Summary

Note: This document is neither thorough in reporting findings nor polished. These compromises were made to rush the document to completion and quickly help Kent School and Law Enforcement in their investigations. Currently the document does not attempt to quantify victims and focuses on broad representations of illegal and inappropriate behavior.

In March 2023, Vancord was hired by Kent School to investigate computer activity for a recently separated employee, Dan Clery. The investigation began on March 15 and initially centered around the incident that led to employee separation. On February 21, Dan Clery was found to have visited an employee's ([redacted] system under the guise of technical support to create and steal an access token which provided access to [redacted] personal Google Photo Library. During this incident it was witnessed by [redacted] that her personal photos were being displayed on Dan's personal smartphone. Kent School has directed Vancord to investigate known Kent School systems involved in this incident to discover whether any other similar activity has occurred.

While investigating a Kent School system that was used to facilitate [redacted] personal photo access with the stolen token, further activities supporting photo theft from the Kent School community were discovered. A software management system which Kent School deployed to support the community was abused by Dan Clery to specifically target mostly female students to find and upload photos saved on their personal computers. Photos appear to be processed on these Kent School systems and likely stored in a cloud location not yet well understood. This activity involves at least dozens of victims and goes back to at least June of 2019.

A separate abuse of the software management system appears to be configuring 'back door' remote access on personal systems and accessing these systems over the network. A frequent activity appears to be probing the network to discover online systems and logging into them.

It was also discovered that Dan has accessed numerous student accounts in Google by abusing his highly privilege administrator access. This includes resetting passwords and generating 'backup codes' to defeat multi-factor authentication when needed. Observed activities with this account access include viewing email, taking photo or movie files and in some cases creating access tokens to Google Photo Library.

During systems review there is evidence found to support password hacking. Tools and techniques for recovering passwords from their encrypted forms were discovered. Review of web browsing history supports unauthorized student account access and showed signs of interest in software piracy/cracking and pornography.

By observation Dan Clery is highly skilled in many technical areas. Most activities around the handling of photos have been done carefully with deliberate process that leaves a small footprint which has been mostly deleted on February 21. Most evidence around this activity comes from copies of files that were likely missed in deletion activities and command history that was also not cleared. Student photos were discovered in a few locations that Dan likely missed cleaning up.