12 March 2015 CFIX@ocfl.net | 407-858-3950 Bulletin #: 15-03-09

# Cyber Intelligence Bulletin

**Central Florida Intelligence Exchange**

Brevard ⋆ Indian River ⋆ Lake ⋆ Martin ⋆ Orange ⋆ Osceola ⋆ Seminole ⋆ St Lucie ⋆ Volusia

## (U) Darkleaks "Online Black Market"

### (U) Scope

(U//FOUO) This bulletin was created by the Central Florida Intelligence Exchange (CFIX) in order to address ***Darkleaks***, a new service where individuals can buy and sell information anonymously. The CFIX bases its analysis in this bulletin from open source reporting and internet postings with varying degrees of reliability. This information is intended to support local, state, and federal government agencies along with other entities in developing / prioritizing protective and support measures relating to an existing or emerging threats to homeland security.

### (U) Overview

(U//FOUO) In January 2015, DarkLeaks was launched in its early stages of testing. Its founders Peter Todd and Amir Taaki created DarkLeaks as a way to anonymously distribute sensitive information. Darkleaks is a decentralized black-market where individuals can sell information for the electronic currency known as BitCoin. The software was created with the intent of being decentralized to allow no identity, no central operator, and no interaction between sellers and buyers.

(U//FOUO) Specific examples of information that can be bought and sold include:

- Hollywood movies
- Trade secrets
- Government secrets
- Proprietary source code
- Industrial designs like medicine or defense
- Zero day exploits
- Stolen databases
- Proof of tax evasion
- Military intelligence
- Corruption

### (U) How it works

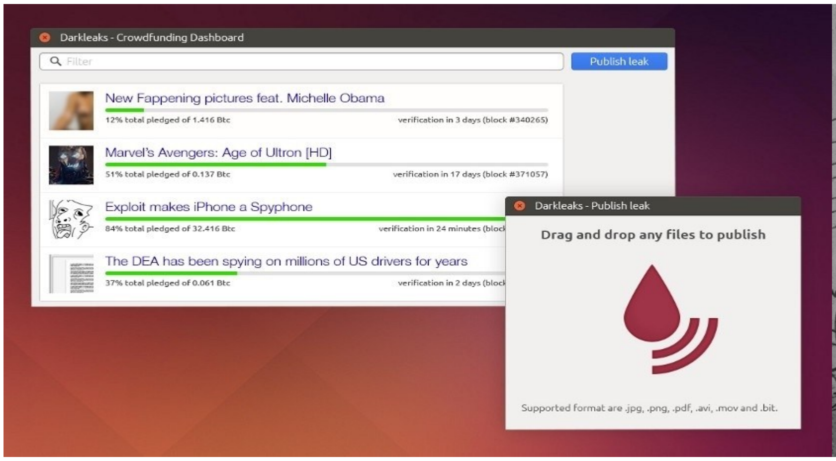
(U//FOUO) Currently, the only way to access DarkLeaks is from the popular code sharing website GitHub, where the source code for the program can be found. Before users can run the program, they must have PyQt4 installed on their device. PyQt4 provides an attractive and easy-to-use interface for the user. According to the first article published on Darkleaks, the document is broken up into segments. Each of these segments is then hashed and a Bitcoin address is generated using the hash as the secret key. This secret key is encrypted with AES256. From this public key, a new key is generated to encrypt the segments. The encrypted segments are released for public download with the list of Bitcoin addresses.

**HANDLING NOTICE:** This information is the property of the **CFIX** and may be distributed to federal, state, tribal and local law enforcement, DoD and U.S. Intelligence Community personnel on a need-to-know basis. This document contains sensitive information **FOR OFFICIAL USE ONLY** that cannot be released to the public, the media, or other personnel who do not have a valid "need-to-know" without prior **CFIX** approval. **Further distribution without CFIX authorization is prohibited.**

(U//FOUO) Darkleaks provides an authenticity mechanism, which allows the community to verify the accuracy of the document. Once the seller announces the document, they choose a date and number of "chunks" or segments to be released. Random numbers are then chosen based on the Bitcoin block hash which unlocks the number of chunks selected by the seller. The community can view these chunks to determine if they would like to purchase the information.

(U//FOUO) If the buyers from the community are satisfied with the product and its' authenticity they start to bid. Buyers send Bitcoins to the Bitcoin addresses that were provided when the chunks to preview the information were released. When the seller is satisfied with the amount of Bitcoins received, they claim them. Bitcoin was designed in a way that once the seller claims the Bitcoins, they must release the public key to allow buyers to decrypt the document.

(U//FOUO) The seller cannot pre-choose the segments that are released. This prevents the seller from providing false addresses to cheat the buyer. Buyers can then verify the addresses are correct and then the segments can be decrypted. This creates an authenticable and trustless mechanism for selling information on the decentralized black market.


Darkleaks - Crowdfunding Dashboard

New Fappening pictures feat. Michelle Obama
12% total pledged of 1.416 Btc verification in 3 days (block #340265)

Marvel's Avengers: Age of Ultron [HD]
51% total pledged of 0.137 Btc verification in 17 days (block #371057)

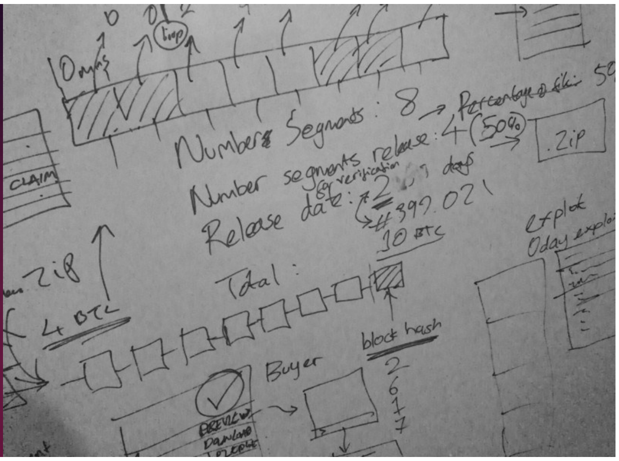
Exploit makes iPhone a Spyphone
84% total pledged of 32.416 Btc verification in 24 minutes (block

The DEA has been spying on millions of US drivers for years
37% total pledged of 0.061 Btc verification in 2 days (block

Darkleaks - Publish leak

Drag and drop any files to publish

Supported format are .jpg, .png, .pdf, .avi, .mov and .bit.



## (U) Outlook and Implications

(U//FOUO) The purpose of this program is to be able to sell and purchase sensitive information while keeping the seller's identity anonymous. In recent years, sensitive information that belonged to the United States government was leaked without incentives and the leaker was identified. Darkleaks allows for individuals the opportunity to leak sensitive information for pay and remain completely anonymous. As use of this program increases, it is likely we could see a rise in sensitive information being leaked from unidentifiable sources.

## (U) Reporting Notice

(U) The Central Florida Intelligence Exchange is providing this information for situational awareness. **For additional information on this product, or to report suspicious activity, please contact the CFIX at (407) 858-3950 or** CFIX@ocfl.net.

(U) Entities and agencies outside of the Central Florida region should report suspicious activity to the appropriate law enforcement agency and their regional or state fusion center.

(U) **Tracked by:** HSEC-1.1, HSEC-1.5, HSEC-1.8

## (U) Sources

(U) hxxps://github.com/darkwallet/darkleaks/blob/master/EXPLANATION
(U) hxxps://medium.com/@ZozanCudi/darkleaks-information-blackmarket-1ee5ac28c892

## (U) Glossary

BitCoin: Peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network.

AES256: The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption. The AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. Key size is unlimited, whereas the block size maximum is 256 bits.

PyQt4: PyQt is one of the two most popular Python bindings for the Qt cross-platform GUI/XML/SQL C++ framework (another binding is PySide).PyQt developed by Riverbank Computing Limited. Qt itself is developed as part of the Qt Project