MENLO SECURITY

☎ 650-614-1705
www.menlosecurity.com
✉ support@menlosecurity.com

Menlo Labs Threat Bulletin

Bulletin: 2022-04

Date: 03/17/2022

Name: QakBot

Classification: Highly Evasive Adaptive Threat (HEAT)

HEAT (Highly Evasive Adaptive Threat)

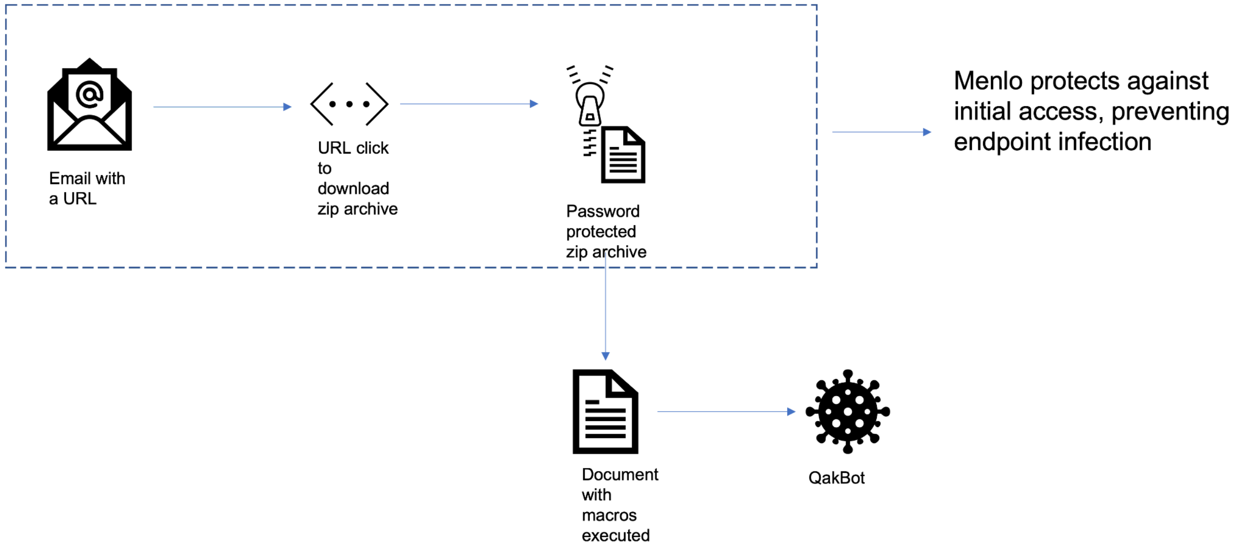
HEAT attacks use evasive techniques to avoid detection by standard malware detection engines. The current campaign uses the following evasive techniques

- The malicious file is an encrypted zip file and as such cloud based AV and Sandbox engines can not examine its content.
- The hosting domain SEHMBI[.]IN is classified as business and economy and uses a technique we track as LURE (Legacy URL Reputation Evasion)

Summary

- QakBot has shifted it’s tactics to now use password protected zip files to evade detection
- The second stage payload is Cobalt Strike
- The Menlo platform prevented this attack by blocking the archive file in the Isolation Core

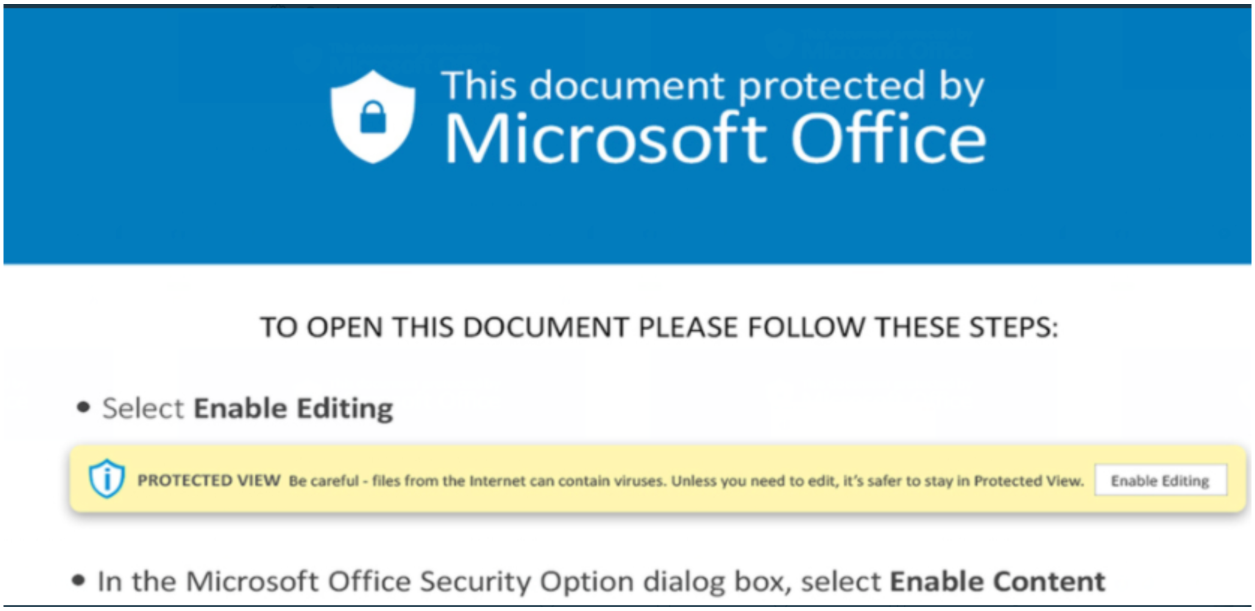
Technical Details


Email with a URL
URL click to download zip archive
Password protected zip archive
Menlo protects against initial access, preventing endpoint infection
Document with macros executed
QakBot

- An email with a URL pointing to a malicious zip file is sent to the victims
- The zip file is password protected
- Inside the zip file is a Microsoft Excel document with macros
- Opening the excel file on the endpoint, runs the macros and installs the QakBot malware
- The infected endpoint then downloads additional files from it's CnC, including the CobaltStrike payload

The screenshot below shows one of the malicious documents on the endpoint.

Menlo Labs Threat Bulletin



This document protected by Microsoft Office

TO OPEN THIS DOCUMENT PLEASE FOLLOW THESE STEPS:

- Select **Enable Editing**

PROTECTED VIEW Be careful - files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

- In the Microsoft Office Security Option dialog box, select **Enable Content**

Menlo Protection

Menlo labs is monitoring the threat and updating the platform accordingly with IOCs. IOCs in this campaign are currently being added to the product and are now categorized as malware. Customers are recommended to set their policy for threat categories, across isolated and application web requests, to block.

The Menlo cloud security platform has multiple content inspection engines that analyze and block such threats from reaching the endpoint. Attackers very often use encrypted archives to circumvent existing solutions. The Menlo platform opens up encrypted documents and archives in cloud containers, away from the endpoint. When a password is provided, the contents of the archive or the document are analyzed before letting it through the endpoint.

Customers can choose to avail the below detection technologies to be integrated into the content inspection engine, providing defense in depth on a single platform.

- AV Engines
- Sandboxes

In addition to the above detection methodologies, the Menlo platform provides an additional layer of security against zero days and new malware campaigns by opening documents in a “safe” mode and letting the customer download a safe version of the document

IOC

- CnC domains identified so far
    - communitybusinesses.info
    - Njmcdirectpay.online
    - Proteogenix.us
- URLs in emails
    - hxxps[://]sehmbi[.]in/essmaitcocccauauac/AS_2846778584.zip