C18 A Case Study: Ransomware Containing Child Pornography Observed on an Android™ Mobile Device

Joseph Levi White, MS, US Army Criminal Investigation Laboratory, Digital Evidence-CFI, 4930 N 31st Street, Forest Park, GA 30297*

After attending this presentation, attendees will expand their general understanding of malicious software through the presentation of a case study involving ransomware observed on an Android™ mobile device.

This presentation will impact the forensic science community by providing an overview and example of forensic analysis performed on ransomware discovered on a mobile device.

Malicious software that is designed to cause harm to an electronic device (computer, mobile device, etc.) may be considered malware. There are multiple types of malware, such as programs to allow one user to control another user's device, programs to allow one user to spy on another, programs to display advertisements on an infected machine, and programs designed to disrupt a device's ability to function normally.

Ransomware is a type of malware designed to threaten the user unless a ransom is paid. Examples of ransomware include the WannaCry ransomware attack of May 2017, which affected several electronic systems worldwide. Ransomware threats may come in the form of data hijacking, data encryption (such as the WannaCry attack), or unwanted data disclosure (such as revealing private records or potentially embarrassing information to either the public or a specific individual).

This presentation follows the examination of a cellular phone submitted for examination to the United States Army Criminal Investigation Laboratory (USACIL). The device was owned by a soldier accused of downloading and possessing child pornography utilizing his Android™ cellular phone. Examination of the device indicated the soldier was actually the victim of a ransomware attack.

The particular ransomware located on the soldier's device was found within Android™ Package (APK) files typically associated with Android™ application installations. Forensic software allowed for unpacking the APK files to explore the contents more thoroughly. In this case, the APK files contained two Hypertext Markup Language (HTML) files (web pages). One of the files displayed obvious child pornography to the user of the device. The second displayed a fraudulent notice from the "DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION" imposing a $500 fine for the user's "ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES."

This presentation will include an overview of the case described above and explore the inner workings of the APK ransomware malware files.

The opinions or assertions contained herein are the private views of the author and are not to be construed as official or as reflecting the views of the Department of the Army (DA) or the Department of Defense (DoD). Names of commercial manufacturers or products included are incidental only, and inclusion does not imply endorsement by the authors, the Defense Forensic Science Center (DFSC), the Office of the Provost Marshal General (OPMG), the DA, or the DoD.

Ransomware, Malware, Examination

*Presenting Author