C20 An Anatomy of a Knockoff

Mark D. Guido, MS, The MITRE Corporation, 7515 Colshire Drive, Mclean, VA 22102; Justin Grover, MS*, The MITRE Corporation, 7515 Colshire Drive, M/S T240, Mclean, VA 22102; Eric Katz, MS, 4435A Beechstone Lane, Fairfax, VA 22033; and Kyle Anthony, MS, The MITRE Corporation, 7515 Colshire Drive, Mclean, VA 22102*

After attending this presentation, attendees will be more knowledgeable of the motivations to create knockoff mobile devices, the forensic characteristics of knockoff mobile devices, and how much they differ from the real thing.

This presentation will impact the forensic science community by directly analyzing a topic that is typically underresearched (i.e., knockoff devices) due to the international and criminal aspects of this described consumer supply chain problem.

This case study involves the technical examination of three international Samsung™ devices purchased through an official Samsung™ reseller. The devices ordered were Samsung™ Galaxy™ S5 phones, model SM-G900F. These devices have a Snapdragon™ processor and are typically used on mostly European carrier networks. Upon receiving the order, each devices' boxes were found to be in a pristine state in which they appeared to be factory sealed within the expected packaging, with stickers denoting the device model SM-G900F. During an examination of two of the devices while in Samsung's™ Download Mode, it was immediately noticed that the devices identified themselves as SM-G9006V and that each device had its warranty bits tripped. Further inspection while in the Android™ operating system revealed that the devices reported a device type of SM-G900F and the bootloader threw an error when an SM-G900F update file was attempted. Having believed that the research team may have been responsible for the warranty bit trips, the third device was unpackaged and inspected. It too exhibited the same behavior and its warranty bit was also tripped.

The Samsung™ GS5 SM-G900F and Samsung™ GS5 SM-G9006V have very similar hardware sets and it appears that in this case, the model SM-G9006V is used as a "knockoff" device for the model SM-G900F. The team was able to identify more knockoff devices with similar characteristics purchased from other authorized resellers, indicative of a more regional supply chain problem. Based on the research team's observations, the existence of a supply chain problem in both Europe and Asia manifesting itself through authorized Samsung™ resellers in the United States is assumed. This study focuses on the technical changes made to mask the original hardware and hypothesizes on the possible motivations for knocking off these particular device models. Using the Periodic Mobile Forensics tool suite, a suite of tools previously discussed at AAFS Annual Scientific Meetings, the research team examined these SM-G900F knockoff devices and will report on its hardware, the shape of the bootloader, the system partitions, and the state of the secure booting integrity. Results will be discussed.

Periodic Mobile Forensics, Android™, Knockoff