INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE
Villalón-Huerta et al., Vol.13, No.2, pp.1-32
https://doi.org/10.55859/ijiss.1431064

Provisioning the external infrastructure for Cyberspace Operations. A spotlight on Russian APT groups

Antonio Villalón-Huerta[1], Ismael Ripoll-Ripoll[2], Hector Marco-Gisbert[2]

[1]S2 Grupo, Ramiro de Maeztu, 7, Valencia, Spain
[2] Department of Computing Engineering, Universitat Politècnica de València, Valencia, Spain
Corresponding Author: antonio.villalon@s2grupo.es

Research Paper Received: 21.03.2024 Revised: 11.04.2024 Accepted: 14.04.2024

Abstract— Advanced threat actors operating on cyberspace rely on external infrastructure for their operations. This external infrastructure encompasses various elements available on the internet, located outside the target's premises. Analyzing this infrastructure and the techniques utilized to maximize its operational efficiency is crucial in understanding threat actors and their activities. However, much of the existing scientific and technical literature predominantly focuses on internal infrastructure components, such as malware implants, and the tactics used by threat actors within their victim's infrastructure. This work aims to provide a comprehensive analysis of external infrastructure and its provisioning techniques. Although our research primarily delves into Russian APT groups and their activities, our findings are applicable to all advanced threat groups and operations. The outcomes of our study can significantly aid analysts in characterizing these groups and their activities, particularly in attribution endeavors. Our proposal presents a logical structure that is easily scalable and adaptable, and it can be used to improve widely accepted industry standards such as MITRE ATT&CK.

Keywords—Advanced Persistent Threat, APT, Russia, Infrastructure, Tactics, techniques and procedures, Resource development, MITRE ATT&CK.

1. Introduction

An Advanced Persistent Threat (APT) is defined [1] [2] as an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical or deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.

Advanced Persistent Threats (APT) operations necessitate the oversight of publicly accessible Internet infrastructure. This infrastructure, which is under the complete or partial control of the threat actor, exists outside the target's scope. It not only facilitates the initial compromise by an APT, but also enables the ongoing exchange of information and commands between the APT and its target throughout the entire life cycle of an operation.

Examining this infrastructure and unraveling the tactics and techniques employed by a threat actor to oversee it presents certain challenges. Evidently, threat actors do not disclose information about their activities, so the information we possess about them is often deduced or gleaned from publicly available reports. Furthermore, these reports primarily center on the malware distributed to the victim rather than concentrating on the external infrastructure of specific campaigns. Nonetheless, analyzing external infrastructure along with its associated tactics and techniques becomes imperative when facing sophisticated threat actors. Understanding how a threat actor readies itself for a campaign not only facilitates its prevention but also enhances the potential for early detection.

1.1. Motivation and Contribution

This paper examines the management of infrastructure for APT operations, with a specific focus on its provisioning Although it is focused on Russian threat groups, most of our findings and proposals can be applied to the modus operandi of APTs from other countries. We explore the techniques employed by active Russian APTs in setting up their infrastructure. Furthermore, a taxonomy of provisioning techniques is provided, and the essential elements that must be provisioned are identified. The main contributions of this paper are the following ones:

- To provide a unified view of the management of external infrastructure in Russian APT campaigns, that can be applied to APT campaigns from other countries.
- To dissect the tactics related to the management of this external infrastructure.
- To identify and dissect the provisioning techniques for external infrastructure.
- To ease the modeling, and thus the detection and neutralization, of advanced threat actors. Particularly, our findings can improve the attribution of operations.

1.2. Organization

The rest of the paper is organized as follows. The background, Section 2, provides a description of Russian intelligence on cyberspace, including the most relevant APT groups, as well as a description of MITRE ATT&CK, as the main framework for the identification of threat actors' tactics and techniques. In Section 3 the description and goals of external infrastructure is presented, in order to better understand why this infrastructure is needed and must be prepared before an operation starts. Section 4 analyzes the different approaches to the identification of infrastructure provisioning, with a general view but also focusing on Russian groups. Section 5 proposes a classification for the provisioning tactic, as well as the identification of infrastructure elements that APT groups require to perform an operation. An alignment of our proposal with MITRE ATT&CK, as the main industry reference, is also provided, in order to improve the practical results of our work. In Section 6 the results of our work are discussed, comparing them with previous approaches and identifying improvements where applicable, as well as future research lines. Finally, Section 7 summarizes the outcome of the overall work.

2. Background

2.1. Russian intelligence on cyberspace

The Russian Federation intelligence community is a complex ecosystem [3] [4]. Different government agencies with formal assignments are defined by the Russian law. In addition, other actors, such as criminal gangs or patriotic hackers, probably have close ties with the government intelligence services [5] [6] [7]. All of these actors possess the capability to conduct hostile operations within cyberspace.

The Russian Federation boasts a diverse array of actors dedicated to state security, encompassing various intelligence services that possess the capabilities to operate within cyberspace. Almost certainly all of these actors have both cyberspace exploitation and cyberspace attack capabilities. However, three main services are linked to known APT groups [8] [9]: FSB, SVR and GRU. For years, they have been targeting multiple victims from different countries and sectors, including governments and strategic companies. Other Russian intelligence services have also developed cyberspace capabilities, such as the Federal Protective Service (Federalnaya Sluzhba Okhrany, FSO). However, no relevant threat actor linked to these services has been identified, so in this section we will not delve into them.

The Federal Security Service of the Russian Federation (Federal'naya Sluzhba Bezopasnosti Rossiyskoy Federatsii, FSB) is the biggest Russian intelligence service. In the realm of the cyber domain, the FSB wields an extensive array of technical and regulatory powers, both within Russia and on an international scale. The FSB has different units engaged in Electronic Intelligence, Signals Intelligence, Cyberspace Defense and offensive capabilities on cyberspace, such as cyber espionage [3] [10].

Foreign Intelligence Service (Sluzhba Vnéshney Razvedki, SVR) is Russia's external intelligence service. Although it is mainly a Human Intelligence agency, SVR has also developed cyberspace capabilities not only from a technical point of view [11] [12], but also from the Psychological Operations perspective [13]. It is highly likely that, similar to the FSB, certain APT groups are associated with the SVR, as will be detailed in the following section.

The Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Glavnoje upravlenije General'nogo shtaba Vooruzhonnykh sil Rossiyskoy Federatsii, GU) is commonly known as the Main Intelligence Directorate (Glavnoye razvedyvatel'noye upravleniye, GRU). It is a military intelligence service, reporting to the Chief of the General Staff and to the Minister of Defense (both FSB and GRU report to the President of the Russian Federation). GRU has not only Cyberspace Exploitation capabilities, but also Cyberspace Attack ones: this military service performs destructive campaigns to neutralize selected targets.

In addition to these services, Russia's official intelligence ecosystem on cyberspace comprises capabilities in military units, research institutes or state enterprises. Almost certainly, many of these elements are able to perform or support both offensive and defensive Cyberspace Operations. More information about this ecosystem can be found on [4] [3] [14] or [15].

2.2. Russian APT groups

Different APT groups, almost certainly sponsored by the Russian Government, have been identified by security researchers and Western governments for years. It is important to highlight here the "almost certainly", as attribution is a difficult process in which we must work with probabilities [16]. In this sense, Thai CERT, the national CSIRT for Thailand, publishes [17] an online resource which creates full profiles of all threat groups worldwide. By selecting the Russian strategically motivated threat groups that are identified as active (this is, whose activity has been seen in 2020 or later), the groups shown in Table 1 are found. A brief description of the main Russian threat groups is presented next. It is important to highlight that one single threat group has multiple names, depending on the company or organization that analyzes it [18].

Being active since 2008 [19], APT29 is a cyber espionage group probably linked to SVR [20]. Through a wide arsenal of malware, this threat actor targets Western governments and related organizations (political think tanks, governmental subcontractors, etc.).

Energetic Bear, also known as Dragonfly, is a Russian state–sponsored actor that has been conducting espionage campaigns targeting the energy sector since 2010 [21]. Probably linked to FSB, Energetic Bear conducts global intelligence operations and performs cyberspace attack campaigns [22] [23].

Gamaredon, almost certainly linked to FSB, has been one of the most active Russian groups targeting Ukraine during the 2022 conflict [24]. It is exclusively active against targets in Ukraine, especially military and government organizations [16]. However, its activity is prior to the Russian 2022 invasion [9] [25]: its first operation was discovered in 2013 [26]. Gamaredon's tactics and techniques are not sophisticated and its operational security is poor [16] compared to other Russian actors, such as APT28 or APT29.

InvisiMole in an actor probably linked to FSB's Gamaredon [27]. It is engaged in cyber espionage activities against the military and diplomatic, particularly targeting Ukraine and other Eastern Europe victims [28].

Also linked to FSB, TURLA is the oldest active Russian group to date, as it has been active since 1996 [29]. TURLA performs highly targeted operations [30] against a wide range of industries and governments. This threat actor has high technical skills. It has developed a complex ecosystem of tools and artifacts, and it is able to control its zombies even through satellite communications [31] [32] [33].

GRU Unit 74455 is also known as Sandworm, an APT group that has been considered "the Kremlin's most dangerous hackers" [34]. Sandworm performs not only cyberspace exploitation, but also cyberspace attack campaigns targeting critical infrastructures [35] [36] [37].

In addition to APT29, APT28 stands out as one of the most renowned Russian APT groups. Linked to GRU Unit 26165, security providers have extensively analyzed APT28 since 2014 [38] [39] [40] [41]. Focused on cyber espionage campaigns, APT28 (again, together with APT29) was responsible for the US Democratic National Committee hacking in 2016 [42] [43].

TEMP.Veles, also known as Xenotime, is a threat group linked to the Central Scientific Research Institute of Chemistry and Mechanics, a Russian government–owned technical research institution [44]. This group has been attributed TRITON, the first Industrial Control System cyber attack, in 2017, on safety instrument systems [45] [46]. TEMP.Veles is an example of the Russian cyber intelligence complex ecosystem: a scientific research institute, not an intelligence or military service, performing advanced offensive cyberspace operations from Russia.

Although Cloud Atlas, named after the use of cloud services for data exfiltration [16], is considered a new iteration of Red October, they are not entirely the same [47]. Its main cyber espionage

Table 1.
Russian strategically–motivated threat groups.

Group	Motivation	First seen	Last seen	Affiliation
APT29	Information theft and espionage	2008	2022	SVR
Energetic Bear	Sabotage and destruction	2010	2020	FSB VCh 71330 (Center 16)
Gamaredon	Information theft and espionage	2013	2023	FSB
InvisiMole	Information theft and espionage	2013	2022	FSB
Turla	Information theft and espionage	1996	2022	FSB
Sandworm	Sabotage and destruction	2009	2023	GRU VCh 74455
APT28	Information theft and espionage	2004	2022	GRU VCh 26165
TEMP.Veles	Sabotage and destruction	2014	2022	MOD Central Scientific Institute of Chemistry and Mechanics
Cloud Atlas	Information theft and espionage	2012	2022	N/A
Saint Bear	Information theft and espionage	2021	2022	N/A

victims are high profile targets located in Russia and other ex Soviet Republics [47]. Since the escalation of the conflict between Russia and Ukraine in 2021, and especially after the outbreak of war in February 2022, Cloud Atlas has been mainly focused on Russia, Belarus and conflicted areas of Ukraine and Moldova [48].

Finally, Saint Bear is a cyber espionage group mainly focused on government and military organizations from Ukraine and Georgia. Its intrusions are conducted to support Information Operations to create public mistrust and to degrade government ability to counter Russian cyber operations [49] [50]. Some of its tactics and techniques are similar to APT28. This fact, together with the analysis of Saint Bear's goals, leads to consider this group somewhat related to GRU [49] [27], although affiliation has not been stated with high confidence.

2.3. MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. This knowledge, contributed by analysts all around the world, can be used as the base for the development of specific threat models and methodologies. Started in 2013 and published in 2015, ATT&CK develops a process for modeling an adversary's post-compromise behavior at a fine level. A description of the framework and the work performed can be found at [51].

Tactics specify what a threat actor is doing, at the highest level of description, to accomplish a certain mission. Techniques specify how tactics are implemented, and procedures describe a particular implementation of a technique. These tactics, techniques, and procedures represent the behavior of a threat actor from the highest level description (tactic) to the lowest level one (procedure). MITRE ATT&CK framework is today's de facto standard to structure tactics and techniques of advanced threat actors. As of March 2023, MITRE ATT&CK had defined 14 enterprise tactics –those related to the activities of an attacker onto its victim– and 193 enterprise techniques associated with those tactics.

Beside tactics and techniques, ATT&CK identifies software (a generic term for tools, artifacts, malware, etc.) that can be used to implement one or more of the techniques, and which is out of the scope of this work.

In the ATT&CK Matrix for Enterprise, the framework represents tactics as the adversary's tactical goals for acting [52]. Although ATT&CK does not provide a kill-chain approach to specify the arrangement of tactics, most of them are presented in the logical order that a threat actor follows in hostile operations. All of them can be achieved through different techniques, and a single technique that can be associated with one or more tactics. There is no formal structure in MITRE ATT&CK for techniques in each tactic, all of them being represented in a plain view. For example, for the Command and Control tactic, representing the goal of enabling the remote control of the compromised infrastructure, the framework identifies techniques such as Data Encoding, Data Obfuscation, Protocol Tunneling, or Remote Access Software. The structure of tactics and techniques in MITRE ATT&CK allows analysts to organize which adversarial actions belong to specific techniques and tactics, thus helping defensive teams to understand what a threat actor may be trying to achieve, how this actor is trying to achieve it and how to better defend against the threat [53].

MITRE ATT&CK also links APT groups to tactics, techniques and software. With 135 identified groups at the time of this writing, all of them are named, aliased, described, and linked to specific techniques (including pre–attack and mobile) and software. In this way, an analyst can establish relationships between those entities to model an adversary and its activities against a target and, most importantly, to establish the defense mechanisms to prevent, detect, and respond to a threat.

MITRE ATT&CK represents an enormous effort to provide to the community a unified framework to identify the activities of advanced threat actors, from their TTP to the software they use, correlate information among those entities, and improve, not only the knowledge about APT, but also the defense mechanisms required for their detection and response. It constitutes a framework that, as usual, has to be improved with continuous work and contributions; in this sense, in MITRE ATT&CK a more defined structure for techniques inside each tactic is missed. The standard specifies all relevant tactics but, for each of them, all related techniques have a plain structure, broken only by the specification of sub techniques and by implementations of specific techniques.

3. The issue

The tools and artifacts related to the post compromise of a target by an APT group, widely known as post exploitation [54] [55], are well–known by security researchers, as they have been largely addressed in scientific literature [56] [57] [18]. However, the infrastructure and capabilities that are provisioned and staged by the threat actor before the initial compromise are a research line that has not been properly addressed. This situation can be due to the fact that the processes, and even the infrastructures, related to the resource provisioning of a threat actor are external to the targeted infrastructures, so their acquisition and analysis for forensic purposes are not as common as the ones of the arsenal deployed on the target.

To execute a majority of cyberspace operations, APT groups have to provision, stage, operate and maintain external infrastructure, often well in advance of their initial access to the target. Provisioning is related to the acquisition of infrastructure, while staging is related to the customization of a provisioned element, tailoring it for a particular goal or operation. After staging, the infrastructure must be maintained as long as it is needed for the operation's success, and even destroyed once it is no longer needed. Provisioning is in most cases operation–independent, and it can be executed identically for most operations, while staging is dependent on a particular operation. Please note that that while the provisioning processes might seem identical across different operations, the infrastructure elements being provisioned may not necessarily the same. It is uncommon for APT groups, especially for Russian ones, to reuse infrastructure between operations, as doing so could potentially introduce Operational Security (OPSEC) risks. The identification and modeling of external infrastructure elements, and the associated tactics and techniques to use them, from their initial provisioning to the final clean up, are relevant to improve the characterization of advanced threat actors, thus also improving their detection and accurate neutralization.

This external infrastructure has four main goals:

1 The initial compromise of the target, through a delivery and exploit infrastructure.
2 The continuous control of the target, through command and control (C2) infrastructure.
3 The information leakage from the target, through exfiltration infrastructure.
4 The concealment of threat actor's real infrastructure, so hindering attribution.

Initial access, C2 and exfiltration are tactics that can be performed through multiple different techniques, and the external infrastructure required in each case depends on the particular technique used in each case. For example, Russian APT groups are able to exploit multiple initial access techniques, such as supply chain compromise or baiting, where the required external infrastructure differs from that used on phishing or watering hole operations. However, the most common mechanism for initial access is to send a piece of malicious code to the victim through a delivery infrastructure, typically in the form of spear phishing. For exfiltration and C2 purposes, threat actors usually rely on the use of different external servers to communicate with from the targeted infrastructure. For this reason, we are describing these kinds of techniques.

Delivery is usually performed through an e–mail with a link or an attached stage–1 malware. When accessing this malicious object, the victim downloads and executes malicious code, staged on an external server. This server hosting the malicious code is known as exploit server [58]. Please note that delivery is a tactic that can be performed without particular delivery infrastructure. The required infrastructure depends on the technique exploited to achieve delivery.

In the persistence stage of the operation, the threat actor also requires external infrastructure. As it has been stated, this infrastructure is used for two main purposes: data exfiltration and C2. Both tactics can be performed by equivalent mechanisms and protocols, such as HTTP(S) or DNS. The compromised systems of the targeted infrastructure, known as zombies, connect to exfiltration and C2 servers through common protocols and with stealth mechanisms, in order to go unnoticed. As with delivery, depending on the exfiltration and C2 particular techniques, it is possible to face operations without particular persistence infrastructure.

Finally, external infrastructure provides Operational Security (OPSEC) to the threat actor. The communications between the external infrastructure and the threat actor's premises are not direct, nor are the communications between the threat actor and its target. These communications are performed through elements that harden the traceability of the actor, in order to hinder the acquisition of technical intelligence.

In Figure 1 the external architecture of an operation, including delivery infrastructure, exploit, C2 and exfiltration servers and OPSEC infrastructure, is shown. Please note that the only mandatory element is the OPSEC infrastructure. Although from a technical point of view a threat actor could connect directly from its premises to its target, this would be considered a huge OPSEC error. For this reason, no campaign where an APT group connects to its victim from its real infrastructures has been identified to date. The other elements are conditional to the particular operation and its associated techniques. As it has been previously stated, not all initial access, C2 or exfiltration techniques require specific infrastructure. For example, threat actors could remotely connect to external facing services of the victim from an OPSEC infrastructure, so in this case no particular delivery, exploit, exfiltration or C2 external elements are required. However, most Russian operations follow the steps detailed in this section. In this point, it is important to highlight that the focus of this work are cyberspace exploitation operations, not cyberspace attack ones. Cyberspace exploitation is focused on information gathering, while cyberspace attack is focused on degradation, destruction and manipulation activities [59] that in some cases do not require data exfiltration.

To make this external infrastructure operational, a threat actor can develop multiple techniques. Elements such as exploit, exfiltration or C2 servers can be acquired, rented, compromised, etc. The same way, the required capabilities for these elements to work, such as connection networks, virtual identities or digital certificates, can be obtained through multiple mechanisms.

4. Techniques and limitations

Little research has been conducted to identify and align the provisioning and staging of external infrastructure used in APT campaigns. As we have stated in this work, the main focus for researchers has been malware and internal elements of a campaign.

As it has been highlighted before, MITRE ATT&CK is the main public effort to establish a classification for tactics and techniques used by threat actors. As on March, 2023, MITRE ATT&CK "Resource Development" tactic, last modified on 30th September 2020 and identified as TA0042, consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. These resources include infrastructure, accounts, or capabilities, and they can be leveraged by the threat actor to aid in other phases of the adversary life cycle. Inside the "Resource Development" tactic, MITRE ATT&CK includes a particular technique "Stage Capabilities", related to the setting up of capabilities that can be used during targeting. The summary of techniques linked to the "Resource Development" tactic is shown in Table 4.

MITRE ATT&CK includes into the "Resource Development" different particular techniques related to obtain or develop capabilities for an operation's success, such as malware, tools or exploits. We argue that these capabilities should be considered apart from public infrastructure for different reasons. First of all, these capabilities can not be considered public infrastructure. An exploit, a vulnerability and even malware is not publicly exposed on the Internet. Of course, they are mandatory elements in most operations, so they must be acquired in some way, but their public exposure is minimum. In addition, external infrastructure is available for general public: everybody can get a Virtual Private

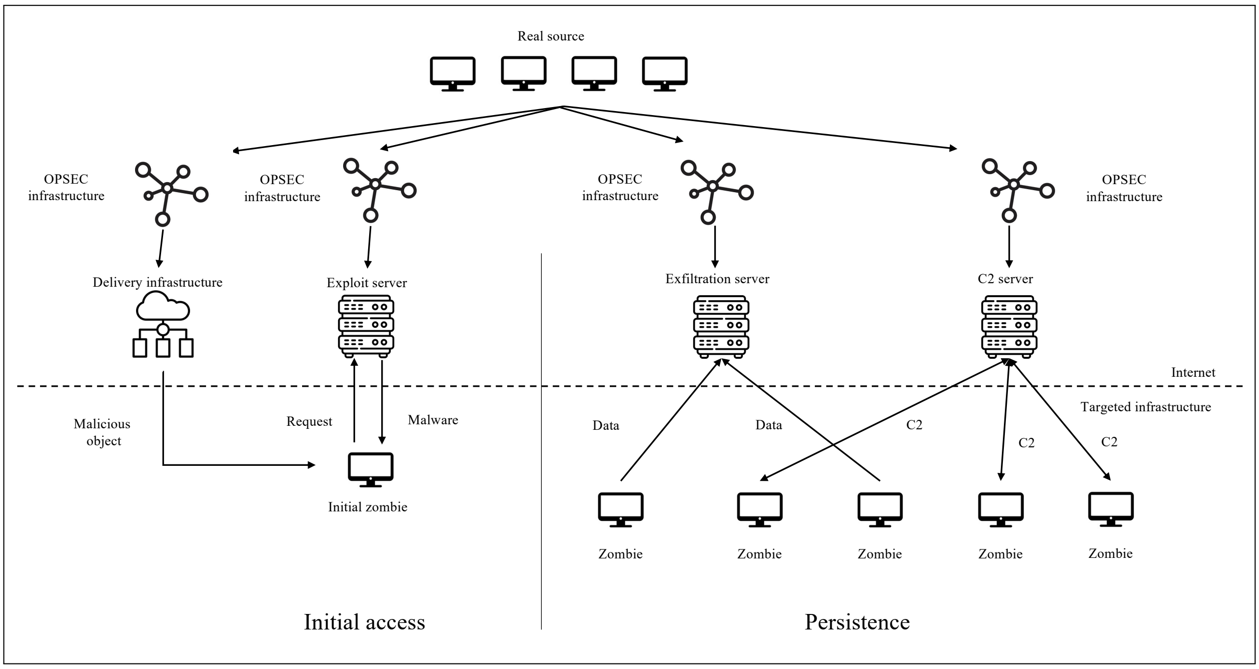

Figure 1. Common external architecture.

Server (VPS), a domain or a social network identity. Exploits or vulnerabilities are not, and they must be internally developed or acquired in black markets in most cases. For these reasons, the provisioning of these capabilities is out of the scope of this work.

In addition, in the case of the “Resource Development” tactic it has been found that MITRE ATT&CK mixes different concepts under the umbrella of techniques and sub techniques. The framework mixes the “what” is to be provisioned (a domain, an identity, a botnet, etc.) with the “how” it will be provisioned, this is, the technique (compromise, acquisition, etc.). It is important to differentiate both elements, as the same technique can be applied to get different elements for an operation and the same element can be obtained through multiple techniques. This mix of concepts has been found in more MITRE ATT&CK tactics, for example in “Reconnaissance”.

Finally, it is important for us to differentiate the provisioning and the staging of resources as two different tactics, not as a single one. MITRE ATT&CK includes the staging of capabilities as a technique inside the “Resource development” tactic. However, the framework addresses only the staging of capabilities, not the staging of infrastructure, such as domain names or virtual servers. We consider that staging should be addressed for external infrastructure, not just for capabilities. In addition, although MITRE ATT&CK does not provide an arrangement for the tactics considered in the framework, we advocate provisioning and staging are different tactics. Not only for clarity purposes, but mainly because as it has been stated before, provisioning is operation–independent and staging is fully linked to a particular operation. For this reason, their associated techniques are completely different.

In addition to the MITRE ATT&CK framework, no relevant analysis focusing on the provisioning and staging of external infrastructure for APT’s operations has been found in scientific literature. In [16] Timo Steffens provides an analysis of the required infrastructure to orchestrate an operation. The author states that threat actors can either compromise legitimate servers or rent their own, being the first approach the most convenient for staying anonymous. Steffens does not provide a comprehensive analysis of this infrastructure, focusing on a general description mainly from an attribution and OPSEC point of view, which is the core of his work. As it can be noted, external infrastructure is included in most references as an accessory element to analyze or discuss. However, as it will be detailed in this work, it is a key element to characterize APT groups and their operations, particularly for attribution purposes.

4.1. Russian APT groups' particular techniques

The particular techniques for the provisioning of external infrastructure for Russian APT's operations have been briefly addressed in multiple technical reports, although none of them is fully focused on this infrastructure. In this paper, public and private APT reports from security providers have been in–depth analyzed in order to identify relevant issues concerning external infrastructure. Some of the public reports have been found in the repositories shown in Table 2. Although the focus of this work are Russian APT groups, we consider that our findings can be applied to groups from all countries.

4.1.1 APT29

Concerning initial access to a target, in [60] French ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) exposes that APT29 performs phishing campaigns through the compromise of e–mail accounts. This technique is also exposed in [61]. In addition, this APT group abuses web services for mass mailing targets [62]. To compromise a phishing victim, APT29 registers domains to host malware [19], in some cases through typo squatting to masquerade legitimate ones [63] [61]. APT29 also compromises domains for malware hosting and delivery [63] [61].

Regarding persistence, APT29 employs different techniques for both exfiltration and C2 purposes, such as the compromise of web servers [64] [65] [19] [63] [66], domain registering [64] [67] [68] [69] and VPS acquisition [70] [66] [71] to stage a C2 server. In some cases, the registered domains are dynamic ones, through the abuse of free providers [72]. They also use legitimate cloud services, such as Dropbox, OneDrive or Twitter, in their operations, and even algorithmically generated Twitter handles [73] [19] [62] [65] [68]. This group has created self-signed digital certificates to enable mutual TLS authentication for the communications between the C2 servers and the malware [74] [75].

Finally, concerning OPSEC infrastructure, APT29 abuses TOR services in certain operations [63] [19].

4.1.2 Energetic Bear

Regarding initial access, Energetic Bear compromises legitimate web sites for watering hole purposes [76] [77]; those sites are related to the targeted sector, in order to ease the compromise of targets [78] [79]. In [80] US Cybersecurity & Infrastructure Security Agency (CISA) states that Energetic Bear registers new domains to target their victims; this techniques is also discussed in [77], where the authors state that Energetic Bear uses typo squatting or punnycode techniques to make their registered domains look as legit ones. CISA also exposes that Energetic Bear compromises legitimate

Table 2.
Public repositories for APT reports.

Repository	Address	Accessed on
APT Groups and Operations	https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit	04 January 2023
MITRE ATT&CK	https://attack.mitre.org/	14 January 2023
ETDA Threat Group Cards: A Threat Actor Encyclopedia	https://apt.etda.or.th/cgi-bin/aptgroups.cgi	14 January 2023
APTMAP	https://andreacristaldi.github.io/APTmap/	06 May 2023

e–mail accounts for spear phishing purposes [79].

In [81] Joe Slowik states that Energetic Bear compromised legitimate websites to host C2 infrastructure and malware modules. This technique has been also exposed in [82]. Also for C2 purposes, the author states that Energetic Bear has acquired Virtual Private Servers (VPS) to be used in their campaigns; this technique is also exposed in [83] and [79]. The group also uses VPS for exfiltration purposes [80]. Energetic Bear also creates identities and registers domains for C2 purposes [84] [77]. This group also compromises routing infrastructure for collection or C2 purposes [85] [86].

Regarding OPSEC infrastructure, Energetic Bear connects to public facing applications through different IP addresses, probably related to VPS infrastructure [80].

4.1.3 Gamaredon

Gamaredon primarily makes use of compromised domains, dynamic DNS providers, Russian and Ukrainian country code top–level domains and Russian hosting providers to distribute their malware [87]. In addition to compromised domains, Gamaredon also registers new domains for the staging of payloads [88] [89] [90] [91], and they also rent VPS for malware distribution [92] [91]. The group also registers fake e–mail addresses for phishing purposes [91] [93].

Domain registering for C2 purposes is also a Gamaredon widely used technique [88] [89] [94] [93] [95] [96]. In some cases, domain registering is performed through free dynamic DNS providers [97] [93]. Gamaredon also compromises domains for C2 purposes [94]; the group has not only compromised legitimate domains, but also hijacked command and control infrastructure from Iranian APT groups [98]. This group also uses VPS for C2 purposes [93] [95] [96], in some cases from a short list of Russian hosting providers [99]. Gamaredon has abused public services for DNS domain resolution in C2 stage, as well as Telegram accounts [95] [96].

4.1.4 InvisiMole

In [100] Zuzana Hromcová provides a description of the malware used by Invisimole, indicating that C2 is performed through the registering of Dynamic DNS names. Similar conclusions are shown in [28].

Related to malware distribution, in [93] the use of acquired VPS is exposed. It is important to highlight that, in addition to the APT group, Invisimole is also the name of the spyware they use to acquire information from their targets. This malware has been also used by other Russian APT groups such as Gamaredon [101], so there is some kind of connection between them .

4.1.5 TURLA

TURLA resource provisioning is mainly based on the compromise of external infrastructure for all purposes. TURLA compromised domains for watering hole [102] [103] [104] [105], as well as routers for malware distribution [106]. It also uses VPS [107] for malware delivery, as well as free DNS domains [108] [109] hosted on VPS.

In [30] and [110] Matthieu Faou states that this APT group usually relies on compromised sites as first stage web servers for C2 purposes, frequently including WordPress sites [111]. The use of compromised sites for C2 purposes is also exposed in [111] [112] and [113]. This APT group has even compromised satellite links to C2 their zombies [32].

For C2 and exfiltration purposes, TURLA has created web accounts including Dropbox and GitHub resources [114]. Together with Gamaredon, this is one of the few APT groups that has hijacked infrastructure from other threat actors: it has been found that TURLA used Iran APT34's C2 infrastructure for its own benefit [115] [116] [117]. This group also compromises legitimate web servers for C2 purposes [102] [118] [105] [119] [120] [121] [122]. In addition to domain compromise, TURLA also uses VPS and dynamic DNS registered names for C2 purposes [123], as well as public resources for connectivity check [118]. They have also abused legitimate services, such as Instagram, for C2 [105].

4.1.6 Sandworm

In [124] Scott W. Brady identifies different techniques for the provisioning and staging of infrastructure in Sandworm's operations. This group register domain names and create web resources designed to mimic legitimate websites, in order to steal credentials of targeted users. Sandworm also creates and maintains social media and e–mail accounts for different purposes during an operation, such as mimicking legitimate organizations for spear phishing campaigns or disseminating stolen data. Scott W. Brady also states that this complex APT group has leased infrastructure through resellers to enable its operations, instead of leasing it directly from hosting companies. Related to this tactic, [124] states that Sandworm Team conducted technical research related to vulnerabilities associated with websites used by their targets.

Regarding initial access, Sandworm has used public mail providers, such as Protonmail and mail.com to register identities [125]. In the same work, Kaspersky researches state the use of these identities to register network domains for phishing purposes, as well as VPS as name servers to orchestrate the initial access. The registering of domain names for initial access is also discussed in [126]. Sandworm also compromises legitimate web servers for malware delivery [127], through different vulnerabilities [126] [128] [129].

In [130] UK National Cyber Security Centre states that Sandworm has established large botnets targeting domestic network devices, such as routers, for C2 purposes. The group has also abused public services such as Google+ to accomplish this tactic [131].

In [132], ESET researchers exposed that Sandworm uses Protonmail accounts for the communication between the threat actor and its targets in destructive operations. The same work shows the use of public resources, such as Telegram, abused my malware authors for C2 purposes.

For OPSEC purposes, Sandworm has used public Virtual Private Network (VPN) services to access their infrastructure [125]. In addition to these public VPN services, Sandworm connects to its targets through the TOR network [128].

4.1.7 APT28

In [133] Shane Huntley presents different provisioning techniques used by APT28. Resource compromising is one of the most relevant ones, as this threat actor compromises e–mail accounts for phishing purposes [134]. Huntley also states that APT28 creates Blogspot resources as an initial landing page for their campaigns, and they also register domains imitating organizations that could be interesting for their victims. This last technique is also discussed in [39]. In addition, for APT28 resource compromising is a technique not only related to e–mail accounts. In [41], researchers from FireEye state that APT28 also compromises legitimate web sites to infect its victims. In addition, APT28 has used commercial VPN infrastructure to compromise its targets [135] [134], as well as dedicated staged infrastructure to host registered domains for phishing purposes [134].

APT28's initial access is performed through the registering of domain names for phishing purposes [136] [137]. The group has also abused legitimate web services, such as OneDrive, to accomplish this tactic [138].

APT28 has used botnets both for OPSEC and C2 purposes [139], particularly when targeting IoT devices [140]. Also regarding C2, APT28 has registered domain names and rented VPS to host these domains as web infrastructure [141] [137] [142] [143] [144] [145] [146] [136]. In [147], Kaspersky researchers state that C2 domain registering is performed through providers with privacy settings, that accept bitcoins and that do not perform security checks during the registration; the identities used for this registration are e–mails from public providers, and SSL certificates to stage C2 web servers are generated on rented VPS. In addition, APT28 has used public web services for beaconing [142] or other C2 purposes [138].

Members of APT28 (GRU VCh 26165), together with members from GRU Unit 22177, were detected and neutralized in The Hague in 2018. This is one of the few close access operations publicly exposed. When the operation was thwarted, Dutch authorities confiscated different hacking equipment. Some of this equipment were purchased in The Hague [148], and it was especially configured to hack WiFi networks [149].

4.1.8 TEMP.Veles

Little information can be found on public sources regarding TEMP.Veles external infrastructure. For C2 purposes, this group has used Virtual Private Servers (VPS), and they have registered their own domains [150]. In addition, for the same purpose, TEMP.Veles compromises legitimate infrastructure [151].

4.1.9 Cloud Atlas

In [48], CheckPoint researchers state that Cloud Atlas mainly establishes accounts in public services, such as e–mail providers, for initial access, or cloud providers for C2 purposes. In addition to cloud providers, the threat actor also acquires domain names and purchases VPS infrastructure to store malware for initial access and to stage C2 capabilities [152] [153] [154] [155] [156], through the registering of e–mail addresses in public providers.

For C2 purposes, Cloud Atlas registers domain names and host web servers into VPS in different countries [157]. The group also abuses cloud providers to stage its C2 infrastructure, registering them through fake e–mail accounts [158]; the range of these cloud providers has been diversified through years [159].

Regarding OPSEC, Cloud Atlas' C2 infrastructure is based on a chain of servers working as proxies and hiding the location of the true C2 server [157]. The group also uses chains of infected routers to act as proxies and mask communications between the attackers and the cloud service providers they use [159].

4.1.10 Saint Bear

In [160], Unit42 researchers state that Saint Bear registers domain names to store malware for initial access and for C2 purposes. In the same work, it is stated that the threat actor also steals legitimate certificates to sign malicious payloads. Saint Bear's initial access is also accomplished through the abuse of legitimate services to store malware [161] [162] [163] [164] and through the registering of domain names [161] [165] [163] [166]. The registration of domain names is not only linked to malware delivery, but also to phishing campaigns [166]. Saint Bear's identities are created through the abuse of public mail providers.

For C2 purposes, Saint Bear has registered domain names [163] [167] and purchased VPS infrastructure [165] [168] to host them. Exfiltration is also performed through VPS [166].

4.1.11 Summary

To identify this initial set of provisioning techniques, a qualitative approach has been followed. In first place, information has been gathered from MITRE ATT&CK. However, as it has been noted, this framework lacks different approaches to the provisioning of infrastructure, so the second, and main, source for data collection has been the examined reports about Russian APT groups and operations. In this way, the techniques exposed in this section have been identified. In Table 5 a summary of these provisioning techniques for Russian APT groups is shown, linking each of them with the particular resource that is provisioned and with the tactic it is used for. The main references that show this relationship are also presented.

5. A structure proposal for provisioning techniques

Once the review of external infrastructure of Russian APT's operations has been performed, it is mandatory to analyze in first place its life cycle. This life cycle represents the tactics that must be executed by a threat actor to make the infrastructure elements available during an operation. From our previous analysis, the following tactics have been identified:

- Provisioning. Obtaining the required resources to perform an operation.
- Staging. Setting up the required resources to perform an operation.
- Operation and maintenance. Keeping these resources fully operational as they are useful for the operation purposes.
- Clean up. Removing the infrastructure elements once they are no longer needed.

In order to render an infrastructure element available for a particular operation, it must be initially provisioned and staged, configured to serve a specific purpose, such as facilitating delivery or enabling exfiltration. As it has been previously stated, it is important to differentiate between provisioning and staging. Staging techniques are not independent from provisioning ones, and they are even linked to the particular infrastructure element to be deployed. Nevertheless, we argue that these two tactics should be distinguished, as they can be executed by different teams and their linked techniques are also different. In addition, we must highlight that all infrastructure elements must be provisioned and staged, but the technical procedures for each of them are different: for example, the provisioning and staging of an e–mail account are different from the provisioning and staging of a VPS.

Once staged, the infrastructure element is ready to work. From this moment, the threat actor operates and maintains the element as long as it is useful for the threat actor's purposes. At this point, it is important to highlight that advanced threat actors do actively monitor their infrastructure not particularly for availability purposes, but mainly to identify suspicious accesses that can be related to a compromise discovery and analysis. If this situation occurs, the infrastructure related to an operation, both external and internal, is usually removed. This removal is also performed when the element is not longer required, in order to hinder the acquisition of technical intelligence if it is discovered. These tactics are not particular to the infrastructure of APT groups and operations: it is possible to find the same ones when dealing with IT infrastructure for any legitimate purpose, from setting up a web server to register a virtual identity. The key difference here is not only the goal, but mainly the OPSEC considerations that advanced threat actors take into account to hinder their discovery and attribution. Finally, it is important to note that the life time of a particular infrastructure element can not be the same as the life time of the whole operation: not all provisioned items are useful during all the operation, so they can be removed before the operation finishes.

The life cycle of external infrastructure, in the form of arranged tactics, is shown in Figure 2.

Although all the tactics in this life cycle are important for a threat actor, the most relevant one from a modeling point of view is provisioning. Staging techniques are related to setting up a provisioned infrastructure element, and apart from OPSEC considerations, they are the same ones that would be executed to set up legitimate infrastructure. Operation and maintenance are related to the normal behavior of the infrastructure, and their associated techniques are not relevant for the characterization of the threat actor (once again, apart from OPSEC considerations). Related to the clean up of the infrastructure, although it is an important tactic to perform once an element is no longer useful (for example, because the operation has been detected), it is not mandatory for an operation's success. In this case, the associated techniques to perform the infrastructure elements' clean up are those linked to Cyberspace Attack techniques, particularly Destruction.

Provisioning stands as an essential tactic demanding consideration when characterizing an operation. For this reason, this work primarily delves into the analysis of provisioning as a key tactic for cyberspace operations. Through the comprehensive analysis of technical reports pertaining to APT operations, two key elements necessitate attention in this analysis: the inherent components of the infrastructure and the techniques employed for their provisioning. Infrastructure elements encompass the technical assets earmarked for operation employ-

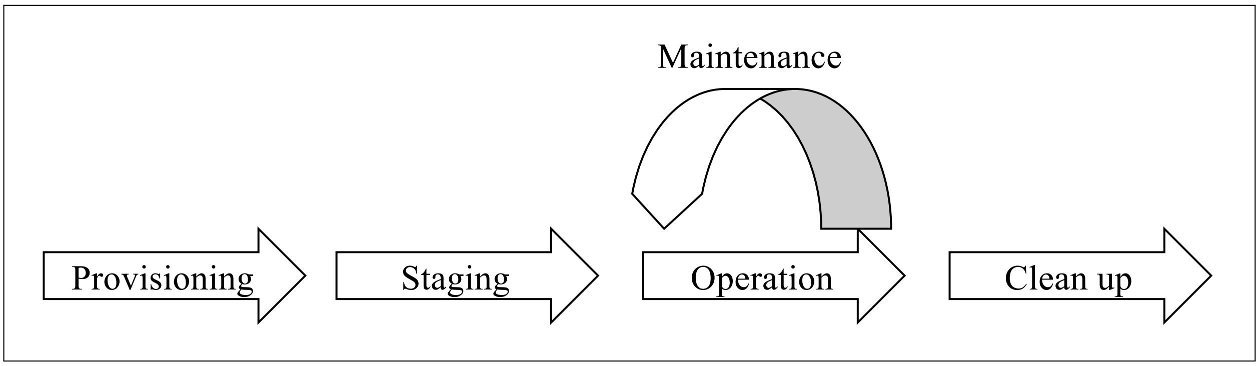

Figure 2. Infrastructure life cycle.

ment, while provisioning techniques encompass the procedures undertaken to secure each infrastructure element. It is important to note that not all techniques are universally applicable across all infrastructure elements.

In Table 5 the infrastructure elements and the techniques used to their provisioning by Russian APT groups are detailed. A summary for all of them is shown in Table 3.

It is important to highlight that the infrastructure items and their associated provisioning techniques exposed in Table 3 are just the plain listing of the analyzed ones. To provide an accurate identification, it is mandatory to structure both elements into a taxonomy. Infrastructure items are not independent between them, and some provisioning techniques are also linked to particular infrastructure elements. For example, to register a domain name it is mandatory to obtain in first place a valid e–mail account, while to host a domain name it is mandatory to acquire hosting infrastructure, such as a VPS.

To structure items and techniques, we propose in first place a hierarchy for infrastructure items. In our analysis, the following key elements have been identified:

- Virtual identities, mainly based on e–mail accounts. These virtual identities are used by Russian threat actors to register into public services and to use them in an anonymous way. Related to this category, it is possible to identify registered accounts on public platforms, in addition to e–mail accounts, which are the basis of virtual identities.
- Private infrastructure, controlled by the threat actor and mainly based on servers that host domains providing web services. Related to this category, it is possible to find domains, VPS, web servers and digital certificates.
- Public infrastructure which is not under the APT group's control and that is being abused by the group, with or without previous registration. Under this category it is possible to find all public services exposed to Internet, particularly web ones, abused by threat actors. Abuse is mainly for C2 purposes (beaconing, internet connectivity checks, etc.), and it can be performed with our without registering into the service.
- Communications infrastructure between the target and the threat actor. Related to this category it is possible to identify VPN services, TOR infrastructure, botnets, routing infrastructure and even satellite links.

It must be highlighted that we are not considering

Table 3.
Infrastructure items and their associated provisioning techniques.

Item	Provisioning techniques
E–mail accounts	Compromise
	Registration
Public services	Abuse
	Registration
Domains	Registration
	Compromise
Web servers	Compromise
	Hijacking
VPS	Purchase
	Hijacking
Digital certificates	Generation
	Stealing
TOR	Abuse
Routing infrastructure	Compromise
Satellite links	Compromise
Identities	Registration
Botnets	Compromise
VPN	Abuse
Physical elements	Purchase

physical elements and their purchase, as they are not pure remote infrastructure resources to execute the operations, but mandatory elements to physically support them.

Regarding provisioning methods, seven techniques have been identified in our analysis:

- Compromise of external infrastructure that is being used for legitimate purposes.
- Hijacking of external infrastructure that is being used for non–legitimate purposes. Hijacking can be considered a sub technique for compromise. It has a key difference that must be highlighted: the original purpose of a hijacked infrastructure item is not legitimate.
- Stealing of legitimate infrastructure. Stealing can be also considered a sub technique for compromise. We differentiate it because stealing involves a copy of the original infrastructure item to be used apart from the original. In addition, the stealing technique is linked to particular infrastructure elements, such as digital certificates,
- Abuse of public legitimate services to achieve the threat actor's goals.
- Registration on public legitimate services to achieve the threat actor's goals. Registration can be considered a sub technique for abuse. We differentiate these two techniques because the registration to abuse public services requires virtual identities.
- Purchase of infrastructure, typically by renting it through virtual identities and digital currencies, in order to enhance OPSEC.
- Generation of new infrastructure to achieve the threat actor's goals. It is important to highlight the difference between Registration and Generation. To generate new infrastructure elements, the threat actor is autonomous, while to register new infrastructure elements the threat actor relies on a service provider, the registrar.

The hierarchy of the identified provisioning techniques is shown in Figure 3. As it can be seen, Russian APT groups compromise, purchase, abuse and generate external infrastructure for their operations. This external infrastructure is divided into virtual identities, public and private infrastructure, and communications infrastructure. All of these items, as well as their associated provisioning techniques, are relevant for the characterization of an APT group, particularly for attribution purposes. For example, when facing an incident where a web server has been compromised for initial access, the probability that we are facing a Saint Bear operation is low. In addition, it is possible to identify what we define as points of singularity: infrastructure elements and their associate provisioning techniques that are linked only to a specific group. For example, if we are facing an incident where satellite links have been compromised for persistence purposes, the probability that we are facing TURLA is very high, as no other groups are using this kind of external infrastructure. Certainly, these attribution assumptions should be complemented by the examination of additional techniques, alongside an analysis of non–technical factors, such as goals and information requirements.

Although the characterization of threat actors and operations is particularly useful for attribution purposes, it is also a relevant element for the detection and neutralization of operations. By identifying the external infrastructure that is provisioned and exploited by specific APT groups, the likelihood of detecting a potential compromise through threat hunting techniques is enhanced.

5.1. Aligning with MITRE ATT&CK

To discuss the completeness and correctness of our work, we have mapped MITRE ATT&CK "Resource Development" techniques to our proposed approach. Being this framework the main industry reference for the analysis of threat actors' tactics and techniques, it is important to align our proposal with MITRE ATT&CK in order to make our results as practical as possible, thus helping to improve the framework.

MITRE ATT&CK "Resource Development" techniques have been previously shown in table 4. As it has been stated, the framework mixes different concepts regarding the "How", the techniques, and the "What", the infrastructure elements to be provisioned or staged. In addition, MITRE ATT&CK considers staging as a particular technique for the "Resource Development" tactic, while we argue that Provisioning and Staging are two different tactics for an offensive operation.

Related to provisioning techniques, the main ones that MITRE ATT&CK defines are acquisition, compromise, development, establishment and obtaining. These techniques are fully aligned with our proposal, establishing a direct relationship between acquisition (purchase), compromise (compromise), development (generation), establishment (registration) and obtaining (purchase). As we can see, the Abuse, Hijacking and Stealing techniques are not considered in the framework. While hijacking and stealing are sub techniques for Compromise and their absence can be due to the granularity of the framework, the Abuse technique is a lack of MITRE ATT&CK. This lack can hinder the attribution of operations performed by APT groups that are abusing public services for C2 or OPSEC purposes, such as Sandworm and APT28.

What MITRE ATT&CK identifies as sub techniques are in fact infrastructure elements provisioned in each case through their main technique. Except for malware, tools, exploits and vulnerabilities, all of these infrastructure items are identified in our proposal. These elements are out of the scope of this work. Although they are provisioned and staged, they can not be considered external infrastructure, but capabilities to achieve the threat actor's goals that can be used against external and internal infrastructure.

As we can verify, all techniques and subtechniques identified by MITRE ATT&CK for the "Resource development" tactic can be mapped to our proposal. Our analysis provides not only this full coverage, but also the ability to identify relevant

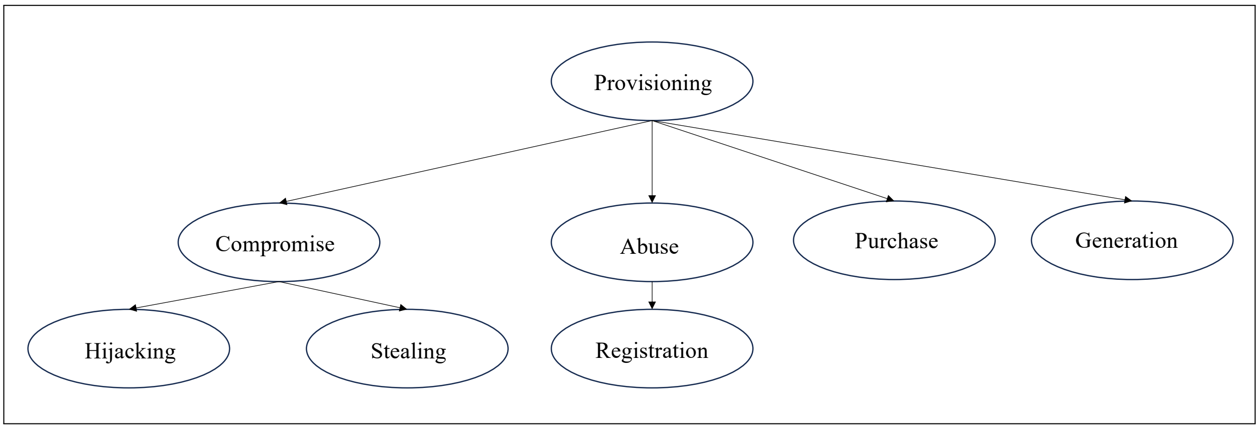

Figure 3. Provisioning techniques hierarchy.

techniques that are not considered by the framework and that can be very relevant for the characterization of APT groups and for the attribution of their operations.

6. Discussion

We have identified the absence of a suitable analysis of external infrastructure used by advanced threat actors in their operations. As we have stated, in front of internal capabilities (particularly, malware implants), external infrastructure is usually not properly addressed in scientific and technical literature. In fact, the main industry framework for the identification of advanced threat actors' tactics and techniques, MITRE ATT&CK, does not provide a suitable structure for provisioning techniques and infrastructure elements. This situation draws our attention, as the techniques related to the provisioning and even to the staging of external infrastructure are a key element not only for the attribution of APT operations, but also for its detection and neutralization. To fill this gap, in this paper, the provisioning of external infrastructure linked to Russian APT groups and operations has been analyzed and discussed.

From the comprehensive analysis of Russian APT groups and operations, their main external infrastructure elements have been identified, together with their provisioning techniques. In this work, four families of infrastructure have been defined: virtual identities created by the APT group, private infrastructure controlled by the APT group, public infrastructure abused but not controlled by the APT group and communications infrastructure abused or controlled by the threat actor, mainly for OPSEC purposes. To use this infrastructure in particular operations, it must be provisioned through different techniques. These techniques are based on the compromise of existing infrastructure to be controlled by the threat actor, the abuse of legitimate infrastructure which provide services to the threat actor, the purchase of ad hoc infrastructure for an operation and the generation of new virtual infrastructure to achieve the threat actor's goals.

The analysis of Russian APT provisioning techniques can be extrapolated to groups from other countries. In fact, from our own experience, resource provisioning techniques are common to all APT groups. However, each one of them executes different techniques for their operations, and these techniques are relevant for the characterization of a group and its operation, particularly for attribution. For example, different Chinese groups such as APT1 or Ke3Chan use Domain Generation Algorithms to generate domains for their operations [169], while this particular technique is not widely used among Russian groups.

To discuss the completeness and correctness of our work, we have mapped MITRE ATT&CK "Resource Development" techniques to our proposed approach. This framework is the main public effort to establish a classification for tactics and techniques used by threat actors. As on June, 2023, MITRE ATT&CK "Resource Development" tactic, identified as TA0042, consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. MITRE ATT&CK provides no structure for techniques inside this tactic; the framework places all of the associated techniques at the same level, providing only specific sub techniques.

Our approach significantly improves the analysis of APT operations and the characterization of advanced threat actors. External infrastructure is not only a key element for attribution, but also for the detection of compromises: many indicators of compromise are related to domains, IP addresses and even virtual identities, so the knowledge and analysis of these elements are imperative for an accurate detection.

Being MITRE ATT&CK the main framework for threat actor's tactics and techniques, as we have stated it draws our attention that the addressing of external infrastructure provisioning techniques can be highly improved. This fact, together with the few public available reports focused on external infrastructure, highlights the need of accurate analysis of infrastructure elements and their linked techniques; in this work we have delved into provisioning, but particularly relevant techniques, such as staging and clean up, should be addressed in future work. This complete analysis would provide a global picture of the use and abuse of external infrastructure by APT groups, so it would improve the characterization of advanced threat actors and their operations, as well as their detection.

Finally, in this section, we identify different relevant research lines to improve our work. The first one, as stated before, is the comprehensive analysis of other techniques linked to the external infrastructure, particularly staging and clean up. The abuse of cloud infrastructure is also an especially interesting research line, as the use of cloud elements (services, platforms and infrastructure) among all kind of organizations increases day by day. APT groups are aware of this situation and they also adapt their operations to use, and abuse, these cloud elements, particularly when targeting organizations that rely on cloud infrastructures [170]. Finally, it draws our attention that little research related to OPSEC infrastructure has been found. Being OPSEC a key requirement for APT's operations, such analysis must be also considered a particularly relevant research line. In fact, as we have stated, OPSEC is the only infrastructure that can be found in all operations, while delivery and persistence infrastructure are common but not mandatory.

7. Conclusions

The provisioning of infrastructure by Advanced Persistent Threats in their operations has not been adequately addressed in scientific literature. Our work fills this gap, identifying the key external infrastructure elements for APT operations and discussing the mandatory relevant tactics to make this infrastructure operational. Furthermore, we have delved into the techniques associated with one of these tactics, provisioning, since it stands as the first essential step when engaging with external infrastructure.

We have identified the main active Russian APT groups. Although attribution is a complex task in which it is mandatory to work with probabilities, most of these groups have ties with Russian Government. Their targets include all kind of organizations, from governments to private companies, where information is a valuable asset. Of course, this is an ongoing work, as new groups can emerge and existing groups can disappear, or just be identified by other name.

Once the main Russian APT groups have been exposed, the external infrastructure used by these groups in their operations has been in–depth analyzed. In this paper, four families of infrastructure items have been identified: virtual identities, private infrastructure, public infrastructure and communications infrastructure. Related to these items, we have identified the tactics and techniques that these groups are using in their operations. Although our work has been focused on Russian APT groups, the outcomes presented can be extended to the analysis of groups originating from other countries, such as China or Iran.

Four tactics for the management of external infrastructure have been identified: provisioning, staging, operation and maintenance and clean up. These tactics are used to make external infrastructure operational during an operation. Focusing on provisioning, their main associated techniques have been identified, as well as particular sub techniques: compromise, abuse, purchase and generation.

Our work improves the global knowledge of APT groups and operations. This knowledge can be directly applied to the modeling of groups and activities, particularly to the attribution process: the identification of a threat actor performing a particular operation. Through this modeling, our work enhances the detection and neutralization capabilities for all kind of organizations. In addition, the alignment of our work with MITRE ATT&CK, the main framework for the dissection of advanced threat actor's tactics and techniques, makes our findings ready to be directly used in industry threat modeling approaches.

References

[1] R. Ross *et al.*, *SP 800-39. Managing information security risk: Organization, mission, and information system view*. National Institute of Standards & Technology, 2011.

[2] P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in *Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings 15*. Springer, 2014, pp. 63–72.

[3] J. Carr, *Inside cyber warfare: Mapping the cyber underworld*. O'Reilly Media, Inc., 2012.

[4] K. Giles, "Information Troops. a russian cyber command?" in *2011 3rd International Conference on Cyber Conflict*. IEEE, 2011, pp. 1–16.

[5] M. Connell and S. Vogler, "Russia's approach to cyber warfare," [Online]. Available: https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf, Center for Naval Analyses, Tech. Rep., September 2016.

[6] V. Akimenko and K. Giles, "Russia's cyber and information warfare," *Asia policy*, vol. 15, no. 2, pp. 67–75, 2020.

[7] M. Grzegorzewski, "Russian cyber operations: The relationship between the state and cybercriminals," in *Historical and legal aspects of cyber attacks on critical infrastructure*, D. Caleta and J. F. Powers, Eds. Ministry of Defense, Republic of Slovenia, 2020, pp. 53–64.

[8] R. Morgus, B. Fonseca, K. Green, and A. Crowther, "Are china and russia on the cyber offensive in latin america and the caribbean? a review of their cyber capabilities and the implications for the US and its partners in the region," [Online]. Available: http://newamerica.org/cybersecurity-initiative/reports/russia-china-cyber-offensive-latam-caribbean/, Tech. Rep., July 2019.

[9] C. Cunningham, "A russian federation information warfare primer," [Online]. Available: https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/, Henry M. Jackson School of International Studies. Washington University, Tech. Rep., 2020.

[10] B. Lilly, *Russian Information Warfare: Assault on Democracies in the Cyber Wild West*. Naval Institute Press, 2022.

[11] V. Nagy, "The geostrategic stuggle in cyberspace between the united states, china, and russia," *Academic and Applied Research in Military and Public Management Science*, vol. 11, no. 1, pp. 13–26, 2012.

[12] S. Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. Georgetown University Press, 2022.

[13] R. Thornton and M. Miron, "Winning future wars: Russian offensive cyber and its vital importance," *The Cyber Defense Review*, vol. 7, no. 3, pp. 117–135, 2022.

[14] B. Lilly and J. Cheravitch, "The past, present, and future of russia's cyber strategy and forces," in *2020 12th International Conference on Cyber Conflict (CyCon)*, vol. 1300. IEEE, 2020, pp. 129–155.

[15] J. V. Brock and B. Zagaris, "Cybercrime, high-value art, and economic sanctions," *IELR*, vol. 36, p. 315, 2020.

[16] T. Steffens, *Attribution of Advanced Persistent Threats*. Springer, 2020.

[17] "Threat Group Cards: A Threat Actor Encyclopedia," [Online]. Available: https://apt.etda.or.th/cgi-bin/aptgroups.cgi, February 2023.

[18] A. Lemay, J. Calvet, F. Menet, and J. M. Fernandez, "Survey of publicly available reports on advanced persistent threat actors," *Computers & Security*, vol. 72, pp. 26–59, 2018.

[19] F-Secure, "The dukes: 7 years of russian cyberespionage," [Online]. Available: https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf, F–Secure, Tech. Rep., September 2015.

[20] I. Thornton-Trump CD, "Russia: the cyber global protagonist," *EDPACS*, vol. 65, no. 3, pp. 19–26, 2022.

[21] M. Pellegrino, "The threat of state-sponsored industrial espionage," [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/9de4b721-6256-43f0-b7df-988e3c4c9451, Tech. Rep., June 2015.

[22] K. Hemsley and R. Fisher, "A history of cyber incidents and threats involving industrial control systems," in *Critical Infrastructure Protection XII: 12th IFIP WG 11.10 International Conference, ICCIP 2018, Arlington, VA, USA, March 12-14, 2018, Revised Selected Papers 12*. Springer, 2018, pp. 215–242.

[23] J. E. Vinnem and I. B. Utne, "Risk from cyberattacks on autonomous ships," in *Safety and Reliability–Safe Societies in a Changing World*. CRC Press, 2018, pp. 1485–1492.

[24] D. Kapur, T. Shloman, R. Venal, and J. Fokker, "Cyberattacks targeting ukraine increase 20–fold at end of 2022 fueled by russia-linked gamaredon activity," *Global Security Mag*, 2023.

[25] M. Schwarz, M. Marx, and H. Federrath, "A structured analysis of information security incidents in the maritime sector," *arXiv preprint arXiv:2112.06545*, 2021.

[26] S. Nate and L. Leca, "Cybersecurity and hybrid warfare challenges in the black sea region," *International Journal of Cyber Diplomacy*, vol. 1, 2020.

[27] J. Juutilainen, "Cyber warfare: A part of the russo-ukrainian war in 2022," Ph.D. dissertation, JAMK University of Applied Sciences, September 2022.

[28] Z. Hromcová and A. Chereanov, "Invisimole: the hidden part of the story. unearthing invisimole's espionage toolset and strategic cooperations," [Online]. Available: https://web-assets.esetstatic.com/wls/2020/06/ESET_InvisiMole.pdf, ESET, Tech. Rep., June 2020.

[29] J. A. Guerrero-Saade, C. Raiu, D. Moore, and T. Rid, "Penquin's moonlit maze. the dawn of nation-state digital espionage," [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf, Tech. Rep., 2017.

[30] M. Faou, "Turla lightneuron. one email away from remote code execution," [Online]. Available: https://www.welivesecurity.com/2019/05/07/turla-lightneuron-email-too-far/, ESET, Tech. Rep., May 2019.

[31] A. Drozhzhin, "Russian-speaking cyber spies exploit satellites," [Online]. Available: https://www.kaspersky.com/blog/turla-apt-exploiting-satellites/9771/, Kaspersky, Tech. Rep., September 2015.

[32] S. Tanase, "Satellite turla: Apt command and control in the sky," [Online]. Available: https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/, SecureList, Tech. Rep., September 2015.

[33] D. Housen-Couriel, "Cybersecurity threats to satellite communications: Towards a typology of state actor responses," *Acta Astronautica*, vol. 128, pp. 409–415, 2016.

[34] A. Greenberg, *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Anchor, 2019.

[35] A. Carlsson and R. Gustavsson, "The art of war in the cyber world," in *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*. IEEE, 2017, pp. 42–44.

[36] E. Izycki and E. W. Vianna, "Critical infrastructure: A battlefield for cyber warfare?" in *ICCWS 2021 16th International Conference on Cyber Warfare and Security*. Academic Conferences Limited, 2021, p. 454.

[37] Y. Meijaard, P.-P. Meiler, and L. Allodi, "Modelling disruptive apts targeting critical infrastructure using military theory," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2021, pp. 178–190.

[38] L. Kharouni, F. Hacquebord, N. Huq, J. Gogolinski, F. Mercês, A. Remorin, and D. Otis, "Operation pawn storm: Using decoys to evade detection," [Online]. Available: https://documents.trendmicro.com/assets/wp/wp-operation-pawn-storm.pdf, Trendmicro, Tech. Rep., October 2014.

[39] FireEye, "Apt28: A window into russia's cyber espionage operations," [Online]. Available: https://services.google.com/fh/files/misc/apt28-window-russia-cyber-espionage-operations.pdf, FireEye, Tech. Rep., September 2014.

[40] ESET, "En route with sednit," [Online]. Available: https://web-assets.esetstatic.com/wls/en/papers/white-papers/eset-sednit-full.pdf, ESET, Tech. Rep., October 2016.

[41] FireEye, "Apt28: at the center of the storm. russia strategically evolves its cyber operations," [Online]. Available: https://www.

mandiant.com/resources/reports/apt28-center-storm, FireEye, Tech. Rep., January 2017.

[42] N. Inkster, "Information warfare and the us presidential election," *Survival*, vol. 58, no. 5, pp. 23–32, 2016.

[43] B. Jensen, B. Valeriano, and R. Maness, "Fancy bears and digital trolls: Cyber strategy with a russian twist," *Journal of Strategic Studies*, vol. 42, no. 2, pp. 212–234, 2019.

[44] F. Intelligence, "TRITON attribution: Russian government-owned lab most likely built custom intrusion tools for TRITON attackers," [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/triton-attribution-russian-government-owned-lab-most-likely-built-tools, Mandiant, Tech. Rep., October 2018.

[45] A. Di Pinto, Y. Dragoni, and A. Carcano, "Triton: The first ics cyber attack on safety instrument systems," in *Proc. Black Hat USA*, vol. 2018, 2018, pp. 1–26.

[46] J. Slowik, "Zeroing in on Xenotime: Analysis of the entities responsible for the TRITON event," in *2022 Virus Bulletin localhost*, September 2022.

[47] J. A. Guerrero-Saade, "Draw me like one of your French APTs – expanding our descriptive palette for cyber threat actors," in *2018 Virus Bulletin Conference*, October 2018, pp. 1–20.

[48] Checkpoint, "Cloud Atlas targets entities in Russia and Belarus amid the ongoing war in Ukraine," [Online]. Available: https://research.checkpoint.com/2022/cloud-atlas-targets-entities-in-russia-and-belarus-amid-the-ongoing-war-in-ukraine/, Checkpoint Research, Tech. Rep., December 2022.

[49] C. T. I. Team, "Who is ember bear?" [Online]. Available: https://www.crowdstrike.com/blog/who-is-ember-bear/, CrowdStrike, Tech. Rep., March 2022.

[50] J. Lelonek, "Analyzing russia's conventional and cyber operations in ukraine," Ph.D. dissertation, Utica University, 2022.

[51] B. E. Strom, J. A. Battaglia, M. S. Kemmerer, W. Kupersanin, D. P. Miller, C. Wampler, S. M. Whitley, and R. D. Wolf, "Finding cyber threats with ATT&CK™-based analytics," [Online]. Available: https://apps.dtic.mil/sti/trecms/pdf/AD1107945.pdf, MITRE Technical Report MTR170202. The MITRE Corporation, Tech. Rep., 2017.

[52] W. Xiong, E. Legrand, O. Åberg, and R. Lagerström, "Cyber security threat modeling based on the MITRE enterprise ATT&CK matrix," *Software and Systems Modeling*, vol. 21, no. 1, pp. 157–177, 2022.

[53] R. Al-Shaer, J. M. Spring, and E. Christou, "Learning the associations of mitre att&ck adversarial techniques," in *2020 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2020, pp. 1–9.

[54] T. Nelson and H. Kettani, "Open source powershell-written post exploitation frameworks used by cyber espionage groups," in *2020 3rd International Conference on Information and Computer Technologies (ICICT)*. IEEE, 2020, pp. 451–456.

[55] R. Benito, "An automated post-exploitation model for offensive cyberspace operations," Ph.D. dissertation, Monterey, CA; Naval Postgraduate School, 2022.

[56] I. Ghafir, V. Prenosil *et al.*, "Advanced persistent threat attack detection: an overview," *International Journal of Advancements in Computer Networks and its Security*, vol. 4, no. 4, p. 5054, December 2014.

[57] M. Ussath, D. Jaeger, F. Cheng, and C. Meinel, "Advanced persistent threats: Behind the scenes," in *2016 Annual Conference on Information Science and Systems (CISS)*. IEEE, 2016, pp. 181–186.

[58] G. Wang, J. W. Stokes, C. Herley, and D. Felstead, "Detecting malicious landing pages in malware distribution networks," in *2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2013, pp. 1–11.

[59] M. Monte, *Network Attacks and Exploitation. A Framework*. John Wiley and sons, July 2015.

[60] ANSSI, "Phishing campaigns by the NOBELIUM intrusion set," [Online]. Available: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-011.pdf, Agence Nationale de la Sécurité des Systèmes d'Information, Tech. Rep., December 2021.

[61] M. Dunwoody, A. Thompson, B. Withnell, J. Leathery, M. Matonis, and N. Carr, "Not so cozy: An uncomfortable examination of a suspected apt29 phishing campaign," [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign, FireEye, Tech. Rep., November 2018.

[62] M. T. I. Center, "New sophisticated email-based attack from NOBELIUM," [Online]. Available: https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/, Microsoft Threat Intelligence Center, Tech. Rep., May 2021.

[63] D. of Homeland Security, "Enhanced analysis of grizzly steppe activity," [Online]. Available: https://www.cisa.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf, Department of Homeland Security, Tech. Rep., February 2017.

[64] R. Nafisi and A. Lelli, "GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM's layered persistence," [Online]. Available: https://www.microsoft.com/en-us/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/, Microsoft Threat Intelligence Center, Tech. Rep., March 2021.

[65] J. Wolfram, S. Hawley, T. McLellan, N. Simonian, and A. Vejlby, "Trello from the other side: Tracking apt29 phishing campaigns," [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/tracking-apt29-phishing-campaigns, Mandiant, Tech. Rep., April 2022.

[66] K. Baumgartner and C. Raiu, "The CozyDuke APT,"

[Online]. Available: https://securelist.com/the-cozyduke-apt/69731/, Kaspersky, Tech. Rep., April 2015.

[67] L. Smith, J. Leathery, and B. Read, "New SUNSHUTTLE Second-Stage Backdoor Uncovered Targeting U.S.-Based Entity; Possible Connection to UNC2452," [Online]. Available: https://www.mandiant.com/resources/blog/sunshuttle-second-stage-backdoor-targeting-us-based-entity, Mandiant, Tech. Rep., March 2021.

[68] E. Research, "Operation ghost: The dukes aren't back – they never left," [Online]. Available: https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/, ESET, Tech. Rep., October 2019.

[69] CISA, "MAR-10327841-1.v1 – SUNSHUTTLE," [Online]. Available: https://www.cisa.gov/news-events/analysis-reports/ar21-105a, Cybersecurity & Infrastructure Security Agency, Tech. Rep., April 2021.

[70] D. Alperovitch, "Bears in the Midst: Intrusion Into the Democratic National Committee," [Online]. Available: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/, CrowdStrike, Tech. Rep., June 2016.

[71] C. Intelligence, "Early bird catches the wormhole: Observations from the stellarparticle campaign," [Online]. Available: https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/, CrowdStrike, Tech. Rep., January 2022.

[72] D. Bienstock, M. Derr, J. Madeley, T. Mclellan, and C. Gardner, "Unc3524: Eye spy on your email," [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/unc3524-eye-spy-email, FireEye, Tech. Rep., May 2022.

[73] FireEye, "Hammertoss: stealthy tactics define a Russian cyber threat group," [Online]. Available: https://www.mandiant.com/resources/reports/hammertoss-stealthy-tactics-define-russian-cyber-threat-group, Fireeye, Tech. Rep., July 2015.

[74] P. W. Coopers, "How wellmess malware has been used to target covid-19 vaccines," [Online]. Available: https://www.pwc.co.uk/issues/cyber-security-services/insights/cleaning-up-after-wellmess.html, Price Waterhouse Coopers, Tech. Rep., July 2020.

[75] PwC, "Wellmess malware: analysis of its command and control (c2) server," [Online]. Available: https://www.pwc.co.uk/issues/cyber-security-services/insights/wellmess-analysis-command-control.html, Price Waterhouse Coopers, Tech. Rep., August 2020.

[76] K. I. CERT, "Energetic bear/crouching yeti: attacks on servers," [Online]. Available: https://securelist.com/energetic-bear-crouching-yeti/85345/, Kaspersky, Tech. Rep., April 2018.

[77] J. Hanrahan, "How adversaries use spear phishing to target engineering staff," [Online]. Available: https://www.dragos.com/blog/how-adversaries-use-spear-phishing-to-target-engineering-staff/, Dragos, Inc., Tech. Rep., October 2022.

[78] S. S. Response, "Dragonfly: Cyberespionage attacks against energy suppliers," [Online]. Available: https://icscsi.org/library/Documents/Cyber_Events/Symantec%20-%20Security%20Response%20-%20Dragonfly%20v1.2.pdf, Symantec, Tech. Rep., July 2014.

[79] CISA, "Advanced persistent threat activity targeting energy and other critical infrastructure sectors," [Online]. Available: https://www.cisa.gov/news-events/alerts/2017/10/20/advanced-persistent-threat-activity-targeting-energy-and-other, Cybersecurity & Infrastructure Security Agency, Tech. Rep., March 2018.

[80] Cybersecurity and I. S. Agency, "Russian State-Sponsored Advanced Persistent Threat Actor Compromises US Government Targets," [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-296a, Cybersecurity & Infrastructure Security Agency, Tech. Rep., December 2020.

[81] J. Slowik, "The baffling Berserk Bear: a decade's activity targeting critical infrastructure," in *2021 Virus Bulletin localhost*, October 2021.

[82] C. T. U. R. Team, "Mcmd malware analysis," [Online]. Available: https://www.secureworks.com/research/mcmd-malware-analysis, Secureworks, Tech. Rep., July 2019.

[83] T. H. Team, "Dragonfly: Western energy sector targeted by sophisticated attack group," [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks, Symantec, Tech. Rep., October 2017.

[84] H. N. S. Authority and C. L. M. I. Team, "Teamspy – obshie manevri. ispolzovat' tolko s razreshenija s-a," [Online]. Available: https://blog.crysys.hu/2013/03/teamspy/, Laboratory of Cryptography and System Security, Tech. Rep., March 2013.

[85] K. Livelli and J. Gross, "Energetic DragonFly DYMALLOY Bear 2.0," [Online]. Available: https://blogs.blackberry.com/en/2018/03/energetic-dragonfly-dymalloy-bear-2-0, BlackBerry, Tech. Rep., March 2018.

[86] C. T. U. R. Team, "Own the router, own the traffic," [Online]. Available: https://www.secureworks.com/blog/own-the-router-own-the-traffic, Secureworks, Tech. Rep., July 2019.

[87] A. Kasza and D. Reichel, "The gamaredon group toolset evolution," [Online]. Available: https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution/, PaloAlto Networks, Tech. Rep., February 2017.

[88] Unit42, "Russia's Gamaredon aka Primitive Bear APT Group Actively Targeting Ukraine," [Online]. Available: https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/, PaloAlto Networks, Tech. Rep., February 2022.

[89] M. T. I. Center, "ACTINIUM targets Ukrainian organizations," [Online]. Available: https://www.microsoft.com/en-us/security/blog/2022/02/04/actinium-targets-ukrainian-

organizations/, Microsoft Threat Intelligence Center, Tech. Rep., February 2022.

[90] G. Mele, Y. Polozov, and T. Gould, "Primitive Bear (Gamaredon) Targets Ukraine with Timely Themes," [Online]. Available: https://www.anomali.com/blog/primitive-bear-gamaredon-targets-ukraine-with-timely-themes, Anomali, Tech. Rep., April 2021.

[91] O. M. Erdogan, "Network footprints of gamaredon group," [Online]. Available: https://blogs.cisco.com/security/network-footprints-of-gamaredon-group, Cisco, Tech. Rep., May 2022.

[92] K. Hiroyuki and E. Maruyama, "Gamaredon apt group use covid-19 lure in campaigns," [Online]. Available: https://www.trendmicro.com/fr_fr/research/20/d/gamaredon-apt-group-use-covid-19-lure-in-campaigns.html, Trendmicro, Tech. Rep., April 2020.

[93] C. UA, "Cert–ua 4434. cyber attack of the uac-0010 group (armageddon) on the state organizations of ukraine," [Online]. Available: https://cert.gov.ua/article/39386, Computer Emergency Response Team of Ukraine, Tech. Rep., April 2022.

[94] J. Lewis, "Operation armageddon: Cyber espionage as a strategic component of russian modern warfare," [Online]. Available: https://www.ecirtam.net/autoblogs/autoblogs/lamaredugoffrblog_6aa4265372739b936776738439d4ddb430f5fa2e/media/88e3da25.Operation_Armageddon_FINAL.pdf, LookingGlass, Tech. Rep., April 2015.

[95] C. UA, "Cert–ua 5134. cyberattacks of the uac-0010 group (armageddon): malicious programs gammaload, gammasteel," [Online]. Available: https://cert.gov.ua/article/1229152, Computer Emergency Response Team of Ukraine, Tech. Rep., October 2022.

[96] U. 42, "Russia's Trident Ursa (aka Gamaredon APT) Cyber Conflict Operations Unwavering Since Invasion of Ukraine," [Online]. Available: https://unit42.paloaltonetworks.com/trident-ursa/, PaloAlto Networks, Tech. Rep., December 2022.

[97] Y. T. Intelligence, "The Russian Shadow in Eastern Europe: Ukrainian MOD Campaign," [Online]. Available: https://yoroi.company/en/research/the-russian-shadow-in-eastern-europe-ukrainian-mod-campaign/, Yoroi, Tech. Rep., April 2019.

[98] I. Group, "Operation gamework: infrastructure overlaps found between bluealpha and iranian apts," [Online]. Available: https://go.recordedfuture.com/hubfs/reports/cta-2019-1212.pdf, Recorded Future, Tech. Rep., December 2019.

[99] T. H. Team, "Shuckworm continues cyber-espionage attacks against ukraine," [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine, Symantec, Tech. Rep., January 2022.

[100] Z. Hromcová, "Invisimole: Surprisingly equipped spyware, undercover since 2013," [Online]. Available: https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/, ESET, Tech. Rep., June 2018.

[101] Z. Hromcova, "Invisimole: First-class persistence through second-class exploits," [Online]. Available: https://securitymea.com/tag/invisimole-first-class-persistence-through-second-class-exploits/, ESET, Tech. Rep., September 2020.

[102] G. Research and A. Team, "The epic turla operation," [Online]. Available: https://securelist.com/the-epic-turla-operation/65545/, Kaspersky, Tech. Rep., August 2014.

[103] J. Wrolstad and B. Bengerik, "Pinpointing targets: exploiting web analytics to ensnare victims," [Online]. Available: https://vulners.com/fireeye/FIREEYE:1245EEC5103BC50641AB2958AAEFECDE, FireEye, Tech. Rep., November 2015.

[104] S. S. Response, "The waterbug attack group," [Online]. Available: https://docs.broadcom.com/doc/waterbug-attack-group, Symantec, Tech. Rep., January 2016.

[105] J.-I. Boutin, "Turla's watering hole campaign: An updated firefox extension abusing instagram," [Online]. Available: https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/, ESET, Tech. Rep., June 2017.

[106] G. Research and A. Team, "Shedding skin – turla's fresh faces," [Online]. Available: https://securelist.com/shedding-skin-turlas-fresh-faces/88069/, Kaspersky, Tech. Rep., October 2018.

[107] K. GReAT, "Turla renews its arsenal with Topinambour," [Online]. Available: https://securelist.com/turla-renews-its-arsenal-with-topinambour/91687/, Kaspersky, Tech. Rep., July 2019.

[108] B. Leonard, "Update on cyber activity in Eastern Europe," [Online]. Available: https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/, Google Threat Analysis Group, Tech. Rep., May 2023.

[109] S. Threat and D. R. Team, "TURLA's new phishing-based reconnaissance campaign in Eastern Europe," [Online]. Available: https://blog.sekoia.io/turla-new-phishing-campaign-eastern-europe/, Sekoia.IO, Tech. Rep., May 2022.

[110] M. Faou, "From agent.btz to comrat v4," [Online]. Available: https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/, ESET, Tech. Rep., May 2020.

[111] I. Group, "Swallowing the snake's tail: Tracking turla infrastructure," [Online]. Available: https://go.recordedfuture.com/hubfs/reports/cta-2020-0312.pdf, Recorded Future, Tech. Rep., March 2020.

[112] A. C. T. Intelligence, "Turla uses hyperstack, carbon, and kazuar to compromise government entity," [Online]. Available: https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity, Accenture, Tech. Rep., October 2020.

[113] H. Unterbrink, "Tinyturla - turla deploys new malware to keep a secret backdoor on victim machines," [Online]. Available:

https://blog.talosintelligence.com/tinyturla/, Cisco Talos Intelligence, Tech. Rep., September 2021.

[114] M. Faou, "Turla crutch: Keeping the "back door" open," [Online]. Available: https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/, ESET, Tech. Rep., December 2020.

[115] N. S. Agency and N. C. S. Centre, "Turla Group Exploits Iranian APT To Expand Coverage Of Victims," [Online]. Available: https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims, NSA/NCSC, Tech. Rep., October 2019.

[116] V. Mavroeidis, R. Hohimer, T. Casey, and A. Jesang, "Threat actor type inference and characterization within cyber threat intelligence," in *2021 13th International Conference on Cyber Conflict (CyCon)*. IEEE, 2021, pp. 327–352.

[117] S. T. Intelligence, "Waterbug: Espionage group rolls out brand-new toolset in attacks against governments," [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/waterbug-espionage-governments, Symanteec, Tech. Rep., June 2019.

[118] E. Research, "Carbon paper: Peering into turla's second stage backdoor," [Online]. Available: https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/, ESET, Tech. Rep., March 2017.

[119] B. Bartholomew, "Kopiluwak: A new javascript payload from turla," [Online]. Available: https://securelist.com/kopiluwak-a-new-javascript-payload-from-turla/77429/, Kaspersky, Tech. Rep., February 2017.

[120] D. Huss, "Turla apt actor refreshes kopiluwak javascript backdoor for use in g20-themed attack," [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/turla-apt-actor-refreshes-kopiluwak-javascript-backdoor-use-g20-themed-attack, Proofpoint, Tech. Rep., August 2017.

[121] ESET, "Gazing at gazer. turla's new second stage backdoor," [Online]. Available: https://web-assets.esetstatic.com/wls/2017/08/eset-gazer.pdf, ESET, Tech. Rep., August 2017.

[122] GovCERT.ch, "APT Case RUAG," [Online]. Available: https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/dokumentation/fachberichte/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf, GovCERT.ch, Tech. Rep., May 2016.

[123] K. Baumgartner and C. Raiu, "The 'penquin' turla," [Online]. Available: https://securelist.com/the-penquin-turla-2/67962/, Kaspersky, Tech. Rep., December 2014.

[124] S. W. Brady, "United States vs. Yuriy Sergeyevich Andrienko et al." [Online]. Available: https://storage.courtlistener.com/recap/gov.uscourts.pawd.272394/gov.uscourts.pawd.272394.1.0.pdf, US District Court. Western District of Pennsylvania, Tech. Rep., October 2020.

[125] G. Research and A. Team, "Olympicdestroyer is here to trick the industry," [Online]. Available: https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/, Kaspersky, Tech. Rep., March 2018.

[126] J. Slowik, "Centreon to exim and back: On the trail of sandworm," [Online]. Available: https://www.domaintools.com/resources/blog/centreon-to-exim-and-back-on-the-trail-of-sandworm/, DomainTools, Tech. Rep., March 2021.

[127] G. Research and A. Team, "Hades, the actor behind olympic destroyer is still alive," [Online]. Available: https://securelist.com/olympic-destroyer-is-still-alive/86169/, Kaspersky, Tech. Rep., June 2018.

[128] ANSSI, "Sandworm intrusion set campaign targeting centreon systems," [Online]. Available: https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-005/, Agence Nationale de la Sécurité des Systèmes d'Information, Tech. Rep., January 2021.

[129] N. S. Agency, "Sandworm actors exploiting vulnerability in exim mail transfer agent," [Online]. Available: https://media.defense.gov/2020/May/28/2002306626/-1/-1/0/CSA-Sandworm-Actors-Exploiting-Vulnerability-in-Exim-Transfer-Agent-20200528.pdf, NSA, Tech. Rep., May 2020.

[130] N. C. S. Centre, "Cyclops blink. malware analysis report," [Online]. Available: https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf, National Cyber Security Centre, Tech. Rep., February 2022.

[131] K. Baumgartner and M. Garnaeva, "Be2 extraordinary plugins, siemens targeting, dev fails," [Online]. Available: https://securelist.com/be2-extraordinary-plugins-siemens-targeting-dev-fails/68838/, Kaspersky, Tech. Rep., February 2015.

[132] A. Cherepanov, "Telebots are back: Supply-chain attacks against ukraine," [Online]. Available: https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/, ESET, Tech. Rep., June 2017.

[133] S. Huntley, "An update on the threat landscape," [Online]. Available: https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/, Google, Tech. Rep., March 2022.

[134] F. Hacquebord, "Pawn storm in 2019. a year of scanning and credential phishing on high-profile targets," [Online]. Available: https://documents.trendmicro.com/assets/white_papers/wp-pawn-storm-in-2019.pdf, Trend Micro Research, Tech. Rep., March 2020.

[135] Microsoft, "Microsoft security intelligence report," [Online]. Available: https://download.microsoft.com/download/E/8/B/E8B5CEE5-9FF6-4419-B7BF-698D2604E2B2/Microsoft_Security_Intelligence_Report_Volume_20_English.pdf, Tech. Rep., November 2015.

[136] M. Elias, "Prime minister's office compromised: Details of recent espionage campaign," [Online]. Available: https://www.trellix.com/blogs/research/prime-ministers-office-compromised/, Trellix, Tech. Rep., January 2022.

[137] C. Guarnieri, "Digital attack on german parliament:

Investigative report on the hack of the left party infrastructure in bundestag," [Online]. Available: https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/, Netzpolitik, Tech. Rep., June 2015.

[138] C. T. I. Team, "In the footsteps of the fancy bear: Powerpoint mouse-over event abused to deliver graphite implants," [Online]. Available: https://www.duskrise.com/2022/09/23/in-the-footsteps-of-the-fancy-bear-powerpoint-mouse-over-event-abused-to-deliver-graphite-implants/, DuskRise, Tech. Rep., September 2022.

[139] Z. Bederna and T. Szadeczky, "Cyber espionage through botnets," *Security Journal*, vol. 33, no. 1, pp. 43–62, 2020.

[140] Q. Wu, Q. Li, D. Guo, and X. Meng, "Exploring the vulnerability in the inference phase of advanced persistent threats," *International Journal of Distributed Sensor Networks*, vol. 18, no. 3, 2022.

[141] Root9B, "APT28 targets financial markets," [Online]. Available: https://github.com/jack8daniels2/threat-INTel/blob/master/2015/FSOFACY.pdf, Root9B, Tech. Rep., May 2015.

[142] R. Falcone and B. Lee, "New Sofacy Attacks Against US Government Agency," [Online]. Available: https://unit42.paloaltonetworks.com/unit42-new-sofacy-attacks-against-us-government-agency/, Unit42. PaloAlto Networks, Tech. Rep., June 2016.

[143] D. Creus, T. Halfpop, and R. Falcone, "Sofacy's 'Komplex' OS X Trojan," [Online]. Available: https://unit42.paloaltonetworks.com/unit42-sofacys-komplex-os-x-trojan/, Unit42. PaloAlto Networks, Tech. Rep., September 2016.

[144] B. Lee and R. Falcone, "Sofacy group's parallel attacks," [Online]. Available: https://unit42.paloaltonetworks.com/unit42-sofacy-groups-parallel-attacks/, Unit42. PaloAlto Networks, Tech. Rep., June 2018.

[145] E. Research, "Lojax: First uefi rootkit found in the wild, courtesy of the sednit group," [Online]. Available: https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/, ESET, Tech. Rep., September 2018.

[146] J. Kennedy, "A Zebra in Gopher's Clothing: Russian APT Uses COVID-19 Lures to Deliver Zebrocy," [Online]. Available: https://intezer.com/blog/research/russian-apt-uses-covid-19-lures-to-deliver-zebrocy/, Intezer, Tech. Rep., December 2020.

[147] G. Research and A. Team, "A slice of 2017 sofacy activity," [Online]. Available: https://securelist.com/a-slice-of-2017-sofacy-activity/83930/, Kaspersky, Tech. Rep., February 2018.

[148] O. Eichelsheim, "GRU close access cyber operation against OPCW," [Online]. Available: https://english.defensie.nl/downloads/publications/2018/10/04/gru-close-access-cyber-operation-against-opcw, Dutch Defence Intelligence & Security Service (Alankomaat), Tech. Rep., October 2018.

[149] L. Smith-Spark and K. Polglase, "Netherlands officials say they caught russian spies targeting chemical weapons body," *CNN*, October 2018.

[150] S. Miller, N. Brubaker, D. K. Zafra, and D. Caban, "Triton actor ttp profile, custom attack tools, detections, and att&ck mapping," [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/triton-actor-ttp-profile-custom-attack-tools-detections, Fireeye Threat Response, Tech. Rep., April 2019.

[151] Dragos, "ICS/OT cybersecurity. Year in review 2022," [Online]. Available: https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Exec-Summary-2022.pdf, Dragos, Inc., Tech. Rep., February 2023.

[152] J. Slowik, "The continuous conundrum of cloud atlas," [Online]. Available: https://www.domaintools.com/resources/blog/the-continuous-conundrum-of-cloud-atlas/, DomainTools, Tech. Rep., February 2021.

[153] P. E. S. Center, "APT Cloud Atlas: Unbroken Threat," [Online]. Available: https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt-cloud-atlas-unbroken-threat/, Positive Technologies, Tech. Rep., December 2022.

[154] T. Lancaster, "Inception attackers target Europe with year-old office vulnerability," [Online]. Available: https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability/, Unit42. PaloAlto Networks, Tech. Rep., November 2018.

[155] G. Research and A. Team, "Recent cloud atlas activity," [Online]. Available: https://securelist.com/recent-cloud-atlas-activity/92016/, Kaspersky, Tech. Rep., August 2019.

[156] P. E. S. Center, "Apt cloud atlas: Unbroken threat," [Online]. Available: https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt-cloud-atlas-unbroken-threat/, Positive Technologies, Tech. Rep., December 2022.

[157] G. Research and A. Team, "The "red october" campaign – an advanced cyber espionage network targeting diplomatic and government agencies," [Online]. Available: https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-identifies-operation--red-october--an-advanced-cyber-espionage-campaign-targeting-diplomatic-and-government-institutions-worldwide, Kaspersky, Tech. Rep., January 2013.

[158] K. GReAT, "Cloud Atlas: RedOctober APT is back in style," [Online]. Available: https://securelist.com/cloud-atlas-redoctober-apt-is-back-in-style/68083/, Kaspersky, Tech. Rep., December 2014.

[159] T. H. Team, "Inception framework: Alive and well, and hiding behind proxies," [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies, Symantec, Tech. Rep., March 2018.

[160] Unit42, "Spear Phishing Attacks Target Organizations in Ukraine, Payloads Include the Document Stealer OutSteel and the Downloader SaintBot," [Online]. Available: https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/, PaloAlto Networks, Tech. Rep., February 2022.

[161] C. UA, "Cert–ua 4145. cyber attack on state organizations of ukraine using malicious programs cobalt strike beacon, grimplant and graphsteel," [Online]. Available: https://cert.gov.ua/article/37704, Computer Emergency Response Team of Ukraine, Tech. Rep., March 2022.

[162] J. Kennedy and N. Fishbein, "Elephant framework delivered in phishing attacks against ukrainian organizations," [Online]. Available: https://intezer.com/blog/research/elephant-malware-targeting-ukrainian-orgs/, Intezer, Tech. Rep., April 2022.

[163] Hasherezade, H. Jazi, and E. Noerenber, "A deep dive into saint bot, a new downloader," [Online]. Available: https://www.malwarebytes.com/blog/threat-intelligence/2021/04/a-deep-dive-into-saint-bot-downloader, Malware Bytes, Tech. Rep., April 2021.

[164] R. Falcone, M. Harbison, and J. Grunzweig, "Threat brief: Ongoing russia and ukraine cyber activity," [Online]. Available: https://register.paloaltonetworks.com/unit42briefingrussiaukraine, Unit42. PaloAlto Networks, Tech. Rep., January 2022.

[165] A. B. S. Ehrlich, "Threat actor uac-0056 targeting ukraine with fake translation software," [Online]. Available: https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/, Sentinel One, Tech. Rep., March 2022.

[166] J. Ji, "APT Retrospection: Lorec53, An Active Russian Hack Group Launched Phishing Attacks Against Georgian Government," [Online]. Available: https://nsfocusglobal.com/apt-retrospection-lorec53-an-active-russian-hack-group-launched-phishing-attacks-against-georgian-government/, NSFocus, Tech. Rep., February 2022.

[167] R. Santos and H. Jazi, "Cobalt Strikes again: UAC-0056 continues to target Ukraine in its latest campaign," [Online]. Available: https://cymulate.com/threats/cobalt-strikes-again-uac-0056-continues-to-target-ukraine-in-its-latest-campaign/, Malware Bytes, Tech. Rep., July 2022.

[168] T. H. Team, "Graphiron: New Russian Information Stealing Malware Deployed Against Ukraine," [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nodaria-ukraine-infostealer, Symantec, Tech. Rep., February 2023.

[169] Z. Ma, Q. Li, and X. Meng, "Discovering suspicious apt families through a large-scale domain graph in information-centric iot," *IEEE Access*, vol. 7, pp. 13 917–13 926, 2019.

[170] F. J. Abdullayeva, "Advanced persistent threat attack detection method in cloud computing based on autoencoder and softmax regression algorithm," *Array*, vol. 10, p. 100067, 2021.

Appendix A

Table 4.
MITRE ATT&CK “Resource Development” techniques.

Technique ID	Name	Sub–techniques
T1583	Acquire Infrastructure	Domains DNS Server Virtual Private Server Server Botnet Web services Serverless
T1586	Compromise Accounts	Social Media Accounts Email Accounts Cloud Accounts
T1584	Compromise Infrastructure	Domains DNS Server Virtual Private Server Server Botnet Web services Serverless
T1587	Develop Capabilities	Malware Code Certificates Digital Certificates Exploits
T1585	Establish Accounts	Social Media Accounts Email Accounts Cloud Accounts
T1588	Obtain Capabilities	Malware Tool Code Signing Certificates Digital Certificates Exploits Vulnerabilities
T1608	Stage Capabilities	Upload Malware Upload Tool Install Digital Certificate Drive–by Target Link Target SEO Poisoning

Appendix B

Table 5.
Summary of external infrastructure provisioning techniques.

Group	Tactic	Resource	Technique	References
APT29	Initial access	E–mail	Compromise	[60] [61]
		Public services	Abuse	[62]
		Domain	Registration	[19] [63] [61]
		Domain	Compromise	[63] [61]
	Persistence	Domain	Registration	[64] [67] [68] [69]
		Web server	Compromise	[64] [65] [19] [63] [66]
		VPS	Purchase	[70] [66] [71] [72]
		Public services	Abuse	[73] [19] [62] [65] [68]
		Digital certificates	Generation	[74] [75]
	OPSEC	TOR	Abuse	[63] [19]
Energetic Bear	Initial access	Domain	Registration	[80] [77]
		Web server	Compromise	[76] [77] [78] [79]
		E–mail	Compromise	[79]
	Persistence	Domain	Registration	[84] [77]
		Web server	Compromise	[81] [82]
		VPS	Purchase	[81] [83] [79] [80]
		Routing infrastructure	Compromise	[85] [86]
	OPSEC	VPS	Purchase	[80]
Gamaredon	Initial access	Domain	Compromise	[87]
		Domain	Registration	[87] [88] [89] [90] [91]
		VPS	Purchase	[87] [92] [91]
		E–mail	Registration	[91] [93]
	Persistence	Domain	Registration	[88] [89] [94] [93] [95] [96] [97] [93]
		Web server	Compromise	[94]
		Web server	Hijacking	[98]
		VPS	Purchase	[93] [95] [96] [99]
		Public services	Abuse	[95] [96]
	OPSEC	N/A	N/A	N/A
Invisimole	Initial access	VPS	Purchase	[93]
	Persistence	Domain	Registration	[100] [28]
	OPSEC	N/A	N/A	N/A

Group	Tactic	Resource	Technique	References
TURLA	Initial access	Web server	Compromise	[102] [103] [104] [105]
		Domain	Registration	[108] [109]
		Routing infrastructure	Compromise	[106]
		VPS	Purchase	[107]
	Persistence	Web server	Compromise	[30] [110] [111] [112] [113] [102] [118] [105] [119] [120] [121] [122]
		Domain	Registration	[123]
		VPS	Purchase	[123]
		VPS	Hijacking	[115] [116] [117]
		Public services	Registration	[114]
		Satellite links	Compromise	[32]
		Public services	Abuse	[118] [105]
	OPSEC	N/A	N/A	N/A
Sandworm	Initial access	Domain	Registration	[124] [125] [126]
		Web server	Compromise	[127] [126] [128] [129]
		VPS	Purchase	[125]
		E–mail	Registration	[124] [125]
		Identities	Registration	[124]
	Persistence	Botnets	Compromise	[130]
		Public services	Abuse	[131] [132]
		E–mail	Registration	[132]
	OPSEC	VPN	Abuse	[125]
		TOR	Abuse	[128]
APT28	Initial access	Domain	Registration	[133] [39] [136] [137]
		Web server	Compromise	[41]
		E–mail	Compromise	[133] [134]
		Public services	Registration	[133] [138]
		Physical elements	Purchase	[148] [149]
		VPS	Purchase	[134]
	Persistence	Botnet	Compromise	[139] [140]
		Domain	Registration	[137] [136] [141]-[147]
		VPS	Renting	[141] [137] [142] [143] [144] [145] [146] [136]
		Public services	Abuse	[142] [138]
	OPSEC	Botnet	Compromise	[139] [140]
		VPN	Abuse	[135] [134]

Group	Tactic	Resource	Technique	References
TEMP.Veles	Initial access	N/A	N/A	N/A
	Persistence	VPS	Purchase	[150]
		Domain	Registration	[150]
		Domain	Compromise	[151]
	OPSEC	N/A	N/A	N/A
Cloud Atlas	Initial access	E–mail	Registration	[48]
		Domains	Registration	[152] [153] [154] [155] [156]
		VPS	Purchase	[152] [153] [154] [155] [156]
	Persistence	Domains	Registration	[152] [153] [154] [155] [156] [157] [158] [159]
		VPS	Purchase	[152] [153] [154] [155] [156] [157]
	OPSEC	VPS	Purchase	[157]
		Routers	Compromise	[159]
Saint Bear	Initial access	Domains	Registration	[160] [161] [165] [163] [166]
		Public services	Abuse	[161] [162] [163] [164]
		Digital certificates	Stealing	[160]
	Persistence	Domains	Registration	[160] [163] [167]
		VPS	Purchase	[165] [168] [166]
	OPSEC	N/A	N/A	N/A