

Content Disarm Reconstruction and Cyber Kill Chain

Muhammad Sahputra

cyberheb@idsecconf.org



Who..?



Muhammad Sahputra

CEO & Co-Founder of PT Mahapatih Sibernusa Teknologi
Indonesia

Your work is going to fill a large part of your life, and the only way to be truly satisfied is to do what you believe is great work. And the only way to do great work is to love what you do. If you haven't found it yet, keep looking. Don't settle. As with all matters of the heart, you'll know when you find it.

(Steve Jobs)



PT Mahapatih Sibernusa
Teknologi



Telkom University



Program Committee

idsecconf

September 2008 – Present (10 years 3 months) | Education

Indonesia IT Security Conference or better known IDSECCONF is an annual activity held in cooperation of the IDSECCONF committee with KEMKOMINFO (Department of Communication and Informatics) and other related parties that aims to provide enlightenment to the general public, students, and particularly among security professionals on the latest information technology security issue.



Experience

CEO & Co-Founder

PT Mahapatih Sibernusa Teknologi

January 2018 – Present (11 months) | Greater Jakarta Area, Indonesia



Senior Engineer

Nokia

March 2007 – June 2017 (10 years 4 months) | Worldwide



IT Security Consultant

Bellua Asia Pacific

January 2010 – December 2011 (2 years) | Greater Jakarta Area, Indonesia



Professional Trainer

InformIT; Inixindo

July 2005 – February 2006 (8 months) | Bandung Area, West Java, Indonesia

Cyber Kill Chain

Kill Chain: The 7 Stages of a Cyber Attack

1. Reconnaissance

Scanning the environment or harvesting information from social media.



3. Delivery

Transmission of weapon/malware to target (e.g. via email, USB, website).



2. Weaponization

Pairing malicious code with an exploit to create a weapon (piece of malware).



4. Exploitation

Once delivered, the weapons/malware code is triggered upon an action. This in turn exploits the vulnerability.



5. Installation

The weapon installs malware on the system.



6. Command and Control

A command channel for remote manipulation of the victim.

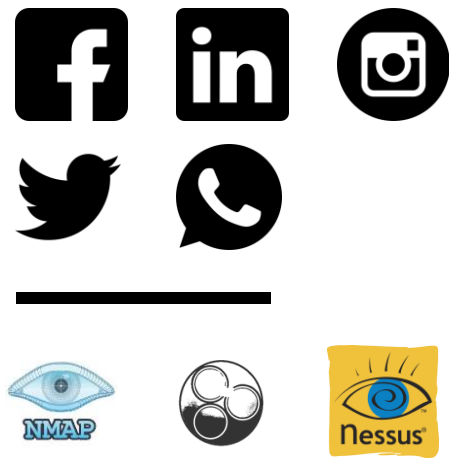


7. Action on objectives

With hands on access the attacker and achieve their objective.



Reconnaissance



- Data Scrapping
- Network Scanning
- Social Media
- Web Intelligence
- Opensource Intelligence

“**Reconnaissance** is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system”

“Finding the most **vulnerable** asset, i.e human resources team, GA, secretary, sales admin, ...”

Dear Customer,

In response to your request, [REDACTED] to provide you with this proposal for its [REDACTED]

The company [REDACTED] that offers wide range of Open Source Web Intelligence solutions for governments, law enforcement, military, and intelligence organizations. The solutions are designed to enable these organizations to effectively gather unique, highly valuable intelligence regarding their targets over the internet.

The company was founded by experienced visionaries, business & technologists' leaders with vast experience in both technical and operational aspects of intelligence-gathering solutions.

Our offering includes:

- Superior field-tested state-of-the-art solution with unique capabilities
- [REDACTED]
- Reliable experienced project management team and proven installation procedures
- In-house training by experienced trainers and a complete documentation package
- [REDACTED]

We are honored to respond to your request for this proposal and welcome the chance given to us.

Sincerely,

Weaponization



- Exploit Kit
- RAT
- FUD Malware

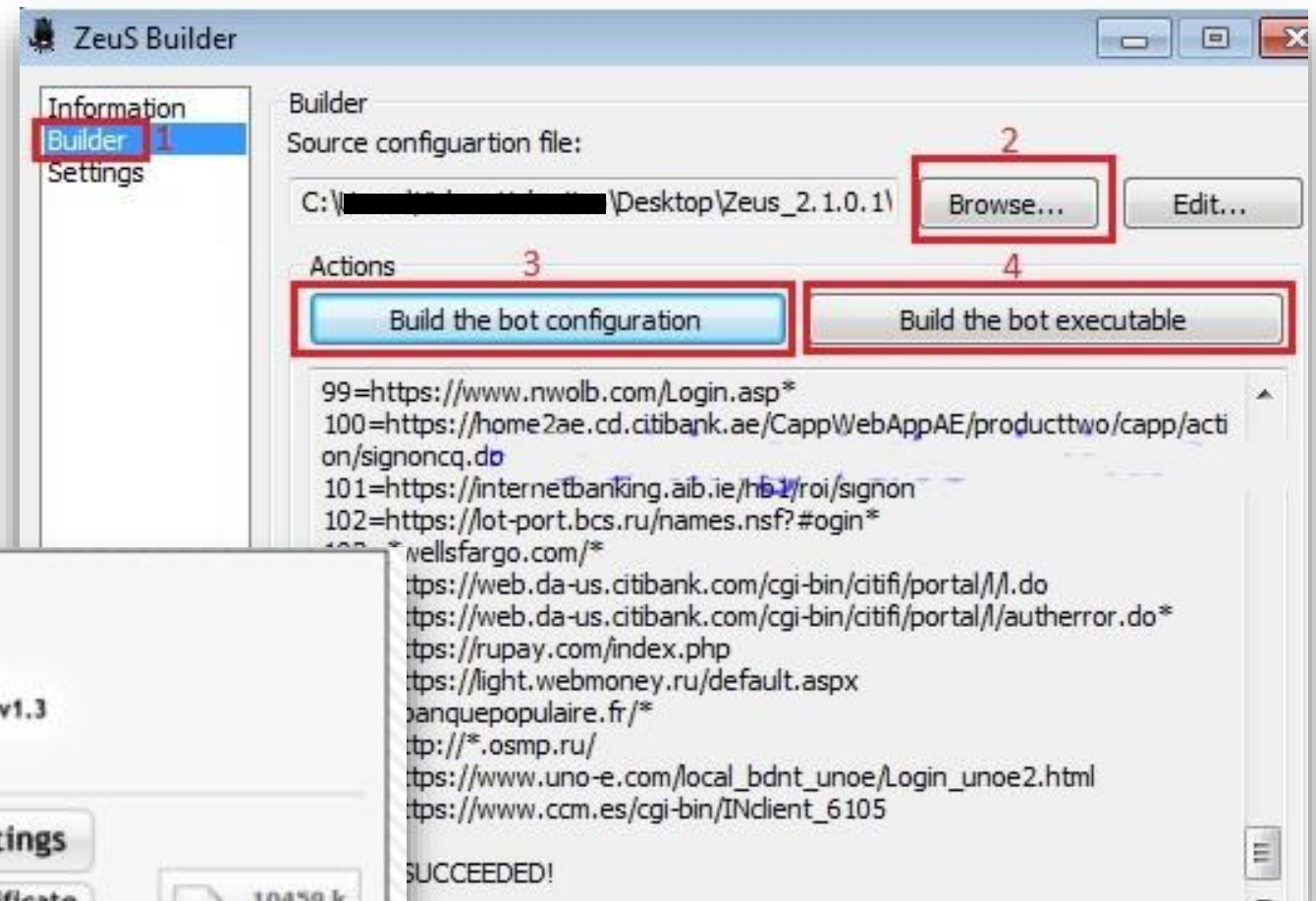
- BotNet
- 0day
- ...

“**Weaponization** creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities”

“Most of the weapon available for sale in **underground / darkweb**”

Weaponization

SpyEye & ZeuS
was once popular
as banking
malware



Delivery



- Email
- USB Drive
- Social Media
- Hacked Website
- Curriculum Vitae
- ...

**“Delivery transmits
weapon to target”**

Exploitation



- Exploiting PDF
- Exploiting Microsoft Word
- Exploiting Internet Browsers
- Exploiting OS
- ...

“Malware weapon's program code triggers, which takes action on target network to exploit vulnerability”

Installation



- Trojan Horse
- Virus
- Backdoor
- ...

“Malware weapon
installs access
point (e.g.,
"backdoor") usable
by intruder”

Command & Control



- Trojan Horse
- Virus
- Backdoor
- ...

“Malware enables intruder to have “hands on the keyboard” persistent access to target network (C&C)”

Actions on Objective



“Intruder takes **action** to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom”

Breaking Kill Chain

Kill Chain: The 7 Stages of a Cyber Attack

1. Reconnaissance

Scouting the environment or harvesting information from social media.



2. Weaponization

Pairing malicious code with an exploit to create a weapon (piece of malware).



3. Delivery

Transferring the weapon/malware to target (e.g. via email, USB, website).



4. Exploitation

Once delivered, the weapons/malware code is triggered upon an action. This in turn exploits the vulnerability.



5. Installation

The weapon installs malware on the system.



6. Command and Control

A command channel for remote manipulation of the victim.



7. Action on Objectives

With help, the attacker achieves their objective.

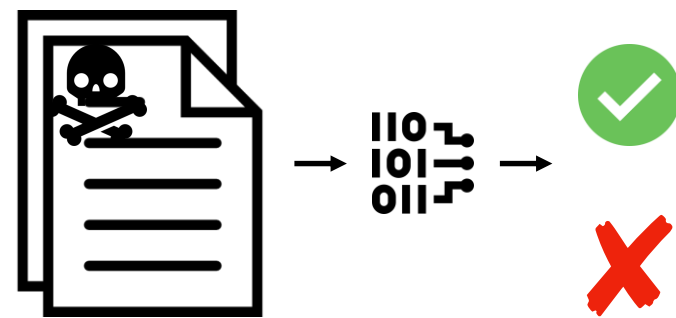


Breaking: Delivery Stage

We will only focus on this stage for the talk
:)

- Signature Based
- SandBoxing
- Artificial Intelligence
- Content Disarm & Reconstruction

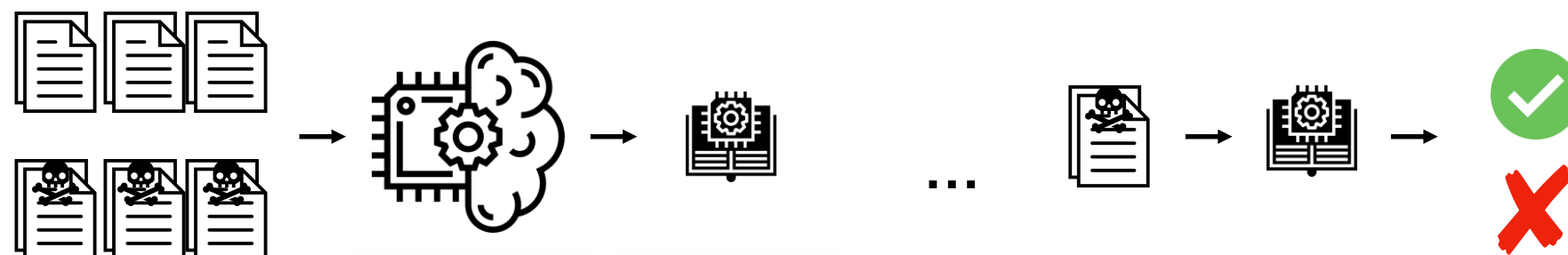
Common Technology



Signature Based



SandBoxing



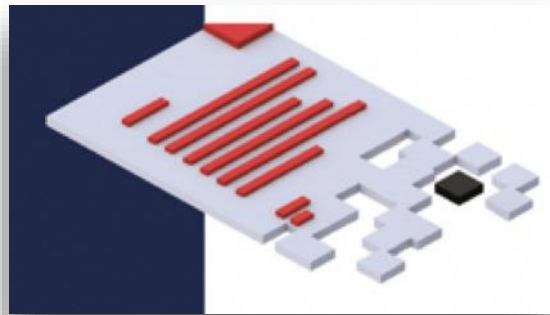
Collected Data
Samples

Feature Extraction
Network Training

Trained Network

Artificial Intelligence

Content Disarm Reconstruction



①

Break down a file into its basic objects and analyse each individual section and metadata

②

Neutralise any threats

③

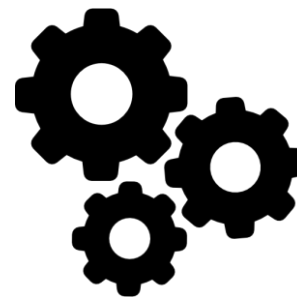
The cleansed files are reconstructed, while preserving the integrity and functionality of the original file, now safe to save and edit

Content Disarm Reconstruction

How it is looked from the inside



Before



CDR

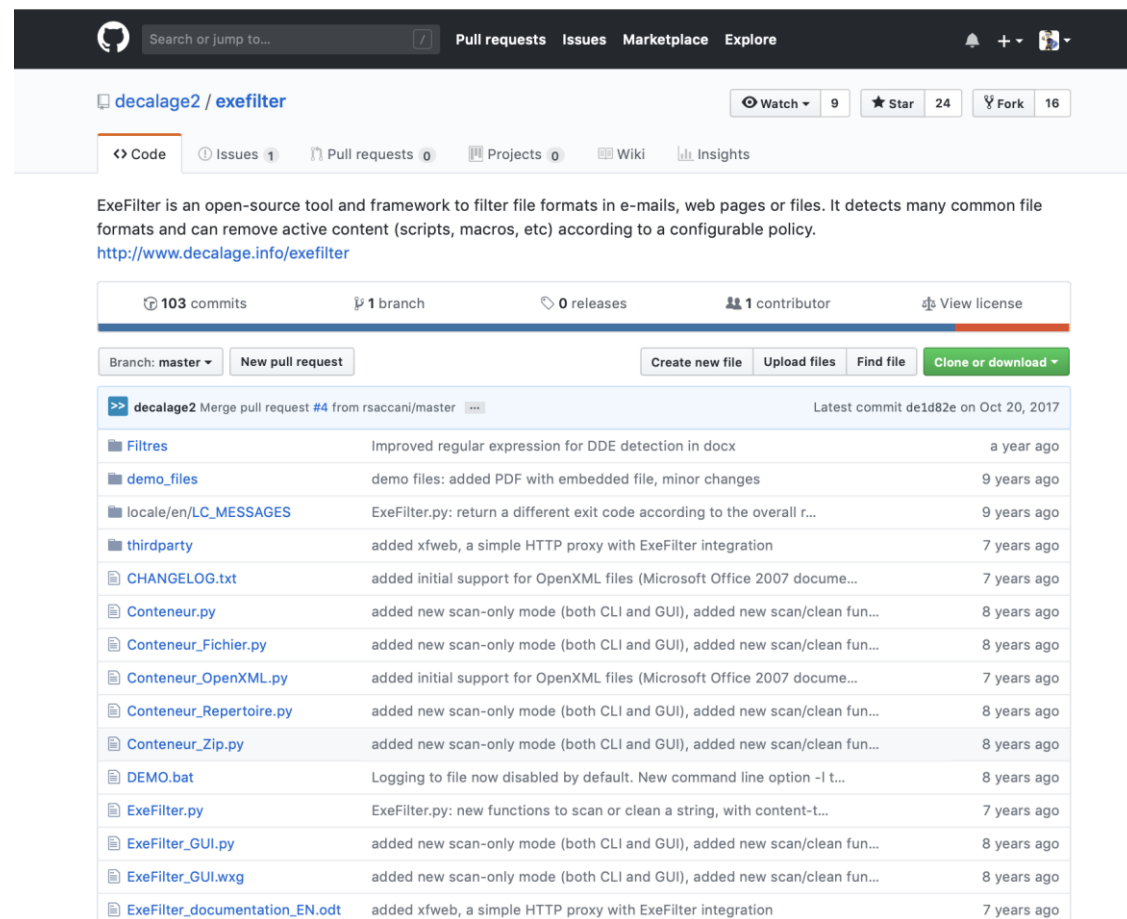


After



Content Disarm Reconstruction

Basic and Early Implementation



decalage2 / exefilter

ExeFilter is an open-source tool and framework to filter file formats in e-mails, web pages or files. It detects many common file formats and can remove active content (scripts, macros, etc) according to a configurable policy.
<http://www.decalage.info/exefilter>

103 commits 1 branch 0 releases 1 contributor View license

Branch: master New pull request Create new file Upload files Find file Clone or download

File	Commit	Time
Filtres	Improved regular expression for DDE detection in docx	a year ago
demo_files	demo files: added PDF with embedded file, minor changes	9 years ago
locale/en/LC_MESSAGES	ExeFilter.py: return a different exit code according to the overall r...	9 years ago
thirdparty	added xfweb, a simple HTTP proxy with ExeFilter integration	7 years ago
CHANGELOG.txt	added initial support for OpenXML files (Microsoft Office 2007 docume...	7 years ago
Conteneur.py	added new scan-only mode (both CLI and GUI), added new scan/clean fun...	8 years ago
Conteneur_Fichier.py	added new scan-only mode (both CLI and GUI), added new scan/clean fun...	8 years ago
Conteneur_OpenXML.py	added initial support for OpenXML files (Microsoft Office 2007 docume...	7 years ago
Conteneur_Repertoire.py	added new scan-only mode (both CLI and GUI), added new scan/clean fun...	8 years ago
Conteneur_Zip.py	added new scan-only mode (both CLI and GUI), added new scan/clean fun...	8 years ago
DEMO.bat	Logging to file now disabled by default. New command line option -l t...	8 years ago
ExeFilter.py	ExeFilter.py: new functions to scan or clean a string, with content-t...	7 years ago
ExeFilter_GUI.py	added new scan-only mode (both CLI and GUI), added new scan/clean fun...	8 years ago
ExeFilter_GUI.wxg	added new scan-only mode (both CLI and GUI), added new scan/clean fun...	8 years ago
ExeFilter_documentation_EN.odt	added xfweb, a simple HTTP proxy with ExeFilter integration	7 years ago



ExeFilter

An open-source framework
for active content filtering

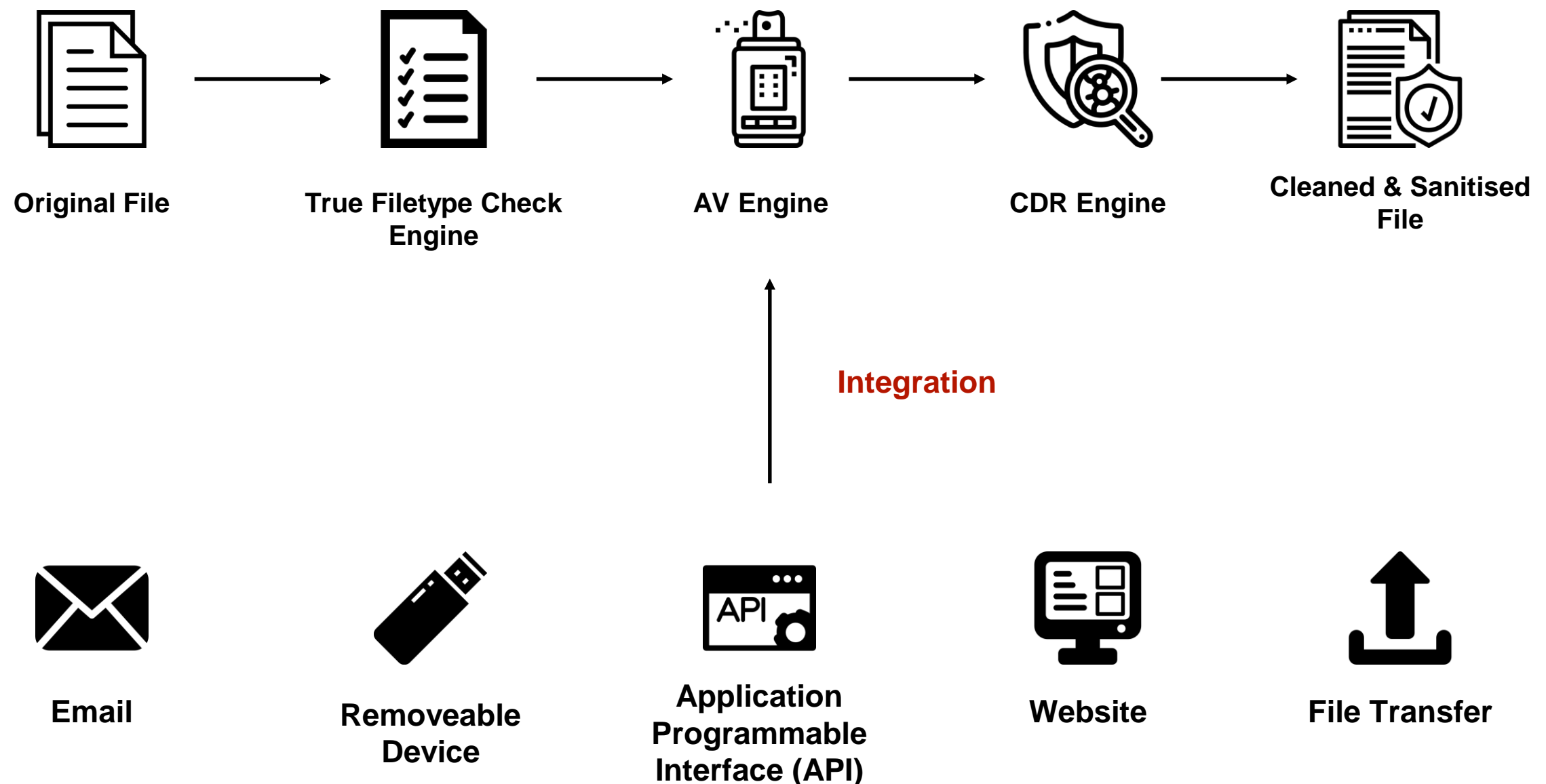
CanSecWest 2008 – 28/03/2008 – <http://cansecwest.com>

Philippe Lagadec – NATO/NC3A
philippe.lagadec@nc3a.nato.int

<https://cansecwest.com/csw08/csw08-lagadec.pdf>

Content Disarm Reconstruction

Core Engine Processes & Integration



Content Disarm Reconstruction

Policy Based Configuration

Default Policy ▾

SAVE

≡

Image

+ Add exception

Case	Default action	Exceptions
Virus	✗	0
Fake File	✓	0
Unknown file	✗	0
Password Protected	✗	0
Large File	✗	0
Complex File	✗	0
Special Case	🛡️	0

ACTION BY FILE TYPE

File type	Default action	Exceptions
PDF	🛡️	0
Image	🛡️	0
AutoCAD	🛡️	0
Ichitaro	🛡️	0
Hancm	🛡️	0
Binary	✗	0
Archive	🛡️	0
RTF	🛡️	0

DEFAULT ACTION

Block

Sanitize

Allow

☐ Rasterize vector images

☒ Add noise

☒ Max compression for lossless formats

Compression level:

Larger File Higher Quality

Smaller File Lower Quality

Content Disarm Reconstruction

Use Case: Email Protection

FILES

File actions

Microsoft Word Document.eml

HtmlBody.html

oledata.mso

Exe.docx

[Content_Types].xml

.rels

app.xml

core.xml

document.xml.rels

document.xml

oleObject1.bin

enprint.emf

FILE INFO

Microsoft Word Document.eml

File Type

EML File

Original Item Hash

ca098b0e664abd17706bfd5bcad853afad633565ff135cd477045941e8bb58c4

From

To

CC

Received Date

16/09/2018 10:58

SANITIZATION LOG

Started: 05/09/2018 | 11:40:48

File Microsoft Word Document.eml recognized as [200] EML File (EML Files).

File Microsoft Word Document.eml sanitization process successfully ended.

Ended: 05/09/2018 | 11:40:54

0.9 sec Total sanitization time

THREATS DETECTED

19

Files sanitized

3

Threats detected

Suspicious Fake File detected in Microsoft Word Document.eml\ol...

Suspicious Executable File detected in Microsoft Word Document.eml\ol...

Suspicious Executable File detected in Microsoft Word Document.eml\Ex...

Content Disarm Reconstruction

**Use Case: Oday Identifier - Suspicious
Macro in DOC File**

FILES

File actions

796c3a18-620c-4edf-8c05-c9e76ebc65a9.eml

order PO-010816-WA0002.doc

[Content_Types].xml

.rels

app.xml

core.xml

document.xml.rels

document.xml

fontTable.xml

image1.png

settings.xml

styles.xml

vbaData.xml

webSettings.xml

FILE INFO

order PO-010816-WA0002.doc

File Type	Word
Original Item Hash	5b2d163462647383488deaddf70d4f64bea821f4f425f8e7999a9db773716060

SANITIZATION LOG

Started: 24/09/2018 | 01:42:18

!

File order PO-010816-WA0002.doc recognized as [10] Word (Microsoft Office).

!

File order PO-010816-WA0002.doc successfully scanned by AviraAntiVirus.

!

File order PO-010816-WA0002.doc successfully scanned by EsetAntiVirus.

🔔

Suspicious Office macro detected [Auto Execution].

🔔

Suspicious Office macro detected [Out-Of-Document Interaction].

Ended: 24/09/2018 | 01:42:19

🕒

0.8 Total sanitization time
sec

THREATS DETECTED

14

Files sanitized

2

Threats detected



Suspicious Auto Execution Macro
detected in
796c3a18-620c-4edf-8c05-c9e7...



Suspicious Out of Document
Interaction Macro
detected in
796c3a18-620c-4edf-8c05-c9e7...

Content Disarm Reconstruction

**Use Case: 0day Identifier - XLS With
Equation Exploit**

The screenshot displays a CDR interface with the following sections:

- FILES:** A list of files extracted from an email (e3bd98b8-596e-441d-819b-e981371c0ac8.eml). The files include `HtmlBody.html`, `PO_SHENG SEN CO.xlsx`, `[Content_Types].xml`, `.rels`, `app.xml`, `core.xml`, `workbook.xml.rels`, `calcChain.xml`, `drawing2.xml.rels`, `drawing1.xml`, `drawing2.xml`, `vmlDrawing1.vml`, and `oleObject1.bin`. The `oleObject1.bin` file is highlighted in blue.
- FILE INFO:** A detailed view of the selected file `oleObject1.bin`. It shows the file type as "Equation Ole Object" and the original item hash as `6cc81bc0ebfcabe0b7dfa6012745adeb8cd7c6dbddcdea9e91f52cb9b8efe703`.
- SANITIZATION LOG:** A log of the sanitization process. It shows the process started on 16/09/2018 at 12:49:21. The log includes three entries: "File oleObject1.bin recognized as [2108] Equation Ole Object (OLE Object).", "File oleObject1.bin successfully scanned by AviraAntiVirus.", and "File oleObject1.bin successfully scanned by EsetAntiVirus.". A final entry with a red minus icon indicates that the file `oleObject1.bin_blocked.pdf` was blocked due to an organization policy violation.
- THREATS DETECTED:** A summary section showing that 24 files were sanitized and 0 threats were detected. A red box highlights the text: "No threat detected by AV but file was sanitised and safe to use".

THREATS DETECTED

24 Files sanitized | 0 Threats detected

No threat detected by AV but file was sanitised and safe to use

Summary

- Every technology / approach has its own pro-cons
- Implementation depend on environment requirements to get optimum result
- CDR technology improved 0day protection capabilities

END