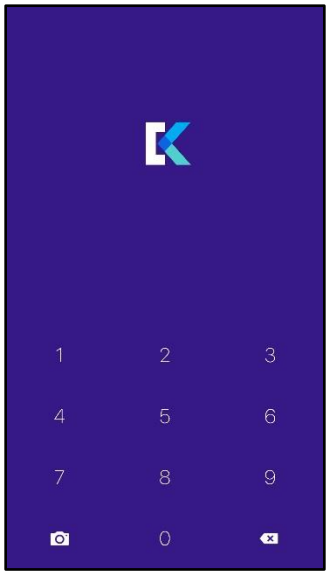
Background

Applications designed to hide photos, videos, and other files have been around for many years. Their availability and functionality has increased along with the popularity of mobile devices. These photo-hiding applications tout the ability to hide or "protect" files from unwanted viewers by importing the files into one or more albums which can only be accessed by entering the correct passcode. In some instances these applications also disguise their purpose by appearing to be another application. Because there are so many similar applications in this category we will focus not on one specific application but on the functions and features that are most common.

What are Photo-Hiding Applications?

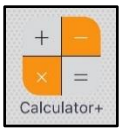
Photo-hiding applications were initially designed to protect one person's photos from others who may use the same mobile device. They quickly expanded to include videos and documents. After importing files into the application, users can gain access to the data only by providing the proper passcode. Depending on the mobile operating system used, the imported files (photos, videos, or other files depending on the application) may be deleted from their original location.

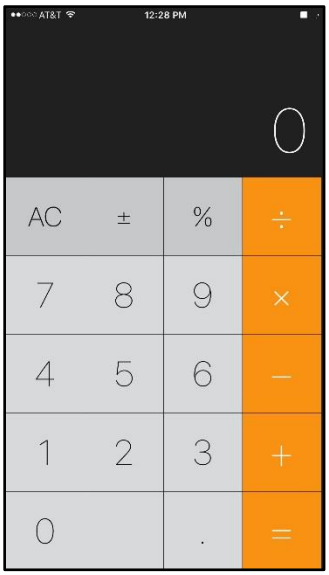


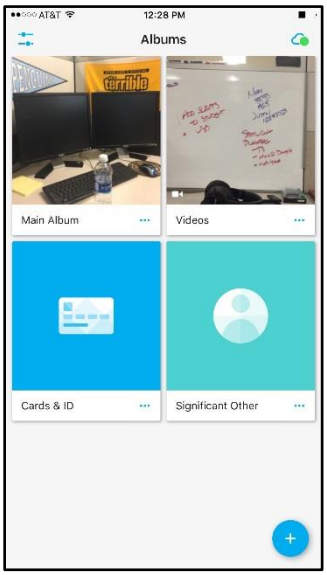
Most photo-hiding applications now share a very similar set of features. The two most common are decoy or fake passcodes, and break-in reporting. Other features could include private web-browsing, password recovery via email, cloud syncing, pattern lock in place of a passcode, and individual album locks.

These photo-hiding applications can be sub-categorized into two different types: ***obvious*** or ***covert***. Applications in the obvious sub-category don't employ any techniques to disguise their purpose. They are immediately identifiable by name and icon as applications designed to hide data, and users are presented with a passcode screen at launch. After entering the correct passcode the hidden data is revealed.

Applications in the covert sub-category try to disguise their purpose to prevent unaware users from identifying that photo-hiding applications are installed and in use. These covert photo-hiding applications masquerade as a benign application. Most emulate a calculator in order to obfuscate the passcode input by using a standard calculator keypad. The applications' names and icons look like the calculator application they try to emulate. When launched, users are presented with a fully functionally calculator. If the correct code sequence is entered the application interface shifts to reveal the hidden data; otherwise, the application functions as a standard calculator.







The ***decoy or fake passcode feature*** allows a user to set a secondary passcode that opens either an empty album or a secondary album of data separate from the data the user is really trying to protect. This feature is designed to trick someone to believe they found the hidden data by giving the impression that the data was successfully unlocked.

Break-in reporting tracks failed passcode attempts and alerts the user upon successful login that failed attempts have occurred. Most applications also take a picture using the front-facing camera to include with the failed break-in report so the user can see who was trying to gain access.

Importance to Law Enforcement

A number of incidents have been reported involving kids using these photo-hiding applications to hide data from their parents. In Canon City, CO, hundreds of high school students were recently caught using a photo-hiding application to trade nude photos of other students.[1] Because of incidents like this one, many news outlets have done reports on the dangers of these types of photo-hiding applications including the fact that most teens are aware of these applications—while their parents are not.[2]

Kids are not the only people using these applications to hide data. The presence of these photo-hiding applications may be an indicator of hidden pornography (both legal and illegal forms), or other illegal activities (such as drug dealing, stalking, and terrorist activities). As more and more people become aware of these photo-hiding applications, law enforcement must understand how they have been and can be used in the investigation of crime.

Investigative Information

Eleven photo-hiding applications were selected for testing and the results of the analysis of their forensic artifacts can be found below. Generally, these applications are designed to protect the data while the mobile device is in use.

Most of these applications DO NOT protect the data from forensic analysis. However, due to the number of different photo-hiding applications available, mobile forensic tools do not normally process the extracted artifacts automatically. Manual analysis of the extracted artifacts is required.

Due to the differences in the Apple® iOS® and Google® Android™ operating systems, how the original data is handled after being imported into the application varies. On iOS devices, only some of the photo-hiding applications offer to delete the original photos and videos after importing. If this option was selected, the data was removed from the Camera Roll and placed in the Recently Deleted album. These images can still be found in the Recently Deleted album for 30 days from time of deletion unless the user manually deletes them. If the application does not offer to delete the original photos and videos, they can still be found in the Camera Roll unless manually deleted by the user.

On Android devices, the original photos and videos are actually moved from Photos and placed in the application's photo storage location. The original photos and videos are NOT available for viewing outside of the hiding application.

Information Retrieved from an iOS Device

The Cybercrime Section with the National White Collar Crime Center (NW3C) downloaded, installed, and imported photos and videos into six different photo-hiding applications on an Apple iPhone 6s Plus® model number A1524 running iOS v 10.1:

- Keep Safe Photo Vault v7.9 (KeepSafe Software Inc.)
- Private Photo Vault v8.5 (Legendary Software Labs LLC)
- Private Photo Vault v5.5.7 (Qiwen Zhang)
- Calculator Vault v1.5 (KeepSafe Software, Inc.)
- Calculator+ v1.6 (Zero Cool)
- Secret Photo Calculator v2.2 (One Wave AB)

The forensic examination machine was an Apple MacBook Pro® running OS X® v10.11.6 – El Capitan and a VMWare Fusion virtual machine running Microsoft® Windows® 10 Professional. A logical extraction was performed using BlackBag Technologies® BlackLight® v2016.2.1 and MSAB® XRY® v7.1. BlackLight and XRY produced identical results during the examination of each application. Both mobile forensic tools were able to extract the location where each photo-hiding application was installed (/mobile/Applications/%application_name%).

The photos and videos that were imported into the applications, as well as the images that were taken by those photo-hiding applications that offered break-in reporting, were able to be recovered from all of the tested applications except Keep Safe Photo Vault and Calculator Vault. Both of these applications are from the same developer (Keep Safe Software Inc.) and the imported photos and videos were encrypted.

Information Retrieved from an Android Device

The Cybercrime Section with the National White Collar Crime Center (NW3C) downloaded, installed, and imported photos and videos into five different photo-hiding applications on a Samsung® Galaxy S7® model number SM-G930U running Android 6.0.1:

- Keep Safe Vault v7.11.0 (Keep Safe Software Inc.)
- Photo Safe v2.0.4 (Slickdroid)
- Private Photo & Video Locker v7.1 (Kohinoor Apps)
- Kalculator v7.11.0 (Keep Safe Software Inc.)
- Calculator Vault v9.3 (Sure Applications)

The forensic examination machine was an Apple MacBook Pro running OS X v10.11.6 – El Capitan and a VMWare Fusion® virtual machine running Microsoft Windows 10 Professional. A logical extraction was performed using MSAB XRY v7.1. XRY was able to extract the location where each photo-hiding application was installed (varied based on application).

The photos and videos that were imported into the applications, as well as the images that were taken by those photo-hiding applications that offered break-in reporting, were able to be recovered from all of the tested applications except Keep Safe Vault and Kalculator. Both of these applications are from the same developer (Keep Safe Software Inc.) and the imported photos and videos were encrypted.

The photos and videos imported into Photo Safe were recovered. However, the application modifies the first 10 bytes of each file imported to prevent access from outside of the application. By replacing the first 10 bytes with the first 10 bytes of a standard image or video of the proper type (PNGs and MP4 in our test sample), access to the photos and videos was restored.

Feedback

For additional information or suggestions please contact cyberalerts@nw3c.org

Sources

[1] McKee, Chris. "Photo hiding apps catching students, parents attention." *KRQE.com.* LIN Television Corporation, a Media General company. 25 Jan. 2016 Web. 21 Nov. 2016

[2] Casey, Pamela. *Does your child have this app – Calculator%?* Prod. Blount County District Attorney-41st Judicial Circuit, 2015. *Facebook.* Web. 22 Nov. 2016

This project was supported by Grant No. 2015-BE-BX-0011 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Photo Credits: "113166020 Copyright Ammentorp, 2016 Used under license from Bigstockphoto.com", "120510959 Copyright Ksander, 2016 Used under license from Bigstockphoto.com"