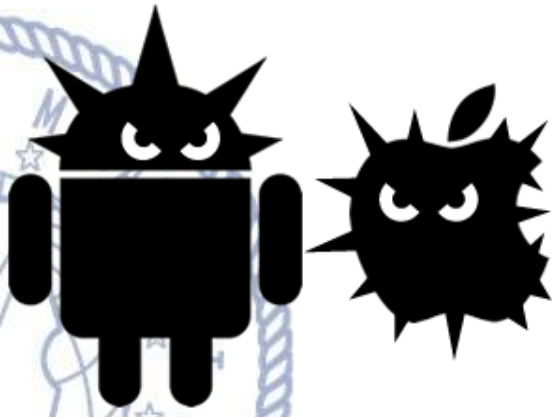
COMPUTER SECURITY BULLETIN

Risk/Impact Rating: Significant

< DualToy >

CSB17-004

Description:



DualToy is a Windows Trojan that is used by attackers to download malicious apps onto Android and iOS devices via USB connection. This is also known as "sideloading."

When a computer running Windows OS becomes infected by DualToy, ads begin to appear and browser settings on the system are altered.

DualToy performs the following activities on Android and iOS devices:

- Downloads and installs Android Debug Bridge (ADB) and iTunes drivers for Windows
- Uses existing pairing/authorization records on infected PCs to interact with Android and/or iOS devices via USB cable
- Downloads Android apps and installs them on any connected Android devices in the background, where the apps are mostly Riskware or Adware
- Copies native code to a connected Android device and directly executes it, and activates another custom to obtain root privilege and to download and install more Android apps in the background
- Steals connected iOS device's information including IMEI, IMSI, ICCID, serial number and phone number
- Downloads an iOS app and installs it to connected iOS devices in the background; the app will ask for an Apple ID with password and send them to a server without user's knowledge (just like AceDeceiver)

Recommendations / Solutions / How To's:

For PNP Personnel

- Use a firewall to block all incoming connections from the Internet to services that should not be publicly available;
- Disable autoplay;
- Turn off file sharing if not needed;
- Turn off and remove unnecessary services;
- Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses; and
- Turned off Bluetooth if not required. If it require, set to "hidden". If device pairing must be used, ensure that all devices are set to "Unauthorized". Do not accept applications that are unsigned or sent from unknown sources.

For Key officers and Technical Staff

- Enforce a password policy;
- Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task;
- When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application;
- If a threat exploits one or more network services, disable, or block access to, those services until a patch is applied;
- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services;
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files;
- Isolate compromised computers quickly;
- Perform a forensic analysis and restore the computers using trusted media; and
- Train employees not to open attachments unless they are expecting them.

References:

http://ae.norton.com/security_response/writeup.jsp?docid=2016-091322-3504-99&tabid=2

http://bestsecuritysearch.com/dualtoy-trojan-infects-android-ios-devices-via-usb/

https://www.cyber.nj.gov/threat-profiles/trojan-variants/dualtoy

http://researchcenter.paloaltonetworks.com/2016/09/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/