Severity

High

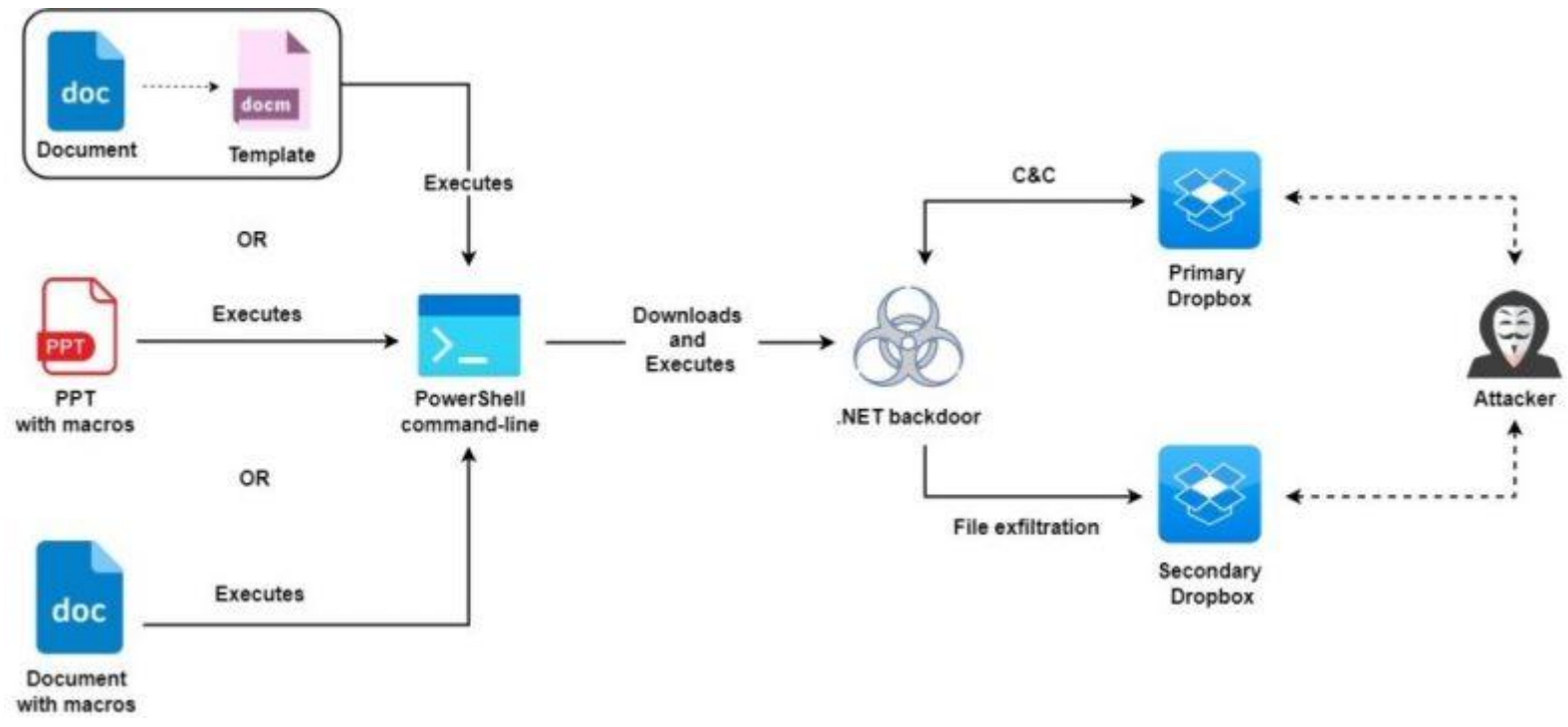
Analysis Summary

Molerats APT — also known as Moonlight, Extreme Jackal, and Gaza Hackers Team — have been active since 2012. They made headlines in 2012 when they conducted a cyberattack against Israeli government. The targeted nations expanded to include Palestine, U.S., and also the UK. Molerats is a politically motivated nation-state actor that is conducting cyber espionage using one new malware variant:

1. Nimble Mamba

NimbleMamba uses the Dropbox API for both command-and-control as well as exfiltration, suggesting its use in highly targeted intelligence collection campaigns.

Molerats use Dropbox, Google Drive, and other legitimate services to drop spyware for cyber espionage against the Middle East.



They use content written in the Arabic language related to the Palestinian conflict with Israel which encloses a macro that can execute a PowerShell command for fetching malware.

Impact

- Data Exfiltration
- Cyber Espionage
- Political and Economic Loss

Indicators of Compromise

MD5

- 0b40170fb946c76465cf7da1bfe0c563

SHA-256

- 31389963b4d49a85866bc0baeca8f1fa7be97655d3f37b23573e1727c03174a5

SHA-1

- 052e08c4ec75482708d2807644660f53d64ca565

Remediation

- Block all threat indicators at your respective controls.
- Always be suspicious about emails sent by unknown senders.
- Search for IOCs in your environment