# FITSEC MalwareDNA

## PRECISE MALWARE PROFILING
*FASTER, DEEPER, SMARTER*

## What are the benefits of MalwareDNA?

| | |
|---|---|
| Takes only seconds | TIME SAVING |
| Precisely identifies malware | ACCURACY |
| Resources to the right target | INVESTIGATION PRIORITIZATION |
| Avoid false sense of security | OPERATIONAL RELIABILITY |
| Stops the attack at once | COMPREHENSIVE DEFENSE |
| Detects whether the threat is linked to a previously observed attack campaign | ATTACK CAMPAIGN DETECTION |

IF YOU SUSPECT THAT A FILE MAY BE MALICIOUS,
UPLOAD IT TO OUR VIRTUAL SERVER AND RECEIVE A RESPONSE INDICATING WHETHER IT IS:
1. A TARGETED ATTACK,
2. BULK MALWARE, OR
3. A SAFE FILE,
ALL WITHIN SECONDS

## What is MalwareDNA?

**MalwareDNA** detects malware by breaking down the file's contents into **genetic code blocks**, which are compared against **Fitsec's extensive malware gene database.** This enables exceptionally **accurate** and **fast** malware detection, fully **automated** and completed **in just seconds.**

### IT REVEALS:

- Whether the file is malicious
- Which malware family it belongs to
- Exactly which malware it is
- Whether the sample contains code seen in previous attacks, even from years ago

THIS IS NOT A TRADITIONAL SIGNATURE-BASED SCAN, BUT A GENETIC-LEVEL ANALYSIS, WHICH IS BASED ON STRUCTURAL SIMILARITY, THAT IS THE FINGERPRINT OF THE CODE

## WHY ARE EXISTING PRACTICES NOT ENOUGH TO RECOGNIZE TARGETED ATTACKS?

**Traditional tools** such as antivirus products or threat intelligence feeds often provide **generic classifications without context**

**ALERT**
- Firewall alert
- Antivirus alert
- User report (e.g. suspicious activity on a machine)
- Other report or observation (indirect signal)

→ UNCERTAIN GENERIC DETECTION WITH NO CONTEXT

→ THREAT SEVERITY UNKNOWN ?

→ HIGHLY LABORIOUS MANUAL INVESTIGATION

→ SERIOUS THREAT MAY GO UNDETECTED

**MalwareDNA SOLVES THIS INACCURACY**
by providing an automatic and precise analysis that reveals whether the case involves a targeted attack or bulk malware, **even if the code has been modified**

## HOW MalwareDNA REDUCES WORKLOAD AND SPEEDS UP RESPONSE

**ALERT**
- Firewall alert
- Antivirus alert
- User report (e.g. suspicious activity on a machine)
- Other report or observation (indirect signal)

→ AUTOMATED GENETIC ANALYSIS STARTS

→ DETECTION READY IN SECONDS

→ CLEAR RESULT PRODUCED

→ TIME, EFFORT, ENERGY, AND MONEY SAVED

FITSEC MalwareDNA
UPLOAD, DETECT, RESPOND IMMEDIATELY

**MalwareDNA** ACCURATELY DETECTS **PE**-FORMAT **BINARY FILES** IN THE **WINDOWS** ENVIRONMENT
- ☑ .exe
- ☑ .dll
- ☑ .sys

**IT DOES NOT** SUPPORT other file types such as **Office documents, PDFs, scripts,** or **web links**



## Who is MalwareDNA intended for?

| | |
|---|---|
| MEDIUM AND LARGE ENTERPRISES WITH IN-HOUSE IT EXPERTISE | COMPANIES AND PROFESSIONALS PROVIDING CYBERSECURITY SERVICES |
| PUBLIC SECTOR OPERATORS WITH DIRECT RESPONSIBILITY FOR CYBERSECURITY | ALSO FOR SMALLER COMPANIES, IF THE ORGANIZATION HAS AN OWN IT STAFF |

## 100% FINNISH EXPERTISE

Have further questions?
Reach out to learn how **MalwareDNA** can support your organization's security operations

TUOMO.HAMALAINEN@FITSEC.COM | SUPPORT@FITSEC.COM