Testing the Efficacy of Content Threat Removal

July 2019

Table of Contents

1 Introduction

1.1 Background

In 2018, Deep Secure undertook a project to test the efficacy of Content Threat Removal (CTR) against known, existing malware. Whilst the true benefit of CTR comes from its ability to defeat unknown, zero-day malware, it is also important to show that existing malware is defeated by the process. This paper describes the results of the testing that was undertaken.

Content Threat Removal is a process developed by Deep Secure to ensure that there is no threat from malware in any content that has been processed. Critically, removing the threat of malware does not depend on finding the malware nor does it depend on sandboxing or machine learning / artificial intelligence to determine if malware might be present.

CTR is, in fact, a simple process of parsing and rendering the content. The key to its success is that CTR utilises an intermediate format to hold the information contained in the original content. This intermediate format, along with the parsing process is designed to only extract content that can be safely rendered.

Malware is carried in the data structures of content, it does not reside in the information that the content carries. The CTR process extracts the information and leaves behind the data structures that carried it, therefore leaving behind any malware that was present. The rendering process then puts the information into clean new data structures to be delivered to the destination.

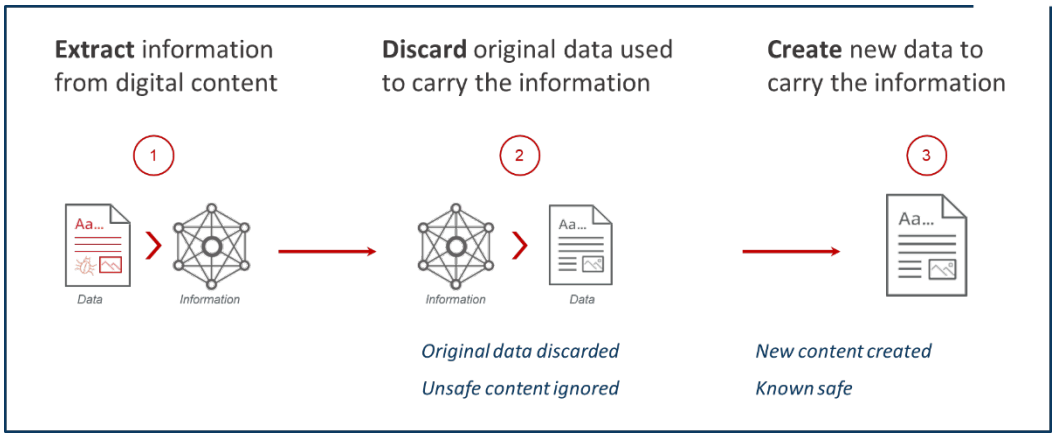

Figure 1: The Content Threat Removal process

The CTR process can be deployed in different ways depending on the use case. For high assurance deployments such as government, defence and critical national infrastructure, CTR can be deployed using physical hardware across multiple machines and includes a separate hardware enforced

independent validation of the data[1]. For commercial organisations, CTR can be deployed using the same core transformation engine in physical, virtual or cloud deployments and using APIs to build into existing applications that handle content.

[1] https://www.deep-secure.com/news-and-events/141-hardsec-hardware-security.php

2 User Requirements

In order to test the efficacy of CTR, Deep Secure used a database of more than 30 million known viruses. The database[2], started in 2011, contains malware of many different forms and is maintained and updated on a regular basis.

In order to process over 30 million virus samples, the testing was automated and run in three phases:

- Commercial AV scan of the file
- Content Transformation of the file
- Commercial AV scan of the resulting file

This process would confirm whether files processed by CTR had in fact removed the threat of malware.

Content Threat Removal, when deployed in its most high assurance form, provides a no-compromise approach to security. File types that can be transformed and so made safe, have their information extracted and new content built from that information. Files that cannot be transformed safely are blocked. With this approach, no unsafe content gets past the CTR process.

Given the size of the database, the initial testing performed was focussed on the commonly used Office and Imagery formats such as PDF, Word and JPEG. Whilst CTR can also handle and safely transform some other file types such as ZIP files, HTML and XML, they were not transformed for these tests and were blocked.

2.1 Anti-Virus Scanning

It is widely accepted that AV scanning cannot effectively deal with unknown, zero-day malware. Simple changes to existing malware make it undetectable and able to get past traditional signature-based AV.

As it turned out, the testing showed that AV scanning is also not always effective against known malware. A number of the files did not show up as malware in the initial scan of the files. This may be because some of the malware tested dates back a number of years and as signature databases grow, signatures for older malware may be dropped to keep the database size manageable.

2.2 Test Results

The chart in *Figure 2* shows the sample malware grouped into categories. It shows that by far the most common file types were executable content (for example, .exe and Java files) making up around two thirds of the total sample. This category also included script files such as Python, Perl and PHP. Mark-up languages (XML and HTML) and Archive files also featured heavily.

[2] www.virusshare.com

The files shown as **Green** on the chart were blocked because they could not be safely transformed. The majority of the malware falls into this category and would fail to get into a system protected by CTR.

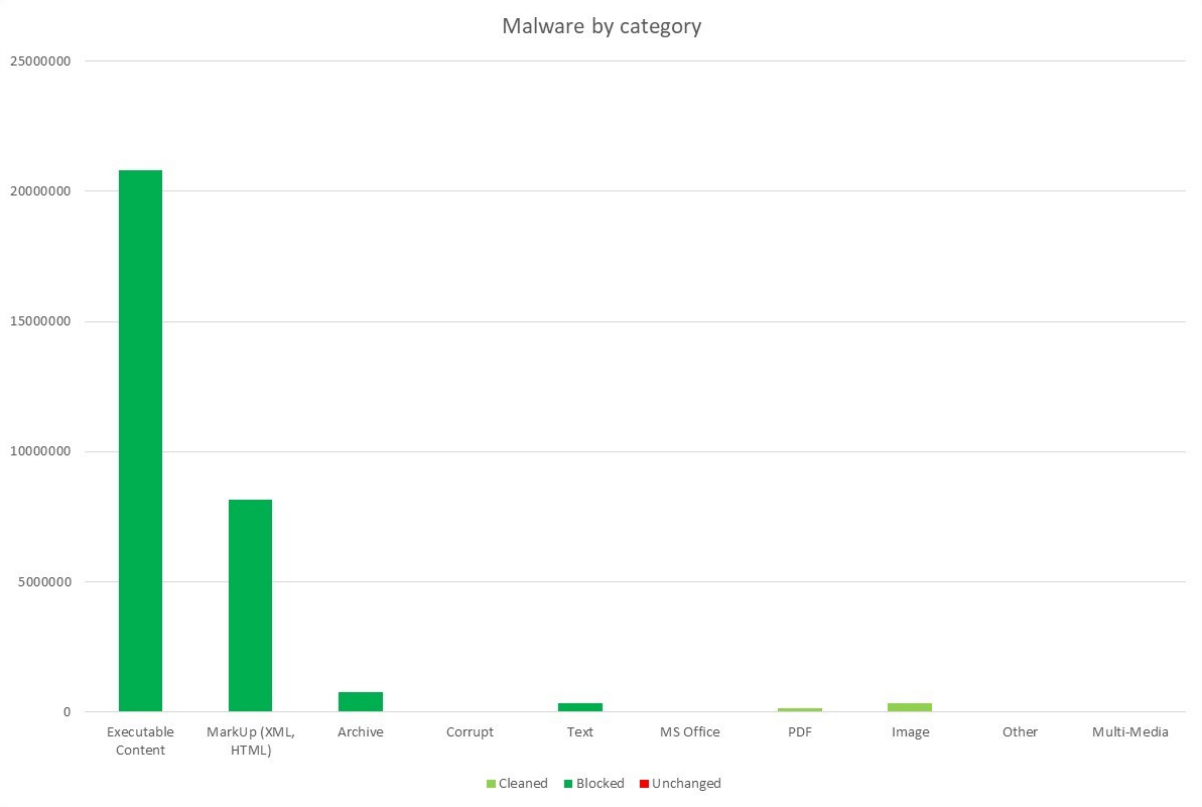

Figure 2: Malware in the virus database by category

The files shown as **Light Green** on the chart were safely transformed and so would be delivered safely into a system protected by CTR. These files would be delivered with the same file format as the original malicious files but would be safe to read and interact with.

There were no files that were processed leaving the malicious content inside (shown as **Red** on the chart).

The chart in Figure 3 looks more closely at the file types that were transformed by CTR. The majority of these files were images (311,900) and the majority of these were transformed (310,759) and so made safe to deliver. A small number of image types could not be transformed and were blocked because they were corrupt beyond repair.

All PDF documents (156,369) and MS Office documents (43,767) processed were transformed and made safe.

These results show that CTR used in the correct way is effective in stopping 100% of malware from entering a protected system. Of the more than 30 million samples, no malware made it through the CTR process to the destination.

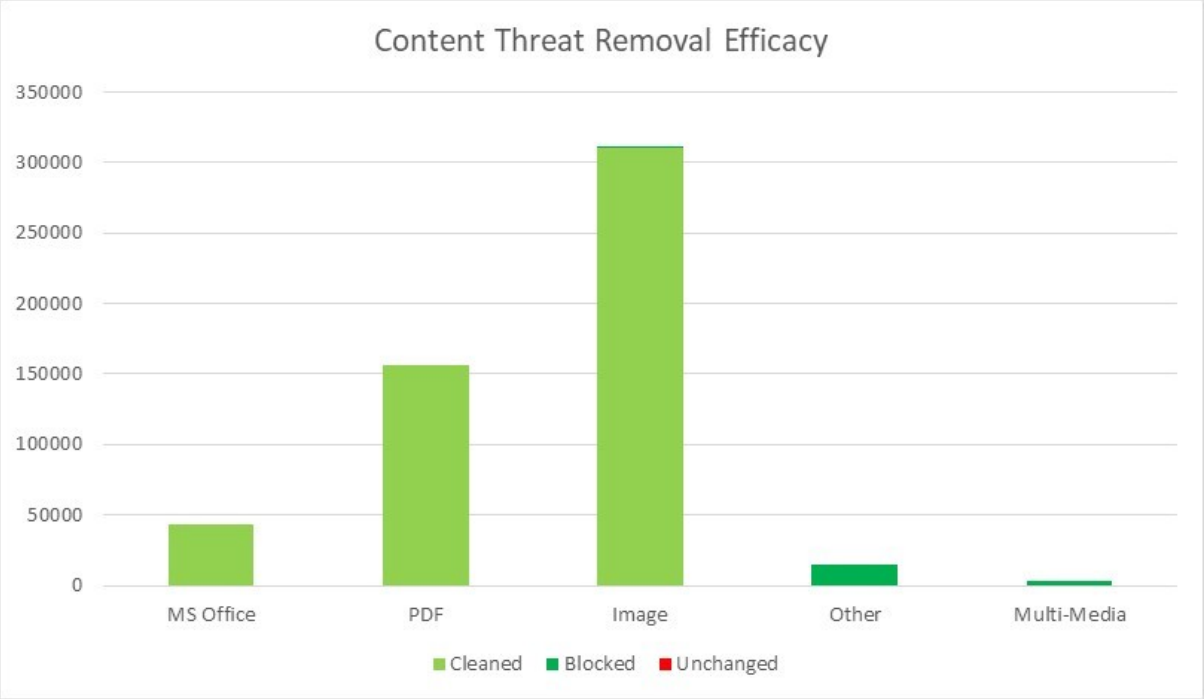

Figure 3: Efficacy of CTR for supported file types

3 Independent Efficacy Testing

Following the Deep Secure testing, a prominent national government agency contracted its engineering arm to perform independent testing of Content Threat Removal. This time, the testing was not using publicly available viruses, but malware created specifically to test the effectiveness of content security solutions and unseen by Deep Secure.

The independent testing covered the following common file formats:

- Adobe PDF (PDF)
- Microsoft Word (DOCX)
- Legacy Microsoft Word 97-2003 (DOC)
- Microsoft Excel (XLSX)
- Legacy Microsoft Excel (XLS)
- Microsoft PowerPoint (PPTX)
- Legacy Microsoft PowerPoint (PPT)
- GIF Image (GIF)
- Text Files (TXT)
- JPEG Image (JPEG)
- Bitmap Image (BMP)
- PNG Image (PNG)

As before, where possible, Content Threat Removal transformed the files, removing any malware in the process. In some cases, where the file type could not be transformed, it would be blocked.

As shown in the chart at Figure 4, the results of the testing showed that for all of the above file types no malicious content got through the transformation process. For these file types, the file was either:

- transformed (**Green on the chart**), removing the malicious content and delivering a safe version of the file
- blocked (**Light Green on the chart**), not allowing the file to be delivered at all

Examples of files that were blocked were files that could not be safely transformed (e.g. executable files) or files that were so corrupt that no useful information could be extracted from them.

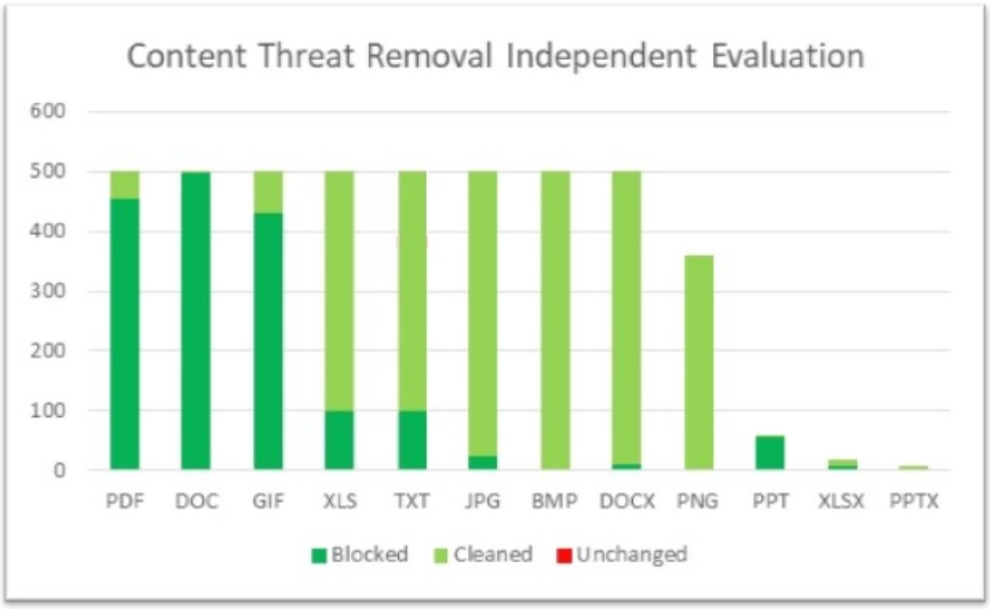

Figure 4: Independent testing of the efficacy of Content Threat Removal

3.1 Text Files

It is worth noting that the Deep Secure product was even able to be configured to prevent scripts in Text files, without the need to know it was a script or to have seen it before. The results of the testing showed that a number of TXT files (25%) would otherwise have been delivered with the malicious content intact. This shows the inherent issue of text as a file format. Scripting languages use a text format and so scripts are carried in text files. Scripts can be malicious and so allowing TXT files to be exchanged and then interpreted as scripts can be dangerous.

Content Threat Removal does not use detection mechanisms to decide if content is safe, it extracts business information and creates new content using the extracted information. This means that scripts carried in text files could potentially be delivered intact.

There are some controls that can be applied during the transformation process; for example, to allow or to block control characters and to check characters against a character set. However, these will not prevent scripts from being allowed in, using a text file format so a translation approach is required for TXT Files.

By converting the TXT files to RTF, the text can be maintained, but the threat is removed. In the final testing of the text file samples using this technique, Deep Secure has shown that the delivered text files are rendered safe and could not be interpreted as scripts. There are additional techniques that can be used to ensure text files are made safe which Deep Secure is implementing into the CTR process

so that TXT files can be brought into a protected system safely. For more information, contact Deep Secure.

4 Summary

Comprehensive in-house and independent testing has shown that Deep Secure Content Threat Removal is 100% effective against known malware[3]. Independent testing carried out on behalf of a respected government agency has shown that CTR is also 100% effective against previously unseen malware.

This is an unprecedented set of results which confirms that Content Threat Removal is the most effective way of eliminating malware. CTR can be used by commercial organisations using on-premise and cloud appliances or as an on-demand cloud service. Furthermore, CTR can also be used by defence, government and critical national infrastructure in an ultra-high assurance platform, whereby the CTR software is protected by a hardware-only device, to provide the ultimate in content security.

[3] For the specified file types