STAR FORCE®

StarForce Leak Investigator

The application for investigating leaks of documents protected by StarForce Content Enterprise solution

Nowadays Challenges

In today's world, information is the most valuable product that can be bought, sold, exchanged, or even stolen.

Despite the actions taken in the field of the IT security, there is a possibility of leaks of protected documents as a result of unscrupulous or careless actions of the company employees.

Documents can fall into the hands of unauthorized persons even with imposed restrictions on printing or sending - there is always a chance that an attacker will take a photo of a document from the screen of the device on which it was being used.

StarForce Leak Investigator

The **Leak Investigator** module in the **StarForce Content Enterprise** system by "Protection Technology" company (Russia) allows you to determine by means of using a compromised document (a photo of a protected document or a scan of a printed copy), on which computer or mobile device this document was opened at the time of stealing. This makes it possible to identify the persons responsible for the leak.

Each time a protected document is opened or printed, the **StarForce Content Enterprise** system saves information in the access log (IP address, user ID, date and time, etc.), which allows you to track who and when performed the specified actions with the document. The identifier of the entry in the document access log using **steganographic techniques** is embedded in the document image displayed on the screen or printer. The steganography is implemented by using small shifts of individual words or other text blocks in the document.

The **StarForce Leak Investigator** compares the compromised document copy with the protected original document and allows you to determine the encoded identifier of the entry in the access log and thereby detect the source of the leak.

Operational Principle

Each time a document is opened on the user's computer or mobile device, an access request is sent to the server and a unique operation number is assigned.

This number is present in the document in 2 forms:

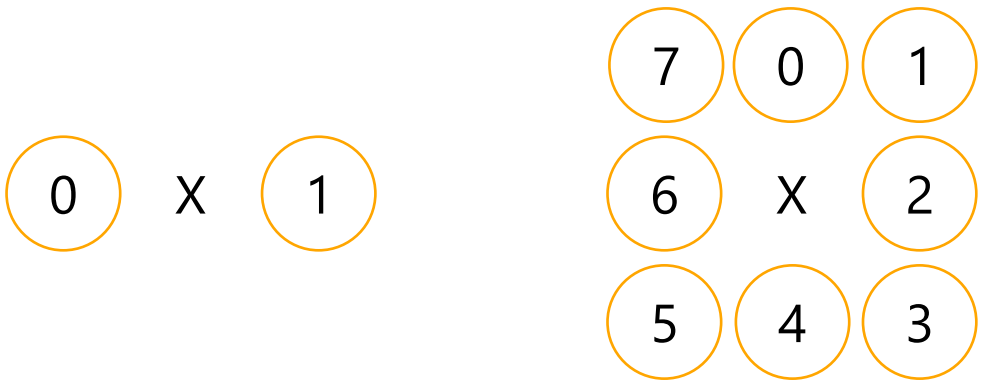
1. Watermark on the document
2. Coded number, implemented by means of using the steganography method (microshifts of different parts of the document)

The Document Encoding Process

1. The number of the document access operation is represented as a 32-bit binary number.

2. When protecting a document, blocks of text or images (words, paragraphs, diagram elements, etc.) are automatically selected on its pages. For each block, shifts are made in two or eight directions.

3. Each shift encodes one or three bits of a binary number. A three-digit binary number is converted to an octal number that determines the direction of the shift (see the figure below).



The Leak Incident Investigations

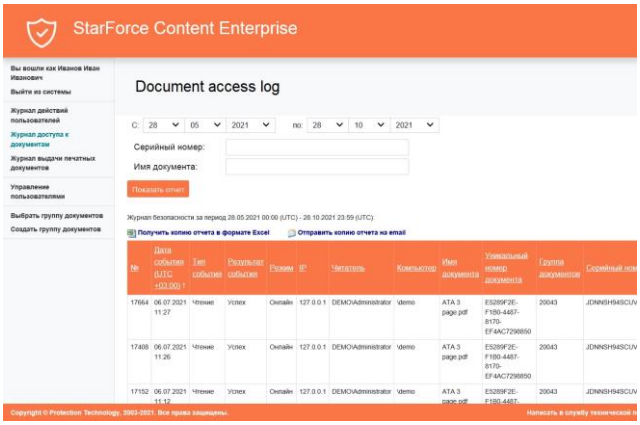
When a document is opened or printed, the new operation number is recorded in the access log, which is available only to the administrator. If the document access number is visible on the copy of the compromised document, you can find the activation record in this log.

If the number of the document access operation is not visible (for example, it is smeared on the screen photo or the document is only partially present), the steganography technology is used to investigate the source of the leak. The document access operation number is determined by comparing the original protected (encrypted) document and the compromised copy.

By using the overlay implemented in the program, you can set encoded shifts, get a number encrypted in binary form, use it to restore the operation number itself and find a correspondence to it in the document access log.

After comparing the compromised document and its original, the administrator receives a unique code that identifies the leak channel.

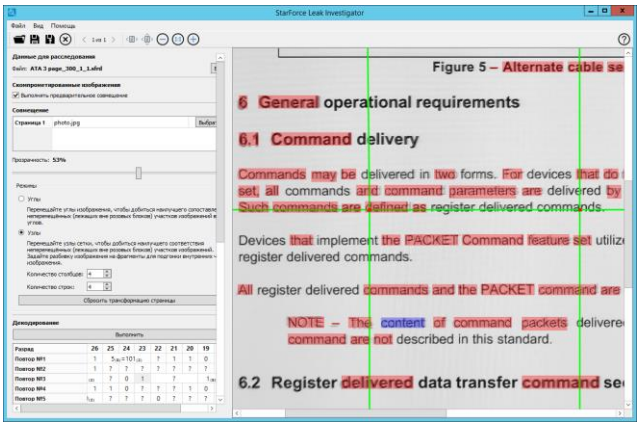
The Admin Interface



The image shows the interface of the **StarForce Content Enterprise** document access log, which collects all information on the use of protected documents.

The interface allows you to see the history of the document use, manage user rights, assign and revoke permissions for a single document or a group of documents.

There is also a database of unique access numbers available.



The image shows the **StarForce Leak Investigator** interface at the time of investigation in order to identify the serial number of the document by using the steganography technology.

The blocks of text with shifts are highlighted in pink, by which the program will set the number of the document access operation.

About us

The **"Protection Technology"** company, which has been releasing its products under the StarForce brand since 2000, creates solutions for protecting IT infrastructure from targeted attacks, protecting information from illegal copying and distribution, as well as means of code obfuscation and data encryption.

More than **70 million licenses** have been sold under the **StarForce** trademark worldwide. Many large Russian and well-known foreign companies in the IT industry in Japan, South Korea, Germany, France, Italy, the USA, and Canada have chosen in favor of the solutions of **Protection Technology LLC**.

Contacts:

StarForce Moscow HQ

127106 Russia, Moscow, Botanicheskaya str. 10D/1 building

Phone +7 (495) 967-14-51

Email: sales@star-force.ru

https://www.star-force.ru