ITEA4

Project Results

DEFRAUDify

Proactive tools for business cybersecurity

The ITEA project DEFRAUDify (Detect Fraudulent Activities in dark web and clear web to protect your business) has developed a toolset to improve cybersecurity for businesses. This focuses on the identification and classification of crypto asset service providers (CASPs), including using off-chain transaction information, and on the attack surface concept to make the threat level of (spear) phishing attacks more tangible.

Internet-enabled crime and fraud is here to stay: online businesses are vulnerable to phishing, ransomware and new forms of money laundering, which were accelerated during COVID-19 due to the disruption of people working from home. In 2021, ransomware revenues were as high as USD 939.9 million. Although data analytics tools to combat cybercrime exist (mostly for law enforcement), these capabilities should be available to private users, particularly advanced analytics of cryptocurrency and dark web data.

DEFRAUDify aimed to achieve this by developing a flexible toolset that can be used by businesses to detect potential illicit activities concerning them. Existing standards, combined with interoperable data exchange, were applied to two primary domains: business fraud and finance. In the former, companies can use strategic monitoring to determine their risk score based on public information and utilise tactical monitoring to identify their attack surface for phishing. In the latter, banks can apply transaction monitoring and Know Your Customer processes to check customer credibility and use virtual currency information for additional data. Rather than one integrated platform, the consortium focused on connecting their existing tools and extending their functionalities, allowing users to tailor a combination of these to their specific needs.

Technology applied

DEFRAUDify's architecture is composed of layers for data acquisition, data pre-processing/data analysis/aggregated insights and use-cases. In the financial fraud use-case, the most crucial data sources are blockchain data and information from the dark web, such as virtual currency addresses found in the context of, for instance, the advertisement of illicit items. Another important data source is a list of bank account numbers of CASPs. This enables the establishment of a link between cryptocurrency addresses, illicit activities and bank transactions. A particular innovation here is the ability to gain some insight into the Lightning Network, which does not record its transactions on the Bitcoin blockchain and therefore provides greater masking of criminal activities. All of this information results in a risk factor calculation that banks can use during their onboarding process to assess potential customers.

The other key use case is a cyber-threat dashboard for the early detection of potentially adverse activities towards companies. With strategic monitoring, businesses can search for information related to them on the dark web (such as how to deal with stolen credit cards) and analyse the source credibility to determine if a threat exists. With tactical monitoring, companies can analyse the attack surface of company staff on the clear web, allowing them to determine the potential for phishing attacks – particularly spear phishing, which targets or mimics specific individuals using their personal information. An important functionality is the use of natural language processing technologies to deduplicate information on individuals. Tactical monitoring also includes the use of honeytokens that bait cybercriminals with seemingly valuable information. By placing enticing documents in strategic locations, DEFRAUDify monitored criminal interest to enable proactive cybersecurity measures.

Making the difference

This level of cybersecurity is still in its infancy and DEFRAUDify has pushed the envelope with a number of innovations. No comparable tools address attack surface analysis and tactical monitoring for spear phishing, helping to create a foundational layer for future developments. As for cryptocurrency analytics, many platforms exist but almost none offer analytics capabilities regarding the Lightning Network. While the market leader has announced a similar functionality, they are prohibitively expensive for many law enforcement agencies; DEFRAUDify therefore hopes to diversify this market to reach players of all sizes in the long term.

In terms of commercialisation, the consortium expects to apply the results both internally and externally. Netsearch, for instance, has been able to add CASP risk exposure functionalities to COINØMON, their platform for forensics over the blockchains of various cryptocurrencies, and are in the process of preparing agreements in the financial sector. Likewise, Web-IQ is exploiting the cyber-threat strategic monitoring dashboard and has closed multiple new deals with threat intelligence companies. Exploitation is also taking place along non-commercial lines: research institute TNO works with the police and military and is looking to expand their NLP to open-source intelligence analysis, while Eindhoven University of Technology has expanded their Caronte platform for research on the dark web. This will support students in projects that deal with similar themes to DEFRAUDify.

Following this promising start, the project partners can now look to further develop the ideas that are most ahead of the curve, particularly honeytokens and the concept of privacy-enhancing technologies in data analytics. Ultimately, the benefits go far beyond the cost savings that can be achieved for both companies and wider society. Cyberattacks are impactful events for individuals too; we need to feel safe and be free not only physically but also online. This is what DEFRAUDify has aimed to safeguard and improve.

Major project outcomes

Dissemination

- 38 publications: white papers, peer reviewed journal articles, MSc theses, newspaper/magazine articles
- 42 presentations at conferences/fairs: scientific conferences (eg, IEEE symposium on security and privacy), business trade shows (eg, Cyber Security & Cloud expo), local seminars, and other platforms (like the Interpol New Technologies Forum)

Exploitation (so far)

Three integrated Key Exploitable Results, all available as Software as a Service:

- Crypto Asset Service Provider risk exposure calcuation
- Cyber Threat strategic dashboard
- Cyber Threat attack surface identification

Seven individual results, all available as software services:

- Using clearweb information to improve Know Your Customer processes
- Natural language processing tool to deduplicate text documents
- Crypto analytics service to detect tax evasion
- A dark web crawling platform that mimics human behaviour
- Lightning layer 2 crypto transactions information
- Honeytokens technology to detect cyber criminal activities
- Merged cryptocurrency analytics & dark web analytics service

DEFRAUDify

18007

Partners

Czech Republic
- netsearch s.r.o.

Greece
- Space Hellas SA

The Netherlands
- Almende B.V.
- bunq B.V.
- CFLW Cyber Strategies
- Cointel
- Eindhoven University of Technology
- Hoffmann
- Slimmer.AI
- TNO
- Web-IQ B.V

Romania
- Beia Consult International

Türkiye
- IntelProbe Defense Tech. Corp.

Project start
October 2019

Project end
September 2023

Project leader
Freek Bomhof, TNO

Project email
freek.bomhof@tno.nl

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

ITEA is the Eureka R&D&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