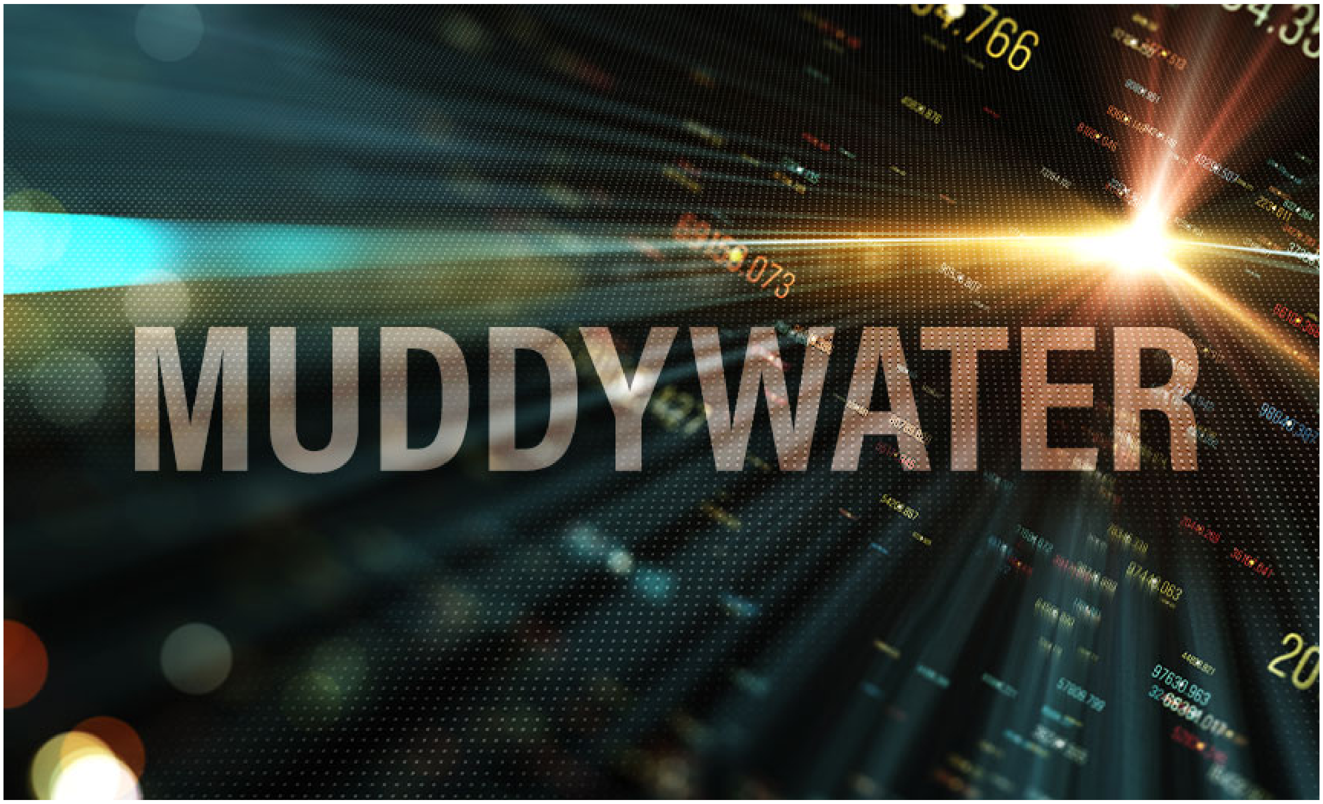
Iranian APT: New Methods to Target Turkey, Arabian Peninsula

govinfosecurity.com/iranian-apt-new-methods-to-target-turkey-arabian-peninsula-a-18706

Cybercrime , Cybercrime as-a-service , Cyberwarfare / Nation-State Attacks

APT MuddyWater Uses Malicious Documents to Deploy RATs Prajeet Nair (@prajeetspeaks) • March 12, 2022



The obfuscated Trojan seeks to execute arbitrary code and commands received from its C&C servers.

Hacking group MuddyWater, which has been linked to the Iranian Ministry of Intelligence and Security, is targeting Turkey and other Asian countries to conduct espionage and intellectual property theft and to deploy ransomware and destructive malware.

The campaign primarily uses malicious documents to deploy remote access Trojans on compromised systems, according to researchers at Cisco Talos. The sectors targeted by this advanced persistent threat actor include national and local governments and ministries, universities and private entities such as telecommunication providers.

Talos researchers observed several instances of maldocs, specifically XLS files, distributed by the APT MuddyWater. These XLS files were observed targeting the Arabian Peninsula through a recent phishing campaign.

The documents consist of a malicious macro that, when triggered, drops two WSF files on the endpoint.

"One of these scripts is the instrumentor script meant to execute the next stage. This instrumentor script is placed in the current user's Startup folder by the VBA macro to establish persistence across reboots," the researchers say. "The second script is a WSF-based RAT we call "SloughRAT" that can execute arbitrary commands on the infected endpoint. This RAT consists of obfuscated code from interweaved Visual Basic and JavaScript."

MuddyWater has been active since at least 2017 and is also known as MERCURY or Static Kitten. U.S. Cyber Command has attributed the APT group to Iran's Ministry of Intelligence and Security (see: *MuddyWater Targets Critical Infrastructure in Asia, Europe*).

The group is known for conducting espionage campaigns against high-value targets in North America, Europe and Asia.

Technical Details

The researchers found that the group is using maldocs to deliver a Windows script file-based remote access Trojan, which Cisco Talos researchers call "SloughRAT," an implant known as "Canopy" in CISA's most recent alert from February 2022 about MuddyWater.

The obfuscated Trojan also attempts to execute arbitrary code and commands received from its command and control servers. The researchers say that their investigation led to the discovery of the use of two additional script-based implants: one written in Visual Basic during 2021-2022 and one written in JavaScript in 2019-2020, which also downloads and runs arbitrary commands on the victim's system.

MuddyWater also relies heavily on the use of DNS to contact their C2 servers, while the initial contact with the hosting servers is conducted via HTTP.

"Their initial payloads usually use 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," the researchers say. "The attackers attempted to deploy the Connectwise Remote Access client on the target's endpoints, a tactic commonly used by MuddyWater to gain an initial foothold on targets' endpoints."

Cisco Talos researchers say that the attackers deployed a RAT in April 2021 and the EXE-based infection vector from August 2021; the maldocs and decoy documents reached out to a common server to download a common image file that links them.

"These campaigns used a homemade implementation of signaling tokens. In this case, the maldocs have an external entity downloaded from an attacker-controller server. This entity consists in a simple image which has no malicious content," say Cisco Talos researchers Asheer Malhotra, Vitor Ventura, and Arnaud Zobec.

They say this may be a way for the attackers to track the initial infection vectors and identify which is more successful. The researchers say it is likely that the attackers used this server as a token tracker to keep track of successful infections in this campaign.

"This token-tracking system was then migrated to CanaryTokens in September 2021 in the attacks targeting Turkey using the malicious Excel documents," the researchers say.

In addition, during the tracing of MuddyWater's activity over the past year, the researchers say that they saw some of the shared techniques are refined from one region to the other, suggesting the teams use their preferred flavors of tools of choice, including final payloads.

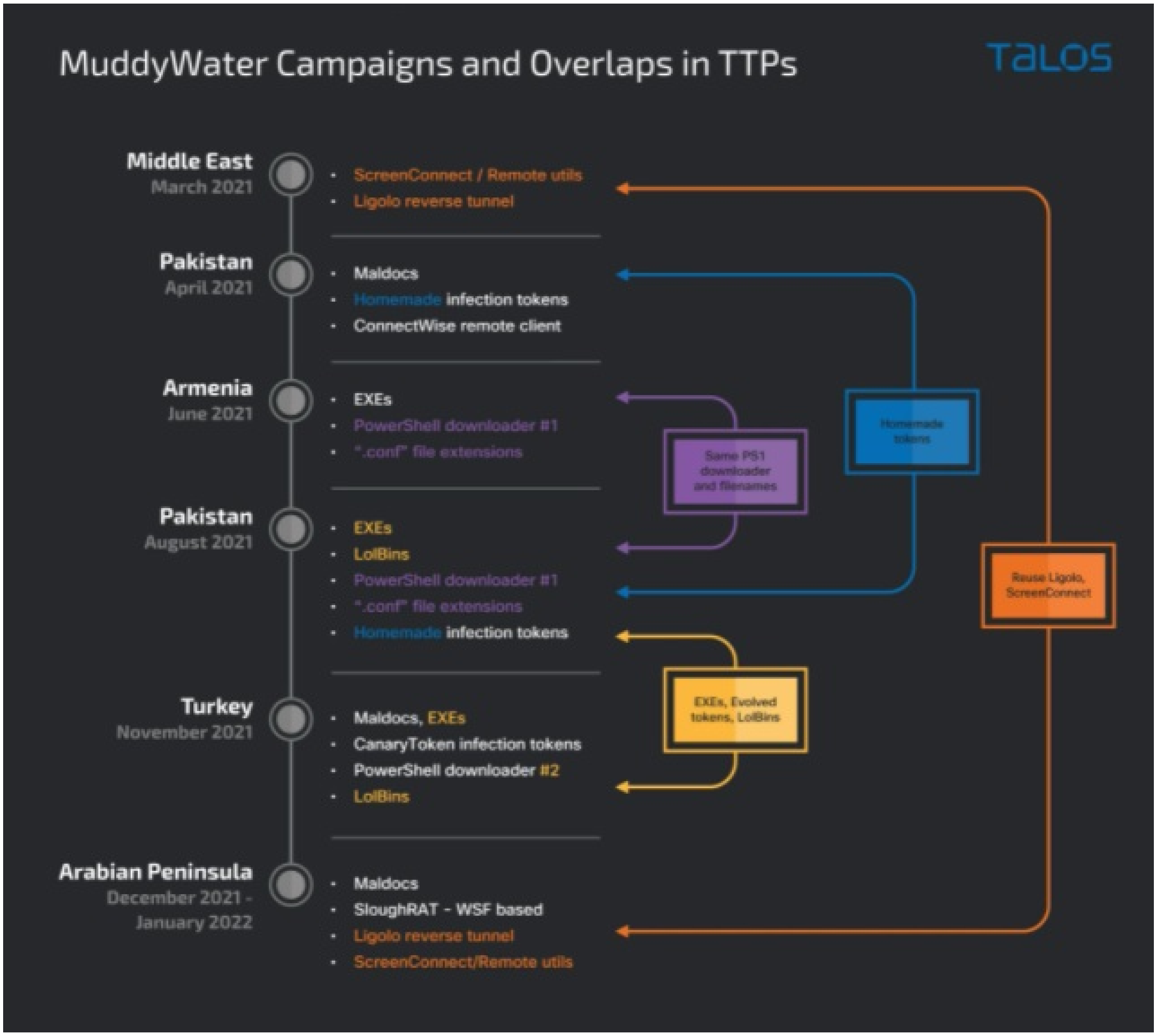
Earlier, the researchers disclosed two campaigns using the same types of Windows executables targeting Turkey in November 2021 and Armenia in June 2021.

"Another campaign illustrated previously used similar executables, this time to target Pakistan. This campaign deployed a PowerShell-based downloader on the endpoint to accept and execute additional PS1 commands from the C2 server. Going further back, in April 2021, we observed another instance of Muddywater targeting entities in Pakistan, this time with a maldoc-based infection vector. The lure document claimed to be part of a court case," the researchers say.

Is MuddyWater a Conglomerate?

The Cisco Talos report says MuddyWater's variety of lures and payloads and its targeting of several different geographic regions strengthens the growing hypothesis that MuddyWater is a conglomerate of subgroups rather than a single actor.

"These sub-groups have conducted campaigns against a variety of industries. While these teams seem to operate independently, they are all motivated by the same factors that align with Iranian national security objectives, including espionage, intellectual theft, and destructive or disruptive operations based on the victims they target," the researchers say.



MuddyWater Campaigns and Overlaps in TTPs

Talos

Middle East
March 2021

- ScreenConnect / Remote utils
- Ligolo reverse tunnel

Pakistan
April 2021

- Maldocs
- Homemade infection tokens
- ConnectWise remote client

Armenia
June 2021

- EXEs
- PowerShell downloader #1
- ".conf" file extensions

Pakistan
August 2021

- EXEs
- LolBins
- PowerShell downloader #1
- ".conf" file extensions
- Homemade infection tokens

Turkey
November 2021

- Maldocs, EXEs
- CanaryToken infection tokens
- PowerShell downloader #2
- LolBins

Arabian Peninsula
December 2021 -
January 2022

- Maldocs
- SloughRAT - WSF based
- Ligolo reverse tunnel
- ScreenConnect/Remote utils

Same PS1 downloader and filenames
Homemade tokens
Reuse Ligolo, ScreenConnect
EXEs, Evolved tokens, LolBins

MuddyWater teams appear to share TTPs

Cisco Talos researchers analyzed a variety of campaigns that are marked by the development and use of distinct infection vectors and tools to gain entry, establish long-term access, siphon valuable information and monitor their targets. But the MuddyWater teams appear to share TTPs, as evidenced by the incremental adoption of various techniques over time in different MuddyWater campaigns.

"We believe there are links between these different campaigns, including the migration of techniques from region to region, along with their evolution into more advanced versions. Overall, the campaigns we describe cover Turkey, Pakistan, Armenia and countries from the Arabian Peninsula," researchers say.