**DualToy Malware**

A recently discovered malware is said to be exploiting Android and iOS devices by stealing iCloud credentials and sideloading risky apps by gaining root privilege on Android devices.

Thanks to the sandboxing security controls of iOS, and the hardened operating system of Android; the attack has not been successful in many instances. Another reason for its failure is its explicit nature, which will result in its failure in most of present day attacks subject to the validity of a certificate.

Claud Xiao, a security researcher at Palo Alto networks says that the DualToy Trojan attacks windows systems that are authorized to work with iPhones, and targets users running customized Android ROMs by exploiting their Android Debug Bridge facility. Once the malware is successfully installed on an Android device, it starts downloading advertising applications and tries to gain rooting privilege in order to install other unsafe apps. When installed on an iOS device, it phishes username, password, IMEI, ICCD, IMSI, phone and serial numbers, and sends the complete stolen information to a remote server.

Windows machines that have Android Debug Bridge facility can actually facilitate the malware to gain root privileges as they run custom ROM and have more chances of being rooted. iOS and Android already put up a check many years ago to prevent similar kind of attacks like DualToy by necessitating user interaction for authorizing two devices to pair with each other. DualToy, however, considers all mobile devices connected to an infected PC to be under single ownership, and uses these already existing pairs for interacting with mobile devices.

Palo Alto has suggested organizations and users to install endpoint as well as network-based malware prevention tools, and to avoid connecting mobile phones through USB to untrustworthy systems. Organizations and individual users need to deploy similar means of iOS and Android application security essentials, create user awareness and carry out regular iOS and Android application security assessments.