# Securing national e-ID infrastructures: Tor networks as a source of threats

Paolo Spagnoletti [1][0000-0003-1950-368X], Gianluigi Me [2][0000-0002-8805-2547], Federica Ceci [3][0000-0002-6998-8534] and Andrea Prencipe [4][0000-0002-5691-2290]

[1] LUISS University, Rome, Italy
[2] LUISS University, Rome, Italy
[2] G. d'Annunzio University, Pescara, Italy
[4] LUISS University, Rome, Italy

**Abstract.** Securing national electronic identification (e-ID) systems requires an in depth understanding of the associated threats. The trade of identity related artefacts in the darknet facilitates illegal activities such as identity theft in both physical and virtual worlds. This paper reports the findings of an exploratory analysis of identity trading in the darknet. We capture the key features of three major markets of fake IDs in Tor networks, and apply attack-defense trees to show how the security of an e-ID infrastructure is affected by this phenomenon.

**Keywords:** Identity theft, Tor, attack tree, identity management, black market.

## 1 Introduction

Electronic identification (e-ID) infrastructures are considered a key enabler for the development of e-services in both public and private sector. In the last decade, many European countries have started nation-wide initiatives to develop their own e-ID infrastructures [1]. Such infrastructures differ in terms of architectures, institutional actors involved, and on the range of services that can be accessed by citizens using digital identities. In some cases, e-ID can be seen as platforms enabling authenticated citizens to access online services provided both by public administrations and private companies. Such platforms are based on federated authentication and authorization architectures in which few certified companies act as Identity Providers (IdP) under the supervision of a governmental institution [2]. Identity Providers must guarantee the identification of citizens and securely manage their personal data while enabling access to Service Providers (SP) in the ecosystem, by the means of standardized protocols.

Alike e-payment systems, e-ID infrastructures can be considered as multi-sided platforms [3]. Depending on the policies defined by governmental sponsors, different strategies can be implemented at the level of provider, technology and users. For instance, in Italy a competitive strategy at the level of Identity Providers has been recently established by AGID, the Public Agency in charge of promoting digitalization.

At the moment, the governmental sponsors have accredited five Identity Providers and they are requested to manage citizens' identities by opening the platform through APIs to any public and private e-service. Citizens can join the SPID (Digital Identity Public Service) at no charge and benefit of a Single-Sign-On service when accessing to e-services connected to the national e-ID infrastructure. The economic sustainability of the overall system relies on transaction fees payed by private companies to the Identity Provider that performs the authentication.

Despite the huge market potential of e-ID platforms, which coincides with the whole state population, governments are struggling in developing e-ID infrastructures and attracting a critical mass of users and service providers [4]. Possible challenges in the development of such infrastructures are related to privacy concerns, lack of inter-governmental coordination, lack of private-public sector cooperation, and tensions such as the trade-off between usability and security. Among those issues, security plays a crucial role by enabling the development of trusted e-service ecosystems. Security is a multidimensional property of systems, data and information [5]. When referred to an IT infrastructure in a business context, information security is often intended as the organizational goal of mitigating operational risks by protecting information from threats to confidentiality, integrity, availability and accountability [6]. However, today's pervasiveness of digital technologies in both work practices and citizens' private life, extends the scope of risk to safety and other human rights. Undesired e-payment transactions, data breaches of healthcare and financial information, sabotage of critical infrastructures (e.g. transportation, electricity, oil and gas, etc.) and unauthorized access to e-voting systems are only few examples of serious violations of rights such as ownership, privacy, safety and freedom [7]. Since e-ID infrastructures serve as a gateway to a vast array of services, their vulnerabilities can have a tremendous impact on organizations and society. In fact, systems integration and interoperability of services enable the propagation of security incidents well beyond the boundaries of a single service with potential effects on the performance of an entire ecosystem [8].

While previous studies have addressed the problem of e-ID security from a technical perspective, in this paper we focus on the risk that malicious users get unauthorized access to federated services by acting on behalf of another user. In order to access e-services, users are requested to demonstrate their identity in the enrolment phase and then to perform an authentication process every time they need to enter the system. The ways in which these activities are performed is defined by IdPs and SPs and regulated by contracts. Every time a successful authentication is performed, users can act by the means of a digital identity, a set of attributes that are exchanged with the SP. Therefore, authorization and authentication processes transfer the user agency to digital identity (e.g. password, scanned documents, e-card, etc.) whose theft and illegal exchange threatens the accountability and hence the security of the overall system. The risks of identity theft are today amplified by the availability of online markets in the Deep Web that allow users to exchange goods anonymously. Within such markets, digital identities can be exchanged like many other illegal goods thus potentially reaching every Internet user. The goal of this study is to explore the emerging risks of

identity theft in the cyberspace and to discuss implications on the design and governance of e-ID infrastructures.

Although some empirical studies have emphasized the business potential of the Deep Web as an intelligence tool [9], it is commonly accepted that the presence of a cyberinfrastructure ensuring anonymity generates new threats for both businesses and citizens. The rise of black markets in the darknet is in fact transforming the ways in which criminals interact in trading illegal products and services [10–12]. These markets are also used to sell identity related goods either in the form of digital information or as physical artefacts such as for instance ID cards and driving licences. We argue that the trade of identity related artefacts in the darknet represents a new source of risk for trusted e-service environments. When federated e-ID infrastructures are in place, fake identities provide criminals with unprecedented capabilities of harvesting private data and acting on behalf of others. Our goal is to shed light on this phenomenon by showing how the illegal trade of identity related product and services on the darknet pave the way to new forms of attacks to e-ID infrastructures.

In this paper, we address this issue by exploring the market of identity documents in the darknet and identifying attack scenarios emerging in the new cybercrime ecosystem. We conduct a case study on the black market of Italian citizens' identities in Tor networks and discuss the implications for the development of secure e-ID infrastructures.

The paper is structured as follows. We first illustrate some key features of black markets in the dark net based on findings from previous studies. Then, we formulate our research question by focusing on the market of illegal identities in the darknet and on the potential risks for e-ID infrastructures. In the third section, we describe the research methodology and the data collection process. In the fourth section, the results of our empirical analysis are presented and the implications of emerging attack scenarios on the development of e-ID infrastructures is discussed.

## 2 Related works

### 2.1 Black markets in the darknet

A darknet is an overlay network that can only be accessed with specific software, configurations, or authorization, often using non-standard communications protocols and ports. Contents of the darknet are not indexed by common search engines such as Google. Black markets existing within the dark net present unique features that make them extremely interesting. For our purposes, we find three particularly interesting features: anonymity of users, anonymity of payments, and resilience.

The first aspect relates to the choice of communities who use and manage black markets to keep their identities secret [13]. The main motivation for anonymity is the illegal nature of the activities carried out by vendors and buyers [14, 15]. However, in some cases, the use of anonymity is chosen to avoid stigma or limit liability, as in the case of purchasing of drugs or political manuals [16, 17]. The need for anonymity has important impact on the organizational choices of markets and communities that man-

age them: research has shown that criminals often design their organizations not to maximize efficiency but to be able to better hide their activities [18] and to limit the dissemination of potentially incriminating information [19]. From a technical viewpoint, the anonymity is guaranteed by protocols that establish end-to-end circuits in which data are tunnelled using public-key cryptography. In these networks, each node only knows its predecessor and successor. New generation anonymity systems, such as Onion Routing networks handle a variety of bidirectional TCP-based applications like web browsing, secure shell, and instant messages. The Tor package is a set of free software tools implementing the Onion Routing network design. Tor users can therefore browse the web, publish web sites and other services without revealing their identity and the location of the site. Anonymity is guaranteed also while accessing and performing transactions on e-marketplaces such as black markets. In these markets identities of vendors and customers are anonymous, no email or other identification are required for the registration to the website, except for their nicknames. To create a system of trust in an area susceptible to scams and overcome the risks of anonymity, buyers can leave feedback on sellers. Moreover, a marketplace can show the number of transactions that buyers and sellers have made under a given nickname.

With regard to the second aspect, the payments are performed by exchanging crypto-currencies like Bitcoin (BTC) by all major black markets. The BTC is a peer-to-peer currency based on the blockchain technology and indexed to the US dollar to avoid excessive inflation or deflation [20, 21]. Because of its decentralized control, it is often considered a threat or an alternative to the conventional central banking system [22]. Although the BTC is characterized by high volatility, it is used on a large scale as an alternative payment system (the market value of bitcoins exceeds 100 billion dollars). Supporters argue that it is the first truly global currency, it does not discriminate against its members on grounds of nationality or position, it is always running, without holidays, it is easy to achieve with very low rates of usage. On the other hand, critics argue that BTC is widely used to buy illegal items and to launder large sums of money [21]. BTC per se do no assure anonymity of transaction; anonymity and untraceability of payments can be obtained hiding IP addresses while making a transaction, or using “mixing” or “tumbling” services. “Mixing” services work by mixing transactions with a large number of other transactions from different sources. By doing this, it becomes difficult or impossible to link specific payments into the mixing service with specific payments coming out of the mixing service. To satisfy the increasing need for anonymity, recently, alternative forms of payments are accepted in black markets. An example is Monero (XMR) that, possessing significant algorithmic differences, assures higher level of privacy and anonymity then Bitcoin.

Finally, regarding resilience in networks, previous studies have emphasized that resilience is a dynamic process, associated to systems that exist and carry out their main tasks under the pressure of external shocks [23]. Sutcliffe and Vogus [24] analysed the existence of two critical conditions implicit in the concept of resilience: (i) "exposure to threats, stress or adversity" and (ii) "the achievement of positive adaptation despite the presence of stress or adversity” (p. 108). Bakker et al. [14] defined the resilience of a dark net as the ability of the network to remain operative in the middle of bumps or attacks ("robustness capacity") or to recover from unpleasant events,

transforming over time ("rebound capacity"). Empirical evidence shows that the communities underlying black markets can quickly re-organize after major attacks. For example, SilkRoad, an e-commerce site founded in 2011 and whose products were classified as contraband by the majority of the world's jurisdictions, was closed October 3rd, 2013 by the FBI. On 6th November of the same year, SilkRoad 2.0 was reopening by the same managing team under the same alias Dread Pirate Roberts, although the FBI has arrested the person that was hidden behind that name. On November 6th, 2014 SilkRoad 2.0 was again closed by the FBI.

### 2.2 The market of identities in cyberinfrastructures

Digital identity is the set of information and resources provided by a computer system to a particular user on the basis of a process of identification. Digital identity is assuming an increasingly important role, given the already widespread use (that will likely increase in the future) of digital identities by public administrations (e.g. SPID), private companies (e.g. Google and Facebook) and individual users (e.g. web reputation). In parallel, there is a new-born black market for digital identities that generates new security threats [25–27].

Previous studies on identity in the information society have emphasized the multiplicity of tensions, themes, application domains and disciplinary approaches related to this subject [28]. However, few studies so far have addressed the impact of illegal trade of identity related goods in the deep market on the security profiles of e-service infrastructures.

## 3 The case of Italian identity trading in the Tor network

### 3.1 Data retrieving methodology

A particular boost to the spread of empirical studies in this area is due to the possibility to access historical data about transactions, vendor profiles and feedbacks. Such amount of data allows researchers to test hypotheses and to implement simulation methods. Despite the potential advantages of applying longitudinal approaches to study evolutionary market dynamics, in this paper we focus on the structural characteristics of anonymous marketplaces in a single point in time.

In order to build the dataset, we crawled six marketplaces in December 2016, visiting each market in order to create a snapshot dataset ready for the analysis. The marketplaces we analyzed were AlphaBay, Dream Market, Hansa, Leo, Outlaw and Bloomfield. Each market adopts a different set of categories for products and services. Our attention was focused on those categories that are potentially related to identity theft activities such as “Counterfeit items/Fake IDs” and “Fraud/Personal information & scans” on AlphaBay, “Digital goods/Fraud” on Dream market and “Fraud Related/Documents & Data” on Hansa. Therefore, we collected items' pages concerning identity documents, and their related images.

For each marketplace, we designed and implemented a custom spider using the Scrapy[1] framework. Spiders are configured to use Tor to have the capability of reaching anonymous marketplaces. Figure 1 shows the logical workflow of our system for the collection, elaboration and analysis of anonymous marketplaces data.

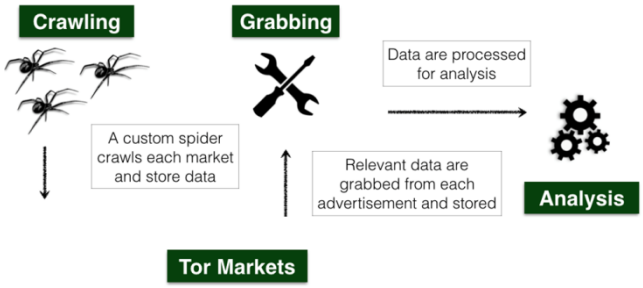


**Figure 1:**Tor marketplaces data retrieval system

Spiders request pages with different waiting times between each request. We also deny the possibility of sending concurrent request to marketplaces. Clearly, these precautions increase the crawling time for each market. Such settings are natively supported by Scrapy, and we resort on them for spiders' configuration.

We gathered data from a dataset of 36 GB in size, where the crawl of each market ranged from 1,682 to 18,831 pages/images, and crawling time took from several hours up to few days. Specifically, we crawl only listings' pages and items' pages. We scraped listing pages to collect items' pages URL, but we store only item's pages, together with items' images. Finally, to prevent undesired actions execution, such as adding items to cart or sending messages, each spider is designed to request only URL of interest.

From each item's page we extracted the information needed to fulfil the table fields reported in Table 1. To grab such information, we took advantage of the HTML structure of each page. A generic HTML page is enclosed in a main HTML tag and divided in two sections identified by the tags head and body. Tags inside the body contain information we look for. The data we want to extract are enclosed in different tags at different level of the HTML structure. Each marketplace has a different structure for its pages, thus we implemented a customized parser for each marketplace. Therefore, every single parser identifies the nodes within the Document Object Model (DOM), through the Xpath selector.

**Table 1:Fields**

| | | |
|---|---|---|
| Name | Vendor_name | Escrow |
| Description | Marketplace | Product_Type |
| Ships_to | Price | Ships_from |

[1] Scrapy: A Fast and Powerful Scraping and Web Crawling Framework http://scrapy.org

The target of data grabbing is to reduce an offer to a tuple containing the relevant field for the purposes of the analysis, as shown in the Table 1.

The marketplace mechanism to place offers makes the overall raw dataset quality very low. In fact, every vendor can place his offer regardless of almost any control, leading to have empty or duplicated offers (in the raw dataset), mistakes in key-text fields, non-uniform metrics/currency. Moreover, offers can be misplaced in the different categories, leading to mismatching overall amounts of offers. Hence, for the abovementioned reasons, the data preparation phase assumes a crucial role in order to achieve reliable results.

Data scrubbing, also called data cleansing, is the process of correcting or removing data in a dataset that is incorrect, inaccurate, incomplete, improperly formatted, or duplicated. This step is important since the validity the data analysis process depends not only on the algorithms, but also on the quality of the data collected. In order to avoid biases in the dataset, it should be characterized by correctness, completeness, accuracy, consistency and uniformity. Residual dirty data can be detected by applying statistical data validation methods and also by parsing the texts or deleting duplicate values. In fact, missing data can lead to bad analysis results.

It is worth to mention that our dataset has some limitations. First, in our case all offers have been considered real and possible scams have been ignored. Second, the "ships from" value is considered reliable since the shipping of identity documents are basically invisible to customs as compared to the exchange of other illegal goods (e.g. drugs, weapons, etc.). Third, the classification of offers into categories is made by vendors which may apply subjective views in this process. It is possible to find offers related to the same kind of product classified under different categories. For instance, the crawler will not detect the offer of a fake ID card if it has been classified under the drug category. Finally, feedback has not been taken into account since it can be biased by vendor tactics such as exit scams. However, feedback could be used in future studies to estimate the revenues of a vendor.

### 3.2 Data analysis

The resulting dataset has been analysed per category and keyword. In particular, the only categories crawled and analysed were those in Table 2. The resulting dataset was the following collection of offers per marketplace: AlphaBay (9120 offers), Dream Market (18506 offers), Hansa (13068 offers), Leo (382 offers), Outlaw (1714 offers) and Bloomfield (111 offers).

The overall resulting offers fields in Table 1 were matched against a set of keyword based on the location and good description (e.g. passport, identity, spid, driving, ita, etc.).

**Table 2: Categories with placed identity documents offers**

| | | |
|---|---|---|
| Carded_Items | CVV_Cards | Fraud |
| Counterfeit_Items | Data | Fraud_Related |
| Counterfeits | Digital_Goods | Fraud_Software |
| IDs_Passports | Other_Dig_Products | Personal_Info |

Hence, we selected Alphabay, Dream and Hansa Market as the three most interesting marketplaces in terms of offers size. For each of these marketplaces we investigated every single offer in order to find data possibly enabling identity theft for the Italian Digital Identity Public Service (SPID). Hence, key offers were those containing Italian documents and their related prices.

The collected data resulted in 58 offers matching these requirements, posing the pillars for the threat detection and evaluation via the attack tree model, further explained in next section.

### 3.3 Threat detection via attack trees

As Bruce Schneier wrote in his introduction to the subject, "Attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks. Basically, it is a model to represent attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes" [29]. Therefore, attack trees provide structure to the risk assessment process, facilitate interactions among stakeholders, and allow to catalogue the identified threats. Furthermore, some tools and techniques based on attack tree models enable advanced quantitative risk analysis with security metrics, e.g. expected time of attack or worst-case impact. Attack trees have been effectively adopted to understand the protection of critical infrastructures such as buildings, pipelines, electrical transmission lines and ATM [30].

Attack trees work well as a building block for threat enumeration: in particular, whereas there are several ways to use attack trees to enumerate threats, we created a tree to detect threats from the scratch. Creating new trees for general use is challenging, even for security experts.

Even assuming that all feasible attacks (identified through pruning) have some non-zero probability, that is still only half of the risk equation. Hostile risk is generally accepted to be the combination of two factors:

$$\text{Attack Risk} = \text{Attack Probability} \times \text{Victim Impact}$$

In order to model threats to a single e-ID provider, we used SecurITree to model how the attacker can obtain a certified digital identity from a generic e-ID infrastructure. The resulting model needs to include the impact each attack scenario will have on the defender.

SecurITree[2] is a graphical Attack Tree modeling tool introduced by Amenaza Technologies. It is a Java application and runs on all major computing platforms. SecurITree allows to draw complex conclusions using capability-based modeling. SecurITree allows an analyst to describe possible attacks against a system in the form of a graphical, mathematical model. The capabilities of motivated attackers are compared with the resources required to perform specific attacks in the model through a

[2] SecureITree, http://www.amenaza.com/documents.php

process called "pruning". Attacks that are beyond the adversary's capability are removed from the model. The remaining attacks are considered highly likely.

# 4 Discussion

## 4.1 The market of Italian citizens' identities

In this section, we describe the main findings of the research, with the aim to provide an overview of the offerings in the market of Italian citizens' identity.
Offerings in black markets are similar to the offerings of usual e-commerce websites present in the surface web such as eBay. An offering can include the following information: description of the product, price proposed and bids (if allowed), profile of the vendor with a classification of the vendor in terms of experience (n. of products sold) and level of trust, feedbacks on the products provided by previous buyers, cost and time for shipping.

The richness of such details varies across products, influenced by the marketing attitude of vendors and typology of products sold. In fig. 2 we report a screenshot of a typical offer in the market.

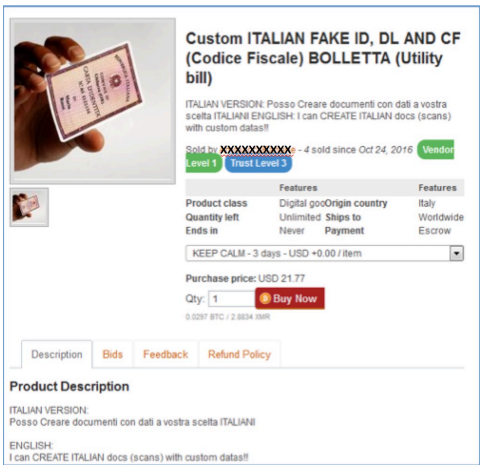


**Figure 2:** Screenshot of a typical offer

Evaluations of vendors are highly considered since they represent a way to obtain credibility with buyers and therefore to increase sales. For instance, in the marketplace called AlphaBay, level and trust of vendors are calculated as follows: level is displayed on listing pages and on the user's profile page and it is influenced by the number of sales, the volume of sales (in $) and the percentage of positive feedback. Trust is independent from the vendor level. Trust increases over the amount of trust gained on the marketplace and the formula for how trust is calculated is not made public.

In our research in the black markets of digital identity, we found 42901 offering from the relevant categories as listed in table 2 in the 6 most important black markets, distributed as follows: 9120 offerings on AlphaBay; 18506 offerings on Dream; 13068 offerings on Hansa; 382 offerings on Leo; 1714 offerings on Outlaw; 111 offerings on Bloomfield.

We selected the three markets with the higher number of offering (AlphaBay, Dream, Hansa) and we reported number of vendors and distribution of offerings to calculate the CR10 (concentration ratio for the first 10 vendors). Results are reported in Table 3. Results shows that Hansa and DreamMarkes are more concentrated than Alphabay and each market has a different structure.

**Table 3:** Size and structure of the three markets

| Market | N. offerings | N. vendors | CR10 |
|---|---|---|---|
| Hansa | 13068 | 201 | 66,6% |
| AlphaBay | 9120 | 1213 | 14,5% |
| DreamMarket | 18506 | 254 | 68,1% |

Among all the offerings listed in the identified categories, we identified 58 offering of interest for the market of Italian citizens' identity. Offerings are distributed as follows: 28 in Alphabay: 19 in Dream Market and 11 in Hansa. Offerings are placed by 38 vendors, 4 of which ship directly from Italy. A detail of the distribution of the offering across marketplaces and categories can be found in table 4.

**Table 4:** Distribution of relevant offerings

| Product_Category | AlphaBay | Dream Market | Hansa | Tot. |
|---|---|---|---|---|
| Carded_Items | 1 | | | **1** |
| Counterfeit_Items | 11 | | | **11** |
| Counterfeits | | | 3 | **3** |
| CVV_Cards | 4 | | | **4** |
| Data | | 1 | | **1** |
| Digital_Goods | | | 2 | **2** |
| E-Books | 1 | 1 | | **2** |
| Fraud | | 2 | | **2** |
| Fraud_Related | | 11 | 5 | **16** |
| Fraud_Software | | | | **0** |
| IDs_Passports | | 4 | | **4** |
| Other_Digital_Products | 1 | | | **1** |
| Other_Fraud | | | | **0** |
| Personal_Information | 9 | | | **9** |
| Services | | | 1 | **1** |
| Social_Engineering | 1 | | | **1** |
| | | | Tot. | **58** |

From an analysis of the relevant offering, we identify three typologies of items that can be purchased to have access to fake identities:

1. Scan/PSD: offering that allows to buy scan of real documents or template to produce a fake ID (e.g. Adobe Photoshop)
2. Fake: offering that allows to buy fake ID
3. Guide/Manual/Info: offering related to guides or tutorials useful to realize fake ID.

The number of offerings related to the three categories is reported in table 5.

**Table 5:** Distribution of offerings among product typologies

| | **Scan/P-D** | **Fake** | **Guide/ Manual** | **Tot:** |
|---|---|---|---|---|
| Id_Card | 11 | 4 | 6 | **19** |
| Passport | 21 | -- | 6 | **21** |
| Driving License | 8 | 7 | 4 | **15** |
| Codice Fiscale | 1 | 4 | -- | **5** |
| Other Docs | 5 | -- | 2 | **6** |

### 4.2 Attack scenarios for e-ID infrastructures

In this section, the results of attack tree analysis from the perspective of a generic e-ID provider is presented. We identified 21 different generic attacks in the attack tree, mainly resumed in:

- e-Id credentials physical theft;
- e-Id credentials purchase on Tor;
- e-Id credentials online purchase through criminal closed groups;
- e-Id credentials exfiltration through third parties attacks;
- valid registration through different authentication factors (smartphones, CNS, e-ID card, SSN etc).

For every single main attack subtree, we checked the feasibility with respect to the items sold in Tor. In particular, the cost associated with a given attack scenario (which may involve several leaf level activities) can be calculated by examining the resource requirements of the scenario's leaf level activities. If the exploit consumes a resource, then the total requirement for that resource is the sum of the scenario's leaf nodes' resource metrics. If the resource can be reused (such as is the case with technical ability) then the resource cost is the maximum of the scenario's leaf nodes' resource metrics. This result can be achieved via the pruning technique, which represents a simple way for evaluating the feasibility of a given adversary performing an attack scenario. The technique compares the resources available to the adversary with the scenario's behavioral indicator costs. Those scenarios with resource requirements greater than the adversary's capabilities can be safely eliminated from consideration (since it is not possible for that adversary to provide them). The attacks that remain

are feasible and, depending whether they are desirable to the threat agent, have some, non-zero level of probability.

The 21 attack scenarios, containing noticeability and technical ability needed to succeed, among which it is possible to identify those affected by the presence of a black market of identities in the dark web.

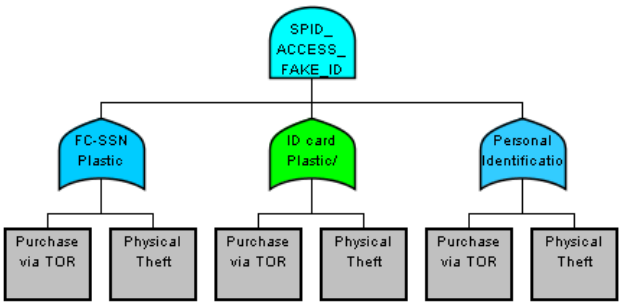


**Figure 3:** Successful attack subtree

In particular, the Figure 3 shows an online registration weakness due to the ease fake identity document retrieval in Tor. In fact, in order to achieve a successful registration to e-ID, in the examined case, we needed a a) physical SSN, b) a physical ID card and c) a de-visu identification performed by an employee of the e-ID provider. Authentication factors in a) and b) can be retrieved in Tor marketplaces (e.g. Alphabay), for an average expense of EUR 500. Hence, all the burden of the identification and authentication is on employee responsibility, which should be trained and equipped to tackle the counterfeited documents. However, this situation is not frequent, because identification is carried out as an ancillary task: for the abovementioned reasons, the Figure 3 represents a practical vulnerability to obtain a not legitimate e-ID.

Moreover, additional factors have an impact on the risk of attack:

- the cost, as above mentioned, is cheap and could not be considered an inhibitor or barrier to commit this crime;
- the technical ability needed is very low, related to the capability to purchase items on Tor marketplaces;
- time is not a relevant variable in this case;
- the noticeability is very low, in case of untrained and unequipped operator for identification, due to the impossibility to verify fake documents.

The exploitation of the abovementioned vulnerability represents a severe threat for all the services based on e-ID: in fact, it harms the reliability and trust of the whole e-ID systems, whose overall security is chained to the weakest provider. A secondary negative effect is represented by the overall situational facilitation enabling even occasional criminals to carry out the identity theft [31].

## 5 Conclusion

The paper presents a measurement study on identity theft in the form of exchange of identity credentials via Tor Hidden Services. With the final goal of investigating the impact of darknet activities on the surface web of digital services, we explore three black markets in search of identity-theft related offers. The phenomenon is then analysed in more detail in the Italian case, where the findings shows that fake passports and id-cards are the most common offers related to identity theft. Finally, we use attack trees to show how the security of national e-ID infrastructures is affected by the easy access to anonymous cyberinfrastructures.

Our study provides both methodological and practical contributions. First, from a methodological point of view, it shows how data collected from the darknet complement more traditional data sources for the analysis of new forms of crimes. Second, it stresses the need to implement technical and organizational countermeasures [5, 6], in order to enhance the link of the e-ID to the physical ID card, which can be easily counterfeited and cheaply purchased from darknet marketplaces.

## 6 REFERENCES


1. Kubicek, H., Noack, T.: Different countries-different paths extended comparison of the introduction of eIDs in eight European countries. Identity Inf. Soc. 235–245 (2010).
2. D'Atri, A., Spagnoletti, P., Za, S.: Institutional Trust and security, new boundaries for Virtual Enterprises. In: Proc. of 2nd International Workshop on Interoperability Solutions to Trust, Security, Policies and QoS for Enhanced Enterprise Systems, IS-TSPQ2007, March 26th, Funchal (Madeira Island), Portugal (2007).
3. Ondrus, J., Gannamaneni, A., Lyytinen, K.: The impact of openness on the market potential of multi-sided platforms: a case study of mobile payment platforms. J. Inf. Technol. 30, 260–275 (2015).
4. Melin, U., Axelsson, K., Söderström, F.: Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective. Transform. Gov. People, Process Policy. 10, 72–98 (2016).
5. Åhlfeldt, R.M., Spagnoletti, P., Sindre, G.: Improving the Information Security Model by using TFI. New Approaches Secur. Priv. Trust Complex Environ. 73–84 (2007).
6. Baskerville, R., Spagnoletti, P., Kim, J.: Incident-centered information security: Managing a strategic balance between prevention and response. Inf. Manag. 51, 138–151 (2014).
7. Cavelty, M.D.: Cyber-security. In: Collins, A. (ed.) Contemporary Security Studies. pp. 362–377. Oxford University Press (2015).
8. Hanseth, O., Ciborra, C.: Risk, complexity and ICT. Edward Elgar Publishing Limited, Cheltenham, UK (2007).
9. Obreja, A.R., Hart, P., Bednar, P.: Potential Benefits of the Deep Web for SMEs Andreea-Roxanna. In: Caporarello, L. (ed.) Digitally Supported Innovation. pp. 63–80. Springer International Publishing (2016).
10. Kraemer-Mbula, E., Tang, P., Rush, H.: The cybercrime ecosystem: Online innovation in the shadows? Technol. Forecast. Soc. Change. 80, 541–555 (2013).
11. Soska, K., Christin, N.: Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. 24th USENIX Secur. Symp. (USENIX Secur. 15). 33–48 (2015).

12. Christin, N.: Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. Proc. 22nd Int. Conf. World Wide Web. 213–224 (2013).
13. Bok, S.: Secrets: On the ethics of concealment and revelation. Vintage (1989).
14. Bakker, R.M., Raab, J., Milward, H.B.: A preliminary theory of dark network resilience. J. policy Anal. Manag. 31, 33–62 (2012).
15. Brinton Milward, H., Raab, J.: Dark networks as organizational problems: elements of a theory 1. Int. Public Manag. J. 9, 333–360 (2006).
16. Hollenbaugh, E.E., Everett, M.K.: The effects of anonymity on self-disclosure in blogs: An application of the online disinhibition effect. J. Comput. Commun. 18, 283–302 (2013).
17. Hudson, B.A., Okhuysen, G.A.: Not with a ten-foot pole: Core stigma, stigma transfer, and improbable persistence of men's bathhouses. Organ. Sci. 20, 134–153 (2009).
18. Baker, W.E., Faulkner, R.R.: The social organization of conspiracy: Illegal networks in the heavy electrical equipment industry. Am. Sociol. Rev. 837–860 (1993).
19. Stohl, C., Stohl, M.: Secret agencies: The communicative constitution of a clandestine organization. Organ. Stud. 32, 1197–1215 (2011).
20. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system, (2008).
21. Ron, D., Shamir, A.: Quantitative analysis of the full bitcoin transaction graph. In: International Conference on Financial Cryptography and Data Security. pp. 6–24. Springer (2013).
22. Dierksmeier, C., Seele, P.: Cryptocurrencies and Business Ethics. J. Bus. Ethics. 1–14 (2016).
23. Batabyal, A.A.: Human actions, the survival of keystone species, and the resilience of ecological–economic systems. Resour. Policy. 28, 153–157 (2002).
24. Sutcliffe, K.M., Vogus, T.J.: Organizing for resilience. Posit. Organ. Scholarsh. Found. a new Discip. 94, 110 (2003).
25. Han, W., Cao, Y., Bertino, E., Yong, J.: Using automated individual white-list to protect web digital identities. Expert Syst. Appl. 39, 11861–11869 (2012).
26. Maler, E., Reed, D.: The Venn of identity. IEEE Secur. Priv. 6, 16–23 (2008).
27. Mont, M.C., Pearson, S., Bramhall, P.: Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services. In: Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on. pp. 377–382. IEEE (2003).
28. Halperin, R., Backhouse, J.: A roadmap for research on identity in the information society. Identity Inf. Soc. 1, 14–15 (2008).
29. Schneier, B.: Attack Trees. Dr. Dobb's J. Softw. Tools. 24, 21–29 (1999).
30. Fraile, M., Ford, M., Gadyatskaya, O., Kumar, R.: Using attack-defense trees to analyze threats and countermeasures in an ATM : A case study. In: Horkoff, J., Jeusfeld, M., and Persson, A. (eds.) The Practice of Enterprise Modeling. PoEM. pp. 326–334. Springer, Cham (2016).
31. Willison, R.: Understanding the offender/environment dynamic for computer crimes. Inf. Technol. People. 19, 170–187 (2006).