A Comprehensive Pattern-based Overview of Stegomalware

Fabian Strachanski[1,2], Denis Petrov[3], Tobias Schmidbauer[4], Steffen Wendzel[2,3]

[1] University of Duisburg-Essen, Germany
[2] FernUniversität in Hagen, Germany
[3] Hochschule Worms, Germany
[4] Nuremberg Institute of Technology, Germany

Context

- It is often claimed that steganography is used by some kind of adversaries, e.g., to render malware more *stealthy*. Such malware is often called **stegomalware**.

Context

- It is often claimed that steganography is used by some kind of adversaries, e.g., to render malware more *stealthy*. Such malware is often called **stegomalware**.

- We wanted to know: **How many cases of stegomalware do actually exist?**

Context

- It is often claimed that steganography is used by some kind of adversaries, e.g., to render malware more *stealthy*. Such malware is often called **stegomalware**.
- We wanted to know: **How many cases of stegomalware do actually exist?**
- **Our research questions:**
  1. Are there actually more than a few cases of malware utilizing steganography?
  2. How many cases of stegomalware are present for digital media (image, audio, video), network, and text steganography?
  3. What kind of methods is used by these malware-cases?

Methodology

- Considered **malware that appeared within the last five years**
- Searched blog articles, threat reports, articles, and analyses from IT security companies and security researchers.
- Searched *Malpedia* [Fraunhofer FKIE(2023)].
  - Keywords: “stegano”, “stego”, “tunnel” and “covert”.
  - Wrote a Python script; resulting 654 entries were checked manually. Script available on *GitHub*.
- IEEEXplore, Google Scholar, SpringerLink, ACM DL, TechRxiv, arXiv and ResearchGate: “MALWARE” AND “Name of the Malware”.
- Consulted *steg-in-the-wild* list by Luca Caviglione [Caviglione(2023)] (version of Sep-28, 2023)

Methodology

- Considered **malware that appeared within the last five years**
- Searched blog articles, threat reports, articles, and analyses from IT security companies and security researchers.
- Searched *Malpedia* [Fraunhofer FKIE(2023)].
  - Keywords: “stegano”, “stego”, “tunnel” and “covert”.
  - Wrote a Python script; resulting 654 entries were checked manually. Script available on *GitHub*.
- IEEEXplore, Google Scholar, SpringerLink, ACM DL, TechRxiv, arXiv and ResearchGate: “MALWARE” AND “Name of the Malware”.
- Consulted *steg-in-the-wild* list by Luca Caviglione [Caviglione(2023)] (version of Sep-28, 2023)

Result

106 malware cases, described in 133 reports (duplicates were already removed manually)

Related Work

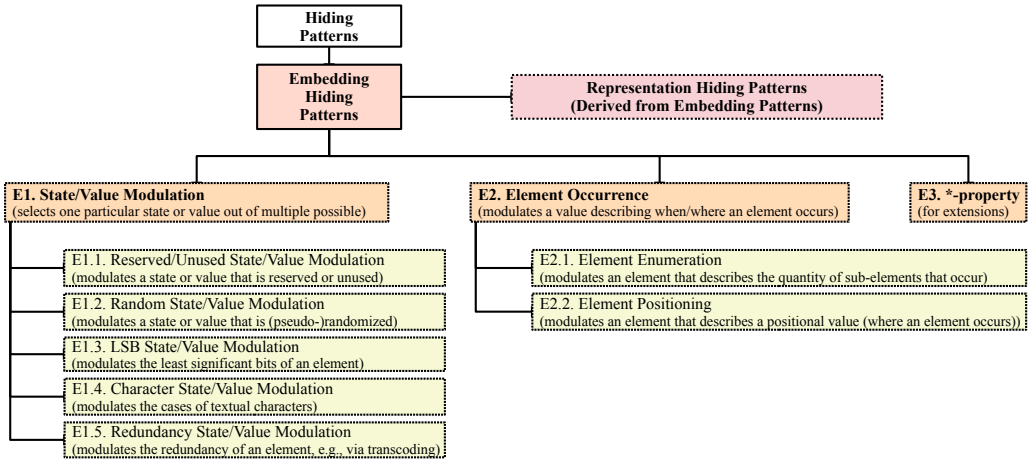
Studies already analyze stegomalware but discuss stegomalware in general or cover only few cases:

Paper	Year	Cases	Categorization
[Wendzel et al.(2014)]	2014	(*) ca. 10	-
[Mazurczyk and Caviglione(2014)]	2014	(*) 47	smartphone characteristics
[Mazurczyk and Caviglione(2015)]	2015	21	three groups
[Cabaj et al.(2018)]	2018	14	four groups
[Caviglione and Mazurczyk(2022)]	2022	18	three groups
Our paper	2024	**106**	pattern-based

* Includes larger fraction of pure academic approaches instead of solely real-world malware.

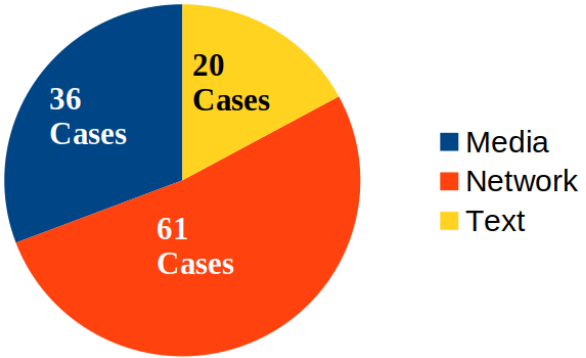
We provide a coverage of the **most recent stegomalware**. Our work is also the **most comprehensive** survey of stegomalware (especially *real* malware samples) and are the first to apply a categorization based on **hiding patterns**.

Taxonomy



[Wendzel et al.(2022)]: *A Generic Taxonomy for Steganography Methods.*

Findings: Overview of Cases per Research Area



→ More than half (57.5%) of stegomalware cases employ **network** steganography.

Media Stegomalware (36 Cases)

Malware	Object	tp*	technique	pattern	Sources
ABK	Image (JPG)		Embeds malicious payload into image files in cleartext	E1d1	[Chen et al.(2019)]
apicolor	Image (PNG)	x	LSB	E1.3d1	[hadar_cpr(2022)]
Avenger	Image		LSB	E1.3d1	[Chen et al.(2019)]
build_downer	Image (JPG)		Uses every fourth byte of the image data	E1d1	[Chen et al.(2019)]
CookieTime	Image (GIF)		Prepends gif header	E1d1	[Park(2021)]
DoubleFinger	Image (PNG)	x	Uses bytes at known offsets (visible)	E1d1	[GReAT and Lozhkin(2023)]
FatDuke	Image (PNG)		Prepends (corrupted) png header	E1d1	[Faou et al.(2019)]
Hammertoss	Image (JPG)	x	Append to end of image file	E1.1d1	[Intelligence(2015)]
IcedID	Image (PNG)		Uses IDAT-Chunk to store encrypted data	E1d1/E1.1d1	[Team(2021a)][tccontre(2021)]
LambLoad	Image (PNG)		Uses wrong size in IDAT-Chunk to store data behind	E1.1d1	[Intelligence(2023)]
lightneuron	Image (JPG)		Uses start of *scan section* and *quantization table*	E1d1	[Faou(2019)]
Lokibot	Image (JPG, PNG)		LSB	E1.3d1	[Team(2019b)]
Lumma	Image (PNG)		Unknown	Unknown	[Ford(2023)][Josue(2022)]
LunarWeb	Image (JPG, GIF)		embeds data inside a JPG comment or in a GIF data block	Unknown	[Jurčacko(2024)]
LunarMail	Image (PNG)		AES encrypted data in IDAT chunks	E1d1	[Jurčacko(2024)]
MiniDuke	Image (JPG)		Prepends JPG header	E1d1	[Faou et al.(2019)]
MoneroMiner	Audio (WAV)		LSB	E1.3d1	[Soni et al.(2019)]
MonPass	Image (BMP)		Starting with the 3rd byte in image data each 4th byte is used to store xor encrypted payload	E1d1	[Camastra(2021)]
Montythree	Image (BMP)	x	LSB + XOR Operations on extracted Covert Information	E1.3d1/E1d1	[Legezo(2020)]
ObliqueRAT	Image (BMP)		Unknown	Unknown	[Malhotra(2021)]
PolyglotDuke	Image (JPG, PNG)	x	Append to end of image file	E1.1d1	[Faou et al.(2019)]
PNGLoader	Image (PNG)		LSB	E1.3d1	[Toulas(2022b)]
PowLoad	Image (PNG)		LSB (Invoke-PSImage)	E1.3d1	[Remillano II and Obuchi(2019)]
RDAT	Image (BMP)		LSB	E1.3d1	[Falcone(2020a)]
RegDuke	Image (PNG)	x	LSB	E1.3d1	[Faou et al.(2019)]
rhadamanthys	Image (JPG) Audio (WAV)		The data is stored after the actual content of the JPG or WAV file, in encrypted form	E1.1d1	[hasherezade(2023)]
Remcos	Image (PNG)	x	LSB	E1.3d1	[Széles(2021)]
ScarCruft	Image (JPG, PNG)		Image file with appended encrypted malicious payload	E1.1d1	[GReAT(2019)]
Serpent	Image (JPG)		Base64 encoded payload append to end of image file	E1.1d1	[VirusShare(2022)]
SlothfulMedia	Image (PNG)		LSB (Invoke-PSImage)	E1.3d1	[Kwiatkowski et al.(2020)]
stegmap	Image (BMP)	x	Unknown	Unknown	[online(2022)][Team(2022b)]
urlzone	Image (PNG)	x	LSB	E1.3d1	[Team(2019a)]
Ursnif	Image (PNG)		LSB (Invoke-PSImage)	E1.3d1	[Dahan(0)]
USBFerry	Image (JPG)		Unknown	Unknown	[Chen(2020a)][Chen(2020b)]
VinSelf	Image (BMP)		LSB	E1.3d1	[Airbus(2022)]
Webbfuscator	Image (JPG)		Embedded certificate with payload	E1d1	[Toulas(2022a)]

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

Media Stegomalware (36 Cases)

Key Findings:

- Almost exclusively image steganography (mostly JPEG, PNG, BMP, few GIF cases)
- 2 cases of audio steganography (2x WAV: appending to end of file / apply LSB stego)
- 0 cases of video Steganography
- Patterns: exclusively forms of **value modulation**:
  - 14x E1.3 (modulation of LSB)
  - 11x E1 (generic value modulation (e.g., appending to end of file / storing data in every *n*th byte etc.))
  - 7x E1.1 (modulation of a reserved/unused value); partially unknown patterns as reports lack detail
  - 5 reports lack details – no pattern was assigned

Network Stegomalware (61 Cases)

malware	protocol	os[a]	tp[b]	technique	pattern	sources
AdvOR	TOR	x		Hides destination and tunnels payload through TOR network	Unknown	[Team(2023)]
AnchorDNS	DNS			DNS A queries with XOR-encoded data in subdomain part	E1.1n1	[division of NTT Ltd.(2020)]
Bondupdater	DNS			DNS A and TXT queries, IP addresses and a custom protocol is used to encode commands	E1.1n1	[Falcone(2018)]
bvp47	PF[c]			Hides Payload in SYN-Packets with specific marker on the infected system via BPF rules	E1.1n1	[Lab(2022)]
Cashy200	DNS			DNS A queries with custom subdomain part, C2 commands hidden in IP addresses	E1.1n1	[Barbehenn(2019b)]
ChaChi	DNS HTTP			encrypted DNS TXT queries, HTTP POST Requests as fallback, base64 and XORed data.	E1.1n1	[Team(2021b)]
Chisel	HTTP	x		TCP/UDP connections encrypted via SSH transported over HTTP, exact method unclear	E1n1	[Pillora(2023)]
ChunkyTuna	HTTP	x		TCP streams over HTTP, exact method unclear	E1n1	[CISA(2020)]
Cloud Snooper	PF[c]			AWS EC2 Firewall bypass via Netfilter Hook	E1.1n1	[Shevchenko(2020)]
Cloudflare Tunnel	TCP		x	APT uses Cloudflare Tunnel Software to hide C2 infrastructure and payload	E1.1n1	[Jaramillo(2023)]
Cobalt Strike	HTTP		x	Directs communication to legitimate CDN's and mimics javascript file download	E1n1	[Wahlén(2021)]
dnscat2	DNS	x		TXT-, MX-, CNAME-, A , and AAAA queries used with encrypted payload	E1.1n1	[Bowes(2023)][Kennedy and Team(2022)]
DnsDig	DNS			DNS TXT queries, base64 for exfiltration, plaintext in C2-TXT-Payload	E1.1n1	[Shivtarkar and Kumar(2022)]
FatDuke	HTTP			mimics legit web applications in GET request URL; transmits data using unsuspicious query	E1.1n1	[Faou et al.(2019)]
FlewAvenue	PF[c]			Custom TCP/IP-Stack with packet redirection	Unknown	[F-Secure(2019)]
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	[Segura and Govers(2022)]
ForeLord	DNS			payload in TXT query subdomains; C2-reply contains obfuscated PS-Script in TXT-Record	E1.1n1	[Team(2020)]
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	[Cooke et al.(2021)]
gost	HTTP TCP UDP	x		This tool offers various information hiding possibilities	various	[ginuerzh(2023)][Zhdanov(2022)]
heyoka (modified)	DNS	x		modified open source tool that uses TXT queries	E1.1n1	[icesurfer and nico(2023)][Chen(2022)]
IDShell	DNS			TXT queries with encrypted payload	E1.1n1	[Chen(2020a)]
Invisimole	DNS			NULL- and AAAA queries with modified base32 encoding	E1.1n1	[Hromcová and Cherepanov(2020)]
Karkoff	HTTP			Base64 and XOR encoded JSON-Payload in HTTP Body	E1n1	[Mercer and Rascagneres(2019)]
LCPDot	HTTP			"Cookie" HTTP Header for C2 Communication	E1.1n1	[Tomonaga(2021)]
lightneuron	SMTP			Malicious Transport Agent scans and modifies E-Mails	E1.1n1	[Faou(2019)]
Ligolo-ng	TCP	x		advanced TLS encrypted TCP tunnel used by APTs	Unknown	[Chatelain(2023)][Deyalsingh et al.(2023)]
LunarWeb	HTTP			impersonates legitimate-looking traffic, spoofing HTTP headers	E1.1n1	[Jurčacko(2024)]
LunarMail	MAPI			sends emails via outlook	E1.1n1	[Jurčacko(2024)]
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	[Kayal et al.(2021)]
Magnat	SSH			forwarding the RDP port through an SSH tunnel	E1n1	[Pereira(2021)]
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	[Rapid7(2023)][Boutin(2019)]
mori	DNS			no specific information found	Unknown	[Nair(2022)]
NightClub	SMTP IMAP DNS			data as attached file; latest version uses TXT queries for the C2 communication	E1.1n1	[Faou(2023)]
neo-reGeorg	HTTP	x		highly customizable HTTP tunnel, payload in header fields or other parts of the HTML file	E1.1n1	[L(2023)][ESC(2023)]
ngrok	HTTP TCP	x	x	TLS encrypted TCP and HTTP tunnel used by APTs	E1n1	[ngrok(2023)][Zhdanov(2022)]
Pingback	ICMP			Payload in data field of ICMP echo and echo reply packets	E1.1n1	[Macrohon and Mendrez(2021)]
PoisonFrog	DNS			exfiltrates Data in subdomains of A queries, response encoded in IP addresses	E1.1n1	[Lepore(2019)]
Polonium	SSH	x		uses plink to spawn a SSH Tunnel	E1.1n1	[Porolli(2022)]
PolyglotDuke	HTTP			Query parameters w/ random names from hardcoded list; data is transferred in the values	E1.1n1	[Tiepolo(2023)]
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	[Falcone(2020a)]
Revsocks	TCP DNS	x		TLS encrypted TCP Socks Proxy with DNS Tunnel capabilities using TXT queries	E1.1n1	[Deyalsingh et al.(2023)]
RogueRobin	DNS			DNS A , AAAA , TXT, CNAME, MX, SOA and SRV queries, rotating between them in a round-robin fashion	E1.1n1	[Lepore(2020)]
RoyalDNS	DNS			DNS TXT queries for C2 communication	E1.1n1	[Hromcová(2019)]
saitama	DNS			DNS A queries and custom base36 encoding which is scrambled each request	E1.1n1	[Stockley(2022)]
ScrableCross	HTTP TCP		x	ChaCha20 encrypted custom message structure send via HTTP or DNS	E1n1/E1.1n1	[Hiroaki and Lee(2021)]
SecShow	DNS			utilizes DNS tunneling to scan network infrastructure and gather real-time data	E1.1n1	[Toulas(2024)]
SideTwist	DNS		x	DNS queries in Word Macros to inform C&C of infection	E1.1n1	[Company(2021)]
Sliver	DNS			Base58/32 encoded subdomain part in DNS queries	E1.1n1	[Breen(2023)]
Small Sieve	HTTP		x	Telegram-Bot API Commands over HTTPS	E1n1	[Centre(2022)]
SmileSvr	ICMP			XOR encrypted data in ICMP echo packets	E1.1n1	[Dai et al.(2021)]
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	[Forry(2023)]
Snugy	DNS			DNS A queries with only one byte capacity to exfiltrate data	E1.1n1	[Falcone(2020b)]
SombRAT	DNS TCP			compressed and AES encrypted DNS A and TXT queries, can switch communication to TCP if needed/requested	Unknown	[Team(2021c)]
Sunburst	OIP			mimicking normal activity as a part of Orion Improvement Program protocol	E1n1	[Datta(2022)][Eckels et al.(2021)]
Symbiote	PF[c] DNS			A queries for the credential exifltration and TXT queries for remote command execution, content is encrypted with RC4	E1.1n1	[Kennedy and Team(2022)]
SysUpdate	DNS			TXT queries are used and the data is encrypted with a hardcoded AES key	E1.1n1	[Lunghi(2023)]
TrkCdn	DNS			E-Mail with content that triggers DNS queries to attack controlled domains	E1.1n1	[Toulas(2024)]
TunnelSpecter	DNS			data encryption and exfiltration over DNS tunneling	E1.1n1	[Rochberger and Frank(2024)]
Webbfuscator	DNS			DNS TXT queries with base64 encoded data	E1.1n1	[Toulas(2022a)]
Wellmess	DNS			DNS A and TXT queries to send and receive base32 encoded data	E1.1n1	[PricewaterhouseCoopers(2020)]
Winnti	DNS		x	DNS NULL- and TXT queries for C2 Server Communication	E1.1n1	[Ebel(2020)]

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

Network Stegomalware (61 Cases)

Key Findings:

- Ca. 79% of all cases use DNS (29 cases), HTTP (14 cases) or both (5 cases).
  - Other protocols are used rarely (e.g., TCP, SMTP, SSH, ICMP, UDP, IMAP, TOR, SOCKS).
- Malware *takes advantage of open source tools*!
  - At least 12 out of 61 cases.
- Patterns: exclusively forms of **value modulation**:
  - 46x E1.1 (modulation of a reserved/unused value)
  - 12x E1 (generic value modulation)
  - 5 reports lack details – no pattern was assigned

Text Stegomalware (20 Cases)

malware	platform	tp[a]	technique	pattern	sources
Astaroth	Youtube	x	posts C2 Server addresses encrypted in Youtube and Facebook Profile descriptions	E1t1	[Brumaghin(2020)][Center(2019)]
Beatdrop	Trello Notion	x	stores victim-info as trello card / downloads payload as attachment	E1t1	[Wolfram et al.(2022)]
ComRATV4	GMail	x	uses e-mail attachements to send encrypted commands and to receive output	E1t1	[Faou(2020)][Lakshmanan(2020)]
DNSpionage	-		hides data in the comments in the HTML code	E1t1	[Mercer and Rascagneres(2019)]
Drokbk	GitHub	x	Uses Readme.md to store URL in plaintext for C2	E1t1	[Team(2022a)]
EasternRoppels	-		hides key in HTML attribute positioning and payload in whitespaces	E2.2t1/E2.1t1	[Dolgushev et al.(2019)]
EnvyScout	Slack	x	creates slack-channel per victim and uses it for communication	E1t1	[Tiepolo(2023)]
FatDuke	-		download id for payload is hidden in img-tag	E1t1	[Faou et al.(2019)]
FunnyDream	-		uses HTTP, xoring/zipping payload in body, infos stored in URL Path	E1t1	[Vrabie(2020)]
GraphicalNeutrino	Notion	x	uses notions API + Database Feature to store victim information and to download payloads	E1t1	[Future(2023)]
Hammertoss	Social Media	x	uses unsuspicious Link posted on twitter to embbed c2 url + offset + key	E1t1	[Tiepolo(2023)]
Ketrican	-		base64 encoded commands between keywords in HTML	E1t1	[BfV(2020)]
lemon_duck	-		renamed bash script (to .png)	E1t1	[Ahuje(2022)]
MiniDuke	X	x	encrypted C2-URL via Twitter Post	E1t1	[Faou et al.(2019)]
njRAT	pastebin	x	Link between marks	E1t1	[Zhang et al.(2020)]
Panda	GitHub	x	Uses GitHub API domains for commands and data extraction	E1t1	[Overwatch Team(2020)]
PolyglotDuke	X Imgur Reddit	x	consumes Japanese, Chinese or Cherokee strings that encode the malware's C&C server	E1t1	[Holt(2020)]
TangleBot	Telegram	x	base64 encoded messages as telegram preview message	E1t1	[Naves et al.(2021)]
TriFive	E-Mail Drafts		base64 encoded and encrypted message-bodies in E-Mail drafts	E1t1	[Barbehenn(2019a)][Falcone(2020b)]
VaporRage	Notion	x	notions API + Database Feature to store victim information and to download payloads	E1t1	[Tiepolo(2023)]

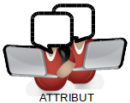
[a] tp: trusted platform

Text Stegomalware (20 Cases)

Key Findings:

- Using different public web platforms, such as Youtube, GMail, GitHub, Slack, X, pastebin etc.; posting comments or video descriptions. Mostly HTML content.
- Patterns (almost exclusively value modulation; only domain with E2 patterns):
  - 19x E1 (generic value modulation)
  - 1x E2.2 (element enumeration), jointly with 1x E2.2 (element positioning)

Next Steps: ATTRIBUT project



ATTRIBUT:
Attribution of covert (information) channels in critical infrastructures and potentials for prevention and response (ATTRIBUT)

- Findings will be fed into the ATTRIBUT project. Focus: attribution of attackers on the basis of stegangoraphy artifacts.

Funded by the Agentur für Innovation in der Cybersicherheit GmbH: Forschung zu "Existenzbedrohenden Risiken aus dem Cyber- und Informationsraum – Hochsicherheit in sicherheitskritischen und verteidigungsrelevanten Szenarien" (HSK) – `https://www.cyberagentur.de/tag/hsk/`. Project website: `https://omen.cs.uni-magdeburg.de/itiamsl/english/projects/attribut.html`.

Conclusions

- Conducted the most comprehensive and most up-to-date survey of stegomalware (106 cases).
- Found that most *known* stegomalware uses network steganography methods (57.5%), followed by digital media steganography methods.
- Of the digital media steganography methods, image steganography was used almost exclusively (73% JPG or PNG).
  - Only two cases for audio steganography methods (both WAV)
  - Zero cases for video-based steganography methods.
- Stegomalware employs open source tools (at least for network steganography)
- Only few patterns were used, i.e., almost exclusively three forms of value modulation (LSB, generic, random/unused field).

Thank You!

Also, have a look at our stego taxonomy! :)

`https://doi.org/10.36227/techrxiv.20215373.v2`

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

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

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

Robert Falcone Barbehenn, Brittany. 2019b.
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/

BfV. 2020.
BfV Cyber-Brief Nr. 01/2020.
Technical Report. Bundesamt für Verfassungsschutz.

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/

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

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/

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

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

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

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

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

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

National Cyber Security Centre. 2022.
Small Sieve Malware Analysis Report.
Technical Report. NCSC.

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

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

Joey Chen. 2020b.
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

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-y

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.

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

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

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/

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

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

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

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

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

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

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

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

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/

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

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/

Robert Falcone. 2020a.
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/

Robert Falcone. 2020b.
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/

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

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/

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/

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

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/

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.

Fraunhofer FKIE. 2023.
Malpedia (Fraunhofer FKIE).
Fraunhofer FKIE.
https://malpedia.caad.fkie.fraunhofer.de/

Recorded Future. 2023.
BlueBravo Uses Ambassador Lure to Deploy GraphicalNeutrino Malware.

ginuerzh. 2023.
GO Simple Tunnel.
https://github.com/ginuerzh/gost

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

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

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/

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/

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

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/

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

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

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

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

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/

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/

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

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/

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

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

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/

L. 2023.
Neo-reGeorg.
https://github.com/L-codes/Neo-reGeorg

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

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

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

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

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

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

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/

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

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

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

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

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

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

ngrok. 2023.
Ngrok — Unified Application Delivery Platform for Developers.
ngrok, Inc.
https://ngrok.com/

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

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

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

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/

Jaime Pillora. 2023.
Chisel.
https://github.com/jpillora/chisel

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

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

Rapid7. 2023.
Metasploit — Penetration Testing Software, Pen Testing Security.
Metasploit.
https://www.metasploit.com/

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

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/

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/

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

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

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

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

János Gergő 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

tccontre. 2021.
Iceid_png_shellcode_extractor.Py.
https://github.com/tccontre/KnowledgeBase/tree/main/malware_re_tools/iceid_stego_shell_decryptor

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

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

Proofpoint Threat Insight Team. 2019a.
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

SonicWall Capture Labs Threat Research Team. 2019b.
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/

Splunk Threat Research Team. 2021a.
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

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

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

Threat Hunter Team. 2022b.
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

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/

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

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

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

Bill Toulas. 2022b.
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/

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/

VirusShare. 2022.
Serpent Dropper — VirusShare.Com.
Corvus Forensics.
https://virusshare.com/file?f6d2becc3531e98e7c6331d3e5b269a54a83c1af8f9605d6daea6531a6d72b99

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

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

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

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.

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

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/

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