A Comprehensive Pattern-based Overview of Stegomalware

Fabian Strachanski
fabian.strachanski@uni-due.de
University of Duisburg-Essen
Duisburg, Germany
FernUniversität in Hagen
Hagen, Germany

Denis Petrov
petrov@hs-worms.de
Hochschule Worms
Worms, Germany

Tobias Schmidbauer
tobias.schmidbauer@th-nuernberg.de
Nuremberg Institute of Technology
Nürnberg, Germany

Steffen Wendzel
wendzel@hs-worms.de
Hochschule Worms
Worms, Germany
FernUniversität in Hagen
Hagen, Germany

ABSTRACT

In recent years, malware increasingly applies steganography methods to remain undetected as long as possible. Such malware is called *stegomalware*. Stegomalware not only covers its tracks on the infected system, but also hides its communication with adversary infrastructure. This paper reviews 106 stegomalware cases on the basis of 133 reports, including digital media (audio, video, images), text, and network steganography. For this purpose, the steganography methods used by the malware are categorized and introduced using a *pattern*-based approach. Our survey reveals that solely a small set of patterns are employed by known malware samples. We also analyzed the commonalities of media-, text-, and network-based stegomalware. We show that only a small variation of network protocols, media types and hiding methods are utilized by stegomalware. For this reason, research may focus on these to counter malicious activities covered by steganography.

CCS CONCEPTS

• **Security and privacy** → **Malware and its mitigation**; *Pseudonymity, anonymity and untraceability*; *Intrusion detection systems*; • **Applied computing** → *Network forensics*; *System forensics*.

KEYWORDS

information hiding, steganography, steganalysis, detection techniques, malware, threat intelligence

ACM Reference Format:
Fabian Strachanski, Denis Petrov, Tobias Schmidbauer, and Steffen Wendzel. 2024. A Comprehensive Pattern-based Overview of Stegomalware. In *The 19th International Conference on Availability, Reliability and Security (ARES 2024), July 30–August 02, 2024, Vienna, Austria.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3664476.3670886

ARES 2024, July 30–August 02, 2024, Vienna, Austria
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1718-5/24/07
https://doi.org/10.1145/3664476.3670886

1 INTRODUCTION

Attacks with malware on companies, governments, NGOs, and their networks have become a daily threat in the last decade [5]. Beside the threat of automated and focused attacks [4], so-called *stegomalware* that utilizes information hiding methods has become a threat [16, 18]. Stegomalware applies information hiding techniques to prevent its detection for as long as possible [4]. Therefore, stegomalware has to be investigated, especially to understand the details of how hiding techniques are utilized.

Lately, the domain of information hiding has been subject to categorization attempts, which lead to the introduction of a novel generic information hiding taxonomy based on so-called *hiding patterns* [148, 149]. Such a taxonomy allows the comparability of different steganographic subdomains, like text, media, CPS, file system, and network steganography. We employ this taxonomy as it allows the categorization of techniques used by stegomalware. In this paper, we introduce a comprehensive overview of steganographic techniques applied by stegomalware in the wild using a pattern-based approach. Our key contributions are as follows:

(1) A systematic analysis of reports for stegomalware that appeared until June 2024;
(2) an overview of the stegomalware methods used in the last five years;
(3) a categorization of the malicious software by steganographic methods using hiding patterns.

The remainder of the paper is structured as follows. In Sect. 2 we will cover fundamentals. Sect. 3 introduces our methodology and the results of our work are evaluated in Sect. 4. Finally, we discuss and summarize our findings in Sect. 5.

2 FUNDAMENTALS

In this section, we first cover the fundamentals of information hiding, followed by a discussion of related work.

2.1 Information Hiding

Information hiding had been categorized in [108] into four major categories, whereas only steganography in means of utilizing (digital) texts or (digital) media as cover object, and covert channels in means of utilizing network protocols as cover objects, are relevant for the remainder of this paper. While for steganography, the covert information (CI) is embedded in the cover objects, covert channels utilize overt communication protocols that are not intended for communication at all [85]. Information hiding techniques have been further analyzed and categorized, which enabled the introduction of so-called *hiding patterns* linked to a taxonomy for network steganography [151]. The network steganography taxonomy had been further generalized to be transferred into a *generic* taxonomy for steganography in [148, 149].

Brief Pattern Overview. The patterns described by the generic taxonomy are divided into two overarching branches: *embedding* and *representation* hiding patterns. Embedding patterns describe how the covert message is embedded into a cover object. For example a secret value could be embedded into a network packet header in such a way that the packet remains valid, but carries the embedded data. The taxonomy defines two such patterns: *E1. State/Value Modulation* and *E2. Element Occurrence*. The first letter of the pattern designates its type, i.e., *E* for embedding or *R* for representation patterns, and is followed by the numerical representation of the pattern and a name. For embedding, the following patterns exist: *E1. State/Value Modulation* covers changes in the state or the value of an element, in order to embed secret data. It is further split into five sub-patterns, which include *E1.1. Reserved/Unused State/Value Modulation* – modulation of reserved or unused fields of the element; *E1.2. Random State/Value Modulation* – exchanging a field's value or an element's state containing random data with the secret message; *E1.3. Least Significant Bit (LSB) State/Value Modulation* – modulation of the least significant bit of a value; *E1.4. Character State/Value Modulation* – changes the features of individual characters; and *E1.5. Redundancy State/Value Modulation* – alters redundancy, e.g., by means of compression. In case of the second major pattern (*E2. Element Occurrence*) the message is hidden through the spatial or temporal location of the element. The pattern comprises two sub-patterns: While *E2.1. Element Enumeration* addresses cases where the quantity or size of sub-elements is changed to carry the covert message, *E2.2. Element Positioning* deals with the position of the element in space and time. Representation patterns are derived from the embedding ones, matching the pattern name and being composed of the same sub-patterns.

Domain-overlapping Hiding Patterns. Note that hiding methods that are represented by some pattern can fall into different steganography domains. For instance, modulating text characters in network traffic can be considered both text steganography and network steganography, cf. Fig. 1 in [149]. Throughout this paper, we assigned patterns based on the major focus of a hiding technique.

2.2 Related Work

Stegomalware-facilitating developments and early stegomalware cases were analyzed in 2014 in [150]. In the same year, Mazurczyk and Caviglione conducted a survey on the use of steganography in smartphones and covered several cases of malware utilizing steganographic methods [95]. Further analysis of stegomalware were performed in 2015 in [96], wherein such malware had been categorized into three groups (stegomalware modulating the status of shared hardware/software resources; methods that inject secret data into network traffic; and methods that embed secret data in digital files). A paper by Cabaj et al. [14] analyzed stegomalware that appeared between 2011 and 2017. Therein, the authors concluded a lack of available countermeasures. In recent work, Caviglione et al. [17, 18] describe that steganography techniques are used frequently by malware to achieve stealthiness. They provide an overview of the employed hiding techniques and show examples for such techniques in the text, media, and network domains. Caviglione maintains a public list of recent examples of malware that use steganography methods [16]. An additional malware catalog called *Malpedia* is provided by the Fraunhofer FKIE [51], but is not limited to stegomalware.

3 METHODOLOGY

This paper aims to provide an overview of the network hiding techniques utilized by malware and therefore evaluates reports that appeared within the last 5 years. Due to the approach described below, the main part of the evaluated material were blog articles, threat reports, articles, and analyses from IT security companies and security researchers. We consulted the databases *Google Scholar*, *IEEE Xplore*, *Springer Link*, *ACM Digital Library*, *TechRxiv*, *arXiv* and *ResearchGate* to find related scientific papers. These were searched for "Malware AND *name of the malware*". The initial starting point of our research are two existing works. First, the list *steg-in-the-wild* [16] maintained by Caviglione, created in April 2020 and last updated on September 28, 2023. All reports from this list, published in the last five years and describing stegomalware, were taken into account and resulted in 39 reports. Second, the directory *Malpedia* [51] from Fraunhofer FKIE. In this index, all malware entries in the *family*-tab of the *inventory* were systematically processed. The references belonging to malware published later than 2018 were scanned for the keywords "stegano", "stego", "tunnel" and "covert". For this purpose, a python script was created that crawled the references and searched for the keywords in the returned HTML content and PDFs. The resulting 654 entries were then checked manually to determine whether the keyword was contained in the content area and mentioned in the context of a covert channel. False positives were sorted out by human-eye review, and the remaining 294 hits were examined more closely. The python script, the output and the manually corrected list are published at GitHub [124].

In the total of 333 reports, duplicates, articles with no added value, and those not related to steganographic methods used in hidden data transfer were removed. When a reviewed article has mentioned another article that described a malware that was not on the list already, that article was included. After all, there was a final count of 133 reports included in this research that described a total of 106 different malware programs. Additional steganographic methods of the malware, which only had an impact on local systems, were not taken into account. Since the spread of malware nowadays largely takes place via the internet, it is difficult to delimit network traffic. Legitimate traffic generated by the user on purpose, such as the download of malware code, is not covered in this work. This paper only analyzes malware that produces network traffic on the infected system by itself (e.g., with the help of a stage 1 downloader).

To investigate similarity of methods, the malware was categorized into the areas media, network and text steganography, whereby a piece of malware can also be present in several areas simultaneously. We enriched the provided overviews with information about the information hiding embedding patterns utilized by the malware.

Trusted Platforms. In our work, the term *trusted platform* refers to popular online platforms that can be considered somehow trustworthy by end-users, such as social media platforms. The use of trusted platforms is widespread, so we decided to cover the utilization by stegomalware. This has the advantage that network traffic to these platforms does not stand out in legitimate network traffic, unlike Command & Control servers controlled by attackers. On the other hand, access to many platforms cannot be blocked easily.

4 EVALUATION

Out of 106 stegomalware cases, the share of network steganography predominates with 61, followed by media steganography with 36 and text steganography with 20 occurrences. We first cover media-based, second network-based, and finally text-based stegomalware.

4.1 Media-based Stegomalware

The overview of all investigated media-based stegomalware is presented in Tab. 1. The focus of such malware is almost exclusively on images. In the examined reports, only two malwares, *rhadamanthys* and *MoneroMiner*, hid data in audio (WAV) files. The used image formats are *PNG* (17 times), *JPG* (13 times), *BMP* (6 times) and *GIF* (2 times). *None* of the evaluated malware used video formats as cover. We found the following information hiding methods:

Legitimate file header. For communication with the C&C server, an image header is written in front of the payload data, so that scanners that only check the file type using magic bytes or other header elements are fooled. There is a high probability that such an "image" will be reported as defective when opened because the information in the header does not match the content [3, 72]. However, such test may also be applied automatically by sandboxes.

Append to a file. The length of some media formats is specified in the header and/or explicit end markers, such as the *IEND* chunk in PNG images [153]. This gives the opportunity of adding further content to the end of an image, as this is ignored by the processing software during image processing. This technique is utilized by *MyKings Botnet* and *Rhadamanthys* to deliver malware [63, 125].

Exploitation of File Specification Characteristics. Image file formats offer various options for hiding information in metadata without influencing the appearance of the image. Reports about *SteamHide* described the use of EXIF fields in JPG files [62]. In PNG files, IDAT-chunks provide space for malicious payload [72, 133].

File Payload. There are several methods to embed steganographic data in image files. The malware *Lumma* uses optical added "microdots" to encode covert information [52, 74]. *DoubleFinger* overwrites entire bytes of an image file with bytes from the malware. Such embedded information can be accessed by offsets while I/O operations are performed by the stegomalware. This procedure leads to visible changes that a trained eye can recognize [58]. Often, the *least significant bits* (LSB) are manipulated, which hardly affect the appearance to human eye [3, 98, 143]. In various attacks, the tool *Invoke-PSImage* [1] was utilized, providing LSB steganography to hide PowerShell scripts in image files [79, 114]. Occasionally, audio files were also used for LSB steganography [122, 130].

Hiding Patterns. Stegomalware utilizing media steganography focuses on few patterns as presented in Tab. 1. Foremost, the pattern E1.3d1 seems to be in focus as LSB steganography seems to be widely spread within malware. Second most common, the modulation of state/value in general (E1d1) had been utilized, followed by the state/value modulation of unused or reserved fields (E1.1d1), that is exploited within file formats. Furthermore, some reports claimed steganography but did not describe the information hiding technique in detail, so the exact pattern could not be derived.

Detection. For the less-sophisticated media stegomalware it is possible to use an approach that checks the files for fixed value traces of the embedded secret data. For more advanced samples, machine learning-based methods can provide better results, although sufficient data has to be acquired first.

4.2 Network-based Stegomalware

Tab. 2 presents stegomalware relying on network information hiding methods. First, it can be noticed that 78.69% of stegomalware relies on the protocols DNS (29 entries), HTTP (14 entries) or on both (5 entries). The remaining stegomalware implementations utilize the following protocols (descending order): TCP, packet filter (PF), SMTP, SSH, ICMP, UDP, IMAP, TOR and SOCKS. In the case of *Sunburst*, the application-specific *Orion Improvement Program* protocol was imitated by malware [38, 136]. The investigated reports often solely name the applications, like mail or telegram, from which we derived the utilized protocols. PF is a technique on the host to hide network traffic, not a transmission type, cf. Sect. 4.5.

By using widespread protocols like DNS and HTTP, malware tries to blend into normal network traffic. Compared to the aggregated data of the *MAWI samplepoint-F* [60] for the year 2020 in [117, p. 5], it stands out that these protocols coincide with the most widely used protocols of the WIDE backbone. Although the share of DNS is very low in terms of volume (e.g. for IPv4) at 0.2%, the packet sizes per request are much smaller than for HTTP. HTTP and HTTPS together make up approximately 3/4 (IPv4) or 3/5 (IPv6) of the total volume of data recorded in 2020. In addition to hiding communication or imitating the network traffic of known programs [14, 50], both transport and content encryption is utilized [36, 48, 107], respectively. Due to the nowadays high proportion of legitimate encrypted communication [49] (i.e., HTTPS), encrypted data traffic from malware is no longer an anomaly and is therefore hard to notice in legitimate traffic.

Protocols. **HTTP(S)** is used to download second stage malware, to communicate with the Command & Control infrastructure, and to exfiltrate data and to tunnel other protocols such as RDP [138]. URL components (path, GET parameters), the header fields (e.g., cookie) [21] and the content are used to hide data. *FatDuke* uses different GET parameters that match script names on the C&C server, so `/homepage/forum.php?newsid=<RANDOM>&article=<VOL-ID+MAC>&user=e40a4bc603a74403979716c932f0523a&revision=3&fromcache=0` imitates a forum, and the parameters *article* and

Table 1: Media steganography malware

Malware	Object	tp[a]	technique	pattern	Sources
ABK	Image (JPG)		Embeds malicious payload into image files in cleartext	E1d1	[26]
apicolor	Image (PNG)	x	LSB	E1.3d1	[61]
Avenger	Image		LSB	E1.3d1	[26]
build_downer	Image (JPG)		Uses every fourth byte of the image data	E1d1	[26]
CookieTime	Image (GIF)		Prepends gif header	E1d1	[106]
DoubleFinger	Image (PNG)	x	Uses bytes at known offsets (visible)	E1d1	[58]
FatDuke	Image (PNG)		Prepends (corrupted) png header	E1d1	[48]
Hammertoss	Image (JPG)	x	Append to end of image file	E1.1d1	[71]
IcedID	Image (PNG)		Uses IDAT-Chunk to store encrypted data	E1d1/E1.1d1	[133][127]
LambLoad	Image (PNG)		Uses wrong size in IDAT-Chunk to store data behind	E1.1d1	[72]
lightneuron	Image (JPG)		Uses start of *scan section* and *quantization table*	E1d1	[45]
Lokibot	Image (JPG, PNG)		LSB	E1.3d1	[132]
Lumma	Image (PNG)		Unknown	Unknown	[52][74]
LunarWeb	Image (JPG, GIF)		embeds data inside a JPG comment or in a GIF data block	Unknown	[75]
LunarMail	Image (PNG)		AES encrypted data in IDAT chunks	E1d1	[75]
MiniDuke	Image (JPG)		Prepends JPG header	E1d1	[48]
MoneroMiner	Audio (WAV)		LSB	E1.3d1	[122]
MonPass	Image (BMP)		Starting with the 3rd byte in image data each 4th byte is used to store xor encrypted payload	E1d1	[15]
Montythree	Image (BMP)	x	LSB + XOR Operations on extracted Covert Information	E1.3d1/E1d1	[86]
ObliqueRAT	Image (BMP)		Unknown	Unknown	[93]
PolyglotDuke	Image (JPG, PNG)	x	Append to end of image file	E1.1d1	[48]
PNGLoader	Image (PNG)		LSB	E1.3d1	[143]
PowLoad	Image (PNG)		LSB (Invoke-PSImage)	E1.3d1	[114]
RDAT	Image (BMP)		LSB	E1.3d1	[43]
RegDuke	Image (PNG)	x	LSB	E1.3d1	[48]
rhadamanthys	Image (JPG) Audio (WAV)		The data is stored after the actual content of the JPG or WAV file, in encrypted form	E1.1d1	[63]
Remcos	Image (PNG)	x	LSB	E1.3d1	[126]
ScarCruft	Image (JPG, PNG)		Image file with appended encrypted malicious payload t	E1.1d1	[57]
Serpent	Image (JPG)		Base64 encoded payload append to end of image file	E1.1d1	[145]
SlothfulMedia	Image (PNG)		LSB (Invoke-PSImage)	E1.3d1	[79]
stegmap	Image (BMP)	x	Unknown	Unknown	[104][137]
urlzone	Image (PNG)	x	LSB	E1.3d1	[131]
Ursnif	Image (PNG)		LSB (Invoke-PSImage)	E1.3d1	[31]
USBFerry	Image (JPG)		Unknown	Unknown	[23][24]
VinSelf	Image (BMP)		LSB	E1.3d1	[3]
Webbfuscator	Image (JPG)		Embedded certificate with payload	E1d1	[142]

[a] tp: trusted platform (this refers to popular online platforms generally considered trustworthy by their companies, i.e., access is usually not prohibited)

user are used to transmit a unique identifier and configuration parameters to the C&C server [48].

DNS is often used to communicate with C&C servers, most frequently with resource record types A, AAAA, CNAME, and TXT. Relatively few data can be forwarded inconspicuously at once due to fixed DNS query structure [99], so data is usually transmitted in the host name and subdomain area. TXT queries are used to retrieve larger amounts of data from C&C servers. Examples for covert communication protocols over DNS can be found in [8, 35, 42, 87, 128], including obfuscation. For instance, without obfuscation, the A query for `passwd.qwerty123.attacker.com` could be sent to extract a password. This query is sent to the DNS server configured on the victim. As the DNS server has no content limitations when answering the TXT query, new commands can be sent in a response that can also be disguised as something common, like an SPF record (`v=spf1 mx a:reboot.1pm.attack.com -all`). In [35] a procedure is shown how *Anchor_DNS* maps commands to IP addresses. This is an example that queries other than TXT can also be used to retrieve data from the C&C server [44], [80, p. 66f.]. Also, DNS over HTTPS (DoH) has been standardized in RFC 8484 [65] and is nowadays already actively used by malware producers. It offers the advantage to the attacker that both the request and the response are transferred undetected through an encrypted HTTPS tunnel. In addition, legitimate DoH servers from Google or Cloudfront are often used, concealing the actual C&C server [69, 100]. C&C communication is not the only application for DNS tunnels. Some APTs are using them in the early phases of an attack to track “victim interactions with phishing email content”and DNS is used “to map out network layouts” and gather real-time data [144].

SSH is the de-facto standard access method for encrypted remote maintenance of Unix/Linux machines [90]. It is therefore quite possible that an additional SSH connection will not be noticed in a Linux/Unix environment. Furthermore, SSH is installed on many Linux operating systems and allows to establish (reverse) tunnels. This means that malware that has infected a server can use available SSH tools to hide its presence on computers and networks, as shown in stegomalware cases [107] and [110].

Since **ICMP** [111] is used in network diagnostics, it is often not blocked by firewalls. Malware such as *Pingback*, and also tunneling tools like *ping tunnel* (https://www.cs.uit.no/~daniels/PingTunnel/) and *vstt – very strange tunneling tool* (https://github.com/cdpxe/NetworkCovertChannels/) take advantage of this situation and send data in the data segment of ICMP echo packets [92].

Packet Payload. In the reports examined, image steganography was mostly used by the malware samples in the payload. A few

Table 2: Network steganography malware

malware	protocol	os[a]	tp[b]	technique	pattern	sources
AdvOR	TOR	x		Hides destination and tunnels payload through TOR network	Unknown	[139]
AnchorDNS	DNS			DNS A queries with XOR-encoded data in subdomain part	E1.1n1	[35]
Bondupdater	DNS			DNS A and TXT queries, IP addresses and a custom protocol is used to encode commands	E1.1n1	[42]
bvp47	PF[c]			Hides Payload in SYN-Packets with specific marker on the infected system via BPF rules	E1.1n1	[82]
Cashy200	DNS			DNS A queries with custom subdomain part, C2 commands hidden in IP addresses	E1.1n1	[8]
ChaChi	DNS HTTP			encrypted DNS TXT queries, HTTP POST Requests as fallback, base64 and XORed data.	E1.1n1	[134]
Chisel	HTTP	x		TCP/UDP connections encrypted via SSH transported over HTTP, exact method unclear	E1n1	[109]
ChunkyTuna	HTTP	x		TCP streams over HTTP, exact method unclear	E1n1	[27]
Cloud Snooper	PF[c]			AWS EC2 Firewall bypass via Netfilter Hook	E1.1n1	[119]
Cloudflare Tunnel	TCP		x	APT uses Cloudflare Tunnel Software to hide C2 infrastructure and payload	E1.1n1	[73]
Cobalt Strike	HTTP		x	Directs communication to legitimate CDN's and mimics javascript file download	E1n1	[147]
dnscat2	DNS	x		TXT-, MX-, CNAME-, A , and AAAA queries used with encrypted payload	E1.1n1	[11][77]
DnsDig	DNS			DNS TXT queries, base64 for exfiltration, plaintext in C2-TXT-Payload	E1.1n1	[120]
FatDuke	HTTP			mimics legit web applications in GET request URL; transmits data using unsuspicious query	E1.1n1	[48]
FlewAvenue	PF[c]			Custom TCP/IP-Stack with packet redirection	Unknown	[41]
FluBot	DNS HTTP		x	DoH to hide resolved domains and to tunnel encrypted and encoded TXT queries, HTTP Requests with XORed or RC4 encrypted payload	E1n1/E1.1n1	[118]
ForeLord	DNS			payload in TXT query subdomains; C2-reply contains obfuscated PS-Script in TXT-Record	E1.1n1	[128]
Gasket	HTTP DNS		x	TXT queries encrypted with XSalsa20/Poly1305 subdomain parts, C2 responses with serialized protobuf in TXT record. HTTP POST is used as fallback with XOR encrypted body	E1.1n1	[29]
gost	HTTP TCP UDP	x		This tool offers various information hiding possibilities	various	[56][155]
heyoka (modified)	DNS	x		modified open source tool that uses TXT queries	E1.1n1	[70][25]
IDShell	DNS			TXT queries with encrypted payload	E1.1n1	[23]
Invisimole	DNS			NULL- and AAAA queries with modified base32 encoding	E1.1n1	[68]
Karkoff	HTTP			Base64 and XOR encoded JSON-Payload in HTTP Body	E1n1	[97]
LCPDot	HTTP			"Cookie" HTTP Header for C2 Communication	E1.1n1	[141]
lightneuron	SMTP			Malicious Transport Agent scans and modifies E-Mails	E1.1n1	[45]
Ligolo-ng	TCP	x		advanced TLS encrypted TCP tunnel used by APTs	Unknown	[22][34]
LunarWeb	HTTP			impersonates legitimate-looking traffic, spoofing HTTP headers	E1.1n1	[75]
LunarMail	MAPI			sends emails via outlook	E1.1n1	[75]
Lyceum	DNS HTTP			DNS A queries with custom base32 encoding and commands placed between h6 and h7-tags in HTML-Pages retrieved via HTTP	E1.1n1/E1t1	[76]
Magnat	SSH			forwarding the RDP port through an SSH tunnel	E1n1	[107]
Meterpreter	DNS	x		Base32 encoded subdomains in AAAA and DNSKEY queries, response encoded in IP addresses or 16KB slices with AES and XOR encrytped data	E1.1n1	[113][10]
mori	DNS			no specific information found	Unknown	[101]
NightClub	SMTP IMAP DNS			data as attached file; latest version uses TXT queries for the C2 communication	E1.1n1	[47]
neo-reGeorg	HTTP	x		highly customizable HTTP tunnel, payload in header fields or other parts of the HTML file	E1.1n1	[81][40]
ngrok	HTTP TCP	x	x	TLS encrypted TCP and HTTP tunnel used by APTs	E1n1	[103][155]
Pingback	ICMP			Payload in data field of ICMP echo and echo reply packets	E1.1n1	[92]
PoisonFrog	DNS			exfiltrates Data in subdomains of A queries, response encoded in IP addresses	E1.1n1	[87]
Polonium	SSH	x		uses plink to spawn a SSH Tunnel	E1.1n1	[110]
PolyglotDuke	HTTP			Query parameters w/ random names from hardcoded list; data is transferred in the values	E1.1n1	[140]
RDAT	HTTP DNS			DNS A , AAAA , TXT queries with AES encryption and base32/64 encoding and HTTP POST requests against EWS-API to set filters and hide/send e-mails	E1.1n1/E1n1	[43]
Revsocks	TCP DNS	x		TLS encrypted TCP Socks Proxy with DNS Tunnel capabilities using TXT queries	E1.1n1	[34]
RogueRobin	DNS			DNS A , AAAA , TXT, CNAME, MX, SOA and SRV queries, rotating between them in a round-robin fashion	E1.1n1	[88]
RoyalDNS	DNS			DNS TXT queries for C2 communication	E1.1n1	[67]
saitama	DNS			DNS A queries and custom base36 encoding which is scrambled each request	E1.1n1	[123]
ScrableCross	HTTP TCP		x	ChaCha20 encrypted custom message structure send via HTTP or DNS	E1n1/E1.1n1	[64]
SecShow	DNS			utilizes DNS tunneling to scan network infrastructure and gather real-time data	E1.1n1	[144]
SideTwist	DNS		x	DNS queries in Word Macros to inform C&C of infection	E1.1n1	[28]
Sliver	DNS			Base58/32 encoded subdomain part in DNS queries	E1.1n1	[12]
Small Sieve	HTTP		x	Telegram-Bot API Commands over HTTPS	E1n1	[20]
SmileSvr	ICMP			XOR encrypted data in ICMP echo packets	E1.1n1	[32]
Snake	PF[c] TCP HTTP			implants filter in TCP stack to hide network traffic, builds overlay network with other implants, customized and encrypted TCP or HTTP Protocol with base62 encoded data	E1n1	[53]
Snugy	DNS			DNS A queries with only one byte capacity to exfiltrate data	E1.1n1	[44]
SombRAT	DNS TCP			compressed and AES encrypted DNS A and TXT queries, can switch communication to TCP if needed/requested	Unknown	[135]
Sunburst	OIP			mimicking normal activity as a part of Orion Improvement Program protocol	E1n1	[33][38]
Symbiote	PF[c] DNS			A queries for the credential exifltration and TXT queries for remote command execution, content is encrypted with RC4	E1.1n1	[77]
SysUpdate	DNS			TXT queries are used and the data is encrypted with a hardcoded AES key	E1.1n1	[91]
TrkCdn	DNS			E-Mail with content that triggers DNS queries to attack controlled domains	E1.1n1	[144]
TunnelSpecter	DNS			data encryption and exfiltration over DNS tunneling	E1.1n1	[115]
Webbfuscator	DNS			DNS TXT queries with base64 encoded data	E1.1n1	[142]
Wellmess	DNS			DNS A and TXT queries to send and receive base32 encoded data	E1.1n1	[112]
Winnti	DNS		x	DNS NULL- and TXT queries for C2 Server Communication	E1.1n1	[37]

[a]os: *open source*, [b]tp: trusted platform, [c]PF: packet filter

of them also hid information in audio files [63, 122] or textually. Steganography in the payload area is discussed in the sections on text and media steganography in more detail.

Open Source Tools. Not everything used by cybercriminals is developed by themselves. Many groups also use *open source* tools to establish covert channels to their victims. Our analysis revealed that at least 12 out of 61 (19.67%) malware used open source tools: *Chisel* [109], *ChunkyTuna* [59], *Go Simple Tunnel (gost)* [56], *Ligolo* [22], *neo-reGeorg* [81], *ngrok* [103], *Revsocks* [78], *heyoka* [70], *Advanced Onion Router (AdvOR)* [30] and *dnscat2* [11]. However, given that reports do not always cover this aspect, we can assume that the fraction of malware employing open source tools (or fractions of their code) is larger.

Hiding Patterns. For network steganography, exclusively state and value modulation patterns were utilized by stegomalware as shown in Tab. 2. Especially, the modulation of unused and reserved information (E1.1n1) is currently exploited by threat actors. Furthermore, it can be observed that also the modulation of existing legitimate information is used to cover information. The software *gost* [56] has to be mentioned separately, as it provides a toolkit of various information hiding techniques, appearing as some sort of swiss knife for network steganography. However, although one threat actor [155] may yet have utilized this tool, it can be assumed the software will be used by various stegomalware in the future. Similarly to the media steganography case, some reports have not described the information hiding methods in detail, so there are some unknown patterns that need further investigation.

Detection. Due to the vast difference of the used methods within network stegomalware, the detection approaches may vary significantly from one another. The most common approach is to look for anomalies within the traffic itself, like an abnormal percentage of the DNS traffic being TXT requests. Machine learning models are also capable to detect some of the available stegomalware.

4.3 Text-based Stegomalware

Investigated stegomalware relying on text steganography is presented in Tab. 3. In the case of textual content, the analyzed reports describe HTML pages that are used for hidden transport. Attributes in HTML elements are swapped or various whitespace and their frequency are used for coding. Instructions were also embedded in HTML comments and in hidden input fields [9, 36, 67, 121].

Some samples place their encrypted or encoded control instructions or C&C server URLs (i.e., visible area of HTML pages) [19, 146]. Trusted platforms are often used as a dead drop (cf. [116]), so data and control commands are hidden in text fields, like *Astaroth*, which uses YouTube and Facebook descriptions [8, 19]. *Beatdrop*, *GraphicalNeutrino* and *VaporRage* communicate via Notion [140]. *ComRatV4* and *TriFive* use email inboxes [44, 46]. *CosmicDuke*, *MiniDuke*, *PolyglotDuke* and *Hammertoss* use social media platforms such as X or Reddit [140]. Slack and GitHub are also used [129, 140].

Hiding Patterns. Like for media and network steganography, the dominant hiding pattern is the *state/value modulation.* E1t1 is utilized almost exclusively, modulating states/values of cover objects. In contrast to media and network steganography, no modulation of unused/reserved information has been exploited. *EasternRoppel* is the *only* case of stegomalware relying on the E2 Element Occurrence branch of all investigated stegomalware in this paper.

Detection. The human eye may easily detect obfuscated and encrypted postings in social media. Text hidden in URLs, APIs, and text hidden in HTML may be detected by intrusion detection systems by applying signatures and heuristics. There also has recently been published research on detection of text steganography utilizing large language models [6, 89].

4.4 Trusted Platforms

The reports mention the Content Delivery Networks (CDN) of *MSN*, *Lastpass*, *Adobe* and *Discord* [94, 147], whereby Discord enforced links to expire after 24 hours since 01.01.2024, to stop the spreading of malware through the platform [55]. Other cloud storage used by malware is *Alibaba Yuque*, *Tencent Platform*, *DropBox*, *GoogleDrive* and *pastebin* [83, 86]. Image hosters such as *imgur*, *postimage.cc* and *cloudinary* are used to distribute steganographically modified image files [39, 126], even the game library *Steam*, where each user can create their own profile (including profile picture), was used as an image hoster [62]. Profiles or posts on social media platforms such as *X (formerly Twitter)*, *Reddit*, *Facebook* and *YouTube* also contain commands or URLs [13, 140]. A total of 29.25% of the malware analyzed uses such platforms for communication. In the individual areas, this results in: 25% for media malware, 14.76% for network malware and 65% for text steganography malware.

4.5 Use of the Packet Filter

Rows marked with PF (for packet filter) in Tab. 2 are programs that either manipulate the TCP/IP stack or set specific PF rules. In this way, packets are redirected to the malware so early that no userland program on the system has the opportunity to detect them. In the case of *Snake* the FBI states [53]: "Snake's TCP traffic interception technique helps to conceal the existence of the Snake malware on its host computer and enables Snake implants on two computers to communicate without detection by ordinary intrusion detection and firewall security products, which typically look for network traffic directed to an unexpected port." The malware *Cloud Snooper* manipulates PF rules and thus enables communication in the AWS cloud bypassing configured AWS security groups.

5 DISCUSSION AND CONCLUSION

In this section, we summarize our work and present our key findings per steganography domain. Further, we present domain-overlapping commonalities and limitations of our work, and finally give an outlook to future work.

Summary. We provided a pattern-based overview of stegomalware from the last 5 years. We investigated different malware databases and collections and summarized 106 malware samples regarding their use of cover objects media, network protocols, and digital texts. For media steganography, we additionally described the utilized cover object and cover object format, for network protocols the used protocol and if open source tools had been utilized, and for text steganography the utilized platform. Furthermore, for all stegomalware examined, we investigated if trusted platforms

Table 3: Text steganography malware

malware	platform	tp[a]	technique	pattern	sources
Astaroth	Youtube	x	posts C2 Server addresses encrypted in Youtube and Facebook Profile descriptions	E1t1	[13][19]
Beatdrop	Trello Notion	x	stores victim-info as trello card / downloads payload as attachment	E1t1	[152]
ComRATV4	GMail	x	uses e-mail attachements to send encrypted commands and to receive output	E1t1	[46][84]
DNSpionage	-		hides data in the comments in the HTML code	E1t1	[97]
Drokbk	GitHub	x	Uses Readme.md to store URL in plaintext for C2	E1t1	[129]
EasternRoppels	-		hides key in HTML attribute positioning and payload in whitespaces	E2.2t1/E2.1t1	[36]
EnvyScout	Slack	x	creates slack-channel per victim and uses it for communication	E1t1	[140]
FatDuke	-		download id for payload is hidden in img-tag	E1t1	[48]
FunnyDream	-		uses HTTP, xoring/zipping payload in body, infos stored in URL Path	E1t1	[146]
GraphicalNeutrino	Notion	x	uses notions API + Database Feature to store victim information and to download payloads	E1t1	[54]
Hammertoss	Social Media	x	uses unsuspicious Link posted on twitter to embed c2 url + offset + key	E1t1	[140]
Ketrican	-		base64 encoded commands between keywords in HTML	E1t1	[9]
lemon_duck	-		renamed bash script (to .png)	E1t1	[2]
MiniDuke	X	x	encrypted C2-URL via Twitter Post	E1t1	[48]
njRAT	pastebin	x	Link between marks	E1t1	[154]
Panda	GitHub	x	Uses GitHub API domains for commands and data extraction	E1t1	[105]
PolyglotDuke	X Imgur Reddit	x	consumes Japanese, Chinese or Cherokee strings that encode the malware's C&C server	E1t1	[66]
TangleBot	Telegram	x	base64 encoded messages as telegram preview message	E1t1	[102]
TriFive	E-Mail Drafts		base64 encoded and encrypted message-bodies in E-Mail drafts	E1t1	[7][44]
VaporRage	Notion	x	notions API + Database Feature to store victim information and to download payloads	E1t1	[140]

[a]tp: trusted platform

had been utilized, and which generic information hiding patterns were fulfilled by the steganographic methods utilized.

Key Findings per Steganography Domain. **Media** steganography methods mainly manipulate images to hide information, with *PNG* and *JPG* formats accounting for 73% of the observed samples. Only the two samples (*rhadamanthys* and *MoneroMiner*) use audio (*WAV*) files, while no malware relied on video formats. In relation to this domain, the most utilized patterns are E1.1d1. Digital Media Reserved/Unused State/Value Modulation and E1.3d1. Digital Media LSB State/Value Modulation.

Network stegomalware mostly focuses on the everyday common protocols HTTP and DNS. This is not surprising, as they account for a large proportion of legitimate network traffic and usually are not heavily restricted when passing network periphery borders. The applied methods are limited to the patterns E1n1 and E1.1n1, which cover the state/value modulation of an element in the protocol.

For **text** steganography, stegomalware abuses textual HTTP payloads, APIs of services, URLs including their parameters, as well as HTML code in various ways. We observed almost an exclusive utilization of trusted platforms for malicious steganography activities. Hidden messages are often obfuscated or even encrypted to avoid detection by machines, but appear conspicuous when viewed by humans. However, machines may also be able to detect obviously obfuscated steganographic texts by searching for anomalies. Nearly all inspected samples have taken advantage of the pattern E1t1. Text State/Value Modulation.

Domain-overlapping Commonalities. Overall, stegomalware of all three domains utilize almost exclusively the pattern E1.1, and two of its sub-patterns, E1.1x1 and E1.3x1. While the LSB-dedicated subpattern E1.3x1 exists in each domain, only media-based stegomalware makes use of it. Our results indicate that threat actors do not utilize timing-based hiding patterns. Surprisingly, only *EasternRoppels* relies on a steganography embedding pattern not covered by modulating states/values or unused/reserved fields of cover objects, respectively (cf. Tab. 3).

Further, only widespread formats, protocols, or services are employed for the covert information exchange. In all three steganography domains, there is a proportion of malware that distributes its data via trustworthy websites; however, especially in case of text steganography. The analysis shows that a plethora of user data storage websites can be used as dead drops (cf. [116]). The utilization of such dead drops has two advantages for the attackers: There is no direct communication between the malware and infrastructure, and the platforms are often whitelisted and cannot be (easily) blocked.

Limitations. Reports that were found and classified as described in Sect. 3 were systematically analyzed. Our python script [124] reported several *false positives*, which required intensive manual reworking. This could be improved by introducing relevance criteria such as *frequency of the word found* and *position of the word*. In addition, relevant reports could have been automatically filtered out based on the selected search terms. Another limiting factor is the rudimentary description of *hiding* techniques in many reports. Most of them mention that information is embedded by steganography methods, but without (detailed) description of the applied methods referred to as "unknown" in the evaluation tables.

Future Work. In future work, we plan to employ a continuous monitoring pipeline for stegomalware to make them available on a GitHub platform. Furthermore, the utilization of information hiding within files and file systems has to be investigated. Also, there has not yet been a comprehensive analysis in which stages of compromise stegomalware avoids detection.

ACKNOWLEDGMENTS

S. Wendzel has been supported by the "Innovative University" program, a joint initiative of the Federal Government and the German States (project *EMPOWER*, FKZ 03IHS242D).

REFERENCES

[1] Barrett Adams. 2023. *Invoke-PSImage.* https://github.com/peewpw/Invoke-PSImage

[2] Manoj Ahuje. 2022. *LemonDuck Botnet Targets Dockerfor Cryptomining Operations | CrowdStrike.* crowdstrike.com. https://www.crowdstrike.com/blog/lemonduck-botnet-targets-docker-for-cryptomining-operations/

[3] Airbus. 2022. *Vinself Now with Steganography - Airbus Defence and Space Cyber.* Airbus. https://www.cyber.airbus.com/vinself-now-steganography/

[4] M. Alenezi, H. Alabdulrazzaq, A. Alshaher, and M. Alkharang. 2020. Evolution of Malware Threats and Techniques: A Review. *International journal of communication networks and information security* 12, 3 (2020), 326–337.

[5] AV-TEST. 2023. *Malware | AV-TEST.* AV-TEST. https://www.av-test.org/de/statistiken/malware/

[6] Benjamin Aziz and Aysha Bukhelli. 2023. Detecting the Manipulation of Text Structure in Text Steganography Using Machine Learning. In *Proc. of the 19th Int. Conf. on Web Information Systems and Technologies, WEBIST 2023, Rome, Italy, November 15-17, 2023,* Francisco J. García-Peñalvo and Massimo Marchiori (Eds.). SCITEPRESS, 557–565. https://doi.org/10.5220/0012260900003584

[7] Robert Falcone Barbehenn, Brittany. 2019. *xHunt Campaign: Attacks on Kuwait Shipping and Transportation Organizations.* Unit 42. https://unit42.paloaltonetworks.com/xhunt-campaign-attacks-on-kuwait-shipping-and-transportation-organizations/

[8] Robert Falcone Barbehenn, Brittany. 2019. *xHunt Campaign: New PowerShell Backdoor Blocked Through DNS Tunnel Detection.* Unit 42. https://unit42.paloaltonetworks.com/more-xhunt-new-powershell-backdoor-blocked-through-dns-tunnel-detection/

[9] BfV. 2020. *BfV Cyber-Brief Nr. 01/2020.* Technical Report. Bundesamt für Verfassungsschutz.

[10] J. Boutin. 2019. *Buhtrap Group Uses Zero-Day in Latest Espionage Campaigns.* ESET. https://www.welivesecurity.com/2019/07/11/buhtrap-zero-day-espionage-campaigns/

[11] R. Bowes. 2023. *DNSCat2.* Retrieved 2023-12-09 from https://github.com/iagox86/dnscat2

[12] Kevin Breen. 2023. *Detecting and Decrypting Sliver C2 – a Threat Hunter's Guide.* Immersive Labs. https://www.immersivelabs.com/blog/detecting-and-decrypting-sliver-c2-a-threat-hunters-guide/

[13] Edmund Brumaghin. 2020. *Threat Spotlight: Astaroth — Maze of Obfuscation and Evasion Reveals Dark Stealer.* Cisco Talos Blog. https://blog.talosintelligence.com/astaroth-analysis/

[14] Krzysztof Cabaj, Luca Caviglione, Wojciech Mazurczyk, Steffen Wendzel, Alan Woodward, and Sebastian Zander. 2018. The New Threats of Information Hiding: The Road Ahead. *IT Professional* 20, 3 (05 2018), 31–39. https://doi.org/10.1109/MITP.2018.032501746

[15] Luigino Camastra. 2021. *Backdoored Client from Mongolian CA MonPass.* Avast Threat Labs. https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/

[16] Luca Caviglione. 2023. *Steg-in-the-Wild.* https://github.com/lucacav/steg-in-the-wild

[17] Luca Caviglione, Micha\ l Choraś, Igino Corona, Artur Janicki, Wojciech Mazurczyk, Marek Pawlicki, and Katarzyna Wasielewska. 2021. Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection. *IEEE Access* 9 (2021), 5371–5396. https://doi.org/10.1109/ACCESS.2020.3048319

[18] Luca Caviglione and Wojciech Mazurczyk. 2022. Never Mind the Malware, Here's the Stegomalware. *IEEE Security & Privacy* 20, 5 (2022), 101–106.

[19] SANS Internet Storm Center. 2019. *Guildma Malware Is Now Accessing Facebook and YouTube to Keep Up-to-Date.* SANS Internet Storm Center. https://isc.sans.edu/diary/Guildma+malware+is+now+accessing+Facebook+andYouTube+to+keep+uptodate/25222

[20] National Cyber Security Centre. 2022. *Small Sieve Malware Analysis Report.* Technical Report. NCSC.

[21] Kaspersky ICS CERT. 2021. *APT Attacks on Industrial Organizations in H1 2021.* Technical Report. Kaspersky.

[22] Nicolas Chatelain. 2023. *Ligolo-Ng : Tunneling like a VPN.* https://github.com/nicocha30/ligolo-ng

[23] J. Chen. 2020. *Tropic Trooper's Back: USBferry Attack Targets Air-gapped Environments.* Technical Report. Trend Micro.

[24] Joey Chen. 2020. *Tropic Trooper's USBferry Targets Air-Gapped Networks.* Trend Micro. https://www.trendmicro.com/en_us/research/20/e/tropic-troopers-back-usbferry-attack-targets-air-gapped-environments.html

[25] Joey Chen. 2022. *Aoqin Dragon | Newly-Discovered Chinese-linked APT Has Been Quietly Spying On Organizations For 10 Years.* SentinelOne. https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/

[26] J. Chen, H. Kakara, and M. Shoji. 2019. *Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data.* Technical Report. Trend Micro.

[27] CISA. 2020. *Iran-Based Threat Actor Exploits VPN Vulnerabilities | CISA.* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-259a

[28] DXC Technology Company. 2021. *Security threat intelligence report.* Technical Report. DXC Technology Company. https://dxc.com/content/dam/dxc/projects/dxc-com/us/pdfs/services/security/DXC-Security-Threat-Intelligence-Report-June-2021.pdf

[29] Quinn Cooke, Alex Hincliffe, and Robert Falcone. 2021. *Mespinoza Ransomware Gang Calls Victims "Partners," Attacks with Gasket, "MagicSocks" Tools.* Unit 42. https://unit42.paloaltonetworks.com/gasket-and-magicsocks-tools-install-mespinoza-ransomware/

[30] A. Cristian. 2023. *Advanced Onion Router.* GitHub. https://github.com/AdvOR

[31] A. Dahan. 0. *New Ursnif Variant Targets Japan Packed with New Features.* Cybereason. https://www.cybereason.com/blog/research/new-ursnif-variant-targets-japan-packed-with-new-features

[32] Nick Dai, Ted Lee, and Vickie Su. 2021. *Tropic Trooper Targets Transportation and Government Organizations.* Trend Micro. https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html

[33] Pratim Datta. 2022. Hannibal at the Gates: Cyberwarfare & the Solarwinds Sunburst Hack. *Journal of Information Technology Teaching Cases* 12, 2 (2022), 115–120. https://doi.org/10.1177/2043886921993126

[34] Jason Deyalsingh, Nick Smith, Eduardo Mattos, and Tyler McLellan. 2023. *ALPHV Ransomware Affiliate Targets Vulnerable Backup Installations to Gain Initial Access.* Mandiant. https://www.mandiant.com/resources/blog/alphv-ransomware-backup

[35] Security division of NTT Ltd. 2020. *TrickBot Variant "Anchor_DNS" Communicating over DNS.* NTT Ltd. https://services.global.ntt/en-us/insights/blog/trickbot-variant-communicating-over-dns

[36] A. Dolgushev, V. Berdnikov, and I. Pomerantsev. 2019. *Platinum Is Back.* Kaspersky. https://securelist.com/platinum-is-back/91135/

[37] A. Ebel. 2020. *WINNTI GROUP: Insights From the Past - QuoIntelligence.* QuoIntelligence GmbH. https://quointelligence.eu/2020/04/winnti-group-insights-from-the-past/

[38] Stephen Eckels, Jay Smith, and William Ballenthin. 2021. *SUNBURST Additional Technical Details.* Mandiant. https://www.mandiant.com/resources/blog/sunburst-additional-technical-details

[39] D. Emm. 2020. *IT Threat Evolution Q2 2020.* Kaspersky. https://securelist.com/it-threat-evolution-q2-2020/98230/

[40] PT ESC. 2023. *Space Pirates: A Look into the Group's Unconventional Techniques, New Attack Vectors, and Tools.* ptsecurity.com. https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-a-look-into-the-group-s-unconventional-techniques-new-attack-vectors-and-tools/

[41] F-Secure. 2019. Killsuit Research. https://blog.f-secure.com/wp-content/uploads/2019/10/Killsuit_Research_01.pdf

[42] Kyle Wilhoit Falcone, Robert. 2018. *OilRig Uses Updated BONDUPDATER to Target Middle Eastern Government.* Unit 42. https://unit42.paloaltonetworks.com/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/

[43] Robert Falcone. 2020. *OilRig Targets Middle Eastern Telecommunications Organization and Adds Novel C2 Channel with Steganography to Its Inventory.* Unit 42. https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/

[44] Robert Falcone. 2020. *xHunt Campaign: Newly Discovered Backdoors Using Deleted Email Drafts and DNS Tunneling for Command and Control.* Unit 42. https://unit42.paloaltonetworks.com/xhunt-campaign-backdoors/

[45] Matthieu Faou. 2019. *TURLA LIGHTNEURON One Email Away from Remote Code Execution.* Technical Report. ESET.

[46] M. Faou. 2020. *From Agent.BTZ to ComRAT v4: A Ten-Year Journey.* ESET. https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/

[47] M. Faou. 2023. *MoustachedBouncer: Espionage against Foreign Diplomats in Belarus.* ESET. https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/

[48] Matthieu Faou, Mathieu Tartare, and Thomas Dupuy. 2019. *OPERATION GHOST The Dukes Aren't Back - They Never Left.* ESET. https://web-assets.esetstatic.com/wls/2019/10/ESET_Operation_Ghost_Dukes.pdf

[49] Stephen Farrell, Farzaneh Badiei, Bruce Schneier, and Steven M. Bellovin. 2023. Reflections on Ten Years Past the Snowden Revelations. RFC 9446. https://doi.org/10.17487/RFC9446

[50] FBI, CISA, USCC, NCSC, GCHQ, and NSA. 2022. *Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks (Product-ID: AA22-055A).* Technical Report. CISA.

[51] Fraunhofer FKIE. 2023. *Malpedia (Fraunhofer FKIE).* Fraunhofer FKIE. https://malpedia.caad.fkie.fraunhofer.de/

[52] Eric Ford. 2023. *Cyber Intel Brief: September 28 – October 03, 2023.* Deepwatch. https://www.deepwatch.com/labs/cyber-intel-brief-september-28-october-03-2023/

[53] T. Forry. 2023. *Application for search warrant: In the matter of the search of information associated with computer constituting associated with computers constituting the Snake malware network: Docket No. 23-MJ-0428 (CLP).* Technical

Report. FBI.

[54] Recorded Future. 2023. BlueBravo Uses Ambassador Lure to Deploy Graphical-Neutrino Malware.

[55] S. Gatlan. 2023. *Discord Will Switch to Temporary File Links to Block Malware Delivery*. BleepingComputer. https://www.bleepingcomputer.com/news/security/discord-will-switch-to-temporary-file-links-to-block-malware-delivery/

[56] ginuerzh. 2023. *GO Simple Tunnel*. https://github.com/ginuerzh/gost

[57] GReAT. 2019. *ScarCruft Continues to Evolve, Introduces Bluetooth Harvester*. ESET. https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/

[58] GReAT and S. Lozhkin. 2023. *DoubleFinger Delivers GreetingGhoul Cryptocurrency Stealer*. Kaspersky. https://securelist.com/doublefinger-loader-delivering-greetingghoul-cryptocurrency-stealer/109982/

[59] L. Grespan. 2023. *ChunkyTuna*. Secarma Ltd. https://github.com/SecarmaLabs/chunkyTuna

[60] MAWI Working Group. 2023. *MAWI Working Group Traffic Archive*. WIDE Project. Retrieved 2023-12-06 from https://mawi.wide.ad.jp/mawi/

[61] hadar_cpr. 2022. *Check Point CloudGuard Spectral Exposes New Obfuscation Techniques for Malicious Packages on PyPI*. Check Point Research. https://research.checkpoint.com/2022/check-point-cloudguard-spectral-exposes-new-obfuscation-techniques-for-malicious-packages-on-pypi/

[62] Karsten Hahn. 2021. *SteamHide: Hiding Malware in Plain Sight | G DATA*. G DATA CyberDefense AG. Retrieved 2023-12-04 from https://web.archive.org/web/20210718145830/https://www.gdatasoftware.com/blog/steamhide-malware-in-profile-images

[63] hasherezade. 2023. *From Hidden Bee to Rhadamanthys - The Evolution of Custom Executable Formats*. Check Point Research. https://research.checkpoint.com/2023/from-hidden-bee-to-rhadamanthys-the-evolution-of-custom-executable-formats/

[64] Hara Hiroaki and Ted Lee. 2021. Earth Baku: An APT Group Targeting Indo-Pacific Countries With New Stealth Loaders and Backdoor. https://documents.trendmicro.com/assets/white_papers/wp-earth-baku-an-apt-group-targeting-indo-pacific-countries.pdf

[65] Paul E. Hoffman and Patrick McManus. 2018. *DNS Queries over HTTPS (DoH)*. Request for Comments RFC 8484. Internet Engineering Task Force. https://doi.org/10.17487/RFC8484

[66] Rene Holt. 2020. *Detecting Elusive Techniques of the Dukes Threat Group with ESET Enterprise Inspector*. ESET. https://www.eset.com/blog/enterprise/detecting-elusive-techniques-of-the-dukes-threat-group-with-eset-enterprise-inspector/

[67] Zuzana Hromcová. 2019. *Okrum and Ketrican: An Overview of recent Ke3chang group activity*. Technical Report. ESET.

[68] Zuzana Hromcová and Anton Cherepanov. 2020. Unearthing invisimole's espionage toolset and strategic cooperations.

[69] Karel Hynek, Dmitrii Vekshin, Jan Luxemburk, Tomas Cejka, and Armin Wasicek. 2022. Summary of DNS Over HTTPS Abuse. *IEEE Access* 10 (2022), 54668–54680. https://doi.org/10.1109/ACCESS.2022.3175497

[70] icesurfer and nico. 2023. *Heyoka: Your Fast&spoofed DNS Tunnel*. https://heyoka.sourceforge.net/

[71] Fireeye Threat Intelligence. 2015. *HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group*. Technical Report. FireEye. https://s3.documentcloud.org/documents/2186063/apt29-hammertoss-stealthy-tactics-define-a.pdf

[72] Microsoft Threat Intelligence. 2023. *Diamond Sleet Supply Chain Compromise Distributes a Modified CyberLink Installer*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2023/11/22/diamond-sleet-supply-chain-compromise-distributes-a-modified-cyberlink-installer/

[73] Paul Jaramillo. 2023. *Akira Ransomware Is "Bringin' 1988 Back"*. Sophos News. https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/

[74] Josue. 2022. *Silent Push Maps over 150 New Lumma C2 Infostealer IOCs*. Silent Push Threat Intelligence. https://www.silentpush.com/blog/lummac2

[75] Filip Jurčacko. 2024. *To the Moon and back(doors): Lunar landing in diplomatic missions*. ESET Research. https://www.welivesecurity.com/en/eset-research/moon-backdoors-lunar-landing-diplomatic-missions/

[76] A. Kayal, M. Lechtik, and P. Rascagneres. 2021. LYCEUM REBORN: counterintelligence in the middle east. In *Virus Bulletin Conference October 2021*. Kaspersky, Israel. https://vblocalhost.com/uploads/VB2021-Kayal-etal.pdf

[77] J. Kennedy and The BlackBerry Research & Intelligence Team. 2022. *Symbiote: A New, Nearly-Impossible-to-Detect Linux Threat*. BlackBerry. https://blogs.blackberry.com/en/2022/06/symbiote-a-new-nearly-impossible-to-detect-linux-threat

[78] kost. 2023. *Revsocks*. https://github.com/kost/revsocks

[79] I. Kwiatkowski, P. Delcher, and F. Aime. 2020. *IAmTheKing and the SlothfulMedia Malware Family*. Kaspersky. https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/

[80] Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon (Eds.). 2013. *Information Security and Cryptology – ICISC 2012: 15th International Conference, Seoul, Korea, November 28-30, 2012, Revised Selected Papers*. Lecture Notes in Computer Science, Vol. 7839. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37682-5

[81] L. 2023. *Neo-reGeorg*. https://github.com/L-codes/Neo-reGeorg

[82] Pangu Lab. 2022. *Bvp47 Top-tier Backdoor of US NSA Equation Group*. Technical Report. Beijing Qi An Pangu Laboratory Technology Co., Ltd. https://www.pangulab.cn/files/The_Bvp47_a_top-tier_backdoor_of_us_nsa_equation_group.en.pdf

[83] Black Lotus Labs. 2022. *ZuoRAT Hijacks SOHO Routers to Silently Stalk Networks - Lumen*. Black Lotus Labs. https://blog.lumen.com/zuorat-hijacks-soho-routers-to-silently-stalk-networks/

[84] Ravie Lakshmanan. 2020. *New ComRAT Malware Uses Gmail to Receive Commands and Exfiltrate Data*. The Hacker News. https://thehackernews.com/2020/05/gmail-malware-hacker.html

[85] Butler W Lampson. 1973. A Note on the Confinement Problem. *Commun. ACM* 16, 10 (1973), 613–615.

[86] D. Legezo. 2020. *MontysThree: Industrial Espionage with Steganography and a Russian Accent on Both Sides*. Kaspersky. https://securelist.com/montysthree-industrial-espionage/98972/

[87] J. Lepore. 2019. *DNS Tunneling Series, Part 1: Chirp of the PoisonFrog*. IronNet. https://www.ironnet.com/blog/chirp-of-the-poisonfrog

[88] Jonathan Lepore. 2020. *DNS Tunneling Series, Part 3: The Siren Song of RogueRobin*. IronNet. https://www.ironnet.com/blog/dns-tunneling-series-part-3-the-siren-song-of-roguerobin

[89] Songbin Li, Jingang Wang, and Peng Liu. 2023. Detection of Generative Linguistic Steganography Based on Explicit and Latent Text Word Relation Mining Using Deep Learning. *IEEE Trans. Dependable Secur. Comput.* 20, 2 (2023), 1476–1487. https://doi.org/10.1109/TDSC.2022.3156972

[90] Chris M. Lonvick and Tatu Ylonen. 2006. *The Secure Shell (SSH) Transport Layer Protocol*. Request for Comments RFC 4253. Internet Engineering Task Force. https://doi.org/10.17487/RFC4253 Num Pages: 32.

[91] D. Lunghi. 2023. *Iron Tiger's SysUpdate Reappears, Adds Linux Targeting*. Trend Micro. https://www.trendmicro.com/en_us/research/23/c/iron-tiger-sysupdate-adds-linux-targeting.html

[92] L. Macrohon and R. Mendrez. 2021. *Pingback: Backdoor At The End Of The ICMP Tunnel | Trustwave*. Trustwave. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/backdoor-at-the-end-of-the-icmp-tunnel/

[93] Asheer Malhotra. 2021. *ObliqueRAT Returns with New Campaign Using Hijacked Websites*. Cisco Talos Blog. https://blog.talosintelligence.com/obliquerat-new-campaign/

[94] C. Malipot. 2023. *Beware Lumma Stealer Distributed via Discord CDN*. Trend Micro. https://www.trendmicro.com/en_us/research/23/j/beware-lumma-stealer-distributed-via-discord-cdn-.html

[95] Wojciech Mazurczyk and Luca Caviglione. 2014. Steganography in modern smartphones and mitigation techniques. *IEEE Communications Surveys & Tutorials* 17, 1 (2014), 334–357.

[96] Wojciech Mazurczyk and Luca Caviglione. 2015. Information Hiding as a Challenge for Malware Detection. *IEEE Security & Privacy* 13, 2 (2015), 89–93. https://doi.org/10.1109/MSP.2015.33

[97] W. Mercer and P. Rascagneres. 2019. *DNSpionage Brings out the Karkoff*. Cisco Talos Blog. https://blog.talosintelligence.com/dnspionage-brings-out-karkoff/

[98] Xavier Mertens. 2023. *ShellCode Hidden with Steganography*. SANS Internet Storm Center. https://isc.sans.edu/diary/ShellCode+Hidden+with+Steganography/30074

[99] P. Mockapetris. 1987. *Domain names - implementation and specification*. Request for Comments RFC 1035. Internet Engineering Task Force. https://doi.org/10.17487/RFC1035 Num Pages: 55.

[100] Mohammadreza MontazeriShatoori, Logan Davidson, Gurdip Kaur, and Arash Habibi Lashkari. 2020. Detection of DoH Tunnels using Time-series Classification of Encrypted Traffic. In *IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress, DASC/PiCom/CBDCom/CyberSciTech 2020, Calgary, AB, Canada, August 17-22, 2020*. IEEE, 63–70. https://doi.org/10.1109/DASC-PICOM-CBDCOM-CYBERSCITECH49142.2020.00026

[101] P. Nair. 2022. *MuddyWater Targets Critical Infrastructure in Asia, Europe*. Global News Desk, ISMG. https://www.inforisktoday.com/muddywater-targets-critical-infrastructure-in-asia-europe-a-18611

[102] Felipe Naves, Adam McNeil, and Andrew Conway. 2021. *Mobile Malware: TangleBot Untangled | Proofpoint US*. Proofpoint. https://www.proofpoint.com/us/blog/threat-insight/mobile-malware-tanglebot-untangled

[103] ngrok. 2023. *Ngrok | Unified Application Delivery Platform for Developers*. ngrok, Inc. https://ngrok.com/

[104] heise online. 2022. *Backdoor in Windows-Logo versteckt*. heise online. https://www.heise.de/news/Backdoor-in-Windows-Logo-versteckt-7282730.html

[105] Crowdstrike Overwatch Team. 2020. Nowhere to Hide 2020 Threat Hunting Report. https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020OverWatchNowheretoHide.pdf

[106] S. Park. 2021. Multi-universe of adversary: Multiple compaigns of LAZARUS group and its connection. In *Virus Bulletin Conference October 2021*. Kaspersky, Republic of Korea. https://vblocalhost.com/uploads/VB2021-Park.pdf

[107] T. Pereira. 2021. *Magnat Campaigns Use Malvertising to Deliver Information Stealer, Backdoor and Malicious Chrome Extension.* Cisco Talos Blog. https://blog.talosintelligence.com/magnat-campaigns-use-malvertising-to/

[108] Fabien A. P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn. 1999. Information hiding-a survey. *Proc. IEEE* 87, 7 (1999), 1062–1078. https://doi.org/10.1109/5.771065

[109] Jaime Pillora. 2023. *Chisel.* https://github.com/jpillora/chisel

[110] M. Porolli. 2022. *POLONIUM Targets Israel with Creepy Malware.* ESET. https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/

[111] J. Postel. 1981. *Internet Control Message Protocol.* Request for Comments RFC 792. Internet Engineering Task Force. https://doi.org/10.17487/RFC0792 Num Pages: 21.

[112] PricewaterhouseCoopers. 2020. *How WellMess Malware Has Been Used to Target COVID-19 Vaccines.* PwC. https://www.pwc.co.uk/issues/cyber-security-services/insights/cleaning-up-after-wellmess.html

[113] Rapid7. 2023. *Metasploit | Penetration Testing Software, Pen Testing Security.* Metasploit. https://www.metasploit.com/

[114] Augusto Remillano II and Kiyoshi Obuchi. 2019. *Examining Powload's Evolution.* Trend Micro. https://www.trendmicro.com/en_us/research/19/c/from-fileless-techniques-to-using-steganography-examining-powloads-evolution.html

[115] Lior Rochberger and Daniel Frank. 2024. *Operation Diplomatic Specter: An Active Chinese Cyberespionage Campaign Leverages Rare Tool Set to Target Governmental Entities in the Middle East, Africa and Asia.* PaloAlto. https://unit42.paloaltonetworks.com/operation-diplomatic-specter/

[116] Tobias Schmidbauer and Steffen Wendzel. 2022. SoK: A survey of indirect network-level covert channels. In *Proc. AsiaCCS.* 546–560.

[117] L. Schumann, T. Doan, T. Shreedhar, R. Mok, and V. Bajpai. 2022. Impact of Evolving Protocols and COVID-19 on Internet Traffic Shares. (15 01 2022). arXiv:2201.00142 [cs] http://arxiv.org/abs/2201.00142

[118] Alberto Segura and Rolf Govers. 2022. *Flubot: The Evolution of a Notorious Android Banking Malware.* Fox-IT International blog. https://blog.fox-it.com/2022/06/29/flubot-the-evolution-of-a-notorious-android-banking-malware/

[119] Sergei Shevchenko. 2020. Cloud Snooper Attack Bypasses AWS Security Measures. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-cloud-snooper-report.pdf

[120] N. Shivtarkar and A. Kumar. 2022. *Lyceum .NET DNS Backdoor.* Zscaler. https://www.zscaler.com/blogs/security-research/lyceum-net-dns-backdoor

[121] Denis Sinegubko. 2021. *Whitespace Steganography Conceals Web Shell in PHP Malware.* Sucuri Blog. https://blog.sucuri.net/2021/02/whitespace-steganography-conceals-web-shell-in-php-malware.html

[122] Anuj Soni, Jordan Barth, and Brian Marks. 2019. *Malicious Payloads - Hiding Beneath the WAV.* BlackBerry. https://blogs.blackberry.com/en/2019/10/malicious-payloads-hiding-beneath-the-wav

[123] Mark Stockley. 2022. *How the Saitama Backdoor Uses DNS Tunnelling.* Malwarebytes. https://www.malwarebytes.com/blog/news/2022/05/how-the-saitama-backdoor-uses-dns-tunnelling

[124] Fabian Strachanski. 2023. *63580 MalpediaScanner.* https://github.com/fastrde/63580-malpedia-scanner

[125] Gabor Szappanos. 2020. *MyKings: The Slow But Steady Growth of a Relentless Botnet.* Technical Report. SophosLabs. https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-mykings-report.pdf

[126] János Gergõ Széles. 2021. Remcos RAT Revisited: A Colombian Coronavirus-Themed Campaign. https://www.bitdefender.com/files/News/CaseStudies/study/390/Bitdefender-PR-Whitepaper-Remcos-creat5080-en-EN-GenericUse.pdf

[127] tccontre. 2021. *Iceid_png_shellcode_extractor.Py.* https://github.com/tccontre/KnowledgeBase/tree/main/malware_re_tools/iceid_stego_shell_decryptor

[128] Counter Threat Unit Research Team. 2020. *Business as Usual For Iranian Operations Despite Increased Tensions.* Secureworks. https://www.secureworks.com/blog/business-as-usual-for-iranian-operations-despite-increased-tensions

[129] Counter Threat Unit Research Team. 2022. *Drokbk Malware Uses GitHub as Dead Drop Resolver.* Secureworks. https://www.secureworks.com/blog/drokbk-malware-uses-github-as-dead-drop-resolver

[130] Guardicore Labs Team. 2023. *Threats Making WAVs - Incident Response to a Cryptomining Attack.* Akamai. https://www.akamai.com/blog/security/threats-making-wavs-incident-reponse-cryptomining-attack

[131] Proofpoint Threat Insight Team. 2019. *URLZone Top Malware in Japan, While Emotet and LINE Phishing Round out the Landscape | Proofpoint US.* Proofpoint. https://www.proofpoint.com/us/threat-insight/post/urlzone-top-malware-japan-while-emotet-and-line-phishing-round-out-landscape-0

[132] SonicWall Capture Labs Threat Research Team. 2019. *Loki-Bot: Started Using Image Steganography And Multi-Layered Protection – SonicWall.* Trend Micro. https://securitynews.sonicwall.com/xmlpost/loki-bot-started-using-image-steganography-and-multi-layered-protection/

[133] Splunk Threat Research Team. 2021. *Detecting IcedID... Could It Be A Trickbot Copycat?* Splunk-Blogs. https://www.splunk.com/en_us/blog/security/detecting-icedid-could-it-be-a-trickbot-copycat.html

[134] The BlackBerry Research & Intelligence Team. 2021. *PYSA Loves ChaChi: A New GoLang RAT.* BlackBerry. https://blogs.blackberry.com/en/2021/06/pysa-loves-chachi-a-new-golang-rat

[135] The BlackBerry Research & Intelligence Team. 2021. *Threat Thursday: SombRAT — Always Leave Yourself a Backdoor.* BlackBerry. https://blogs.blackberry.com/en/2021/05/threat-thursday-sombrat-always-leave-yourself-a-backdoor

[136] Threat Hunter Team. 2021. *SolarWinds: How Sunburst Sends Data Back to the Attackers.* Symantec. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-sunburst-sending-data

[137] Threat Hunter Team. 2022. *Witchetty: Group Uses Updated Toolset in Attacks on Governments in Middle East.* Symantec. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/witchetty-steganography-espionage

[138] Threat Hunter Team. 2023. *Bluebottle: Campaign Hits Banks in French-speaking Countries in Africa.* Symantec. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africa

[139] Threat Intelligence Team. 2023. *Uncovering RedStinger - Undetected APT Cyber Operations in Eastern Europe since 2020.* Malwarebytes. https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger/

[140] Gianluca Tiepolo. 2023. *Sophisticated APT29 Campaign Abuses Notion API to Target the European Commission.* Medium. https://mrtiepolo.medium.com/sophisticated-apt29-campaign-abuses-notion-api-to-target-the-european-commission-200188059f58

[141] Shusel Tomonaga. 2021. *Operation Dream Job by Lazarus.* JPCERT/CC Eyes. https://blogs.jpcert.or.jp/en/2021/01/Lazarus_malware2.html

[142] Bill Toulas. 2022. *Hackers Hide Malware in James Webb Telescope Images.* BleepingComputer. https://www.bleepingcomputer.com/news/security/hackers-hide-malware-in-james-webb-telescope-images/

[143] Bill Toulas. 2022. *Worok Hackers Hide New Malware in PNGs Using Steganography.* BleepingComputer. https://www.bleepingcomputer.com/news/security/worok-hackers-hide-new-malware-in-pngs-using-steganography/

[144] Bill Toulas. 2024. *Hackers use DNS tunneling for network scanning, tracking victims.* BleepingComputer. https://www.bleepingcomputer.com/news/security/hackers-use-dns-tunneling-for-network-scanning-tracking-victims/

[145] VirusShare. 2022. *Serpent Dropper | VirusShare.Com.* Corvus Forensics. https://virusshare.com/file?f6d2becc3531e98e7c6331d3e5b269a54a83c1af8f9605d6daea6531a6d72b99

[146] Victor Vrabie. 2020. Dissecting a Chinese APT Targeting South Eastern Asian Government Institutions. https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf

[147] Wahlén. 2021. *Notorious Cybercriminals Evil Corp Actually Russian Spies? - Trulysuper.* Truesec. https://www.truesec.com/hub/blog/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies

[148] Steffen Wendzel, Luca Caviglione, Wojciech Mazurczyk, Aleksandra Mileva, Jana Dittmann, Christian Krätzer, Kevin Lamshöft, Claus Vielhauer, Laura Hartmann, Jörg Keller, and Tom Neubert. 2021. A Revised Taxonomy of Steganography Embedding Patterns. In *ARES 2021: The 16th International Conference on Availability, Reliability and Security, Vienna, Austria, August 17-20, 2021*, Delphine Reinhardt and Tilo Müller (Eds.). ACM, 67:1–67:12. https://doi.org/10.1145/3465481.3470069

[149] Steffen Wendzel, Luca Caviglione, Wojciech Mazurczyk, Aleksandra Mileva, Jana Dittmann, Christian Krätzer, Kevin Lamshöft, Claus Vielhauer, Laura Hartmann, Jörg Keller, Tom Neubert, and Sebastian Zillien. 2022. A Generic Taxonomy for Steganography Methods. (2022). https://www.techrxiv.org/doi/full/10.36227/techrxiv.20215373

[150] Steffen Wendzel, Wojciech Mazurczyk, Luca Caviglione, and Michael Meier. 2014. Hidden and uncontrolled–on the emergence of network steganographic threats. In *ISSE 2014 Securing Electr. Business Processes: Highlights of the Inf. Sec. Sol. Europe 2014 Conf.* Springer Fachmedien Wiesbaden, Wiesbaden, 123–133.

[151] Steffen Wendzel, Sebastian Zander, Bernhard Fechner, and Christian Herdin. 2015. Pattern-Based Survey and Categorization of Network Covert Channel Techniques. *ACM Computing Surveys (CSUR)* 47, 3 (2015), 1–26.

[152] john Wolfram, Sarah Hawley, Tyler McLellan, Nick Simonian, and Anders Vejlby. 2022. *Tracking APT29 Phishing Campaigns | Atlassian Trello.* Mandiant. https://www.mandiant.com/resources/blog/tracking-apt29-phishing-campaigns

[153] Karlo Zanki. 2021. *Malware in Images: When You Can't See 'the Whole Picture'.* ReversingLabs. https://www.reversinglabs.com/blog/malware-in-images

[154] Yanhui Zhang, Chris Jia, and Navarrete Haozhe. 2020. *njRAT Spreading Through Active Pastebin Command and Control Tunnel.* Unit 42. https://unit42.paloaltonetworks.com/njrat-pastebin-command-and-control/

[155] A. Zhdanov. 2022. *Fat Cats.* Group-IB. https://www.group-ib.com/blog/blackcat/