Daniella Boulos, Julianna Russo, Tyler Kaminer
November 14, 2024
NIST Case: Timeline of Cases
Computer Forensics

(1) Case Overview

The case revolves around a suspected data breach within Beat Step, focusing on the leakage of sensitive audio files, *Sample-1.mp3* and *Contraband.mp3*. Kamryn, an individual associated with the organization, displayed numerous suspicious behaviors that included account creation, software downloads, and interactions with unauthorized contacts. Over several weeks, Kamryn accessed, modified, and transmitted Beat Step's proprietary audio files through secure and unmonitored channels. The nature of the evidence strongly indicates premeditated data exfiltration intended for reputational gain, in this case, "street cred".

(2) Story of the Evidence

The timeline of Kamryn's actions shows carefully orchestrated steps designed to collect, modify, and transfer confidential files:

1. **Preparatory Actions (March 5 - March 10)**: Kamryn's initial actions involve setting up new accounts on platforms like Outlook and downloading file-sharing software, uTorrent and Thunderbird. This suggests she was laying the groundwork for unauthorized data transfers. The installation of uTorrent—a common file-sharing application—points to her intent to use peer-to-peer (P2P) networking to evade traditional monitoring systems.
2. **Acquisition and Modification of Files (March 21)**: Kamryn's activity increases on March 21, when an external email, *willis.gibbs@outlook.com*, sends her *Sample-1.mp3*. Shortly after receiving the file, Kamryn modifies it. She then accesses several files, including *List-1.txt*, *List-2.txt*, and *List-3.txt*, which could contain sensitive information or metadata she needed for the transfer.
3. **Data Transfer Through Torrents (March 21 & March 27)**: Kamryn uses uTorrent to initiate the transfer of *Sample-1.mp3.torrent* and, later, *Contraband.mp3.torrent*. Torrenting allows for decentralized data transfer, which could make it more challenging to trace file distribution or detect unauthorized recipients. Her repeated use of torrenting is an indicator of intent to share these files beyond authorized personnel, potentially to Threat Actors within a leaker network interested in proprietary content.
4. **Unauthorized Emailing and Sharing (March 27)**: Kamryn escalates her actions by sending emails containing audio files to unauthorized recipients, *realltrin@gmail.com* and *ram91284@hotmail.com*. In these emails, she implies her intent to share the files covertly, highlighting that they should deny obtaining them from her. This move indicates her awareness of the risk involved and her attempt to dissociate herself from the files after they left her possession.

5. **Final Modifications and Accesses (March 27)**: Kamryn makes several modifications to *Contraband.mp3*, which show her efforts to prepare the files for additional transfers or to obfuscate the origins of the content. The last accessed and modified timestamps indicate continued interaction with these files, reinforcing her role in actively managing and distributing the confidential materials.

The evidence paints a picture of someone with clear knowledge of file-sharing techniques, capable of evading detection by using external software and non-corporate email accounts. Kamryn's sequence of actions and choices of software—such as torrenting and Thunderbird—suggest she sought to minimize her digital footprint and leverage unmonitored avenues to accomplish her goals.

(3) Conclusions and Implications for Beat Step

The evidence collected points to Kamryn as the primary actor in this data breach, with a high probability that she intended to distribute confidential content to unauthorized parties. Her actions display an understanding of digital forensics obfuscation and suggest potential motives, including personal or reputational gain within an outside community.

For Beat Step, this case highlights the need for in-depth data security policies that include monitoring for the use of external file-sharing software, email filtering for external file exchanges, and real-time alerts for accessing or modifying sensitive files. The lack of restrictions on P2P applications and unmonitored email software contributed to Kamryn's ability to exfiltrate files, indicating potential gaps in Beat Step's internal security controls.

In conclusion, Kamryn's premeditated actions, choice of external software, and repeated file modifications serve as critical evidence of her involvement in the data leak. These findings support the recommendation for improved security measures and serve as a case study on the risks posed by insufficient monitoring of digital assets.