Transparency-based reconnaissance for APT attacks

1st Alessio Rugo
Servizio Certificazione e Vigilanza
Agenzia per la Cybersicurezza Nazionale (ACN)
Rome, Italy
a.rugo@acn.gov.it

2nd Claudio Agostino Ardagna
Dipartimento di Informatica Giovanni degli Antoni
Università Statale di Milano
Milan, Italy
claudio.ardagna@unimi.it

***Abstract*—Transparency is a fundamental administrative principle for public institutions. One of its main implementations is the publication of goods and service acquisition tenders, as prescribed by EU and national legislation. This need of transparency can however undermine the security of public institutions, which are disseminating information that could be leveraged by advanced threat actors to bring disruptive attacks. In this paper, we analyse how threat actors can extract useful information from this publicly available information, taking advantage from transparency. We introduce a new technique named *transparency-based reconnaissance*, which implements a passive recognition process using transparency information published under law requirements. To better highlight the value of the gathered data, we experiment its effectiveness by simulating a *transparency-based reconnaissance* run against an Italian public institution, obtaining complete technological and supply chain inventories. The collected inventories enabled the creation of an unsophisticated malware bypassing the defences in place, along with a weaponization and delivery strategy. Finally, we propose a list of potential countermeasure areas, both technical and organizational, to protect information while still safeguarding transparency through a graduated approach.**

***Index Terms*—transparency, cyber security, reconnaissance**

I. Introduction

Transparency is a fundamental administrative principle that allows citizens to participate and assess the work of public institutions on their behalf. It also helps create a deeper trust in government operations and, at the same time, reduce corruption. Lack of transparency may also contribute to the creation of the breeding ground for misinformation campaigns and conspiracy theories [7].

A major practical implementation of transparency principle is the publishing of public tender information on the internet, allowing economic operators to apply for tenders. European public tender legislation demands EU, Nation States, and other relevant entities to promote European-wide competitions, with tender data made available on a public web portal [6]. This portal offers information about both open and already awarded tenders, with data spanning from the contracting administration point of contacts (including names and emails) to the specific individuation of products brought, including IT security systems and the related technical specifications. National lawmakers can impose even stronger constraints in terms of data to be published and retention time.

In this paper, we analyse how threat actors, mostly Advanced Persistent Threat (APT), can benefit from the transparency principle, describing real world examples. We specifically focus on the European legislation, with a further drill-down in the current Italian relevant law landscape, to assess potential national legislation additional impacts (Section III).

After introducing existing abstraction tools used by threat analysts to standardize advanced cyberattack steps (Section II), we show how to perform *transparency-based reconnaissance* (Section IV), a passive victim recognition using transparency information found on public tender publication websites. Additionally, we analyse how the information obtained can be used to effectively plan an attack, detecting at least the most promising entry points and relevant defences (e.g., anti-malware tools). Transparency-based reconnaissance greatly differs from standard OSINT-based reconnaissance techniques proposed in literature, due to its specific focus and peculiarities that lead to potentially obtain - easily, passively and safely from outside the target network - information that usually requires a foothold in the target organization. To better highlight the gathered information value, we also experiment the transparency-based reconnaissance against an Italian public institution (Section V), where we detect different IT products in use and relevant administration contacts, showing how to use them for a hypothetical attack. Finally, due to the importance of balancing transparency and security, we propose a first discussion on possible countermeasures to protect information still guaranteeing a level of transparency (Section VI).

II. Basic concepts and related works

A sophisticated attack conducted by an APT undergoes different phases, starting from studying the target victim up to concealing exfiltrated data and stealthy upload them to the C&C attacker server. Phases can be progressively repeated and interlaced in many ways. Attack frameworks help breaking down a complex attack and describing events from the initial steps up to the final target exploitation, creating a common language for threat intelligence analysts and cybersecurity specialists. One of the first proposed frameworks is the *cyber kill chain* [13], which divides complex attacks, thus also including APTs, into 7 fundamental stages as follows.

1) **Reconnaissance**: a passive study of the target and relevant partners, as well as the identification of target systems and entry points, leading to more active actions such as vulnerability assessment.

2) **Weaponization**: the creation or configuration of the toolset to perform the attack.
3) **Delivery**: actual delivery/deployment/use of the created cyber weaponry.
4) **Exploitation**: actions to further infiltrate the target and create a path towards the objectives.
5) **Installation** of more advanced tools on the victim systems.
6) **Command and Control (C2)**: creation of a connection back to a system controlled by the attacker.
7) **Action on objectives**.

The reconnaissance is normally the first step of an attack, useful both to find weaknesses on the victim premises and to gather information that can help the design and execution of the next attack phases. While it may be easy, even if specific hardening is performed, to assess exposed technologies, the discovery of the internal architecture and tools may be performed only after the attackers has gained the first foothold in the internal network. Thus, the time spent for the internal reconnaissance might be a barrier against the attack also in case of APT: this type of threat actor usually benefits from minor attack timing constraints, due to greater motivations and available resources, but still suffers from the increase of the risks of being detected when operating from inside the target network, potentially having to postpone or reconsider plans in case of victim "blue team" intervention. On the contrary, transparency-based reconnaissance support low-cost acquisition of information without active interactions and from outside the organization. In the related scientific literature, reconnaissance was mostly discussed as one of the steps of the attack within the overall attack kill chain [23]. A few surveys presented in [20] introduce the main reconnaissance techniques, dividing them into three conceptual categories: *i) technical*, mostly focused on network sniffing and scanning techniques [4], but also considering side channels; *ii) social engineering*, through people trust exploitation; *iii) OSINT*, further classified into active or passive techniques and executed from inside or outside the target organization. The OSINT category was further specified by Mazurczyk and Caviglione [14], which identified internet/WWW (i.e., internet intelligence) source type. Odun-Ayo et al. [15] also described the main reconnaissance tools. While also transparency-based reconnaissance may be seen at first glance, oversimplifying, as gathering information from publicly available sources as for the generic OSINT, only attackers specifically aware of this technique will fully benefit from its rapidity and from the completeness of the collectable information, allowing them to focus, in a short time, straight to the relevant transparency information and also on the potentially non-indexed related documents. Moreover, transparency information are published in a relatively structured and consistent way across public administrations, allowing for a more consistent information gathering process (i.e. the transparency-based reconnaissance) and even for its potential automation. Finally, work on countermeasures were focused on the mitigation of active technical reconnaissance operations only, proposing coherent technical measures such as early detection, network interface randomization and deception [2], [3], [11], [12], [16], [19].

III. Transparency regulations and side effects

Transparency is one of the EU foundational values, as stated by *Trattato di Amsterdam*, art. 1, and by *Consolidated Version of the Treaty on European Union*, the basis of the UE law. European institutions are directly targeted by this principle, as provided by the Treaty on the Functioning of the European Union (TFEU), which declares that UE institutions have the responsibility of conducting their work as transparently as possible, including access to documents produced in their administrative work. The most relevant transparency requirements for Member States on the topic is related to tenders held by public institutions under the provisions of Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement, which requires UE member states public institutions to:

- award medium and higher value contracts ($>$ 139k€ for central public institutions) through competitive procedures [5];
- publish tenders that fall under EU rule in the online version of the Supplement to the Official Journal of the European Union (Tenders Electronic Daily – TED) [6].

TED is a public portal that does not need any enrolment or authentication: a plain user can search current and past (up to 10 years) tenders, filtering results by Common Platform Enumeration (CPE) or Common Procurement Vocabulary (CPV)[1] codes (e.g., searching for AV products), type of business, institution, and the like. TED publishes more than 400k calls for tender/yr (€420bn exchanges estimated on 2017 [18]).

National level law prescription can overlap and be even stricter than EU legislation, as for the Italian case. Italy has a long-term issue with corruption in the public sector [1], which makes it one of the strictest legislations on the matter. It provides a limited discretional power in the hand of public administration under the combined action of the *Decreto Trasparenza* (D.Lgs n. 33/2013, called "Transparency Act" [9]) and the *Nuovo Codice degli Appalti* (D.Lgs. 18th April 2016, n. 50 [10], Italian current public tenders and contracts legislation created as Directive 2014/24/EU national implementation). The Italian Transparency Act (ITA in the following) requires Italian public administrations to publish information about active or already awarded economic tenders and related documents. This information is normally published in each administration institutional website, in dedicated areas usually named *Amministrazione Trasparente* and *Bandi di gara*. More in detail, ITA requires national public administrations and public tender operators to publish on their website those acts and information listed in art. 1 of law November 6th, 2012, n. 190 (tender proponent, object, list of

[1]CPV is a classification system for public procurement that standardize references used by contracting authorities. CPE is specifically dedicated to IT systems and software. They have a structured (hierarchical) naming schema.

the invited economic operators, the awarded operator and the due amount, service/acquisition timing) and all the documents and information related to the tender, under the requirements of the above mentioned *Nuovo Codice degli Appalti*. The latter documents include all the administration-relevant internal acts, the tender awarding commission appointed members, and their curricula. Information publishing does not generally depend on the tender value/amount.

As side effects of the aforementioned prescriptions, published information provide a broad insight into Public Administrations commercial relationships, which also include technical support contracts and ICT products, exposed, without any entrance barriers, in easily identifiable spots on the public network. To obtain a similar level of insight, a threat actor should perform active reconnaissance actions, rather then merely passive, in some cases even needing a foothold in the organization internal network. This represents a huge advantage for the attacker in implementing a proper kill chain, as for the APT case. Moreover, it is important to note that the transparency-related information will be equally published either in case of commercial agreements directly with the vendor or, as commonly seen for complex acquisitions, whether an intermediate system integrator is involved: tender technical specifications must be provided in any case, in advance, to ensure that the supplied object adhere to the public administration expectations.

IV. Transparency-based reconnaissance

We define transparency-based reconnaissance when the recognition is performed gathering the transparency contents published online. We identify three different types of information as follows:

- *Contacts* (name, position, email addresses, and the like), found inside tender documents (e.g., points of contact, responsible for the procedure) or even as metadata related to these documents (e.g., document creator name automatically inserted by the automation software). This information may be useful for orchestrating a spear phishing campaign impersonating the partner.
- *Technology acquired by the administration*. Tender data usually contains also the period of validity of the contract, which provides valuable hints about their current use in the target network. Information includes: *i)* cybersecurity products, which help to choose the best tactics to avoid detection; *ii)* IT system in general, such as internal software (e.g., office suite) or remote access tools (e.g., VPN). Knowing in advance what kind of tools are deployed can accelerate the initial external recognition phase by the attacker and also speed-up the research for a vulnerability in those systems that may allow for a remote access or code execution.
- *Supply chain information*, checking the companies awarded for one or more tenders. Threat actors may consider exploiting relevant third parties by penetrating the partner network or IT systems, or even recruiting workers inside the partners to gain access to valuable information or a pathway to their real target, such as in the SolarWind case [8].

This information may be gathered using two channels, EU TED and national transparency web portal(s), where Tender processes are made increasingly digital.

Transparency sources in EU (TED portal). TED web portal is accessible via browser at https://ted.europa.eu. A threat actor would probably focus on the "business opportunity" area, where it can search by country. TED provides a granular search engine, where it is possible to specify, among the others, the CPV code, the country and name of the buyer, the relevant dates, the type of notice.

Reconnaissance in Italy (*Amministrazione Trasparente*). Threat actors interested in Italian government institutions can benefit from information related to tenders by passively acquiring them from the sections *Amministrazione Trasparente* and *Bandi di gara* of their institutional website. Searching for past-awarded tenders, similarly to TED, it is possible to find a wealth of information, both related to contacts, technologies, and third-party contracts. In this case, information can be even broader, due to higher customization of the dedicated website section, designed by each public administration on its own, with custom constraints on contents to be uploaded (e.g., whole scanned documentation instead of manually inserting the minimum data required by law). Given the variety of the uploaded documents file formats, search engines may not be generally able to apply consistent indexing, thus requiring the web site sections exploration by the threat actor. Without a proper data minimization process implemented and monitored by the organizations, threat actor reconnaissance benefit level may also depend on the specific operator awareness, leading to more or less relevant data to be uploaded/inserted. Low level of awareness can be assumed, since *transparency-based reconnaissance* is not currently recognized, to the best of our knowledge, as a threat.

According to law, the subsections of the website where tender information is published must be open (no restrictions or authentication), timely updated, and kept online and publicly available for a lifespan of 5 years. These requirements go beyond the public advertising lower bounds imposed by the *Codice degli Appalti* law, which requires the tender information to be available for 180 days.

V. A practical example of transparency-based reconnaissance

We discuss the potential of transparency-based reconnaissance, presenting an attempt to extract information about technologies in place in an existing Italian central Public Administration (IPA, in the following). The first step is to locate section *Amministrazione Trasparente* in the website, which contains many different types of acts.

We note that each administration can organize the required contents within section *Amministrazione Trasparente* freely. This means that the threat actors may have to spend some time in studying the organization of the website. In the IPA

case, there are different sections that may contain valuable information. We note that we focused on a simplified technology overview, neglecting contacts and supply chain inventory.

From the content of the document depicted in Figure 1 we can identify that the antivirus protection equipped by IPA is from McAfee and licences will expire in August 2022. In the same section, we can also spot non-IT relevant contracts, such as the cleaning service, which can be potentially used for a physical attack via supply chain exploitation. To obtain technology-related information, we searched the most promising sections of the website *Amministrazione Trasparente* at IPA. An interesting subsection, *Informazioni sulle singole procedure*,[2] provides information regarding the single emitted invoices. This subsection permits advanced searches, where the threat actor can specify the target department. All sections in the web portal allowed a threat actor to complete, within a few hours, a partial technological recognition for IPA internal and external networks (partial excerpt in Table I).

A complementary operation can be performed with web search engines (e.g., via google dorks [17]), by searching relevant keywords (e.g., EDR) and narrowing the query to focus specifically on the website of *Amministrazione Trasparente* , as confirmation of the completeness of the manual investigation.

The technological findings in this section made it possible to detect 4 interesting target network properties, identified as most promising to plan the attack.

- *Finding 1: VPN access to the organization network.* An attacker can identify an entry point and search for the (already known) commercial product vulnerabilities and weakness.
- *Finding 2: Specific anti-malware tool.* An attacker can use this information to design a malware that deceives the installed anti-malware tool (and not trying to evade most of them).
- *Finding 3: No Endpoint Detection and Response (EDR).*
- *Finding 4: Adoption of Microsoft Office and Adobe Acrobat.*

Following the Cyber Kill Chain, the next step is the weaponization. Based on collected information, we generated a macro malware specifically targeted for Microsoft Word. For this step, we use *msfvenom* tool [22] to create:

- a first stage Microsoft Office .doc macro malware, with the task of downloading the second stage malware;
- the second stage malware, crafted to be compatible with the target platforms (Windows, as we detected from the transparency-based reconnaissance) and able to bypass the specific antivirus product in use. This payload will try to spawn a reverse shell using *Meterpreter* [21].

To lower down antivirus detection rate, we used the following basic deceptive steps:

1) execute msfvenom to easily obtain a memory injection reverse shell code;
2) compile a custom executable embedding the obtained shellcode:
- import the msfvenom output inside a C++ basic console project template, along with instructions to execute it. This avoid using the default msfvenom *exe* template, easily detectable from antiviruses. We also include a variable string to iteratively change the compiled exe hash;
- compile a x64 executable without debug symbols.

With this simple process, we reduced the detection rate of the anti-malware tools, including McAfee (see Figure 2), the one found during the reconnaissance run, to less than 50%.

[2]https://trasparenza.mise.gov.it/index.php/lista-trasparenza-acquisti

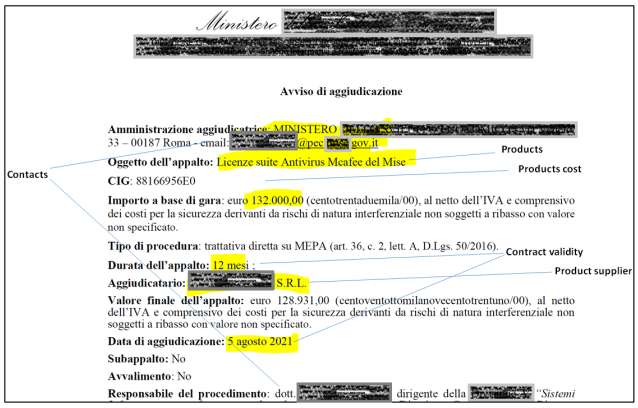

Fig. 1. An example of tender document provided in the section *Amministrazione Trasparente* of IPA.

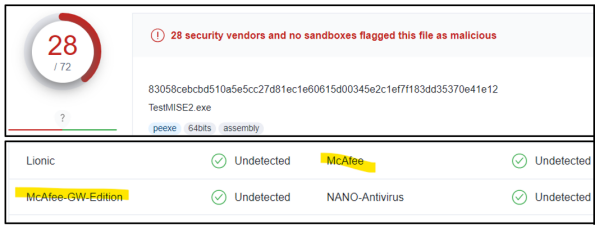

Fig. 2. Excerpt from the Virus Total report on the malware sample. McAfee were not able to detect it.

VI. Challenges, Countermeasures and Research Actions

We described how data published under transparency legislation may enable a stealthy and complete passive reconnaissance of the administration IT infrastructure and supply chain. Anyway, transparency remains an important asset for the citizen-state relationship in terms of openness and accountability and a tool for anti-corruption. While we focused on the security and technical aspects of the topic, it is clear that there is an important balance of interests between the potential cyber-risks rise and the completeness of transparency information provided, whose inclination mainly depends on political decisions at EU and Member State level, also considering the applicable constitutional principles, as well as on the economic and social risk appetite of the specific historical period. As a consequence, it is not possible to determine a

TABLE I
TECHNOLOGY INFORMATION AFTER ENRICHMENT.

Product type	Producer	Start date	Duration
Antivirus	McAfee "Suite Antivirus e Threat Defence"	05/08/2021	12 months
Storage	Datacore SDS	20/01/2021	36 months
Firewall/VPN	Sonicwall	SMA9200V	13/01/2021
DBMS	Oracle	19/11/2021	11 months
Software	PRTG network monitor	18/08/2021	24 months
Software	Ivanti Service Desk	22/03/2021	36 months
Software	Adobe Premier Pro	05/08/2020	n.a.
Hardware/Software	RSA SIEM (Appliance HybridRSA)	21/02/2020	n.a.
Software	Microsoft Office	16/07/2018	24 months
Hard/Software	Potenziamento SIEM RSA	26/06/2018	n.a.

priori the best balancing approach between transparency and security and this is, anyway, beyond the scope of this paper. While transparency-based reconnaissance can be effectively exploited, it is not considered a priority for increasing the public administration protection levels.

However, risk mitigation usually derives from a combination of controls, rather than a single countermeasure (defence in depth approach), and it should take transparency-based reconnaissance into account. Limiting information, both qualitatively and in terms of time of publication, without fully hampering transparency foundations, should be practiced at least on a national basis. In our opinion, the most relevant, yet simpler intervention is to shed light on the topic: transparency-based reconnaissance is not yet considered, even on a intuitive plane, both form EU and national law-makers and public administrations. An increase of awareness on the topic may help conceiving further relevant law updates concerning transparency also embedding security aspects. On a short time frame, public managers may also review their current operative transparency procedures to ensure that i) published information is restricted to the minimum needed both from law previsions and effective tender needs, ii) transparency operators (e.g. the transparency web site area back-office operators) are fully aware and strictly adhere to the procedures specifying which information to publish and documents to be uploaded for each type of tender phase and, finally, iii) transparency-based reconnaissance is considered within the risks landscape to allow to include it in the related analysis.

As a first, more specific contribution to the matter, we then propose the following potential countermeasure areas:

- reconsider historical records retention, keeping data fully available only for the minimum required period. Data can still be made available for statistical reasons after a generalization step (e.g., changing the product type from *anti-malware* to the more general *security software* by shifting to the previous CPV level on the hierarchy).
- Concerning the active tender period, restricting data only to interested economic operators, thus not hampering transparency or the economic competition. As an example, creating an EU-level portal for public tenders (e.g., extending TED with enrolment and authentication). Again, APTs may create a fake company but this would require an active action, providing information for investigations and an early warning.
- After a tender is awarded, transparency requires a subset of related information to be published. We propose to introduce the possibility for the administration to label each tender, at submission time, as *sensitive* whenever relevant information may have adverse effects on cybersecurity. This classification can be used during the active tender process and after it is awarded further limit display time and information made publicly available. To reduce transparency hampering, this would be applied only to a predefined set of products and services.

Approach taken from personal data protection techniques can be adopted for sensitive tenders, such as: *i)* generalize product type data (e.g., by CPV hierarchy level shifting above); *ii)* mask producer and awarded operator data.

To counter-balance the loss of transparency, additional administrative warranties may be provided, such as prescribing national competent authorities (e.g. Corte dei Conti in Italy) mandatory revisions on every sensitive tender. Semi-automatic revision processes using AI can be also implemented to identify critical contracts, as a further improvement to reduce the effort. This will be the topic of our future work.

As more general advices to protect tender data inside the document or its electronic representation:

- transparency website section should include the minimum data required by law to avoid unnecessary data leakage. This is also an awareness problem, due to the fact that transparency-based reconnaissance issues have not been included in the threat landscape yet;
- remove administration contacts and names, whenever possible, from tender documentation;
- require a document metadata cleaning process on uploading to the transparency section.

In any case, a complete *security by obscurity* approach, with tender data made unavailable for the general public, would be unbalanced: putting more efforts in a holistic protection to defend the organization according to environmental risks would lead to more effective results than simply hiding information.

VII. CONCLUSIONS

Our paper first examined the basic principle of transparency in the citizen-government relationship and how it evolved over time. Transparency contributes to create a deeper trust in

government operations and reducing corruption: lower levels of transparency create the breeding ground for misinformation campaigns and conspiracy theories.

We then identified the practice of publishing public administration's tender information as one of the relevant concrete transparency principle implementation, allowing citizens to perform administration control and widening the competition between economic operators. In Europe, tenders above a certain economic threshold requires to be published in the *Tender Electronic Daily* portal, but national law may also place stronger requirements, as in the Italian case. At the same time, we analyzed how all these data, which also encompasses IT and cybersecurity systems, can be exploited by threat actors to reduce attack risks and time, identifying, to the best of our knowledge, a new type of reconnaissance technique called *transparency-based reconnaissance*: a passive victim recognition using transparency information found on required tender websites (TED and transparency dedicated national websites). It greatly differs from reconnaissance techniques in literature: while the broad OSINT-based reconnaissance category (e.g., "internet intelligence" in [14] or, more generally, OSINT in [20]) includes searches on the WWW, transparency-based reconnaissance has a specific focus and peculiarities that lead to potentially obtain, passively and safely from outside the target network, information that usually requires a foothold in the target organization. Moreover, transparency information are published in a relatively structured and consistent way across public administrations, allowing for a more consistent information gathering process (i.e. the transparency-based reconnaissance) and even for its potential automation.

We experimentally evaluated transparency-based reconnaissance in real world scenarios, focusing on European legislation, also proposing a drill-down in the current Italian relevant law landscape to assess potential national legislation additional impacts. We performed a complete reconnaissance run against an Italian public institution, where we were able to detect many software products in use and relevant administration contacts, showing how to use them for a hypothetic attack. Anti-malware information has been used to create a poorly sophisticated malware being able to avoid escape malware detectors in the target network.

Finally, we highlighted the balance of interests between security and transparency. Given the high number of different stakeholders (e.g., national law-makers, economic private operators, public administration), these results may be seen as the first step to start a multidisciplinary discussion on the topic with the relevant operators and experts, thus finding the best balance between principles and counter-effects in the specific historical period. As most promising intervention on a short term period, we proposed the goal of raising the awareness on the topic, both for the law-makers and public administrations, also by including transparency-based reconnaissance within the current risks landscape. We then proposed a list of practical areas that could be further explored to provide additional countermeasures on a longer term while still allowing to graduate transparency levels.

REFERENCES

[1] Vannucci Alberto. L'evoluzione della corruzione in italia: evidenza empirica, fattori facilitanti, politiche di contrasto. *La corruzione amministrativa. Cause, prevenzione e rimedi*, 2010.

[2] Elias Bou-Harb, Mourad Debbabi, and Chadi Assi, editors. *On detecting and clustering distributed cyber scanning*. IEEE, July 2013. https://ieeexplore.ieee.org/xpl/conhome/6578011/proceeding.

[3] Elias Bou-Harb, Mourad Debbabi, and Chadi Assi. A systematic approach for detecting and clustering distributed cyber scanning. *Computer Networks*, 2013.

[4] Elias Bou-Harb, Mourad Debbabi, and Chadi Assi. Cyber scanning: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 2014.

[5] europa.eu. Public tendering rules. https://europa.eu/youreurope/business/selling-in-eu/public-contracts/public-tendering-rules/index_en.htm, 2023.

[6] europa.eu. Ted home - ted tenders electronic daily. https://ted.europa.eu/TED/main/HomePage.do, 2023.

[7] europeanlawblog.eu. An agenda for transparency in the eu – european law blog. https://europeanlawblog.eu/2019/10/23/an-agenda-for-transparency-in-the-eu, 2022.

[8] Jibilian Isabella and Canales Katie. The us is readying sanctions against russia over the solarwinds cyber attack. here's a simple explanation of how the massive hack happened and why it's such a big deal. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T, 2021.

[9] Repubblica Italiana. Decreto legislativo 14 marzo 2013, n. 33. https://www.bosettiegatti.eu/info/norme/statali/2013_0033.htm, 2013.

[10] Repubblica Italiana. Decreto legislativo 18 aprile 2016, n. 50. https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2016-04-19&atto.codiceRedazionale=16G00062, 2016.

[11] Jafar Haadi Jafarian, Ehab Al-Shaer, and Qi Duan. An effective address mutation approach for disrupting reconnaissance attacks. *IEEE Transactions on Information Forensics and Security*, 2015.

[12] Huanruo Li, Yunfei Guo, Shumin Huo, Hongchao Hu, and Penghao Sun. Defensive deception framework against reconnaissance attacks in the cloud with deep reinforcement learning. *Science China Information Sciences*, 2022.

[13] Lockheed Martin. Cyber kill chain® — lockheed martin. [online]. Available at https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[14] Wojciech Mazurczyk and Luca Caviglione. Cyber reconnaissance techniques. *ACM*, 2021.

[15] Isaac Odun-Ayo, Emmanuel Owoka, Otavie Okuoyo, Opeyemi Ogunsola, Obaro Ikoh, Olumide Adeosun, Deborah Etukudo, Victoria Robert, and Gabriel Oyeyemi. Evaluating common reconnaissance tools and techniques for information gathering. *Journal of Computer Science*, 2022.

[16] Kartik Palani and David M. Nicol. Hardening critical infrastructure networks against attacker reconnaissance. https://www.researchgate.net/publication/346002662_Hardening_Critical_Infrastructure_Networks_Against_Attacker_Reconnaissance, August 2020.

[17] AwatiIvy Rahul and Wigmore Ivy. What is a google dork query? https://www.techtarget.com/whatis/definition/Google-dork-query, n.a.

[18] Isabel Rosa. Electronic procurement in the eu. https://store.proebiz.com/europske-trendy-isabel-rosa-europska-komisia.pdf, 2017.

[19] Neil C. Rowe and Han C. Goh, editors. *Thwarting Cyber-Attack Reconnaissance with Inconsistency and Deception*. IEEE SMC Information Assurance and Security Workshop, 2007. https://ieeexplore.ieee.org/document/4267555.

[20] Shanto Roy, Nazia Sharmin, Jaime C. Acosta, Christopher Kiekintveld, and Aron Laszka. Survey and taxonomy of adversarial reconnaissance techniques. *ACM*, 2023.

[21] Offensive Security. Meterpreter basic commands. https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/, n.a.

[22] Offensive Security. Msfvenom. https://www.offensive-security.com/metasploit-unleashed/msfvenom/, n.a.

[23] Tarun Yadav and Arvind Mallari Rao, editors. *Technical Aspects of Cyber Kill Chain*. Springer International Publishing Switzerland, August 2015. https://link.springer.com/chapter/10.1007/978-3-319-22915-7_40.