The **innovative** appliance of network security.

Q1 / 2022

Roberto Camerinesi

. CTO @CyberEvolution
. Inventor of LECS Project
. Network Penetration Tester
. Security Researcher

Roberto Camerinesi is a researcher in cyber security, developer and CTO of Cyber Evolution SRL. Embracing the filosofy of **Ethical Hacking** in his adolescence, he has been working for over **11 years in the ICT and Security branch.**

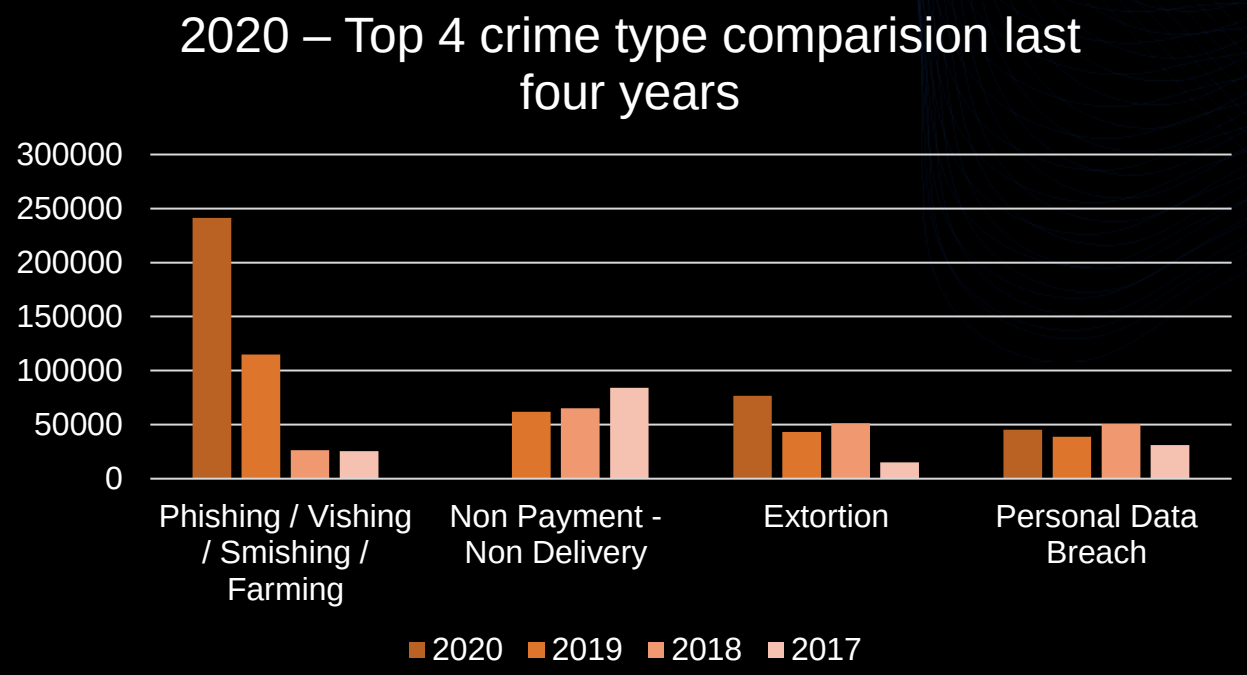
During his life he acquired various **International Certification** in this field and in Network Defence such as **Penetration Tester.**

He believes that security is an idea that needs to be spread, and for this he divulges and studies sistems to **capillarise security**, inventing and **patenting air-gap defense sistems.**
As a **popularizer and speaker**, he has spoken at important events and training institutions such as the Experis Academy master, ITASEC21 and as a finalist in the WMF20 startup competition.

He writes and **contirbutes to several national newspapers** such as Hackin9, InfoSec and CyberSecurity360.

CYBER EVOLUTION

The Problem



* Fonte: FBI Report (USA – 2020)

WHY ARE CYBER THREATS MORE FREQUENT
EVEN IF NOWADAYS PROTECTION SYSTEMS ARE EVER-EVOLVING?

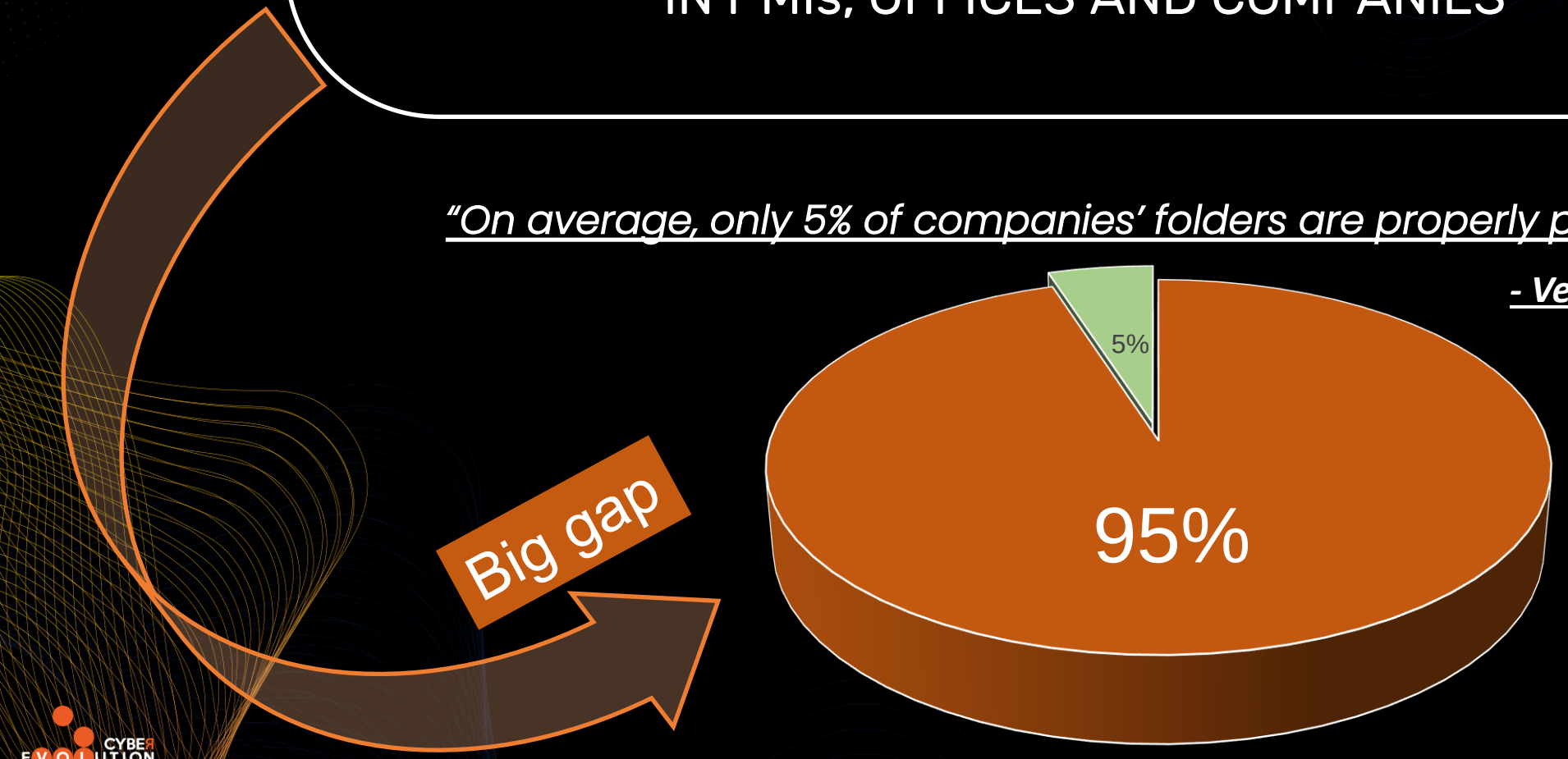
CYBER EVOLUTION

The Cause

A STRONG LACK OF CYBER SECURITY IMPLEMENTATION IN PMIs, OFFICES AND COMPANIES

"On average, only 5% of companies' folders are properly protected"

- Venture 2021



CYBER EVOLUTION

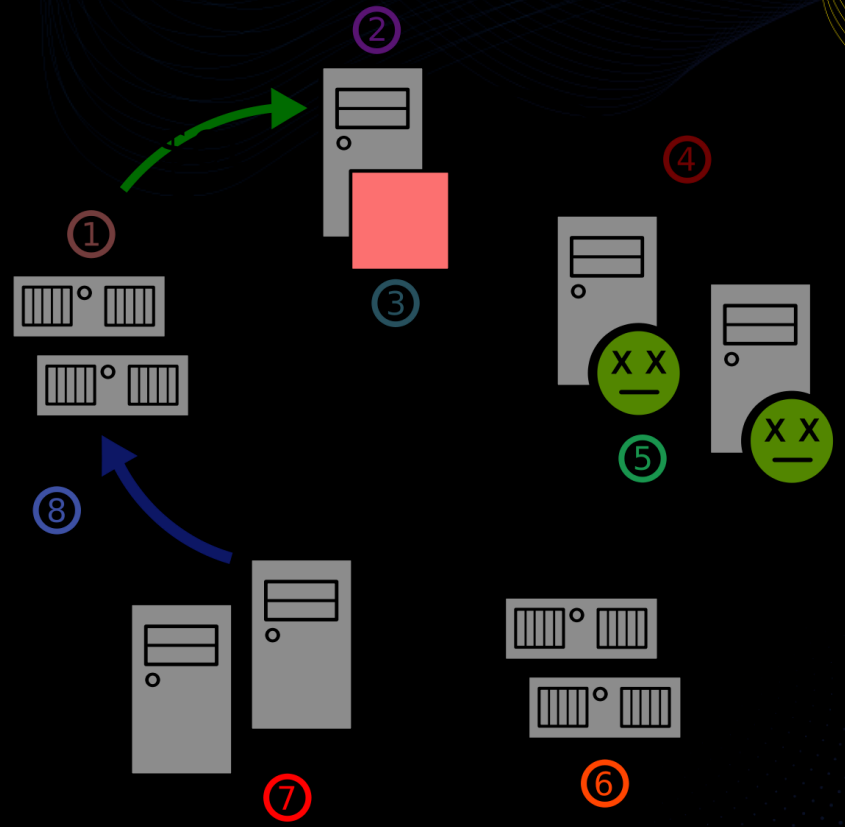
Nowadays Problems

Know-How
Unqualified staff and unsufficient formation.

Not security by Design
Inadeguate network topologies, BYOD implementations and structures

Costs
Installation/ Implementation/ Maintenance

Weak Points
Social Eng, IoT, Distance Learning, Remote Work



CYBER EVOLUTION

Aftermath

High Threat Prolification

Zombie Botnets, spywares, ad ransomwares have a wide operation range.

Buisness Loss related Costs

Turnover's reduction, inflation and loss of reputation.

Local damages and «not GDPR/16»

Loss of normal and sensitive data, mail and credit card breaches, notification costs to victims and authorities

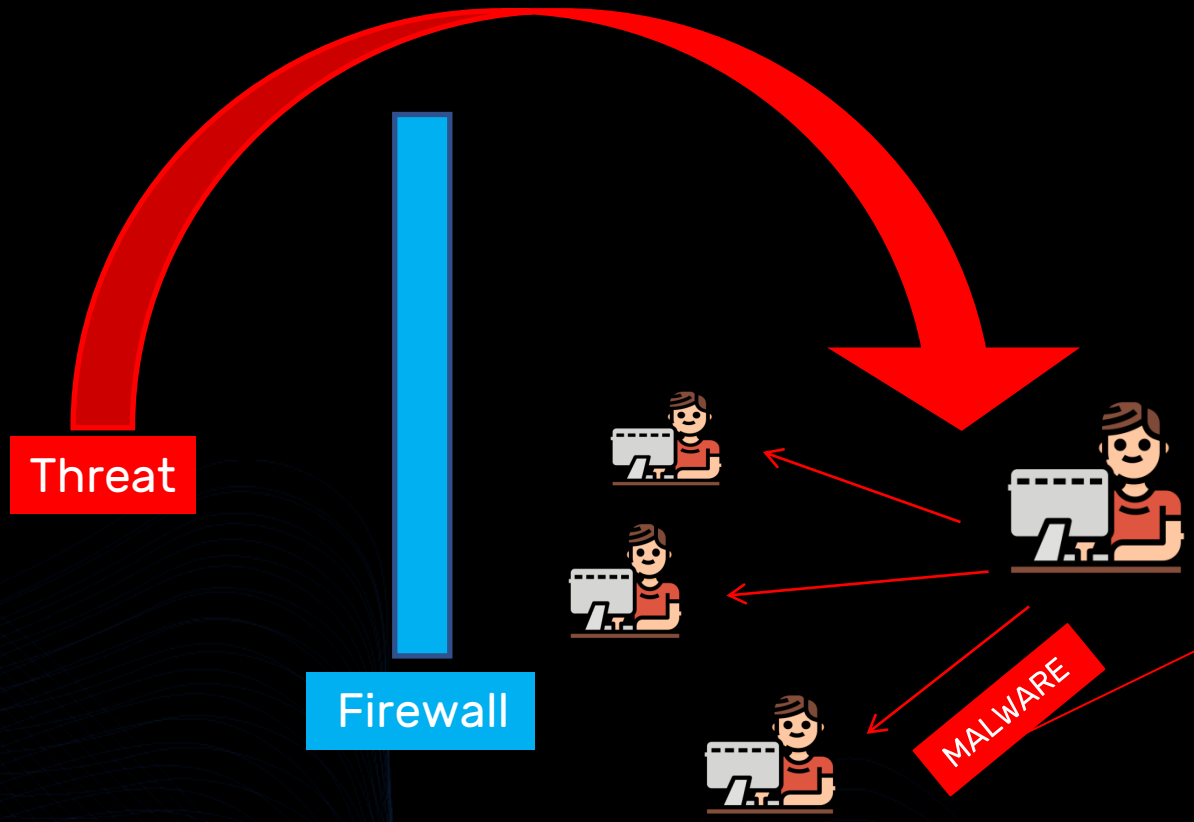
Costs detection ed escalation

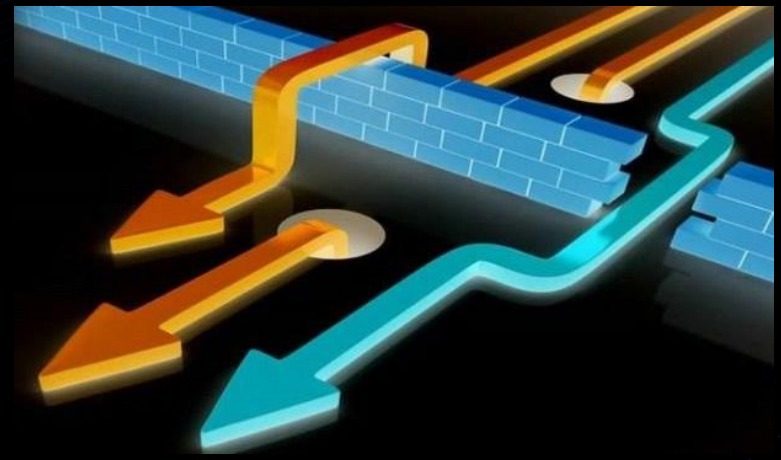
Help-Desk, investigative activites and forense, IRT organization and assessment services related costs.

CYBER EVOLUTION

Eluding Security

MOST OF DANGEROUS INTRUSIONS HAPPEN THROUGH EMAILS,
ALWAYS CHANGING METHOD AND APPEARANCE



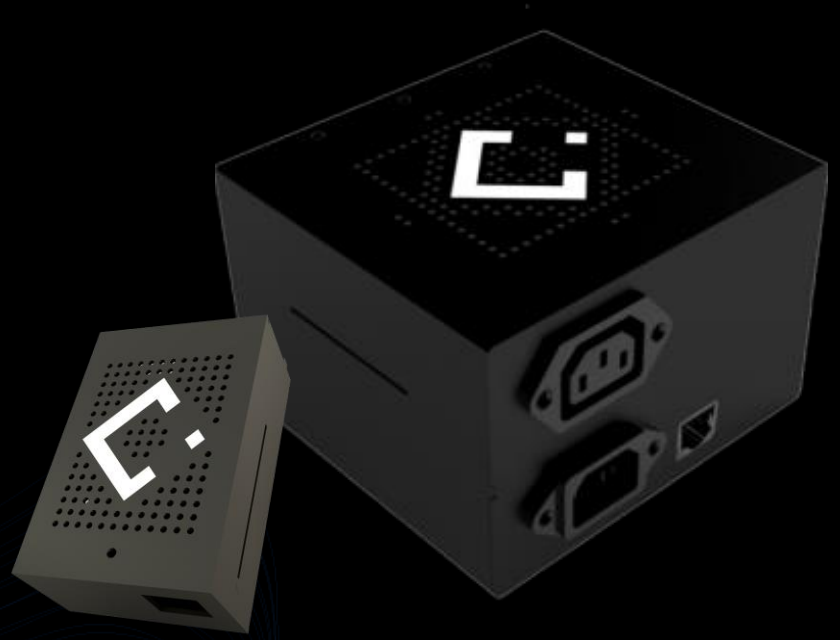


Why it's not being detected inside the network?

CYBER EVOLUTION

LECS

The **innovative** appliance of network security



Protect your company with LECS, the very first **Plug&Play** cyber security device
that safeguards from attacks and IT threats everytype of net, device, Industry or IoT in the LAN.

--
No Maintenance.
No Configuration.
Predictive.
Smart.
Autonomous.
--

Top-tier protection, for everyone.

Ministero dello sviluppo economico

Sistema Brevettato

Made &
Data in Italy

How It Guards You

The Technology →

The Alghoritms →

Application Fields →

LECS: How does it work

LECS'S ACTIVE PROCEDURE

SPECTO

- Trap/Strategic BlackBox in the net hidden among other hosts, without disturbing normal operations
  Real Time Analisis of the threats in the net
- Classification of threats based on their impact
- Parameterization based on it's AI/ML and proprietary algorithms

RAISES

- In case of high impact threats the disconnection engine starts:

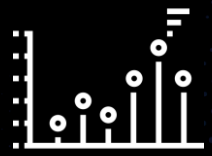
  Energetic Physical L1 OSI, according to patented procedure
  Procedural Physical L2, 3 OSI, according to patented procedure

- Instant alerting notification via mail/app/SMS

TIRESIA

- Restores network connection
- Checks the presence of other threats
- Machine Learning Method and Predictive System
- LOG-SIEM long-term storeing and monitoring statistics

=



Tiresia
Threat Forecast

CYBER EVOLUTION

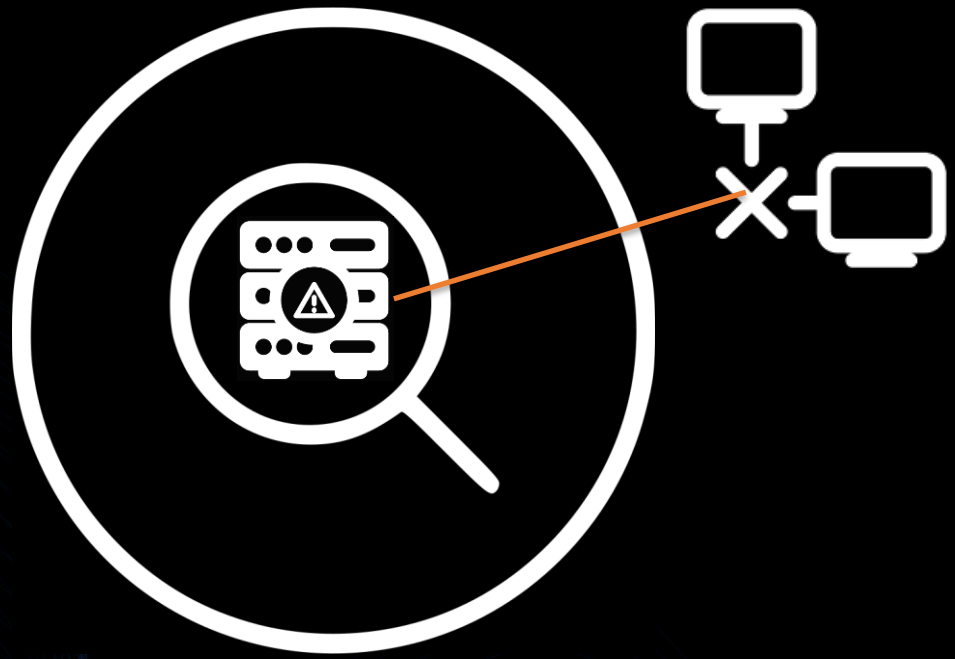
LECS: Security over the threats

Internal Network Error Debugger

Synergy

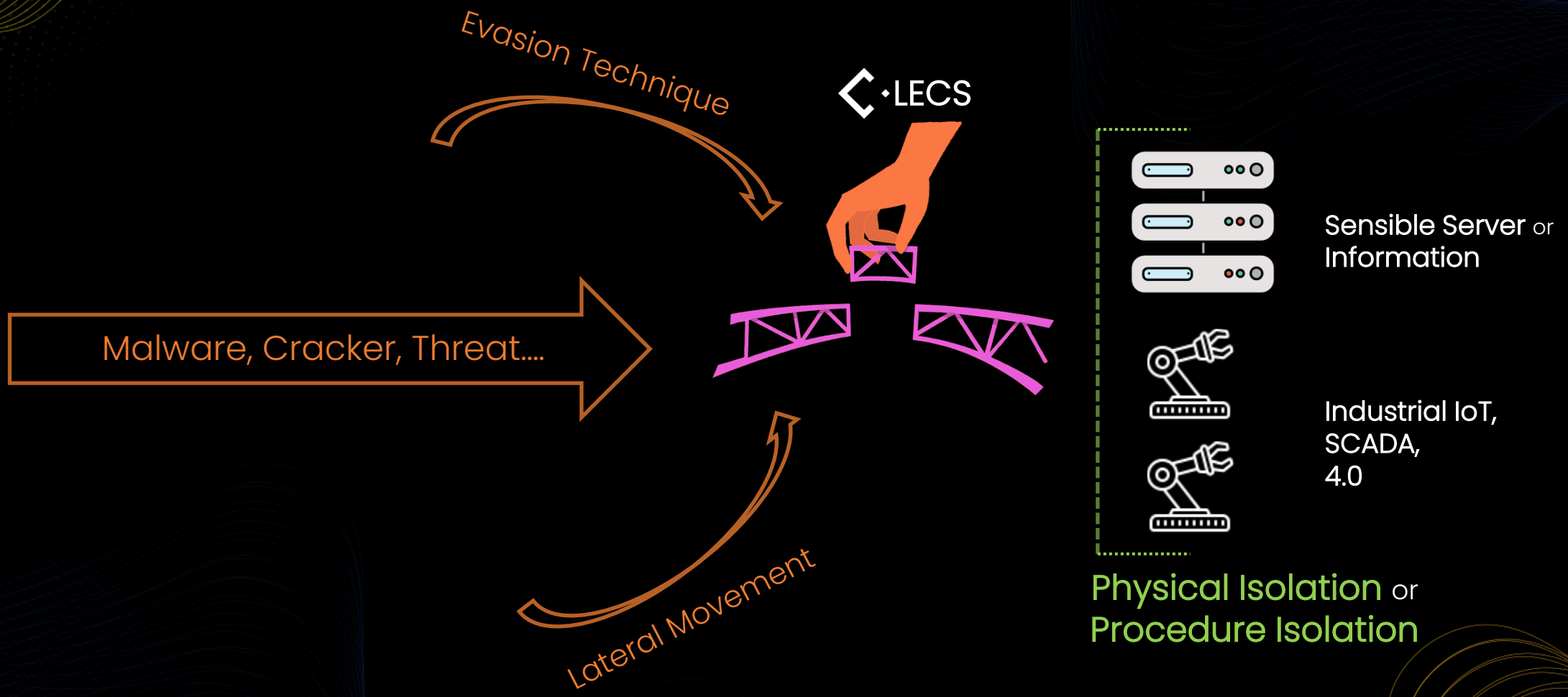
Specto

Network Error Engine



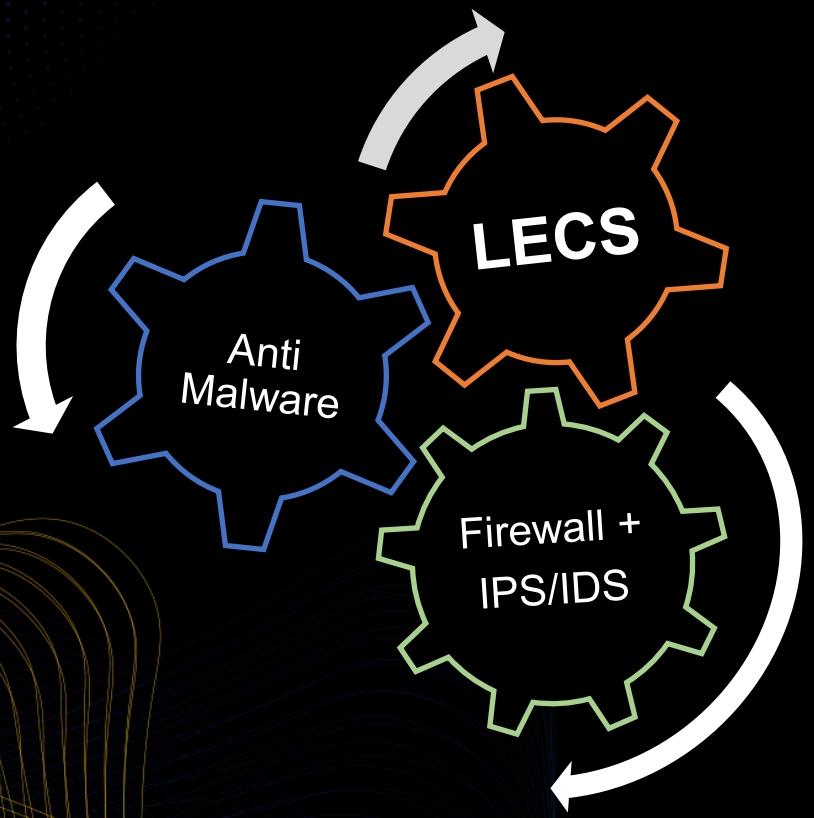
Anomalies
Flow error
Transport layer
Error
Retransmission
……

LECS: Air-Gap RAISES systems advantages



CYBER EVOLUTION

LECS: Features



INTEGRABILITY

LECS can be either installed stand-alone
or as an addition and support to pre-existent systems like firewalls, antimalwares and similars, increasing their efficiency.

VERSATILITY

It protects every type of network and nodes while supporting
a lot of protocols.
Device IoT, Industrial-IoT, Server, Desktop, Mobile OS...

PLUG & PLAY

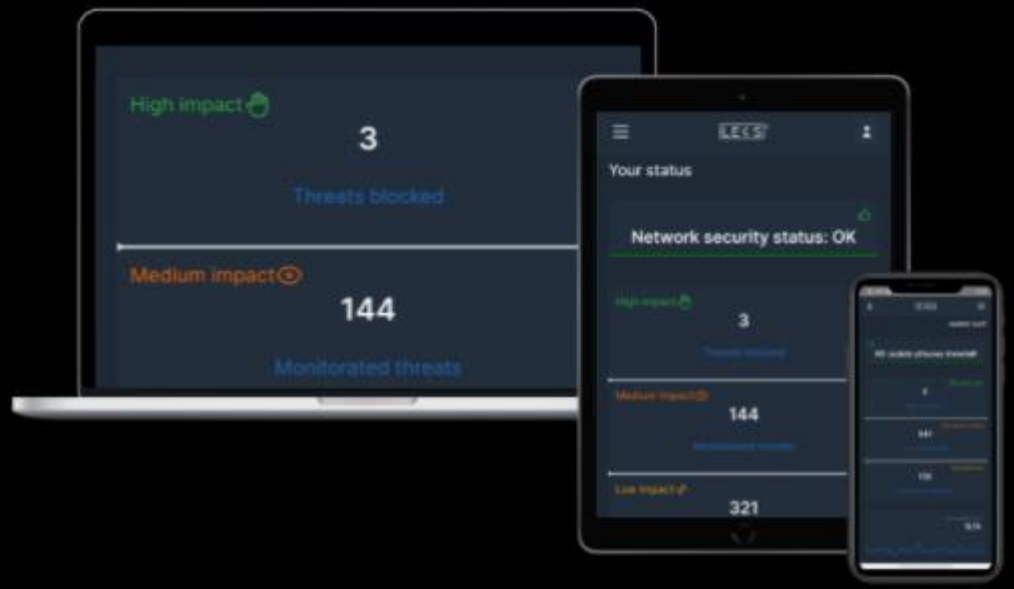
LECS's simplicity of implementation aims to give more protection against dangerous attacks at a lower price of mainentance and implementation of security appliances

CYBER EVOLUTION

LECS: Comparison

Caratteristiche	LECS	Antivirus	Firewall	IPS
Plug & Play	✓	✗	✗	✗
Contromisura elettrica o procedurale innovativa	✓	✗	✗	✗
Protegge attivamente dispositivi IoT ed Ind.IoT	✓	✗	✓	✓
Agisce da trappola nascosta	✓	✗	✗	✓
Archivio LOG fisico lunga durata - blackbox	✓	-	✗	✗
Protezione intra-network	✓	-	✓	✓
Installazione parallela, no pass-thru	✓	-	✗	✓
Nessun know-how tecnico per manutenzione	✓	✓	✗	✗

LECS: Simplfied LOG Management



The app allows to check
the LOGS acquired by LECS.

The classification is based on the
type and severity of the attack,
acquiring statistics and much more

Weekly report

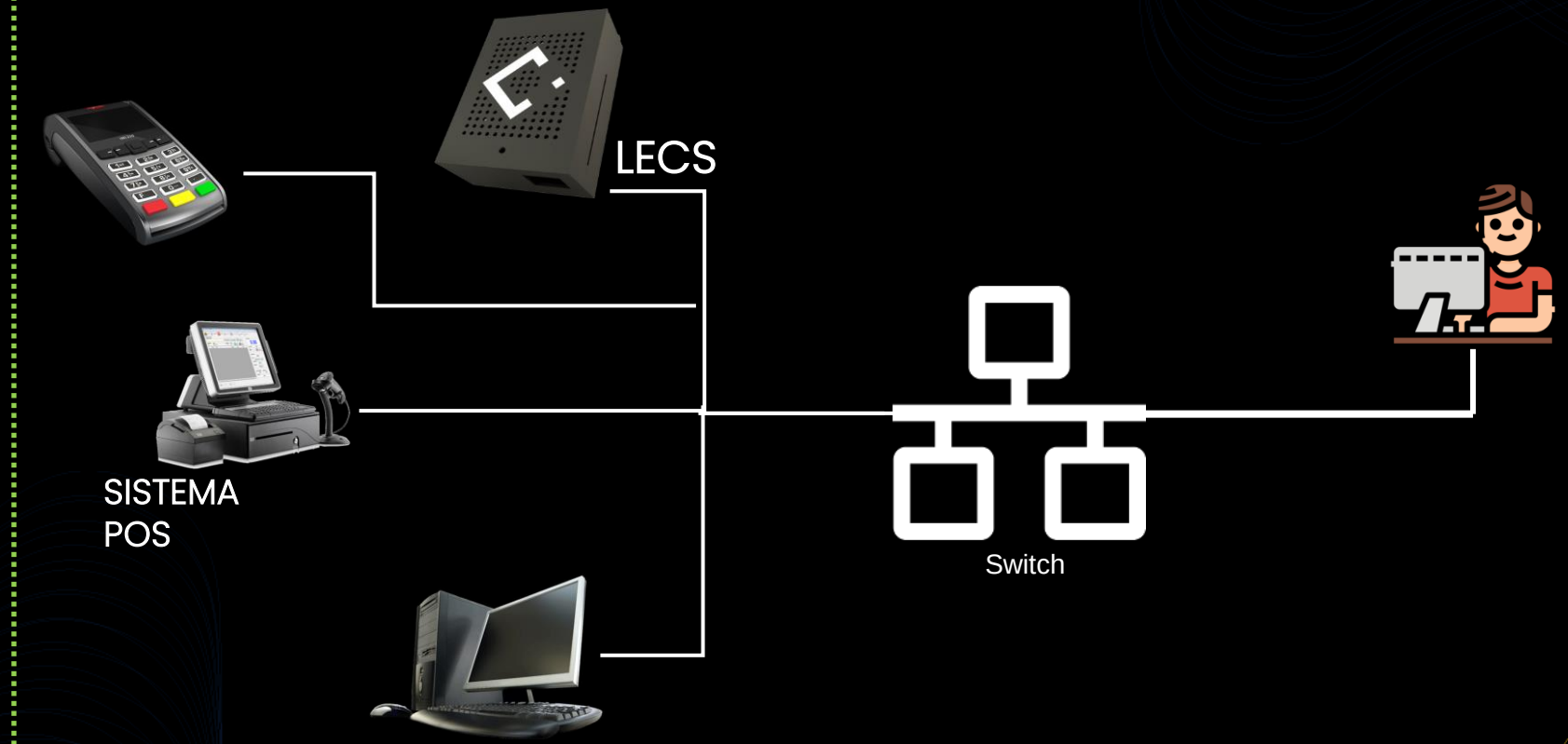
Via the web app is possible to
recieve notifications and emails
about urgent attacks.

CYBER EVOLUTION

LECS: Advanced Dashboard

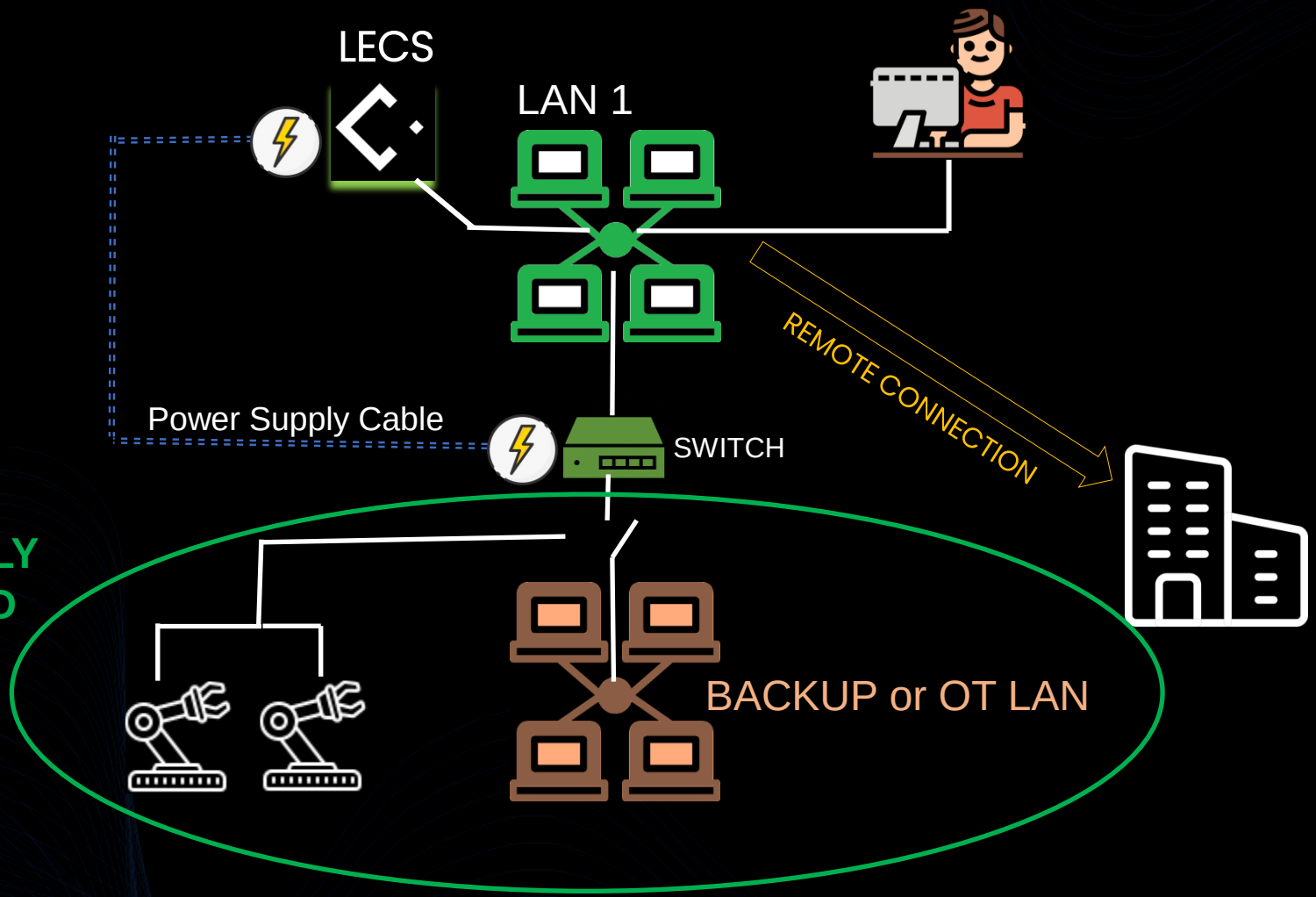
LECS: Implementation

STRATEGIC POSITIONING IN m-PMI and IT AMBIENTS



LECS: Implementation

STRATEGIC POSITIONING IN INTEGRATOR/4.0 AMBIENTS



CYBER EVOLUTION

LECS: The right side of force

VS Advanced Ransomware Kill-Chain

HOME › NEWSROOM › WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION

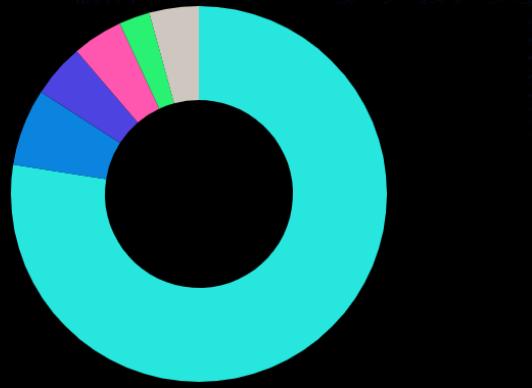
WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION

27 January 2021

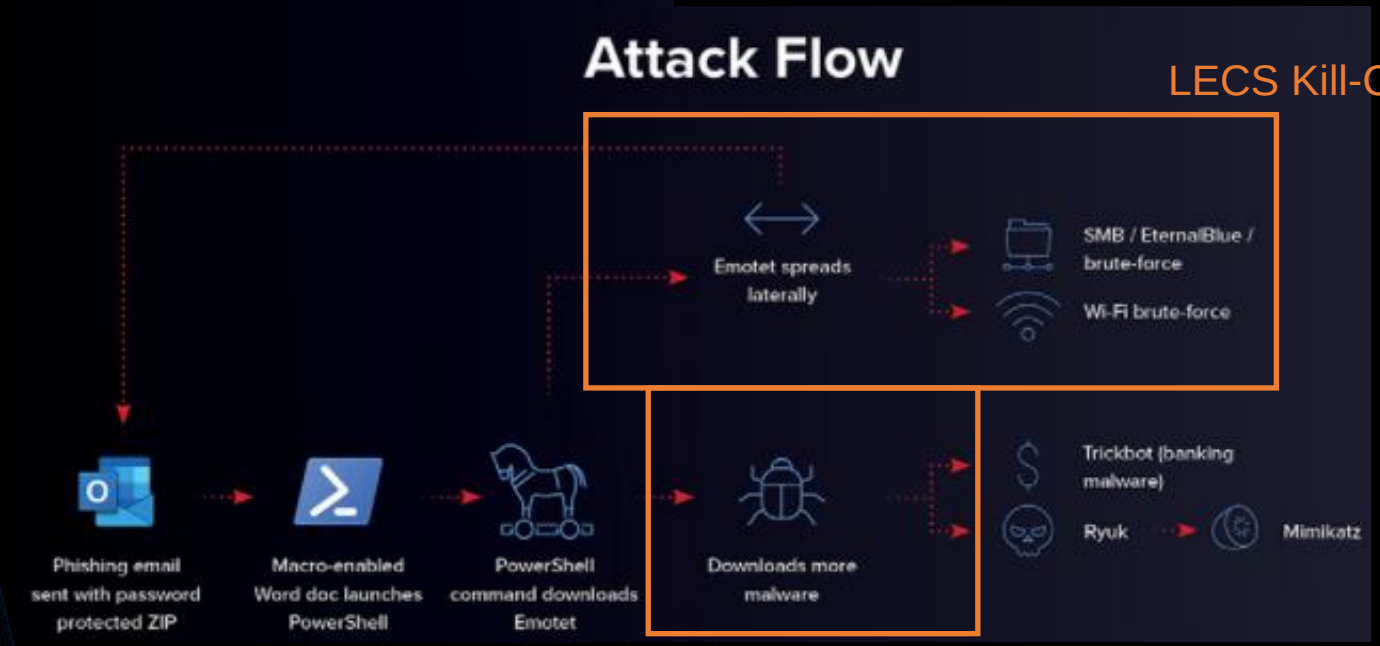
Press Release

2.000.000.000 $ in losses

Law enforcement and judicial authorities worldwide have this week disrupted one of most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an international coordinated action.



Top five malware using EternalBlue in 2019 based on detections from SPN



LECS Kill-Chain BLOCK

CYBER EVOLUTION

LECS: Version

LECS SaaS

Procedural virtualized version.
Installable on servers or single clients.

Coming soon Q3 2022

LECS

Version that has a Procedural countermeasure Software
Compact design.
anodized aluminum body.

LECS +

Version with hardware countermeasure.
Cubic design.
anodized aluminum body.
Shucko sockets IEC13-14 220v

LECS 4.0

Custom Version.
Rack 1U implementation.
anodized aluminum body.
Customizable countermeasures

LECS: Market Target/ Partner

EMBEDDED IMPLANT

Industrial Projects
Machines 4.0

SYSTEM INTEGRATOR

Rapid Installations
Parallel implementation
No incompatibilities
with other vendors
Scalability

STANDALONE SOLUTION

PMI
Privates
Substitute to other measures
Plug & Play Solution
Scalability

LECS: Main Advantages

01. Innovative and Patented efficent countermeasures
02. Plug & Play, no configuration needed, many less costs
03. Parallel or Stand Alone integration to every network or pre-existent protection system
04. Simplicity in the comunication of details to the user or IT
05. Support to the 4.0 Industrial IoT and related sistems
06. Security by design, blackbox approach
07. GDPR / ISO / NIST Framework Compliance Support

CYBER EVOLUTION

Press & Media

Sky TG 24

WMF 2020

Il Resto Del Carlino

2021 B2B SWG Report

ItaSec21 – Presentazione tecnologia LECS

Experis™ Academy
ManpowerGroup

Testimonianza c/o master Experis 05/2021

CYBER EVOLUTION

Thanks !

Follow us:

@cyberevolution

@LECS_Security

info@cyberevolution.it

WebSite:

lecs.io