Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Check Point SandBlast Mobile 2.71
For more about this product, see the SandBlast Mobile Product Page https://www.checkpoint.com/products/sandblast-mobile/

More Information

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 February 2018</td>
<td>First release of this document</td>
</tr>
<tr>
<td>22 February 2018</td>
<td>Android version release 2.71.0-RELEASE-3138</td>
</tr>
<tr>
<td>5 March 2018</td>
<td>Android version release 2.71.0-RELEASE-3140</td>
</tr>
</tbody>
</table>
2.71 Updates (iOS v2.71.3762, Android v2.71)

1. Dashboard Schedule Reports.

Schedule reports are generated each calendaring month or for the last 30 days, the report includes:

1. Device Status Snapshot
   - Active: 324
   - Promoted: 107
   - Inactive: 135

2. Active Device Risk Status Snapshot
   - Low: 34
   - Medium: 71
   - High: 163
   - NO RISK: 56

3. Device Status Over Time
   - 89 Added
   - 70 Activated
   - 85 Deleted

4. Device Activation Over Time

5. App Installations By Risk Level
   - Total: 953
   - High: 48
   - Medium: 110
   - Low: 788

6. App install Over Time

7. Network Attacks
   - 3 SSL Stripping
   - 31 SSL Interception
   - 1,300 Captive Portal Redirection

8. Network Attacks over time
9. SMS Phishing

10. SMS Phishing Over time

11. Device Security Settings Events

To register for the dashboard schedule reports dashboard admin needs to edit his personal profile settings by clicking on the profile setting icon and enabling the schedule report.

To get a onetime report on the last 30 days click the ‘Create’ button
2. iOS MDM profile dashboard detection

This feature is only relevant for dashboards which are configured to work without device management server or dashboards which have selected to install MDIS Profile.

The MDM profile detection is now done on the dashboard side so in case user have removed the MDM profile from his iOS device (iPhone/iPad) the dashboard will show an event and the device will pop up with a risk instructing the user to install the MDM profile.

3. Policy Setting for WIFI Network

MITM attack risk level can be configured by dashboard admin:
To edit the settings click on Settings-> Policy Settings -> WIFI Network

SSL Striping - MITM attack - intercepts all network traffic redirection from HTTP to HTTPS and "strips" the HTTPS call leaving the traffic as HTTP.

SSL Interception (Basic) - MITM attack - intercepts HTTPS traffic by using an invalid certificate that does not exist on the device's trusted certificates or not trusted by a root CA.

SSL Interception (Advanced) - MITM attack - intercepts HTTPS traffic by using a valid certificate that does not match the certificate of the server.
4. Man in the Middle Detection to External URLs

MITM attacks are detected by inspecting the communication from the device to a honeypot, in case an attacker drop the connection to the honeypot the MITM detection will fail to detect the attack.

Inspecting the connection to additional sites will make the MITM detection more robust, enabling to detect such targeted attacks where specific sites and not all traffic are mangled. It is recommended to add websites that are used by the organization for its day to day business.

5. MDM advance setting - App sync interval

App sync interval can be configured in the ‘Device Management Advance Setting’. App sync is the process of getting app list for iOS devices in the dashboard. The app sync interval needs to be in multiples of 10 min.

This configuration may be used in order to reduce the number of APIs to the MDM.
6. Runtime permission for devices running Android 6.0 (API level 23) or higher.

The version is released in gradual rollout; devices may not get the update immediately, full rollout is expected to be by 8 of March.

The new Android release now support runtime permission for devices running Android 6.0 (API level 23) or higher.
The new feature will only affect new installs. Users which will update to the new version will not notice the change.

New app installs will require the user to approve Phone permission on app launch, this permission is needed in order to get device IMEI and to auto register the device in case the dashboard is configured to work with a MDM server.
The app will not work without this permission. In case user does not approve the permission another message will be displayed that explain why this permission is needed, the app will stay at this state until the user approve the Phone permission.

Once the user approve the phone permission the app will try to auto register the user and get the dashboard security policy.
In case the security policy requires more permission, for example view SMS messages, the app will display a screen with all the permission needed.
In case the user did not approve the permissions displayed on the permission screen, the app will alert the user by raising the device risk, based on the dashboard policy and an event will be logged on the dashboard.

**Mobile Client Supported Platforms**

iOS: 8.x, 9.x, 10.x, 11.x

Android: 4.x, 5.x, 6.x, 7.x, 8.x.