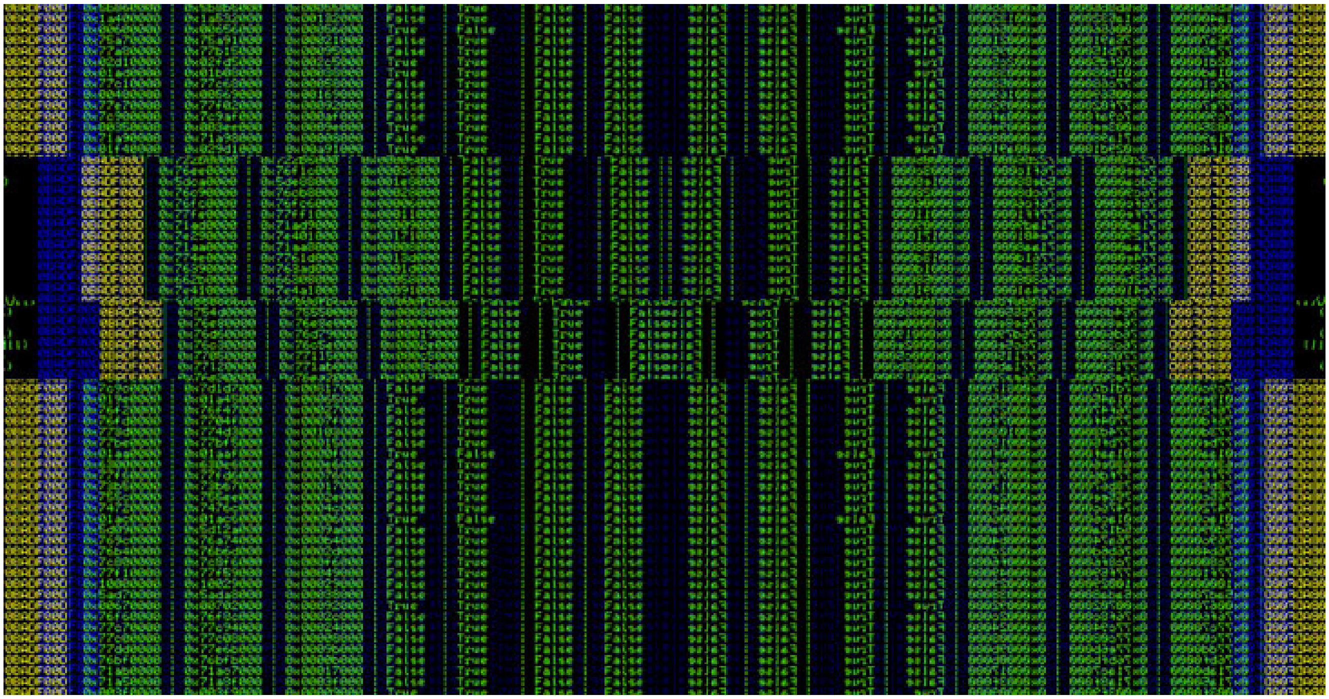
Palestine-Aligned Hackers Use New NimbleMamba Implant in Recent Attacks

thehackernews.com/2022/02/palestinian-hackers-using-new.html

February 8, 2022



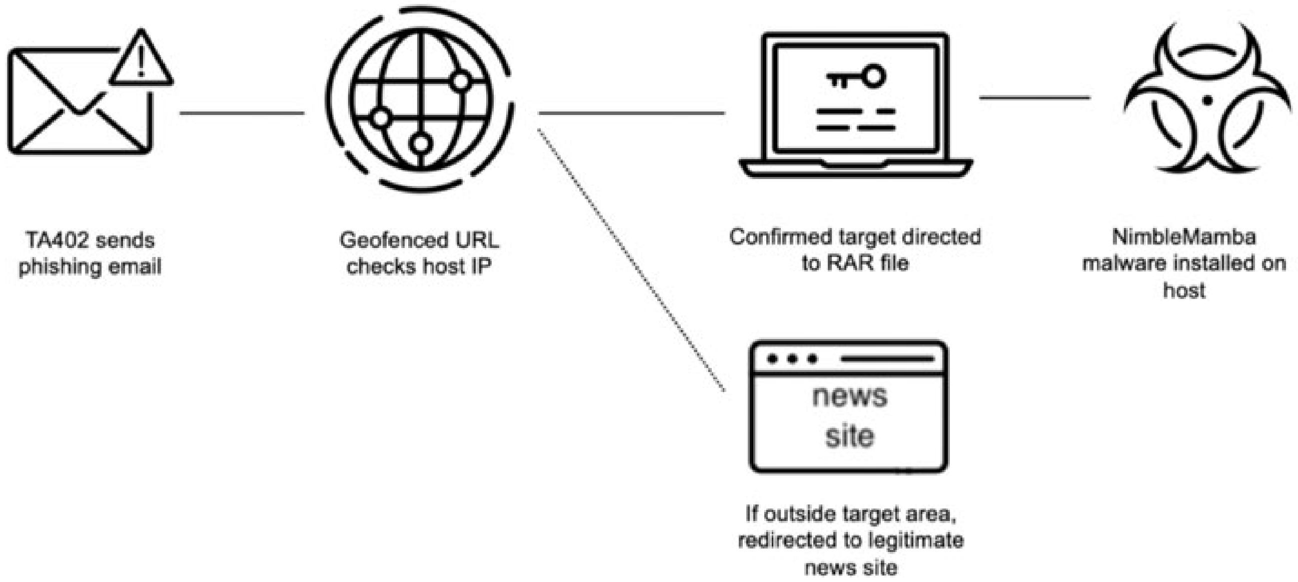
An advanced persistent threat (APT) hacking group operating with motives that likely align with Palestine has embarked on a new campaign that takes advantage of a previously undocumented implant called **NimbleMamba**.

The intrusions leveraged a sophisticated attack chain targeting Middle Eastern governments, foreign policy think tanks, and a state-affiliated airline, enterprise security firm Proofpoint said in a report, attributing the covert operation to a threat actor tracked as Molerats (aka TA402).

Notorious for continuously updating their malware implants and their delivery methods, the APT group was most recently linked to an espionage offensive aimed at human rights activists and journalists in Palestine and Turkey, while a previous attack exposed in June 2021 resulted in the deployment of a backdoor called LastConn.

But the lull in the activities has been offset by the operators actively working to retool their arsenal, resulting in the development of NimbleMamba, which is designed to replace LastConn, which, in turn, is believed to be an upgraded version of another backdoor called SharpStage that was used by the same group as part of its campaigns in December 2020.

"NimbleMamba uses guardrails to ensure that all infected victims are within TA402's target region," the researchers said, adding the malware "uses the Dropbox API for both command-and-control as well as exfiltration," suggesting its use in "highly targeted intelligence collection campaigns."


TA402 sends phishing email
Geofenced URL checks host IP
Confirmed target directed to RAR file
NimbleMamba malware installed on host
news site
If outside target area, redirected to legitimate news site

Also delivered is a trojan dubbed BrittleBush that establishes communications with a remote server to retrieve Base64-encoded commands to be executed on the infected machines. What's more, the attacks are said to have occurred in tandem with the aforementioned malicious activity targeting Palestine and Turkey.

The infection sequence mirrors the exact same technique used by the threat actor to compromise its targets. The spear-phishing emails, which act as the starting point, contain geofenced links that lead to malware payloads — but only if the recipient is in one of the targeted regions. If the targets live outside of the attack radius, the links redirect the user to a benign news website like Emarat Al Youm.

CyberSecurity

However, more recent variations of the campaign in December 2021 and January 2022 have involved the use of Dropbox URLs and attacker-controlled WordPress sites to deliver malicious RAR files containing NimbleMamba and BrittleBush.

The development is the latest example of adversaries using cloud services, such as Dropbox, to launch their attacks, not to mention how quickly sophisticated actors can respond to public disclosures of their invasion methods to create something potent and effective that can go past security and detection layers.

"TA402 continues to be an effective threat actor that demonstrates its persistence with its highly targeted campaigns focused on the Middle East," the researchers concluded. "The [two] campaigns demonstrate Molerats' continued ability to modify their attack chain based on their intelligence targets."

SHARE □ □ □ □ ךָ
SHARE □