EMEA BASED PUBLIC SECTOR CLIENT

CASE STUDY

LT Cyber Security

A division of LoughTec

4 Bankmore Business Park,
Omagh, Co. Tyrone, BT79 0BQ

T: +44 (0)28 82 25 2445
E: info@LoughTec.com
W: LoughTec.com

The challenge

To give an EMEA-based public sector client the ability to ingest/receive files into their secure network (photos, video, Excel spreadsheets, Word documents etc) safely and without threat. On the face of it, this challenge sounds simple, but that couldn't be further from the truth. When a public sector organisation opens up its network to the wider world, they immediately become a target for cybercriminals.

Cyber threat landscape

There has been significant growth in cyber criminality in the form of high-profile ransomware campaigns in recent years. Breaches of this kind have leaked massive levels of personal data, leaving victims vulnerable to fraud. Lives were put at risk and services were damaged by the WannaCry ransomware campaign in 2017, which notably, affected the NHS and many large organisations worldwide. Tactics are currently shifting, as businesses are being targeted over individuals, and although the numbers of phishing attacks on individuals are increasing, fewer are falling victim as people have become more alert.

Cybercriminals seek to exploit human or security vulnerabilities to steal passwords, data or money directly. The most common cyber threats include:

- Hacking - including social media profiles and email passwords.
- Phishing - bogus emails asking for security information and personal details.
- Malicious software – including ransomware through which criminals hijack files and hold them to ransom.
- Distributed denial of service (DDOS) attacks against websites – often accompanied by extortion.

The scale and complexity of cyber-attacks are wide-ranging. 'Off the shelf' tools mean that less technically proficient criminals are now able to commit cybercrime, and do so as awareness of the potential profits becomes more widespread. The evolving technical capabilities of malware means evolving harm as well as facilitating new crimes, such as the crypto mining malware which attacks digital currencies like Bitcoin.

Specific threat

Once an organisation starts to receive files from outside their network, they then become a target. No file is a simple file. What appears as safe can have malicious threats embedded deeply in the file structure.

All files are composed of one or more computer files along with metadata. For example, a digital image may include metadata that describes how large the picture is, the colour depth, the image resolution, when the image was created, the shutter speed etc. A text document's metadata may contain information about how long the document is, who the author is when the document was written, and a summary of the document. Archive files are used to collect multiple data files together into a single file for easier portability and storage, or simply to compress files to use less storage space.

Archive files often store directory structures, error detection and correction information, arbitrary comments, and sometimes use built-in encryption.

For example, a PowerPoint document can contain thousands of files in a presentation; images, snips, text, macros, Excel documents.

This presents the cybercriminal with an opportunity. Cybercriminals can hide malicious code in a completely innocent looking file; something that will detonate when that file is opened or even sit dormant for a long time and then detonate.

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the colour of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

The LoughTec approach

In very simple terms, LoughTec has built a cloud environment, where a public sector client can process files to ensure that they can receive files into their network safely. **How?** We have used two key pillars of our cybersecurity technology stack to remove unknown and malicious threats before the files come into their network.

McAfee SOPHOS TREND MICRO CROWDSTRIKE

KASPERSKY lab Symantec. Bitdefender

eset Avira COMODO WEBROOT an opentext company

Stage 1 - AV Multiscanning - advanced threat prevention with simultaneous anti-malware engines.

Multiscanning is an advanced threat detection and prevention technology that increases detection rates, decreases outbreak detection times and provides resiliency to anti-malware vendor issues. This includes having over 30 anti-malware engines available to deliver enhanced protection from a variety of cyber threats. Signature-based, heuristics-based, and machine learning detection methods are not perfect. Single anti-malware engines detect (at best) up to 91.8 per cent of common cyber threats, and the majority of them only have a 40 to 80 per cent detection rate.

Stage 2 - Deep Content Disarm and Reconstruction (Deep CDR)

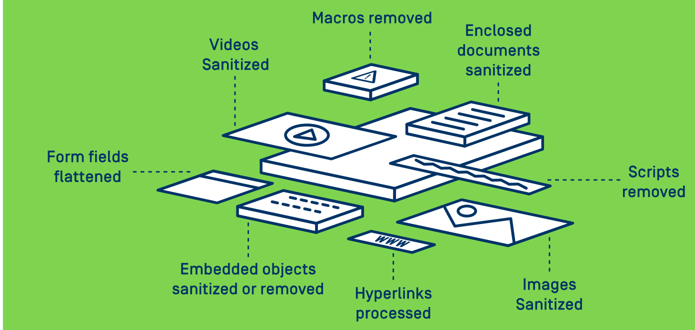
Content disarm and reconstruction (CDR), also known as data sanitisation, assumes all files are malicious and sanitises and rebuilds each file ensuring full usability with safe content.

By sanitising each file and removing any potential embedded threats, CDR effectively 'disarms' all file-based threats including known and unknown threats; complex and sandbox-aware threats; threats that are equipped with malware evasion technology such as fully undetectable malware, VMware detection, obfuscation amongst others.

Our deep CDR technology is a market leader, with superior features like multi-level archive processing, accuracy of file regeneration, and support for 100+ file types. We provided in-depth views of what is being sanitised and how – enabling the public sector client to make informed choices and define configurations.

To arrange your LT Cyber Security Assessment call +44 (0)28 82 25 2445

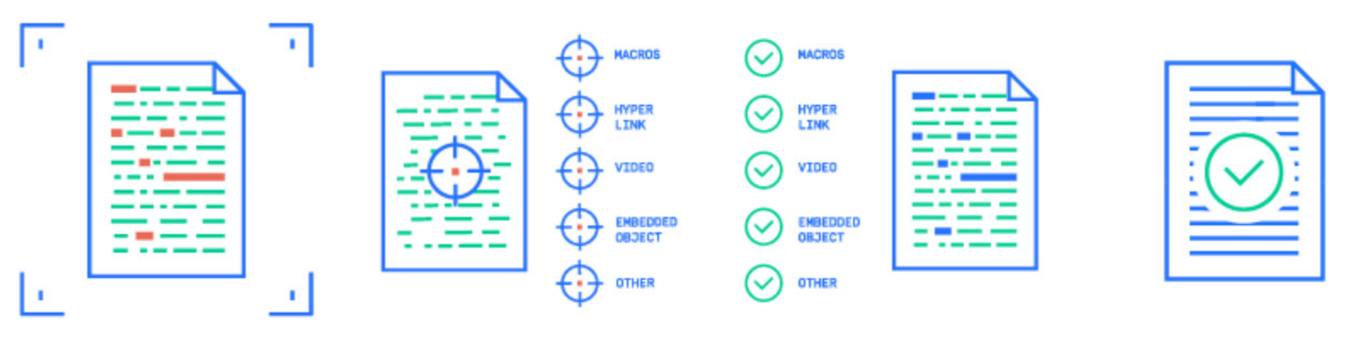
We delivered safe files with 100% of threats eliminated within milliseconds so that the organisation's workflow was not interrupted.



What LoughTec delivered

- A safe and secure data workflow to ingest files into the client's network.
- A safe and secure workflow to transfer files to other public sector departments.
- Enabled the retainment of all file metadata to ensure file evidence was legally compliant for court purposes.
- Unknown threats like steganography are now no longer a worry or a concern.
- Manpower savings – video evidence can now be uploaded directly to the client, meaning personnel do not need to travel to site to collect such evidence.
- Video and photographic evidence can be collected quickly, safely, legally and efficiently.

How CDR works



1. Files are evaluated and verified as they enter the sanitisation system to ensure file type and consistency.

File extensions are examined to prevent seemingly complex files from posing as simpler files, and red-flagged for malicious content, alerting organisations when they are under attack.

2. File elements are separated into discrete components and malicious elements are removed or sanitised.

3. Files are rebuilt in a fast and secure process. Metadata and all file characteristics are reconstructed.

4. New files are recompiled, renamed, and delivered - preserving file structure integrity so that users can safely use the file without loss of usability.

To arrange your LT Cyber Security Assessment call +44 (0)28 82 25 2445

LT Cyber Security

A division of **LoughTec**

4 Bankmore Business Park,
Omagh, Co. Tyrone, BT79 0BQ

T: **+44 (0)28 82 25 2445**
E: **info@LoughTec.com**
W: **LoughTec.com**