ASC27

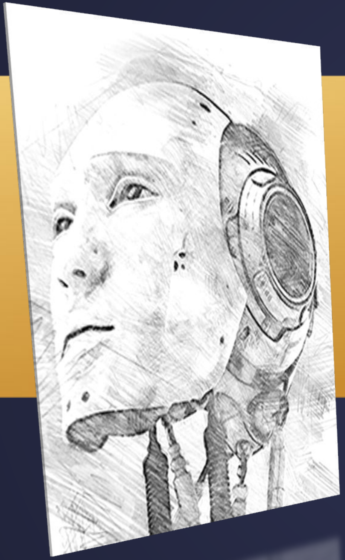
AI BlackBox INSPECTOR

CYBER-SECURITY AIDED BY ARTIFICIAL INTELLIGENCE

ASC27 | 2022. REV 1.0 ENG

What We Do

THE AI COMPANY “We Build Knowledge”



ARTIFICIAL **INTELLIGENCE**

CYBER **SECURITY**

Passionate people

Our dream Team

30 PEOPLE TEAM

Offices in **Rome**, **Milan**, **Bologna**, and **Chieti**
AVG HeadCount growth +10%/month
Multiple Award winnings
Entitled supplier of many large enterprises

Find us on Ariba Network

400 YEARS EXPERIENCE

15 DEVELOPERS

8 ARTIFICIAL INTELLIGENCE

We develop WITH them

Software PARTNERS

ARTIFICIAL INTELLIGENCE
Google Cloud Platform

ARTIFICIAL INTELLIGENCE
Microsoft for Startups

ARTIFICIAL INTELLIGENCE
aws

CYBER SECURITY
irdeto

We develop ON them

Silicon PARTNERS

ARTIFICIAL INTELLIGENCE
NVIDIA
INCEPTION PROGRAM

ARTIFICIAL INTELLIGENCE
HUAWEI

ARTIFICIAL INTELLIGENCE
alhua TECHNOLOGY

ARTIFICIAL INTELLIGENCE
Panasonic

ARTIFICIAL INTELLIGENCE
JMCGROUP®
TECHNOLOGY DESIGNER

ARTIFICIAL INTELLIGENCE
and more...

Best Startup Pitch **WINNER**

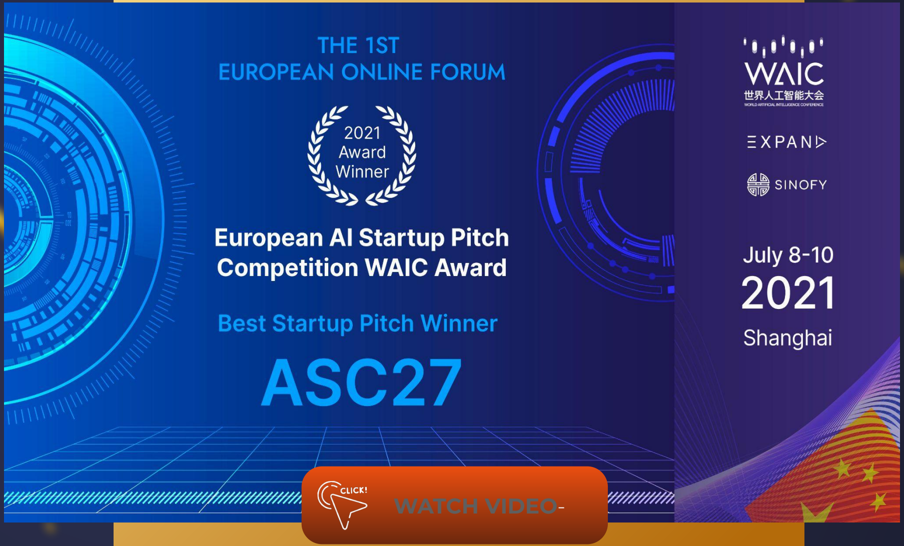
WAIC
2021世界人工智能大会
WORLD ARTIFICIAL INTELLIGENCE CONFERENCE

Awarded by

WORLD ARTIFICIAL INTELLIGENCE CONFERENCE 2021

WITH

asimov



THE 1ST
EUROPEAN ONLINE FORUM

2021
Award
Winner

European AI Startup Pitch Competition WAIC Award

Best Startup Pitch Winner

ASC27

WAIC
世界人工智能大会
WORLD ARTIFICIAL INTELLIGENCE CONFERENCE

EXPAND

SINOFY

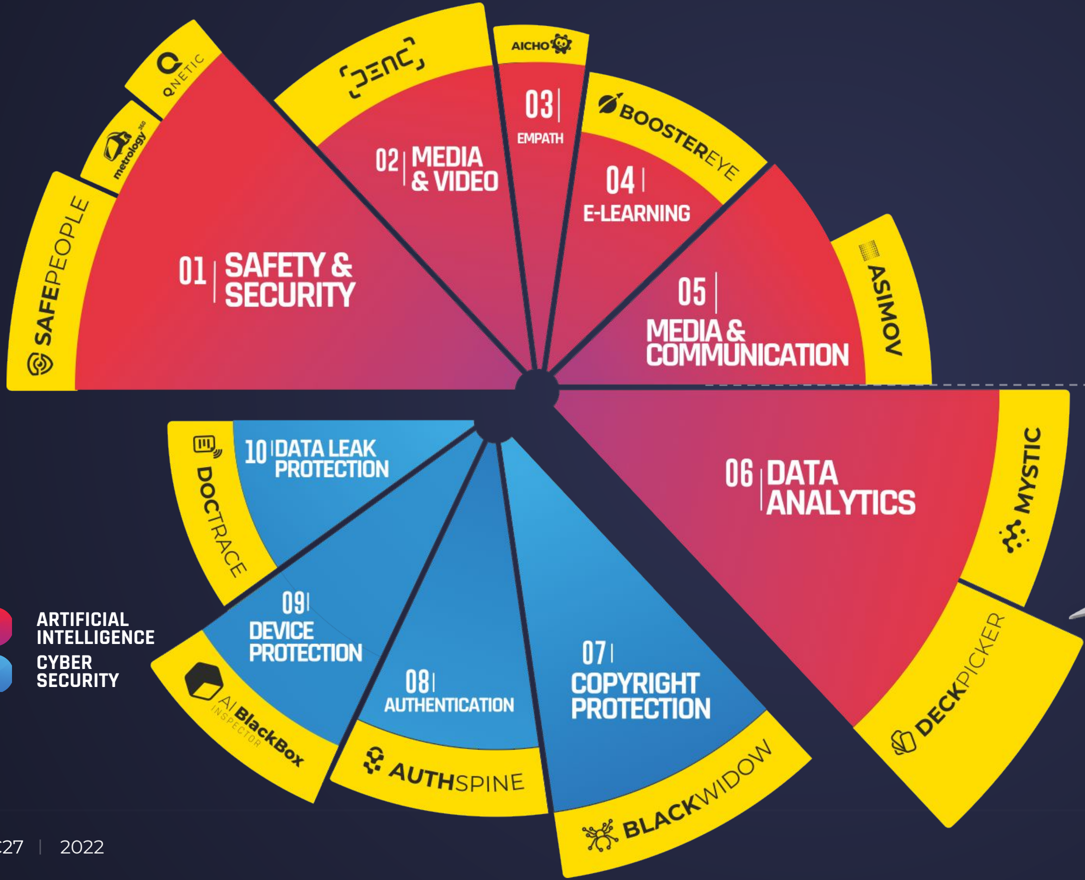
July 8-10
2021
Shanghai

CLICK!
WATCH VIDEO

World **TOP 10 BPAA**

(Best Practice Applied Algorithms)

Product Portfolio



01 | SAFETY & SECURITY
SAFEPEOPLE
metrology
QNETIC

02 | MEDIA & VIDEO
DENC

03 | EMPATH
AICHO

04 | E-LEARNING
BOOSTEREYE

05 | MEDIA & COMMUNICATION
ASIMOV

06 | DATA ANALYTICS
MYSTIC
DECKPICKER

07 | COPYRIGHT PROTECTION
BLACKWIDOW

08 | AUTHENTICATION
AUTHSPINE

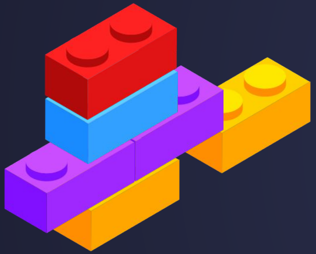
09 | DEVICE PROTECTION
AI BlackBox INSPECTOR

10 | DATA LEAK PROTECTION
DOCTRACE

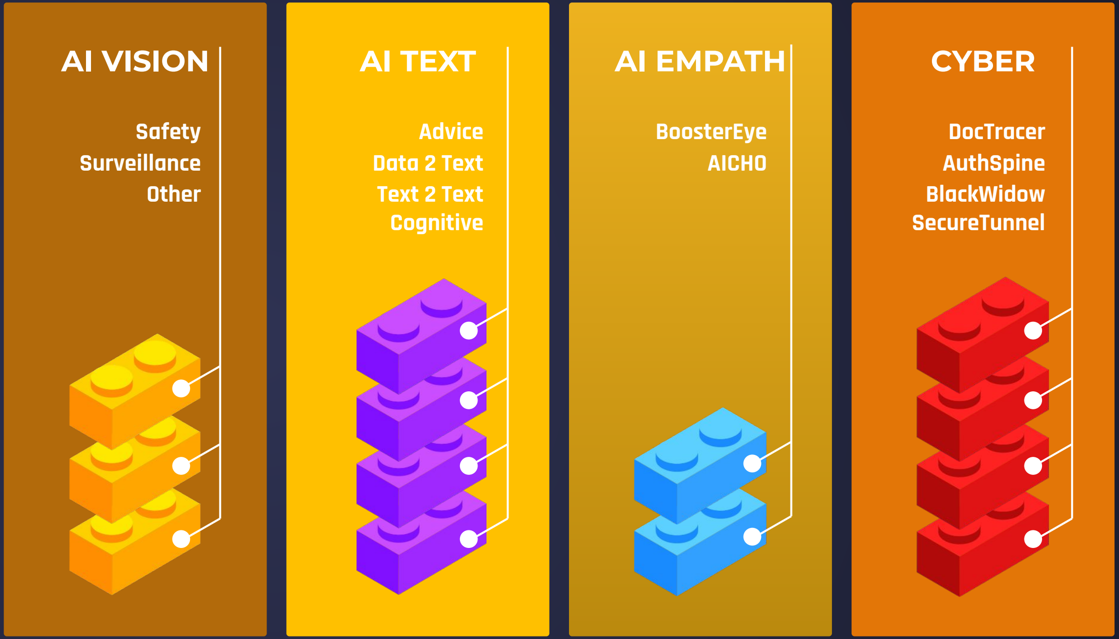
🟥 ARTIFICIAL INTELLIGENCE
🟦 CYBER SECURITY

HOMEBREWED SKILLS

We don’t RENT AI, We DO AI for our customers.



Customization and vertical developing capacity from ground up. We can arrange our Cognitive pipeline bricks to satisfy our customer’s needs. AI Engineering and software skills in a single Company. From Embedded systems to the Cloud and beyond.



AI VISION

Safety
Surveillance
Other

AI TEXT

Advice
Data 2 Text
Text 2 Text
Cognitive

AI EMPATH

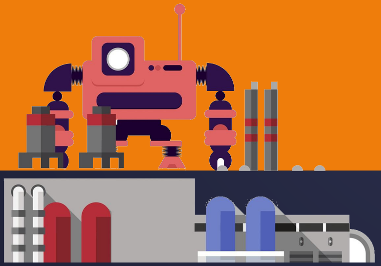
BoosterEye
AICHO

CYBER

DocTracer
AuthSpine
BlackWidow
SecureTunnel

PROBLEM

Nowadays, **all industry** plants are plenty of **unknown IoT and embedded devices.**
Very often, the owners **don't have the capability to inspect the source code** of those devices.
BlackBox inspection is a time-consuming Activity.
No one can check ALL the devices they had attached to their network.



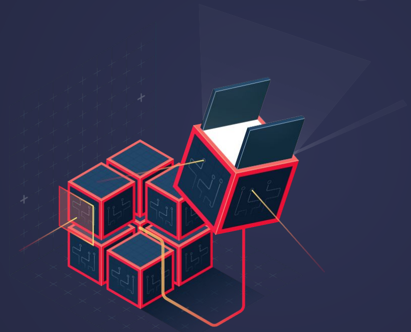
SOLUTION

AI POWERED

Using AI BlackBox Inspector, humans can focus only on the devices that need their attention.

IOT DEVICES

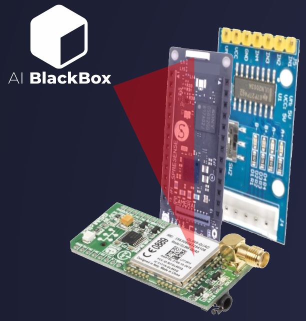
TRL6

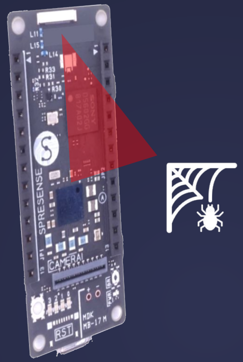


AI POWERED

Security also in external devices: from device the firmware is extracted and analyzed, identifying backdoors and security issues.

ALL IN ONE



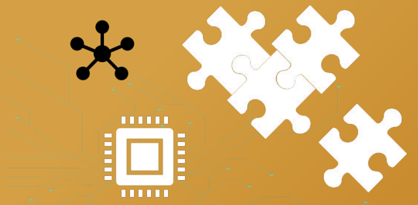


01. Firmware Extraction

- Device based
- OTA Update based
- Repository Based

02. Binary Inspection

- Binary Analytics
- Backdoor Database
- Vulnerability Database



03. Language Lifting

- Convert sequences of 0 and 1 into a natural language description and transform the code making it more **understandable** and **human-readable**.

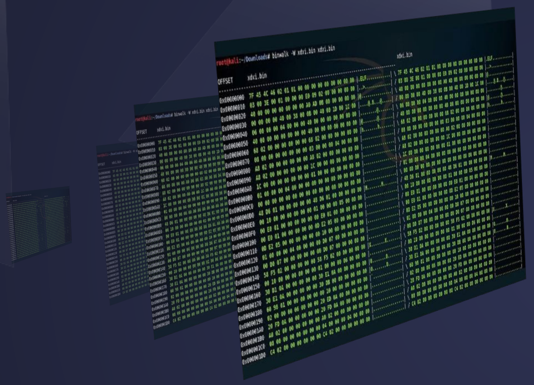
04. AI Inspection

- Use **AI** to identify possible **hidden threats** in the device internal functions. **All in one platform.**

HOW IT WORKS?

IOT Device

The software analyzes and is able to read any device inside any circuit



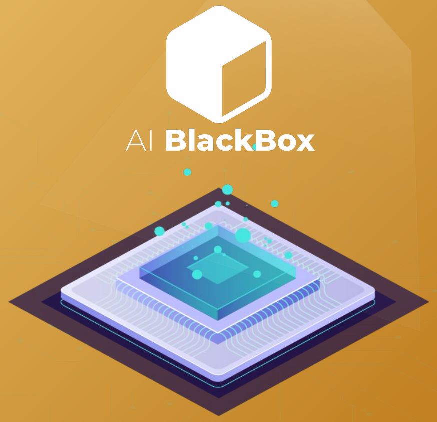
Binary Firmware **Extraction**

The software extracts the binary code of the firmware

AI POWERED

High Level Language **Lifting**

Refinement of the binary code and subdivision into classes and categories according to the functions in an High-Level language



AI POWERED search backdoor

The AI analyzes the refined code and autonomously detects backdoor or security problems

Information Extrapolation

Extract and display information about the specified firmware:

- **Disassembled/decompiled** individual function code navigable and displayed in blocks.
- Various information from the binary (text, constants, etc).
- Possibility to analyze the firmware **directly from our platform**.

DEEP

IN DEPTH DESCRIPTION OF THE FEATURE

Analysis

Deep neural network-based behavioral analysis:

- Creation of **ad-hoc models** and **heuristics** for the discovery of **abnormal and undocumented behaviors** in the specified firmware.
- Creation of a **functionality profile** and detection of possible **deviation from the expected behavior**.
- Alarming and analysis system for the detections mentioned above.

DEEP

IN DEPTH DESCRIPTION OF THE FEATURE

Deep Neural Network

Deep neural network analysis for backdoor detection with **automatic alarm**:

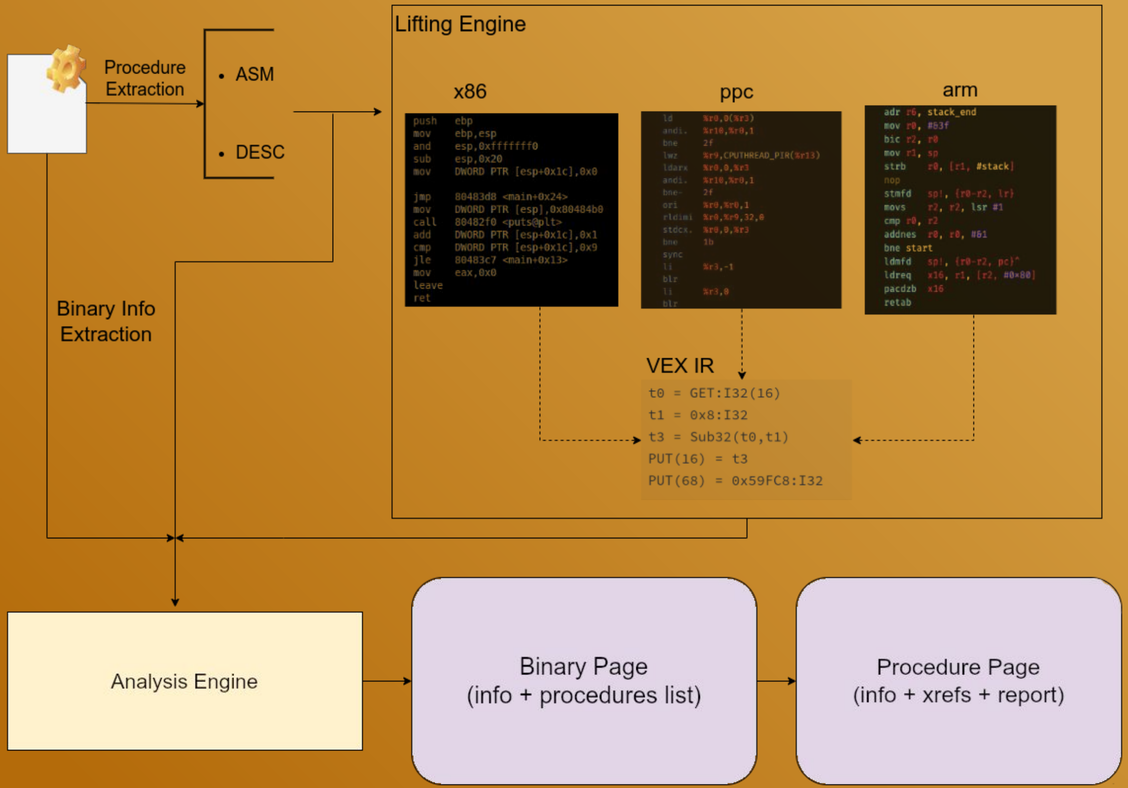
- Creation of **ad-hoc models** for **backdoor detection** in the specified firmware.
- Pre-existing backdoors.
- Firmware compromised in transit **(update)**.
- Firmware compromised during use (modified by **exploitation** of a device vulnerability).

DEEP
IN DEPTH DESCRIPTION OF THE FEATURE

Architecture Overview (Information Extraction)

TECHNICAL

VERY TECHNICAL DESCRIPTION OF THE PROJECT



x86

```
push   ebp
mov    ebp,esp
and    esp,0xfffffff0
sub    esp,0x20
mov    DWORD PTR [esp+0x1c],0x0

jmp    80483d8 <main+0x24>
mov    DWORD PTR [esp],0x80484b0
call   80482f0 <puts@plt>
add    DWORD PTR [esp+0x1c],0x1
cmp    DWORD PTR [esp+0x1c],0x9
jle    80483c7 <main+0x13>
mov    eax,0x0
leave
ret
```

ppc

```
ld      %r0,0(%r3)
andi.   %r10,%r0,1
bne     2f
lwz     %r9,CPUTHREAD_PIR(%r13)
ldarx   %r0,0,%r3
andi.   %r10,%r0,1
bne-    2f
ori     %r0,%r0,1
rldimi  %r0,%r9,32,0
stdcx.  %r0,0,%r3
bne     1b
sync
li      %r3,-1
blr
li      %r3,0
blr
```

arm

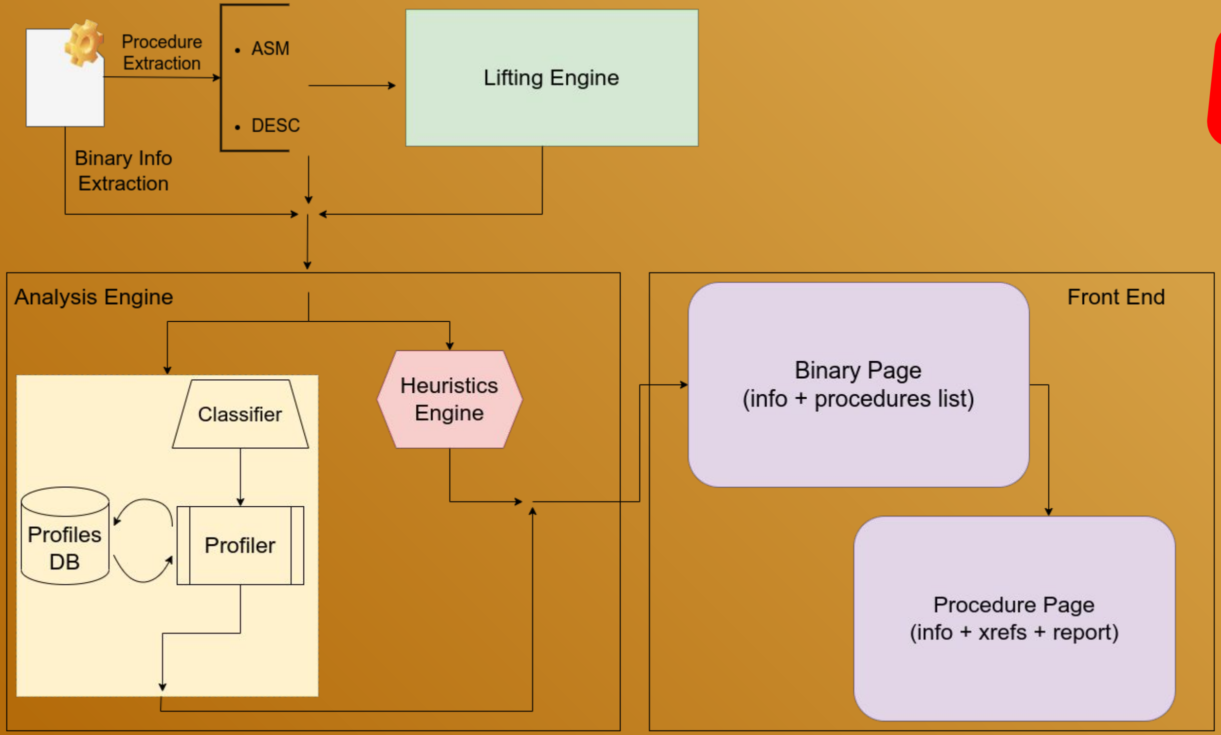
```
adr r6, stack_end
mov r0, #63f
bic r2, r0
mov r1, sp
strb    r0, [r1, #stack]
nop
stmfd   sp!, {r0-r2, lr}
movs    r2, r2, lsr #1
cmp r0, r2
addnes  r0, r0, #61
bne start
ldmfd   sp!, {r0-r2, pc}^
ldreq   x16, r1, [r2, #0x80]
pacdzb  x16
retab
```

VEX IR

```
t0 = GET:I32(16)
t1 = 0x8:I32
t3 = Sub32(t0,t1)
PUT(16) = t3
PUT(68) = 0x59FC8:I32
```

Architecture Overview (AI Powered Analysis)

TECHNICAL
VERY TECHNICAL DESCRIPTION OF THE PROJECT

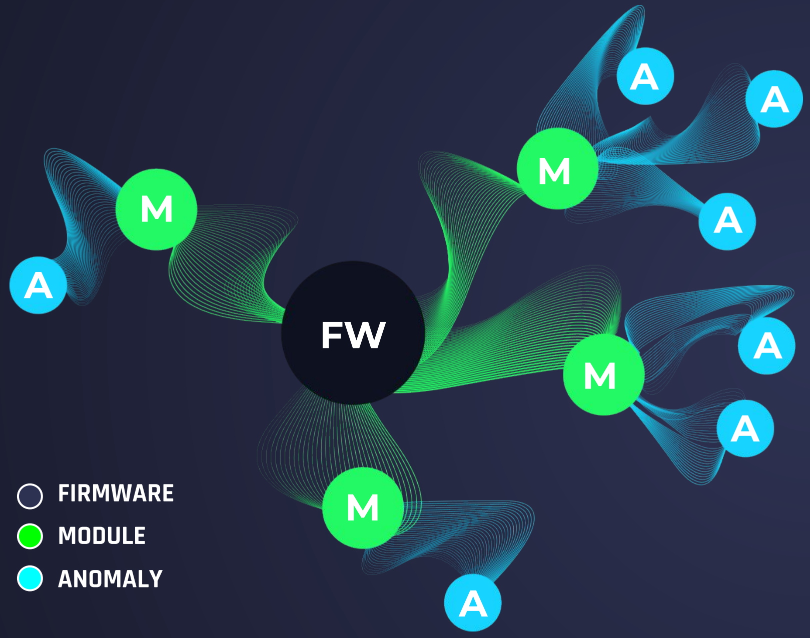


Architecture Overview (Information Extraction)

	AI BlackBox	Traditional
Architecture Independent Analysis	✓	✗
Overall Data Analysed	✓	✓
Architectures Scalability	✓	✓
Features Scalability	✓	✗
Maintenance Effort	✓	✗

ASC27

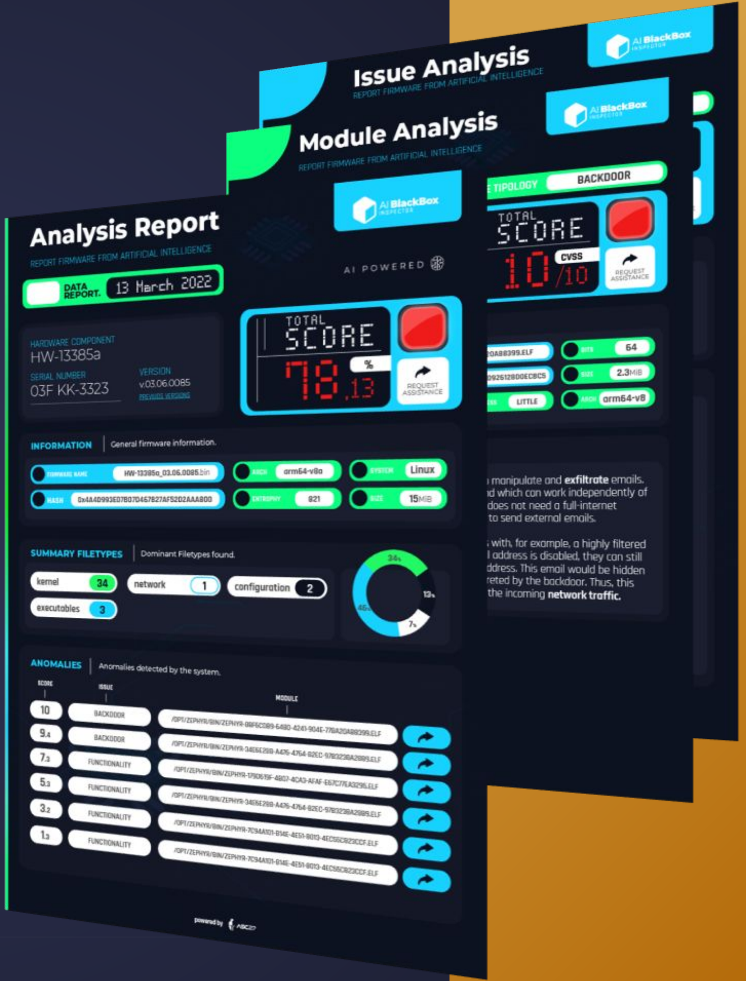
ALL IN ONE



○ FIRMWARE

🟢 MODULE

🔵 ANOMALY



Issue Analysis

REPORT FIRMWARE FROM ARTIFICIAL INTELLIGENCE

TIPOLOGY BACKDOOR

TOTAL SCORE 10/10 CVSS

0A88399.ELF | BITS 64

092612800EC8CS | SIZE 2.3MIB

LITTLE | ARCH arm64-v8

manipulate and **exfiltrate** emails. d which can work independently of does not need a full-internet to send external emails.

with, for example, a highly filtered l address is disabled, they can still ddress. This email would be hidden reted by the backdoor. Thus, this the incoming **network traffic.**

Module Analysis

REPORT FIRMWARE FROM ARTIFICIAL INTELLIGENCE

Analysis Report

REPORT FIRMWARE FROM ARTIFICIAL INTELLIGENCE

DATA REPORT. 13 March 2022

HARDWARE COMPONENT
HW-13385a

SERIAL NUMBER
03F KK-3323

VERSION
v.03.06.0085
PREVIOUS VERSIONS

TOTAL SCORE 78,13 %

INFORMATION | General firmware information.

FIRMWARE NAME HW-13385a_03.06.0085.bin | ARCH arm64-v8a | SYSTEM Linux

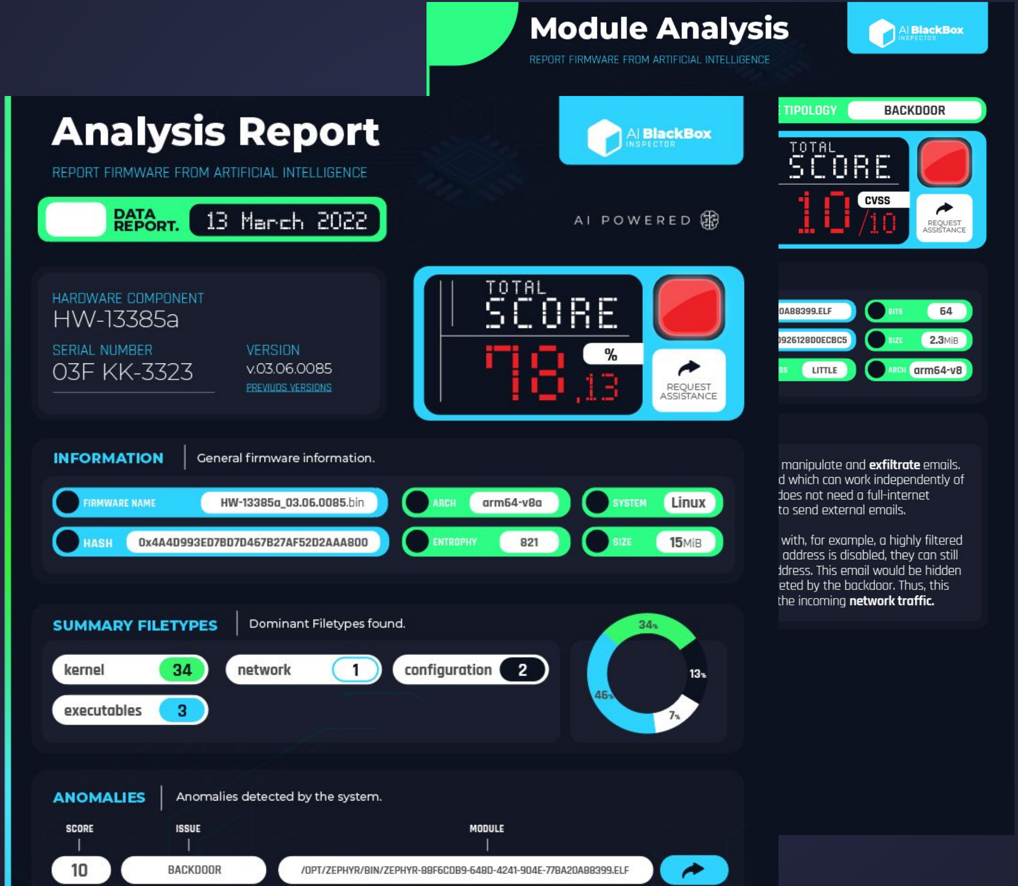
HASH 0x4A4D993E07B07D467B27AF5202AAA800 | ENTROPY 8.21 | SIZE 15MIB

SUMMARY FILETYPES | Dominant Filetypes found.

kernel	34
network	1
configuration	2
executables	3

ANOMALIES | Anomalies detected by the system.

SCORE	ISSUE	MODULE
10	BACKDOOR	/OPT/ZEPHYR/BIN/ZEPHYR-0BF6C0B9-6480-4241-904E-77BA20A88399.ELF
9.4	BACKDOOR	/OPT/ZEPHYR/BIN/ZEPHYR-34E6E298-A476-4764-B2EC-97B3238A2989.ELF
7.3	FUNCTIONALITY	/OPT/ZEPHYR/BIN/ZEPHYR-1790619F-4807-4CA3-AFAF-E67C77EA3295.ELF
5.3	FUNCTIONALITY	/OPT/ZEPHYR/BIN/ZEPHYR-34E6E298-A476-4764-B2EC-97B3238A2989.ELF
3.2	FUNCTIONALITY	/OPT/ZEPHYR/BIN/ZEPHYR-7C94A101-B14E-4E51-8013-4EC55C823CCF.ELF
1.3	FUNCTIONALITY	/OPT/ZEPHYR/BIN/ZEPHYR-7C94A101-B14E-4E51-8013-4EC55C823CCF.ELF



Module Analysis

REPORT FIRMWARE FROM ARTIFICIAL INTELLIGENCE

AI BlackBox INSPECTOR

TIPOLOGY BACKDOOR

TOTAL SCORE 10 CVSS /10

REQUEST ASSISTANCE

	0A88399.ELF	BITS	64
	92612800ECBC5	SIZE	2.3MiB
SS	LITTLE	ARCH	arm64-v8

manipulate and **exfiltrate** emails.
d which can work independently of
does not need a full-internet
to send external emails.

with, for example, a highly filtered
address is disabled, they can still
ddress. This email would be hidden
eted by the backdoor. Thus, this
the incoming **network traffic.**

Analysis Report

REPORT FIRMWARE FROM ARTIFICIAL INTELLIGENCE

AI BlackBox INSPECTOR

DATA REPORT. 13 March 2022

AI POWERED

HARDWARE COMPONENT
HW-13385a

SERIAL NUMBER
03F KK-3323

VERSION
v.03.06.0085
PREVIUOS VERSIONS

TOTAL SCORE 78 % ,13

REQUEST ASSISTANCE

INFORMATION | General firmware information.

FIRMWARE NAME	HW-13385a_03.06.0085.bin	ARCH	arm64-v8a	SYSTEM	Linux
HASH	0x4A4D993ED7BD7D467B27AF52D2AAA800	ENTROPHY	821	SIZE	15MiB

SUMMARY FILETYPES | Dominant Filetypes found.

kernel	34
network	1
configuration	2
executables	3

ANOMALIES | Anomalies detected by the system.

SCORE	ISSUE	MODULE
10	BACKDOOR	/OPT/ZEPHYR/BIN/ZEPHYR-88F6CDB9-648D-4241-904E-77BA20A88399.ELF

THANK YOU

Q&A TIME

AI **BlackBox**
INSPECTOR

CEO Nicola **Grandis** ✉ nicola@asc27.com