iOS device Threat Hunting in SOC

Chintan Gurjar

Why!

- Threat hunting mainly focuses on systems that are built on Windows and Linux OS within many companies. Mature SOC divisions in many companies also monitor the security of mobile devices.
- Threats can be:
  - Insider threats (Company employees stealing, leaking confidential data)
  - Malware (Malware and rough applications stealing confidential data)
  - Unusual activity posed by user accidentally or legitimately.
- Today I am going to share a small checklist to let organisations know what things they can monitor for the iOS devices in their threat hunting division to ensure they are secure and not being compromised.
- *Here I have already assumed that any company who utilises this checklist have already security scanner/EDR agents installed on all of their iOS devices within their organization and they are receiving every type of logs from the devices.*
- *Splunk or similar would be handy to pick up threats.*

Checklist

1. Identify whether the signing of any code has tampered, infected or corrupted? Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed (Wikipedia). Identify whether an application's code signing has tampered or not.
2. Monitor whether the Bluetooth is enabled on any devices or not. It is unusual to see Bluetooth enabled on any of the iOS devices in the corporate organization. This can be used for any filesharing activity or mobile hotspot filesharing activity.
3. Identify whether the iOS device is jailbroken or whether there is any attempt to jailbreak the iOS device or not.
4. Users can download a configuration profile from a website or an email message in iOS 12.2 or later or in iPadOS, including profiles to enrol in Mobile Device Management. Users can install it by using the Settings app (Apple Support). Identify whether any new configuration is loaded on the iOS device.
5. Define keywords such as password, secret, key, email id, OTP, etc. Identify whether any content is copied to the clipboard, which contains such type of keywords that are potential for your organization?
6. Check for the certificate pinning on a regular basis to identify whether it has been compromised on any of the devices or not.

Checklist cont.

7. Monitor every DNS request generated on the iOS device. Compare with your organization's whitelist/blacklist policy and identify apps or users trying to navigate to any of the following:
   - Cloud file-sharing websites or apps
   - Remote administration websites or apps
   - Proxy/VPN websites or apps

   These are some of the indicators of malicious activities being performed in order to exfiltrate data from the device.
8. Incidents should be detected if there is an activity to wipe the device data or an attempt to disable/deactivate the security agents on the device.
9. Identify whether any iOS device or application common hacking/Pentesting tools are being used/installed or injected through any other processes. Some of the most common tools are:
   - OpenSSH, Syslogd, Otool, Cycript, nm, dump_keychain, class-dump, TrustME, Snoop-it, idb, Frida, Introspy, iRET, Clutch, Dumpdecrypted, plutil, xCON, theos, keychaindumper, BinaryCookieReader, memscan, appmon.