CERT-EU

Corporate Mobile Device Management system breach

Threat Memo - Date: 08/05/2020 - Version: 1.0
TLP:WHITE

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Cybercrime Cyberspionage	Unauthorised access	World	Corporate IT	A1

Key Points

- Researchers have discovered a case where a mobile device management (MDM) system has been abused to spread malware to a large number of mobile devices in an enterprise.
- The central role MDMs play in managing mobile devices gives them unique access potential in case they are breached.

Summary

On April 29, researchers of the security company Checkpoint reported[1] on a novel attack technique targeting a corporate environment using the mobile device management (MDM) system. In particular, the attackers managed to first infiltrate the enterprise network, moved laterally, took control of the MDM system and then used it to spread the Android malware Cerberus to at least 75% of the connected mobile devices.

Mobile Device Management systems provide a solution for controlling corporate or private devices of an organisation's personnel so they can be used for business purposes and access protected assets. They achieve this in a two-fold approach:

a) by installing and mandating specific applications known and trusted for exclusive corporate usage, and
b) by enforcing particular networking routes to reach business systems, that ensure encrypted transit while on the internet and traffic analysis and control when on the internal network (via intrusion prevention systems, data leakage prevention systems, etc.)

Additionally MDMs provide mobile device inventory and homogenization of operating system versions forcing necessary updates that users themselves could neglect to install. In this respect, MDMs are essential for ensuring the secure and monitored access of a mobile workforce to corporate systems.

In the event reported by Checkpoint the breach of the MDM led to the probably automated installation to most devices of a variation of the Cerberus Android banking malware. The particular variant has additional full remote access trojan (RAT) capabilities to log keystrokes, intercept messages (including SMS and 2-factor-authentication – 2FA), and remotely control the devices. It also steals Google authenticator credentials, Gmail passwords, and phone unlocking patterns.

Interestingly also, after acquiring initial consent from the user (due to a continuous pop-up), it can also mimic user interaction for menu choices and clicks. This way it executes a sequence of actions that connect it to the threat actor's Command and Control (C2) network, download additional modules, and activate data exfiltration as well as other surveillance actions.

The implications both for the individuals and the organisation are potentially severe:

- All personal and business information on the mobile device are exposed. Additionally banking access passwords as well as intercepting 2FA responses are available to the attacker.
- Administrators that may attempt to access infrastructure systems will reveal their passwords along with any 2FA token. In any case accessing such systems from the mobile devices offers a gateway for the attackers to these systems as well.

Comments

As a system with a central role in corporate IT, MDMs provide also a pathway to broad control of assets, namely the mobile devices of a big proportion of the personnel and possible access paths to critical infrastructure components.

In July 2018, researchers had discovered another case of an MDM being used to spy on a number of mobile devices in India[2] in the period 2015-2018. The attackers had replaced legitimate social networking and messaging apps with malicious versions.

The potential of abusing MDMs but threat actors to perform highly targeted espionage operations should also not be underestimated.

[1] https://research.checkpoint.com/2020/mobile-as-attack-vector-using-mdm/
[2] https://thehackernews.com/2018/07/mdm-software-hack-iphone.html