The Irrelevance of K-Byte Detection – Building a Robust Pipeline for Malicious Document

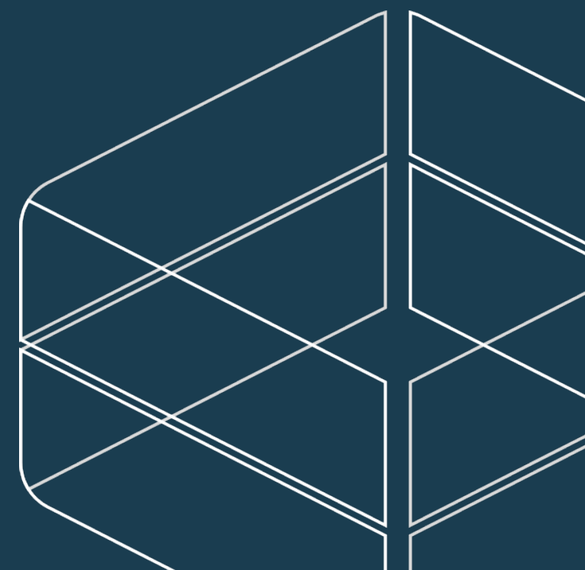
Dor Knafo
Security Research Leader

Dan Amiga
Co-Founder and CTO

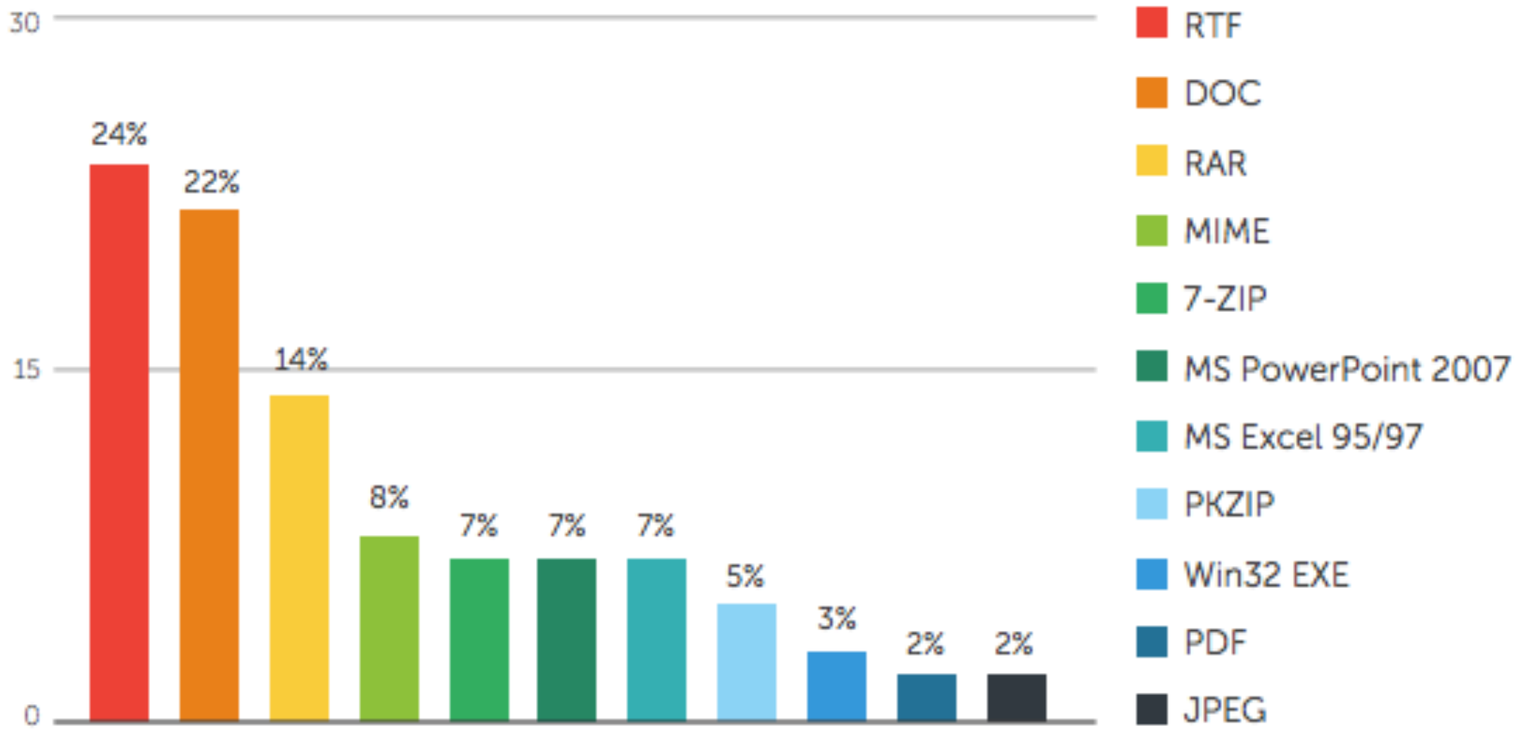
Agenda

- Introduction
- Document analysis pipeline
- File type detection
- Anti malware components and flaws
- Suggested workflows

QUICK INTRO



Targeted email attacks



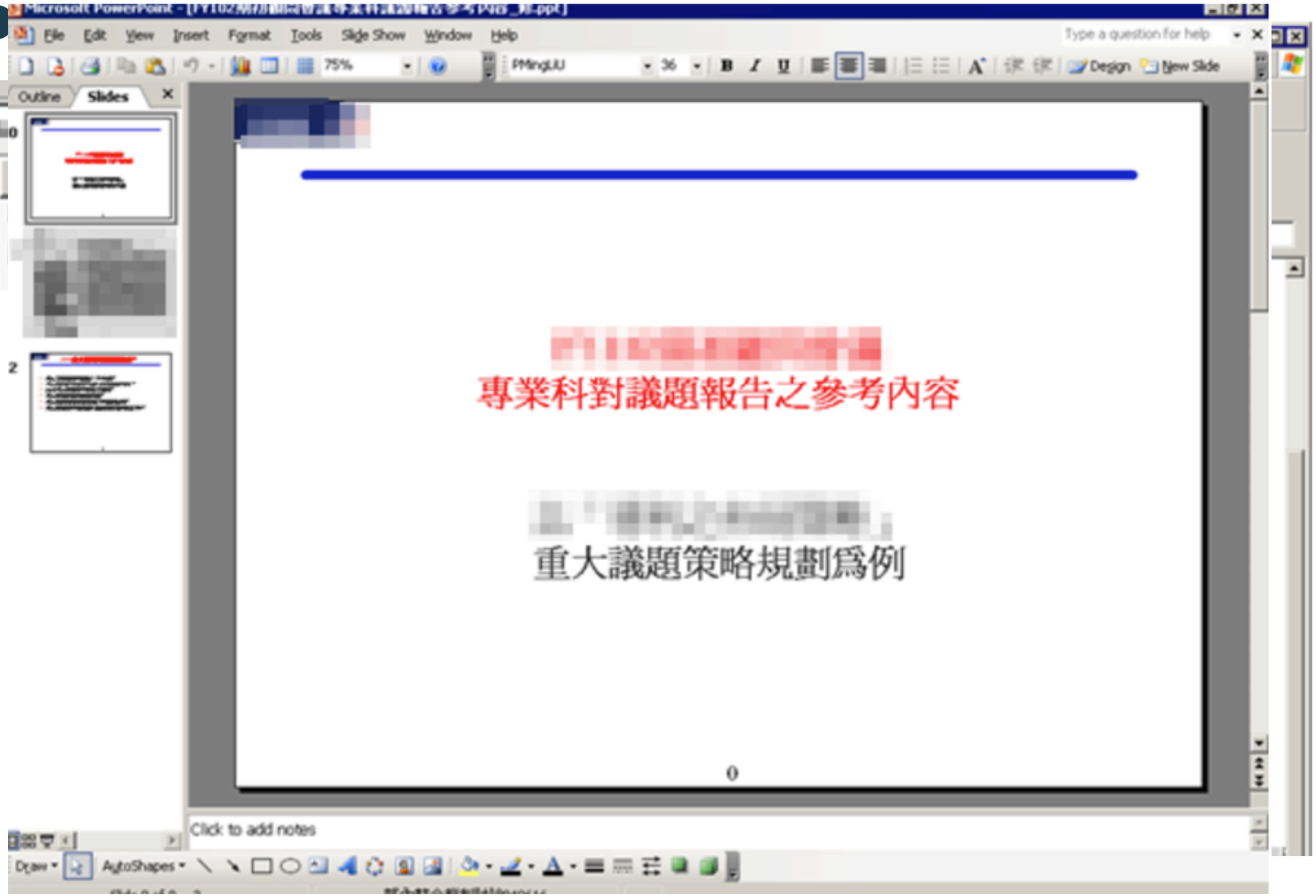
*According to ”TrendLabs 2014 Targeted attack Campaign Report”

Targeted email attacks

- Operation Pawn Strom – first seen as far back as 2004 operates until today
- Targets mostly governments, military and media entities in the US and US allies.
- Many notable incidents in the past few years, most of them based on spear phishing email containing malicious document

Operation P

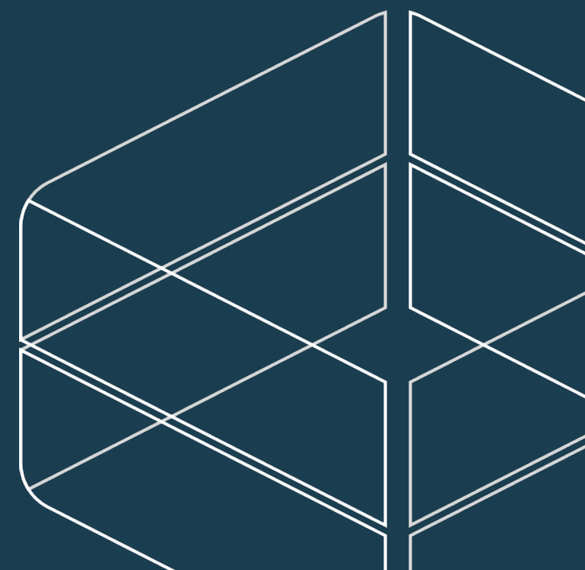
- Targets goverr
- RTLO (U+202e)



Document Analysis Pipeline

- Defense in depth
- Robustness
- One broken link won’t fail your system

COMPONENTS

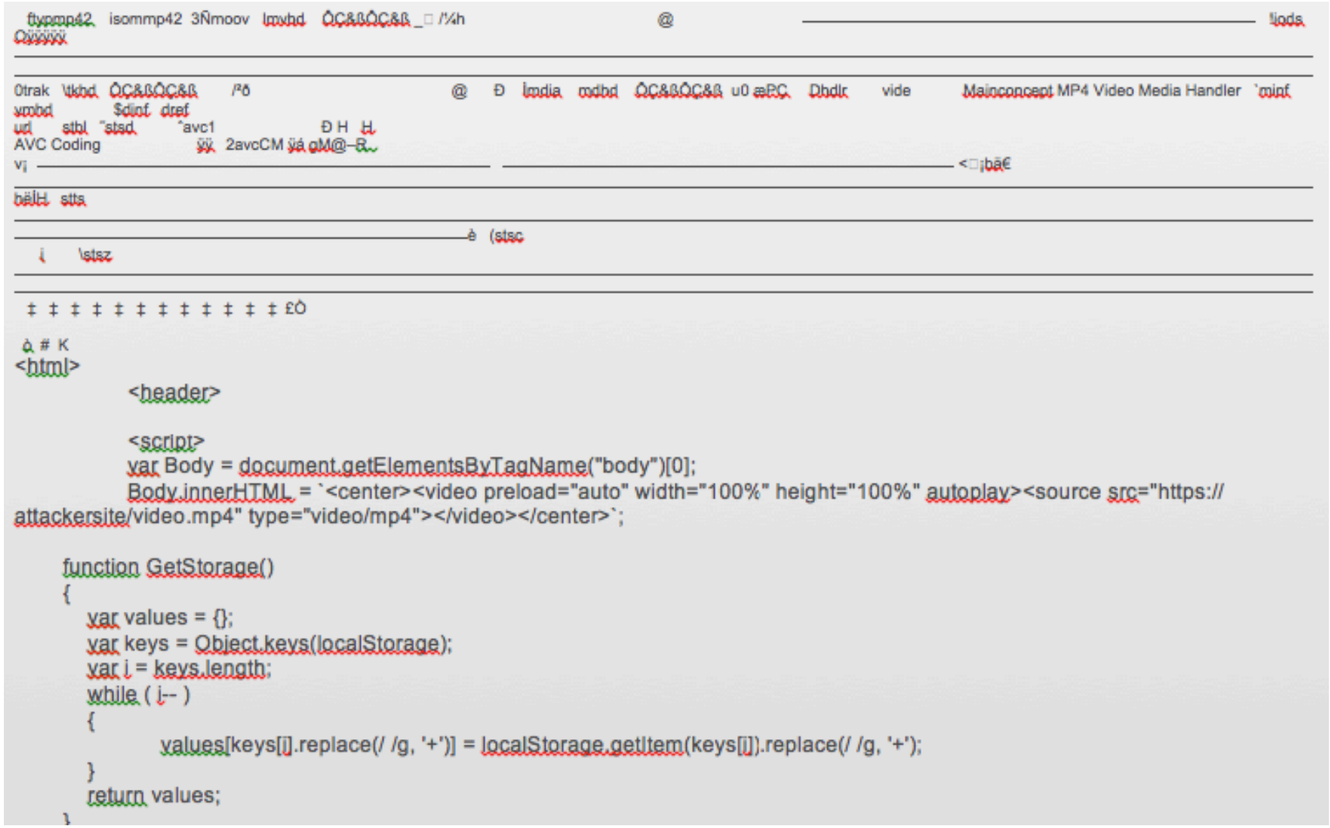


File type detection

- Extensions
- Magic bytes
- Character distribution
- Telegram / WhatsApp latest hack

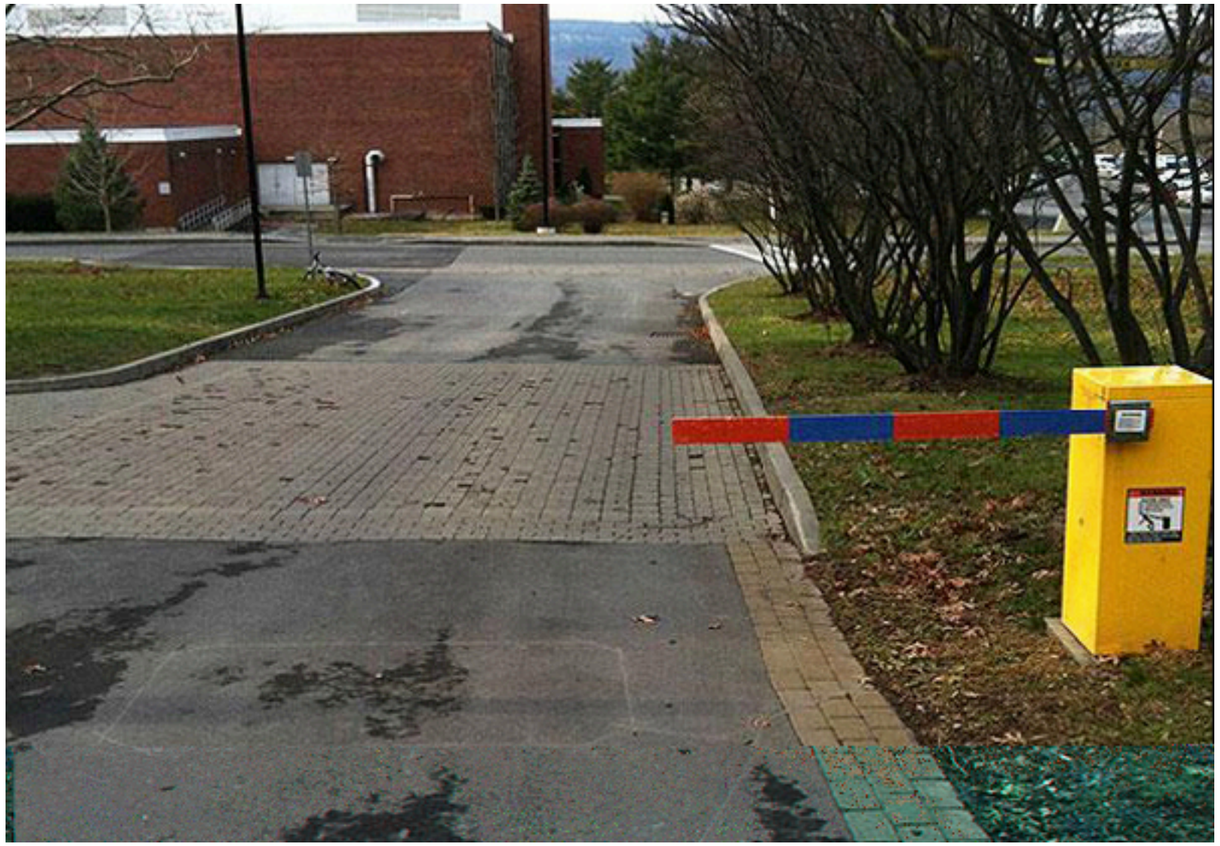
Telegram’s case

- End-to-end encryption
- Rely on client side detection validation
- The file is playable by the browser
- When open in new tab, executes Javascript on Telegram’s domain



Signatures

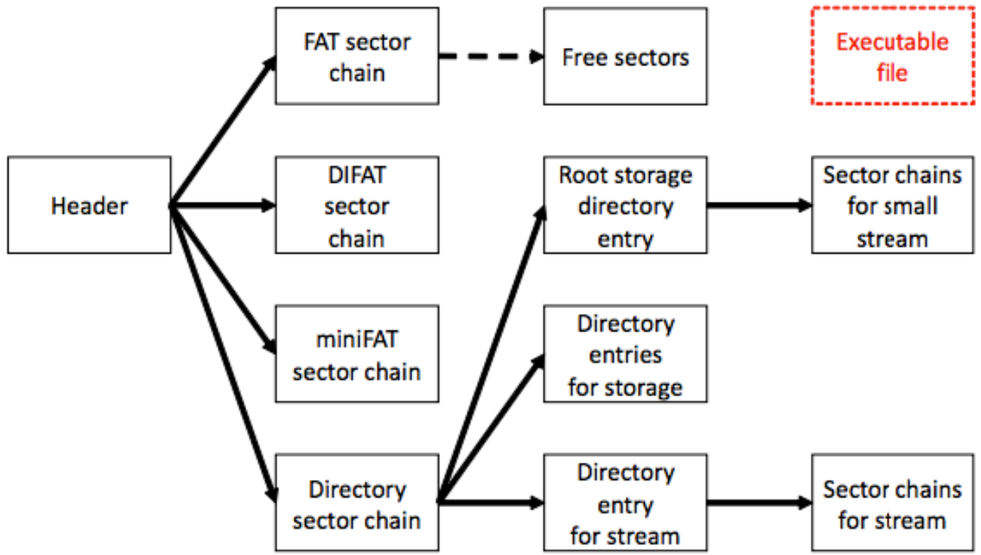
- Recognize known threats
- Very brittle
- Shared signatures



Static Analysis

- Based on heuristics:
  - Code (opcodes) shouldn't appear inside PDFs or Office files.
  - Looks for components out of the file structure.

- Hard to detect malicious macros
- shared knowledge



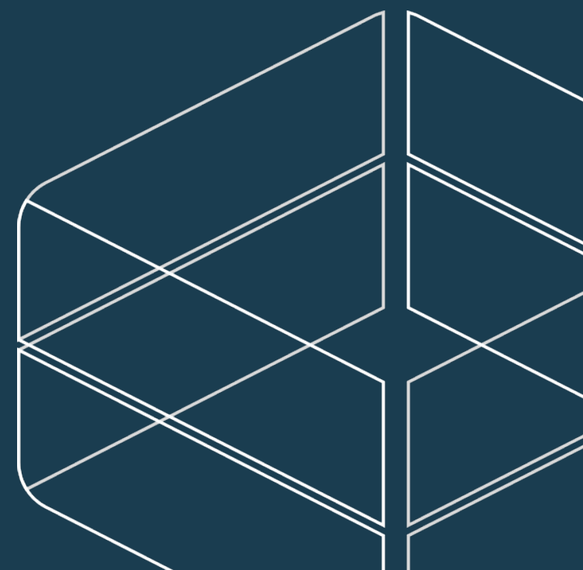
Sandbox

- Inspects a website or a file.
- Inspects the content while it being opened and tries to access memory or CPU.
- If it were malware, it will cause anomalous behavior and the sandbox will detect this activity.

Sandbox

- Rely on known indicators
- It’s all about the context
  - Check if they are running on a real PC or VM.
  - Delay loop of a few days before actually running the malware
  - Malware that uses the location it downloaded to as a key to the payload
    - \Users\<username>\Downloads (In windows)
  - Encrypt the content with a payload that will be translated using google translate to hide the malicious domain

DEMO



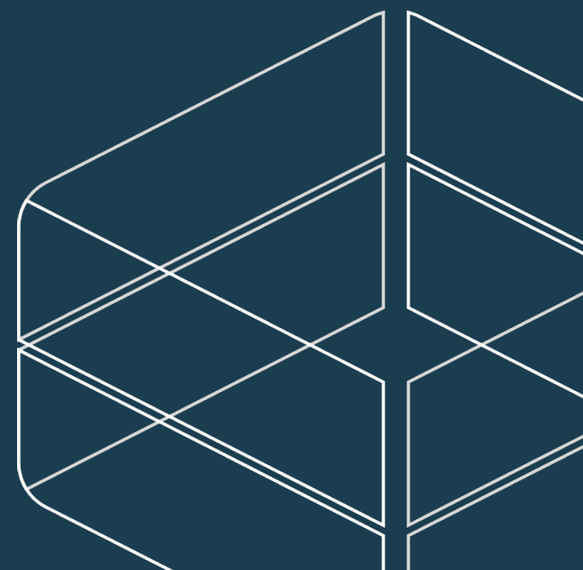
Content Disarm and Reconstruction

- Altering the internal file structure
- Removing embedded objects (scripts, macros, etc.)
- Converting the file format

Isolation

- Open the document inside an isolated environment
- Interact with the file with VDI based solutions

PIPELINE



Real-Time Pipeline

File Type detection

Signatures

Static analysis

Link to isolated version

Near Real-Time Pipeline

File Type detection

Signatures

Static analysis

CDR

Link to isolated version

Offline Pipeline

File Type detection

Signatures

Static analysis

Link to isolated version

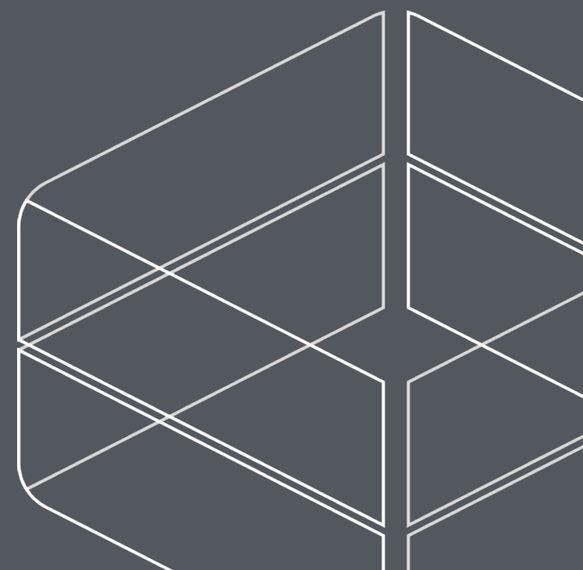
CDR

Sandbox

Summary

- Build your defense based on multiple strategies
- Differentiate between real-time and offline analysis

Q&A



The Irrelevance of K-Byte Detection – Building a Robust Pipeline for Malicious Document

Dor Knafo
Security Research Leader – Dor@fire.glass

Dan Amiga
Co-Founder and CTO - Dan@fire.glass