Archived: 2026-04-05 16:09:02 UTC

Cisco Talos has illustrated the ways in which the Iranian backed hacker group has attempted countries for cyberattacks.

Adobe

Iranian APT Supergroup MuddyWater has been identified as the hackers linked to attempted phishing attacks against Turkey and other Asian countries according to findings published by Cisco Talos. The conglomerate, which has been linked to Iran's Ministry of Intelligence and Security by the U.S. Cyber Command, has been now identified as multiple different subgroups acting under the name of MuddyWater rather than one unified threat actor.

How and when the cyberattacks happened

The hacker group has reportedly been targeting these countries using a Windows script file (WSF) based remote access trojan (RAT) deemed "SloughRAT" by Cisco Talos. Using this form of malware, MuddyWater has attempted to conduct espionage, steal intellectual property and commit ransomware attacks against countries in the Arabian Peninsula the group has zeroed in on. The malicious actors attempted two campaigns against Turkey

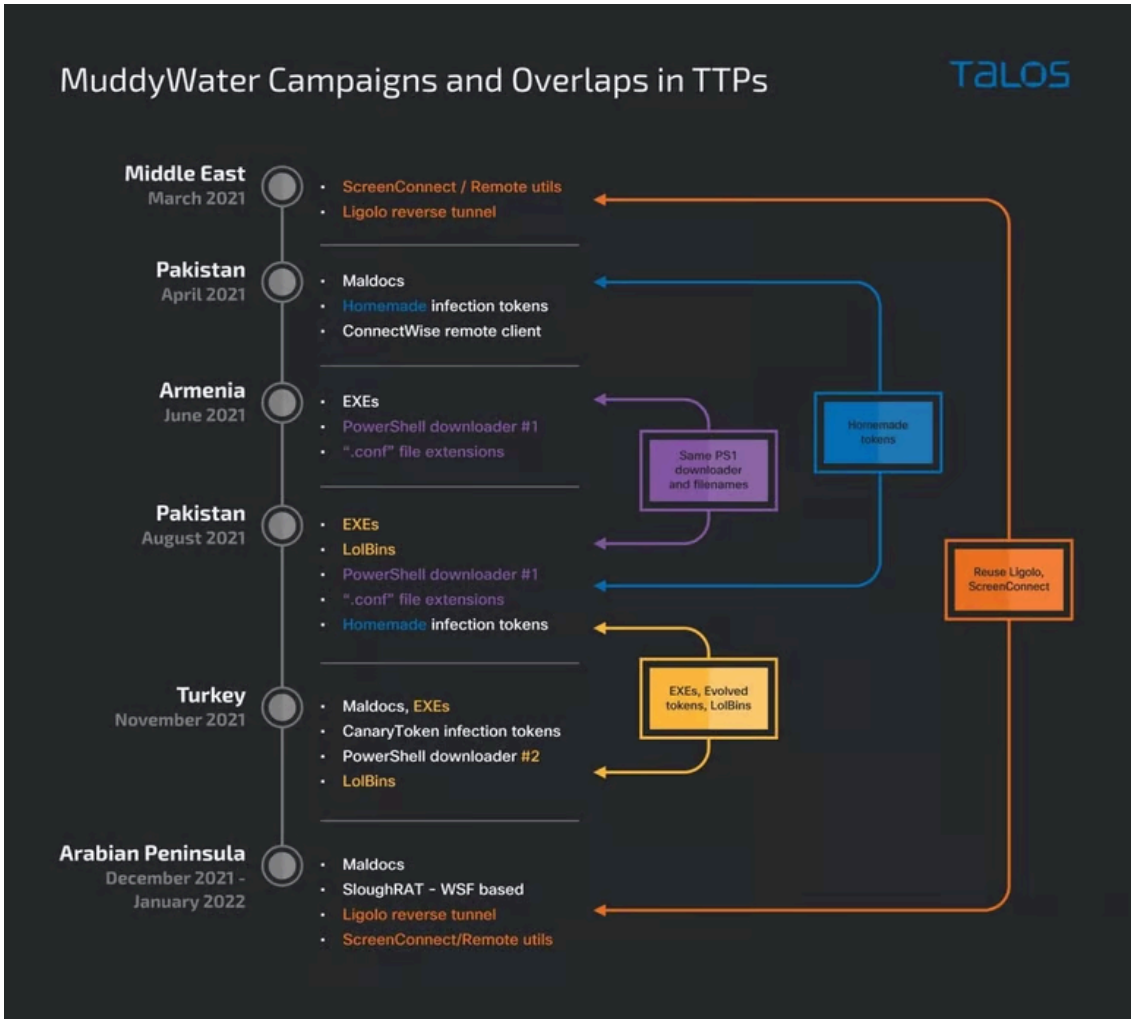
in November 2021, and targeted Armenia in June of the same year using the same types of Windows executable files.

In April 2021, Cisco Talos observed that this group also launched an attack against Pakistan via two different delivery systems – one employing a PowerShell-based downloader to accept and execute additional PS1 commands from the C2 server and another using malware document infection point that claimed to be part of a court case in Pakistan.

The group, also known as "MERCURY" or "Static Kitten", has been active since at least 2017, and is known for utilizing ransomware in their previously attempted attacks. According to the cybersecurity firm, the threat group has been known to use domain name system (DNS) attacks on its intended victims by using "PowerShell, Visual Basic and JavaScript scripting along with living-off-the-land binaries (LoLBins) and remote connection utilities to assist in the initial stages of the infection."

SEE: [Google Chrome: Security and UI tips you need to know](#) (TechRepublic Premium)

MuddyWater as a collection of groups



Credit: Cisco Talos

According to Cisco Talos' findings, the hacking group's "Variety of lures and payloads — along with the targeting of several different geographic regions — strengthens our growing hypothesis that MuddyWater is a conglomerate of sub-groups rather than a single actor."

The cybersecurity firm believes that the hacking group is a combination of smaller teams, targeting specific regions such as the Arabian Peninsula and Asia utilizing the different types of attacking techniques above. While MuddyWater is incorporated by smaller sub-groups, Cisco Talos believes that some of these teams are contracted out for attacks by the leaders and organizers of MuddyWater. One reason for this belief is that there have been unique strings and watermarks identified as being shared between MuddyWater and the Phosphorus/Charming Kitten APT groups.

These shared techniques among these smaller teams are seemingly preferred by threat actors in certain regions, making them identifiable as not belonging to the same areas as other attacks by the collective. The two preferred methods of attacks highlighted by the cybersecurity firm were the SloughRAT Windows executable file, and the Ligolo reverse tunneling tool which was used against Middle Eastern countries in March 2021.

SEE: Password breach: Why pop culture and passwords don't mix (free PDF) (TechRepublic)

How to secure yourself and your business

While this hacker group has been specifically targeting regions and countries throughout the world, cyber threats remain an important thing to keep in mind for both individuals and organizations. With this in mind, it is important to be ready with both antivirus software and extremely thorough training to make sure that systems have not been compromised and employees are aware of the online risks to avoid being victimized.

Share Article

Also Read

- How to become a cybersecurity pro: A cheat sheet
- NIST Cybersecurity Framework: A cheat sheet for professionals (free PDF)
- What are mobile VPN apps and why you should be using them
- Cybersecurity and cyberwar: More must-read coverage

Brian Stone

Brian is an award-winning journalist covering technology and the news behind it, having written for both print and online outlets in his previous stops as a writer.
