ITEA 4

Project Profile

VESTA

Proactive protection from ransomware attacks

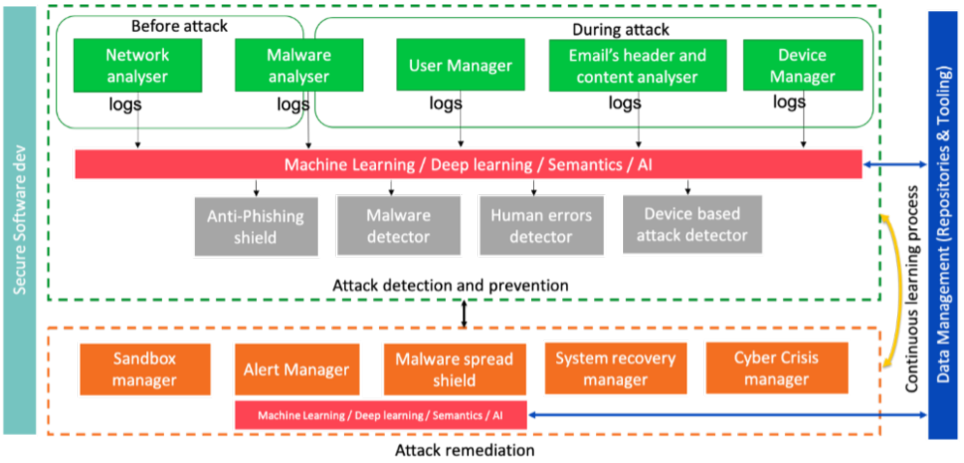
Combining techniques such as artificial intelligence (AI), machine learning (ML), data & knowledge extraction, human behaviour analysis and sandboxing, the ITEA project VESTA (proactiVe protEction againST phishing-based rAnsomware) will build a multilayer platform capable of preventing, defending and remediating ransomware attacks.

Addressing the challenge

Ransomware is a type of malware that employs encryption to hold a victim's information to ransom, which costed around EUR 40 billion in 2024 alone[1]. Millions of attacks take place annually, with roughly EUR 10.1 billion paid in ransoms in 2019 alone. Common causes include phishing, user error, and command & control attacks that exploit vulnerabilities. How can organisations and users be protected before, during and after a ransomware attack? And how to detect and recover from human errors to avoid spreading ransomware within a system?

Proposed solutions

To proactively protect systems against phishing-based ransomware, VESTA will develop a cybersecurity platform capable of preventing, defending and remediating such attacks. The core technology is AI/ML techniques that take logs from different components as input and provide (re)trained models accordingly. For the prevention phrase, VESTA will build high-quality prediction models that harness a continuous, online learning process to increase prevention and detection rates. The defensive phase deals with threats that evade the previous phase and uses techniques like email header and content analysis to swiftly detect ongoing attacks. A defensive module will protect the organisation's information system in real time, allowing the remediation phase to contain the malware to a minimal portion of the system. Efficient data recovery can then take place via data backups. Additionally, VESTA will define best practices and user awareness rules and guidelines to make recommendations on ransomware vulnerabilities. The results will be demonstrated in four use-cases: email, network ve code analysis for malware prevention, detection and remediation; brand intelligence; network traffic analysis on smart grid; voice-based phishing and voicemail-based malware analysis.



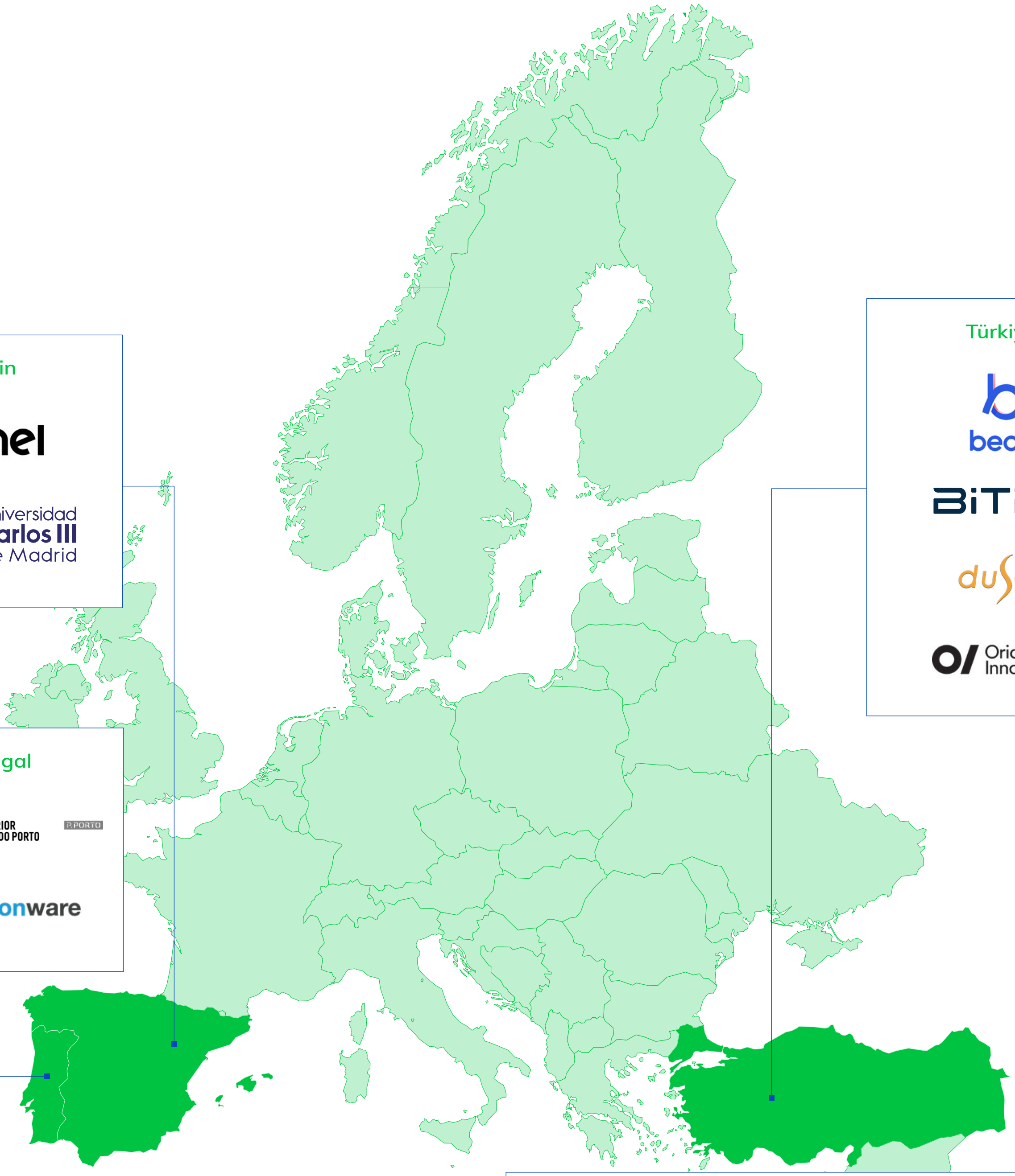
Projected results and impact

One of VESTA's main objectives is to dramatically decrease the economic impact on the partners' customers, which ranges from remediation costs and company downtime to damaged reputation and stolen intellectual property. This can be achieved by increasing detection and prevention rates: most current phishing blacklists have a <20% success rate at the zero-hour, which VESTA expects to double. The project's demonstrator also aims to reduce detection time by 50% versus a system without VESTA, for which three days is typically needed. Through these innovations, among others, the project will allow its industrial partners to provide more competitive commercial offerings in a wide range of markets, as any social or economic entity can be a ransomware target. VESTA's Europe-wide nature will also enable the consortium to target international markets, business segments and clients as the solution will be compliant with European security requirements and rules. Ultimately, by reducing the number of ransomware attacks, VESTA contributes not only to economic safety but to a society in which the personal data of citizens is more secure.

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

Project partners

VESTA
21011



Spain

panel

uc3m | Universidad Carlos III de Madrid

Portugal

ISEP INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO P.PORTO

visionware

Türkiye

beam

BITES

duSoft

Orion Innovation

Project funded by

ANI AGÊNCIA NACIONAL DE INOVAÇÃO

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

CDTI INNOVACIÓN

TÜBİTAK

Project start
January 2024

Project end
December 2026

Project leader
Murat Duran, duSoft Yazılım A.Ş.

Project email
murat.duran@dusoft.com.tr

Project website
https://itea4.org/project/vesta.html

ITEA is the Eureka RD&I Cluster on software innovation, enabling a large international community of large industry, SMEs, start-ups, academia and customer organisations, to collaborate in funded projects that turn innovative ideas into new businesses, jobs, economic growth and benefits for society. ITEA is part of the Eureka Clusters Programme (ECP).

https://itea4.org

ITEA4

eureka