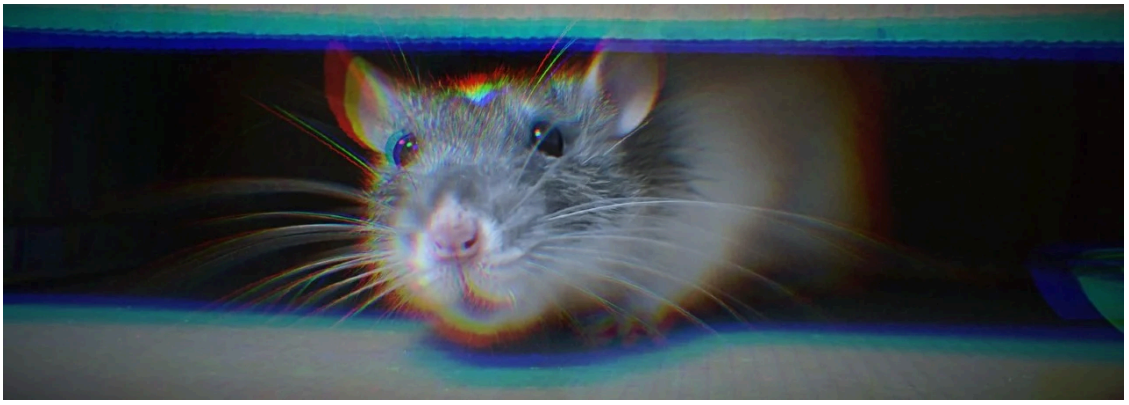
Hacking group’s new malware abuses Google and Facebook services

By Ionut Ilascu

Published: 2020-12-14 · Archived: 2026-04-05 15:37:26 UTC

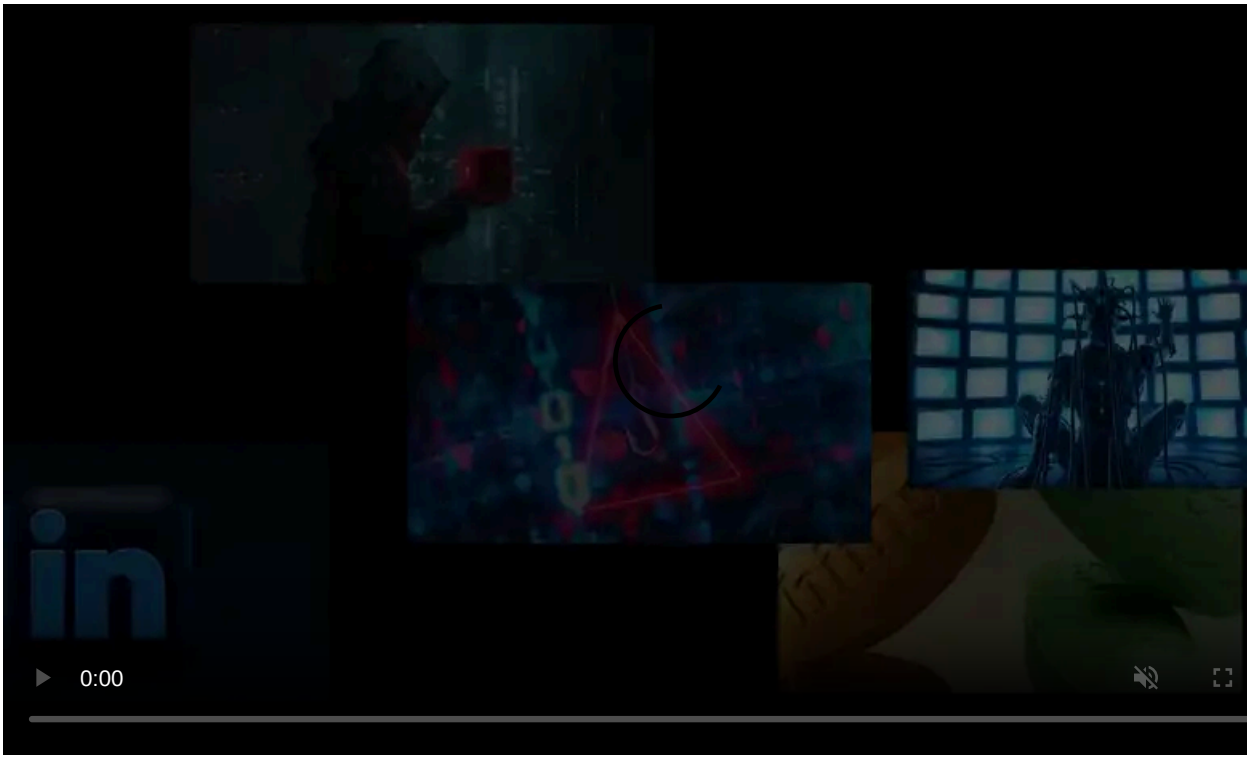


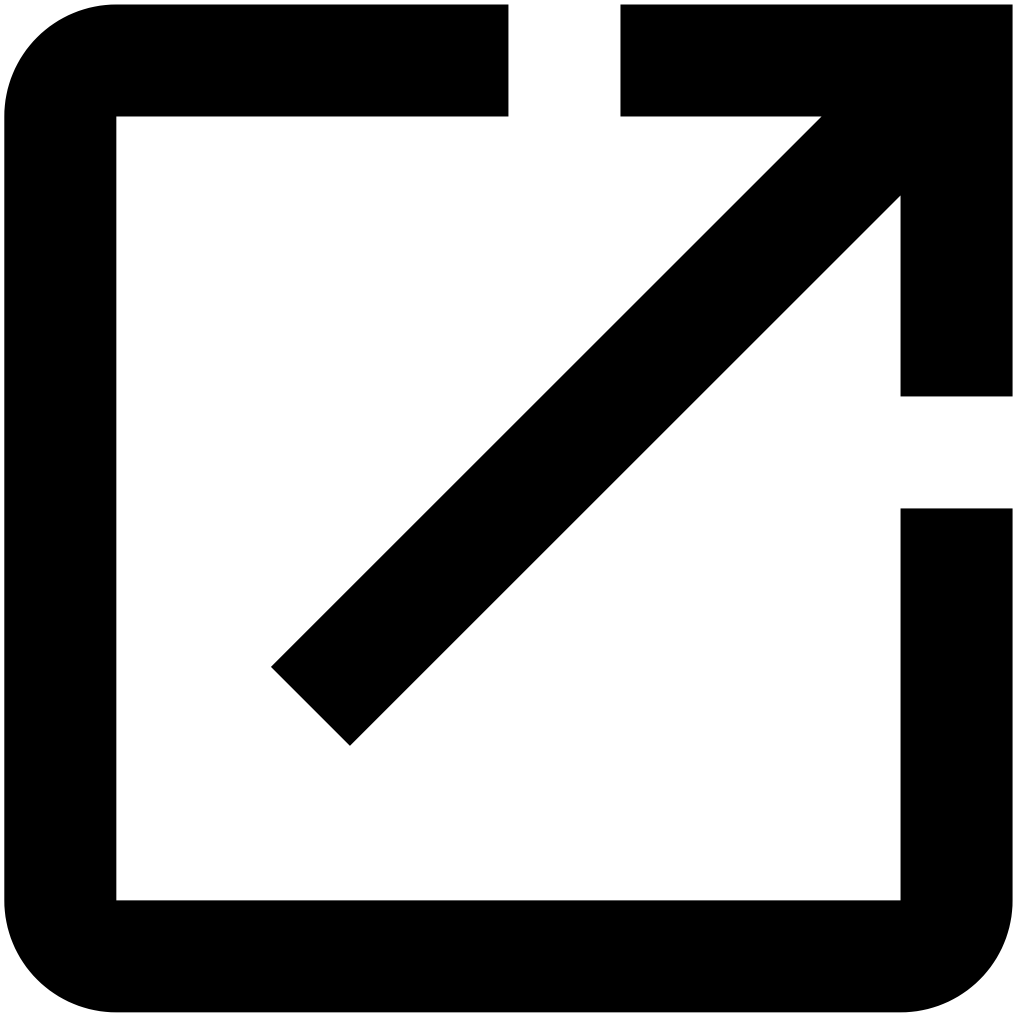
Molerats cyberespionage group has been using in recent spear-phishing campaigns fresh malware that relies on Dropbox, Google Drive, and Facebook for command and control communication and to store stolen data.

The hackers have been active since at least 2012 and are considered to be the low-budget division of a larger group called the Gaza Cybergang.

Two backdoors and a downloader

The Molerats threat actor used in recent operations two new backdoors - called SharpStage and DropBook, and one previously undocumented malware downloader named MoleNet.


0:00



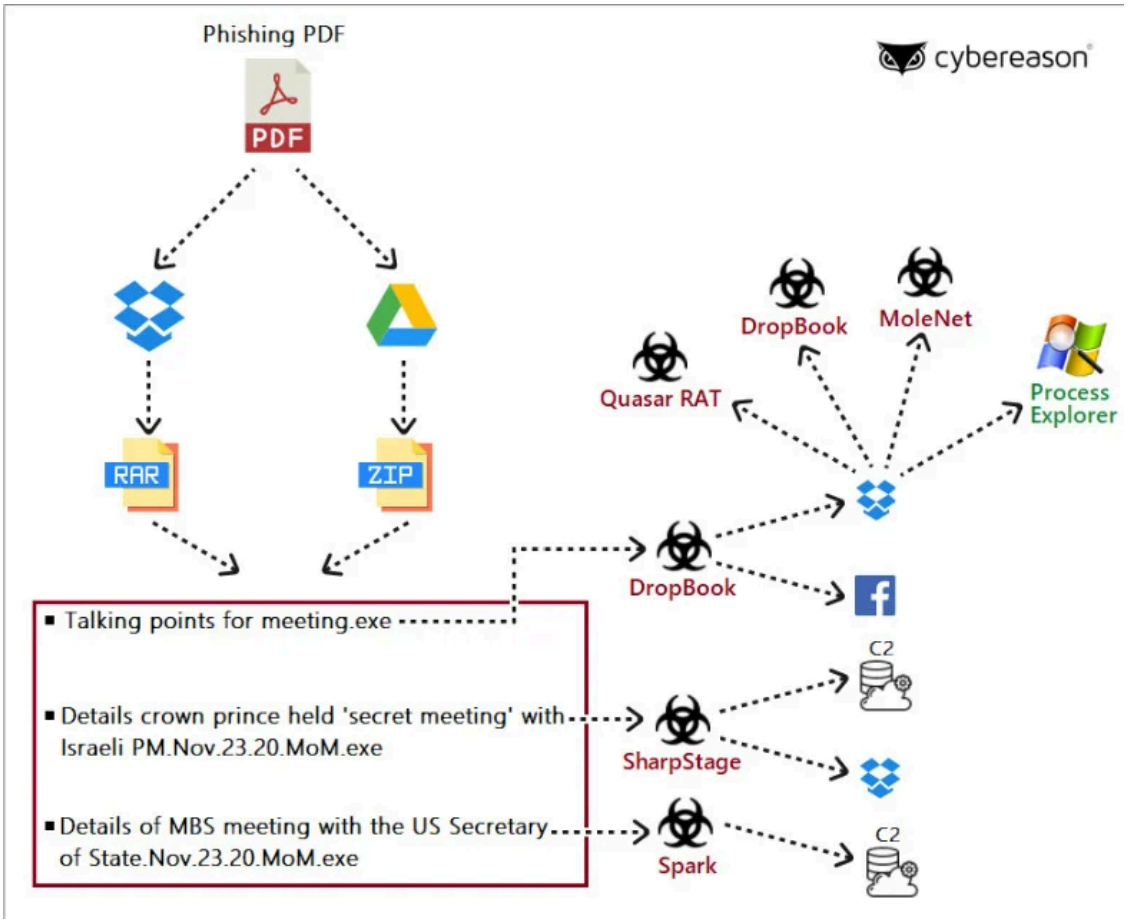
Designed for cyberespionage, the malware attempts to avoid detection and takedown efforts by using Dropbox and Facebook services to steal data and receive instructions from the operators. Both backdoors implement Dropbox to extract stolen data.

The attack starts with an email luring political figures or government officials in the Middle East (Palestinian Territories, UAE, Egypt, Turkey) to download malicious documents.

One of the lures in campaigns delivering the new malware was a PDF file referencing the recent talks between Israeli Prime Minister Benjamin Netanyahu and His Royal Highness Mohammed bin Salman, Saudi Crown Prince.

The document showed only a summary of the content and instructed the recipient to download password-protected archives stored in Dropbox or Google Drive for the full information.

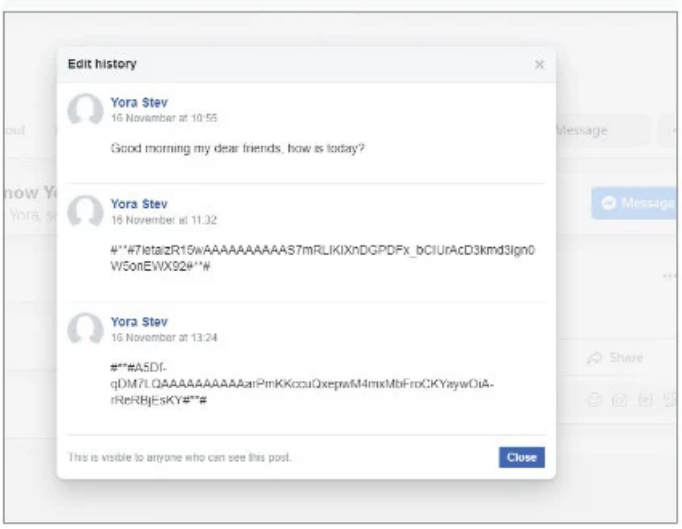
Two of these files were SharpStage and DropBook backdoors, which called a Dropbox storage controlled by the attacker to download other malware. A third one was another backdoor, Spark, also used by Molerats in previous campaigns.



Commands over Facebook

A technical report from Cybereason's Nocturnus Team [PDF] notes that the Python-based DropBook backdoor distinguishes from other tools in Molerats' arsenal because it receives instructions only through fake accounts on Facebook and Simplenote, the note-taking app for iOS.

The hackers control the backdoor through commands published in a post on Facebook. They used the same method to provide the token necessary to connect to the Dropbox account. Simplenote acts as a backup in case the malware cannot retrieve the token from Facebook.



With commands coming from multiple sources on a legitimate service, taking down the malware's communication with the attacker becomes a more difficult task.

DropBook's capabilities include checking installed programs and file names for reconnaissance, executing shell commands received from Facebook or Simplenote, and fetching additional payloads from Dropbox and running them.

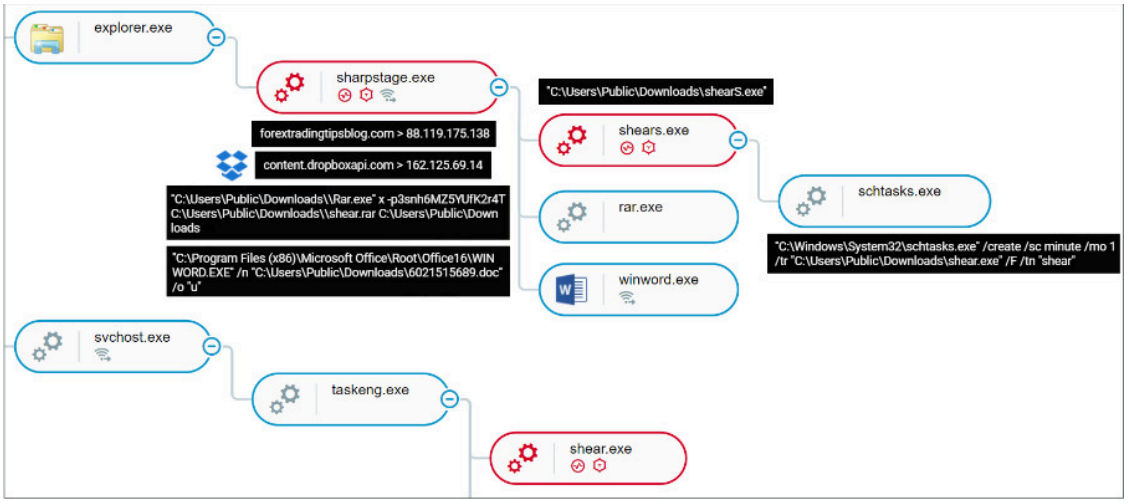
The researchers believe that DropBook is the work of the same developer that made JhoneRAT, a remote access tool written in Python that uses legitimate services (Google Drive, Twitter, ImgBB, and Google Forms) for command and control, to store malicious documents, or exfiltrate data.

SharpStage and MoleNet

Unlike DropBook, the SharpStage backdoor is written in .NET depends on a traditional command and control (C2) server. Cybereason discovered three variants of this malware, with compilation timestamps between October 4 and November 29. All are under constant development.

All variants share similar functionalities, including taking screenshots, executing arbitrary commands (to run PowerShell, the command line, WMI), and decompress data received from the C2 (payload, persistence module). SharpStage also comes with a Dropbox API for data download and exfiltration.

Both backdoors target Arabic-speaking users. They use code that checks if the compromised machine has the Arabic language installed. This way, the attacker avoids systems belonging to non-relevant individuals as well as most sandboxes, Cybereason researchers note.



MoleNet, the third malware that Cybereason discovered, can run WMI commands to profile the operating system, check for debuggers, restart the machine from the command line, upload details about the OS, fetch new payloads, and create persistence.

While the researchers found it only recently, MoleNet has been under development since at least 2019 and relies on infrastructure that has been in use since at least 2017. Yet, it remained unnoticed.

Even if they skimp on resources by using free services for their operations, Molerats shows that it can create new malware for stealthy operations.

Cybereason provides comprehensive details about the new tools leveraged by Molerats in recent campaigns, covering the attack chain, infrastructure, and connections with other malware that the threat group used in the past.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
