Deliverable 2.1

Use case definitions

DEFRAUDify - Detecting Fraudulent activities on the internet

Author: Eljo Haspels (Cointel)

Date: 24-03-2021

Status: final

Version: 1.0

Table of Contents

Contents

[Table of Contents 2](#_Toc67490232)

[Acronyms 3](#_Toc67490233)

[1. Introduction 5](#_Toc67490234)

[2. Business problem definition and scope of use cases 6](#_Toc67490235)

[2.1. Strategic monitoring: “the Hoffman use case” 6](#_Toc67490236)

[2.2. Unusual financial transaction assessment: “the Bunq use case” 7](#_Toc67490237)

[Data sources and KPIs 8](#_Toc67490238)

[2.3. Strategic monitoring: “the Hoffman use case” 8](#_Toc67490239)

[2.4. Unusual financial transaction assessment: “the Bunq use case 8](#_Toc67490240)

[Annex A: “The Hoffman use case” – CEO Fraud 9](#_Toc67490241)

[Annex B: “The Bunq use case” 13](#_Toc67490242)

Acronyms

|  |  |
| --- | --- |
| Acronym | Explanation |
| AI | Artificial Intelligence |
| AD |  Anomaly Detection |
| AOC | Area Under Curve |
| AML | Anti-Money Laundering |
| BKR | Bureau Krediet Registratie (NL registration of debts) |
| CASE | Cyber-investigation Analysis Standard Expression |
| CTFI | Cyber Threat & Fraud Intelligence |
| CVSS | Common Vulnerability Scoring System |
| DDoS | Distributed Denial of Service |
| DW | Dark Web |
| DKIM | Domain Keys Identified Mail |
| FDS | Fraud Detection System |
| FPS | Fraud Prevention System |
| GDPR | General Data Protection Regulation |
| ICO | Initial Coin Offering |
| LEA | Law Enforcement Agency |
| ML | Machine Learning |
| MSSP | Managed Security Service Providers  |
| NLP | Natural Language Processing |
| OSINT | Open Source INTelligence |
| PCI-DSS | Payment Card Industry Data Security Standard |
| SIEM | Security Information and Event Management |
| SPF | Sender Policy Framework |
| UCO | Unified Cyber Ontology |
| VC | Virtual currency |

1. Introduction

To ensure tool developers are working towards a product of value, we start this project with a strong focus on the business problem we want to solve, also known as the use case. We emphasize this in the start of the project to make sure we align before we start to build.

In the project proposal, there were two initial use cases described, which had to be addressed by the Dutch participants of the consortium. This document describes the ambitious goals of the DEFRAUDify project translated into practical use cases, containing the business problems and possible approaches to solve these based on real world applications at the business partners of the project. The practical examples of what could be achieved within the project are only indications due to the early stage of the project.

This document is input for the next phase in which tool developers and end-users will work together to create an integral toolset addressing the use cases

1. Business problem definition and scope of use cases

As indicated there are two main use cases addressed by the DEFRAUDify project which are described in detail below and in the annexes.

* 1. Strategic monitoring: “the Hoffman use case”

From the project proposal, we learned there is a growing need for: “organizations to efficiently prioritize their security monitoring actions and“ ”allow them to strategically plan their monitoring and threat prioritization decisions”. The project partner Hoffmann offers their clients a variety of services centred around prevention, detection and recovery in relation to fraud. Within the digital domain, they see an increase in several types of fraud. After several brainstorm sessions, Hoffmann indicated that a preventive service in the area of fraud would be of high business value to them. Currently, their services targeting fraud are repressive in nature and a preventive service would be a new addition.

More brainstorm sessions allowed the consortium to establish a basis for the use case, namely CEO fraud: a specific fraud domain that has not only seen a rapid rise of occurrences, but is poorly understood and lacking appropriate tooling for prevention. This makes it an ideal domain for DEFRAUDIFY to focus on.

Firstly, it was important to gain a sufficient understanding of CEO fraud, as well as an understanding of how it is conducted by cybercriminals, in order to brainstorm about possible preventive strategies. Several sessions were spent on gaining this understanding, which is still developing using the expertise of Hoffmann.

Secondly, the sessions shifted to describing and writing a use case (see appendix 1), which at first developed as a broad scenario. Through revision sessions, the use case became more focused and detailed: the whole process of cyber criminals committing fraud was dissected into 8 separate phases (from planning to execution to flight), and how potential actions of an integral toolset operated by Hoffmann could prevent CEO fraud.

Based on this CEO fraud use case, we envision the scope for the DEFRAUDIFY project to be phases 1 to 5, which could concretely result in:

* A theoretical framework on CEO fraud, describing known modus operandi of cybercriminals;
* An overview of state of the art CEO fraud tools, training and CEO-Crime-as-a-Service solutions based on crawling and scraping the DarkWeb and other sources;
* A database of potential victims based on indicators being found in scraped data from DarkWeb pages and closed discussion groups, as well as a process by a NLP based service to detect intent;
* A tool to analyse and actively detect changes in the scraped data, for example an increase in mentions of CEO fraud;
* Perform a controlled test by trying CEO fraud as a “white hat hacker”, as well as experimenting with a “honey pot company”, and see which information is easily accessible and useful for an attack;
* A paper on best practices to prevent CEO fraud
* A detection service for similar URL/domain/email-addresses creation;
* And if data allows, create a tool for detecting anomalies within companies internal information (emails, documents, etc.).

Again, these are solution directions which need further investigation to determine validity, but for now provide us a clear idea of what we ideally want the DEFRAUDify-toolset to perform.

* 1. Unusual financial transaction assessment: “the Bunq use case”

From the project proposal we learned: “Banks are legally obliged to report risky transactions, like unusual financial transactions in general and more specifically also suspects of money laundering. Recent press coverage in the Netherlands shows that banks struggle to prioritize information in this area; which has led to serious fines for banks that were not able to fulfil the legal obligation. One area not yet explored is the cross-over between virtual currencies and ‘real’ currencies. The pilot aims to create automated risk assessment of transactions from and to virtual currency exchanges”.

The project partner Bunq is a Dutch bank, offering financial services to their clients. Next to consumers being their customers, they also service corporations, among them several virtual currency exchanges and brokers. During several sessions we have formulated 3 use cases, described in appendix 2.

Based on these use cases in the domains of “Know your Customer”, “Know your transaction” and “Detect patterns” we envision the scope of this project to include:

* A service to check DarkWeb and social media activity based on specific identifiers for a potential customer of Bunq;
* A service to check the risk score of virtual currency addresses;
* A service to signal specific transactions to the FIU;
* A ground truth data set containing fraudulent transactions;
* A machine learning algorithms, tasked to detect known fraudulent activities, based on the training set.

These are preliminary ideas which need further investigation.

1. Data sources and tool KPIs

To address the described use cases, the envisioned tools need to access specific data sources.

* 1. Strategic monitoring: “the Hoffman use case”

Possible data sources are:

* DarkWeb, including forums and markets;
* Databases, such as Chamber of Commerce or Land Register;
* Network traffic on company websites, or company e-mails;
* Social media, such as Facebook and LinkedIn;
* Other type of message boards, such as 4chan boards;
* Social media chat groups.

Possible KPIs to measure the effectiveness of the tools are:

* Number of relevant DarkWeb pages;
* Number of companies mentioned by name, in combination with possible ‘trigger’ terms that are flagged (‘target’, ‘attack’, etc.).
	1. Unusual financial transaction assessment: “the Bunq use case

Possible data sources are:

* Internal transaction data at Bunq;
* Most commonly used cryptocurrency ledgers (Bitcoin etc);

Possible KPIs to measure the effectiveness of the tools are:

* Number of flagged transactions;
* Number of flagged accounts;
* Number of false positives.
1. “The Hoffman use case” – CEO Fraud

#### Context of CEO-fraud

Four main attack tactics by criminals in cybercrime:

* **Phishing** = a cybercrime that uses tactics like deceptive emails, websites and text messages to steal money or information. Large number of emails are send, with phishing links or false domains. Can be send to CEOs themselves, or just broadly to entire companies.
* **Spear Phishing** = very targeted emails against individuals and businesses. Cybercriminals use the internet (mainly open source) to collect personal data about their targets. Recipients of the email trust the email sender, because e.g. it comes from a company they often do business with, or references an event they attended.
* **Social engineering** = using carefully written emails, text messages or phone calls, the cybercriminal wins the victim’s trust and convinces them to provide the requested information or send them a wire transfer.
* **Executive Whaling** = criminals impersonate company CEOs, CFOs and other executives, hoping to trick victims into acting. Goal is to use the executive’s authority/status to convince the recipient to respond quickly, without verifying the request. Can be done with false email-addresses or false domain names.

#### Use case

Notes: In this use case/scenario, we exclude the involvement of an inside-man (e.g. dissatisfied employees, employees that are being blackmailed, etc.).

Overall, criminals have a set of phases that they walk through when committing a crime.

1. Select the target.
2. Gather information about target.
3. Surveillance of the target.
4. Planning.
5. Collecting resources to commit the crime.
6. Practice.
7. Execution.
8. Flight.

#### Phase 1: selecting the target

Actions of criminals:

* Limited open source investigation;
* Queries on Dark Web/Clear Web/chat groups/forums about possible targets;
* Internal discussion (chat groups, forums, etc.) about the selection of the target.

Actions of DEFRAUDify-toolset:

* Be up-to-date about trends in fraud, e.g. are we seeing a wave of financial institutions or government institutions being hit?
* Have knowledge on how cybercriminals specifically decide their target;
* Monitor & crawl Dark Web/Clear Web/social media/closed chat groups & forums.

#### Phase 2: gather information about target

Gathering information in this phase is almost completely anonymous, without any interaction. Criminals will gather information on what employees of a company work in what departments, in order to create an organization tree.

Through using the CoC register, they will be able to pinpoint those in the company who actually have the signing authority for large sums of money. The register also shows the limits of signing authority: for example, parts of line management will only be authorized to transfer up to 100,000,-. This will influence the criminals’ decision on what type of specific fraud to perpetrate and who they will focus on (phishing, social engineering, focus on CEO or employees).

Actions of criminals:

* Extensive open source investigation to familiarize themselves with a company:
* Social media;
* Company websites;
* Databases (semi-closed sources such as Chamber of Commerce, land register, etc.);
* Extensive open source investigation to familiarize themselves with individual employees (which will allow them to target specific employees with specific techniques, such as advertisements specifically designed for individual employees):
* Focus on social media, such as LinkedIn, Facebook.
* Creating basic profiles of both the company, CEO, CFO, or other individual employees.

Actions of DEFRAUDify-toolset:

* Monitor & crawl Dark Web/Clear Web/social media, including access requests to certain databases;
* Monitor visits to specific company websites (closed source).

#### Phase 3: surveillance of the target

Continued actions of phase 2, both for criminals and DEFRAUDify-tool, but gathering information more actively: interacting with the target. Criminals might call the general customer surface to gather information, for example on creditors or the payment administration, or even to be connected to them. Or fraudsters will send emails to gather more information.

Actions of criminals:

* Extensive open source investigation;
* Contact moments to gather more information: e.g. mail company employees of financial administration, call customer service, etc.
* Creating more extensive profiles of both the company, CEO, CFO, or other individual employees. These profiles also include personal information, to allow for impersonating either employees or even the CEO (personal interests etc.).

Actions of DEFRAUDify-toolset:

* Flag open source investigation into target company;
* Work with target company to flag certain suspicious contact moments/activities.

#### Phase 4: planning

The criminals have to decide what attack method to start with. Important to note: cybercriminals are notorious for attempting a wide variety of attack methods to perpetrate the same company. They won’t stop after a single attempt using a specific technique, but instead, will continue until they find a weak spot.

Actions of criminals:

* Internal discussion (chat groups, forums, etc.) about the selection of attack method;

Actions of DEFRAUDify-toolset:

* Be up-to-date about trends in attack methods, e.g. are we seeing a wave of phishing mails? Or a large, sudden spike in the amount of reported spear phishing attacks?
* Monitor & crawl Dark Web/Clear Web/social media/closed chat groups & forums.

#### Phase 5: preparation, collecting resources to commit the crime

Actions of criminals:

* Queries on Dark Web/Clear Web/chat groups/forums about attack methods;
* Creation of false or nearly identical domain names;
* Creation of false or nearly identical email-addresses;
* Or buying the above, using cryptocurrency transactions;

Actions of DEFRAUDify-toolset:

* Be up-to-date about trends in attack methods, e.g. are we seeing a wave of phishing mails? Or a large, sudden spike in the amount of reported spear phishing attacks?
* Monitor & crawl Dark Web/Clear Web/social media/closed chat groups & forums;
* Flag the creation of false/nearly identical domain names;
* Flag the creation of false/nearly identical email addresses.

#### Phase 6: practice

Continued actions of phase 5, both for criminals and DEFRAUDify-toolset.

#### Phase 7: execution

Depending on the specific attack technique, the criminals will start the execution of their operation. Possible scenarios can include:

* Phishing emails are send to the CEOs themselves or to the entire company, including deceptive websites or text messages. Can be websites designed to look like real and well-known domains, or ‘Nigerian prince’ messages.
* Spear Phishing: specific employees were targeted by the criminals. For example, employees receive an advertisement of the gym that they are a member of. Or an advertisement about house renovation deals, for an employee who was in the process of renovating a house.
* Social engineering: winning trust of specific employees.
* Executive Whaling: from a similar email address to that of the CEO, a mail was sent to the financial administration, in the style of the CEO and knowledge of CEO him/herself, or company procedures.

Actions of criminals:

* Sending phishing / spear phishing emails;
* Internal communication on Dark Web / chat groups;
* Possibly setting up and using deepfaking/spoofing equipment;
* Transfer possible received funds away through cryptocurrency transactions.

Actions of DEFRAUDify-toolset:

* Monitor & crawl Dark Web and closed chat groups & forums;
* Detect the use of deepfaking or spoofing equipment;
* Flag the creation of false/nearly identical domain names;
* Flag the creation of false/nearly identical email addresses.

#### Phase 8: flight

Possible extraction from company servers by the criminals, finishing up cryptocurrency transactions, deleting chat groups / forums etc.

1. “The Bunq use case”

#### Context of detection of fraud within financial services

Banks have an essential role in our society and have a lot of rules and regulations which they need to comply to, to prevent fraud. Although a lot is already done in this domain, the increase of use of cryptocurrencies by their customers has brought a new dimension of fraud detection.

#### Use case 1: Know your customer

A consumer opens a new bank account at Bunq, which can be done in just a few clicks. Several external services are used to validate the authenticity of the ID, check for any terror related links, check for registration at the BKR, etc.

One new service could check if the name, email, nickname, etc. of the new customer is present somewhere on the darkweb or used in specific chat rooms with illicit intent. If a match is found, the data on the darkweb is assessed with NLP to detect the context and this leads to a score which is taken into considerations while assessing the total risk of providing banking services to this customer.

If the risk is deemed high, an employee of Bunq can access with 1 click the data that led to the conclusion to validate the results.

Actions of DEFRAUDify-toolset:

* Provide API to do DarkWeb check;
* Provide NPL model to classify matches;
* Provide interface to employees for manual validation.

#### Use case 2: Know your Virtual Asset Transaction

The increasing amount of transactions from and to virtual currency exchanges, put extra pressure on banks to ensure fraudulent activities are detected. Although exchanges have a compliancy obligation themselves, banks want to improve their capabilities on this front as well.

A consumer with an account at Bunq has received a transaction from a known virtual currency exchange and this transaction has a value above a certain threshold. Bunq intercepts this transaction and asks the customer to provide additional information before it can process the transaction. This additional information is requested in the app, by asking to provide the virtual currency address the transaction originated from. The customer provides this information and Bunq directly checks via an external service if there are any known risks associated with this address and the cluster it belongs to. If the transactions is associated with a risk an employee of Bunq receives a call to action an can manually check the source of the risk and assesses if the transaction should remain on hold to inform the FIU or if it can be released to the customer.

Actions of DEFRAUDify-toolset:

* Provide API to check risk score for VC address;
* Provide API to signal suspicious transaction to FIU.

#### Use case 3: Detect suspicious behaviour

Although all banks already use some form of automation to detect suspicious transactions, this domain can still be expanded a lot. From the naive approach of flagging all transactions of a large size in combination with black/white listing of accounts, more advanced techniques could be based on machine learning with training sets containing known (and/or often used) fraudulent patterns.

A consumer with a bank account at Bunq has made a large amount of transactions with a virtual currency Exchange. All individual transactions have passed the tests of fraud within Bunq but a nightly pattern detection process as detected the large amount of small transactions as a known money laundering technique and flags the account. An employee at Bunq is tasked with following up this detection by performing a more in-depth investigation into the customer.

Actions of DEFRAUDify-tool:

* Create ground truth dataset;
* Provide service to detect annomalies.