BHKShield
Project in Ransomware
Presentation

BHKShield

Overview

- Front-end service:
  - Enabling the user to configure the service, user credentials and cloud storage provider
  - Notifies the user when needed
- Back-end service:
  - Manage multiple users and their credentials
  - Register for notifications from the cloud storage API
  - Process the events and detect
  - Remediate when needed
  - Notify
- Bonus points:
  - Detection accuracy
  - Manage multiple cloud storage providers
  - Add Windows 10 toast notifications
  - Add rollback function for the user
  - Protect SharePoint and OneDrive for Business

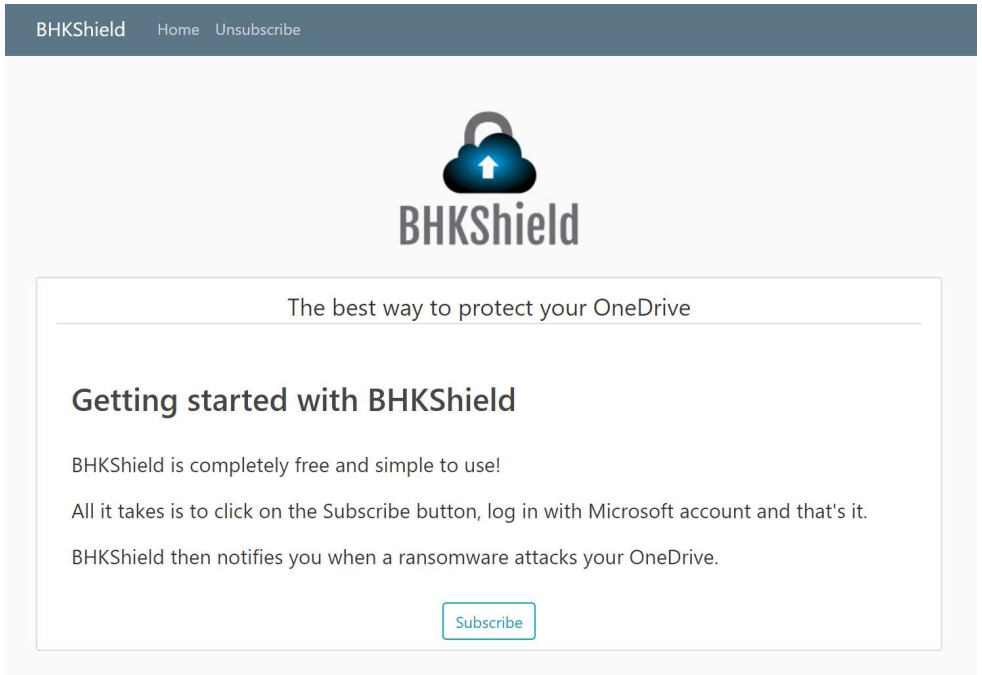
BHKShield

Detection Rules

- Extension black list
- Content blacklist
- Honeypots
- Entropy

BHKShield

Front-end



https://bhkshield-project.azurewebsites.net/

A python web application that uses Django framework.
The web app enables the user to subscribe to our service and deactivate the service as well.
Login is processed via Microsoft OAuth 2.0 API.

Responsibilities:

- Handles un/subscription.
- Handles inserting user files into our DB.
- Handles spreading honeypots into user's Drive.

BHKShield

Back-end

An Azure Function which uses webhook notifications in order to handle the processing of the changes in user's OneDrive to detect a ransomware attack.
When ransomware attack is occurring, the function notifies the user by e-mail.

BHKShield

Front-end

A python web application that uses Django framework.
The web app enables the user to subscribe to our service and deactivate the service as well.
Login is processed via Microsoft OAuth 2.0 API.

Responsibilities:

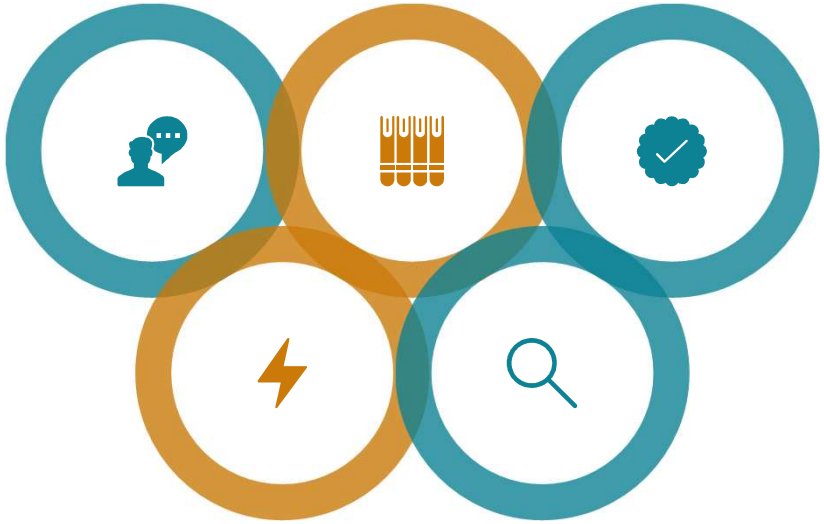
- Handles un/subscription.
- Handles inserting user files into our DB.
- Handles spreading honeypots into user's Drive.

BHKShield

Detection Rules

Honeypots

Black list



Entropy

Content Change

Extension Change

BHKShield

Black list

BHKShield uses two kinds of blacklists:

Ransomware extension blacklist

A list which consists of extensions that are known for ransomware attacks.

Ransomware file content blacklist

A list that consists of suspicious contents that might indicate of an encrypted file.

BHKShield

Honeypots

General Information

- Honeypots name is "__BHKShield.txt"
- Honeypots are stored in a different DB
- Every folder has a honeypot
- Not supposed to be changed by user

How do we use honeypots?

Based on the assumption that the user does not change the honeypots,
when notification of a changed honeypot is received, BHKShield will detect it as a ransomware attack and notify user

BHKShield

Entropy

Regular file

- Entropy threshold = 7.99

Compressed file

- Entropy threshold = 7.998

BHKShield

File Inspection

New file

- Check extension blacklist
- Check content blacklist
- Check entropy

Existing file

- Check extension blacklist
- Check content blacklist
- Check changed entropy

Maintain counter of suspicious files and total entropy change

BHKShield

Bugs
&
Drawbacks

Bugs

- Realistically, user can change the honeypots and it will lead to false-positive.
- The honeypots files are not removed when the user deactivates the service.

Drawbacks

- The content of the honeypots is fixed.
- Honeypots do not spread dynamically. When user create a new folder/deletes honeypots, honeypots do not spread there.
- Size of file does not come into consideration.

Video demonstration

Questions?

Thank You