OPSCURUS encryption system

OPSCURUS (Obfuscated Procedural neurally Scrambled Unified Reciever/Upload Schema) is a means of transmitting and files information securely in a way that cannot be decrypted by a quantum decoder. This information (money, documents, programs, and even AI, ST Backups and ROM constructs) can sit on a network, stored for years on end under complete anonymity - ready to be recalled at a moments notice.

Once recalled, the pieces are laid into the 'template' and the information restored. It is common practice for the template to have changed over time, and thus the information which is recalled have an error rate of 0.1% or so - making it unusable on sequential systems but executable on refferential systems.

Also important is that a 'shadow' or multiple 'shadow' documents is also made with the original, usually from a different source. This document demands a different password and read-scheme, but will recall in almost exactly the same way, producing a completely different document. In court, where refusing to hand over encrypted information is an offense, this functionality nullifies that offense - by allowing a user to hand over whatever information they want the court to see.

Statistics

Type: Information Encryption Software Designers: Lazarus Consortium Nomenclature: N/A Manufacturer: Lazarus Consortium Production: Mass Production

More about Opscurus

Safety features
Encryption steps

The system works by digitally shredding a file and scrambling the file. It is then transmitted up into “the cloud” (Lazarus Nodes and their P2P systems) and mirrored extensively - where it can be stored for years at a time.

1. The information is stored in multiple locations simultaneously
    1. Each unaware of any other of the constituents, appearing as garbage information
    2. This information is checked against a procedurally generated checksum.
    3. When the checksums of the neural address space and file fragment match, the piece of the puzzle is placed.
2. The information is transmitted inside marred versions of conventional transfers. Webpages, documents, videos and even normal transmissions
    1. These transmissions are subtlly altered by Lazarus nodes as the transmission travels throught them - adding the raw data in ways other systems will simply identify as subtle transmission errors.
    3. The edges of the segments are blurred, making sequential reconstruction and information forensic techniques useless.
        1. Each component randomly scaled - often rendering information within it redundant and repeated nonsensically, rather than actually just taking a bigger chunk of the file itself.
4. The necessary techniques of the cypher are primarilly logic based and not algorythmically based.
    1. Since quantum computers are algorhythmically based, they can't leverage their processing advantage over conventional computers in any meaningful way.
    2. Quantum brute-forcing is made harder by non-conventional logic systems that reward wrong answers and cancel out correct answers - using this system of inferrence to “shadow” the correct answer before making it. This is especially effective since any good quantum computer algorhythm ensures that computational paths leading to a wrong answer cancel out and paths leadingto a correct answer re-enforce

Recall steps

The address information to recall the files - and the order in which they were shredded is assigned via a neural print which requires both a classic password and address space password, and a recall method (one of 300) as well as a matchig brain or ROM Construct, to recall the file.

When the app is run, the user assigns the classic password, the 52 bit address-space password (composed of 52 unique characters, listed as the elements of a deck of cards) and a third piece of information - the read/write order/style of the neural device. This unusual 'deck' style alphabet (four suites, 12 cards + wildcard/joker) lends itself well to encryption due to the difficulty in repeating patterns, making brute-forcing (even with quantum systems) very difficult.

975,289,505,440,883,277,824,000,000,000,000. To give you an idea of how many that is, here is how long it would take to go through every possible permutation of cards. If every star in our galaxy had a trillion planets, each with a trillion people living on them, and each of these people has a trillion packs of cards and could shuffle a trillion times per second, and they'd been doing that since the Big Bang, they'd only just now be starting to repeat shuffles. Fun, huh? ~ J. Kaspar|

5. The unusual nature of neural encryption removes patterns found in other raw information systems, since each instance of similar information is differentiated
    1. No unit of similar information ever repeats during the decryption sequence. In this way, it is almost impossible to find patterns - making AI based forensic systems ineffective.
6. All transmissions occur in random order deliberately different from that of the recall sequence.
7. When the upload is complete, the information is burned from the Lazarus node P2P system and all traces are removed, 24 hours after the transmission.
8. It is common practice to destroy the object or the storage device assigned to the object that the complete version of the file was stored upon, ensuring no physical forensic evidence of its existence exists.
9. Many Lazarus hardware systems have a self-destruct sequence which is armed when false information is intentionally given - meaning at gun-point, a Lazarus operative or employee can render a situation entirely legally deniable if an investigative body is involved and demands the release of sensitive information.
    1. Often, this self-destruct system is stored in the physical body of a ROM Construct, as an aetheric bomb (usually offline alltogether, making it hard or impossible to detect, since no unusual emissions are given off
    2. This device (known as a precaution warhead) is just dead hardware until armed) which arms only when the information is given.
    3. In most cases, the construct-body has an override code, though this can only be recalled when specific biometric permaeters (stress levels, heart-rate, etc) are in 'safe' levels - or if an outside source of Lazarus origin (such as another construct) can confirm the validity of the information.
    4. This information is usually known only by the original source of a construct and is very rarely issued to them unless specific circumstances arise in which they are authorized to use this system.

Alternative storage locations

In this way, documents, programs, money and even ROM Constructs can be stored for years at a time under complete anonymity. Importantly, the fragments can be stored anywhere - on any system - not just on the cloud. For example, in the “noise” area of a person's genetics - or even their neural-pathways or that of AI - allowing high density information to be hidden in plain sight.

From:
https://wiki.stararmy.com/ - **STAR ARMY**

Permanent link:
https://wiki.stararmy.com/doku.php?id=corp:lazarus:opscurus

Last update: **2023/12/21 00:57**