Molerats APT: New Malware and Techniques in Middle East Espionage Campaign

By Cybereason Team

Archived: 2026-04-05 21:25:46 UTC

Security researchers observed a politically motivated APT called “Molerats” using three new malware variants to conduct espionage in the Middle East.

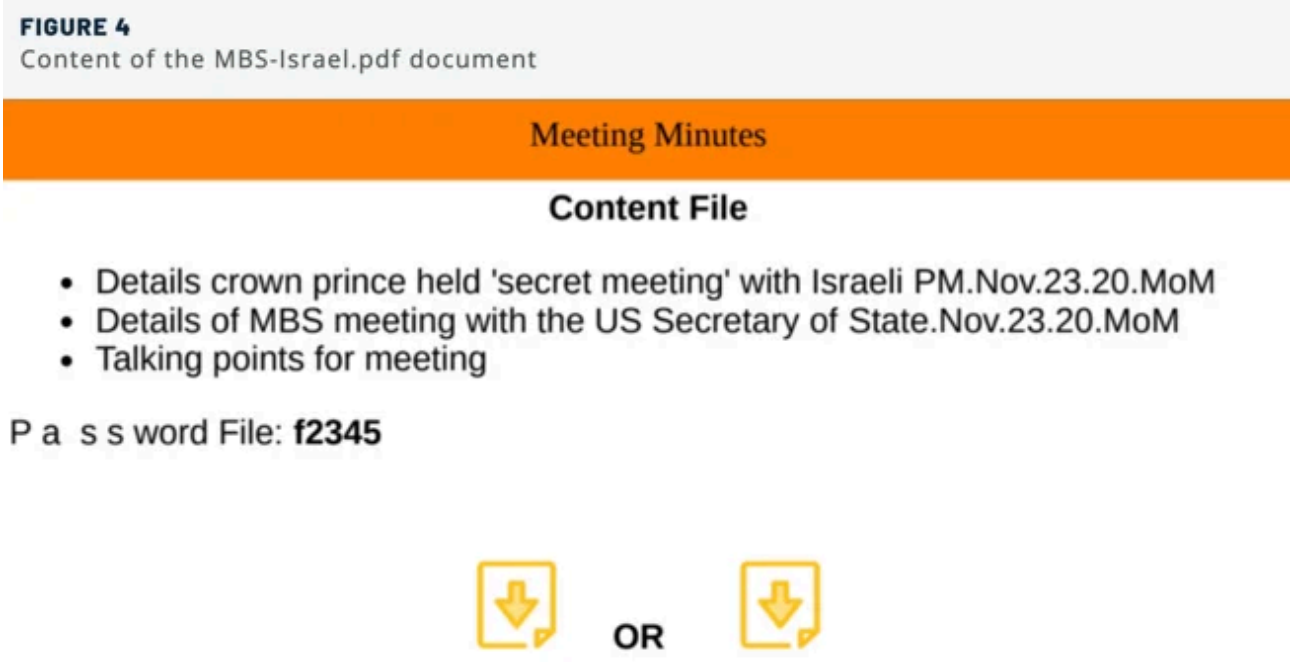
Overview of the Campaign

On December 9, Cybereason published a report that revealed that they had uncovered a new attack campaign launched by Molerats. This operation cohered with previous attacks launched by the APT in that it used political events in the Middle East as lures.

In particular, the campaign focused on the ongoing normalization process between Israel and its Arab neighbors. One of the phishing documents, a PDF file titled “MBS-Israel,” explored that development by referencing the peace talks between Israeli Prime Minister Benjamin Netanyahu and His Royal Highness Mohammed bin Salman, Saudi Crown Prince.

The PDF document instructed the recipient to download password-protected archives that claimed to contain the contents of those peace talks.

FIGURE 4
Content of the MBS-Israel.pdf document



At the time of discovery, Molerats was using Dropbox and Google Drive to host those password-protected archives at:

https://www.dropbox[dot]com/s/r81t6y7yr8w2ymc/MOM.zip?dl=1

and

https://drive.google[dot]com/uc?export=download&id=1NnMlUPwkxK4_wAJwrqxqBAfdKCPDxyeh

Both archives arrived with several executables whose names referenced the talks.

Malware Variant #1: SharpStage Backdoor

One of those executables, “Details Crown Prince held 'secret meeting' with Israeli PM.Nov.23.20.MoM.exe,” was responsible for infecting the victim’s computer with SharpStage.

The first of the three new malware variants detected by Cybereason Nocturnus, SharpStage is a .NET malware with backdoor capabilities.

Cybereason’s researchers identified three variants of the SharpStage threat. Those three versions registered compilation timestamps between October 4 and November 29, 2020. They also shared similar functionality in terms of code modularity, obfuscation and persistence.

Upon successful installation, SharpStage enables the attackers to capture snapshots of a victim’s screen, download and execute additional files and specifically check for the presence of Arabic on the infected machine to avoid executing on computers outside of its purview.

The backdoor also came equipped with a Dropbox API. This feature enabled SharpStage to communicate with Dropbox using a token in order to download and exfiltrate stolen data.

SharpStage registered the detection rate of 1/70 with VirusTotal at the time of discovery.

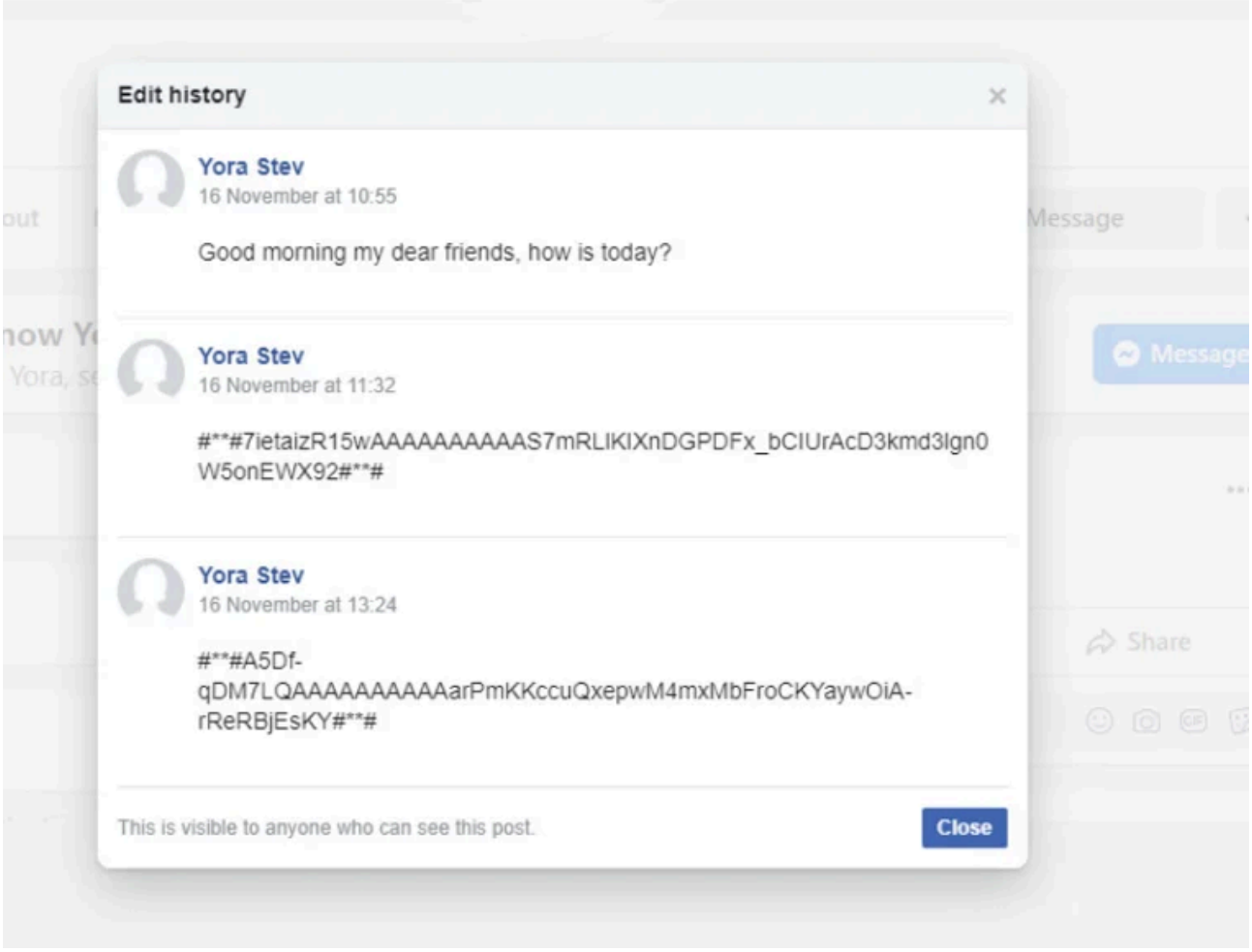
Malware Variant #2: DropBook Backdoor

The second executable, “Talking points for meeting.exe,” infected the machine with a sample of the DropBook backdoor.

Similar to SharpStage, DropBook executed on a machine only if the infected machine had configured the Arabic language. But this malware also came with another precondition: the machine needed to have WinRAR perhaps in order for a later stage of the attack to work.

DropBook also mimicked SharpStage by using DropBox for file uploads and downloads. The threat didn’t stop there with its abuse of legitimate services, however. It also used posts on Facebook and note-taking application Simplenote to receive a Dropbox token as well as command-and-control (C2) instructions from the attackers.

FIGURE 25
Dropbox token in Facebook



Assaf Dahan, Sr. Director, Head of Threat Research, explained how this technique helped the attackers to evade detection:

Molerats created fake Facebook accounts that specifically for this campaign, those accounts are effectively being used by the group for command-and-control purposes by sending instructions to the malware using Facebook posts. This is a clever way of hiding in plain sight, abusing the trust given to a legitimate platform such as Facebook. This helps the group to remain under the radar.

By using Facebook and Simplenote as communication channels, the attackers could proceed to drop additional threats onto the infected computer. Those secondary malware strains included the Quasar RAT and SharpStage.

Malware Variant #3: MoleNet Downloader

DropBook also served as a vehicle through which attackers could install the MoleNet Downloader, a tool which has been in active development since at least 2019.

Heavily obfuscated and written in .NET, the MoleNet Downloader enabled the attackers to profile the OS of the infected machine and submit the resulting information to the C2. The malware also came with the ability to download additional payloads from the C2 and to establish persistence using PowerShell.

Similar Techniques to Come

After analyzing the attack campaign, Cybereason Nocturnus reported the abuses it had documented to Google, Facebook, Dropbox and Simplenote. Some of those vendors responded to the security team and informed them that they were launching an investigation to determine what had happened. Others had not yet responded at the time of this writing.

Overall, Dahan feels that this new campaign helps to indicate the general direction in which Molerats as an APT is moving:

We see constant changes and developments and an increased level of sophistication. The group invests time and resources to try to keep the activity under the radar and evade detection. They are doing a good job with evading automatic sandbox analysis by checking for Arabic language settings. Otherwise, the malware won’t run. We estimate that the abuse of legitimate cloud platforms and social media will only increase, as attackers see the value in blending in and hiding in plain sight.

More information about some of Molerats’ earlier attack activity is available here and here. Open the chatbot on the lower right-hand side of this blog to download your copy of the Indicator's of Compromise, which includes C2 Domains, IP addresses, Docx files SHA-1 hashes, and Msi files.
