Background

Dust©, formerly known as Cyber Dust is an application available on both Android™ and iOS© backed by Mark Cuban and owned by Radical App, LLC. Its motto "dust - a safer place to text" was designed with privacy is mind after Mark Cuban sat by during a hearing where his "private" messages were read back and used against him. How Mark Cuban solved this problem was to make message erase after 24 hours (Auto-Dust), immediately after a user reads the message (Dust), at the user's discretion after sending (Dust) and by not showing who said what (No-Proof Screenshots).

> *"With texts, emails, snaps, tweets, you lose control and ownership of the message the minute you hit send. The person you send it to, or the platform takes ownership, forever"*
>
> *– Mark Cuban*

What is the dust Application?

Dust is a communication based application with some social networking components. To create a Dust account, a user must be older than 13, and must provide a phone number and optional email address for password recovery. Users can allow Dust to search through their contacts or manually search for a user based on a handle. Once they have located someone they would like to talk to, the user sends them a message and carries on a conversation, assured their messages will be private based on Dust's messaging and encryption models.

- **Auto-Dusting:** *Messages automatically delete after 24 hours or as soon as they're read.*
- **Dust(ing):** A user manually deletes a message, removing it from the recipient's phone, after the message has been sent.
- **Encrypted:** *Messages are encrypted and stored in RAM on Dust's servers and are encrypted in both direct messaging and public posts.* Dust provides detailed information about its *Encryption Model.*

- **No-Proof Screenshots:** *The sender's identity is hidden in 1-to-1 messages and Dust will detect and notify the user if any screenshots are taken[1]. Figure 1 shows an example in which a No-Proof Screenshot was taken. A notification appears (in orange text), and the application obscures the identities of both sender and recipient—unlike a standard SMS.*

  According to the Dust FAQs, the user's ability to take screenshots depends on the device's operating system

  - **iOS:** *Users have the ability to take screenshots due to Apple's decision to prevent applications from blocking screenshot capabilities on iOS devices. If a user takes a screenshot of your message, you will be alerted that a screenshot has been taken.*
  - **Android and Windows:** *Users cannot take screenshots. In the event a screenshot is taken, no names appear in the window, rendering messages without context.*[2]

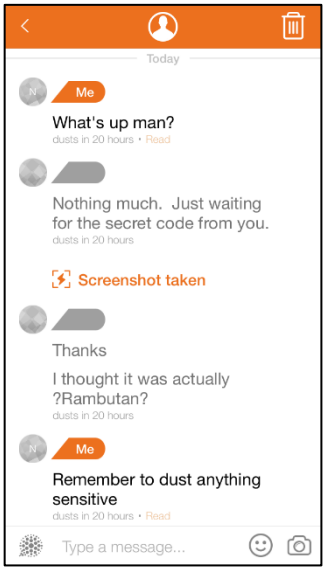

Figure 1: No-Proof Screenshots

The social networking component Dust offers is the ability to connect with people and businesses in certain industries. Each entity has a public feed, where they can share a post from someone else or post something original. Users can search entities based on categories and share posts, reply to posts, or add an entity to their contacts—which allows that entity's posts to appear in the user's public feed. Once added, *Figure 2* shows the entity's posts will appear in the user's Public feed. This feature is similar to how Facebook© and Twitter© work.

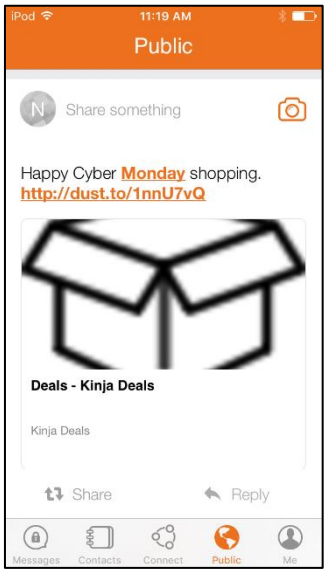

Figure 2: Public Feed

Importance to Law Enforcement

Dust is like any other communication application with privacy and security in mind. The information communicated through this application is protected by the messaging and encryption model. In order to gather the content of messages sent on Dust, law enforcement must have direct access to the sender's or recipient's device within 24 hours after the messages were sent.

Investigative Information

Below are pieces from Dust's privacy policy related to serving legal process and the information that is collected by Dust. This subscriber information collected could assist law enforcement by

providing additional identifying information about the target or a potential location. The information not available is the actual content from a message.

Legal requests

Legal process can be served via a physical address or email address:

ATTN: Customer Service 2233 Barry Ave. Los Angeles CA 90064

info@usedust.com

Information We Collect

We collect information you provide directly to us when you create your account. This may include your username, password, email address, phone number, age and any other information you choose to provide. With your authorization, we may also have access to your contact list(s) (e.g. so you may find friends) or photo roll(s) (e.g., so you may send photos).

Information collected automatically

We may collect usage Information, including time, date, sender and recipient of message, the number of messages sent and received, and the amount of time you spend on Dust. We may collect information about your use of our websites, including your browser type and language, access times, pages viewed, your IP address and the website you visited before navigating to our websites.

Cookies and automated information collection

When you access the Service, We collect certain technical information in order to analyze the usage of our Sites and Services and provide a more personalized experience. We and service providers acting on our behalf, such as Google Analytics, use Log Files and tracking technologies to collect and analyze certain types of technical information, including cookies, IP addresses, device type, device identifiers, browser types, browser language, referring and exit pages, and URLs, platform type, the number of clicks, domain names, landing pages, pages viewed and the order of those pages, the amount of time spent on particular pages, and the date and time of activity on our application, and other similar information. In some cases, we will associate this information with your user ID number for our internal use.[3]

Information Retrieved from an iOS Device

The National White Collar Crime Center (NW3C) Cybercrime Section downloaded, installed, and used Dust version 3.1.0.266 on an Apple iPod Touch 5 model (A1421) running iOS version 9.3.5. The test machine was running MacOS Yosemite 10.10.5, a logical extraction of the device was completed using BlackBag's BlackLight version 2016.2.

The artifacts recovered during the logical extraction came from the **private/var/mobile/Applications/com.mentionmobile.cyberdust** folder. Examining the folder provided two files of interest. The first file, **default.realm** was located in the subfolder *Documents.* This file contained a contact list (*Figure 3*) to include names and numbers from the phone and if the user had added them to their contacts through dust. If the user looked at someone's bio, searched for an entity or even in the user's public feed, the information can appear in this file.

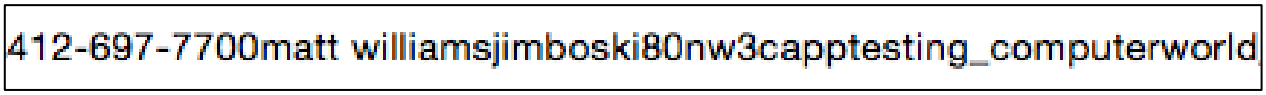

Figure 3: Contacts from default.realm

The second file, **com.mentionmobile.cyberdust.plist** was located in the subfolders *Library/Preferences*. *Table 1* shows four keys that stood out: date and time when the application was first used, the user name (*nw3capptesting*), what appears to be a unique user id and the user name again

Key	Type	Value
GAIFirstInitTimeStamp	Date	2016-11-22 15:31:24
RAUserLogginInAccountLookupIndentifierInDefaults	String	nw3capptesting
userIdInDefaults	String	58347075e4b0e96c5222ef2
userNameInDefaults	String	nw3capptesting

Table 1: Relevant Keys from com.mentionmobile.cyberdust.plist

On a second test machine running Windows 8.1 Enterprise, a logical extraction was used with MSAB's XRY 7.1 and the same information was found and verified to be the same.

Information Retrieved from an Android Device

The NW3C Cybercrime Section downloaded, installed, and used dust version 3.1.1 on a LG Nexus 5 model D820 running Android version 6.0.1 Marshmallow. The first test machine was running Windows 8.1 Enterprise. A logical extraction was used with MSAB's XRY 7.1 showed the

application was an installed application with a package name of **com.radicalapps.cyberdust** Other than this breadcrumb, there wasn't any pertinent data recovered. The second test machine was running MacOS Yosemite 10.10.5. A logical extraction was used with BlackBag's BlackLight Version 2016.2 but no pertinent data was recovered.

Feedback

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

Sources

[1] Dust. (2016, November 28). *Homepage*. Retrieved from Welcome|Dust|A safer place to text: https://www.usedust.com/
[2] Dust. (2016, Novemeber 28). *FAQ*. Retrieved from Frequently Ask Questions|dust|A safer place to text: https://www.usedust.com/faqs#does-cyber-dust-prevent-screenshots
[3] Dust. (2016, November 28). *Privacy Policy*. Retrieved from Privacy Policy|Dust|A safer place to text: https://www.usedust.com/privacy-policy

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: "86019758 Copyright robuart, 2016 Used under license from Bigstockphoto.com", "61830467 Copyright eric 1513, 2016 Used under license from Bigstockphoto.com"

©2016. NW3C, Inc. d/b/a the National White Collar Crime Center. All rights reserved.