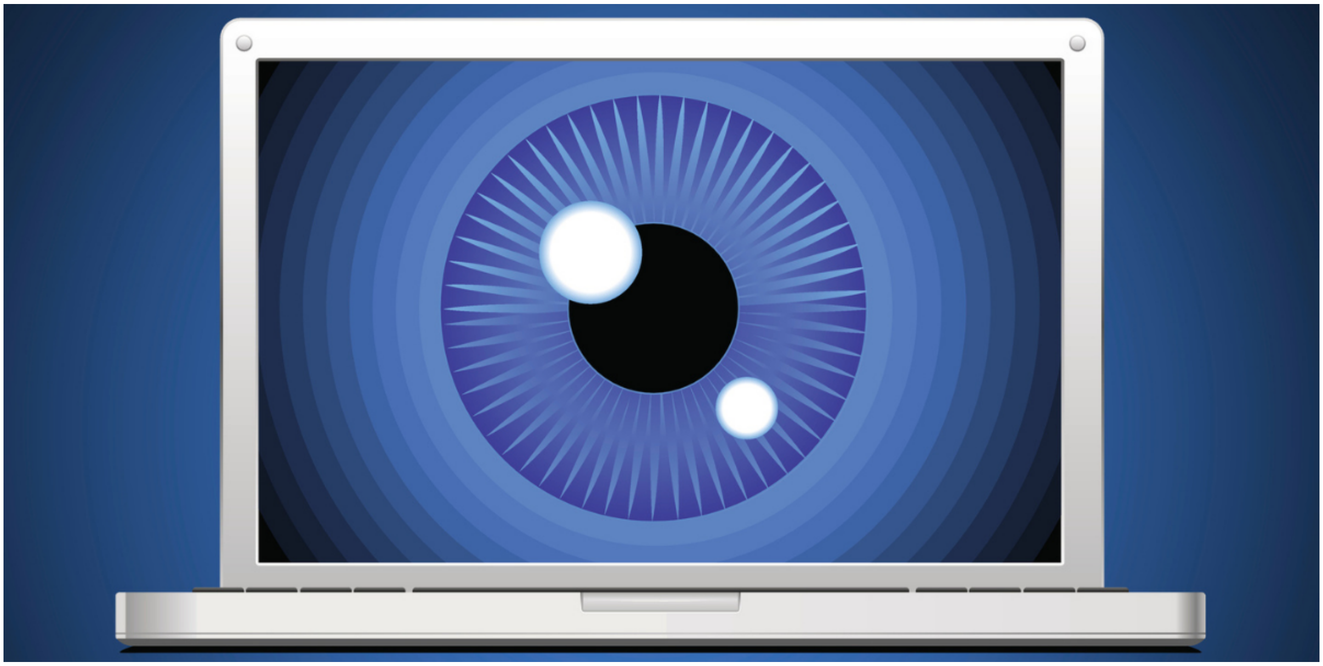
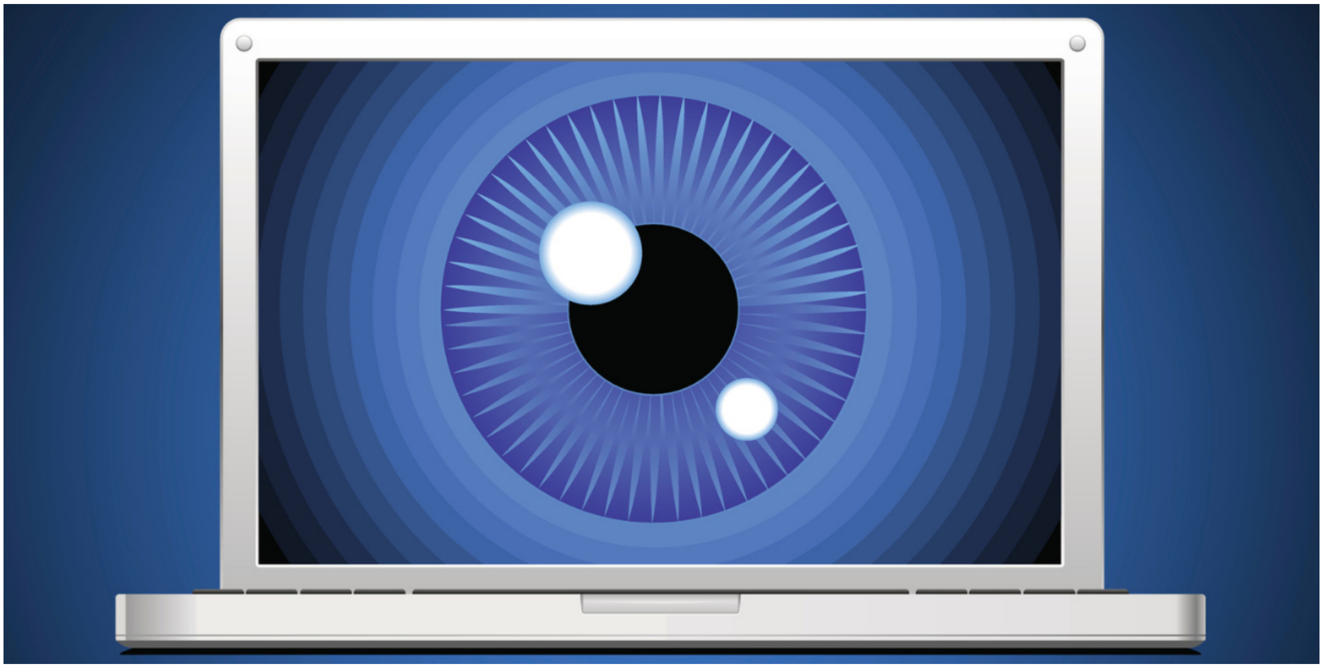
New Malware Arsenal Abusing Cloud Platforms in Middle East Espionage Campaign

cybereason.com/blog/new-malware-arsenal-abusing-cloud-platforms-in-middle-east-espionage-campaign





Written By
Cybereason Nocturnus

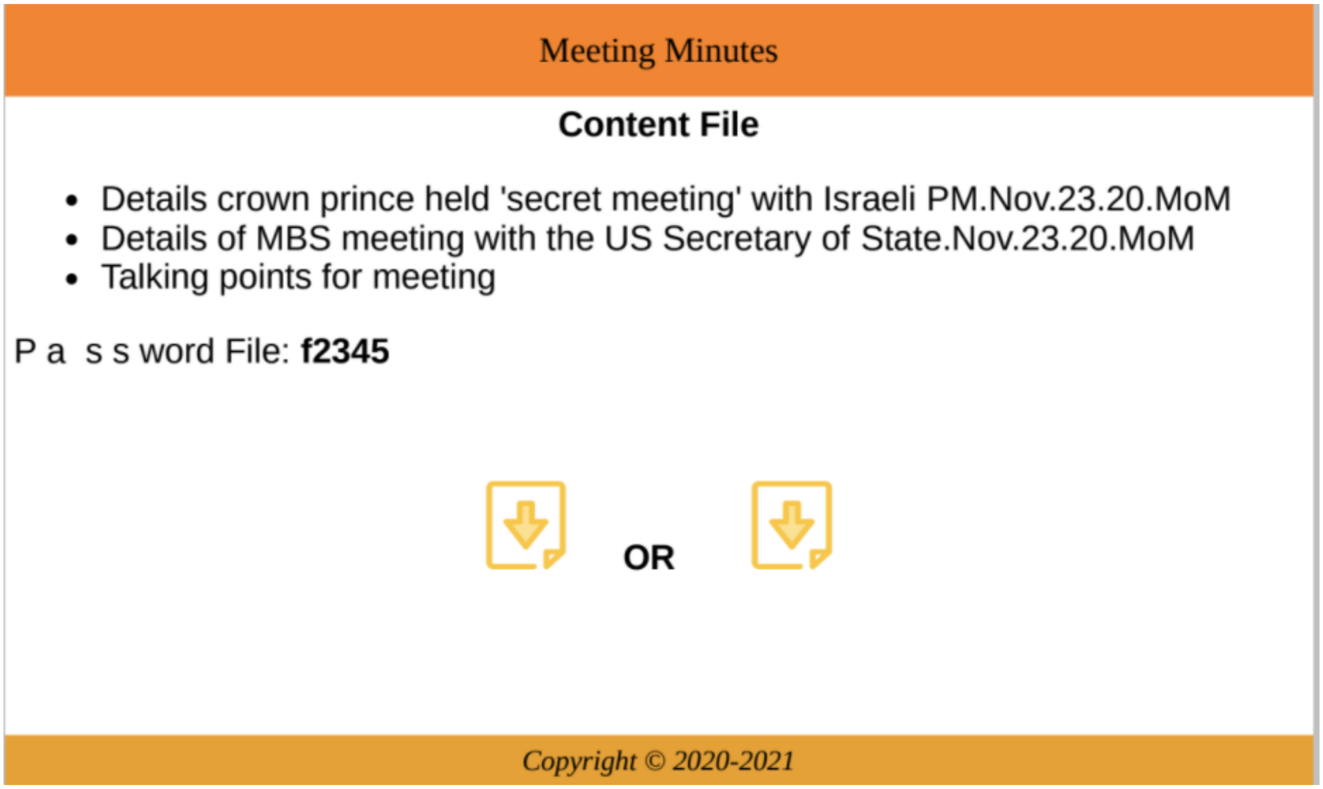
December 9, 2020 | 2 minute read

The Cybereason Nocturnus Team has identified an active espionage campaign employing three previously unidentified malware variants that use Facebook, Dropbox, Google Docs and Simplenote for command & control and the exfiltration of data from targets across the Middle East. The full report can be downloaded here (ungated) and the Indicators of Compromise can be downloaded using the link in the header at the top of this blog.

In February 2020, Cybereason researchers reported the discovery of the Spark and Pierogi backdoors that were assessed to be part of targeted attacks against Palestinian officials. The attacks were attributed to Molerats (aka The Gaza Cybergang), an Arabic-speaking, politically-motivated APT group that has operated in the Middle East since 2012.

The Cybereason Nocturnus Team has continued tracking the group, and in recent months detected a new campaign leveraging two previously unidentified backdoors dubbed *SharpStage*, *DropBook*, as well as a downloader dubbed *MoleNet*.

This latest campaign leverages phishing documents that include various themes related to current Middle Eastern events, including a reportedly clandestine meeting between His Royal Highness Mohammed bin Salman, Crown Prince of Saudi Arabia, the U.S. Secretary of State Mike Pompeo and Israeli PM Benjamin Netanyahu.



Meeting Minutes

Content File

- Details crown prince held 'secret meeting' with Israeli PM.Nov.23.20.MoM
- Details of MBS meeting with the US Secretary of State.Nov.23.20.MoM
- Talking points for meeting

Password File: **f2345**

OR

Copyright © 2020-2021

Content of the MBS-Israel.pdf document

Key Research Findings:

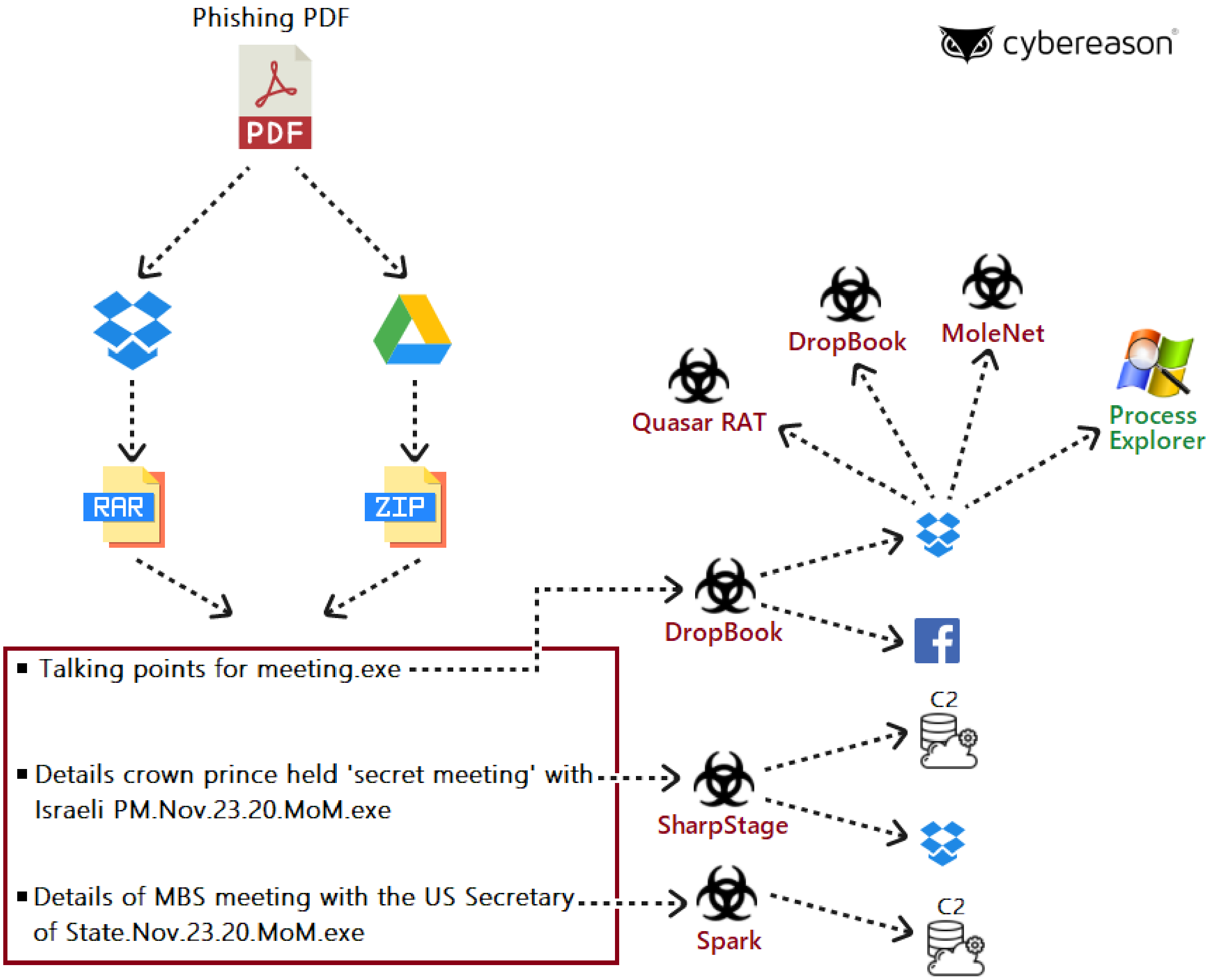
New Espionage Tools Developed by Molerats: Cybereason identified two new backdoors dubbed *SharpStage* and *DropBook,* as well as the *MoleNet* downloader, all of which can allow the attackers the ability to execute arbitrary code and collect sensitive data for exfiltration from infected computers.

The newly discovered *DropBook* backdoor used fake Facebook accounts or Simplenote for command and control (C2), and both *SharpStage* and *DropBook* abuse a Dropbox client in order to exfiltrate stolen data as well as for storing their espionage tools.

Political Phishing Themes: Themes used to lure the victims included the Israeli-Saudi relations, Hamas elections, Palestinian politicians as well as other regional events including a secretive meeting between His Royal Highness Mohammed bin Salman, Crown Prince of Saudi Arabia, the U.S. Secretary of State and the Israeli Prime Minister

Connections to Previous Middle Eastern Campaigns: The newly discovered backdoors have been observed being used in conjunction with the *Spark* backdoor previously attributed to Molerats. The attackers also used the new espionage tools to download additional payloads including the infamous open-source *Quasar RAT* that was used previously by Molerats.

Targeting Across the Middle East: The operation was primarily observed targeting the Palestinian Territories, UAE, Egypt as well as Turkey. Given the nature of the phishing content, Cybereason assesses that the campaign operators seek to target high ranking political figures and government officials in the Middle East.


Phishing PDF
PDF
cybereason
RAR
ZIP
Talking points for meeting.exe
Details crown prince held 'secret meeting' with Israeli PM.Nov.23.20.MoM.exe
Details of MBS meeting with the US Secretary of State.Nov.23.20.MoM.exe
DropBook
Quasar RAT
DropBook
MoleNet
Process Explorer
C2
SharpStage
Spark
C2

Molerats' latest campaign Infection Chain

The full report, titled *Molerats in the Cloud: New Malware Arsenal Abuses Cloud Platforms in Middle East Espionage Campaign*, is available for download 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.

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world’s brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus