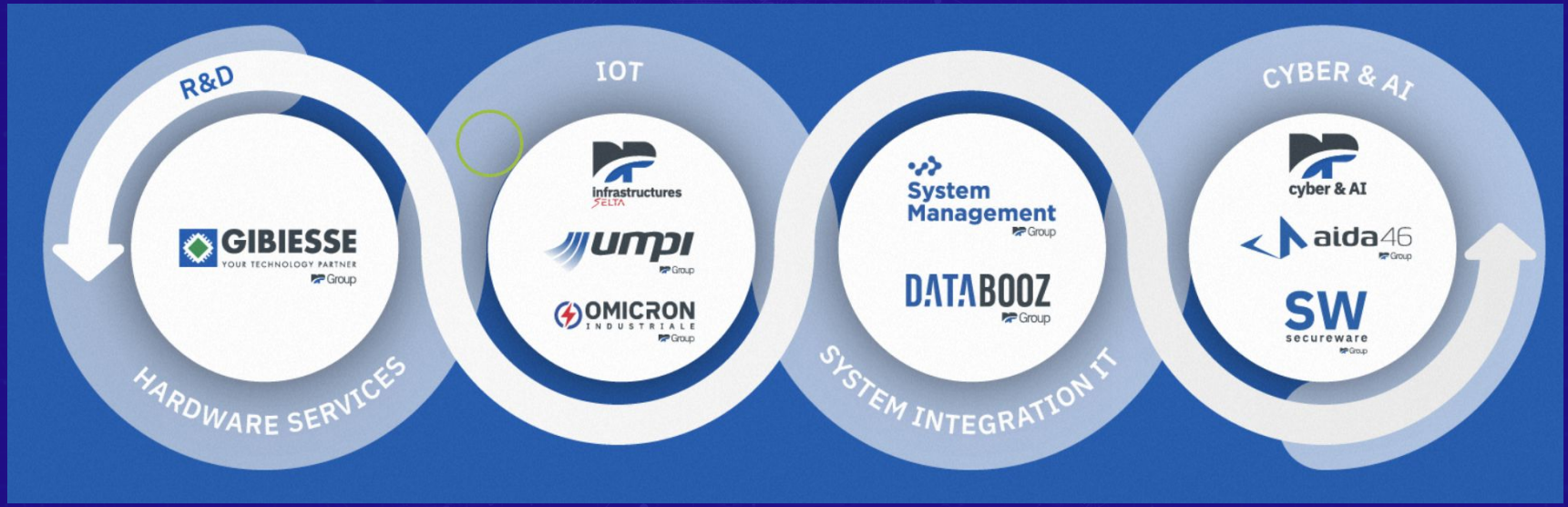
Cyber Minacce Industriali: Come Difendersi dai Rischi dei Dispositivi di Rete e IoT

www.aida46.com
www.dplatforms.it

Alessandro Capucci - CTO



1
CAPOGRUPPO

7
AZIENDE CONTROLLATE

16
SEDI TUTTE IN ITALIA

460+
TOTALE DIPENDENTI,
+12% RISPETTO AL 2022

87%
TECNICI, COMMERCIALI &
R&D SU TOT. DIPENDENTI

Infrastrutture IT sempre più ricche di dispositivi:

- **Sempre più potenti**
- **Connessi e iperconnessi**
- **Connettività LAN, WAN, 4/5G, LoraWan, ZigBee, ModBus, OPC UA, …**
- **Sempre più funzioni e complessità**

Apparati di Networking

Videosorveglianza

Domotica

Automazione Industriale

I dispositivi in rete hanno la possibilità di:

- Monitorare
- Esfiltrare informazioni
- Creare disservizi e blocchi di altri sistemi
- Creare un punto di accesso alla rete aziendale a soggetti terzi

Ma:

- Quasi mai sono intenzionali
- Spesso sono dovuti a BUG o superficialità progettuale sfruttate da malintenzionati

Come difendersi:

- **Progettazione dell'infrastruttura IT (best practices, segmentazione, segregazione, isolamento, policy)**
- **Apparati attivi di monitoraggio e analisi del traffico di rete**
- **Analisi preventiva del software (firmware)**

Ridurre al minimo i rischi garantendo:

- **operatività**
- **amministrabilità**
- **contenimento dei costi**

VECTOR LAB
Offensive Security Lab and Research

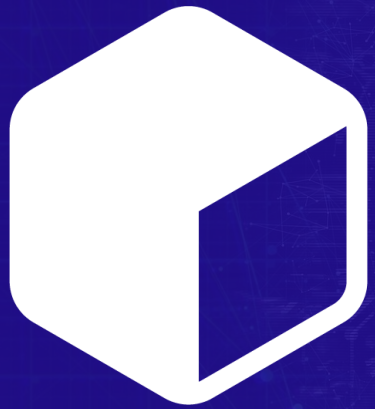
- **Team di AIDA46 dedicato al reverse engineering e analisi dei firmware degli apparati connessi in rete**
- **Analisi sui device e sul contesto operativo in cui operano, i fattori di rischio e le possibili contromisure**
- **Attività svolte per enti governativi, infrastrutture critiche e industria**
- **Utilizzo di strumenti sviluppati dal team stesso, come AIBlackBox (AIBB) basato su una AI addestrata sull'esperienza del team per una pre-analisi dei fattori di rischio usabile anche da non specialisti**

VECTOR LAB
Offensive Security Lab and Research

Esempi di rischi identificati dal VectorLab:

- **Account/Password di servizio statiche**
- **Reset di password non protette**
- **Accesso remoto al dispositivo non dichiarato e non persistente**
- **Accesso remoto al dispositivo e non protetto**
- **Bypass dell’autenticazione utente**
- **Procedure “fuori contesto” per il tipo di dispositivo o di debug**

aida46 Group



AI BlackBox INSPECTOR

AI BlackBox INSPECTOR

aida46 Group

WHAT IS ITS PURPOSE

USING AI BLACKBOX INSPECTOR, HUMANS CAN FOCUS ONLY

on the devices that need their attention

PROBLEM

- Unknown IOT and embedded devices
- Owners don't have the capability to inspect the source code
- No one can check ALL the devices they had attached to their network.

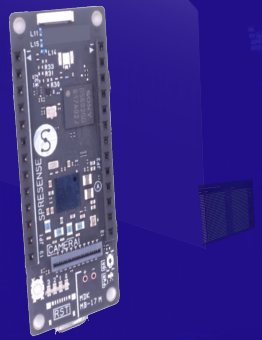
SOLUTION AI BlackBox INSPECTOR

- FIRMWARE EXTRACTION I DEVICE BASED I OTA UPDATE BASED I REPOSITORY BASED
- BINARY INSPECTION I BINARY ANALYTICS I BACKDOOR DATABASE I VULNERABILITY DATABASE
- LANGUAGE LIFTING I TRANSFORM THE CODE MAKING IT MORE UNDERSTANDABLE AND HUMAN-READABLE.
- AI INSPECTION I USE AI TO IDENTIFY POSSIBLE HIDDEN THREATS

AI BlackBox
INSPECTOR

aida46 Group

HOW IT WORKS

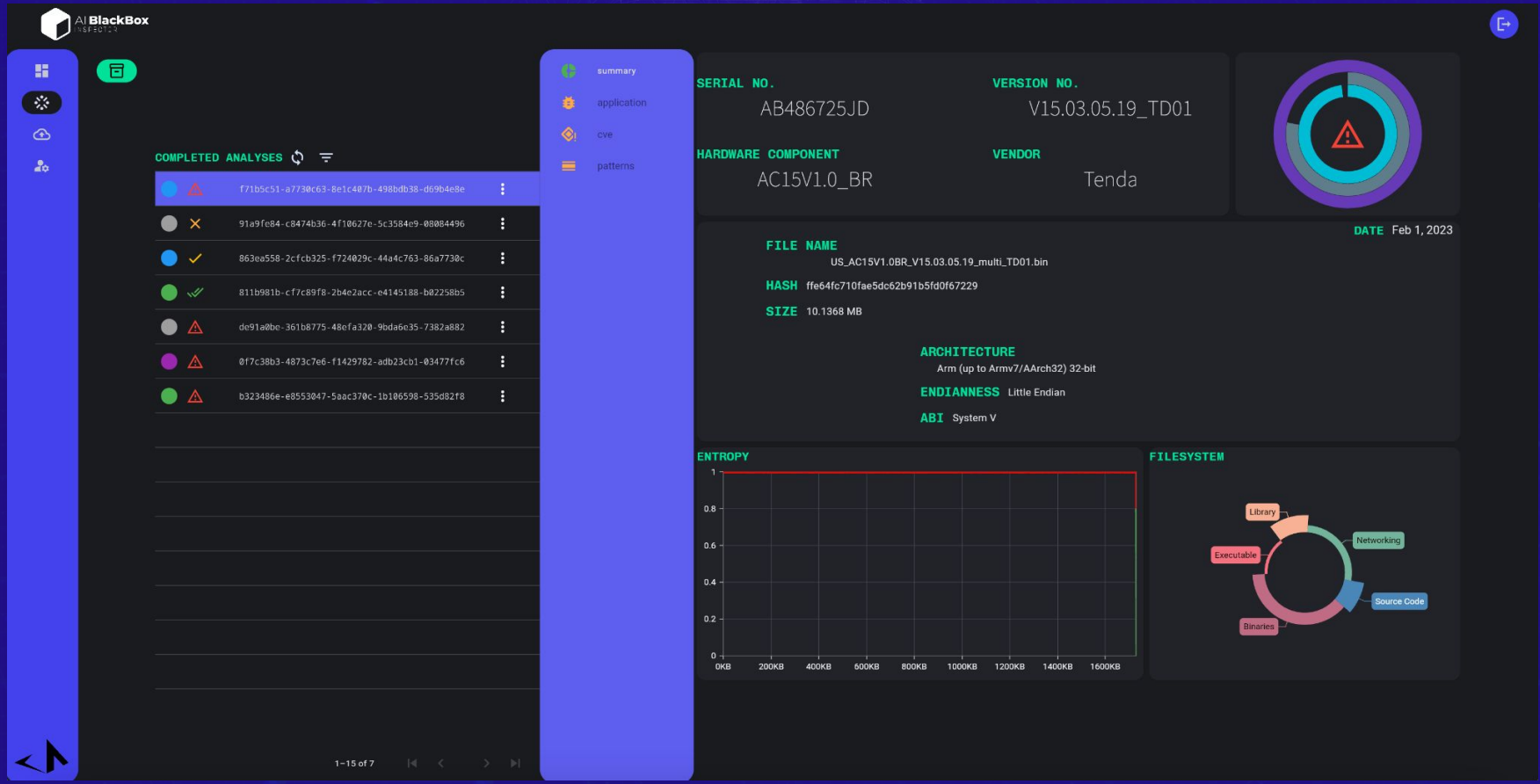


IOT
Device

Binary Firmware
Extraction

High Level
Language **Lifting**

AI POWERED
search backdoor
and vulnerability


AI BlackBox
COMPLETED ANALYSES
f71b5c51-a7730c63-8e1c407b-498bdb38-d69b4e8e
91a9fe84-c8474b36-4f10627e-5c3584e9-08084496
863ea558-2cfcb325-f724029c-44a4c763-86a7730c
811b981b-cf7c89f8-2b4e2acc-e4145188-b02258b5
de91a0be-361b8775-48efa320-9bda6e35-7382a882
0f7c38b3-4873c7e6-f1429782-adb23cb1-03477fc6
b323486e-e8553047-5aac370c-1b106598-535d82f8
1–15 of 7
summary
application
cve
patterns
SERIAL NO.
AB486725JD
VERSION NO.
V15.03.05.19_TD01
HARDWARE COMPONENT
AC15V1.0_BR
VENDOR
Tenda
DATE Feb 1, 2023
FILE NAME
US_AC15V1.0BR_V15.03.05.19_multi_TD01.bin
HASH ffe64fc710fae5dc62b91b5fd0f67229
SIZE 10.1368 MB
ARCHITECTURE
Arm (up to Armv7/AArch32) 32-bit
ENDIANNESS Little Endian
ABI System V
ENTROPY
1
0.8
0.6
0.4
0.2
0
0KB
200KB
400KB
600KB
800KB
1000KB
1200KB
1400KB
1600KB
FILESYSTEM
Library
Networking
Executable
Source Code
Binaries

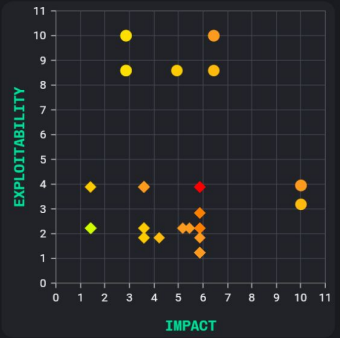
summary
application
cve
patterns

SERIAL NO.
AB486725JD

VERSION NO.
V15.03.05.19_TD01

HARDWARE COMPONENT
AC15V1.0_BR

VENDOR
Tenda



SCORE	VULN ID	SERVICE
9.8	CVE-2016-0746	/usr/bin/nginx
9.8	CVE-2017-20005	/usr/bin/nginx
9.8	CVE-2017-14491	/usr/sbin/dnsmasq
9.8	CVE-2017-14492	/usr/sbin/dnsmasq
9.8	CVE-2017-14493	/usr/sbin/dnsmasq
9.8	CVE-2018-1000517	/bin/busybox
9.8	CVE-2016-2148	/bin/busybox
8.8	CVE-2017-16544	/bin/busybox

- summary
- application
- cve
- patterns

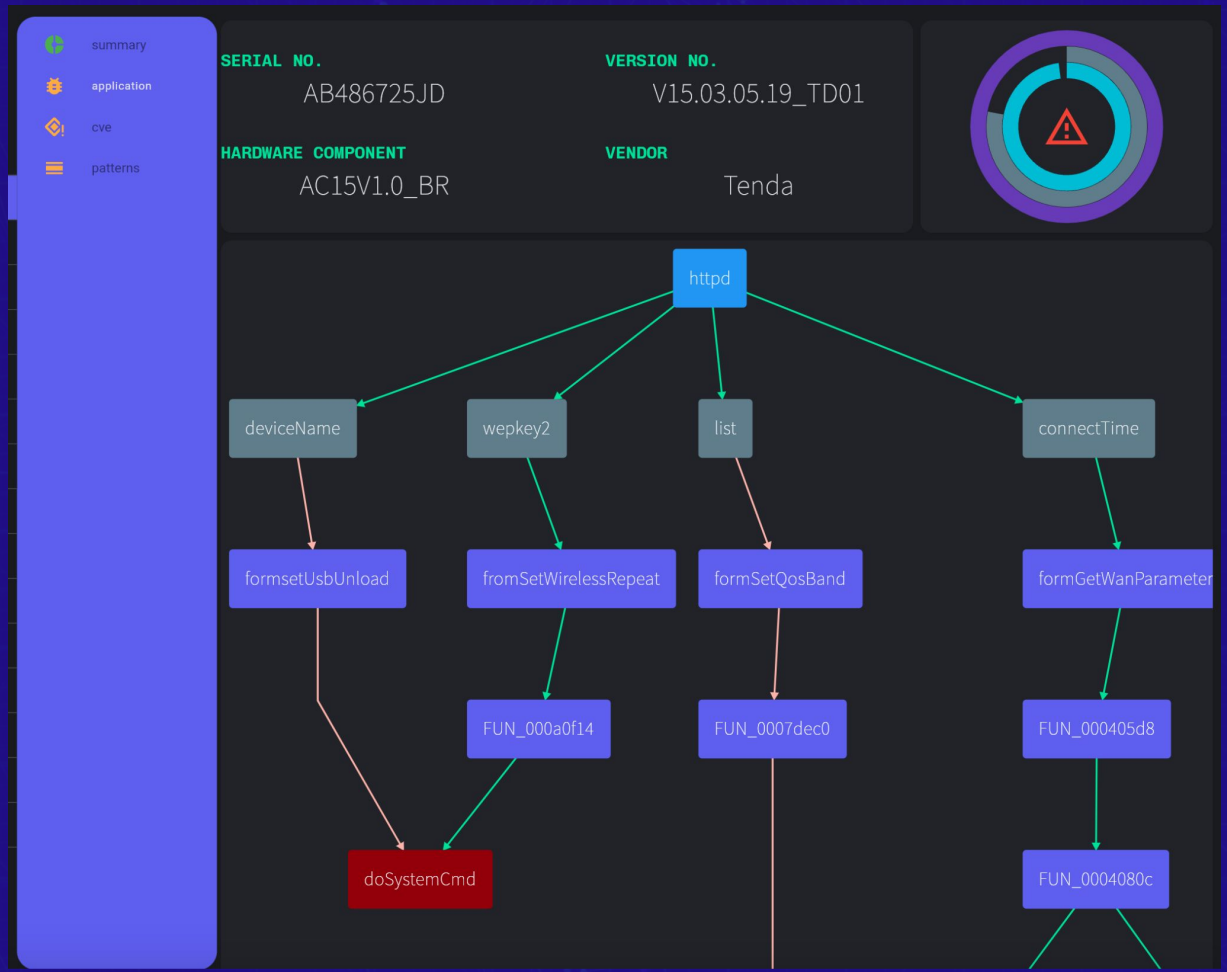
SERIAL NO.
AB486725JD

VERSION NO.
V15.03.05.19_TD01

HARDWARE COMPONENT
AC15V1.0_BR

VENDOR
Tenda

ip addresses	/webroot_ro/js/macro_config.js	(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9...
ip addresses	/webroot_ro/js/static_route.js	(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9...
ip addresses	/webroot_ro/js/yun_safe.js	(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9...
ip addresses	/webroot_ro/js/remote_web.js	(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9...
ip addresses	/webroot_ro/js/main.js	(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9...
ip addresses	/webroot_ro/js/pptp_server.js	(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9...
ip addresses	/webroot_ro/js/index.js	(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9...
ip addresses	/webroot_ro/img/loading-upgrade.gif	(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9...
cryptographic material	/webroot_ro/pem/certSrv.crt	(----BEGIN.{7,22}-----(?:\n|\r|\r\n)(?:[0-9a-zA-Z\+\/=]{6...
cryptographic material	/webroot_ro/pem/privkeySrv.pem	(----BEGIN.{7,22}-----(?:\n|\r|\r\n)(?:[0-9a-zA-Z\+\/=]{6...
ip addresses	/webroot_ro/goform/GetPptpClientCfg.txt	(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9...
ip addresses	/webroot_ro/goform/GetNetControlList.txt	(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9...
ip addresses	/webroot_ro/goform/GetSambaCfg.txt	(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9...
ip addresses	/webroot_ro/goform/getOnlineList.txt	(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9...

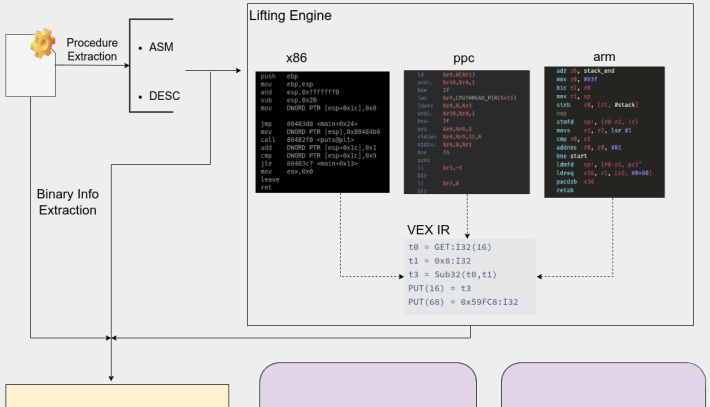

summary
application
cve
patterns
SERIAL NO.
AB486725JD
VERSION NO.
V15.03.05.19_TD01
HARDWARE COMPONENT
AC15V1.0_BR
VENDOR
Tenda
httpd
deviceName
wepkey2
list
connectTime
formsetUsbUnload
fromSetWirelessRepeat
formSetQosBand
formGetWanParameter
FUN_000a0f14
FUN_0007dec0
FUN_000405d8
doSystemCmd
FUN_0004080c

AI BlackBox INSPECTOR

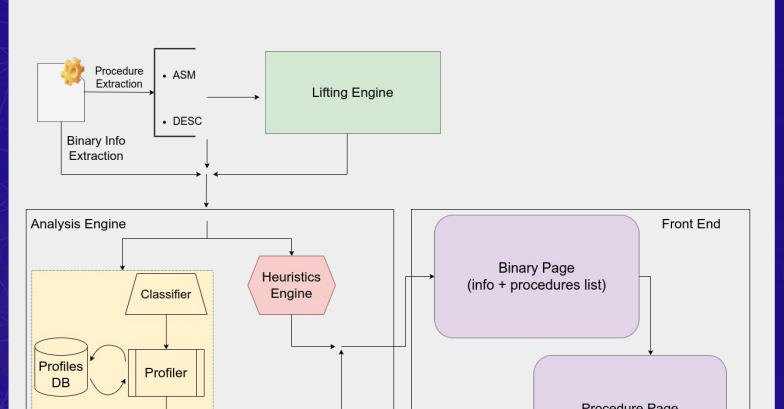
aida46 Group

ARCHITECTURE OVERVIEW

INFORMATION EXTRACTION



AI POWERED ANALYSIS




aida46
Group