Abusing Cloud-Based Legitimate Services As A Command-and-Control Communication Channel: A Systematic Review

TURKI AL LELAH, Cardiff University, UK
GEORGE THEODORAKOPOULOS, Cardiff University, UK
PHILIPP REINECKE, Cardiff University, UK
AMIR JAVED, Cardiff University, UK
EIRINI ANTHI, Cardiff University, UK

Legitimate web-based and cloud-based solutions play an essential role in today's various disciplines, such as health, banking, government, and industry. These solutions are authorised in an enterprise environment and trusted implicitly by users. Unfortunately, botnets have abused these services in recent years for command-and-control infrastructure (often referred to as 'C&C' or 'C2' channels). Botnet authors abuse them as a C&C mechanism to blend malicious traffic with benign traffic to evade detection. This is of interest because although the existing reviews have focused on botnet attack techniques and detection, less attention has been paid to the abuse of legitimate platforms as end-to-end C&C malware channels. The current study carries out a systematic literature review (SLR) of the academic and industrial literature concerning the abusive techniques that cybercriminals employ to leverage legitimate platforms for C&C communication. This review covers literature published between 2008 (when the first abuse was reported) through to October 2021. The primary objectives of the current study are to categorise the techniques of abusing legitimate cloud-based services as C&C servers and detection approaches. The analysis shows that the number of cloud-based abuses has grown significantly since 2011 due to the adoption of steganography, encoding, cryptography, fraudulent account, botmasters' credentials or hard-coded token, real victims' accounts, COM hijacking, malicious process injection into the legit process, and the ComSpec environment variable. Surprisingly, little research has been conducted into the detection aspect of these abusive techniques. Of 113 published studies, only 13 studies discuss the detection side. Six make high-level detection suggestions, and seven implement detection mechanisms focused on social networking platforms, but each has a drawback. The current study is the first to systematically review cloud-based abusive and detection techniques. The findings of this study contribute to a better understanding of emerging trend techniques which are essential to defend against botnets. Therefore, organisations must be aware of such harmful approaches and deploy an appropriate detection system.

CCS Concepts: • **Applied computing** → Enterprise computing infrastructures; • **Computer systems organization** → Cloud computing; • **Networks** → Web protocol security; Cloud computing; Online social networks; • **Information systems** → Email; • **Security and privacy** → Malware and its mitigation.

Additional Key Words and Phrases: Botnet, Command-and-Control C&C, Legitimate Cloud-Based Services (CBS).

Authors' addresses: Turki Al lelah, allelaht@cardiff.ac.uk, Cardiff University, School of Computer Science and Informatics, Cardiff, UK, CF240DP; George Theodorakopoulos, Cardiff University, School of Computer Science and Informatics, Cardiff, UK, theodorakopoulosg@cardiff.ac.uk; Philipp Reinecke, Cardiff University, School of Computer Science and Informatics, Cardiff, UK, reineckep@cardiff.ac.uk; Amir Javed, Cardiff University, School of Computer Science and Informatics, Cardiff, UK, JavedA7@cardiff.ac.uk; Eirini Anthi, Cardiff University, School of Computer Science and Informatics, Cardiff, UK, AnthiES@cardiff.ac.uk.

Manuscript submitted to ACM

ACM Reference Format:
Turki Al lelah, George Theodorakopoulos, Philipp Reinecke, Amir Javed, and Eirini Anthi. 2021. Abusing Cloud-Based Legitimate Services As A Command-and-Control Communication Channel: A Systematic Review. 1, 1 (January 2021), 30 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Individuals and diverse sectors are continually targeted by various malwares. Botnets and ransomware are types of malware that are implemented by cybercriminals. Bots steadily increase and incarnate in a botnet which is a collection of compromised computers that are remotely controlled by one or multiple controllers referred to as a botmaster via C&C infrastructure [37]. TThese bots are the most dominant threat vector for many environments and the most widely used malicious activities that lead to severe threats to Internet security on a global scale. The earliest bots were developed for non-malicious purposes to facilitate and coordinate basic automation tasks [69]. However, by leveraging the bots for other purposes, a botmaster can conduct malicious operations such as obtaining confidential exfiltration data, degrading systems, distributed denial of service (DDoS) and phishing. By their very nature, a botmaster employs evasive techniques involving C&C communication in botnet operations to accomplish their malicious aims by disseminating commands to armies of bots [37]. Botnets utilise C&C communication channels to achieve the goals of the botmaster and realise malicious operations. These C&C channels have evolved into multiple Internet protocols and botnet architectures (e.g., IRC, HTTP, DNS, peer-to-peer (P2P), centralised, etc.). In practice, once a victim's vulnerability has been exploited, the infected computer is then instructed to establish a remote connection 'call-back' or 'rallying' with the attacker to be directly controlled. Conventionally, bots locate their C&C server through their IP addresses, DNS names or node identifiers in P2P overlays contained in the binary code.

Sophisticated adversaries who perform targeted attacks must adhere to stringent stealth requirements and include detection-evasion techniques. Over time, there has been an increase in attacks that have transferred to legitimate cloud services for this purpose [20, 50, 63]. This transformation appears to be a logical choice because the service's infrastructure is administered by a legitimate cloud-based provider and the C&C malicious network traffic merges with the benign traffic. Accordingly, botnet authors have customised the stealthiest approaches for C&C communication channels to be more resilient and robust against takedown actions by abusing legitimate cloud-based services (e.g., Microsoft Outlook, OneDrive, Slack, Dropbox, Pastebin, Twitter, Google Drive) as a server-less C&C infrastructure. Therefore, the botmaster will communicate with a backdoor implanted on a victim's system and evade detection. Ultimately, these stealthy communication channels are formed by combining three main thrusts to evade detection: enterprise authorised trusted services; software from reputable vendors; a secure communication protocol Transport Layer Security (TLS) which provides adversaries with an extra layer of protection. Hence, the trust relationship that users and enterprises have with the cloud is exploited for C&C functionalities. Meanwhile, monitoring network traffic for suspicious connections is effectively futile because there is no discernible difference between network traffic initiated by malware and that of legitimate users. Also, it is more challenging for network-level security products to detect malicious traffic because the traffic will appear benign. Various legitimate web and cloud-based services have been abused for C&C communication infrastructure to carry out malicious activities (e.g., sensitive information exfiltration, installing further malicious payloads, storing malicious content, and controlling the compromising computers through the C&C channel). As a result, host and network abnormal logs will most likely be generated by the infected endpoint. Detecting these odd activities through logs, in turn, will successfully guard against malware attacks.

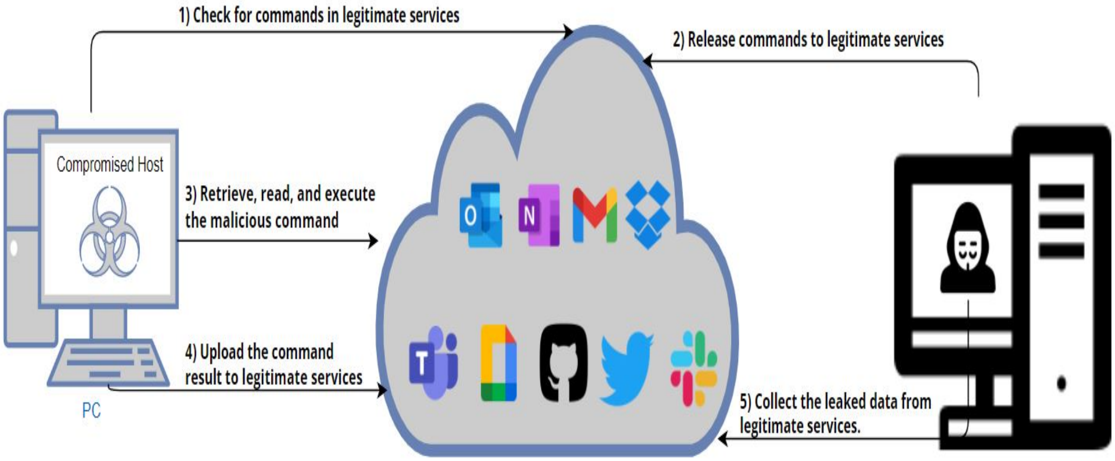

1) Check for commands in legitimate services
2) Release commands to legitimate services
Compromised Host
3) Retrieve, read, and execute the malicious command
4) Upload the command result to legitimate services
PC
5) Collect the leaked data from legitimate services.

Fig. 1. A diagram illustrating legitimate cloud-based platforms being abused as C&C channel.

Therefore, to foster further research, a SLR is presented in the current study which focuses on analysing the current state of abusing legitimate cloud-based services as C&C servers and detection approaches. Despite there being a published closely related survey that has addressed abuses against popular cloud-based services [94], this review does not take into account all abusive tactics that leverage legitimate platforms as C&C server-less. This review reports only four abusive techniques: encoding, steganography, free accounts, and user generation algorithms (UGAs). In contrast, the current study addresses nine techniques. The study that was conducted by [84], was focused on social bots and listed two detected abuse incidents in which they adopted image steganography and cryptography as techniques to leverage Facebook and Twitter as a C&C medium. To the best of our knowledge, this is the first study to systematically review the current state categorisation of techniques employed to abuse legitimate platforms as a C&C infrastructure.

After further decomposition of the aforementioned problem statement, the following research categories and sub-questions were formulated that the current review sought to answer:

- **Abuse technique questions:**
  Q1: Which techniques are employed to abuse legitimate services (e.g., Microsoft Outlook, OneDrive, Slack, Dropbox) via the C&C channel?
  Q2: What type of legitimate services are targeted for abuse using the C&C channel?
  Q3: How common have these abusive techniques become?
- **Abuse detection question:**
  Q4: Which countermeasures have been proposed to detect platform abuses?

The findings of the aforementioned questions are intended to provide insight into the current state of abusive characterisation techniques, thereby helping to bring to the attention of organisations' defenders the insight that helps to anticipate and propose resilience solutions to detect threat actors' sophisticated behavioural patterns and effectively combat them. Despite the fact that researchers have devised a variety of defence mechanisms, the current research reveals that the security controls and solutions still lack ways to cope with the aforementioned stealthy techniques that abuse the legitimate services. This significant research gap has been identified based on survey results from academia, real-world experience, and research proof-of-concept evidence.

The plan of the current paper is as follows. Section II presents the motivations, research questions and contributions. Related surveys are discussed in Section III. Meanwhile, Section IV describes the SLR adopted as the review methodology. Section V discusses the evasive techniques that were employed to misuse legitimate services for the C&C covert communication channel. Finally, the detection-related works are addressed in Section VI.

2 RELATED SURVEYS

Botnets are an extensively-studied topic that have been the subject of many scholarly review publications in the empirical literature. They seek to reveal the technical aspects of botnets and defence mechanisms. Although there is a considerable number of surveys [80, 82, 98, 101] that have focused on botnet attacks and detection mechanisms, only one review paper [94] has considered botnets that abuse legitimate cloud-based services as a C&C channel. The review of [80] proposes a comprehensive taxonomy of the botnet phenomenon. There are three sub-taxonomies in this survey: botnet behaviour, detection, and defence mechanisms. This comprehensive categorisation allows for a broader overview of both the botnet issue and the solution space. Furthermore, this survey briefly mentions an evasive tactic that abuses social networking websites such as Facebook and Twitter for C&C functionalities. The author describes a trend in which cloud-based services are used for either creating bots (i.e., the botcloud) on the cloud or hosting the C&C on the cloud in the near future.

Another survey [82] set out to investigate disruptive botnet techniques, the threats posed, and defence techniques. Furthermore, this review refers to a stealthy method [101], which abuses email-based services for C&C communications but they did not investigate it in detail.

Moreover, [98] conducted a taxonomy based on the botnet components, threats, architecture, C&C protocols, detection techniques: honeynets and intrusion detection system (IDS), defence techniques: propagation and bot communication. In addition, the authors discuss the five lifecycle phases of botnets: initial injection; secondary injection; connection or rally; malicious activities; and maintenance and upgrading of the botnet. Without in-depth exploration, this review mentions one abusive technique (encoding) to employ social networks as the C&C channel and they anticipate that a Socialbot Network (SbN) will emerge in the coming years.

A botnet taxonomy has been proposed and the botnet's lifecycle and architecture described [101], highlighting the need to focus on the entire botnet's lifecycle rather than just one factor. As the authors states, if one stage in the botnet's life-cycle is interrupted, the whole botnet is useless. They found that detection research focuses on one or more life-cycle stages but this review does not provide a taxonomy for the abuse of cloud-based or detection mechanisms.

The authors of [94] introduced four abusive tactics: hiding communications within text-based social media (SM) posts using encoding, using steganography, using free accounts, and using the username generation algorithm (UGA). Although this recent survey [94] recognised four abusive techniques, compared to the current study's ten identified techniques, research has yet to systematically review these abusive techniques.

In another review [84], the author proposes a taxonomy of malicious social bots and characterisation of various attack types at different stages (initiation-stage, listening-stage, execution-stage attacks). Whilst the review in [84] mainly focus on a social bot, two detected abuse incidents were explored which were adopted image-steganography and cryptography as techniques to leverage Facebook and Twitter as C&C mediums.

Collectively, such reviews remain narrow in focus regarding exploring the behaviour, detection, and defence of the traditional C&C communication channel that uses Internet protocols and botnet architectures (e.g., IRC, HTTP, DNS, P2P, centralised, etc.) However, they don't investigate the emerging techniques, one of which is the abuse of cloud-based services for C&C operations.

3 THREAT MODEL

According to a study by the International Data Group [23], 81% of organisations' IT infrastructures use cloud technology. Thus, this substantial proportion increases the likelihood that these legitimate services may be exploited for malicious purposes. Adversaries may abuse legitimate cloud-based services in end-user machines as the C&C channel to carry out malicious activities (e.g., sensitive information exfiltration, installing further malicious payloads, storing malicious content, and controlling compromised computers through the C&C Channel). Figure 1 illustrates how the threat actor leverages legitimate cloud-based services as C&C channels. After a successful compromise, the bot at the compromised victim's machine needs a remote control mechanism to communicate with the C&C server for further malicious instructions. To better equip and set up this remote C&C channel, bot connection requests are routed to the C&C server via legitimate cloud services rather than a direct connection [49, 56]. This structure is generally stealthy and undetectable because the way for the bot to retrieve commands and exfiltrate data is through legitimate cloud-based services. Accordingly, it is harder for network defenders and security solutions to discern between malicious and benign network traffic.

4 REVIEW METHODOLOGY

4.1 Methodology

Based on the review's aims, the methodological framework of [81] was adopted in the current SLR to guide the literature search. The guidelines applied in [81] consist of instructions that can be undertaken in accordance with a predefined protocol. The review process of the framework in [81] summarises the stages of SLR into three main phases: planning phase, conducting phase and reporting phase, respectively. The initial motivation for following these stages is to identify, analyse and interpret all of the available empirical literature related to the abuses of legitimate platforms as C&C infrastructure.

4.2 Research strategy

It is necessary to follow a predefined protocol to reduce the risk of bias that may occur when conducting the research. The systematic review began with the selection of the bibliography databases to be searched, as well as the development of a set of inclusion and exclusion criteria and search strings. The search strings were used to conduct a query into two primary sources: academic and grey (industrial) literature. The abbreviations and synonyms (alternative forms of the same word) of any search terms were compiled and concatenated into a search string using the Boolean operators OR and AND. To retrieve the relevant empirical literature, the search strings were restricted to titles, abstracts and keywords.

4.2.1 ***Academic digital libraries***

To extract all of the literature relevant to the defined research questions, the search strategy was implemented by applying *the Boolean expressions 'AND' and 'OR' to combine search terms. These combined queries were then carried on to a set of electronic databases that contain general computer science archives to ensure that studies associated with the topic were not missed, namely, IEEE Xplore Digital Library, SpringerLink, ACM Digital Library, ScienceDirect and Scopus. Out of the 596 articles retrieved using the search strategy (see Fig. 4), only 33 publications satisfied the inclusion criteria.*

4.2.2 Grey literature (cyber threat intelligence reports)

To extract the relevant misuses that occurred, the current research was extended to the threat intelligence technical repositories and security research tools such as FireEye, TrendMicro, welivesecurity, f-secure, unit42 Palo Alto, and securelist. Thus, a total of 56 white papers and technical reports were extracted.

4.2.3 Search Terms:

- **Boolean search strings for online digital libraries**

  (C2 **OR** C&C **OR** "Command and Control")

  AND

  (cloud **OR** Legitimate **OR** platform **OR** Service **OR** public **OR** "public service"**OR** OSN **OR** "social network"**OR** blogging **OR** blog)

  AND

  (bot **OR** botnet **OR** malware)

  AND

  (abuse **OR** exploit)

- **Boolean search strings for the grey literature**

  The Google search engine was used as a supplementary tool to help screen the grey literature (antimalware and threat intelligence report sites):

  (site:fireeye.com **OR** site:trendmicro.com **OR** site:securelist.com)

  (C2 **OR** C&C **OR** "Command and Control")

  AND

  (cloud **OR** Legitimate **OR** platform **OR** Service **OR** public **OR** "public service"**OR** OSN **OR** "social network"**OR** blogging **OR** blog)

  AND

  (bot **OR** botnet **OR** malware)

  AND

  (abuse **OR** exploit)

4.3 Study eligibility selection

The search was restricted to include only literature concerning the topic of abusing the web and cloud-based services as C&C communication channels. Because of the significant number of articles that would be obtained using the previously mentioned research strategy, it was necessary to use an assessment criterion to select those that best addressed the stated research questions. To retrieve the most relevant published articles, the following selection criteria were applied.

Inclusion criteria:

- Studies published from 2008 (when the first abuse incident was discovered) through to May 2020.
- Studies that emphasise the area of abuse cloud-based services as C&C communication channels.
- Studies that discuss approaches for identifying and/or preventing the abuse of legitimate services as C&C communication channels.

Exclusion criteria:

- Written in a language other than English.

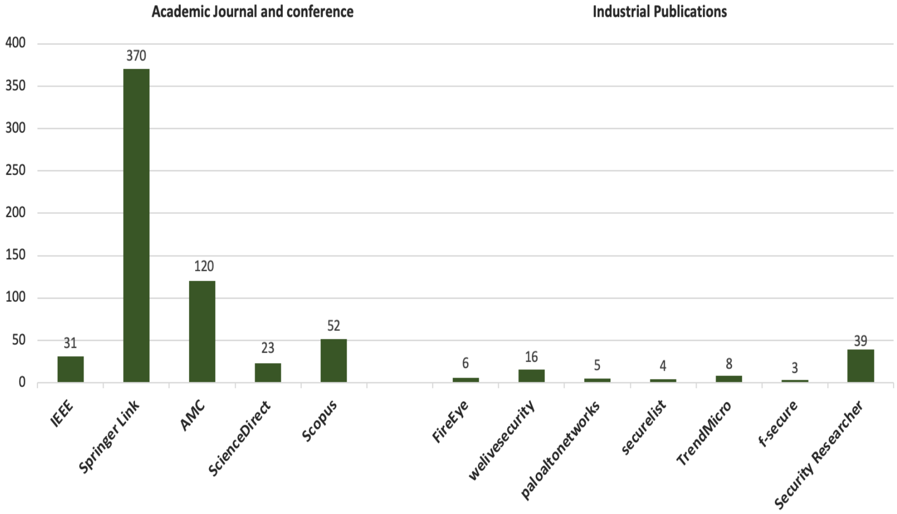


Fig. 2. The Number of Retrieved Articles from the Selected Sources According to the Academic and Industrial Publishers

- Studies that focus on the behaviour of malicious accounts or automated accounts, bots, and the use social media to amplify and spread misinformation, increase the number of fake followers, and impersonate genuine (human) accounts.
- Studies that don't provide answers to the research questions.

4.4 Data extraction strategy

Each article has been thoroughly read and the following information has been collected.

- Article title, authors' names, publication date.
- The abused cloud-based/web-based platform.
- The masquerade techniques employed to abuse legitimate platforms as C&C.
- The proposed detection mechanisms for combating the abuses of the legitimate platforms.

5 DISCUSSION:

This section presents the main findings extracted from the relevant studies with reference to the predetermined research questions. Subsequently, the research gap is addressed based on the survey results for further investigation. This review explores the masquerading techniques that have been employed to abuse cloud-based services as C&C communication channels. The significant difference between cloud-based botnets and traditional botnets is the communication mechanism. In a traditional botnet, the communication channels rely on widespread protocols such as internet relay chat (IRC), HTTP and HTTPS. However, in a cloud-based botnet, the botnet utilises legitimate platforms as C&C communication infrastructure to remain undetected for an extended period before security detection technologies have an opportunity to respond. Many abuses of cloud-based services have been performed through sophisticated mechanisms. The data in Figure 4 indicate an apparent trend in the reported abuses per year over the

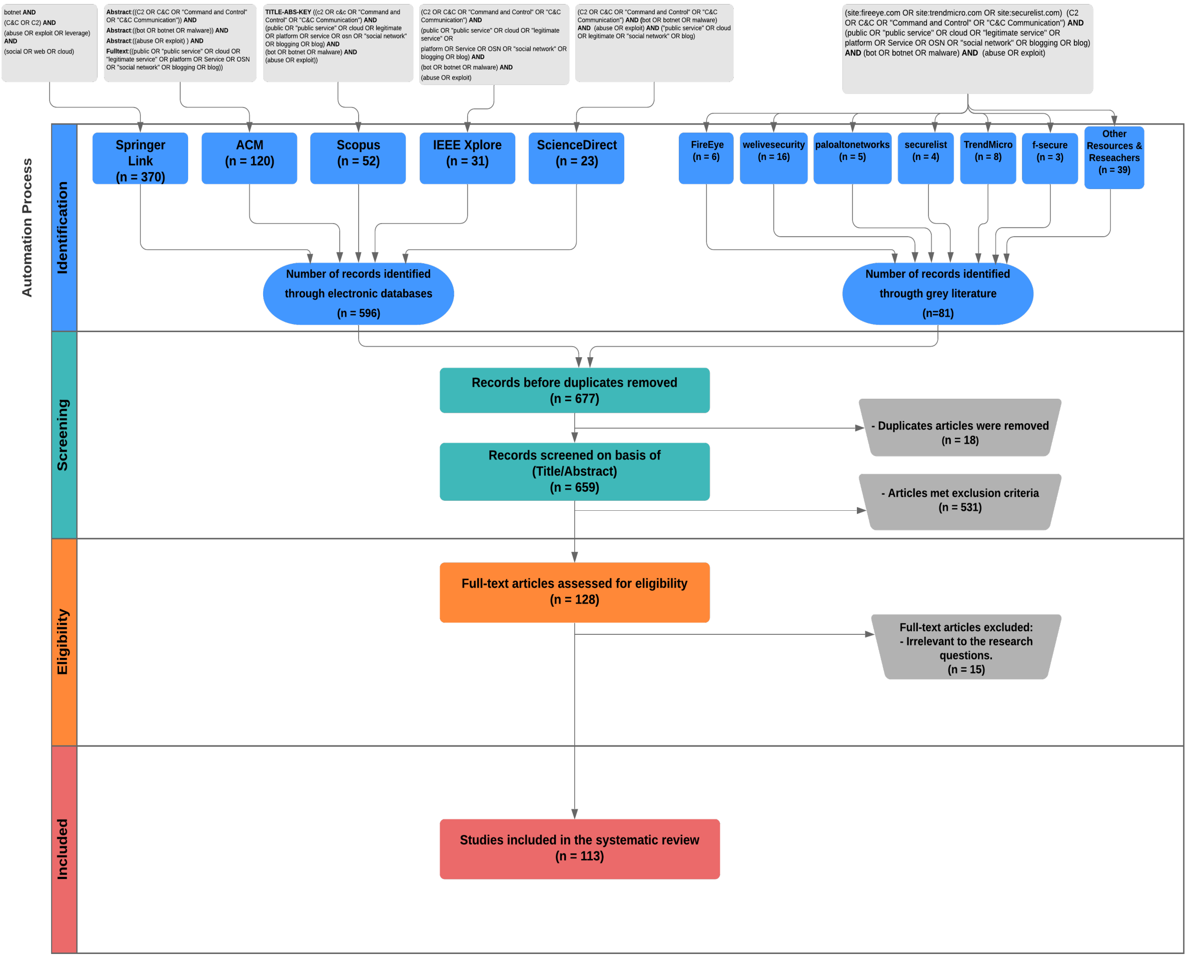

botnet AND
(C&C OR C2) AND
(abuse OR exploit OR leverage) AND
(social OR web OR cloud)
Abstract:((C2 OR C&C OR "Command and Control" OR "C&C Communication")) AND
Abstract:((bot OR botnet OR malware)) AND
Abstract:((abuse OR exploit)) AND
Fulltext:((public OR "public service" OR cloud OR "legitimate service" OR platform OR Service OR OSN OR "social network" OR blogging OR blog))
TITLE-ABS-KEY ((c2 OR c&c OR "Command and Control" OR "C&C Communication") AND
(public OR "public service" OR cloud OR legitimate OR platform OR service OR osn OR "social network" OR blogging OR blog) AND
(bot OR botnet OR malware) AND
(abuse OR exploit))
(C2 OR C&C OR "Command and Control" OR "C&C Communication") AND
(public OR "public service" OR cloud OR "legitimate service" OR
platform OR Service OR OSN OR "social network" OR blogging OR blog) AND
(bot OR botnet OR malware) AND
(abuse OR exploit)
(C2 OR C&C OR "Command and Control" OR "C&C Communication") AND (bot OR botnet OR malware) AND (abuse OR exploit) AND ("public service" OR cloud OR legitimate OR "social network" OR blog)
(site:fireeye.com OR site:trendmicro.com OR site:securelist.com) (C2 OR C&C OR "Command and Control" OR "C&C Communication") AND (public OR "public service" OR cloud OR "legitimate service" OR platform OR Service OR OSN OR "social network" OR blogging OR blog) AND (bot OR botnet OR malware) AND (abuse OR exploit)
Automation Process
Identification
Springer Link (n = 370)
ACM (n = 120)
Scopus (n = 52)
IEEE Xplore (n = 31)
ScienceDirect (n = 23)
FireEye (n = 6)
welivesecurity (n = 16)
paloaltonetworks (n = 5)
securelist (n = 4)
TrendMicro (n = 8)
f-secure (n = 3)
Other Resources & Reseachers (n = 39)
Number of records identified through electronic databases (n = 596)
Number of records identified throught grey literature (n=81)
Screening
Records before duplicates removed (n = 677)
- Duplicates articles were removed (n = 18)
Records screened on basis of (Title/Abstract) (n = 659)
- Articles met exclusion criteria (n = 531)
Eligibility
Full-text articles assessed for eligibility (n = 128)
Full-text articles excluded: - Irrelevant to the research questions. (n = 15)
Included
Studies included in the systematic review (n = 113)

Fig. 3. Flow chart of relevant articles extraction process

previous decade. The masquerade techniques extracted from the respective studies are illustrated in Figure 5 and depicted in Tables 2 and 3. For each cloud-based service, one or more empirical proof-of-concept published studies and real-world incidents reported by threat intelligence services are presented. Ultimately, these studies and incidents are categorised and described further below for each abuse technique.

The aim of this section is to answer the aforementioned questions by developing a taxonomy that classifies the employed abuse techniques based on data collected from the relevant articles. Each abuse technique was employed for one or both of the following two dimensions: **abused as a primary C&C communication channel** and **Abused as redirector to C&C domain.**

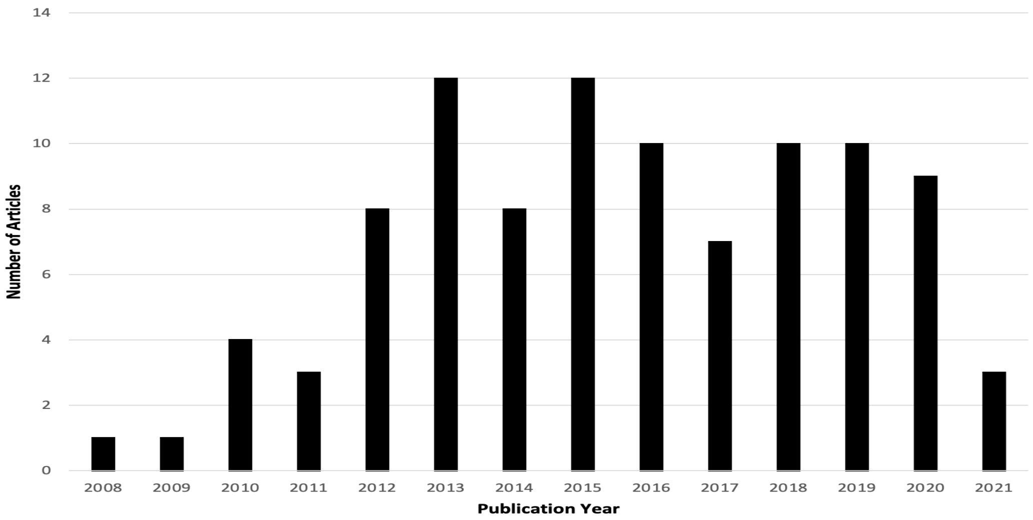


Fig. 4. The Number of Relevant Publications Per Year

5.1 Steganography

The purpose of this section is to explore the advances made in abusing the web and cloud-based platforms through image and text-steganography. The use of steganography as a covert strategy has attracted considerable attention from academia (proofs-of-concept) and threat actors (real hacking incidents). As a result, the widespread real-world experience of leveraging steganography approaches should enhance steganography countermeasures. However, the current review revealed several incidents in which legitimate services were misused using steganography techniques.

5.1.1 ***Abused as a primary C&C communication channel****.*

Elusive Social Army (ELISA) [58] is an OSN-based botnet that misused Facebook as a C&C covert channel and used victims' social media accounts as a means to spread messages. ELISA built a covert channel using a unicode steganography technique that injects non-printable characters (invisible glyphs) into the user-generated messages posted on OSNs which are not displayed during rendering. Stegobot [88] is another OSN-based botnet that leverages Facebook as a primary C&C communication channel. Stegobot utilises YASS [26] as the JPEG image steganography scheme that uses image steganography techniques to establish a communication channel within the social network. Meanwhile, Punobot [85] is an Android mobile botnet that utilises Google Cloud Messaging (GCM) as a C&C channel. GCM is an official Android push notification service (PNS). PNS is a notification service that most mobile operating systems provide to enable developers to send messages about other events to applications installed on devices. Punobot employs a steganography technique which translates the original messages into new messages to evade user and PNS server detection. HAMMERTOSS [10] is a backdoor developed by the APT29 threat-active community.

HAMMERTOSS was designed to cover the tracks of APT29 using several techniques from building an algorithm that produces regular Twitter handles to stenographic embedding images with malicious commands. Moreover, they use a domain generation algorithm (DGA) to create new Twitter handles. Whenever the malware creates a new handle, the Twitter page corresponding to that handle is fetched and the page searches for a particular pattern which is the encrypted C&C URL. HAMMERTOSS utilises Github and cloud storage services as the primary C&C communication channel to transmit commands and relay the data stolen from compromised networks. To obtain malicious commands, HAMMERTOSS implements steganography techniques through the images. Once HAMMERTOSS obtains the GitHub URL from its regular Twitter account, it will visit the page and retrieve the steganographic images that contain encrypted data. Upon successful connection and downloading, HAMMERTOSS begins the process of decryption to extract the actual command and perform the intended malicious operation.

RegDuke [20] malware employs steganography and cryptography techniques to hide data in PNG images. RegDuke's developer misuses Dropbox by hosting steganography images containing an encrypted malicious command for covert C&C operations. The backdoor lists the Dropbox directory corresponding to a client ID and the compromised machine and downloads the embedded PNG files. When images from the Dropbox directory are downloaded, RegDuke's code scans through all of the image pixels and extracts data from them. Specifically, the hidden data are extracted from the implant and the content is decrypted using an advanced encryption standard (AES) key that is hard-coded in the payload and can be one of the following other weapons of attack: Windows executable, Windows DLL, or PowerShell script.

This backdoor only resides in memory and relies on steganography to hide data in images by applying a technique called "least significant bit" to store and combine just 8 bits of data into a total of 24 bits of data per pixel: 8 for red, 8 for green and 8 for blue. RegDuke consists of a loader and a payload, both components are written in .NET. RegDuke persists by using a WMI consumer named Microsoft Office Updates. The threat technical report [20] shows that four different primary variants of the RegDuke loader were identified between August 2017 and June 2019. The first version was not obfuscated and was hard-coded on the code with the encryption key. Later versions directly read the encryption key from the Windows registry and use various means of obfuscation such as flattening the control flow or using .NET Reactor which is a commercial obfuscator.

In 2012, Shuai et al. [97] proposed a malware called SUbot that leverages blog websites to create covert channel communications to evade detection. SUbot's author implements steganography and cryptography strategies using RC4 to hide a secret message and appends the ciphertext message to the end of a JPG file. Then SUbot's author uploads the modified JPG file containing an executable command to a Blog. After the infected mobile device visits the URL of the blog site, it downloads and retrieves plain text commands from the JPG image.

*5.1.2 **Abused as redirector to C&C domain**.*

Twitter has been abused by HAMMERTOSS malware as a mapper for the malicious URL by visiting the associated Twitter account. It works by searching for a tweet with a URL and a hashtag; the URL points to the location of the C&C website with one or more images, whereas the hashtag enables HAMMERTOSS to extract encrypted instructions from an image file. The hashtag means that 101 bytes of the secret data are offset into the image file and "docto" is the characters used for decryption.

PolyglotDuke [20] is malware that is used by APT29 cyber espionage as a downloader for the MiniDuke backdoor. It uses various public websites such as Twitter, Imgur, ImgBB, or Evernote public notes to retrieve and decode the C&C URLs. Moreover, it relies on image steganography for its C&C communication channel.

*5.1.3 **Insight:***

There are several possible techniques that can be used to hide information. Essentially, methods such as steganography

Legitimate Services	Abuse Occurrences	Incident Categories	
		Reported Real-World Incident	Proof of Concept (PoC) Malware
Dropbox	13	RegDuke [20] LOWBALL [3] PlugX RAT[87] Chafer APT [40] BoxCaon [33] Crutch [64] APT31 [24] ROKRAT[106]	Chen *et al.*[54] C3[28, 51] DropSmack [108] DropboxC2 [5, 9] DropboxC2C [12, 52]
Twitter	11	HAMMERTOSS[10] PolyglotDuke[20] Nazario [89, 99] JhoneRAT [107] ROKRAT [15]	Kartaltepe *et al.*[79] Sebastian *et al.*[96] He *et al.*[71] Yulong *et al.*[62] Singh *et al.*[42] Twittor[4]
Youtube	7	Stantinko [72] Janicab[75] Casbaneiro[16] Astaroth[57, 90] Javali[32] Numando[35] Ousaban[36]	—
Google Drive	6	DarkHydrus [93], Raccoon [30], JhoneRAT [107], Pawn Storm [65] Holy Water / GOSLU [31, 74]	CloudBot [54]
Google Docs	6	Korplug [26], CARBANAK [68, 91], Backdoor.Makadocs [46, 59], JhoneRAT [107], SideWalk [102], Ousaban [36]	—
Facebook	6	Koobface [103] [39], Blackgear [53] , Javali [32]	ELISA [58] , Stegobot [88] , He *et al.* [71]
Github	6	HAMMERTOSS [10] , SunOrcal [78] , Winnti [4], MoleRATs/SneakyPastes [17], SLUB [49], Badnews [61]	—
Slack	5	SLUB [49], SLUBv2 [50] ,	Slackor [18] , SlackShell [13] , slack-c2bot [19, 22] , Hilt *et al.* [11]
Google Cloud Messaging (GCM)	4	—	Punobot [85] , CloudBot [54] , C2DM [113] , Push-Styled botnet [54]
Microsoft Outlook	4	Turla [45, 66] , GADOLINIUM [43], APT32 [8, 60]	Callidus [29]
Microsoft OneDrive	4	CLOUDDUKE [73, 75], InkySquid [34], PowerStallion [86]	CloudBot [54]
Gmail	4	ComRAT [63]	Gcat [14], Gdog [6], Singh *et al.* [101]
Pastebin	4	Scote [70], CARBANAK [68, 91] Rocke [21, 83], Numando [35]	—
Telegram	3	Telecrypt [7, 39], TeleBot.AA [56], TeleRAT [95]	—
Discord	2	—	DaaC2 [25, 27]
Evernote	2	BKDRVERNOT.A [65], PlayglotDuke [20]	—
ImgBB	2	PolyglotDuke [20], JhoneRAT [107]	—
Microsoft TechNet	1	BLACKCOFFEE [2]	—
CloudMe	1	CloudAtlas [1]	—
Imgur	1	PolyglotDuke [20]	—
Google Scripts	1	CARBANAK [68, 91]	—
Google+	1	Scote [70]	—
Facebook Instance Messenger	1	—	Socellbot [55]
File.io	1	SLUB [49]	—
Yahoo	1	CONFUCIUS_B [104]	—
Quora	1	CONFUCIUS_B [104]	—
Microsoft Teams	1	—	Callidus [29]
Microsoft OneNote	1	—	Callidus [29]
Google Sites	1	Grandoreiro [32]	—
Instagram	1	Turla [45]	—
Exchange Web Services (EWS)	1	RDAT [92]	—

Tabelle 1. Summary of Abuse Occurrences Identified per Legitimate Service from Threat Actors as a "Real-World Malware". and Security Researchers as a "Proof-of-Concept (PoC)".

have privacy-preserving mechanisms to conceal user data from unauthorised users. However, this technique has been leveraged negatively using techniques such as image steganography, text steganography, audio steganography, and file-embedding. The current research reveals a total of eight exploitation incidents in which malware employed the information hiding method to conceal malicious commands within an image or text. In particular, six malwares used steganography as their primary C&C channel, whereas the others used it as a mapper to the C&C domain name and IP address.

5.2 Encoding

5.2.1 ***Abused as a primary C&C communication channel***.

Nazario [89, 99] came across a Twitter account that was being used maliciously as a C&C operations coordinator. The botmaster set up a Twitter account called üpd4t3"to conceal and spread the malicious C&C messages. The botmaster sends out a tweet with Base64-encoded commands, which the bot then retrieved via RSS feed, decoded, and executed.

5.2.2 ***Abused as redirector to C&C domain***.

ESET researchers have discovered the Korplug [26] variant used by the Winnti group, Advanced Persistent Threat group, which utilises publicly shared Google Docs files to retrieve the C&C address of a seemingly legitimate block of text using the well-known DZKS and DZJS delimiter strings.

A trojan backdoor is shielded in an extension of Firefox that has been employed by an APT group called Turla to retrieve the C&C URL. Turla APT is a cyberespionage group that has been active for more than ten years. The C&C URL path is not contained in the extension code anywhere. The C&C URL path is accessed by utilising Instagram's comments posted on a particular Instagram post. In the analysed sample of this [**?**] threat report, the C&C domain was concealed using an encoding technique on the comment of a well-known celebrity posted to her official Instagram account. More precisely, the Firefox extension will parses through the official Instagram account's photo comments and calculates a custom hash value. If the comment hash value matches 183, this regular expression $(? : \backslash\backslash u200d(? : \#|@)(\backslash\backslash w)$ will then run against the matched comment to obtain the C&C shortened URL path, which then leads to the actual C&C URL.

Stantinko [72] is a remotely configured crypto-mining module that exhausts most of the resources of the compromised machine. Stantinko malware doesn't directly interact with its mining pool, but through a proxy's an IP address that is gathered from the YouTube video description. These C&C IP addresses are concealed in hexadecimal format in the video description string.

Janicab malware leverages YouTube citeNewsfrom45:online to obtain the C&C IP. To retrieve the actual C&C IP, the malware will navigates via the comments of particular YouTube's videos and if the *"our 50380702789658th psy anniversary"* format has been matched, the obscured number of satisfactory comments, leading to the C&C IP, will be extracted and converted to actual IP.

Palo Alto [104] addressed two different variations of malware (CONFUCIUS_A and CONFUCIUS_B) that function in very similar ways and use similar techniques, abusing the legitimate websites, instead of using DNS lookups to retrieve C&C server IP addresses. The following demonstrates how the IP for the C&C domain is decoded. CONFUCIUS_A and CONFUCIUS_B utilize Yahoo and Quora to evade traditional mechanisms by parsing keywords between specific phrases previously posted by the threat actor. Subsequently, the malware decodes the interim phrase by substituting words for components of an IP address. More precisely, A basic lookup table is adopted to decode and derive the C&C IP address.

A new variant of the SunOrcal malware family has been analysed by Palo Alto [78] which abuses the GitHub service by leveraging a de-obfuscation process of base64 and XOR decoding and to extract a C&C server. Tactically, in order to extract the data that would ultimately direct to the real C&C server, this particular sample was configured to connect to a specific file hosted at the GitHub repository. Any text between two particular strings is parsed and encoded through this target file to derive the C&C URL.

The Scote backdoor malware was discovered by Palo Alto Networks [70] and misuses legitimate third-party web platforms such as Pastebin and Google+ as a covert C&C communication channel. The Scote payload establishes the connection to these legitimate platforms' URLs to retrieve data and parse for specific commands to be executed by the compromised machine.

5.2.3 *Insights*.

All identified malware variants that use encoding as a tool to evade detection have only utilised legitimate services for a single pattern type which is a resolver to retrieve its C&C IP/domain address.

5.3 Cryptography

5.3.1 *Abused as a primary C&C communication channel*.

Shuai et al. [97] presented an innovative botnet called SUbot that is suitable for mobile platforms. SUbot leverages microblogging for evasion purposes and implements cryptography using RC4 to hide a secret message, the malicious command, and append the end of a JPG file. SUbot's author then uploads the modified JPG file containing an executable command to a Blog. When the infected mobile device visits the URL of the site, it downloads and retrieves the ciphertext commands from the JPG image.

A botnet was designed by Sebastian *et al.* [96] was able to conceal malicious commands inside a tweet in anticipation of using it as a primary C&C communication medium. The Botmaster surreptitiously injects malicious encrypted commands into tweets to evade security solutions. The malware followed the formula of `#keyword command` tweet, where the value of `command` is encrypted. Subsequently, the bot retrieves the tweet from the botmaster's fake Twitter accounts and then extracts the given cipher command which is then decrypted and interpreted to launch the attack on the infected machine.

He*et al.* [71] developed web test automation rootkit (WTAR) bot prototypes (Fbbot, Twbot, and Wbbot) that misuse Facebook, Twitter, and Weibo as C&C structures. Initially, the WTA technique was developed to automate browsers and testing websites, which can perform filling in forms, reading data from web pages, and clicking elements on web pages. The WTAR-based technique has been leveraged to imitate typical users behaviour on an OSN. To better hide the communications between WTARs and the botmaster and make it harder to be detected, both the botmaster and bot utilised the Data Encryption Protocol (DES) to encrypt the commands and their corresponding execution results using a predefined key. Turla backdoor is malware that abuses the Outlook mailbox of the victim and use it as a transport layer for its C&C, receiving commands and exfiltration data. To better conceal the malicious commands and execution results, the Turla backdoor designer takes advantage of the victim's previously opened session to gain access to the default mailbox profile [66]. In addition, the backdoor creator employs the MISTY1 symmetric encryption method, which creates specially crafted PDF documents that contain either an encrypted malicious instruction or confidential information and these are attached to the inbox of the compromised Outlook account.

ESET researchers [63] investigated a backdoor variant called ComRAT which abuses Gmail as a covert C&C channel to receive commands and exfiltrate data. The ComRAT botnet authorises the Gmail account through the credential crafted in the malware payload and then ComRAT connects to the Gmail HTML web interface to facilitate parsing for an email containing a particular subject. Once matched, the email attachment is downloaded and decrypted via the AES-256 algorithm to extract the malicious command for execution. The executed command result is then encrypted using RSA-2048 and emailed to the threat actor, often hosted on GMX or VFEmail. To ensure persistence, ComRAT developers rely on a technique known as COM hijacking to tamper with the Windows registry which leads to the ComRAT botnet being executed every time the user logs in.

RegDuke [20] malware utilises cryptography techniques to secure the data transmitted between the botmaster and bots. As illustrated in Section 5.1.1, once an image is downloaded from Dropbox, the bot loops over the image pixels and extracts the data. The bot then decrypts the information with an AES key hard-coded in the payload to retrieve malicious commands.

The CloudMe platform was misused by CloudAtlas malware [1] as a covert channel of communication. As a securement of the transmitted messages to be undetectable between the attacker and the victim, the CloudAtlas malware's designer employed cryptography with AES and data compression with LZMA techniques. The malware was configured to include encrypted content of the following: C&C's CloudMe URL, a username and password, two folders on the CloudMe server to store malicious commands and upload the victim's data. The encrypted malicious commands are uploaded to the account by the threat actor which the malware downloads, decrypts and interprets. The malware then uses the same mechanism to upload the result back to the server.

5.3.2 *Abused as redirector to C&C domain*.

A botnet design that combines QR codes, Twitter search, DGA, cryptography (AES and RSA), and Tor has been proposed [62]. In their design, Twitter has been utilised as a mapper to the C&C web server by querying the Twitter search engine for a particular keyword to locate the published post from the botmaster, including the QR code image. After the QR code has been successfully scanned, the encoded combination of the three components (the C&C web server address, the hard-coded token, and the RSA public key) is retrieved. The recovered RSA public key is used to encrypt the leaked data to be conveyed to the C&C web server.

Casbaneiro botnet [16] utilises the YouTube website to store its C&C server domains. The malware operator of Casbaneiro leverages the contained description of a specific YouTube video to embed an encrypted C&C web server address in a bogus Facebook or Instagram URL to redirect compromised machines to the threat actor's C&C infrastructure.

5.3.3 *Insights*.

To better conceal the bidirectional transmitted information between the botmaster and its bots, the Cybercriminals encrypt messages using different encryption techniques to mask the command and execution results. Thus, this poses a challenge to security protection solutions. Furthermore, whereas some encryption algorithms are easy to crack, this decryption process can be time consuming and expensive.

5.4 Fraudulent accounts

5.4.1 *Abused as a primary C&C communication channel*.

ELISA [58] is an OSN-based botnet that allows the botmaster to communicate with their bots by relying on the unaware user's interactions and hiding their messages inside the victim's posts. ELISA forms an overlay network which interacts with typical users to deliver messages to the whole botnet. For the sake of confidentiality, C&C communication is secured using encryption and a signature between the botmaster and their bots.

Sebastian et al. [96] used Twitter as a key C&C communication medium by creating malware that concealed a malicious command within a tweet. The bot (described in Section 5.1.1) receives a tweet from the botmaster's bogus Twitter accounts and extracts the provided cipher command which is then decrypted and interpreted to initiate an attack on the infected system.

5.5 Botmaster Login Credentials or Hard-coded Token

5.5.1 ***As Primary C&C Communication Channel.***

Nazario [89, 99] recognised a Twitter account that was being utilised maliciously as the C&C operations coordinator. To disguise and disseminate the malicious C&C commands, the botmaster created a Twitter account called üpd4t3."The botmaster used this account to send out a tweet containing Base64-encoded commands, which the bot then obtained via really simple syndication (RSS) feed, decoded, and executed to establish a covert C&C communication route.

Singh *et al.* [42] developed another OSN-based botnet called SocialNetworkingBot that utilises Twitter for its C&C structure. The malware author leverages an official Twitter account authentications to post tweets containing disguised commands interpreted by bots. The botmaster posts tweets from approximately 300 pre-defined keywords to help fetch the tweets. To retrieve these tweets from the botmaster account that serves as a rendezvous point, bots send a query to the Twitter search engine for particular keywords. The bots will fetch these tweets to execute the malicious commands.

Telecrypt is ransomware [7, 39] that abuses the Telegram instant messaging service API for its C&C infrastructure. Initially, the botmaster created a Telegram bot, which uses TeleCrypt ransomware to communicate between the threat actors and the victim's machine. Once infected a machine. Once a machine has been infected, the ransomware employs two methods of the Telegram ('GetMe' and 'sendMessage') which enables the ransomware via the 'GetMe' method to determine whether or not the attacker's telegram bot exists. Following the successful existence, the 'sendMessage' method is used to exfiltrate the victim's data to the chat thread of the attacker's number which is hard-coded into the ransomware body. The leaked parameters include the number of the chat with the cybercriminal, the name of the infected computer, the infection ID, and the number used to generate the file encryption key.

ESET researchers revealed a unique malicious toolkit called TeleBot.AA [56] which was created by the TeleBots group APT and was designed to abuse Telegram as its main C&C communication channel. Telegram abuse is carried out using the Telegram Bot API. Each backdoor version has unique hard-coded credentials, implying that each sample has a Telegram Messenger account. The C&C communication interactions, post commands and retrieve results between the attacker and the compromised computers occur through Telegram private chats.

Palo Alto Networks [95] explored a malicious Android trojan called "TeleRAT"which had a malicious version of the app for abusing the Bot API of Telegram as a means of spreading C&C activities. The TeleRAT spyware gains access to the victim's Telegram app by disguising itself as a legitimate application that claims to be able to give a count of how many people have visited the victim's Telegram profile. The attacker's Telegram bot API keys are hard-coded in the APKs to use to continually beacon at regular intervals of every 4.6 seconds and listen for specific commands.

TrendMicro [65] detected malware called BKDR_VERNOT.A that uses a clever manoeuvre to evade detection by misusing legitimate services such as Evernote (a web note-taking app) as a proxy server to communicate with the botmaster. If the BKDR_VERNOT.A successfully infects the victim's machine, it will drop a .DLL file that injects itself into a legitimate process, creating genuine network traffic to avoid detection by security solutions. The BKDR_VERNOT.A payload connects to the saved notes using official Evernote account credentials that are hard-coded into the malware, allowing the backdoor to retrieve the malicious commands and upload the stolen data as a drop-off zone.

SLUB is a backdoor that was discovered and evaluated by TrendMicro [49], which abuses three legitimate platforms (Slack, GitHub, and File.io) for its C&C infrastructure. The threat actor sets up a Slack workspace and GitHub account to serve as the SLUB backdoor C&C's operations. In order to communicate with the Slack API, the SLUB's designer embeds two hard-coded authentication tokens. SLUB's operator uploads malicious commands to GitHub snippets, extracted and executed by the backdoor; the commands' results are then uploaded to a Slack and File.io. Four months after the first version of SLUB was identified, TrendMicro [50] discovered a variant of the SLUB. However, the evolved version stopped using GitHub for C&C operations and instead adopted Slack's workspaces as a C&C covert communication channel between the malware and its handler. The revised version of the SLUB applies the same authentication approach as the previous version between the backdoor and its controller. Once the victim's machine has been infected by the SLUB backdoor and they wants to join Slack's workspace, it creates a new channel titled `<use_name>-<pc_name>`. If the SLUB threat actor wants to execute a malicious command, they releases the message to a victim-specific channel in Slack, SLUB in the victim machine, and then correspond by parsing and executing the requested command.

The CloudMe platform was abused by CloudAtlas malware [1] as a covert channel of communication. To ensure that the transmitted messages between the attacker and victim cannot be detected, the CloudAtlas malware's designer employs cryptography with AES and data compression with LZMA techniques. The malware was configured to include encrypted content of the following: C&C's CloudMe URL, a username and password, and two folders on the CloudMe server to store malicious commands and upload the victim's data. The encrypted malicious commands are uploaded to the account by the botmaster which the malware downloads, decrypts and interprets. The malware then uses the same mechanism to upload the result back to the server.

CloudAtlas malware [1] abuses the CloudMe platform, as noted in Section 5.3.1. The CloudAtlas malware's inventor uses AES and Lempel-Ziv-Markov chain-Algorithm (LZMA) encryption and compression methods to ensure that the communications transmitted between the botmaster and its bot remain undetected. CloudAtlas was developed to encrypt the following information: C&C's CloudMe URL, a username and password, and two folders on the CloudMe server to store the malicious commands and upload the victim's data. The encrypted malicious commands upload to the account of the botmaster and they are then downloaded by the bot, decrypted and interpreted to carry out additional adversarial operations.

Zhao et al. [113] introduced C2DM, a novel Android botnet architecture that abuses Google's Cloud to Device Messaging (C2DM) for C&C command dissemination. C2DM is a cloud-based push notification service for Android app developers. The Google C2DM service was utilised in this botnet to avoid a direct connection between the botmaster and the bots. The malicious bot traffic is blended with the C2DM traffic of other legal Android smartphone apps to covertly transmit C2DM botnet traffic. Furthermore, Zhao et al. [113] indicated that many of the latest botnet detection strategies are incapable of detecting push-like mobile because all push-style bots and legal applications bind official push servers to receive updates.

Chen *et al.* developed a CloudBot which is an enhanced version of the Push-Styled botnet [54]. CloudBot is a smartphone hybrid structure botnet (e.g., hierarchy structure and P2P structure) that exploits ten cloud-based push services (GCM, JPush, XGPush, ZYPush, GeXinPush, Airbop.) as a C&C downstream channel and renowned cloud services including Dropbox, Microsoft OneDrive, and Google Drive as a C&C upstream channel. CloudBot's design enables botmasters to send commands to bots disguised as legitimate push traffic through cloud-based push services and CloudBot then uploads the extracted data via cloud-based storage services. The crucial aspect of a mobile botnet using push services is to avoid direct communication with C&C servers to retrieve commands. CloudBot gains access to cloud storage services by encapsulating the account information and access token in a push message that is then conveyed to bots leveraging the push services. Cloud-based push services only support text messages. To satisfy this requirement and evade detection during command transmission, the CloudBot is equipped with three levels of obfuscation: encryption, encoding and high-order mimic functions.

5.5.2 ***As redirector to C&C domain.***

Chen *et al.* [54] designed and implemented a push-style botnet that was Android-based and leveraged Google's message push service GCM as a mapper to direct users to the C&C URL domain to carry out malicious activities.

5.6 Real victims' accounts

5.6.1 ***Abused as a primary C&C communication channel.***

The Turla malware [66], as discussed in Sections 5.3.1 and 5.7.1, takes advantage of the victim's previously opened session to gain access to the default mailbox profile [66]. Hence, it occurs between the Outlook compromised email and botmaster email via either an encrypted malicious instruction or encrypted PDF attachments.

5.6.2 ***Abused as redirector to C&C domain.***

The Koobface botnet [103] [39] is a social botnet that leverages popular social networking sites such as Facebook and Twitter as its primary means of propagation. To accomplish this task, legitimate social network users are spammed and routed across several URL redirection obfuscation levels to evade blocklist detection using blogs, RSS feeds and shortened URLs to resolve and connect to the C&C URL.

5.7 Component object model (COM) hijacking

5.7.1 ***Abused as a primary C&C communication channel.***

Researchers from ESET [66] have analysed Turla backdoor which is malware that abuses the Outlook mailbox of the victim and uses it as a transport layer for its C&C communication channel, receiving commands and exfiltration data. Once Turla backdoor has infected the host, it leverages the legitimate messaging application programming interface (MAPI) to interact with Outlook and access the target mailbox profile using the compromised system. Subsequently, the malware has complete control over the target mailbox in addition to the other MAPI features. For persistence and stealth, Turla backdoor operators rely on a technique known as COM to tamper with the Windows registry. COM is a Microsoft technology that allows developers to manage and modify other applications' objects. Communications between the botmaster and its bot rely on the email-based C&C channel, meaning that the operational commands and leaked information will be transmitted between the Outlook compromised email and botmaster email via specially-crafted and encrypted PDF attachments.

5.8 Bot's malicious process injects itself into benign process

5.8.1 ***Abused as a primary C&C communication channel.***

As discussed in Section 5.5.1, The BKDR_VERNOT.A malware [65] abuses the Evernote platform and uses official Evernote account credentials that are hard-coded into the bot's binary the bot to retrieve the malicious commands and upload the stolen data as a drop-off zone.

5.9 COMSPEC environment variable

5.9.1 ***Abused as a primary C&C communication channel.*** BoxCaon backdoor was unveiled by a checkpoint researcher [33], which abuses the Dropbox service as a C&C infrastructure. For the backdoor to execute the malicious command, it uses the COMSPEC environment variable, which points to the command line interpreter (cmd.exe).

5.10 Exploit multiple processes

5.10.1 ***Abused as a primary C&C communication channel.*** Wbbot is a social bot designed by Yuede et al. [76] to abuse Twitter for C&C operations by dividing malicious behaviours into multiple processes to evade behaviour detection. In this way, each process only engages in one malicious behaviour and then behaves benignly.

6 WIDELY ABUSED LEGITIMATE WEB AND CLOUD-BASED SERVICES

The categories of abused notable legitimate web and cloud-based services that have been reported in the empirical literature as C&C stealthy communication channels are listed below in terms of their popularity, as illustrated in Table 1:

- Social media platforms (e.g., Twitter and Facebook)
- Online cloud storage sites (e.g., Dropbox, Mediafire, and GoogleDrive)
- Business communication platform (e.g., Slack)
- Online developers' repositories. (e.g., GitHub)
- Online clipboard sites (e.g., Pastebin)
- Push services for iOS and Android notification (e.g., GCM,JPush,XGPush,ZYPush,GeXinPush, and Airbop)
- Online photo and video sharing (e.g., YouTube and Instagram)
- Email service (e.g., Outlook and Gmail)
- Digital distribution platform (e.g., Discord)
- Cloud-based instant messaging software (e.g., Telegram, Facebook Instance Messenger)

7 DETECTION MECHANISM

There are only four countermeasure approaches that have been proposed to detect could-native platforms abuses as C&C communication channels. Three of the detection strategies have been implemented in the computer environment [77, 79, 105], whereas only one has been implemented in the Android phone environment [38].

Kartaltepe *et al.* [79] advocate abuse detection at two levels: client-side and server-side. At the host-side detection zone, three features have been defined to determine provenance. They presume that connecting to social media is suspicious if it is not the result of human behaviour. They use behavioural biometrics, reacting to user inputs and using graphical user interfaces as a detection attribute to distinguish between legitimate users and bots. For server-side detection, they assume that communication with social media is suspicious if the transmitted message or post is textually encoded. They use the J48 decision tree algorithm to classify input messages to discriminate between Base64 or Hexadecimal-encoded text and plain language content. However, these detection approaches have certain drawbacks, as follows: i) lack of real-time detection because the detection mechanisms are simulated in the post-analysis environment lab; ii) this means of detection may be defeated if the malware author has intimate knowledge of the implementation details of the detection system; iii) this detection approach will be bypassed if the adversary uses the image-steganography technique to conceal a malicious command within the post.

Botnet/PoC Tool)	Abused Platform	Abused As	*Employed Masquerade Techniques and Adversary Methodologies*								
			Stenography	Encoding	Cryptography	Fraudulent Account	Botmaster Credentials Hard-coded Token	Real victims' accounts	COM Object Hijacking	Malicious Process Inject into Legit Process	ComSpec environment variable
Singh *et al.* [101]	Gmail	Primary C&C Channel			✓		✓				
ELISA (Elusive Social Army) [58]	Facebbok	Primary C&C Channel	✓			✓					
Stegobot [88]	Facebbok	Primary C&C Channel	✓								
RegDuke [20]	Dropbox	Primary C&C Channel	✓								
HAMMERTOSS [10]	Twitter Github	Redirector to C&C Domain Primary C&C Channel	✓		✓						
Punobot [85]	Google Cloud Messaging (GCM)	Primary C&C Channel	✓								
PlayglotDuke [20]	Twitter, Evernote, Imgur, ImgBB	Redirector to C&C Domain		✓	✓						
Nazario [89, 99]	Twitter	Redirector to C&C Domain		✓							
Kartaltepe *et al.* [79]	Twitter	Redirector to C&C Domain		✓							
Korplug [26]	Google Docs	Redirector to C&C Domain		✓							
Turla [45, 66]	Microsoft Outlook Instagram	Primary C&C Channel Redirector to C&C Domain		. ✓	✓ .				✓ .		
Stantinko [72]	Youtube	Redirector to C&C Domain		✓							
Janicab [75]	Youtube	Redirector to C&C Domain		✓							
CONFUCIUS_B [104]	Yahoo, Quora	Redirector to C&C Domain		✓							
SunOrcal [78]	GitHub	Redirector to C&C Domain		✓							
TeleBot.AA [56]	Telegram	Primary C&C Channel					✓				
Shuai *et al.* [97]	Blog, picture-hosting site	Primary C&C Channel	✓		✓						
Sebastian *et al.* [96]	Twitter	Primary C&C Channel		✓	✓	✓					
He*et al.* [71]	Twitter, Facebook, Weibo	Primary C&C Channel			✓						
Yulong*et al.* [62]	Twitter	Redirector to C&C Domain		✓	✓						
ComRAT [63]	Gmail	Primary C&C Channel			✓				✓		
CloudAtlas [1]	CloudMe	Primary C&C Channel			✓		✓				
Casbaneiro [16]	Youtube	Redirector to C&C Domain			✓						
BKDR_VERNOT.A [65]	Evernote	Primary C&C Channel					✓			✓	
Singh *et al.* [42]	Twitter	Primary C&C Channel					✓				
Telecrypt [7, 39]	Telegram	Primary C&C Channel					✓				
TeleRAT [95]	Telegram	Primary C&C Channel					✓				
SLUB [49]	Slack, Github, File.io	Primary C&C Channel					✓				
SLUBv2 [50]	Slack	Primary C&C Channel					✓				
Scote [70]	Pastebin, Google+	Redirector to C&C Domain		✓							
C2DM - Zhao*et al.* [113]	Google Cloud Messaging (GCM)	Primary C&C Channel					✓	✓			
Socellbot [55]	Facebook Instance Messenger	Redirector to C&C Domain		✓							
Koobface [103] [39]	Facebook, Twitter	Redirector to C&C Domain		✓				✓			
CARBANAK [68, 91]	Google Docs, Google Scripts, Pastebin	Primary C&C Channel					✓				
Backdoor.Makadocs [46, 59]	Google Docs	Primary C&C Channel					✓				
Astaroth [57, 90]	Youtube	Redirector to C&C Domain		✓	✓						
Rocke [23, 83]	Pastebin	Primary C&C Channel		✓							

Tabelle 2. Real-World Botnet and Proof of Concept (POC) Research liked to the Abused Platforms and Employed Adversarial Techniques

Reference Botnet/Research Tool)	Abused Platform	Abused As	Employed Masquerade Techniques and Adversary Methodologies								
			Stenography	Encoding	Cryptography	Fraudulent Account	Botmaster Credentials Hard-coded Token	Real victims' accounts	COM Hijacking	Malicious Process Inject into Legit Process	ComSpec environment vari
LOWBALL [3]	Dropbox	Primary C&C Channel					✓				
BLACKCOFFEE [2]	Microsoft TechNet	Redirector to C&C Domain		✓							
Winnti (BKDR64_WINNTIONM) [4]	Github	Redirector to C&C Domain		✓			✓				
Blackgear [53]	Facebook	Redirector to C&C Domain		✓							
PlugX RAT [87]	Dropbox	Redirector to C&C Domain					✓				
CLOUDDUKE [73, 75]	Microsoft OneDrive	Primary C&C Channel					✓				
DarkHydrus [93]	Google Drive	Primary C&C Channel		✓							
Raccoon [30]	Google Drive	Redirector to C&C Domain			✓						
GADOLINIUM [43]	Outlook	Primary C&C Channel						✓			
Holy Water / GOSLU [31, 74]	Google Drive	Primary C&C Channel		✓			✓				
APT32 [8, 60]	Outlook	Primary C&C Channel		✓				✓			
JhoneRAT [107]	Twitter, ImgBB, Google Forms, Google Drive	Primary C&C Channel		✓		✓					
Pawn Storm [65]	Google Drive	Primary C&C Channel		✓			✓				
Chafer APT [40]	Dropbox	Primary C&C Channel					✓				
Badnews [61]	Github	Redirector to C&C Domain		✓							
InkySquid [34]	Onedrive	Primary C&C Channel					✓				
BoxCaon [33]	Dropbox	Primary C&C Channel					✓				✓
Crutch [64]	Dropbox	Primary C&C Channel			✓		✓				
APT31 [24]	Dropbox	Primary C&C Channel			✓		✓				
Javali [32]	Youtube, Facebook	Redirector to C&C Domain			✓						
PowerStallion [86]	Microsoft OneDrive	Primary C&C Channel			✓		✓				
ROKRAT [15, 106]	Twitter, Yandex cloud, Mediafire, PCLOUD, Dropbox	Primary C&C Channel					✓				
Numando [35]	YouTube, Pastebin	Redirector to C&C Domain			✓						
SideWalk [102]	Google Docs	Redirector to C&C Domain			✓						
Ousaban [36]	Google Docs, YouTube	Redirector to C&C Domain			✓						
Grandoreiro [32]	Google Sites	Redirector to C&C Domain					✓				
RDAT [92]	Exchange Web Services (EWS)	Primary C&C Channel	✓				✓	✓			
SLBot, BTM, PR-Bot [109–111]	Dropbox, pastebin, MediaFire,	Primary C&C Channel	✓	✓	✓						
DropboxC2 [5, 9, 52]	Dropbox	Primary C&C Channel					✓		✓		
DropboxC2C [12]	Dropbox	Primary C&C Channel					✓				
C3 [28, 51]	Dropbox	Primary C&C Channel					✓				
DropSmack [108]	Dropbox	Primary C&C Channel						✓			
Twittor [4]	Twitter	Primary C&C Channel					✓				
Slackor [18]	Slack	Primary C&C Channel			✓		✓				
SlackShell [13]	Slack	Primary C&C Channel					✓				
slack-c2bot [19, 22]	Slack	Primary C&C Channel					✓				
DaaC2 [25, 27]	Discord	Primary C&C Channel	✓			✓					
Rocke [21]	Pastebin	Redirector to C&C Domain				✓					
Gdog [6]	Gmail	Primary C&C Channel			✓		✓				
Gcat [14]	Gmail	Primary C&C Channel					✓				
Callidus [29]	Microsoft Teams, Outlook, OneNote	Primary C&C Channel				✓					
CloudBot Chen et al [54]	Google Cloud Messaging (GCM)	Redirector to C&C Domain	✓					✓			

Yuede *et al.* [77] proposed a behaviour tree-based detection framework for identifying social bots by monitoring host activity. The proposed framework comprised three components: a host behaviour monitor, host behaviour analyser, and detection approach. To better understand and construct a suspicious host behaviour tree for analysis purposes, they designed a social botnet called wbbot as well as utilising a collection of samples from two resources: existing real-world social bots [[103] [39] [42, 99] and researcher malware samples of social bots [88]. After executing and analysing the collection of social media for a period of time, offline processes were utilised to generate a template library which was then used to calculate the highest similarity value between the suspicious behaviour trees. Following the construction of the behaviour tree, the similarity with the template was calculated using the tree edit distance to generate the final detection result. The drawback with this detection approach is the high rate of 29.6%. It can also be evaded if the attacker uses a multiple process mechanism or splits malicious behaviour across multiple time windows.

Ahmadi *et al.* [38] presented a detection approach to identify malicious Android applications using GCM flows. The authors used the modified Flowdroid tool [41] for flow analysis which was extended to extract GCM flows from Android apps by discriminating the GCM callbacks. These GCM flows were then utilised as vector space features in a machine learning model. The mean impurity rating for each feature was calculated to reduce noise and remove irrelevant features, and the features with the highest ratings were retained. These derived features of GCM flows can effectively discriminate malicious applications from benign applications.

Vo *et al.* [105] presented an API verifier which is a tool that uses CAPTCHA verification to verify the social media account authentication using the MAC address and determine if an API call is from a human or a bot before performing the API call to prevent automated bot actions. However, modern botnets can bypass verification code verification by using a technique known as a relay attack.

Ghanadi *et al.* [67] investigated stego-botnets that utilise steganographic images on online social networks for C&C functions. They presented SocialClymene, which is constructed to calculates each user's negative reputation score based on their history. In a suspicious group activity graph, SocialClymene adds up the incoming normalised suspicious values, which are weighted by the negative reputation scores of their neighbours.

By measuring causality between user activity and network traffic, Burghouwt *et al.* [47] presented a causality detection mechanism for identifying Twitter-based C&C channel communication. According to the authors, any network-traffic event to the OSN that is not caused by human events based on specific keystrokes or mouse actions is anomalous. The causality detection approach uses a timeframe that starts immediately after a user event to distinguish between network events triggered by user actions and those that are bot-originated. However, this detection approach suffers from drawbacks. First, legal API used for periodically automated polling on Twitter will be assumed to be anomalous. Second, the main parameters used to assess the timeframe between user activity and the network request are inaccurate because each machine and operating system has different delay times and performs differently. Third, specific advanced bots can bypass this detection technique by monitoring user events and executing based on user-triggered events.

Yuede *et al.* [76] empirically evaluated some of the previous abusive social bot mechanisms by collecting the source codes, builders and execution traces of several existing social botnets including Twitterbot (Singh [100]),Twebot (Burghouwt *et al.* [48],Yazanbot (Boshmaf *et al.* [44]), Nazbot (Kartaltepe *et al.* [79]), wbbot (Ji *et al.* [112]), and fbbot, to analyse mechanisms used to evade existing detection approaches. Then, based on an analysis of the social bots, the authors introduced a detection strategy that includes nine newly identified features with spatial and temporal correlations and nine features from existing detection methods. A spatial correlation is a way to combat malicious behaviours spread across multiple processes by uniting the children processes.

Although most of the previous detection mechanisms suffer from limitations, as stated above, all detection works are primarily concerned with detecting abuse on social networking platforms. Thus, further research is required to detect the abuse of cloud-based services as a C&C infrastructure.

Tabelle 4. Summary of the detection mechanisms for the Cloud-Based Abuses as C&C Channel, for details refer to section 7

Reference	Detection of Cloud-Based Abuses as C&C Channel								Detection Mechanism
	Signature-Based				Anomaly-Based				
	Passive		Active		Passive		Active		
	Host-Based	Server-Based	Host-Based	Server-Based	Host-Based	Server-Based	Host-Based	Server-Based	
Yuede *et al.* [77]					✓				Use behavior tree-based to identifying the bot through monitoring host activity. Once the behavior tree has been constructed, the similarity to the template will be calculated using the tree edit distance to generate the final detection result.
Kartaltepe *et al.* [79]					✓	✓			*Host-Based:* Assumes that connecting to social media is suspicious if it is not the result of human behavior. Using behavioral biometrics: reacting to user input via a keyboard or mouse and using Graphical User Interface (GUI)as a detection attribute to distinguish between legitimate user and bot. *Server-Based:* Assumes that communication with social media is suspicious if the sent message or post are textually encoded. To classify input messages: J48 decision tree algorithm was implemented to classify input messages.
Ahmadi *et al.* [38]					✓				Use modified Flowdroid tool as flow analysis to extract GCM flows. Then, it utilised the GCM as vector space features in a machine learning model to identify the malicious Android application.

Table 4 continued from previous page

Reference	Detection of Cloud-Based Abuses as C&C								Detection Mechanism
	Signature-Based				Anomaly-Based				
	Passive		Active		Passive		Active		
Vo *et al.* [105]								✓	Employ CAPTCHA verification to verify the social media account using the MAC address and determine if an API call is from a human or a bot
Ghanadi *et al.* [67]								✓	SocialClymene sums the incoming normalised suspicious values, which are weighted by the negative reputation scores of its neighbours.
Burghouwt *et al.* [47]					✓				The causality detection approach uses a time frame that starts immediately after a user event to distinguish between network events triggered by user actions and those bot-originated.
Yuede *et al.* [76]					✓				Use spatial correlation and new features to combat malicious behaviors spread across multiple processes by uniting the children processes.

8 CONCLUSION AND FUTURE WORK

According to the findings of this analysis, the majority of the publications in this review investigate abusive strategies, whereas less emphasis has been dedicated to detection approaches. Because of the tremendous expansion in the use of cloud-based solutions by individuals, small companies, large enterprises and governments, threat actors are increasingly abusing such platforms. To confront such an open problem, it is necessary to understand evolving covert channel strategies as malware developers continually devise new ways to evade detection. Thus, the current study has systematically reviewed the relevant empirical literature and presented SLR to provide a comprehensive description of numerous offensive techniques employed to abuse cloud-based legitimate services as a relay and C&C mechanism. Between 2008 and October 2021, 113 relevant articles from academic and industry publications were chosen and evaluated for this SLR. A taxonomy of the abusive strategies has been presented which includes the following: steganography, encoding, cryptography, fraudulent account, COM hijacking, and bots injecting themselves into other benign processes. The primary objective of the current research was to attract the attention of organisations and the research community to these sophisticated threats which leverage legitimate services to disguise malware's C&C functions. According to the research examined in the current paper, the security strategies proposed in the empirical literature still lack mechanisms to identify these obfuscation stealth tactics. Therefore, further research should be carried out to design a robust real-time detector.

LITERATUR

[1] 2014. Cloud Atlas: RedOctober APT is back in style | Securelist. https://securelist.com/cloud-atlas-redoctober-apt-is-back-in-style/68083/.

[2] 2015. APT17: Hiding in Plain Sight - FireEye and Microsoft Expose Obfuscation Tactic | FireEye. https://www.fireeye.com/current-threats/apt-groups/rpt-apt17.html.

[3] 2015. China-based Cyber Threat Group Uses Dropbox for Malware Communications and Targets Hong Kong Media Outlets | Mandiant. https://www.mandiant.com/resources/china-based-threat. 14.

[4] 2015. GitHub - PaulSec/twittor: A fully featured backdoor that uses Twitter as a C&C server. https://github.com/PaulSec/twittor.

[5] 2016. GitHub - Arno0x/DBC2: DBC2 (DropboxC2) is a modular post-exploitation tool, composed of an agent running on the victim's machine, a controler, running on any machine, powershell modules, and Dropbox servers as a means of communication. https://github.com/Arno0x/DBC2.

[6] 2016. GitHub - maldevel/gdog: A fully featured Windows backdoor that uses Gmail as a C&C server. https://github.com/maldevel/gdog.

[7] 2016. TeleCrypt - the ransomware abusing Telegram API - defeated! | Malwarebytes Labs. https://blog.malwarebytes.com/threat-analysis/2016/11/telecrypt-the-ransomware-abusing-telegram-api-defeated/.

[8] 2017. APT32, SeaLotus, OceanLotus, APT-C-00, Group G0050 | MITRE ATT&CK®. https://attack.mitre.org/groups/G0050/.

[9] 2017. Command and Control – DropBox – Penetration Testing Lab. https://pentestlab.blog/2017/08/29/command-and-control-dropbox/.

[10] 2017. HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group | FireEye. https://www.fireeye.com/current-threats/apt-groups/rpt-apt29.html.

[11] 2017. How New Chat Platforms Can Be Abused by Cybercriminals - Noticias de seguridad - Trend Micro ES. https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/how-new-chat-platforms-abused-by-cybercriminals.

[12] 2018. GitHub - 0x09AL/DropboxC2C: DropboxC2C is a post-exploitation agent which uses Dropbox Infrastructure for command and control operations. https://github.com/0x09AL/DropboxC2C.

[13] 2018. GitHub - bkup/SlackShell: PowerShell to Slack C2. https://github.com/bkup/SlackShell.

[14] 2018. GitHub - byt3bl33d3r/gcat: A PoC backdoor that uses Gmail as a C&C server. https://github.com/byt3bl33d3r/gcat.

[15] 2018. Threat Analysis: ROKRAT Malware - VMware Security Blog - VMware. https://blogs.vmware.com/security/2018/02/threat-analysis-rokrat-malware.html.

[16] 2019. Casbaneiro: Dangerous cooking with a secret ingredient | WeLiveSecurity. https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerous-cooking/.

[17] 2019. Gaza Cybergang Group1, operation SneakyPastes | Securelist. https://securelist.com/gaza-cybergang-group1-operation-sneakypastes/90068/.

[18] 2019. GitHub - Coalfire-Research/Slackor: A Golang implant that uses Slack as a command and control server. https://github.com/Coalfire-Research/Slackor.

[19] 2019. GitHub - praetorian-inc/slack-c2bot: Slack C2bot that executes commands and returns the output. https://github.com/praetorian-inc/slack-c2bot.

[20] 2019. Operation Ghost: The Dukes aren't back – they never left | WeLiveSecurity. https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/.

[21] 2019. Rocke Evolves Its Arsenal With a New Malware Family Written in Golang | Anomali Labs. https://www.anomali.com/blog/rocke-evolves-its-arsenal-with-a-new-malware-family-written-in-golang.

[22] 2019. Using Slack Web Services as a C2 Channel (ATT&CK T1102) - Praetorian. https://www.praetorian.com/blog/using-slack-as-c2-channel-mitre-attack-web-service-t1102/.

[23] 2020. 2020 Cloud Computing Study • IDG. https://www.idg.com/tools-for-marketers/2020-cloud-computing-study/.

[24] 2020. APT-31 Leverages COVID-19 Vaccine Theme | Zscaler Blog. https://www.zscaler.com/blogs/security-research/apt-31-leverages-covid-19-vaccine-theme-and-abuses-legitimate-online.

[25] 2020. DaaC2 - Using Discord as a C2 | Crawl3r. https://crawl3r.github.io/2020-01-25/DaaC2.

[26] 2020. ESET_Threat_Report_Q22020.pdf. https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf.

[27] 2020. GitHub - crawl3r/DaaC2: Discord as a C2. https://github.com/crawl3r/DaaC2.

[28] 2020. GitHub - FSecureLABS/C3: Custom Command and Control (C3). A framework for rapid prototyping of custom C2 channels, while still providing integration with existing offensive toolkits. https://github.com/FSecureLABS/C3.

[29] 2020. Introduction to Callidus. https://3xpl01tc0d3r.blogspot.com/2020/03/introduction-to-callidus.html.

[30] 2020. Raccoon Stealer's Abuse of Google Cloud Services and Multiple Delivery Techniques - TrendLabs Security Intelligence Blog. https://blog.trendmicro.com/trendlabs-security-intelligence/raccoon-stealers-abuse-of-google-cloud-services-and-multiple-delivery-techniques/.

[31] 2020. Targeted attacks using Fake Flash against Tibetans | Volexity. https://www.volexity.com/blog/2020/03/31/storm-cloud-unleashed-tibetan-community-focus-of-highly-targeted-fake-flash-campaign/.

[32] 2020. The Tetrade: Brazilian banking malware goes global | Securelist. https://securelist.com/the-tetrade-brazilian-banking-malware/97779/.

[33] 2021. IndigoZebra APT continues to attack Central Asia with evolving tools - Check Point Research. https://research.checkpoint.com/2021/indigozebra-apt-continues-to-attack-central-asia-with-evolving-tools/.

[34] 2021. North Korean APT InkySquid Infects Victims Using Browser Exploits | Volexity. https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/.

[35] 2021. Numando: Count once, code twice | WeLiveSecurity. https://www.welivesecurity.com/2021/09/17/numando-latam-banking-trojan/.

[36] 2021. Ousaban: Private photo collection hidden in a CABinet | WeLiveSecurity. https://www.welivesecurity.com/2021/05/05/ousaban-private-photo-collection-hidden-cabinet/.

[37] Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose, and Andreas Terzis. 2006. A multifaceted approach to understanding the botnet phenomenon. In *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*. 41–52.

[38] Mansour Ahmadi, Battista Biggio, Steven Arzt, Davide Ariu, and Giorgio Giacinto. 2016. Detecting misuse of google cloud messaging in android badware. In *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices*. 103–112.

[39] FEDOR SINITSYN ANTON IVANOV. 2016. The first cryptor to exploit Telegram | Securelist. https://securelist.com/the-first-cryptor-to-exploit-telegram/76558/.

[40] Liviu ARSENE. 2020. Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia. https://www.bitdefender.com/blog/labs/iranian-chafer-apt-targeted-air-transportation-and-government-in-kuwait-and-saudi-arabia/.

[41] Steven Arzt. 2017. Static data flow analysis for android applications. (2017).

[42] Kevin Ross Ashutosh Singh, Annie H. Toderici and Mark Stamp. [n.d.]. ([n. d.]).

[43] Joe Hannon Ben Koehl. 2020. Microsoft Security—detecting empires in the cloud - Microsoft Security Blog. https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/.

[44] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. 2013. Design and analysis of a social botnet. *Computer Networks* 57, 2 (2013), 556–578.

[45] Jean-Ian Boutin. 2017. Turla's watering hole campaign: An updated Firefox extension abusing Instagram | WeLiveSecurity. https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/.

[46] Chris Brook. 2012. Windows 8 Malware Using Google Docs to Target Brazilians | Threatpost. https://threatpost.com/windows-8-malware-using-google-docs-target-brazilians-111912/77227/.

[47] Pieter Burghouwt, Marcel Spruit, and Henk Sips. 2011. Towards detection of botnet communication through social media by monitoring user activity. In *International Conference on Information Systems Security*. Springer, 131–143.

[48] Pieter Burghouwt, Marcel Spruit, and Henk Sips. 2013. Detection of covert botnet command and control channels by causal analysis of traffic flows. In *International Symposium on Cyberspace Safety and Security*. Springer, 117–131.

[49] Jaromir Horejsi Joseph C Chen William Gamazo Sanchez Cedric Pernet, Elliot Cao. 2019. New SLUB Backdoor Uses GitHub, Communicates via Slack. https://www.trendmicro.com/en_gb/research/19/c/new-slub-backdoor-uses-github-communicates-via-slack.html.

[50] Jaromir Horejsi Joseph C. Chen William Gamazo Sanchez Cedric Pernet, Elliot Cao. 2019. SLUB Gets Rid of GitHub, Intensifies Slack Use - TrendLabs Security Intelligence Blog. https://blog.trendmicro.com/trendlabs-security-intelligence/slub-gets-rid-of-github-intensifies-slack-use/.

[51] Alfie Champion. 2020. Attack Detection Fundamentals: C2 and Exfiltration - Lab #3. https://labs.f-secure.com/blog/attack-detection-fundamentals-c2-and-exfiltration-lab-3/.

[52] Raj Chandel. 2019. Command and Control with DropboxC2. https://www.hackingarticles.in/command-and-control-with-dropboxc2/.

[53] Joey Chen. 2018. Blackgear Cyberespionage Campaign Resurfaces. https://www.trendmicro.com/en_us/research/18/g/blackgear-cyberespionage-campaign-resurfaces-abuses-social-media-for-cc-communication.html.

[54] Wei Chen, Peihua Gong, Le Yu, and Geng Yang. 2013. An adaptive push-styled command and control mechanism in mobile botnets. *Wuhan University Journal of Natural Sciences* 18, 5 (2013), 427–434.

[55] Wei Chen, Xiapu Luo, Chengyu Yin, Bin Xiao, Man Ho Au, and Yajuan Tang. 2017. CloudBot: Advanced mobile botnets using ubiquitous cloud technologies. *Pervasive and Mobile Computing* 41 (2017), 270–285.

[56] Anton Cherepanov. 2016. The rise of TeleBots: Analyzing disruptive KillDisk attacks | WeLiveSecurity. https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/.

[57] Catalin Cimpanu. 2020. Astaroth malware hides command servers in YouTube channel descriptions | ZDNet. https://www.zdnet.com/article/astaroth-malware-hides-command-servers-in-youtube-channel-descriptions/.

[58] Alberto Compagno, Mauro Conti, Daniele Lain, Giulio Lovisotto, and Luigi Vincenzo Mancini. 2015. Boten ELISA: A novel approach for botnet C&C in online social networks. In *2015 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 74–82.

[59] Lucian Constantin. 2012. Malware uses Google Docs as proxy to command and control server. https://www.pcworld.com/article/455736/malware-uses-google-docs-as-proxy-to-command-and-control-server.html.

[60] Assaf Dahan. 2017. Operation Cobalt Kitty: A large-scale APT in Asia carried out by the OceanLotus Group. https://www.cybereason.com/blog/operation-cobalt-kitty-apt.

[61] Cedric Pernet Daniel Lunghi, Jaromir Horejsi. 2017. Untangling the Patchwork Cyberespionage Group. https://www.trendmicro.com/en_gb/research/17/l/untangling-the-patchwork-cyberespionage-group.html.

[62] Yulong Dong, Jun Dai, and Xiaoyan Sun. 2018. A mobile botnet that meets up at Twitter. In *International Conference on Security and Privacy in Communication Systems*. Springer, 3–21.

[63] Matthieu Faou. 2020. From Agent.BTZ to ComRAT v4: A ten-year journey | WeLiveSecurity. https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/.

[64] Matthieu Faou. 2020. Turla Crutch: Keeping the "back door" open | WeLiveSecurity. https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/.

[65] Lord Alfred Remorin Feike Hacquebord. 2020. Pawn Storm's Lack of Sophistication as a Strategy. https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html.

[66] Tomáš Foltýn. 2018. Turla: In and out of its unique Outlook backdoor | WeLiveSecurity. https://www.welivesecurity.com/2018/08/22/turla-unique-outlook-backdoor/.

[67] Mansoureh Ghanadi and Mahdi Abadi. 2014. Socialclymene: A negative reputation system for covert botnet detection in social networks. In *7'th International Symposium on Telecommunications (IST'2014)*. IEEE, 954–960.

[68] Nicholas Griffin. 2017. Carbanak Group uses Google for malware command-and-control | Forcepoint. https://www.forcepoint.com/blog/x-labs/carbanak-group-uses-google-malware-command-and-control.

[69] Julian B Grizzard, Vikram Sharma, Chris Nunnery, Brent ByungHoon Kang, and David Dagon. 2007. Peer-to-Peer Botnets: Overview and Case Study. *HotBots* 7, 2007 (2007).

[70] Josh Grunzweig. 2018. The TopHat Campaign: Attacks Within The Middle East Region Using Popular Third-Party Services. https://unit42.paloaltonetworks.com/unit42-the-tophat-campaign-attacks-within-the-middle-east-region-using-popular-third-party-services/.

[71] Yukun He, Guangyan Zhang, Jie Wu, and Qiang Li. 2016. Understanding a prospective approach to designing malicious social bots. *Security and Communication Networks* 9, 13 (2016), 2157–2172.

[72] Vladislav Hrčka. 2019. Stantinko botnet adds cryptomining to its pool of criminal activities | WeLiveSecurity. https://www.welivesecurity.com/2019/11/26/stantinko-botnet-adds-cryptomining-criminal-activities/.

[73] Noora Hyvärinen. 2015. The Dukes: 7 Years Of Russian Cyber-Espionage - F-Secure Blog. https://blog.f-secure.com/the-dukes-7-years-of-russian-cyber-espionage/.

[74] PIERRE DELCHER IVAN KWIATKOWSKI, FÉLIX AIME. 2020. Holy water: ongoing targeted water-holing attack in Asia | Securelist. https://securelist.com/holy-water-ongoing-targeted-water-holing-attack-in-asia/96311/.

[75] Karmina Jarkko. 2015. News from the Lab Archive : January 2004 to September 2015. https://archive.f-secure.com/weblog/archives/00002803.html.

[76] Yuede Ji, Yukun He, Xinyang Jiang, Jian Cao, and Qiang Li. 2016. Combating the evasion mechanisms of social bots. *computers & security* 58 (2016), 230–249.

[77] Yuede Ji, Yukun He, Xinyang Jiang, and Qiang Li. 2014. Towards social botnet behavior detecting in the end host. In *2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS)*. IEEE, 320–327.

[78] Jen Miller-Osborn Josh Grunzweig. 2017. SunOrcal Adds GitHub and Steganography to its Repertoire, Expands to Vietnam and Myanmar. https://unit42.paloaltonetworks.com/unit42-sunorcal-adds-github-steganography-repertoire-expands-vietnam-myanmar/.

[79] Erhan J Kartaltepe, Jose Andre Morales, Shouhuai Xu, and Ravi Sandhu. 2010. Social network-based botnet command-and-control: emerging threats and countermeasures. In *International conference on applied cryptography and network security*. Springer, 511–528.

[80] Sheharbano Khattak, Naurin Rasheed Ramay, Kamran Riaz Khan, Affan A. Syed, and Syed Ali Khayam. 2014. A Taxonomy of Botnet Behavior, Detection, and Defense. *IEEE Communications Surveys Tutorials* 16, 2 (2014), 898–924. https://doi.org/10.1109/SURV.2013.091213.00134

[81] Barbara Kitchenham and Stuart Charters. 2007. Guidelines for performing systematic literature reviews in software engineering. (2007).

[82] SM Kuitert. 2009. War on Botnets. (2009).

[83] TONY LAMBERT. 2021. Threat Hunting in Linux For Rocke Cryptocurrency Mining Malware. https://redcanary.com/blog/rocke-cryptominer/.

[84] Majd Latah. 2020. Detection of malicious social bots: A survey and a refined taxonomy. *Expert Systems with Applications* 151 (2020), 113383.

[85] Hayoung Lee, Taeho Kang, Sangho Lee, Jong Kim, and Yoonho Kim. 2013. Punobot: Mobile botnet using push notification service in android. In *International workshop on information security applications*. Springer, 124–137.

[86] Romain Dumont Matthieu Faou. 2019. A dive into Turla PowerShell usage | WeLiveSecurity. https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/.

[87] Maersk Menrige. 2014. PlugX RAT With "Time Bomb" Abuses Dropbox for Command-and-Control Settings - TrendLabs Security Intelligence Blog. https://blog.trendmicro.com/trendlabs-security-intelligence/plugx-rat-with-time-bomb-abuses-dropbox-for-command-and-control-settings/.

[88] Shishir Nagaraja, Amir Houmansadr, Pratch Piyawongwisal, Vijit Singh, Pragya Agarwal, and Nikita Borisov. 2011. Stegobot: a covert social network botnet. In *International Workshop on Information Hiding*. Springer, 299–313.

[89] Jose Nazario. 2015. Twitter based botnet command and control (2009).

[90] Edmund Brumaghin Nick Biasini and Nick Lister. 2020. Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Threat Spotlight: Astaroth — Maze of obfuscation and evasion reveals dark stealer. https://blog.talosintelligence.com/2020/05/astaroth-analysis.html.

[91] STEVE MILLER BARRY VENGERIK NICK CARR, KIMBERLY GOODY. 2018. On the Hunt for FIN7: Pursuing an Enigmatic and Evasive Global Criminal Operation | Mandiant. https://www.mandiant.com/resources/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.

[92] Vladimir Radunović and Mladen Veinović. 2020. Malware Command and Control Over Social Media : Towards the Server-less Infrastructure. 17, 3 (2020), 357–375.

[93] Bryan Lee Robert Falcone. 2019. DarkHydrus delivers new Trojan that can use Google Drive for C2 communications. https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/.

[94] Rafael A. Rodríguez-Gómez, Gabriel Maciá-Fernández, and Pedro García-Teodoro. 2013. Survey and Taxonomy of Botnet Research through Life-Cycle. 45, 4 (2013). https://doi.org/10.1145/2501654.2501659

[95] Kyle Wilhoit Ruchna Nigam. 2018. TeleRAT: Another Android Trojan Leveraging Telegram's Bot API to Target Iranian Users. https://unit42.paloaltonetworks.com/unit42-telerat-another-android-trojan-leveraging-telegrams-bot-api-to-target-iranian-users/.

[96] Silpa Sebastian, Sonal Ayyappan, and P Vinod. 2014. Framework for design of Graybot in social network. In *2014 international conference on advances in computing, communications and informatics (ICACCI)*. IEEE, 2331–2336.

[97] Wang Shuai, Cui Xiang, Liao Peng, and Li Dan. 2012. S-URL flux: A novel C&C protocol for mobile botnets. In *International Conference on Trustworthy Computing and Services*. Springer, 412–419.

[98] Sérgio SC Silva, Rodrigo MP Silva, Raquel CG Pinto, and Ronaldo M Salles. 2013. Botnets: A survey. *Computer Networks* 57, 2 (2013), 378–403.

[99] Ryan Singel. 2009. Hackers Use Twitter to Control Botnet | WIRED. https://www.wired.com/2009/08/botnet-tweets/.

[100] Ashutosh Singh. 2012. Social networking for botnet command and control. (2012).

[101] Kapil Singh, Abhinav Srivastava, Jonathon Giffin, and Wenke Lee. 2008. Evaluating email's feasibility for botnet command and control. In *2008 IEEE International Conference on Dependable Systems and Networks With FTCS and DCC (DSN)*. 376–385. https://doi.org/10.1109/DSN.2008.4630106

[102] Mathieu Tartare Thibaut Passilly. 2021. The SideWalk may be as dangerous as the CROSSWALK | WeLiveSecurity. https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/.

[103] Kurt Thomas and David M Nicol. 2010. The Koobface botnet and the rise of social malware. In *2010 5th International Conference on Malicious and Unwanted Software*. IEEE, 63–70.

[104] Micah Yates Tom Lancaster. 2016. Confucius Says...Malware Families Get Further By Abusing Legitimate Websites. https://unit42.paloaltonetworks.com/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/.

[105] Nguyen H Vo and Josef Pieprzyk. 2010. Protecting web 2.0 services from botnet exploitations. In *2010 Second Cybercrime and Trustworthy Computing Workshop*. IEEE, 18–28.

[106] Jungsoo An Warren Mercer, Paul Rascagneres. 2017. Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: ROKRAT Reloaded. https://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html.

[107] Vitor Ventura Eric Kuhla. Warren Mercer, Paul Rascagneres. 2020. Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: JhoneRAT: Cloud based python RAT targeting Middle Eastern countries. https://blog.talosintelligence.com/2020/01/jhonerat.html.

[108] Jake Williams. 2013. DropSmack: How cloud synchronization services render your corporate firewall worthless. https://docs.huihoo.com/blackhat/europe-2013/bh-eu-13-dropsmack-jwilliams-wp.pdf.

[109] Di Wu, Binxing Fang, Jie Yin, Fangjiao Zhang, and Xiang Cui. 2018. Slbot: A serverless botnet based on service flux. In *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)*. IEEE, 181–188.

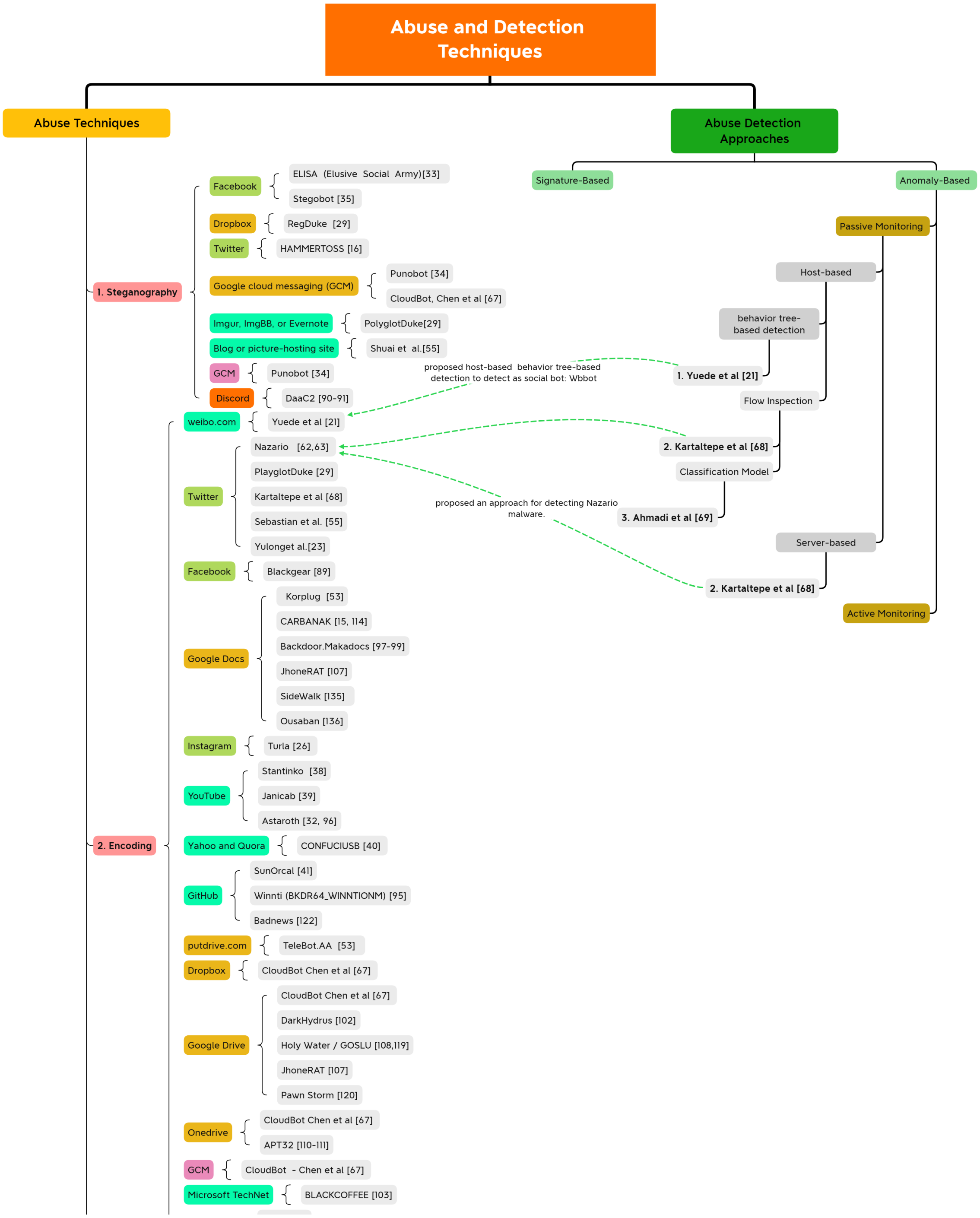
[110] Cui Xiang, Fang Binxing, Shi Jinqiao, and Liu Chaoge. 2013. Botnet triple-channel model: towards resilient and efficient bidirectional communication botnets. In *International Conference on Security and Privacy in Communication Systems*. Springer, 53–68.

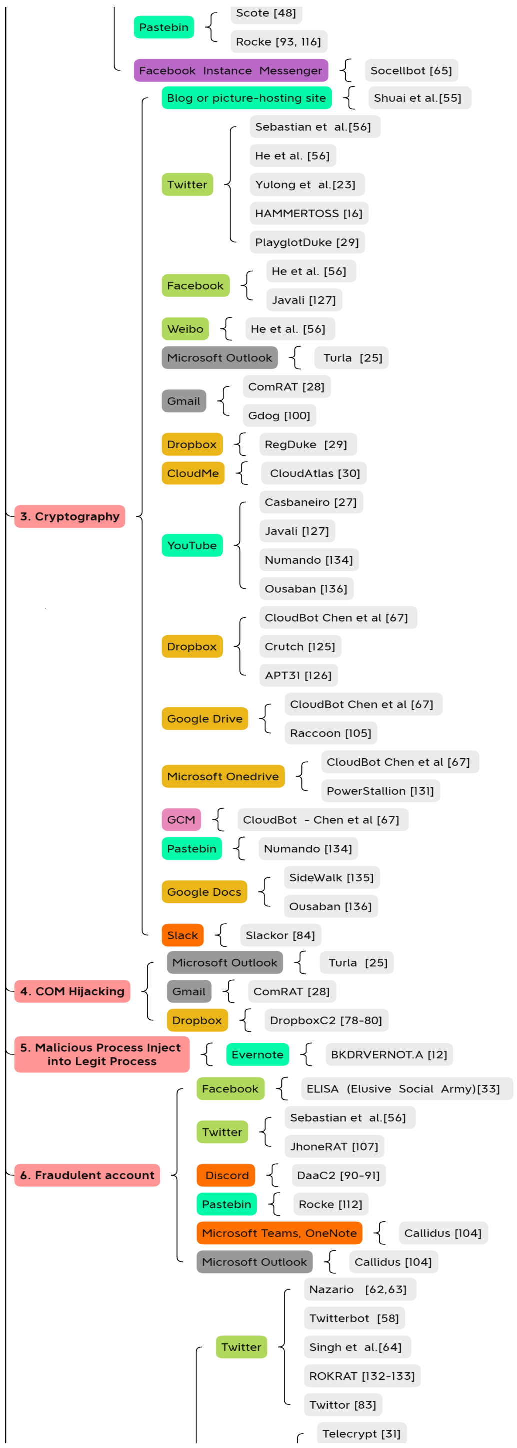
[111] Jie Yin, Heyang Lv, Fangjiao Zhang, Zhihong Tian, and Xiang Cui. 2018. Study on advanced botnet based on publicly available resources. In *International Conference on Information and Communications Security*. Springer, 57–74.

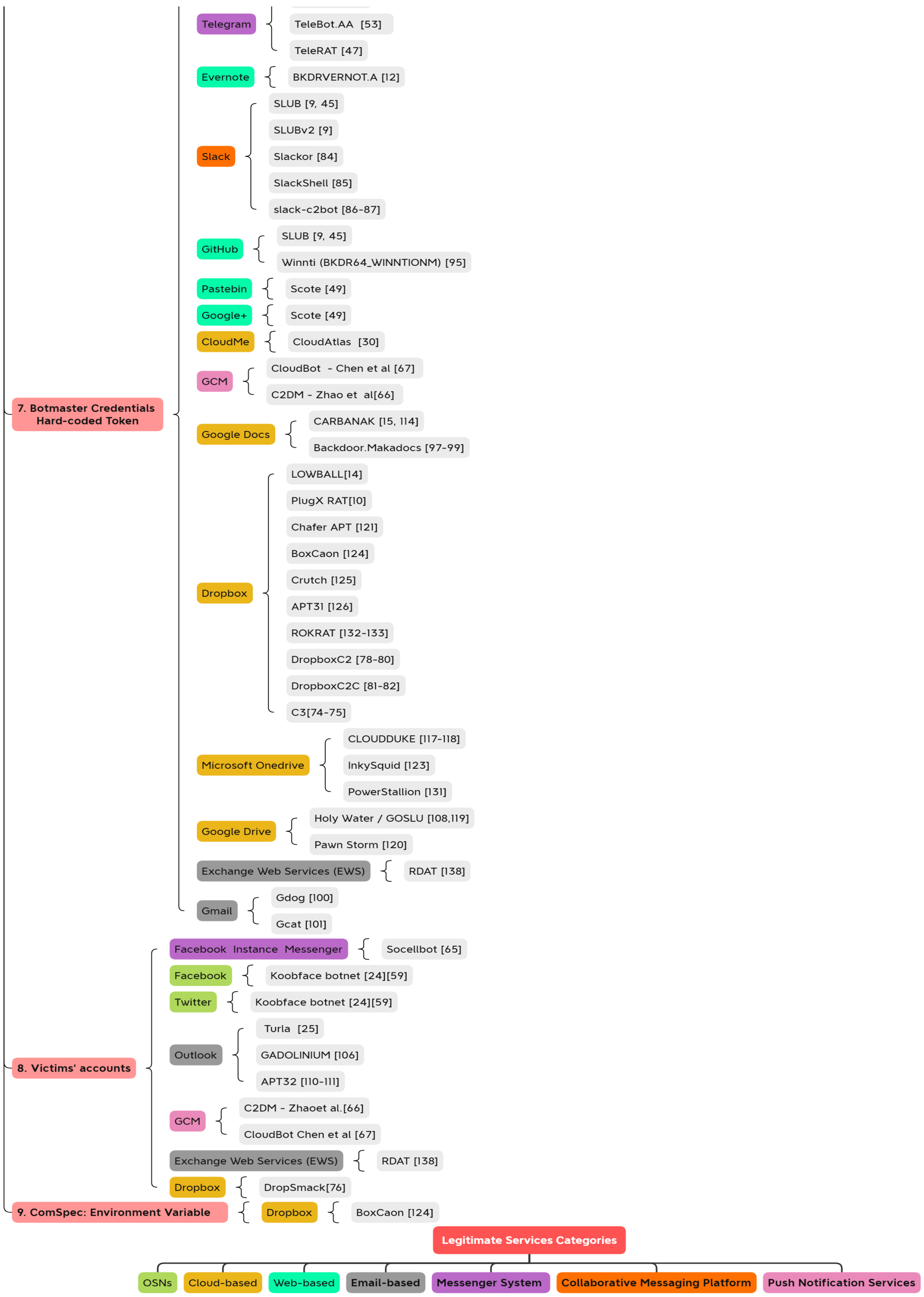
[112] Dewei Zhu Qiang Li Dong Guo Yuede Ji, Yukun He. 2014. A mulitiprocess mechanism of evading behavior-based bot detection approaches. In *International conference on information security practice and experience*. Springer, 75–89.

[113] Shuang Zhao, Patrick PC Lee, John CS Lui, Xiaohong Guan, Xiaobo Ma, and Jing Tao. 2012. Cloud-based push-styled mobile botnets: a case study of exploiting the cloud to device messaging service. In *Proceedings of the 28th Annual Computer Security Applications Conference*. 119–128.

A ABUSIVE TECHNIQUES LINK TO LEGITIMATE PLATFORMS




Pastebin
Scote [48]
Rocke [93, 116]
Facebook Instance Messenger
Socellbot [65]
Blog or picture-hosting site
Shuai et al.[55]
Twitter
Sebastian et al.[56]
He et al. [56]
Yulong et al.[23]
HAMMERTOSS [16]
PlayglotDuke [29]
Facebook
He et al. [56]
Javali [127]
Weibo
He et al. [56]
Microsoft Outlook
Turla [25]
Gmail
ComRAT [28]
Gdog [100]
Dropbox
RegDuke [29]
CloudMe
CloudAtlas [30]
3. Cryptography
YouTube
Casbaneiro [27]
Javali [127]
Numando [134]
Ousaban [136]
Dropbox
CloudBot Chen et al [67]
Crutch [125]
APT31 [126]
Google Drive
CloudBot Chen et al [67]
Raccoon [105]
Microsoft Onedrive
CloudBot Chen et al [67]
PowerStallion [131]
GCM
CloudBot - Chen et al [67]
Pastebin
Numando [134]
Google Docs
SideWalk [135]
Ousaban [136]
Slack
Slackor [84]
4. COM Hijacking
Microsoft Outlook
Turla [25]
Gmail
ComRAT [28]
Dropbox
DropboxC2 [78-80]
5. Malicious Process Inject into Legit Process
Evernote
BKDRVERNOT.A [12]
6. Fraudulent account
Facebook
ELISA (Elusive Social Army)[33]
Twitter
Sebastian et al.[56]
JhoneRAT [107]
Discord
DaaC2 [90-91]
Pastebin
Rocke [112]
Microsoft Teams, OneNote
Callidus [104]
Microsoft Outlook
Callidus [104]
Twitter
Nazario [62,63]
Twitterbot [58]
Singh et al.[64]
ROKRAT [132-133]
Twittor [83]
Telecrypt [31]


Telegram
TeleBot.AA [53]
TeleRAT [47]
Evernote
BKDRVERNOT.A [12]
Slack
SLUB [9, 45]
SLUBv2 [9]
Slackor [84]
SlackShell [85]
slack-c2bot [86-87]
GitHub
SLUB [9, 45]
Winnti (BKDR64_WINNTIONM) [95]
Pastebin
Scote [49]
Google+
Scote [49]
CloudMe
CloudAtlas [30]
GCM
CloudBot - Chen et al [67]
C2DM - Zhao et al[66]
7. Botmaster Credentials Hard-coded Token
Google Docs
CARBANAK [15, 114]
Backdoor.Makadocs [97-99]
Dropbox
LOWBALL[14]
PlugX RAT[10]
Chafer APT [121]
BoxCaon [124]
Crutch [125]
APT31 [126]
ROKRAT [132-133]
DropboxC2 [78-80]
DropboxC2C [81-82]
C3[74-75]
Microsoft Onedrive
CLOUDDUKE [117-118]
InkySquid [123]
PowerStallion [131]
Google Drive
Holy Water / GOSLU [108,119]
Pawn Storm [120]
Exchange Web Services (EWS)
RDAT [138]
Gmail
Gdog [100]
Gcat [101]
Facebook Instance Messenger
Socellbot [65]
Facebook
Koobface botnet [24][59]
Twitter
Koobface botnet [24][59]
8. Victims' accounts
Outlook
Turla [25]
GADOLINIUM [106]
APT32 [110-111]
GCM
C2DM - Zhaoet al.[66]
CloudBot Chen et al [67]
Exchange Web Services (EWS)
RDAT [138]
Dropbox
DropSmack[76]
9. ComSpec: Environment Variable
Dropbox
BoxCaon [124]
Legitimate Services Categories
OSNs
Cloud-based
Web-based
Email-based
Messenger System
Collaborative Messaging Platform
Push Notification Services