

POLYTECHNIC UNIVERSITY OF TURIN

Master Degree Course
in Computer Engineering

Master Degree Thesis

Advanced C2 Fingerprinting



Advisor

Paolo Ernesto Prinetto

Co-advisors

Nicolò Maunero

Liborio Pepi

Advisors' signatures

.....
.....
.....

Candidate

Lucio De Fusco

Candidate's signature

.....

Academic Year 2022-2023

*A Fabio Rispoli,
mio professore,
mentore e amico*

Abstract

The growth of the digitalized world has increased with the number of malicious actors. Cybercrime is now organized like structured companies, with human resources, developers, operators and executives. On the other hand, public and private organizations have a lot of exposed IT infrastructures, often with sensible assets, security flaws, and with little or zero knowledge about the risks. With such an attractive business, cybercrime incidents occur on a massive scale every day. Even after global law enforcement interventions, the phenomenon has not significantly decreased. For these reasons, it became necessary to build equally structured cyber defense measures, to stop these attacks as soon as possible. Among the several methods of countering compromise, those related to cyber threat intelligence are growing in importance. The work proposed here is a new way to standardize the Command and Control (C2) fingerprinting, an intelligence technique used to proactively detect and negate communications with malicious servers. Historically, it is concerned with identifying cyber attacks, running on local endpoints, in the Command-and-control phase, when the adversary operating infrastructure communicates with the victim hosts for Post-compromise activities.

In recent times, however, C2 fingerprinting has been applied to the entire cyberspace of the Internet. Research has already shown that it can have a crucial impact on protecting hosts. Despite having been developed several methods to obfuscate C2 infrastructures, the IP of the servers must be present on the Internet, and at least with one publicly accessible service for communications. Starting from this fact, the researchers began to outline the common characteristics of these servers. Relying on some cyberspace search engines, they proved that it is possible to hunt the Internet looking for malicious hosts.

However, the time spent manually probing the Internet is often far from being negligible. In addition, there are new command and control boards emerging day by day, many features to compare by hand, and small-time windows for more in-depth investigations. These are just some of the limitations of the actual C2 fingerprinting technique. Here it's proposed a new approach to overcome such constraints. The aim was to bring order to a confusing and mostly practical coverage of the subject. From this perspective, the C2 fingerprinting process has been split into eight well-defined phases. Each phase tries to define standard logic to follow and a support nomenclature. The common thread is to design every aspect to be automatable, for instance by replacing human assessment of C2 server characteristics with a simple but effective mathematical formula. Just a basic implementation of this approach has shown very promising results. The Proof of Concept developed showed how it is possible to automate, expand and classify the hunting

of C2 servers. By linking various systems, such as cyberspace search engines and intelligence feeds, to a framework with aggregation and query capabilities, it was possible to trace more than a hundred C2 families at the time of writing. The practical results produced, i.e. lists of IP addresses associated with one or more command and control servers, can be integrated within cybersecurity environments with different purposes and levels of awareness.

Acknowledgements

Greetings to Paolo Prinetto for the opportunity to draw up this paper and contribute to scientific production in the Cybersecurity field.

Greetings to Liborio Pepi and his undisclosed company for the shared experience, the resources, the time and attention spent in my work and professional growth.

Contents

List of Figures	10
1 Introduction	13
2 Cybersecurity	15
2.1 The Sliding Scale of Cyber Security Model	15
2.1.1 Architecture	16
2.1.2 Passive Defense	17
2.1.3 Active Defense	18
2.1.4 Intelligence	19
2.1.5 Offense	21
3 Cyber Threat Intelligence	23
3.1 CTI types	23
3.1.1 Strategic	23
3.1.2 Operational	24
3.1.3 Tactical	24
3.2 Threat Group Categories	25
3.2.1 Hactivism	25
3.2.2 Cybercrime	25
3.2.3 Nation-state	26
3.2.4 Unknown	26
3.3 Cyber Threat Frameworks	27
3.3.1 Cyber Kill Chain	27
3.3.2 MITRE ATT&CK	27
3.3.3 Unified Kill Chain	29
4 Command and Control	31
4.1 Definition	31
4.2 Topologies and techniques	31
4.3 Frameworks	33
4.3.1 Metasploit	33
4.3.2 Cobalt Strike	34
4.3.3 Sliver	35

4.3.4	Covenant	36
4.3.5	Brute Ratel	37
4.3.6	Havoc	38
4.4	Malware	38
4.4.1	ISFB	39
4.4.2	QakBot	39
4.4.3	Quasar	39
4.4.4	Pupy	40
4.4.5	SocGhosh	40
4.4.6	TrueBot	40
5	C2 Fingerprinting	43
5.1	Definition	43
5.2	State Of The Art	44
5.3	A practical example	46
5.3.1	Collecting	47
5.3.2	Cleaning	47
5.3.3	Comparing	47
5.3.4	Pivoting	48
5.3.5	Refining	48
5.3.6	Fingerprinting	48
5.3.7	Hunting	48
5.3.8	Re-checking	49
6	A new approach	51
6.1	Project Questions	51
6.1.1	Why	51
6.1.2	What	52
6.1.3	Who	52
6.2	Process	52
6.2.1	Collecting	52
6.2.2	Cleaning	52
6.2.3	Comparing & Pivoting	53
6.2.4	Refining	54
6.2.5	Fingerprinting	54
6.2.6	Hunting	54
6.2.7	Re-checking	55
6.3	PoC	55
7	Results	57
7.1	Advantages	59
7.2	Limitations	59
8	Future Work	61

9 Conclusions	63
Bibliography	65

List of Figures

2.1	The Sliding Scale of Cyber Security [167]	16
2.2	Value Towards Security (Left) vs. Cost (Right) [98]	17
2.3	Roles of the People in a Security Operations Center [166]	19
2.4	The Relationship of Data, Information, and Intelligence [98]	20
3.1	Lockheed Cyber Kill Chain [95]	28
3.2	Unified Kill Chain [107]	30
4.1	Metasploit msfconsole [105]	34
4.2	Cobalt Strike GUI [195]	35
4.3	Sliver console [206]	36
4.4	Covenant Dashboard [39]	36
4.5	Brute Ratel GUI [18]	37
4.6	Havoc GUI [154]	38
5.1	Censys Search	45
5.2	C2 fingerprinting state-of-the-art flow [108]	46
5.3	C2 fingerprinting process	46
6.1	Cobalt Strike generated modules query	55
7.1	Average matches between 02/07/2023 and 09/07/2023	57
7.2	Average matches between 02/07/2023 and 09/07/2023 - matches detail	58

*The best way to predict
the future is to create it*

[A. LINCOLN]

Chapter 1

Introduction

People and machines are increasingly interconnected. This was true fifty years ago and it is even more so now, especially after the Covid-19 pandemic. The preventive quarantine has forced a shift of activities to the web as much as possible. Despite the remote working percentage almost returning to the pre-Covid level [197], the displacement of individuals' and companies' assets to the Internet continues apace. These assets are information, that represents the currency of our era. A simple metaphor like this, however, can't be extended to the type of protection that such currency needs. We can't just think of securing our information by putting them in a vault or a bank. No globally recognized system dealing with this work exists, and even if it did, it would have a very different and complex structure compared to what we are used to thinking. Complexity is an enemy of the users even if well-standardized security mechanisms such as multi-factor authentication and password manager's autofill exist, people tend to evade complexity overheads with approaches like reusing passwords across different accounts and easily sharing them [174]. These habits make humans the weakest link in protecting digital assets. This is even more true in enterprises, where breaches start mainly with the compromise of credentials [57]. Together with low awareness and machine flaws, these facts describe the current state of information protection in most global organizations. For such reasons, the so-called "cybersecurity posture", that is the ability of a company to withstand cyber attacks, is growing in terms of priority and investments [19]. There are two major approaches to handling attacks in cyberspace: threat detection and threat hunting [183]. The first one is reactive, as it is concerned with managing and mitigating active alerts. The second, instead, is proactive in the sense of preventing future attacks and discovering lurking undetected menaces. In recent years a new approach, that of threat intelligence, has grown in importance. This method empowers the other two with knowledge about old and possible future threats. This is accomplished in practice by sharing threat details, analyzing known cybercrime tactics, and producing new information from criminal investigations [43]. The work presented here settles in the current state of the art of cyber threat intelligence [79]. The aim was to find, study and improve a promising intelligence technique in terms of threat prevention. Among many, it has been chosen to delve into Command and Control (C2) fingerprinting, a very young and powerful approach in preventing threats. This technique consists in outlining common characteristics belonging to malicious servers,

called Command Control or C2 servers, from which attacks are conducted. To improve such a method, it has been mandatory to start by building the knowledge base behind it. From cybercrime behavior to threat models, it was important to go through all the steps needed to understand why this technique was born. Then, the C2 fingerprint itself has been analyzed and used in the wild. Unfortunately, there weren't many sources from which to find information about it. Most of the people involved in using this technique are cyber threat researchers, who do not belong to the academic world. Therefore, being in a company specializing in cyber defense has been essential in drafting this paper. After practicing with the various phases and tools used in Command Control fingerprinting, the paper starts analyzing its actual limits, most of which are related to timeliness and manual effort. In order to expand these boundaries, the work presented here attempts to build a new approach based on what we know so far about manual C2 fingerprinting. By using cyberspace search engines, automated processes, and a query language, it has been possible to ingest threat feeds from different sources, elaborate them, and produce new threat intelligence information. This way of operating opened a new set of possibilities, many more than required. It enabled not only the automation of classical C2 fingerprinting but also the complete redesign of the steps involved in it. Even if the Proof of Concept developed here has wide room for improvement, the results of this approach are already very promising, and they can be spent right away in the everyday cybersecurity context to add a strong proactive line of defense. This journey will start by providing a base knowledge about cybersecurity and cyber threat intelligence, achieving our goal with a bottom-up approach, from theory to practice.

Chapter 2

Cybersecurity

From an educational point of view, cybersecurity, also called computer security, is a branch of information security discipline [173, 22, 84, 58]. Since a globally recognized definition of what cybersecurity is does not exist, we will take into account the one that seems most compatible with our work, stated as: *"the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users"*[173].

Confidentiality, integrity and availability, usually acronymized as CIA, are considered «the core principles of information security». In particular, with regard to information systems: • confidentiality prevents disclosure to unauthorized individuals or systems. [172]:

- **Confidentiality** prevents disclosure to unauthorized individuals or systems.
- **Integrity** avoids changes without authorization.
- **Availability** guarantees access when needed.

2.1 The Sliding Scale of Cyber Security Model

When talking about cybersecurity, we noticed that the term is mostly used when we refer to security concepts, strategies, and goals. When, on the other hand, we refer to the practical measures needed to protect resources, the term *cyber defence* (or *defense*) seems more accurate [63, 48, 98]. In "The Sliding Scale of Cyber Security", a «model for the progression of security maturity in an organization», and more distinctions are drawn [167].

According to the SANS Instructor Robert M. Lee, author of the model, the framework «is useful in a number of ways, which include explaining technical safety issues to non-specialists, prioritizing and tracking the investment of resources and skillsets, measuring security posture, and confirming the accuracy of incidents' root cause analysis». Graphically, the model is represented by a non-static sliding scale 2.1 that, from left to right,

defines in five categories how to build defenses in a more meaningful way, from both utility and cost perspectives. In particular, the value towards security given by each category is inversely proportional to the cost required to implement its requirements. We'll explore these categories one by one to have a general overview of cyber defense practices, which will be helpful for further topics.

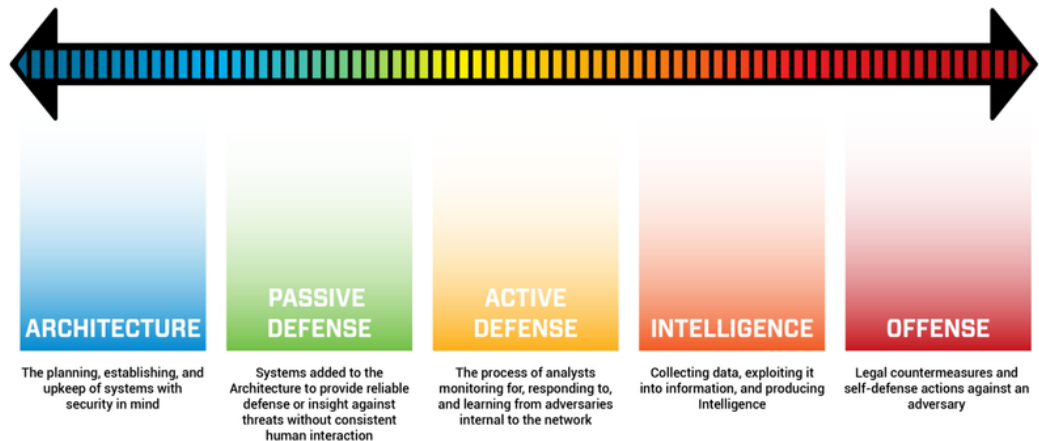


Figure 2.1. The Sliding Scale of Cyber Security [167]

In particular, the value towards security given by each of category is inversely proportional to the cost required to implement its requirements 2.2. We'll explore these categories one by one to have a general overview of cyber defence practices, which will be helpful for further topics.

2.1.1 Architecture

Architecture is the first and most valuable class of the model. It is defined as «the planning, establishing, and upkeep of systems with security in mind». This category represents the foundations «upon which all other aspects of cyber security can build». Its requirements (hardening systems, patching software, avoid misconfigurations...) could be summarised with the adoption of OWASP¹ security by design² principles applied both to hardware and software, like minimizing attack surface area, secure defaults, least privileges and fix security issues correctly [152].

¹Open Source Foundation for Application Security

²«Security by design is an approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attack as possible through such measures as continuous testing, authentication safeguards and adherence to best programming practices» [189]

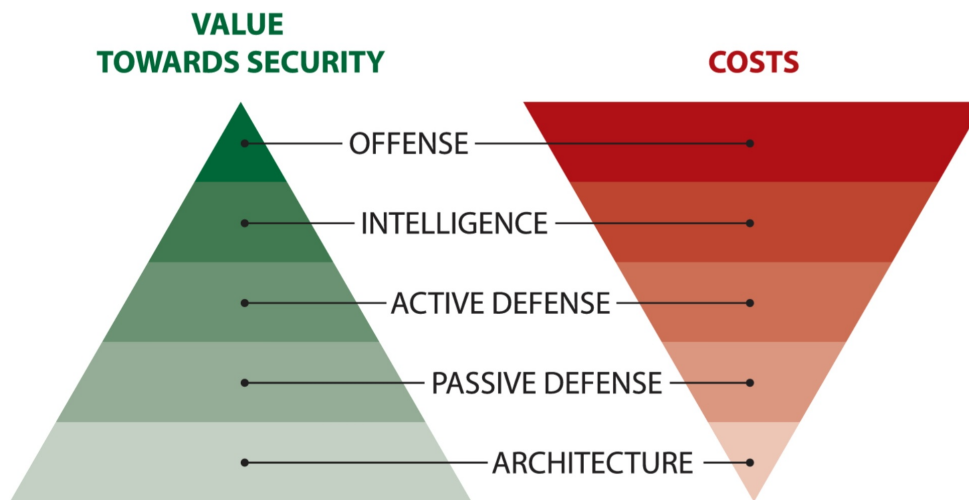


Figure 2.2. Value Towards Security (Left) vs. Cost (Right) [98]

2.1.2 Passive Defense

With a solid architectural base, we can move on to the next step: passive defense. According to this category, we should put add-on defensive structures on top of existing systems. A definition of passive defense is given: «systems added to the architecture to provide consistent protection against or insight into threats without constant human interaction». An akin concept is *defense in depth*, present both in OWASP security by design principles that in the Defense Cyber Operations of US Department of Defense cited by the author. The principle expresses the need to use several passive protection layers of different kinds, so as to increase the effort required by the adversaries to achieve their goals. A practical example could be putting an antivirus³ and an intrusion prevention system⁴ downstream of a firewall⁵, so that the attacker is forced to bypass all three before he can compromise the machines.

³«A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents» [127].

⁴« A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets [137].»

⁵«An inter-network connection device that restricts data communication traffic between two connected networks» [132].

2.1.3 Active Defense

Often mistaken with "hack-back"⁶ practices, Active Defense is instead «the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats internal to the network». The author regroups roles like incident responders and malware reverse engineers under the same figure as an analyst. However, it would be more accurate to refer to the division of roles in a Security Operation Center ⁷, effectively summed up by Nugraha in his "A Review on the Role of Modern SOC in Cybersecurity Operations" [148]:

- Tier 1 - Alert Analyst: often known as Cybersecurity Analysts or CyberOps Associates, track incoming notifications, verify that a true incident has occurred, and, if appropriate, forward tickets to Tier 2.
- Tier 2 - Incident Responder: these experts are in charge of conducting in-depth investigations into incidents and recommending remediation or intervention.
- Tier 3 - Threat Hunter: these experts have advanced knowledge of network, endpoint, threat intelligence, and malware reverse engineering. They are experts at tracing malware's processes to assess its effect and how to delete it. They're also heavily involved in the search for new threats and the deployment of threat detection software. Threat hunters look for cyber threats that are yet to be identified but are present in the network.
- SOC Manager: this individual is in charge of the SOC's resources and acts as a point of contact with the larger company or client 2.3.

After this clarification, we can explain Active Defense as a perimeter interactive approach to security focused on SOC human components. We can provide a practical example by citing another Lee model, "The Active Cyber Defense Cycle", which is «the continual process of four phases of actions that defenders can take to actively monitor for, respond to, and learn from adversaries»:

- Threat intelligence consumption: improving defenders' activities with learnings derived from past systems compromise.
- Asset identification and network security monitoring: identifying the assets to be protected and monitoring the network for anomalies.
- Incident response: «detect, respond to, and limit consequences of malicious cyber attacks» [136].

⁶«Intrusive action against a cyber-attacker on technical assets or systems not owned or leased by the person taking action or their client» [163].

⁷«A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization's systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner» [83].

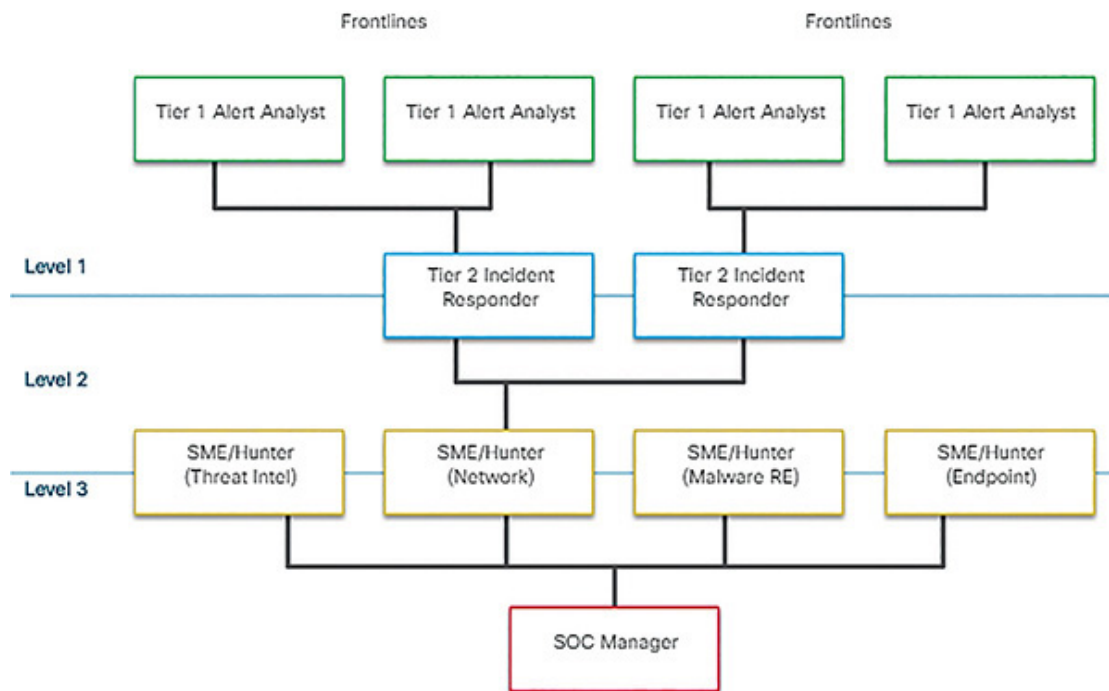


Figure 2.3. Roles of the People in a Security Operations Center [166]

- Threat and environment manipulation: analysing, interacting with and manipulating the threat in a controlled and customizable environment.

[96]

2.1.4 Intelligence

To consume intelligence someone must produce it before. If we want to be the ones to do so, first we have to understand that intelligence is not only a product but also and above all a process. To provide a definition of intelligence as-a-process, Lee adapts the one from the military field to the cybersecurity scope as: «the - cyclic - process of collecting data, exploiting it into information, and producing an assessment that satisfies a previously identified knowledge gap» 2.4. In this triptych, consisting of data, information, and assessment/intelligence product, much care is taken by the author, who refers to another of his articles for a better understanding [97]. Briefly:

- **Data** are those collected, in a raw format, from organization's or adversary's operational environment.
- **Information** is the result of processing one or more portions of raw data into a usable form.

- **Intelligence as-a-product** is the assessment, with a variable level of confidence, about information from different sources.

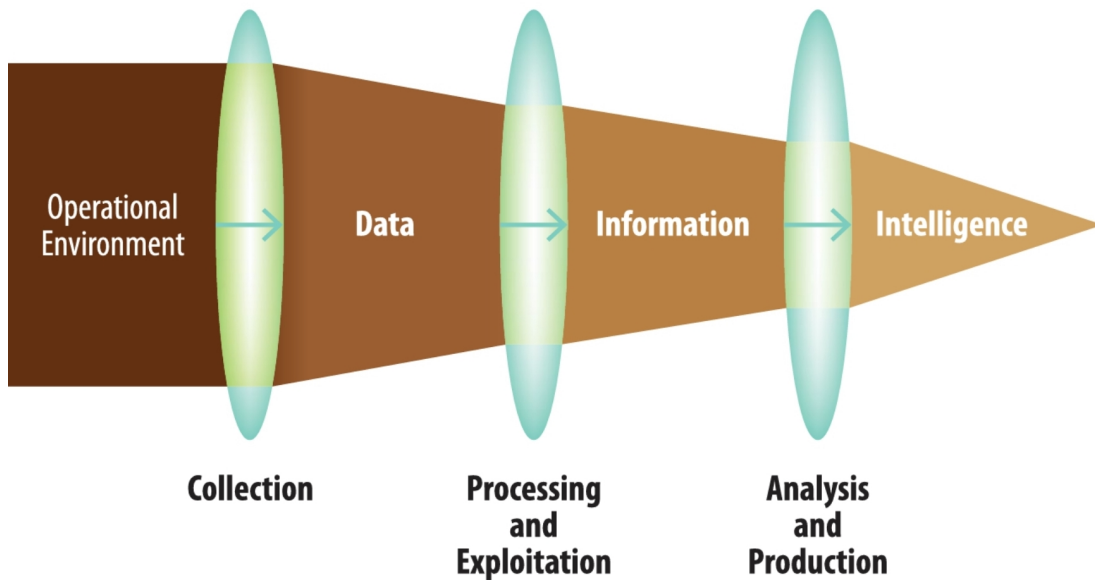


Figure 2.4. The Relationship of Data, Information, and Intelligence [98]

In the first two cases, the use of tools is possible if not essential, as the required interaction is reducible to a simple yes-no question⁸. In the last, however, it is impossible to know the answer with certainty, therefore only people with expertise in the field can perform the «analysis of competing hypotheses».

Finally, we provide a practical example of intelligence: an automated system collects logs⁹ (data) from laptops of an organization. In cascade, the software analyzes the logs and produces some alerts (information) relative to an identified malicious software. Then, a threat hunter associates that information with findings found on a criminal web market and with external analysis of the software's code. In the end, he generates a report (intelligence-product) in which he attributes that software to a specific gang of criminals with a high level of confidence. In this instance, intelligence has been produced, more precisely threat intelligence that, as we will see in the next chapter, «seeks to give defenders knowledge of the adversary, their actions within the defender's environment, and their capabilities as well as their tactics, techniques, and procedures».

⁸A yes-no or yes/no question is a type of question whose answer can only be affirmative or negative [32].

⁹«A record of the events occurring within an organization's systems and networks» [138].

2.1.5 Offense

The last-step of the scale is offense, intended as "offensive cyber operation", that is «direct action taken against the adversary outside friendly networks». Offense is the most expensive class, not only regarding the single action but also because it requires solid foundations, carved from all the previous categories. It is important to outline that such offense can only be carried out in compliance with national and international law. Consequently, offense can never be an act of aggression, but only an «act of cybersecurity [...], national policy or conflict». Moreover, the author states that offensive cyber operations cannot be undertaken by civilian organizations, nor they can be based on vengeance or retaliation in any way. In the end, Lee tries to provide a summary definition of these concepts: «legal countermeasures and counterstrike actions taken against an adversary outside of friendly systems for the purpose of self-defense».

A recent illustrative example is the disruption of Emotet botnet¹⁰ from global action of the international law enforcement agencies in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine [53]. This offense, coordinated by Europol and Eurojust, dismantled one of the largest existing botnet in 2021, redirecting in the end bots' communications to law-enforcement controlled servers, in order to submit a benign file that unthetered victim computers from the malicious network [149]. Two people associated with Emotet were finally arrested in Ukraine [151, 150].

¹⁰The word "botnet" is formed from the words "robot" and "network." Cyber criminals use special Trojan viruses to breach the security of several users' computers, take control of each computer, and organize all the infected machines into a network of "bots" that the criminal can remotely manage [130].

Chapter 3

Cyber Threat Intelligence

In this chapter, we will deal with intelligence, particularly threat intelligence. According to the National Institute of Standards and Technology, threat intelligence or cyber threat intelligence (CTI) is «threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.» [145] Gartner, instead, provides a more practical interpretation: «threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard.» [65] Thus, threat intelligence allows to understand specific behaviours of threat actors, in order to make ad-hoc decisions when attempting to prevent or detect attacks from them.

Depending on which type of knowledge is required, three types of CTI are defined: strategic, operational and tactical [179]. Each type reply to the different questions relative to the threat actor:

- **Who** is the target and **why** is targeted?
- **How** and **where** the attack is conducted?
- **What** are the evidence of the attack that took place?

In the next sub-chapters we’ll dig inside each one taking as reference Hive, a very famous case of Ransomware¹-as-a-Service (Raas) examined in a report by SentinelLabs [177].

3.1 CTI types

3.1.1 Strategic

This type of CTI allows to understand the who and why behind the threat actor. In particular, by analyzing the trends in organizations targeted (*who*) and motivations (*why*)

¹«Ransomware is a type of malicious attack where attackers encrypt an organization’s data and demand payment to restore access.», [147]

it is possible to build more effective defenses. Organizations can vary by sector, funds or even country, while motivations are usually financial or informational.

Concerning Hive gang, they are known to target healthcare (*who*) with ransomware attacks (*why*). This high-level information can help cyber executive figures, like Chief Information Security Officers (CISOs) or Chief Information Officers (CIOs) protecting such business, in their decision-making process.

3.1.2 Operational

The set of threat actor's tactics, techniques and procedures (TTPs) composes operational cyber threat intelligence. This trio is perfectly explained by the MITRE ATT&CK®, a «globally-accessible knowledge base of adversary tactics and techniques based on real-world observations» [115]. The framework² will be explored further on the paper. For now it's sufficient to map the words tactics, techniques and procedure to goals, methods and tools used in a compromise. This type of information helps the Security Operation Center (SOC), a team of security professionals involved in monitoring organizations' IT infrastructure [78], to know *how* and *where* the attack will place, simplifying and speeding up detection and mitigation processes.

Back to the example, Hive affiliates attacks life cycle is made of many TTPs. The first goal is to gaining an initial access (*tactic*) to one of the host in the targeted organization. This is done delivering fraudulent email with malicious attachments (*procedure*) through phishing³(*technique*) campaigns. Then the persistence on the machine is achieved by executing an illegitimate or legit remote control software inside the attachment. SentinelLabs reports that, in this phase, the most used tool by Hive ransomware gang is Cobalt Strike, a framework for post-exploitation activities. After dumping credentials from the infected host while discovering other possible victims, the last step is to deploy the Hive ransomware. In the end, all data of the organization are encrypted and a ransom note is deposited inside each folder.

3.1.3 Tactical

The lowest-level of CTI information is tactical information, that focuses on *what* exactly happened by extracting the so-called "indicators of compromise (IoCs)" from the host victims. Usually, IoCs are file hashes⁴, IP addresses and domain names. These evidences represent unique tracks left by the attacker that can be used to feed security technologies

²«A layered structure indicating what kind of programs can or should be built and how they would interrelate. Some computer system frameworks also include actual programs, specify programming interfaces, or offer programming tools for using the frameworks», [133]

³«A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.», [141]

⁴According to NIST, hashing is «the process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.», [134]

like Security Information and Event Management (SIEM), Intrusion Detection/Prevention Systems (IDS/IPS) and firewalls.

In the example are reported many hashes, related to Hive Ransomware samples, and the IP address used for remote communication. Even if the hashes of the malware samples are not very useful (because they are different for each compromise), blocking that IP address can be helpful from both detecting and proactive perspectives. Moreover, we will see that analyzing the infrastructure related to IP addresses like this, more proactive work can be done. For example, in this case we know from the report that the IP is associated with the first-cited tool Cobalt Strike. If we could block all IP addresses of this type it would empower a lot proactive defenses.

3.2 Threat Group Categories

Following the same order in which the different types of CTI have been described, we will begin to dig into the strategical one. For such purpose, we need to understand *who* is the threat actor and *why* it seeks to compromise IT systems.

Excluding script kiddies [192], there are four macro-categories of threat groups: hacktivism, cybercrime, nation-state⁵ and unknown [51].

3.2.1 Hacktivism

This type of threat is placed in a gray area, where compromise are in the name of defense of human rights and freedom speech. Other motivations can be political or about religious beliefs. Common attacks for such threat are DDoS⁶, website defacement and data exfiltration for public disclosure. A very famous example of hacktivism is Anonymous community. This decentralized group counts members from all over the world with various skill levels. Some of the last activities they carried out have been "cyber operations" against Russia, to support Ukraine in the war started on 24 Febraury 2023 [114].

3.2.2 Cybercrime

In a completely black area, instead, we find cybercrime, where there is a single purpose behind attacks: business. This category is the largest one in terms of members. Often, cybercriminals act as structured organizations with various levels of sophistication. Common activities typical about this threat are credentials stealing, demands of ransom and point-of-sale-systems compromise. These goals are usually achieved through malware deployment. Criminal organizations can buy, sell or rent malicious services accessing the

⁵The author refers to nation-state groups as "cyber espionage" groups. However, we found that espionage is not the only activity associated to these type of threat actors. Therefore, we renamed this category to the more general "nation-state" term.

⁶«DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.», [59]

Dark Web, «an encrypted portion of the internet that is not indexed by search engines and requires specific configuration or authorization to access» [191]. The previously covered case of Hive RaaS group falls in the cybercrime class.

3.2.3 Nation-state

The most dangerous adversaries belong to this category. They are groups sponsored by their nation, usually with the scope of obtain a geopolitical advance through stealing sensitive information like intellectual properties and internal communications. To refer to such groups, often it is used the term Advanced Persistent Threat, that is a «an adversary with sophisticated levels of expertise and significant resources» [126]. This type of operation targets a small number of predetermined victims with very sophisticated tactics and attack vectors, like spear-phishing⁷, custom-made malware, zero-day exploits⁸ and watering-hole attacks⁹. An example of nation-state sponsored cyber threat is the notorious Lazarus Group, associated with the Democratic People's Republic of Korea. On 29 March 2023, it has been discovered a large supply-chain attack¹⁰ against 3CX, an international software developer [1]. The company has been compromised in order to target cryptocurrency firms. Biggest cybersecurity organizations like CrowdStrike, Sophos and Kaspersky linked the operation to Lazarus group, well-known for both cyber espionage and cryptocurrency stealing, used by Pyongyang to fund its national priorities and objectives [175].

3.2.4 Unknown

It is not always clear and immediate to place an adversary in one of the three classes dealt with so far. When a threat cross multiple categories, we can only place it in an unknown bucket, keeping track of its behaviours and operations. This process is called "attribution", defined as «tracking, identifying and laying blame on the perpetrator of a cyberattack or other hacking exploit» [190]. One of the last documented case of APT attribution is related to GoldenJackal, a new group possessing an advanced custom-made malware toolset. Kaspersky began monitoring this threat since 2020, but it is remained largely unknown until May 2023, when the russian cybersecurity company successfully linked to it cyber espionage operations on diplomatic entities in Middle East and South Asia, ongoing since 2019 [89].

⁷«a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents.», [52]

⁸«A zero-day exploit is an exploit that takes advantage of a publicly disclosed or undisclosed vulnerability prior to vendor acknowledgment or patch release.», [200]

⁹In a watering hole attack, the attacker compromises a site likely to be visited by a particular target group, rather than attacking the target group directly., [135]

¹⁰«Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.», [144]

3.3 Cyber Threat Frameworks

To help with the attribution process, several frameworks have been developed. The most used ones, chronologically ordered, are:

- Cyber Kill Chain
- Mitre ATT&CK
- Unified Kill Chain

With different approaches and levels of detail, each of them proposes a model to enrich and classify information about threats in the cyberspace [180] [170]

3.3.1 Cyber Kill Chain

Developed by the American corporation Lockheed Martin in 2011, the Cyber Kill Chain (CKC) is the cybersecurity adaptation of the military's kill chain, a «step-by-step approach that identifies and stops enemy activity» [40]. The chain depicts the workflow from the attacker point of view, composed of seven phases 3.1:

- Reconnaissance: collecting information about target.
- Weaponization: preparing the malicious payloads¹¹ needed for the attack.
- Delivery: delivering the payloads.
- Exploitation: bypassing defenses to execute payloads.
- Installation: gaining persistent access to infected systems.
- Command and Control: controlling infected systems from attacker infrastructure.
- Actions on Objectives: achieving the desired goals.

3.3.2 MITRE ATT&CK

Since the Cyber Kill Chain was focused mostly on first stages of an attack, the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework was created in 2013 by the MITRE corporation, a MIT spin-off no-profit company [162] [196]. ATT&CK not only expand the number of phases with respect to Cyber Kill Chain, but provide a more realistic and precise mapping of attacker behaviours. This framework, indeed, is not a frozen theoretical model but an evolving research product about real attack cases, continuously fed by the cybersecurity community. After the high-level phases called "Tactics", the model drill down adversary's Techniques and Procedures, that is how tactic goals are

¹¹«in computer networking, a payload is the part of a data packet containing the transmitted data», [193]

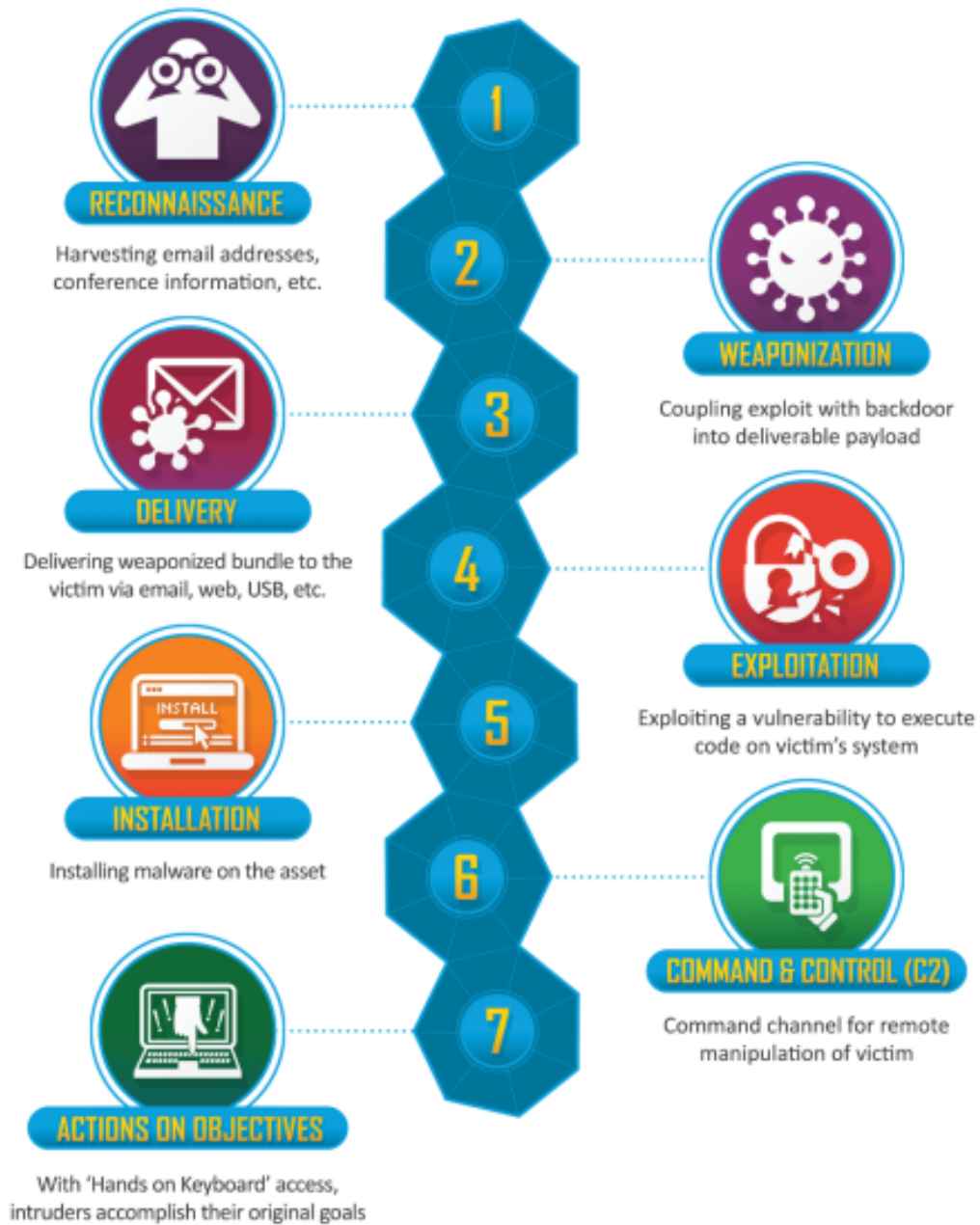


Figure 3.1. Lockheed Cyber Kill Chain [95]

achieved and a practical implementation of that [118]. To understand the power of this we can give a practical example: Blue Mockingbird, a real threat actor, has been seen to gain credential access (*tactic*) through dumping the memory of Local Security Authority

Subsystem Service¹²(*technique*) with Mimikatz tool (*procedure*) [120]. Proceeding in this way it is possible to maintain more organized information, speed up attribution process and build effective ad-hoc countermeasures. The framework counts a total of 14 tactics:

- Reconnaissance: collecting information about target.
- Resource development: preparing infrastructure for the attack.
- Initial access: gaining initial access to target system.
- Execution: executing malicious payload.
- Persistence: establishing persistent access.
- Privilege escalation: acquiring higher privileges.
- Credential access: stealing credential artifacts.
- Discovery: collecting information about systems.
- Lateral movement: jumping from one compromised system to another.
- Collection: selecting data for exfiltration.
- Command and control: communicating with compromised systems.
- Exfiltration: stealing data from the system.
- Impact: manipulating, interrupting or destroying systems and data.

3.3.3 Unified Kill Chain

In 2017, Paul Pols published in his master's thesis an attempt to reconcile the two frameworks discussed above: The Unified Kill Chain. This work unifies high-level phases of Cyber Kill Chain and strict time-agnostic ATT&CK classification to provide a model capable of defend to end-to-end cyberattacks, with more focus on APT. Analyzing attacks of FOX-IT's Red Team¹³ and Fancy Bear threat actor, Pols realised that eighteen steps were needed to track all possible behaviours from these different entities. Then, he subdivided the steps in three high-level phases of time: Initial Foothold, Network Propagation and Action on Objectives 3.2.

To effectively map all the adversary attack path, phases can be repeated and steps can be both repeated and used in different order. All the phases have a goal and they are linked by elements called "choke points", that is actions «that an attacker is forced through» to reach next phase. For example, the Initial Foothold goal is to compromise

¹²The LSAAS process stores users' and domain admin's credential, [111]

¹³«A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture», [142]

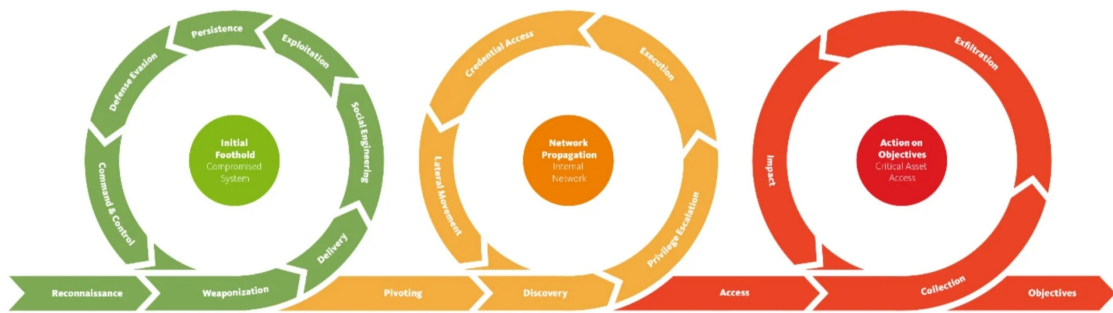


Figure 3.2. Unified Kill Chain [107]

the system, and only by "pivot"¹⁴ on it is possible to reach Network Propagation phase, spreading the compromise on the target environment. [156] The three phases with relative steps are:

- Initial Foothold: compromising system.
 - Reconnaissance: collecting information about target.
 - Weaponization: preparing infrastructure and payloads.
 - Delivery: delivering the payloads.
 - Social Engineering: tricking victim into opening payloads.
 - Exploitation: full payload execution.
 - Persistence: establishing persistent access.
 - Defense Evasion: bypassing security defenses.
 - Command and Control: communicating with compromised system.
- Network Propagation: spreading infection.
 - Discovery: collecting information about system.
 - Privilege Escalation: acquiring higher privileges.
 - Execution: executing arbitrary malicious code.
 - Credential Access: stealing credential artifacts.
 - Lateral Movement: jumping from one compromise system to another.
- Action on Objectives: achieving attack goals.
 - Collection: selecting data for exfiltration.
 - Exfiltration: stealing data from systems.
 - Impact: manipulating, interrupting or destroying systems and data.

¹⁴«Pivoting describes the act of tunneling traffic through one system to connect to other internal systems that may otherwise be inaccessible», [156]

Chapter 4

Command and Control

To get closer to our specific area of interest, we need to deepen the Command and Control, an attack stage present in all the previously examined frameworks. We believe that breaking the chain at this point can leave the initial-infected system largely intact, because it is not possible, as we will see, to perform interactive operations on it before this phase.

4.1 Definition

The expression Command and Control (C2 or C&C [64]) usually refers to the «management of personnel and resources in the context of a military mission». More generally, it denotes «the set of organizational and technical attributes and processes by which an enterprise marshals employs human, physical, and information resources to solve problems and accomplish missions». [205] In the cybersecurity field, «Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network.» [116]

4.2 Topologies and techniques

There are three main network topologies that describe how the victim hosts can communicate with adversary infrastructure: centralized, decentralized and random.

The first is the earliest and most common type of approach. Basically, it consists of a client-server communication between infected host and C2 server. Centralised topology is the easiest to build up but lacks of scalability and failure-resistance to focused attack.

The opposite pros and cons are achieved by decentralised network type. This is a peer-to-peer¹ approach in which infected and adversary hosts are at the same level of

¹«In a peer-to-peer (P2P) network, each computer acts as both a server and a client—supplying and receiving files—with bandwidth and processing distributed among all members of the network», [15]

hierarchy. Attacker can just upload commands to one or more peer and then implicit flooding mechanism will spread them across the entire network of compromised hosts.

Sometimes, adversaries can be very creative in using channels completely different from this classic duo. For example, it has been observed the use of licit web services and famous social network like Yahoo and Twitter for hosting C2 communications. [64]

In each topology it is possible to use multiple techniques for establish the connection with the adversary infrastructure. The Mitre ATT&CK framework describes sixteen different Command and Control techniques:

- Application Layer Protocol: communications are blended with existing application layer traffic.
- Communication Through Removable Media: commands transfer to network-disconnected system using removable media.
- Data Encoding: encoding² communications to evade detection.
- Data Obfuscation: masking C2 traffic with junk data or vectors.
- Dynamic Resolution: selecting dynamically C2 to which connect.
- Encrypted Channel: encrypting C2 communications.
- Fallback Channels: increasing reliability of communications adding extra channels.
- Ingress Tool Transfer: downloading additional tools from C2 for post-compromise activities.
- Multi-Stage Channels: communications go through multiple C2s to evade defections.
- Non-Application Layer Protocol: using an OSI³ non-application layer protocol.
- Non-standard Port: using application protocols over non-default ports.
- Protocol Tunneling: hiding malicious traffic by encapsulating existing protocol layers into extra layers.
- Proxy: avoiding direct connection between infected system and C2 to avoid detection.
- Remote Access Software: using of licit remote management software.
- Traffic Signaling: using data as "watchwords" to enable ports on adversary infrastructure and thus allowing communications.
- Web Service: using of licit services like website or social media.

²Note that encoding data means transform plaintext from some form to another. Unlike encryption, it doesn't provide any form of confidentiality. [82]

³«The open systems interconnection (OSI) model [...] can be seen as a universal language for computer networking. It is based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last», [37]

4.3 Frameworks

From Unified Kill Chain chapter, we know that it was built upon analysis of attacks from FOX-IT's Red Team and Fancy Bear. While the latter is a real threat actor with malicious intents, the first is a red team, that is a «group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture». [142] To effectively simulate adversaries with reasonable time and flexibility, many frameworks have been built. Typically, a C2 framework consists of a platform designed to control network of compromised systems. The platform has two components: a server component installed on adversary infrastructure and a client component, called "agent" or "beacon" or even "implant", installed in the victim system. [13] [185]

As reported by C2 Matrix, a project created by SANS author and instructor Jorge Orchilles, «It is the golden age of Command and Control (C2) frameworks». [20] [169] The goal of C2 Matrix is to help red teamers in the choice of best C2 framework for their needs. At the time of writing the project is tracking 132 different Command and Control products, of which 12 are proprietary, 119 are open-source⁴ and 1 is unknown. [21] Even if these frameworks are created for help organizations in strengthen their cybersecurity posture, they are extensively abused by threat actors for their ease of use. [24]

In the next sub-chapters we will explore the most popular Command and Control frameworks used to date.

4.3.1 Metasploit

Originally conceived as exploit creation suite by H D Moore⁵, Metasploit was released for the first time in 2003. After further development and significant appreciation from the cybersecurity community, the project was acquired by Rapid7, a company leader in the vulnerability-scanning field. [90] Today the framework is available both in proprietary and open-source version. [161] Through the *msfconsole* 4.1, the Metasploit terminal-styled core, it is possible to conduct all the needed operations for a penetration test⁶, from information gathering to Command and Control. This phase, in particular, is lead by deploying an agent called "Metpreter", that allows remote command execution. Finally, it is possible to link the console to *Armitage*, a quite intuitive GUI⁷ created by Raphael Mudge in 2010, that enables collaborative work and fast visualization of the pentest

⁴«The term “open source software” means software for which the human-readable source code is available for use, study, re-use, modification, enhancement, and re-distribution by the users of such software», [204]

⁵This is not an error, H and D are actually his first and middle name. [198]

⁶A penetration test or pentest is «a method of testing where testers target individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited to compromise the application, its data, or its environment resources.», [140]

⁷«Graphical User Interface (GUI), a computer program that enables a person to communicate with a computer through the use of symbols, visual metaphors, and pointing devices» [16]

environment. [176]

```

dBBBBBBb dBBBP dBBBBBBP dBBBBBBb .
' dB' BBP
dB'dB'dB' dBBP dB' dB' BB
dB'dB'dB' dB' dB' dB' BB
dB'dB'dB' dBBBBP dB' dBBBBBBB

dBBBBBP dBBBBBBb dB' dB' dBBBBBP dB' dBBBBBBP
| dB' dB' dB'.BP
--o-- dBP dBBBB' dB' dB'.BP dBP dBP
| dBP dBP dBP dB'.BP dBP dBP
| dBBBBP dBP dBBBBP dBBBBP dBP dBP

o
To boldly go where no
shell has gone before

=[ metasploit v4.17.3-dev ]
+ -- --[ 1795 exploits - 1019 auxiliary - 310 post ]
+ -- --[ 538 payloads - 41 encoders - 10 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >

```

Figure 4.1. Metasploit msfconsole [105]

4.3.2 Cobalt Strike

Cobalt Strike is the most used Command and Control framework at the time of writing [165]. First released in 2012 by the Armitage creator Raphael Mudge, the framework consisted of Metasploit and Armitage as base plus improvements like spear-phishing and reporting capabilities, in order to cover a full-attack simulation path [121]. In 2020, the project was acquired by Fortra cybersecurity company, with Mudge leading the development [62]. Today Cobalt Strike is a big platform 4.2 with plenty of powerful and unique functionalities, like dynamically changing beacon characteristics with "Malleable C2 Profile"⁸ and automated creation of "team servers"⁹ [60]. Cobalt Strike is also very popular among criminals. For example, Conti ransomware group invested \$60000 in acquiring a valid license for Cobalt Strike. [92] Moreover, 34 cracked versions have been found in the wild¹⁰. [74] To stop this trend, Microsoft, Fortra and Health Information Sharing and Analysis Center are «taking technical and legal action to disrupt cracked, legacy copies

⁸«This is domain specific language for user-defined storage-based covert communication», [122]

⁹«The server, referred to as the team server, is the controller for the Beacon payload and the host for Cobalt Strike's social engineering features. The team server also stores data collected by Cobalt Strike and it manages logging.», [61]

¹⁰«A term defining the scope and impact of malicious software. In-the-wild malware is active and can be found on devices belonging to ordinary users». [87]

of Cobalt Strikes and abused Microsoft software, which have been used by cybercriminals to distribute malware, including ransomware». [109]

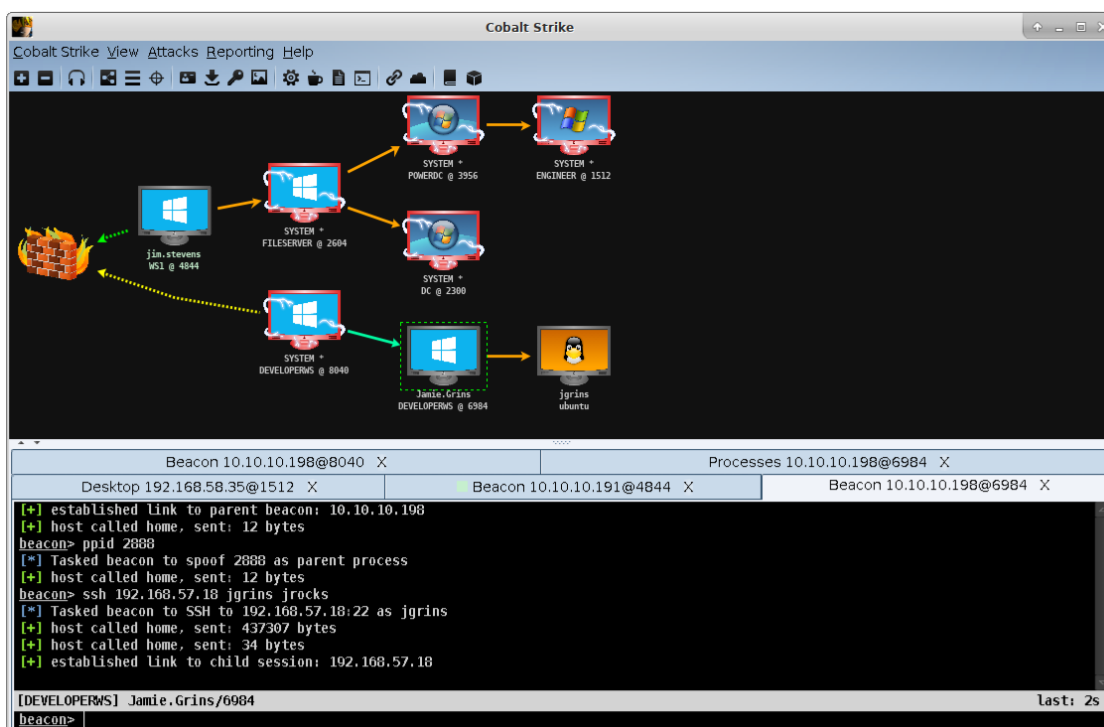


Figure 4.2. Cobalt Strike GUI [195]

4.3.3 Sliver

Sliver was released on GitHub¹¹ in 2019 by the Bishop Fox offensive security¹² company, with the aim of becoming an open-source alternative to Cobalt Strike. [12] [69] It has succeeded so well in his intention that even APT groups largely started to use it [42]. Even if the framework has some advantages over Cobalt Strike like more built-in modules and sort of "controlled execution"¹³, it has quite the same capabilities, with the except of a GUI 4.3. The most significant reason behind large adoption of Sliver by cybercriminals is that, compared to Cobalt Strike, it has been spotted a lot less in the wild, thus they can take advantage of the gap in detection coverage [45].

¹¹ «GitHub is a code hosting platform for version control and collaboration», [69]

¹² «Offensive security is a proactive and adversarial approach to protecting computer systems, networks and individuals from attacks - in contrast to "defensive security" that - focuses on reactive measures, such as patching software and finding and fixing system vulnerabilities», [188]

¹³ «Sliver can limit execution to specific time frames, hosts, domain-joined machines, or users» [45]

```

kali@kali:~/Desktop$ sudo ./sliver-client
[*] Connecting to 192.168.0.21:31337 ...
[*] vk9ops has joined the game

sliver >

```



```

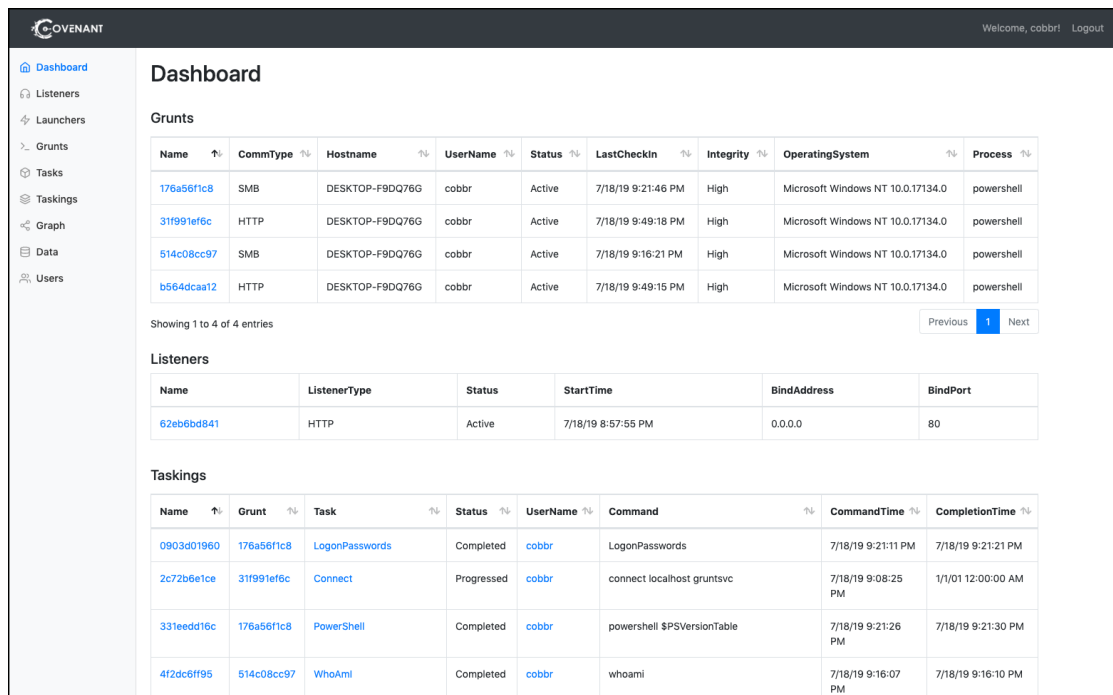
All hackers gain renown
[*] Server v1.0.6 - 2295a995f91f0ca733170bf6bee651ea60c62d0e
[*] Welcome to the sliver shell, please type 'help' for options

sliver >

```

Figure 4.3. Sliver console [206]

4.3.4 Covenant



Dashboard

Welcome, cobbr! Logout

Grunts

Name	CommType	Hostname	UserName	Status	LastCheckIn	Integrity	OperatingSystem	Process
176a56f1c8	SMB	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:21:46 PM	High	Microsoft Windows NT 10.0.17134.0	powershell
31f991ef6c	HTTP	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:49:18 PM	High	Microsoft Windows NT 10.0.17134.0	powershell
514c08cc97	SMB	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:16:21 PM	High	Microsoft Windows NT 10.0.17134.0	powershell
b564dcaa12	HTTP	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:49:15 PM	High	Microsoft Windows NT 10.0.17134.0	powershell

Showing 1 to 4 of 4 entries

Listeners

Name	ListenerType	Status	StartTime	BindAddress	BindPort
62eb6bd841	HTTP	Active	7/18/19 8:57:55 PM	0.0.0.0	80

Taskings

Name	Grunt	Task	Status	UserName	Command	CommandTime	CompletionTime
0903d01960	176a56f1c8	LogonPasswords	Completed	cobbr	LogonPasswords	7/18/19 9:21:11 PM	7/18/19 9:21:21 PM
2c72b6e1ce	31f991ef6c	Connect	Progressed	cobbr	connect localhost gruntsvc	7/18/19 9:08:25 PM	1/1/01 12:00:00 AM
331eedd16c	176a56f1c8	PowerShell	Completed	cobbr	powershell \$PSVersionTable	7/18/19 9:21:26 PM	7/18/19 9:21:30 PM
4f2dc6ff95	514c08cc97	WhoAmI	Completed	cobbr	whoami	7/18/19 9:16:07 PM	7/18/19 9:16:10 PM

Figure 4.4. Covenant Dashboard [39]

Released from Ryan Cobb in 2019, Covenant is an open-source valid alternative to others emblazoned C2 frameworks. Covenant’s architecture has three main component: *Covenant* as server, *Elite* as client for operators and lastly *Grunt* as implant to install on target systems. It is completely written in C# using the Microsoft .NET¹⁴ framework, making it cross-platform compatible¹⁵, natively docker¹⁶ supported and thus a great choice for collaborative work through his dashboard 4.4 [39]. At the time of writing, it seems that it is mainly used by red teamer, as there are no or weak evidences of use by criminals and APT groups [194].

4.3.5 Brute Ratel

Sold as «The most advanced Red Team & Adversary Simulation Software in the current C2 Market» 4.5, Brute Ratel was created by Chetan Nayak in 2020. Nayak held senior positions in big cybersecurity firms like Mandiant and CrowdStrike [46, 47]. Thanks to this experience, Brute Ratel has become «uniquely dangerous in that it was specifically designed to avoid detection by endpoint detection and response (EDR) and antivirus (AV) capabilities» [153]. This characteristic makes it very appealing to cybercriminals. In fact, after Nayak reported that Brute Ratel was leaked and cracked [203], it has been spotted in the wild as valuable piece in the armoury of Black Cat, Black Basta and LAPSUS\$ ransomware groups and APT 29 [181, 112, 201, 153].

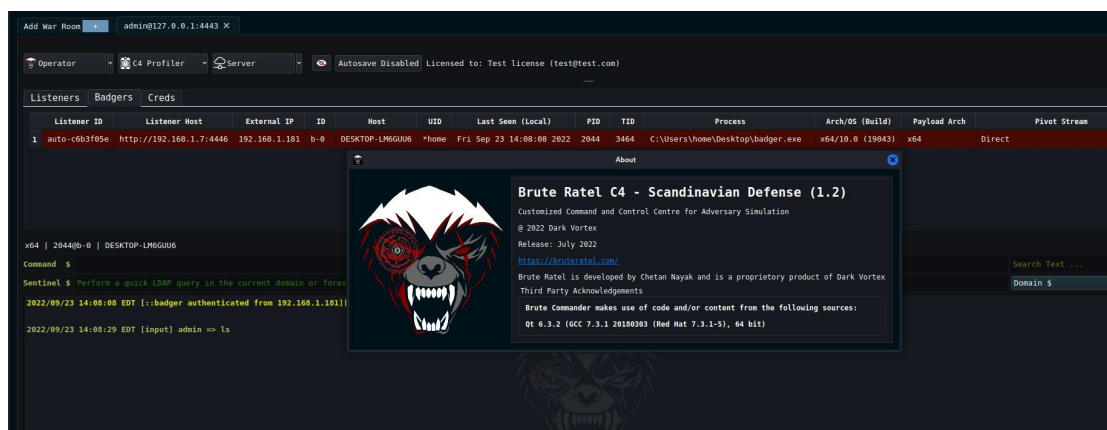


Figure 4.5. Brute Ratel GUI [18]

¹⁴ «.NET is a free, cross-platform, open source developer platform for building many different types of applications». It supports C#, F#, and Visual Basic languages. [110]

¹⁵ «able to be used with different types of computer systems». [23]

¹⁶ «It is an open platform can be used for building, distributing, and running applications in a portable, lightweight runtime and packaging tool». [159]

4.3.6 Havoc

Havoc is one of the latest additions to the Command and Control scene. Realised by Paul Ungur, also known as C5pider, in September 2022 [68], Havoc rapidly become an «alternative to paid options such as Cobalt Strike and Brute Ratel» [14]. This open-source framework 4.6 can boast advanced evasion techniques, making it capable of bypassing last version of Windows Defender. Despite its youthfulness, Havoc has already been used in recent malicious campaigns [210, 168].

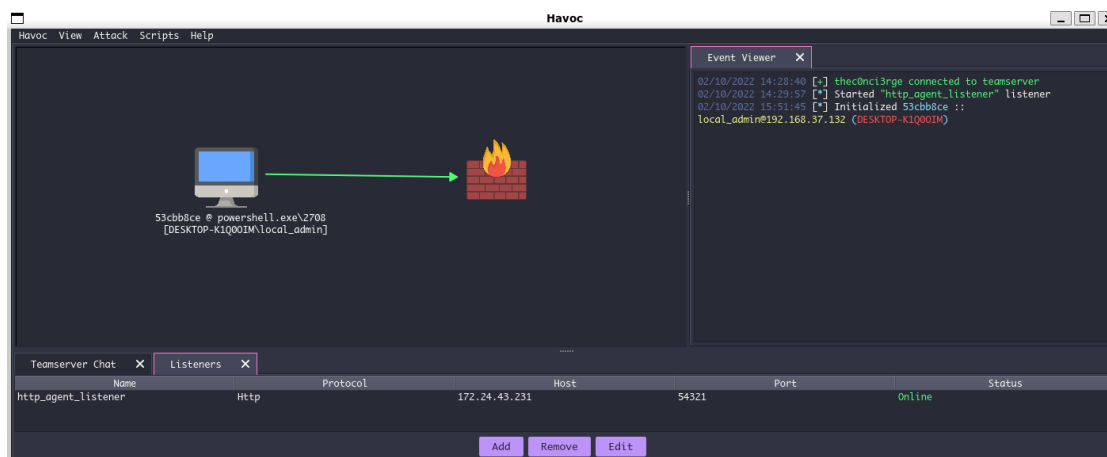


Figure 4.6. Havoc GUI [154]

4.4 Malware

Command and Control technique isn't a prerogative of penetration testing frameworks. Also malicious software called "malware" [160] make extensive use of this. The National Institute of Standards and Technology defines malware as «software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system» [139].

A malware can belong to one or multiple classes; the most common are:

- Virus: attached to other files, it can spread infection across multiple systems causing performance degradation and denial of service.
- Worms: independent malicious piece of code, it can replicate itself through several devices and emails.
- Trojan Horse: usually downloaded by users confusing it with licit software, it can steal and disrupt data.
- Rootkit: can cheat antivirus and hide other malware by taking control of the operating system.

- Spyware: used to secretly collect user’s activities and personal information.
- Adware: get financial benefit by playing advertisement without user permission.
- Bot: add the infected system remote control of the infected system to carry out subsequently malicious activities through it.
- Keylogger: record all key strokes.
- Ransomware: encrypt data to subsequently ask a ransom for decrypting it.

[186]

In the next sections we will report some examples of active malware, selected on the basis of the greatest affinity with the purpose of this research work.

4.4.1 ISFB

ISFB is a trojan created between 2011 and 2012. It is often confused with Gozi and Ursnif malware because it born from a leaked version of Gozi, born in turn from the ashes of Ursnif. [106] ISFB is usually delivered as attachment of a phishing email and it targets mostly financial institution [17]. Once installed on the machine, ISFB collects all the information related to banking accounts like credentials, balances, transfers, authentication mechanisms and phone number [36]. In practice, it acts as an info-stealer, that is subtype of spyware that «can harvest keystrokes, screenshots, network activity, and other information from systems» [102]. Italy is one of the most targeted state, with several phishing campaigns that convey the ISFB banking trojan starting in 2020 until May 2023 [2, 3, 4, 5, 8, 6, 7].

4.4.2 QakBot

Active since 2007, QakBot, also know as Qbot, is another informational stealer focused on financial data [100]. From 2020 it appeared in the in the list of most popular malware [103], fluctuating in the top positions from November 2022 to April 2023 [27, 26, 30, 29, 31, 28]. QakBot operators target a wide variety of fields, from transports to education, with more prevalence on healthcare and manufacturer [33]. Other than as info-stealer, the malware has been used as dropper¹⁷ for ransomware like ProLock and BlackBasta [209, 41].

4.4.3 Quasar

Released on GitHub by the German developer “MaxXor” in 2014 , Quasar is the perfect example of Remote Access Trojan [73]. RAT is a «class of malware, which is developed constantly with new methods, enabling the attacker to connect to the victim’s system remotely and interactively» [184]. Quasar, in particular, today offers all the tools needed

¹⁷«A dropper, or Trojan downloader, is a type of malware that installs other malware on the affected system. The other malware is part of the same executable, which is usually in compressed form». [103]

for Command and Control operations, like remote desktop, registry editor and keylogger. Over the years, the RAT has been customized by APT groups from all over the world to adapt their specific needs, as for Chinese APT10, North Korean Kimsuky, Indian Patchwork and Palestinian Gaza. [158, 119]

4.4.4 Pupy

Pupy is a RAT developed since 2016 as open-source project by "n1nj4sec", pseudonym for the bug bounty¹⁸ hunter Nicolas Verdier [72, 202]. Thanks to docker compatibility, Pupy is cross-platform and can run on Windows, Linux-based OSs, macOS and even Android. Even if it was designed for red-teaming exercising, it become broadly abused by cybercriminals, especially by Iranian APT groups like Elfin, Cobalt Gipsy and Charming Kitten [164, 81].

4.4.5 SocGholish

Active since 2018, SocGholish is a famous example of loader (or downloader) [157, 199, 99], that is a malware that «grab malicious executables or payloads from an attacker-controlled server. [...] Unlike their cousins, the dropper, loaders don't come pre-installed with payloads, and instead they download them from a remote URL» [54]. Also referred to as FAKEUPDATES, this malware is known for providing an initial access to the target system. With a “drive-by” download style, it is delivered after loading malicious JavaScript payload, previously injected into compromised websites. Depending upon the profile of the infected system, SocGholish has been seen to load different second-stage malware like ransomware (WastedLocker, Hive, LockBit) and RATs.

4.4.6 TrueBot

Discovered for the first time in 2017 by Kaspersky's researchers [88], Truebot is a «first-stage downloader module that can collect system information and take screenshots, developed and attributed to the Silence - russian speaking - hacking group» [34, 101]. Starting in August 2022, there were an increase of infections by TrueBot loader since August 2022, with the most recent occurred in June 2023. [35, 207]. According to Cisco Talos Intelligence, currently there are two different botnets related to the malware: a worldwide one and a mostly US one. The first has been created by exploiting a vulnerability into a Netwrix software¹⁹ and through USB drives infected with Raspberry Robin worm [113]. The last one, created in November, uses an as yet unknown attack vector. Due to the fact that TrueBot delivered FlawedGrace RAT [117] and Clop ransomware as last-stage

¹⁸«A method of compensating individuals for reporting software errors, flaws, or faults (“bugs”) that might allow for security exploitation or vulnerabilities». [131]

¹⁹The software concerned is Netwrix Auditor, an «IT auditing software used to track assets within an organization.» The vulnerability affects all version prior to 10.5, allowing an attacker to execute arbitrary code with presumably high privileges. [11]

payloads, both the activities have been linked to EvilCorp, a financially motivated Russian group that notoriously deploys these malware. However, no strong evidences exist at the time of writing.

Chapter 5

C2 Fingerprinting

Usually, to detect in the wild these C2 frameworks and malware, hashes of beacons and malware's samples are generated and shared in the form of IoCs. When one of these indicators is seen on a system, whether by passive or active defense elements, the associated file is blocked and no further communications can take place. The problem with this approach is that both beacons and malware are polymorphously created, that is their source code is constantly changed while «maintain(ing) the same general functionality» [10]. In this manner, they cannot be detected by signature-based detection systems, because the hash result differs each time. To overcome this limitation, both code and behavioural analysis are performed on the malicious instance [10, 171].

Another way to solve the polymorphic problem is through the emerging technique core of this paper: C2 fingerprinting.

5.1 Definition

Starting from the term *fingerprinting* (in networking field), a broad definition is given in the RFC¹ 6973: «the process of an observer or attacker uniquely identifying (with a sufficiently high probability) a device or application instance based on multiple information elements communicated to the observer or attacker» [38]. In this case, it would be more accurate to talk about network protocol system fingerprinting, as exhaustively explained by Ohio State University researchers Shu and Lee. For the sake of completeness of information, we report here an extract of their "Network Protocol System Fingerprinting - A Formal Approach":

«Network protocol system fingerprinting refers to the process of identifying specific features of a network protocol implementation by analyzing its input/output behaviors. Usually these identifiable features may reveal specific protocol versions, vendor information, and configurable parameters, and can be stored as the “fingerprint” for matching and

¹«A Request For Comments is a formal standards-track document developed in working groups within the Internet Engineering Task Force (IETF)» [143].

comparison. While the original purpose was to identify remotely what Operating System is running on the target host, the applications of fingerprinting techniques nowadays cover a much wider range of areas. [...] The presence of protocol system fingerprint is due to a basic fact that most network protocols are not specified completely and deterministically. As a result, there is no unique conforming implementation. This nondeterminism in protocol specification can be from explicit statement of optional features and designer's choices, or from the unspecified behaviors under certain circumstances. In the latter case the implementer has the freedom to decide the response to an unspecified input, which, for instance, could possibly be an error message or no response at all. Given different valid implementations, the goal of fingerprinting is to identify one of them by analyzing the input/output behaviors of an implementation, which is often modeled by a "black-box" [178].

There are three main classes that define how the fingerprinting of the target is conducted:

- passive: observing only network traffic.
- semi-passive: interacting with existing communication.
- active: initiating communication.

[91]

Given the scope of our research and the high level of "volatility" of servers used for Command and Control purposes, we will take into account only the last one. Moreover, we can make further distinctions within the class of active fingerprinting by recalling the terms scanning and probing. Often used as synonyms due to the overlapping techniques used, scanning concerns identifying the presence of active hosts and ports, while probing «involves the use of crafted protocol requests for the purposes of eliciting responses that can provide more detailed information» [124].

Lastly, we try to provide here a definition of C2 fingerprinting: identifying, with sufficiently high probability, unique clusters² of Command and Control servers, on the basis of network protocol information collected through scanning and probing activities.

5.2 State Of The Art

It is not new applying the network protocol system fingerprinting technique to detection of Command and Control communication. In fact, «a wide range of approaches have been studied and multiple different systems have been proposed», due to the fact that «C&C channels are often the weakest link in the operation of advanced malware» [93]. However, these approaches consider only implementations as passive defense measures. In practice, only traffic generated by malicious samples in local protected environment and sandboxes is subjected to fingerprinting.

²«A group of things of the same type that grow or appear close together» [49].

In recent years, researchers started to apply this technique in large scale to the outside world of their organisation. [104, 124, 182]. Relying on scanning and probing tools like Zmap, Masscan and Unicornscanner [123], indeed, it is possible to census the entire Internet in reasonable time. "Knock-knocking" each host, these tools collect characteristics like DNS³ names, TLS certificates⁴ and exposed services. Next, we can find all hosts with one or more common characteristics by searching on this data. The method of finding the presence of a C2 server is the same as for fingerprinting network protocol systems in a local environment, we only have changed the range of investigation. Moreover, we are not obliged to setting up a mass scanning and probing process on premise, as several Internet applications have been developed for this purpose. Some global security companies and research institutions, in fact, provide free and paid search engine services for cyberspace [94]. They not only collect raw data about Internet hosts, but also process it into usable information. On the basis of these information, we can looking for specific group of results, as we would do for a simple web search. For example, the picture 5.1

The screenshot shows the Censys search interface. At the top, there is a search bar with the query: `services.software.product="nginx" and services.software.version="1.9.12" and services.port="80"`. Below the search bar, the results are displayed in a list format. The first result is for IP address **101.200.238.166**, which is associated with ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd. (37963) in Beijing, China. It lists several services: 22/SSH, 80/HTTP, 443/HTTP, 2101/HTTP, and 8080/HTTP. The second result is for IP address **47.115.85.177**, associated with ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd. (37963) in Guangdong, China, listing 22/SSH, 80/HTTP, and 443/HTTP. The third result is for IP address **34.220.14.142** (ec2-34-220-14-142.us-west-2.compute.amazonaws.com), associated with AMAZON-02 (16509) in Oregon, United States, listing 22/SSH, 80/HTTP, and 123/NTP. The fourth result is for IP address **116.198.52.96**, associated with CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation (23724) in Beijing, China, listing 80/HTTP, 8060/HTTP, and 8081/HTTP. On the left side, there are 'Host Filters' and 'Autonomous System' sections with various labels and counts.

Figure 5.1. Censys Search

³The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or any resource connected to the Internet or a private network. [...] Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for the purpose of locating and identifying computer services and devices with the underlying network protocols. [85]

⁴«TLS server certificates serve as machine identities that enable clients to authenticate servers via cryptographic means» [9, 50]

shows how we can retrieve all hosts with a specific version of the nginx⁵ web server running on port 80.

It is our opinion that, even if other solutions exist (like the on premise one), using these search engine is actually the fastest way to obtain consistent results in C2 clustering.

Among the most well-known cyberspace search engine, that is Shodan, Censys, BinaryEdge, ZoomEye and Fofa, we choose Censys for the fastest scanning frequency and uniformity of data [94]. These characteristics are the most valuable for C2 fingerprinting purposes, because we have found that servers used by cybercriminals have very limited lifespan, in order to avoid detections.

5.3 A practical example

Here we give a full example of the current state of the art about C2 fingerprinting, well represented in the picture 5.2 below.



Figure 5.2. C2 fingerprinting state-of-the-art flow [108]

The example’s subject will be the Cobalt Strike framework, for which it is made the hypothesis that no past information is available other than IoCs, as it would be for a new unknown threat. There is no well-know or globally-recognised pattern to follow for this activity, thus the following is our interpretation of C2 fingerprinting, that we have divided in eighth phases 5.3.



Figure 5.3. C2 fingerprinting process

⁵«Nginx [engine x] is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server, originally written by Igor Sysoev» [125].

5.3.1 Collecting

The first step is to start collecting all Open Source Intelligence (OSINT)⁶ information available for the threat, with particular focus on indicators of compromise.

As stated on the hypothesis, we only found that a new menace has been discovered while being used in some malware campaigns. After further investigations, we found some hints that it could be a leaked version of the famous Command and Control framework Cobalt Strike, used for licit red teaming activities. Some IOC have been submitted to publicly available websites like Virus Total⁷ and ThreatFox⁸, and also posted on Twitter by researchers. We will take the ones relative to IP addresses and TCP/UDP ports⁹ to advance to the next step.

5.3.2 Cleaning

To make sure that our hunt get off on the right foot, we must be sufficiently sure that the IP addresses taken as starting base are reliable. Usually, indeed, these IoCs are extracted by analyzing all communications occurring in a sandbox while the malicious software is running, without further checks on the validity. In particular, we observed that malware and beacons contact several licit IP addresses together with the malicious one, in order to avoid this type of automated processing. Therefore, we had to "clean" the IoCs by performing one-by-one checks through Virus Total, Whois¹⁰ lookup servers and OSINT, in order to discard unrelated IP addresses. Doing some intelligence work in this phase is crucial, because we can have a mismatch even with a red flag by Virus Total, as IP addresses can be reassigned in quite short time to different malicious infrastructure or to completely different licit service.

5.3.3 Comparing

At this point we put each IP address on Censys. If the search engine recently scanned these addresses, it will show a list of field-value pairs containing information like geolocation, Internet Service Provider, ports open and services banner¹¹. We have to find by-hand similarities between these values, with particular focus on services related to ports noted

⁶ «Publicly available information that has been discovered, determined to be of intelligence value, and disseminated by a member of the IC (Intelligence Community)» [208].

⁷ «VirusTotal is a popular service that scans malicious files and web URLs. [...] VirusTotal works with 68 third-party security vendors» [155].

⁸ «A free platform operated by abuse.ch that collects and shares indicators of compromise» [86].

⁹ «a destination port number generally identifies a service listening on the destination host, and a source port usually identifies the port number on the source host that the destination host should reply to» [146]

¹⁰ «WHOIS is a TCP-based transaction-oriented query/response protocol that is widely used to provide information services to Internet users» [44]

¹¹ «Application type and version that is transmitted by a remote port when a connection is initiated» [129].

on each IoC, discarding the addresses that don't match in any way with the others. This step can take us a lot of time, but we have to carefully annotate all alike pairs and generic anomalies, even the ones that seem useless to us. Obviously, processing by-hand hundreds of IP is not feasible in reasonable time, thus we recommend to get only the most relevant ones.

5.3.4 Pivoting

This is the most tricky step, as we have to find which field-value pairs are representative for the Cobalt Strike cluster. From OSINT we have learnt that Cobalt Strike is the most used framework for C2 both for licit and illicit purposes, so we expect to retrieve a decent amount of results. With an iterative process, we search each item on the previously generated list, paying attention to pairs that return a number of results less than or equal to the one expected. In the case of Cobalt Strike, we expect around one thousand of hosts.

5.3.5 Refining

After further reducing the numbers of eligible fields and values, we need to refine the results by removing false positives as much as possible. For this purpose, we have to find other pairs from the list that, chained with the previous through a boolean AND, still produce results in the same order of magnitude but without false positives. To determine whether an IP address is a true or false positive with a certain level of confidence, it is mandatory to do some intelligence work, always with the help of OSINT tools like VirusTotal and Whois servers.

5.3.6 Fingerprinting

In the end, we have to produce one or more "fingerprintings", or better-known "signatures", that identify a cluster. These signatures are composed by the most-valuable pairs chained together through boolean operators. It is not required that clusters identified by different signatures don't overlap, as it is likely that they share multiple common characteristics. We can adopt two major approaches in writing signatures: putting all together or make a signature for each relevant field-value pair. If we choose the first approach, however, we must pay attention to not exceed the limit of characters supported by the search engine. Moreover, if the engine can't process the query in reasonable time no results will be produced, thus writing long complex query is not recommended.

5.3.7 Hunting

Once the signatures have been generated, this step requires planning when manually querying the cyberspace search engine and where to store the list of results. Although it might be quite obvious, underestimating this aspect could cause practical difficulties as the number of C2 families we are monitoring increases.

5.3.8 Re-checking

This optional step consists in performing further checks on results of our signatures. In some cases, indeed, it is possible to know for sure if a service exposed by an IP address it is actually related to a C2 framework. When the infrastructure target doesn't implement filters on incoming communications, it is possible to code some tools that mimic beacon or malware behaviour, in order to interact with the C2 server and retrieving a tangible evidence of his presence. For Cobalt Strike, several scripts have been developed to download the beacon configuration [71, 67, 66, 70].

Chapter 6

A new approach

In this chapter is presented the approach to C2 fingerprinting designe in during this Thesis work.

6.1 Project Questions

On the base of built knowledge and practice done, here we propose a new way to approach the C2 fingerprinting task.

6.1.1 Why

We noticed huge time effort in every phase of the C2 fingerprinting workflow and several other limitations like:

- Collecting: storing IoCs can be a bit complicated without a well-established database.
- Cleaning: next steps rely too much on cleaning performance.
- Comparing: impossibility to compare by-hand dozens of fields about hundreds of IP.
- Pivoting: high probability to lose some valuable relations.
- Refining: high probability to stale on the same AND fields through different C2 family investigation.
- Fingerprinting: high probability to lose some true positives of the cluster.

Furthermore, the absence of rigorousness in notation, workflow and support tools used, increase unnecessarily the time needed to accomplish the entire process. Finally, we recall that timing is essential in C2 fingerprinting, as active IoCs related to criminal activities are usually only available for a limited period and new malware and frameworks are developed with high frequency.

6.1.2 What

To overcome such limitations, we rethought the entire C2 fingerprinting process, separating theory from implementation. In particular, to reduce time required, to increase reliability and accuracy and to store results for intelligence scope, each step of the process has been designed to be automatable. Instead of taking only a subset of IoCs for starting the investigation, now they are all processed and stored at fixed interval of time. All the human interaction, required for comparing field-value pairs through the cyberspace search engine, has been replaced by a simple but effective mathematical formula and by a clustering system. Then, we changed the way signatures are produced, going from a boolean to a modular approach. Instead of having few signatures composed by boolean combination of some selected pairs, now several signatures are produced for each valuable pair, finding more in-depth relations and increasing the reliability of matches in the hunting phase. Lastly, each step of the process is supported by the developed nomenclature, which can also serves as basis for future work on the subject.

6.1.3 Who

Every cybersecurity environment, even with low maturity levels, can benefit from importing threat information generated with this approach, as it produce ready-to-use results without configuration needed. It can be also used to feed passive defense components like firewalls and intrusion prevention systems. Finally, a threat hunter team can quickly retrieve past information to help with investigations and attribution process.

6.2 Process

In this chapter we will explore each re-defined phase of C2 fingerprinting process. Some not implemented features will be discussed in Future Work chapter.

6.2.1 Collecting

To stay up-to-date with emerging threats we need a reliable source of IoCs. In this case, reliability means "freshness", variety and amount of indicators of compromise available. To easily maintain the IoCs local database, we recommend an incremental approach. Essentially, it consists in initially fetching a full copy of all sources chosen and then updating them at fixed interval of time. As researchers can push IoCs at any time in a day, the advice is to choose a short time interval in the order of minutes for fetching recent data.

6.2.2 Cleaning

Since the entire process are conceived in a completely different way from the typical approach, now this step is not so impactful. We have determined that just discarding

malformed and private IP addresses¹ is sufficient to provide a decent input to the next step.

6.2.3 Comparing & Pivoting

Given the automation done in the architecture step, now we can process all available IoCs through the cyberspace search engine chosen. Every field-value pair is extracted from the results for further analysis. Given the manner in which pairs will be used to build a signature, we will refer to field-value pairs as *modules*. Moreover, a mathematical formula is applied to transform the human interaction, required in by-hand comparing and by-hypothesis scoring, to an automated process. For this reason, the pivoting phase is now included in the comparing one. We defined a formula to determine how much a module is likely representative of the C2 family under investigation:

$$\frac{IoCs_matched}{IoCs} * \log_{10}(IoCs) * (\log_{10}(\frac{hosts}{hosts_matched}))^2$$

Where:

- IoCs: total of IoCs.
- IoCs_matched: total of IoCs with the specified field-value pair under investigation.
- hosts: total of global hosts available for search on the cyberspace search engine.
- hosts_matched: total of global hosts with the specified field-value pair under investigation.

This mathematical expression is composed by three parts:

- $\frac{IoCs}{IoCs_matched}$: IoCs true positive rate².
- $\log_{10}(IoCs)$: base-10 multiplicative coefficient based on total number of IoCs.
- $(\log_{10}(\frac{hosts}{hosts_matched}))^2$: base-10 global hosts true positive rate inverse.

The first component of the formula describes just how many IoCs contain that field-value pair. The second component translates the need to increase "reliability", proportionally to the number of available IoCs, and it ensures that a zero score is given if only an IoC is available. This is because there is no point in comparing a unit with itself. Nevertheless, we still store modules with a zero score for possible manual investigations. The third and last component rises the score the smaller the number of global matches, because it is clear that hosts belonging to a specific C2 family will be a tiny part of the

¹«A private IP address is a range of non-internet facing IP addresses used in an internal network» [187].

²The true positive rate (TPR) gives the proportion of correct predictions in predictions of positive class» [80].

Internet. Finally, we observed that, when counting matches of a signature in C2 fingerprinting, it is common practice to reason in powers of ten. Therefore, we chose to use a logarithmic function in base 10.

This formula is the result of many practical tests, however, we believe there is still room for improvement.

6.2.4 Refining

Refining is now made by clustering modules. Instead of removing false positive performing intelligence researches, we specified four types by which categorize modules, according to their score and "coverage". We define *coverage* the number of global results returned by searching that field-value pair on the cyberspace search engine. The four module types, descending in terms of relevance, are:

- Type1: high score, low coverage.
- Type2: high score, high coverage.
- Type3: low score, low coverage.
- Type4: low score, high coverage.

6.2.5 Fingerprinting

Usually, fingerprinting phase would generate only one or two signatures with typical approach, because we are limited by manual work in comparing field-value pairs and in signature management. The architecture we are designed, instead, allow us to proceed in a different way. First, we chain all type1 modules related to a specific field through some boolean OR. We define the result of this operation a *block*. Then, we put in AND the block created with one or more relevant blocks built on type2 modules, producing what we define as *signature*. These steps are repeated for each field and for each C2 family.

6.2.6 Hunting

With a scheduled task, we query the generated signatures against cyberspace search engine database. The set of results obtained is added to the one returned by the next iteration. If an IP address is in more than one set, then his "confidence" value grows. We define *confidence* as threat information reliability degree, an indicator that describes how likely that IP address is associated with the C2 family under investigation. We store in the database each IP address with signatures matched, his confidence value and summary information like geolocation, Autonomous System³ Number and DNS names associated.

³«An Autonomous System specifies a network, mostly an organization that can own or announce network addresses to the Internet» [128]

6.2.7 Re-checking

Optional re-checking is done in the same way as before. Obviously, implementing and automating third-party scripts is far simpler in the context of our new approach.

6.3 PoC

We accurately designed this proof of concept in order to accomplish all our goals in the time available for the thesis. The most suitable way we found was to built a light platform. It is composed by :

- Web framework: Flask [55].
- Database engine: SQLite [56].
- Query language and db schemas: GraphQL [76].
- Query capabilities: Graphene-Python [75].
- IoCs fetching client: self-made ThreatFox and Shodan python client.
- Search engine client: censys-python [25].
- Processing scripts: self-made python scripts.
- Front-end GUI: GraphiQL IDE [77].

The screenshot shows the GraphiQL IDE interface. On the left, a query is defined: `query CobaltStrikeModules{ modules(filters:{c2Id:4}){ totalCount edges{ node{ c2{ name } field{ id name } fieldValue scoreFloat count coverage{ count } } } }`. On the right, the JSON response is displayed, showing a total count of 422 modules and a list of edges. One edge is expanded to show details for a module with ID '1' and name 'services.banner_hashes', including a SHA256 hash, a score float of 17.54569086949753, a count of 38, and a coverage count of 1213.

Figure 6.1. Cobalt Strike generated modules query

Flask and SQLite are just the simplest frameworks that we can use for setting up a web application and a database. GraphQL, Graphene and GraphiQL allowed us to

aggregate different APIs⁴, to uniform raw data and to easily query threat information through built-in GUI, as shown in the picture above 6.1. ThreatFox has been selected as primary source for the IoCs because is the first choice for researchers sharing C2 insights. Moreover, in some cases we included Shodan data as secondary source, because they track few C2 products with high accuracy. The reference cyber search engine is again Censys.

⁴«A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality»

Chapter 7

Results

Taking all ThreatFox IoCs, we were able to track more than one hundred of Command and Control server families. Scoring of modules extracted works very well to denote most interesting field-value pairs. In particular, we found lots of similarities with pairs used in manual investigation of other researchers, but without spending hours in comparing by-hand. Also, some new valuable modules have been discovered. Signatures generated are already at ready-to-use level for hunting. Lastly, In the refining phase, we took only first two types as they are the most relevant for our automated C2 fingerprinting process, however planning better how to link different types of modules would strongly improve hunting results.

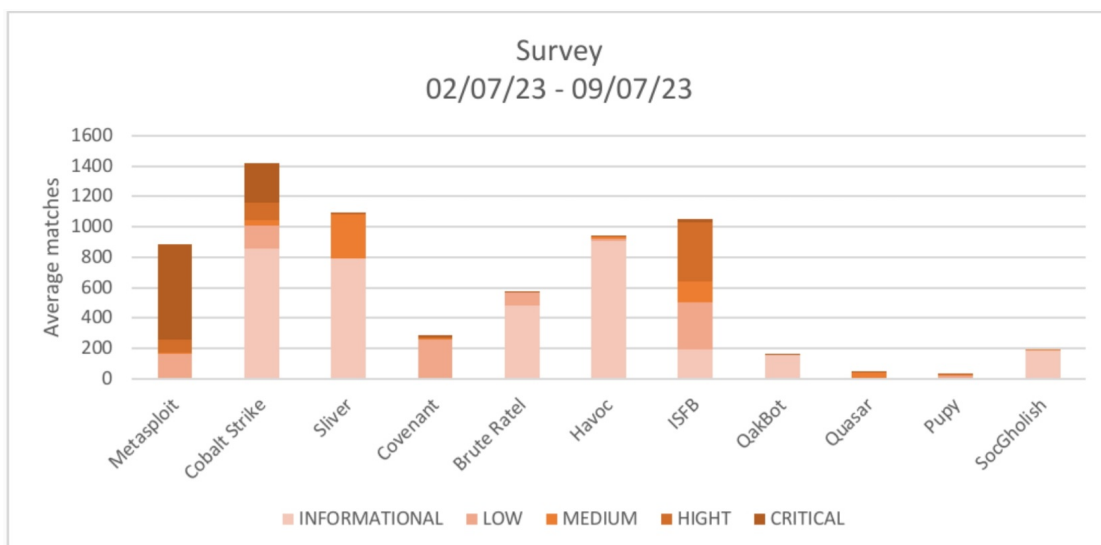


Figure 7.1. Average matches between 02/07/2023 and 09/07/2023

Merely applying the conceived approach to a basic PoC gave us very promising results. These are not theoretical-only results, as we can spend right now the knowledge produced

in real cybersecurity environments. Passive defense and intelligence are the classes that benefit most from this new approach. In the graph 7.1, we show the average matches of seven days of survey on the C2 frameworks and malware previously covered. TrueBot is not present because no instances were found in the survey period.

We divided the results according to five levels of confidence:

- Informational: only one signature match.
- Low: exactly two signatures match.
- Medium: between three and five signatures match.
- High: between six and eight signatures match.
- Critical: from nine signatures match upwards.

C2	INFORMATIONAL	LOW	MEDIUM	HIGHT	CRITICAL	TOTAL
Metasploit	1	163	7	88	626	885
Cobalt Strike	859	147	37	114	263	1420
Sliver	790	1	293	1	2	1087
Covenant	0	262	4	6	14	286
Brute Ratel	486	81	0	2	11	580
Havoc	907	12	16	2	2	939
ISFB	194	312	136	389	20	1051
QakBot	158	2	0	0	1	161
Quasar	0	0	47	0	1	48
Pupy	10	11	11	0	4	36
SocGhosh	186	1	9	0	0	196

Figure 7.2. Average matches between 02/07/2023 and 09/07/2023 - matches detail

In the table 7.2, we broadly highlighted in green the true positives and in red the false positives. As we can see, the number of true positives is quite solid from low level upwards. Most of the false positives are in the informational column, although this column can't be ignored. QakBot, for example, is often identified by a single signature, thus his samples will be in the informational column. The worst results are the ones related to ISFB malware. This because most relevant ISFB signature is built on a specific sequence of values, like "1" and "XX", inside certificate's properties (Organizational Unit, Common Name, Country, etc.). In this case, only critical results are reliable because they match all the values of the ISFB default certificate. This problem could be solved by better linking modules of different types. However, we can say that it is unlikely that proactively blocking even false positives could cause serious damage. In particular, this could happen only if the set of false positives overlaps with the set of IP addresses related to the organization's communications. Considering the number of false positives, the number of IP addresses contacted by hosts of an organization and the number of global IP addresses, the probability of a collision with a false positive is very low.

7.1 Advantages

Next we briefly list pros of our approach:

- Generating modules is **field-agnostic**. Even if there are changes in the cyberspace search engine, in the structure of scanning and probing responses or in the communication protocols, the process will continue to work without any issue.
- Confidence concept allows to choose threat information to use according to its **reliability degree**. An organization can decide how many results to import and how much risk to take in blocking false positives.
- All tasks can be **scheduled**, avoiding loss of valuable information and providing ready-to-use results for proactive defence. Timing problem about C2 servers volatility is completely solved, as fingerprinting can be repeated even at small interval of time.
- **Query capabilities** and efficient **storage** can be very helpful for investigations. Threat researchers can retrieve and filter past results to speed up the attribution process.
- **Single view** for IoCs, C2 families, signatures and matched hosts.
- **Fast, scalable** and **easy** to maintain.

7.2 Limitations

Even if tests gave excellent results, there are a few limitations:

- More **false positives** if the C2 family is uniquely identified by many signatures, as unrelated hosts that match the intermediate group of signatures will also be in the results.
- Querying very often through cyberspace search engine chosen can be quite **expensive**. Each query, indeed, is associated with a certain number of credits and with a type of subscription.
- **Skilled threat actor** could avoid scanning and probing of his infrastructure. Cyberspace search engine must identify themselves for legal reasons before scanning and probing an host, thus it is possible to prohibit them to do so.
- If most of the **IoCs** posted by researchers are wrong, then results quality will decrease significantly, as the source from which modules are processed is unrelated to the C2 family.
- Some **fields** are incorrectly mapped or not searchable through the search engine. For example, some C2 families are identified by optional http headers that can't be queried.

Chapter 8

Future Work

First results strongly encourage us to continue this work. Here we list some of the features that could be interesting to implement:

- Enhanced refining: more ways can be found to combine different types of clusters.
- Scoring machine-learning driven: machine-learning algorithms could substitute the fixed scoring formula for modules.
- recursive-hunt: IP addresses matched with a sufficient level of confidence could become new IoCs for the fingerprinting process.
- Internet-db raw access: with a raw access to a db containing information about most of the Internet public IP addresses, it would be possible to overcome limitations about pre-processed field-value pairs.
- Cyberspace information diversification: taking information about Internet devices from more cyberspace search engines makes it more difficult for attackers to block scanning and probing.
- API additions: integrating more OSINT API to better supporting all the phases.
- Output export: implementing export feature about information in the database for well-know cyber threat intelligence sharing formats.

Chapter 9

Conclusions

Fingerprinting of Command and Control servers for proactive defence is a relatively youth activity. This could lead us to think that it still doesn't need improvements. However, adversaries tactics and techniques evolve rapidly and defenders have to be sure to not be outdone. In the eternal fight between guard and thieves, that continues also in the cyberspace, even a single advantage can make the difference. In our case, fingerprinting C2 servers can do much of the required proactive work. Specifically, we tried to put this technique to the theoretical limit given by actual technological level. With this goal in mind, we designed a simple and solid way to build an effective shield against menaces with a low or medium level of sophistication. Our new approach can be implemented inside every cybersecurity environment, without strong knowledge needed. Furthermore, both newly produced and past stored threat information can be used for intelligence purposes, helping threat hunters with their attribution process about new threats and APTs. In this perspective, we can think implementations of our C2 fingerprinting way as new investigation tool in a broader and more comprehensive intelligence platform. Finally, from an academic point of view, we provided all the base knowledge needed to understand theory and motivations behind our approach. We tried also to define a robust nomenclature, hoping it will help with our and other future work on the subject.

Bibliography

- [1] 3CX. Security incident update saturday 1 april 2023. <https://www.3cx.com/blog/news/security-incident-updates/>, 2023. Last accessed on 27 May 2023.
- [2] Agenzia delle Entrate. Nuova campagna di diffusione del malware ursnif. <https://www.agenziaentrate.gov.it/portale/web/guest/attenzione-alle-false-e-mail/avviso-del-25-novembre-2020-nuova-campagna-diffusione-del-malware-ursnif>, 2020. Last accessed on 08 June 2023.
- [3] Agenzia delle Entrate. Avviso del 18 febbraio 2022. <https://www.agenziaentrate.gov.it/portale/web/guest/avviso-del-18-febbraio-2022>, 2022. Last accessed on 08 June 2023.
- [4] Agenzia delle Entrate. Avviso del 22 marzo 2022 - nuove campagne di diffusione malware tramite allegati malevoli, 2022. Last accessed on 08 June 2023.
- [5] Agenzia delle Entrate. Avviso del 7 dicembre 2022. <https://www.agenziaentrate.gov.it/portale/web/guest/avviso-7-dicembre-2022-malware>, 2022. Last accessed on 08 June 2023.
- [6] Agenzia delle Entrate. Avviso del 14 marzo 2023 - false comunicazioni di “compensi” per “operosità fiscale”, 2023. Last accessed on 08 June 2023.
- [7] Agenzia delle Entrate. Avviso del 26 maggio 2023 - false comunicazioni su istanze civis. <https://www.agenziaentrate.gov.it/portale/web/guest/avviso-del-26-maggio-2023-false-comunicazioni-su-istanze-civis>, 2023. Last accessed on 08 June 2023.
- [8] Agenzia delle Entrate. Avviso del 5 gennaio 2023 - ulteriore campagna di malspam gozi/ursnif. <https://www.agenziaentrate.gov.it/portale/web/guest/avviso-del-5-gennaio-2023-ulteriore-campagna-di-malspam-gozi-ursnif>, 2023. Last accessed on 08 June 2023.
- [9] Mehwish Akram, William Barker, Rob Clatterbuck, Donna Dodson, Brandon Everhart, Jane Gilbert, William Haag, Brian Johnson, Alexandros Kapsouris, Dung Lam, et al. Securing web transactions: Tls server certificate management. Technical report, National Institute of Standards and Technology, 2020.
- [10] Joma Rajab Salim Alrzini and Diane Pennington. A review of polymorphic malware detection techniques. *International Journal of Advanced Research in Engineering and Technology*, 11(12):1238–1247, 2020.
- [11] Bishop Fox. Netwrix auditor advisory. <https://bishopfox.com/blog/netwrix-auditor-advisory>, 2022. Last accessed on 09 June 2023.

- [12] BishopFox. Sliver: Cross-platform general purpose implant framework written in golang. <https://bishopfox.com/tools/sliver>. Last accessed on 05 June 2023.
- [13] BITM. Open-source c2's for purple teaming. <https://bitm.co.za/blog/open-source-c2s-for-purple-teaming>. Last accessed on 04 June 2023.
- [14] BleepingComputer. Hackers start using havoc post-exploitation framework in attacks. <https://www.bleepingcomputer.com/news/security/hackers-start-using-havoc-post-exploitation-framework-in-attacks/>, 2023. Last accessed on 06 June 2023.
- [15] Britannica. P2p. <https://www.britannica.com/technology/P2P>. Last accessed on 04 June 2023.
- [16] Britannica. graphical user interface. <https://www.britannica.com/technology/graphical-user-interface>, 2023. Last accessed on 05 June 2023.
- [17] buguroo. New gozi campaigns designed to avoid web fraud detection target global brands. <https://www.yumpu.com/en/document/read/55869790/fraud-detection-target-global-brands>, 2016. Last accessed on 07 June 2023.
- [18] bushidotoken. Brute ratel cracked and shared across the cyber-criminal underground. <https://blog.bushidotoken.net/2022/09/brute-ratel-cracked-and-shared-across.html>, 2022. Last accessed on 08 July 2023.
- [19] BusinessWire. 78% lack confidence in their company's cybersecurity posture, prompting 91% to increase 2021 budgets. <https://www.businesswire.com/news/home/20210224005176/en/78-Lack-Confidence-in-Their-Company's-Cybersecurity-Posture-Prompting-91-to-Increase-2021-Budgets>, 2021. Last accessed on 04 May 2023.
- [20] C2Matrix. <https://www.thec2matrix.com/about>. Last accessed on 04 June 2023.
- [21] C2Matrix. <https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4IgPsSc>. Last accessed on 04 June 2023.
- [22] Krzysztof Cabaj, Dulce Domingos, Zbigniew Kotulski, and Ana Respício. Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, 75:24–35, 2018.
- [23] CambridgeDictionary. cross-platform. <https://dictionary.cambridge.org/dictionary/english/cross-platform>. Last accessed on 06 June 2023.
- [24] Red Canary. Command and control (c2) frameworks. <https://redcanary.com/threat-detection-report/trends/c2-frameworks/>. Last accessed on 04 June 2023.
- [25] Censys. <https://github.com/censys/censys-python>. Last accessed on 20 June 2023.
- [26] Check Point. December 2022's most wanted malware: Glupteba entering top ten and qbot in first place. <https://www.checkpoint.com/press-releases/december-2022s-most-wanted-malware-glupteba-entering-top-ten-and-qbot-in-first-pl> 2022. Last accessed on 08 June 2023.
- [27] Check Point. November 2022's most wanted malware: A month of comebacks for trojans as emotet and qbot make an impact. <https://www.checkpoint.com/press-releases/>

- [november-2022s-most-wanted-malware-a-month-of-comebacks-for-trojans-as-emetet-and-qbot-2022](#). Last accessed on 08 June 2023.
- [28] Check Point. April 2023's most wanted malware: Qbot launches substantial malspam campaign and mirai makes its return. <https://blog.checkpoint.com/security/april-2023s-most-wanted-malware-qbot-launches-substantial-malspam-campaign-and-mirai-ma> 2023. Last accessed on 08 June 2023.
- [29] Check Point. February 2023's most wanted malware: Remcos trojan linked to cyberespionage operations against ukrainian government. <https://www.checkpoint.com/press-releases/february-2023s-most-wanted-malware-remcos-trojan-linked-to-cyberespionage-operations-ag> 2023. Last accessed on 08 June 2023.
- [30] Check Point. January 2023's most wanted malware: Infostealer vidar makes a return while earth bogle njrat malware campaign strikes. <https://www.checkpoint.com/press-releases/january-2023s-most-wanted-malware-infostealer-vidar-makes-a-return-while-earth-bogle-nj> 2023. Last accessed on 08 June 2023.
- [31] Check Point. March 2023's most wanted malware: New emotet campaign bypasses microsoft blocks to distribute malicious onenote files. <https://www.checkpoint.com/press-releases/march-2023s-most-wanted-malware-new-emetet-campaign-bypasses-microsoft-blocks-to-distri> 2023. Last accessed on 08 June 2023.
- [32] William Chisholm, Louis T Milic, and John AC Greppin. *Interrogativity: A colloquium on the grammar, typology and pragmatics of questions in seven diverse languages, Cleveland, Ohio, October 5th 1981-May 3rd 1982*, volume 4. John Benjamins Publishing, 1984.
- [33] CISA. Qbot/qakbot malware. https://www.cisa.gov/sites/default/files/2023-02/202010221030_qakbot_tlpwhite.pdf, 2020. Last accessed on 08 June 2023.
- [34] CISA. #stopransomware: Cl0p ransomware gang exploits cve-2023-34362 moveit vulnerability. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a>, 2023. Last accessed on 09 June 2023.
- [35] Cisco Talos. Breaking the silence - recent truebot activity. <https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/>, 2023. Last accessed on 09 June 2023.
- [36] Cleafy. Digital banking fraud: how the gozi malware works. <https://www.cleafy.com/cleafy-labs/digital-banking-fraud-how-the-gozi-malware-work>, 2021. Last accessed on 07 June 2023.
- [37] Cloudflare. What is the osi model? <https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/>. Last accessed on 04 June 2023.
- [38] Alissa Cooper, Hannes Tschofenig, Dr. Bernard D. Aboba, Jon Peterson, John Morris, Marit Hansen, and Rhys Smith. Privacy Considerations for Internet Protocols. RFC 6973, July 2013.

- [39] Covenant. Entering a covenant: .net command and control. <https://github.com/cobbr/Covenant>. Last accessed on 06 June 2023.
- [40] Crowdstrike. What is the cyber kill chain? process & model. <https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/>, 2022. Last accessed on 31 May 2023.
- [41] Cybe. Threat alert: Aggressive qakbot campaign and the black basta ransomware group targeting u.s. companies. <https://www.cybereason.com/blog/threat-alert-aggressive-qakbot-campaign-and-the-black-basta-ransomware-group-targeting-u.s.-companies>, 2022. Last accessed on 08 June 2023.
- [42] Cybereason. Sliver c2 leveraged by many threat actors. <https://www.cybereason.com/blog/sliver-c2-leveraged-by-many-threat-actors>, 2023. Last accessed on 05 June 2023.
- [43] CyberProof. Managed threat intelligence. <https://www.cyberproof.com/cyber-101/managed-threat-intelligence/>. Last accessed on 05 May 2023.
- [44] Leslie Daigle. WHOIS Protocol Specification. RFC 3912, September 2004.
- [45] DarkReading. 'sliver' emerges as cobalt strike alternative for malicious c2. <https://www.darkreading.com/vulnerabilities-threats/-sliver-cobalt-strike-alternative-malicious-c2>, 2022. Last accessed on 06 June 2023.
- [46] DarkVortex. About chetan nayak. <https://0xdarkvortex.dev/about/>. Last accessed on 06 June 2023.
- [47] DarkVortex. Features & documentation. <https://bruteratel.com/tabs/features/>. Last accessed on 06 June 2023.
- [48] Robert S Dewar. The “tritych of cyber security”: A classification of active cyber defence. In *2014 6th International Conference On Cyber Conflict (CyCon 2014)*, pages 7–21. IEEE, 2014.
- [49] Oxford Learner’s Dictionaries. cluster. https://www.oxfordlearnersdictionaries.com/definition/english/cluster_1. Last accessed on 16 June 2023.
- [50] DigiCert. What is ssl, tls & https? <https://www.digicert.com/what-is-ssl-tls-and-https>. Last accessed on 16 June 2023.
- [51] Jon DiMaggio. *The Art of Cyberwarfare: An Investigator’s Guide to Espionage, Ransomware, and Organized Cybercrime*, pages 110–116. No Starch Press, San Francisco, 1st edition, 2022.
- [52] DNI. Spear phishing and common cyber attacks. https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf. Last accessed on 27 May 2023.
- [53] Europol. World’s most dangerous malware emotet disrupted through global action. <https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action>. Last accessed on 15 June 2023.
- [54] Flashpoint. Malware loaders continue to evolve, proliferate. <https://flashpoint.io/blog/malware-loaders-continue-to-evolve-proliferate/>, 2018. Last accessed on 09 June 2023.

-
- [55] Flask. <https://flask.palletsprojects.com/en/2.3.x/>. Last accessed on 20 June 2023.
- [56] Flask. <https://www.sqlite.org/index.html>. Last accessed on 20 June 2023.
- [57] Forbes. Alarming cyber statistics for mid-year 2022 that you need to know. <https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/>, 2022. Last accessed on 02 May 2023.
- [58] Forbes. Information security vs. cybersecurity: What's the difference? <https://www.forbes.com/advisor/education/information-security-vs-cyber-security/>, 2022. Last accessed on 11 June 2023.
- [59] Fortinet. What is ddos attack? <https://www.fortinet.com/resources/cyberglossary/ddos-attack>. Last accessed on 24 May 2023.
- [60] Fortra. Cobalt strike release notes. <https://download.cobaltstrike.com/releasenotes.txt>. Last accessed on 05 June 2023.
- [61] Fortra. Starting the team server. https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/topics/welcome_starting-cs-team-server.htm. Last accessed on 05 June 2023.
- [62] Fortra. Helpsystems (now fortra) acquires cobalt strike to expand core security business. <https://www.fortra.com/resources/press-releases/helpsystems-acquires-cobalt-strike-expand-core-security-business>, 2020. Last accessed on 05 June 2023.
- [63] Darko Galinec, Darko Možnik, and Boris Guberina. Cybersecurity and cyber defence: national level strategic approach. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, 58(3):273–286, 2017.
- [64] Joseph Gardiner, Marco Cova, and Shishir Nagaraja. Command & control: Understanding, denying and detecting—a review of malware c2 techniques, detection and defences. *arXiv preprint arXiv:1408.1136*, 2014.
- [65] Gartner. Definition: Threat intelligence. <https://www.gartner.com/en/documents/2487216>, 2012. Last accessed on 21 May 2023.
- [66] GitHub. Cobaltstrikeparser. <https://github.com/Sentinel-One/CobaltStrikeParser>. Last accessed on 19 June 2023.
- [67] GitHub. grab_beacon_config. https://github.com/whickey-r7/grab_beacon_config. Last accessed on 19 June 2023.
- [68] GitHub. Havoc. <https://github.com/HavocFramework/Havoc>. Last accessed on 06 June 2023.
- [69] GitHub. Hello world. <https://docs.github.com/en/get-started/quickstart/hello-world>. Last accessed on 05 June 2023.
- [70] GitHub. melting-cobalt. <https://github.com/splunk/melting-cobalt>. Last accessed on 19 June 2023.
- [71] GitHub. pointer. <https://github.com/shabarkin/pointer>. Last accessed on 19 June 2023.
- [72] GitHub. pupy. <https://github.com/n1nj4sec/pupy>. Last accessed on 08 June 2023.

- [73] GitHub. Quasar. <https://github.com/quasar/Quasar>. Last accessed on 08 June 2023.
- [74] Google. Making cobalt strike harder for threat actors to abuse. <https://cloud.google.com/blog/products/identity-security/making-cobalt-strike-harder-for-threat-actors-to-abuse>, 2022. Last accessed on 05 June 2023.
- [75] Graphene. <https://graphene-python.org/>. Last accessed on 20 June 2023.
- [76] GraphQL. <https://graphql.org/>. Last accessed on 20 June 2023.
- [77] GraphQL. <https://github.com/graphql/graphiql>. Last accessed on 20 June 2023.
- [78] IBM. Security operations center (soc). <https://www.ibm.com/topics/security-operations-center>. Last accessed on 21 May 2023.
- [79] IBM. What is threat intelligence? <https://www.ibm.com/topics/threat-intelligence>. Last accessed on 01 June 2023.
- [80] IBM. True positive rate. <https://www.ibm.com/docs/en/cloud-paks/cp-data/4.6.x?topic=overview-true-positive-rate-tpr>, 2023. Last accessed on 21 June 2023.
- [81] Infinitum IT. Charming kitten (apt35). <https://www.infinitumit.com.tr/charming-kitten-apt35/>, 2022. Last accessed on 08 June 2023.
- [82] Infosec. Encryption vs encoding. <https://resources.infosecinstitute.com/topic/encryption-vs-encoding/>, 2020. Last accessed on 03 June 2023.
- [83] Joint Task Force. Security and privacy controls for information systems and organizations. Technical report, National Institute of Standards and Technology, 2017.
- [84] Joint Task Force on Cybersecurity Education. *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Association for Computing Machinery, New York, NY, USA, 2018.
- [85] Joinup. About dns (rfc 1034 - rfc 1035) - domain name system. <https://joinup.ec.europa.eu/collection/ict-standards-procurement/solution/dns-rfc-1034-rfc-1035-domain-name-system/about>. Last accessed on 16 June 2023.
- [86] Eric Jollès, Sébastien Gillard, Dimitri Percia David, Martin Strohmeier, and Alain Mermoud. Building collaborative cybersecurity for critical infrastructure protection: Empirical evidence of collective intelligence information sharing dynamics on threat-fox. In *International Conference on Critical Information Infrastructures Security*, pages 140–157. Springer, 2022.
- [87] Kaspersky. Exploitation in the wild (itw). <https://encyclopedia.kaspersky.com/glossary/exploitation-in-the-wild-itw/>. Last accessed on 06 June 2023.
- [88] Kaspersky. Silence like a cancer grows. <https://www.kaspersky.com/blog/silence-financial-apt/19993/>, 2017. Last accessed on 09 June 2023.
- [89] Kaspersky. Don't expect any howls: Goldenjackal apt spying on diplomatic entities in middle east and south asia. https://www.kaspersky.com/about/press-releases/2023_dont-expect-any-howls-goldenjackal-apt-spying-on-diplomatic-entities-in-middle-east 2023. Last accessed on 28 May 2023.

-
- [90] David Kennedy, Jim O’gorman, Devon Kearns, and Mati Aharoni. *Metasploit: the penetration tester’s guide*, pages 22–23. No Starch Press, 2011.
- [91] Tadayoshi Kohno, Andre Broido, and Kimberly C Claffy. Remote physical device fingerprinting. *IEEE Transactions on Dependable and Secure Computing*, 2(2):93–108, 2005.
- [92] Brian Krebs. Conti ransomware group diaries, part iii: Weaponry. <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/>, 2022. Last accessed on 05 June 2023.
- [93] Luukas Larinkoski et al. Detecting encrypted command & control channels with network fingerprints. Master’s thesis, 2016.
- [94] Ruiguang Li, Meng Shen, Hao Yu, Chao Li, Pengyu Duan, and Lihuang Zhu. A survey on cyberspace search engines. In *Cyber Security: 17th China Annual Conference, CNCERT 2020, Beijing, China, August 12, 2020, Revised Selected Papers 17*, pages 206–214. Springer Singapore, 2020.
- [95] Lockheed Martin. Cyber kill chain. <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>. Last accessed on 08 July 2023.
- [96] Robert M. Lee. Active cyber defense cycle. In *BSides Huntsville 2015*. NAC-ISSA, 2015.
- [97] Robert M. Lee. Data, information, and intelligence: Why your threat feed is likely not threat intelligence. <https://www.sans.org/blog/data-information-and-intelligence-why-your-threat-feed-is-likely-not-threat-intelligence> 2015. Last accessed on 13 June 2023.
- [98] Robert M. Lee. The sliding scale of cybersecurity. *SANS Institute*. Retrieved January, 24:2018, 2015.
- [99] Malpedia. Fakeupdates. <https://malpedia.caad.fkie.fraunhofer.de/details/js.fakeupdates>. Last accessed on 09 June 2023.
- [100] Malpedia. Qakbot. <https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot>. Last accessed on 08 June 2023.
- [101] Malpedia. Silence group. https://malpedia.caad.fkie.fraunhofer.de/actor/silence_group. Last accessed on 09 June 2023.
- [102] Malwarebytes. Spyware.infostealer. <https://www.malwarebytes.com/blog/detections/spyware-infostealer>. Last accessed on 07 June 2023.
- [103] Malwarebytes. 2020 state of malware report. https://www.malwarebytes.com/resources/files/2020/02/2020_state-of-malware-report.pdf, 2020. Last accessed on 08 June 2023.
- [104] Bill Marczak and John Scott-Railton. The million dollar dissident: Nso group’s iphone zero-days used against a uae human rights defender. *Citizen Lab*, 24, 2016.
- [105] Medium. Kali linux & metasploit: Getting started with pen testing. <https://medium.com/@nickhandy/kali-linux-metasploit-getting-started-with-pen-testing-89d28944097b>, 2018. Last accessed on 08 July 2023.
- [106] Medium. Chapter 1 — from gozi to isfb: The history of a mythical malware family. <https://medium.com/csis-techblog/>

- [chapter-1-from-gozi-to-isfb-the-history-of-a-mythical-malware-family-82e592577fef](#), 2022. Last accessed on 07 June 2023.
- [107] Medium. Unified kill chain in cyber threat intelligence. <https://warnerchad.medium.com/unified-kill-chain-in-cyber-threat-intelligence-b577bf340ceb>, 2022. Last accessed on 08 July 2023.
- [108] Medium. Hunting malicious infrastructure using jarm and http response. <https://michaelkoczvara.medium.com/hunting-malicious-infrastructure-using-jarm-and-http-response-bb4a039d4119>, 2023. Last accessed on 09 July 2023.
- [109] Microsoft. Stopping cybercriminals from abusing security tools. <https://blogs.microsoft.com/on-the-issues/2023/04/06/stopping-cybercriminals-from-abusing-security-tools/>, 2023. Last accessed on 05 June 2023.
- [110] Microsoft. What is .net? <https://dotnet.microsoft.com/en-us/learn/dotnet/what-is-dotnet>. Last accessed on 06 June 2023.
- [111] Microsoft. Detecting and preventing lsass credential dumping attacks. <https://www.microsoft.com/en-us/security/blog/2022/10/05/detecting-and-preventing-lsass-credential-dumping-attacks/>, 2022. Last accessed on 01 June 2023.
- [112] Microsoft. Extortion economics. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v>, 2022. Last accessed on 06 June 2023.
- [113] Microsoft. Raspberry robin worm part of larger ecosystem facilitating pre-ransomware activity. <https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activit>, 2023. Last accessed on 09 June 2023.
- [114] Dan Milmo. Anonymous: the hacker collective that has declared cyberwar on russia. *The Guardian*, 2022. Last accessed on 24 May 2023.
- [115] Mitre. <https://attack.mitre.org/>. Last accessed on 21 May 2023.
- [116] Mitre. Command and control. <https://attack.mitre.org/tactics/TA0011/>, 2019. Last accessed on 03 June 2023.
- [117] Mitre. Flawedgrace. <https://attack.mitre.org/software/S0383/>, 2019. Last accessed on 09 June 2023.
- [118] Mitre. Mitre att&ck@: Design and philosophy. <https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf>, 2020. Last accessed on 01 June 2023.
- [119] Mitre. Kimsuky. <https://attack.mitre.org/groups/G0094/>, 2022. Last accessed on 08 June 2023.
- [120] Mitre. Os credential dumping: Lsass memory. <https://attack.mitre.org/techniques/T1003/001/>, 2023. Last accessed on 01 June 2023.
- [121] Raphael Mudge. A history of cobalt strike in training courses. <https://www.cobaltstrike.com/blog/>

- [a-history-of-cobalt-strike-in-training-courses/](#). Last accessed on 05 June 2023.
- [122] Raphael Mudge. User-defined storage-based covert communication. <https://www.cobaltstrike.com/blog/user-defined-storage-based-covert-communication/>. Last accessed on 05 June 2023.
- [123] David Myers, Ernest Foo, and Kenneth Radke. Internet-wide scanning taxonomy and framework. In *Proceedings of the 13th Australasian Information Security Conference (AISC 2015)[Conferences in Research and Practice in Information Technology (CRPIT), Volume161]*, pages 61–65. Australian Computer Society, 2015.
- [124] Yuki Nakamura and Björn Åström. Scanning and host fingerprinting methods for command and control server detection, 2021.
- [125] Nginx. nginx. <https://nginx.org/en/>. Last accessed on 17 June 2023.
- [126] NIST. advanced persistent threat. https://csrc.nist.gov/glossary/term/advanced_persistent_threat. Last accessed on 06 July 2023.
- [127] NIST. Antivirus software. https://csrc.nist.gov/glossary/term/antivirus_software. Last accessed on 12 June 2023.
- [128] NIST. As. <https://csrc.nist.gov/glossary/term/as>. Last accessed on 22 June 2023.
- [129] NIST. Banner grabbing. https://csrc.nist.gov/glossary/term/banner_grabbing. Last accessed on 17 June 2023.
- [130] NIST. Botnet. <https://csrc.nist.gov/glossary/term/botnet>. Last accessed on 15 June 2023.
- [131] NIST. bug bounty. https://csrc.nist.gov/glossary/term/bug_bounty. Last accessed on 08 June 2023.
- [132] NIST. firewall. <https://csrc.nist.gov/glossary/term/firewall>. Last accessed on 12 June 2023.
- [133] NIST. Framework. <https://csrc.nist.gov/glossary/term/framework>. Last accessed on 04 June 2023.
- [134] NIST. hashing. <https://csrc.nist.gov/glossary/term/hashing>. Last accessed on 22 May 2023.
- [135] NIST. https://csrc.nist.gov/glossary/term/watering_hole_attack. https://csrc.nist.gov/glossary/term/watering_hole_attack. Last accessed on 27 May 2023.
- [136] NIST. incident response plan. https://csrc.nist.gov/glossary/term/incident_response_plan. Last accessed on 12 June 2023.
- [137] NIST. intrusion prevention system (ips). https://csrc.nist.gov/glossary/term/intrusion_prevention_system. Last accessed on 12 June 2023.
- [138] NIST. Log. <https://csrc.nist.gov/glossary/term/log>. Last accessed on 13 June 2023.
- [139] NIST. malware. <https://csrc.nist.gov/glossary/term/malware>. Last accessed on 07 June 2023.
- [140] NIST. penetration testing. https://csrc.nist.gov/glossary/term/penetration_testing. Last accessed on 05 June 2023.
- [141] NIST. phishing. <https://csrc.nist.gov/glossary/term/phishing>. Last accessed on 21 May 2023.

- [142] NIST. Red team. https://csrc.nist.gov/glossary/term/red_team. Last accessed on 04 June 2023.
- [143] NIST. Rfc. <https://csrc.nist.gov/glossary/term/rfc>. Last accessed on 15 June 2023.
- [144] NIST. supply chain attack. https://csrc.nist.gov/glossary/term/supply_chain_attack. Last accessed on 28 May 2023.
- [145] NIST. threat intelligence. https://csrc.nist.gov/glossary/term/threat_intelligence. Last accessed on 21 May 2023.
- [146] NIST. Guidelines on firewalls and firewall policy. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-41r1.pdf>, 2009. Last accessed on 20 June 2023.
- [147] NIST. Ransomware protection and response. <https://csrc.nist.gov/projects/ransomware-protection-and-response>, 2022. Last accessed on 21 May 2023.
- [148] IPED Nugraha. A review on the role of modern soc in cybersecurity operations. *Int. J. Current Sci. Res. Rev*, 4(5):408–414, 2021.
- [149] U.S. Department of Justice. Emotet botnet disrupted in international cyber operation. <https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation>. Last accessed on 15 June 2023.
- [150] National Police of Ukraine. (trad.) cyberpolice exposes transnational group of hackers for spreading emotet virus. https://www.youtube.com/watch?v=_BL0mClSSpC, 2021. Last accessed on 15 June 2023.
- [151] National Police of Ukraine. (trad.) cyberpolice exposes transnational group of hackers in spreading the world’s most dangerous computer virus "emotet". <https://www.npu.gov.ua/news/kiberpolitsiya-vikrila-transnatsionalne-ugrupovannya-khakeriv-u-rozpovsyudzhenni-1>, 2021. Last accessed on 15 June 2023.
- [152] OWASP. Security by design principles. https://wiki.owasp.org/index.php/Security_by_Design_Principles. Last accessed on 11 June 2023.
- [153] PANW. When pentest tools go brutal: Red-teaming tool being abused by malicious actors. <https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/>, 2022. Last accessed on 06 June 2023.
- [154] Payload Café. Havoc c2 intro & inline c# compilation within powershell. <https://payload.cafe/2022/10/02/havoc-c2-intro-inline-csharp-compilation-within-powershell/>, 2022. Last accessed on 08 July 2023.
- [155] Peng Peng, Limin Yang, Linhai Song, and Gang Wang. Opening the blackbox of virustotal: Analyzing online phishing scan engines. In *Proceedings of the Internet Measurement Conference*, pages 478–485, 2019.
- [156] Paul Pols and Jan van den Berg. The unified kill chain. *CSA Thesis, Hague*, 2017.
- [157] Proofpoint. Part 1: Socgholish, a very real threat from a very fake update. <https://www.proofpoint.com/us/blog/threat-insight/part-1-socgholish-very-real-threat-very-fake-update>, 2022. Last accessed on 09 June 2023.

- [158] Qualys. Stealthy quasar evolving to lead the rat race. <https://www.qualys.com/docs/whitepapers/qualys-wp-stealthy-quasar-evolving-to-lead-the-rat-race-v220727.pdf>, 2022. Last accessed on 08 June 2023.
- [159] Babak Bashari Rad, Harrison John Bhatti, and Mohammad Ahmadi. An introduction to docker and analysis of its performance. *International Journal of Computer Science and Network Security (IJCSNS)*, 17(3):228, 2017.
- [160] Yisrael Radai. The israeli pc virus. *Computers & Security*, 8(2):111–113, 1989.
- [161] Rapid7. Metasploit pen testing tool. <https://www.rapid7.com/products/metasploit/download/editions/>. Last accessed on 04 June 2023.
- [162] Rapid7. The mitre att&ck framework. <https://www.rapid7.com/fundamentals/mitre-attack/>. Last accessed on 31 May 2023.
- [163] Rapid7. Rapid7 position on private sector hack back. https://www.rapid7.com/globalassets/_pdfs/policy/hack-back-position-20210617.pdf, 2021. Last accessed on 12 June 2023.
- [164] Recorded Future. European energy sector organization targeted by pupyrat malware in late 2019. <https://go.recordedfuture.com/hubfs/reports/cta-2020-0123.pdf>, 2020. Last accessed on 08 June 2023.
- [165] Recorded Future. 2022 adversary infrastructure report. <https://www.recordedfuture.com/2022-adversary-infrastructure-report>, 2022. Last accessed on 04 June 2023.
- [166] ResearchGate. Cybersecurity and the security operations center. <https://www.ciscopress.com/articles/article.asp?p=2928195&seqNum=5>, 2019. Last accessed on 08 July 2023.
- [167] ResearchGate. The sliding scale of cybersecurity. https://www.researchgate.net/figure/The-Sliding-Scale-of-Cybersecurity_fig1_365820432, 2022. Last accessed on 08 July 2023.
- [168] Reversing Labs. Open-source repository malware sows havoc. <https://www.reversinglabs.com/blog/open-source-malware-sows-havoc-on-supply-chain>, 2023. Last accessed on 06 June 2023.
- [169] SANS. Sans cybercast sans@mic - c2 matrix. <https://www.sans.org/blog/introducing-slingshot-c2-matrix-edition/>, 2020. Last accessed on 04 June 2023.
- [170] SANS. Cyber kill chain, mitre att&ck, and purple team. <https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team/>, 2022. Last accessed on 31 May 2023.
- [171] Oleksandr Saprykin. Models and methods for diagnosing zero-day threats in cyberspace. *Herald of Advanced Information Technology*, 2(4):155–167, 2021.
- [172] Y Sattarova Feruza and Tao Hoon Kim. It security review: Privacy, protection, access control, assurance and system security. *International journal of multimedia and ubiquitous engineering*, 2(2):17–32, 2007.
- [173] Daniel Schatz, Rabih Bashroush, and Julie Wall. Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, 12(2):8, 2017.

- [174] Security. America's password habits 2021. <https://www.security.org/resources/online-password-strategies/>, 2023. Last accessed on 02 May 2023.
- [175] SecurityWeek. 3cx supply chain attack: North Korean hackers likely targeted cryptocurrency firms. <https://www.securityweek.com/3cx-supply-chain-attack-north-korean-hackers-likely-targeted-cryptocurrency-firms>, 2023. Last accessed on 28 May 2023.
- [176] SecurityWeekly. Throwback: Armitage with raphael mudge (ep260). <https://www.youtube.com/watch?v=bjKpVwmKDKE>, 2011. Last accessed on 05 June 2023.
- [177] SentinelOne. Hive attacks | analysis of the human-operated ransomware targeting healthcare. <https://www.sentinelone.com/labs/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/>, 2021. Last accessed on 21 May 2023.
- [178] Guoqiang Shu and David Lee. Network protocol system fingerprinting - a formal approach. In *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, pages 1–12. IEEE, 2006.
- [179] Oleg Skulkin. *Incident Response Techniques for Ransomware Attacks*, pages 41–50. Packt Publishing Ltd., Birmingham, 1st edition, 2022.
- [180] Oleg Skulkin. *Incident Response Techniques for Ransomware Attacks*, pages 187–196. Packt Publishing Ltd., Birmingham, 2022.
- [181] Sophos. Blackcat ransomware attacks not merely a byproduct of bad luck. <https://news.sophos.com/en-us/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck/>, 2022. Last accessed on 06 June 2023.
- [182] Markus Sosnowski, Johannes Zirngibl, Patrick Sattler, Georg Carle, Claas Grohnfeldt, Michele Russo, and Daniele Sgandurra. Active TLS stack fingerprinting: Characterizing TLS server deployments at scale. *arXiv preprint arXiv:2206.13230*, 2022.
- [183] Splunk. Threat hunting vs. threat detecting: Two approaches to finding & mitigating threats. https://www.splunk.com/en_us/blog/learn/threat-hunting-vs-threat-detecting.html, 2023. Last accessed on 05 May 2023.
- [184] Thomas F Stafford and Andrew Urbaczewski. Spyware: The ghost in the machine. *The Communications of the Association for Information Systems*, 14(1):49, 2004.
- [185] SunnyValleyNetworks. What is command and control (c&c or c2) in cybersecurity? <https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-command-and-control-c2>. Last accessed on 05 June 2023.
- [186] Rabia Tahir. A study on malware and malware detection techniques. *International Journal of Education and Management Engineering*, 8(2):20, 2018.
- [187] TechTarget. Public IP address. <https://www.techtarget.com/whatis/definition/private-IP-address>. Last accessed on 20 June 2023.
- [188] TechTarget. offensive security. <https://www.techtarget.com/whatis/definition/offensive-security>, 2012. Last accessed on 05 June 2023.
- [189] TechTarget. security by design. <https://www.techtarget.com/whatis/definition/security-by-design>, 2015. Last accessed on 11 June 2023.
- [190] TechTarget. cyber attribution. <https://www.techtarget.com/searchsecurity/definition/cyber-attribution>, 2017. Last accessed on 28 May 2023.

- [191] TechTarget. dark web (darknet). <https://www.techtarget.com/whatis/definition/dark-web>, 2021. Last accessed on 25 May 2023.
- [192] TechTarget. script kiddie. <https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie>, 2021. Last accessed on 05 May 2023.
- [193] TechTerms. Payload. <https://techterms.com/definition/payload>. Last accessed on 31 May 2023.
- [194] Telsy. Possible attack to telco company in middle east, 2021. Last accessed on 06 June 2023.
- [195] The DFIR Report. Cobalt strike, a defender’s guide. <https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/>, 2021. Last accessed on 08 July 2023.
- [196] TheBedfordCitizen. What do they do there anyway – mitre. <https://thebedfordcitizen.org/2022/11/what-do-they-do-there-anyway-mitre/>, 2022. Last accessed on 31 May 2023.
- [197] TheHill. Millions of americans stopped working from home in 2022: Labor dept. <https://thehill.com/business/3919102-millions-of-americans-stopped-working-from-home-in-2022-labor-dept/>, 2023. Last accessed on 02 May 2023.
- [198] Threatpost. Q&a: Hd moore on metasploit, disclosure and ethics, 2010. Last accessed on 04 June 2023.
- [199] Trend Micro. Thwarting loaders: From socgholish to blister’s lockbit payload. https://www.trendmicro.com/en_us/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html, 2022. Last accessed on 09 June 2023.
- [200] TrendMicro. Zero-day exploit. <https://www.trendmicro.com/vinfo/us/security/definition/zero-day-exploit>. Last accessed on 27 May 2023.
- [201] TrendMicro. Black basta ransomware gang infiltrates networks via qakbot, brute ratel, and cobalt strike. https://www.trendmicro.com/de_de/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html, 2022. Last accessed on 06 June 2023.
- [202] Twitter. Nicolas verdier. <https://twitter.com/n1nj4sec>. Last accessed on 08 June 2023.
- [203] Twitter. <https://twitter.com/NinjaParanoid/status/1575104655558049792>, 2022. Last accessed on 06 June 2023.
- [204] US-Congress. Public law 115–232. <https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf>, 2018. Last accessed on 04 June 2023.
- [205] Marius S Vassiliou, David S Alberts, and Jonathan Russell Agre. *C2 re-envisioned: the future of the enterprise*, page 1. CRC Press, 2014.
- [206] VK9 Securty. How to set up & use c2 sliver. <https://vk9-sec.com/how-to-set-up-use-c2-sliver/>, 2020. Last accessed on 08 July 2023.
- [207] VMware. Carbon black’s truebot detection. <https://blogs.vmware.com/security/2023/06/carbon-blacks-truebot-detection.html>, 2023. Last accessed on 09 June 2023.

- [208] Heather J Williams and Ilana Blum. Defining second generation open source intelligence (osint) for the defense enterprise. Technical report, Rand Corporation, 2018.
- [209] ZDNet. Fbi: Prolock ransomware gains access to victim networks via qakbot infections. <https://www.zdnet.com/article/fbi-prolock-ransomware-gains-access-to-victim-networks-via-qakbot-infections/>, 2020. Last accessed on 08 June 2023.
- [210] Zscaler. Havoc across the cyberspace. <https://www.zscaler.com/blogs/security-research/havoc-across-cyberspace>, 2023. Last accessed on 06 June 2023.