CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

August 16, 2023

Threat Actors Leverage Internet Services to Enhance Data Theft and Weaken Security Defenses

Executive Summary

Threat actors are increasingly abusing trusted platforms like Google Drive, OneDrive, Notion, and GitHub as part of their infrastructure, blurring their malicious activities within ordinary traffic. This approach not only improves their efficiency in data theft and operations but significantly weakens traditional defenses. The rate of adoption for this method of "living off trusted sites" is expected to rise, with advanced persistent threat (APT) groups often spearheading innovation and less sophisticated groups swiftly following suit. This trend underscores the need for a dynamic defense strategy that evolves in sync with threat actor innovations.

In the short term, defenders should flag or block legitimate internet services (LIS) that are not used within their environment and are known to be used maliciously. In the long term, organizations need to invest resources into understanding how employees legitimately use certain services, and how they are used for malicious purposes. This will enable the development of effective, more nuanced detection mechanisms and bolster the overall protection of organizations. At the same time, advanced technologies such as TLS network interception are gaining relevance; such technologies offer enhanced visibility flexibility to organizations but also bring new privacy and compliance implications.

As threat actors continue to adapt methods of LIS abuse for their infrastructure, the efficacy of existing defenses such as traditional IOC blocking and basic detections will decline at an accelerated rate. In addition to behavioral analytics, defenders will need to prioritize orchestrating the "triangle of detections" consisting of network-, file-, and log-based approaches. This multi-pronged approach allows for the detection of malicious activity from one angle, even when there are visibility gaps from the other two. Defenders will also need to proactively identify legitimate internet services that could potentially be abused for malicious purposes and test their environments through attack simulations to stay one step ahead of threat actors.

Key Findings

- We examined more than 400 malware families for this report and found that 25% of them abused LIS in some way as part of their infrastructure. Out of the malware families that abused LIS, 68.5% abused more than 1 LIS for either the same or distinct infrastructure purposes.
- 37% of infostealers abuse LIS, making them the most inclined to abuse such services across all malware categories. Likely reasons for this inclination are their primary objective to exfiltrate data — meaning reduced infrastructure requirements — combined with the importance of easy infrastructure setup for operators who lack technical expertise.
- There are 4 distinct infrastructure schemes; which scheme is chosen depends heavily on the malware category. For instance, among infostealers that abuse LIS, the majority (72%) utilize them for data exfiltration. On the other hand, most loaders (71%) abuse LIS for payload delivery.
- Among all LIS categories, cloud storage platforms such as Google Drive are the most commonly abused — our data set identified 43 malware families abusing such platforms. Messaging

applications follow closely with 30 malware families, followed by email services with 14, and social media with 13.
- Telegram is the most prevalent messaging LIS abused by malware, representing 66.7% of the instances, followed by Discord at 27.8%. Infostealers are primarily associated with most instances involving Telegram (87.5%) and Discord (80%).
- The lack of comparable reporting makes it challenging to quantify a definitive trend, but we will likely see an increase in LIS abuse for adversary infrastructure given the gradual adoption of LIS abuse methods and infrastructure by well-established malware families, the prevalence of LIS abuse activity among more recent malware strains, and the rapid pace of innovation in abusing LIS by APT groups.

Background

It is not uncommon for malware and threat actors to use legitimate internet services (LIS) such as Telegram, GitHub, or OneDrive for their command-and-control (C2) infrastructure in 2023. This is not only a way to counter the persistent takedown and seizure of C2 domains and servers but also an attempt to blend in with normal traffic; while C2 communications to these LIS may not be advanced, they add a layer of complexity for security defenders who may mistakenly designate abuse of LIS as benign. Defenders now not only have to stay on top of malicious infrastructure but also need to assume that LIS are regularly being abused in attacks against them. One reason for the growing adoption of LIS for C2 communications by both cybercriminals (such as Vidar's usage of Telegram) and advanced persistent threat (APT) groups (such as BlueBravo using Notion) — a technique also referred to as "living off trusted sites" (LOTS) — is the improved ability of organizations and tooling to identify anomalies in network traffic using obscure / custom protocols, non-standard ports, or known malicious or suspicious IP addresses and domains. These are all detection indicators for C2 communications used by network defenders, and threat actors can potentially avoid detection by using popular LIS.

Using LIS for C2 doesn't just allow threat actors to evade detection in victim networks by blending in with benign network traffic. Other benefits include:

- Reduced operational overhead by simplifying the overall C2 server installation process through serverless architectures or piggybacking on publicly endorsed TLS encryption
- Lower infrastructure costs by saving on typical hosting or registration fees
- Better operational security by reducing error proneness, quickly taking down LIS pages after operations, and eliminating the need to register domains and certificates and wait for DNS changes to take place
- High uptime with LIS designed to be highly available, with redundant servers and failover mechanisms
- Minimal vetting to register new accounts on LIS, and limited detection possibilities for service providers (especially with regard to human-controlled accounts)
- Limited availability of tooling for threat modeling when it comes to serverless C2 threats and other innovative threats, and little actionable threat intelligence specific to such infrastructure setups

The advantages LIS gives threat actors can create challenges for defenders:

- Due to limited web access controls in most organizations and their acceptance of communications to many of the LIS abused for C2, blocking communications from adversaries can be difficult.
- Despite the availability of numerous tools designed to assist organizations in handling TLS from a detection perspective (such as web proxies for TLS inspection), the widespread adoption of ubiquitous encryption on LIS creates additional challenges in detection (finding second-stage C2 addresses, for example) and necessitates a reevaluation of visibility strategies.
- Threat feeds are currently unable to mitigate the risks posed by LIS given the presence of false positives and the potential harm caused by mistakenly including a legitimate and widely used service on the list.
- With threat actors leaving behind less distinctive network traffic traces, the work of tracking, clustering, and eventually attributing threat activity is further complicated by the lack of pivoting points (as self-signed certificates or domain registrations as common means to track infrastructure become less prevalent). As a result, organizations become more reliant on malware samples and host artifacts.

Threat actors do face some obstacles when attempting to abuse LIS, however, such as the limitations imposed by the functionality and restrictions of the abused services, the ease with which these services can be blocked within the victim network, and the existence of dedicated teams within LIS specifically tasked with detecting and countering system abuse.

While the evolution of C2 techniques is carefully studied by security researchers, there has been no systematic overview of how LIS are leveraged for malicious purposes (both in qualitative and quantitative terms). This report provides an overview of the current state of LIS abuse methods and builds upon the analysis of the classic C2 setups that were the focus of our adversary infrastructure report. This report first provides a high-level conceptual analysis of how LIS are used in adversary infrastructure schemes. It then examines trends and themes based on Recorded Future Triage sandbox submissions and concludes with mitigation and detection strategies and our assessment of how LIS abuse trends and schemes are likely to evolve going forward.

Threat Analysis

Types of LIS Infrastructure Schemes

The ways in which attackers can abuse LIS can be conceptually divided into 4 main categories. These categories or infrastructure schemes are not mutually exclusive, meaning they overlap in functionality and may be used in combination.

Full C2

Full C2 using LIS refers to a scenario in which the attacker and the malware do not directly communicate with each other. Instead, they rely on an intermediary proxy or "abstraction layer", such as services like GitHub or Mastodon, to exchange communications. Any service with a publicly accessible API (application programming interface) that can be used for programmatically reading and writing data can theoretically serve as such an abstraction layer.

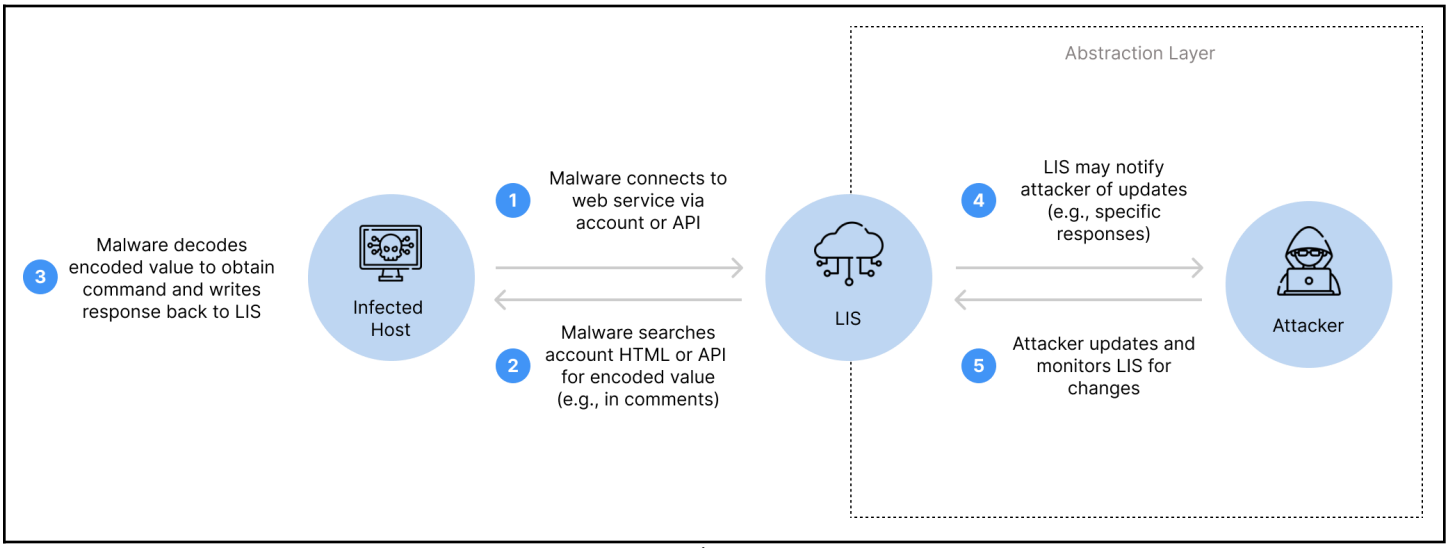

Figure 1: *Overview of a full C2 infrastructure setup using LIS (Source: Recorded Future)*

Dead Drop Resolving

Dead drop resolving (DDR) refers to a technique in which a malware is set up to retrieve its actual C2 server from a web service. The term DDR draws inspiration from traditional intelligence techniques, referring to a situation in which an agent covertly leaves valuable information in an inconspicuous location, referred to as a "dead drop". Although there are instances where the IP addresses or domains of C2 servers are listed in plain text (as in the case of Vidar C2 servers being added to Mastodon profiles), in many cases, threat actors employ encryption and encoding techniques to render detection more challenging (as when Astaroth hides encoded C2 information in YouTube comments) or opt for steganography-based approaches. In contrast to full C2 setups, in DDR the malware establishes direct communication with the C2 server after retrieving the address from the web service. In principle, any

web service allowing for data reading can be used for DDR; some common examples are YouTube and Steam Community, where the accounts can be created by the threat actor or stolen.

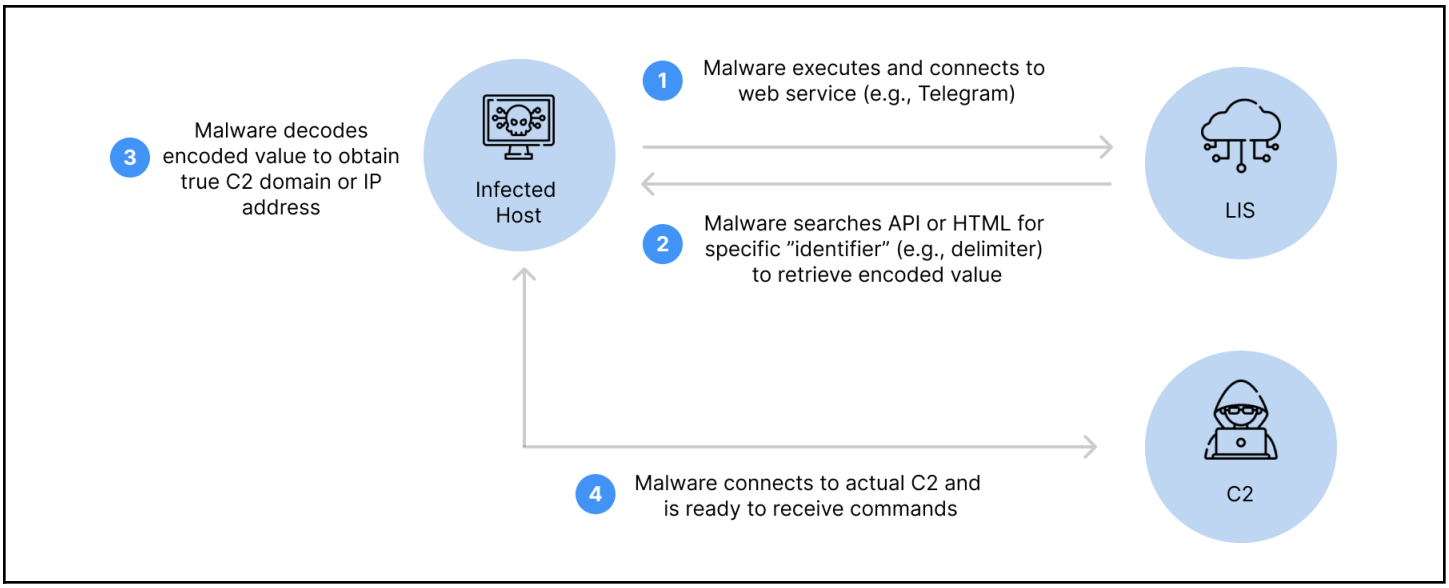

Figure 2: *Overview of DDR infrastructure setup (Source: Recorded Future)*

Payload Delivery

LIS are often abused by threat actors as a means to deliver payloads. These services provide a platform where users can share and store information (such as text-based information and binaries), making them attractive for abuse due to their accessibility and wide usage. As with DDR, in principle, any web service allowing for data reading can be used for payload delivery. Common examples include cloud storage services such as Pastebin (as in the case of Agent Tesla's loader fetching base64-encoded, obfuscated code in a multi-stage procedure), Google Drive (Guloader, for example, typically stores encrypted payload on Google Drive), and Discord (as seen, for example, in Sandworm using Discord to load the WhisperGate wiper).

Exfiltration

LIS are also abused for exfiltration. In principle, any web service allowing for data writing or sending can be used for the purpose of exfiltration. This includes services such as publicly accessible APIs (as when Snake Keylogger exfiltrates through the Telegram Bot API) or email services (as when Darkstealer exfiltrates over SMTP), among others. It is important to note that ransomware campaigns use legitimate cloud storage tools such as mega.io or MegaSync for exfiltration purposes as well, even though the malware itself may not directly exploit these tools.

A Note on Underlying Data and Bias

The data set used for the analysis in this report is predominantly based on malware families detected by Recorded Future Triage, supplemented with additional malware families detected and tracked by Recorded Future using other sources. Therefore, our data is biased toward "known threats" within these

collection systems and the specific malware families to which they belong. The categorization of malware families and the evaluation as to whether or not a malware family abuses LIS was conducted with a combination of manual and automated methods. Several malware categories such as ransomware and miners were excluded from the analysis, as they rarely have their own C2 servers and are frequently used in conjunction with other malware. It is important to acknowledge that the choice of infrastructure by a malware family can be influenced by several factors, including the specific campaign under observation and the operator behind it. **Table 1** shows the number of malware families associated with the 4 most common malware categories analyzed in this report.

Malware Category	Count	Example Malware Family
Infostealer	116	Vidar
RAT/Backdoor	106	AsyncRAT
Loaders/Droppers	50	ModiLoader
Mobile	36	Agent Smith

***Table 1**: Count of malware families for the top 4 malware categories in this report (Source: Recorded Future)*

For ease of discussion and better trend analysis, we defined 10 different LIS categories (see **Table 2**). The categorization was made based on the primary purpose of a particular application or service.

LIS Category	Example LIS
Cloud Storage Platform	OneDrive
Messaging	Discord
Email Services	Gmail SMTP
Social Media	Mastodon
Code Repositories	GitHub
Development Platforms	Firebase
Blockchain	Bitcoin blockchain data
Project Management	Notion
Serverless	AWS Lambda
Malware Repositories	VirusTotal

***Table 2**: LIS categories and examples (Source: Recorded Future)*

Infostealers Are the Most Common Malware Category Abusing LIS

Based on our data set from 2021 and 2022, 25% of the malware families observed made use of LIS in some way as part of their infrastructure (see **Figure 3**). When splitting the data by malware categories, infostealers stand out, with 37% of them abusing LIS. In comparison, mobile malware, RATs/backdoors, and loaders/droppers exhibit substantially lower percentages, with 17%, 15%, and 14% of them abusing LIS, respectively.

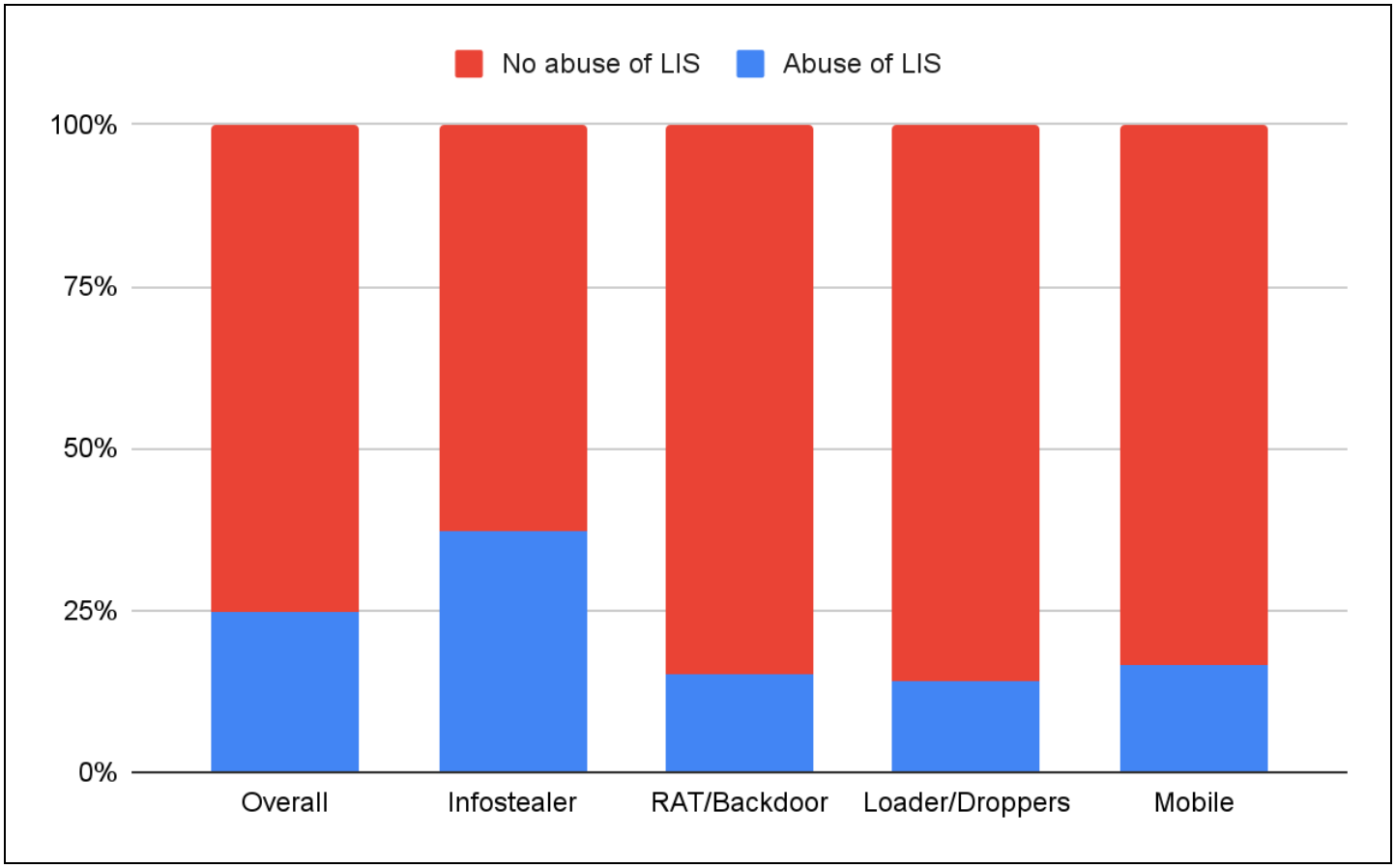

Figure 3: *Proportion of malware families abusing LIS by malware category (Source: Recorded Future)*

There are several possible reasons why infostealers are more inclined to abuse legitimate services than other malware categories. First of all, because infostealers are a key element within the constantly evolving cybercrime ecosystem, they often lead the way in terms of innovation. In addition, since their primary objective is data exfiltration rather than remote access trojan (RAT) functionality, infostealers often have lower infrastructure requirements, which can be easily achieved by leveraging publicly accessible APIs. Furthermore, many infostealers are sold on underground and dark web forums to operators who may lack technical expertise, making the ease of infrastructure setup an important selling point.

Out of the malware families that abuse legitimate services, 68.5% abused more than 1 LIS for either the same or different purposes (see **Figure 4**). For example, MoqHao has been observed obtaining C2 information using DDR in the form of user profiles on various LIS including Imgur, Baidu, VKontakte (VK), Rotten Tomatoes, Live Journal, and Pinterest. Similarly, Vidar has been using TikTok, Mastodon, Telegram, Tumblr, and Steam Community for DDR, and PrivateLoader has been observed using Pastebin for DDR and then Discord or VK for final payload delivery.

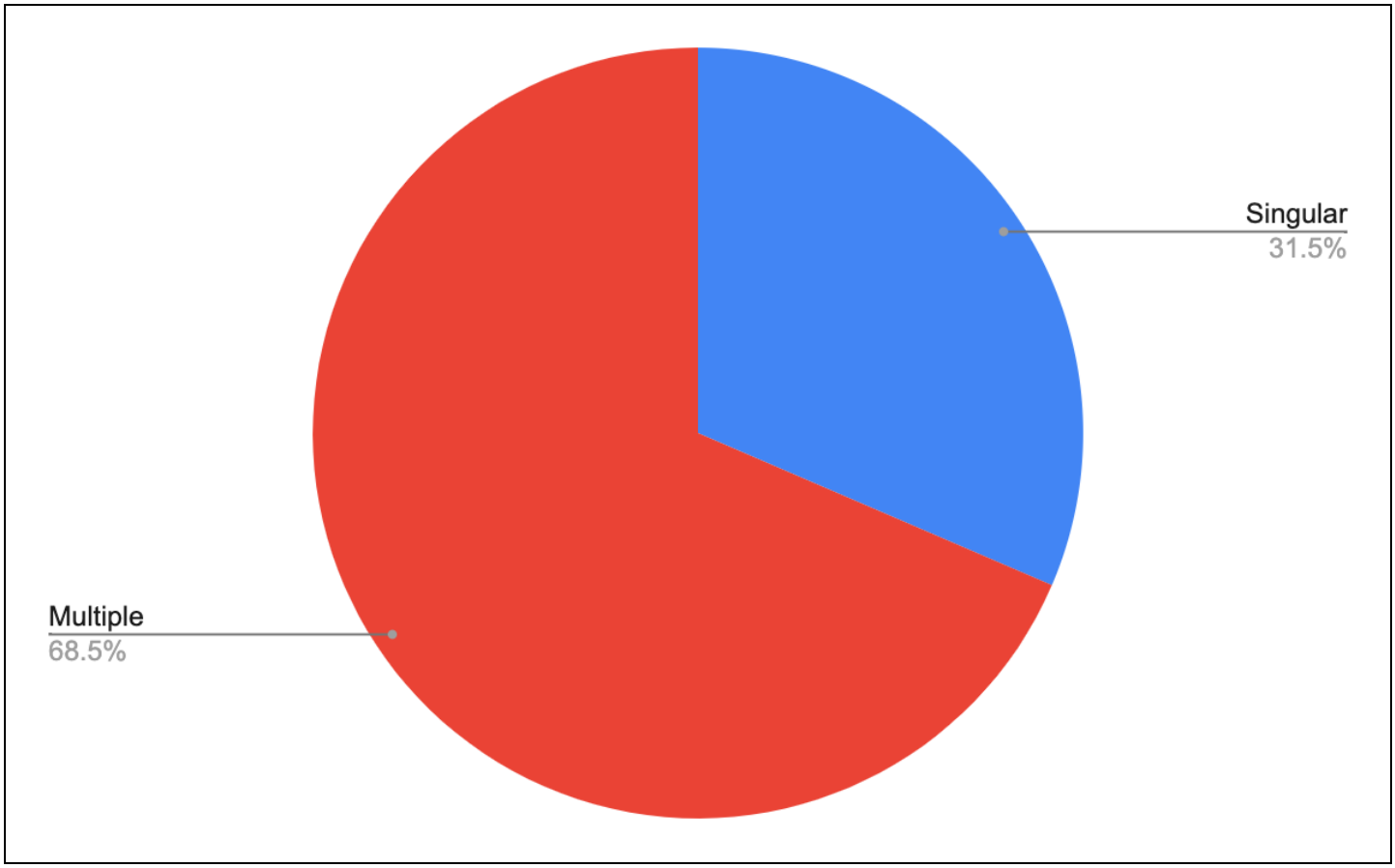

Figure 4: *Proportion of malware families abusing multiple LIS (Source: Recorded Future)*

LIS Abuse for Adversary Infrastructure Likely Increasing

While the absence of comparable reporting makes it difficult to quantify or even demonstrate a clear trend, it is likely that the abuse of LIS for adversary infrastructure is on the rise based on the following evidence:

- Research by Anomali from 2016 found that among the malware samples it examined, only 9% had the ability to abuse LIS for C2. It is important to note, however, that the statistics in Anomali's report are based on the number of individual malware samples, rather than on the number of malware families abusing LIS.

- Multiple long-existing malware families such as Agent Tesla have gradually incorporated support for abusing LIS over time, with Agent Tesla now almost exclusively using Discord, Telegram, and SMTP for exfiltration based on analyzed samples.
- Due to the convenience (and likely, stealth) in some environments, it has become extremely common for more recent commodity infostealer families (such as Icarus Stealer, DarkCloud, BlackGuard, or Blank Grabber) to include support for abusing LIS, instead of using only traditional C2 setups.
- The rapid pace of innovation observed among APT groups as they transition from one abused service to another — for example, BlueBravo moved from Notion to Microsoft OneDrive for C2, and had previously abused Trello, Firebase, and Dropbox — demonstrates a widespread interest in abusing LIS and serves as evidence of ongoing investments in this area.

Choice of Infrastructure Scheme Depends Heavily on Malware Category

According to our data set, 29% of the analyzed malware families that abuse LIS use them as part of a full C2 setup. However, a closer examination by malware category reveals significant variations. For example, only 9% of infostealers (such as Masad Stealer) utilize LIS for full C2 purposes, compared to 38% of backdoors and RATs (such as FireStarter and CloudMenis), as seen in **Figure 5**. This difference is likely linked to the characteristics of infostealers, which typically involve minimal post-infection interaction and focus primarily on the rapid collection and exfiltration of data. In contrast, backdoors and RATs are designed to remain persistent over time for continued, long-term access. The proportion of loaders and droppers as well as mobile malware using LIS for full C2 purposes is at 29% and 33%, respectively.

Overall, the abuse of LIS for exfiltration purposes stands out as the most prevalent infrastructure scheme, accounting for 47% across all malware families. When focusing solely on infostealers, the percentage rises even further to 72%, which aligns with their primary objective of data exfiltration. In addition, while in total only 24% of all malware families abuse LIS for DDR, 50% of mobile malware families were observed doing so (see **Figure 5**).

It is not entirely clear why mobile malware families are more likely to abuse LIS for DDR than other malware categories, but reasons may include that:

- The lack of pre-configured C2 data potentially allows for more lightweight malware that could be easier to install on a mobile device that may be of limited capacity
- The lack of a pre-configured C2, a potential detection point, may make mobile malware more likely to pass a review by the Google Play Store or the Apple App Store

Lastly, in terms of abusing LIS for payload delivery, loaders and droppers lead at 71% across all malware categories, which is unsurprising considering this usage aligns with their primary objective. In contrast, this behavior is observed in only 27% of all malware categories combined.

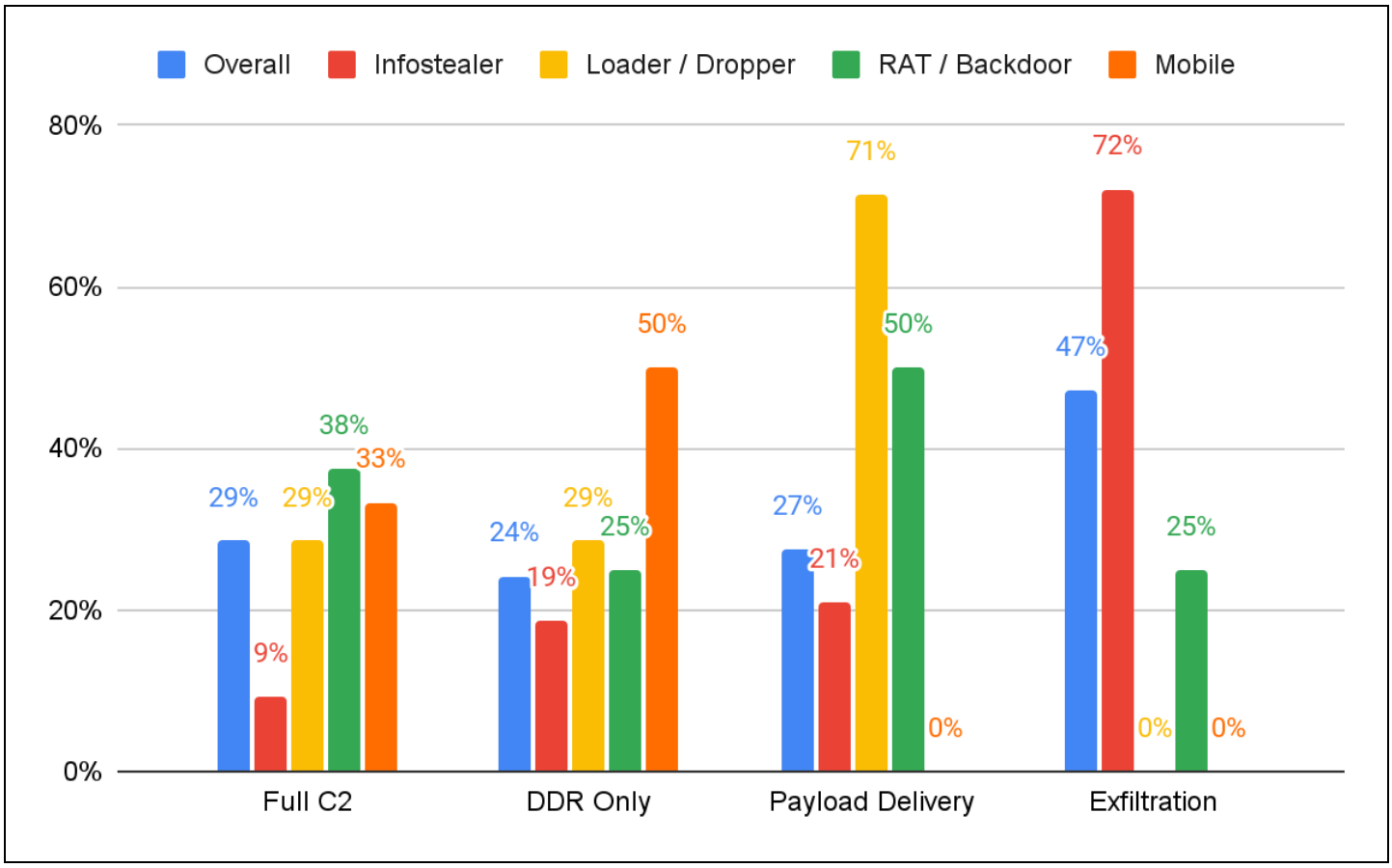

Figure 5: *Proportion of malware families abusing LIS by infrastructure scheme (Source: Recorded Future)*

Cloud Platforms Are the Most Frequently Abused LIS, with Pastebin on Top

Out of all LIS categories, cloud storage platforms (such as Google Drive) are the most frequently abused — 43 malware families abuse these platforms, based on our data set, followed by messaging applications (abused by 30 malware families), email services (14), and social media (13) (see **Figure 6**). The diversity of available services with cloud storage providers, the potential for blending in within corporate environments that utilize these services for legitimate purposes, and the ease of implementation likely serve as the driving factors behind the frequent abuse of cloud storage platforms. **Table 3** shows the most common infrastructure scheme per LIS category.

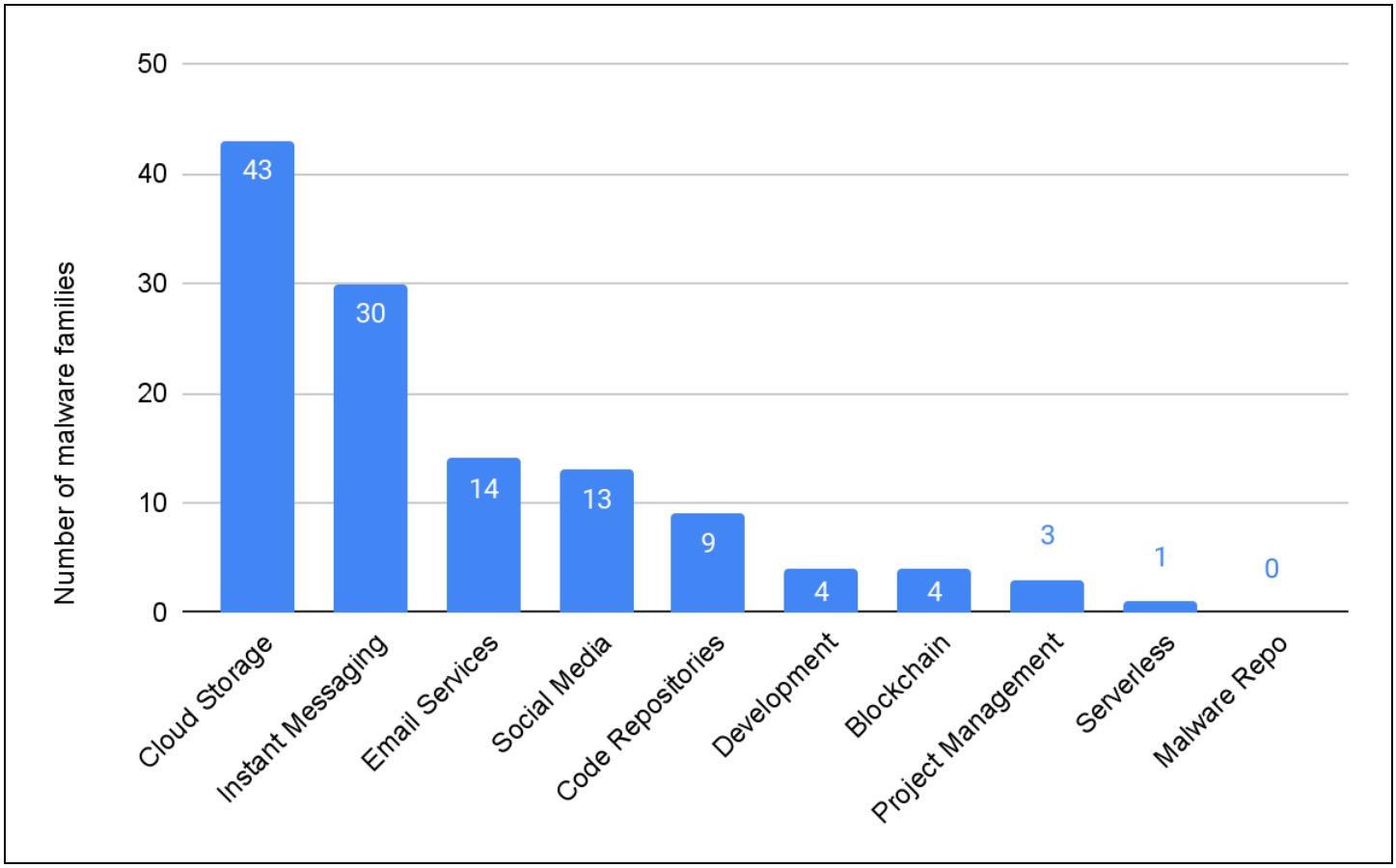

Figure 6: *Types of LIS abused by number of different malware families (Source: Recorded Future)*

LIS Category	Most Common Infrastructure Scheme
Cloud Storage	Payload Delivery
Messaging	Exfiltration
Email Services	Exfiltration
Social Media	DDR
Code Repositories	Payload Delivery
Development Platforms	Full C2
Blockchain	DDR
Project Management Platforms	Full C2
Serverless Architecture	Full C2 (note: only 1 instance)
Malware Repositories	N/A

Table 3: *Most common infrastructure scheme by LIS category (Source: Recorded Future)*

Upon closer examination of cloud storage platforms as the most frequently abused LIS category, it becomes evident that Pastebin is the predominant service abused, constituting 26.4% of the instances (see **Figure 7**). Half of these instances are associated with RATs and backdoors, and, in most cases, Pastebin is used for either DDR or payload delivery. Although paste[.]ee provides a similar service to Pastebin, it has been observed in significantly fewer cases. Pastebin is closely followed by Google Drive and Dropbox, accounting for 24.5% and 7.5% of instances, respectively. While Google Drive has been observed being used for full C2 (such as with GIMMICK) and payload delivery (such as with GuLoader), among others, Dropbox tends to be used for exfiltration (such as the DropBook backdoor by Molerats) but also for C2 communications and payload delivery (as with NOBELIUM/BlueBravo).

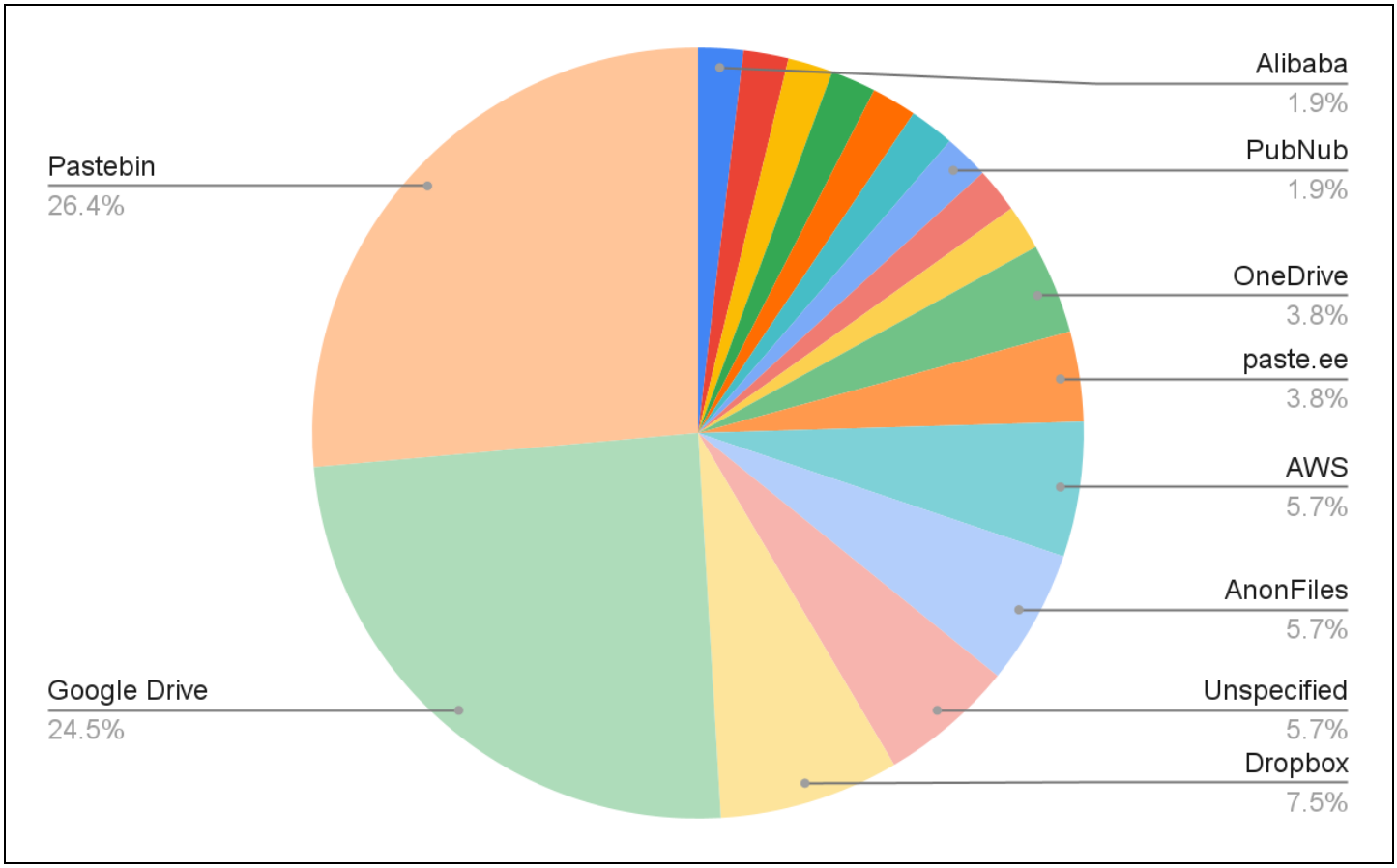

Figure 7: *Proportion of specific LIS abused for C2 among all cloud storage instances (Source: Recorded Future)*

Telegram Is the Most Commonly Abused Messaging Application

Similarly when conducting a detailed analysis of messaging applications, which is the second most commonly abused LIS category, it becomes evident that Telegram is by far the most common service, accounting for 66.7% of the instances, followed by Discord with 27.8% (see **Figure 8**). Both services are free, widely used in both victim environments and the cybercriminal underground, and thus hard to block, and their APIs are also user-friendly and straightforward to use. Firebase Cloud Messaging is an outlier with few observations (such as Donot's Firestarter), and Slack has only been observed being

used by tools created by security researchers (such as Slackor), based on our data set. However, other research has shown that Slack has also been abused by APT groups such as APT29.

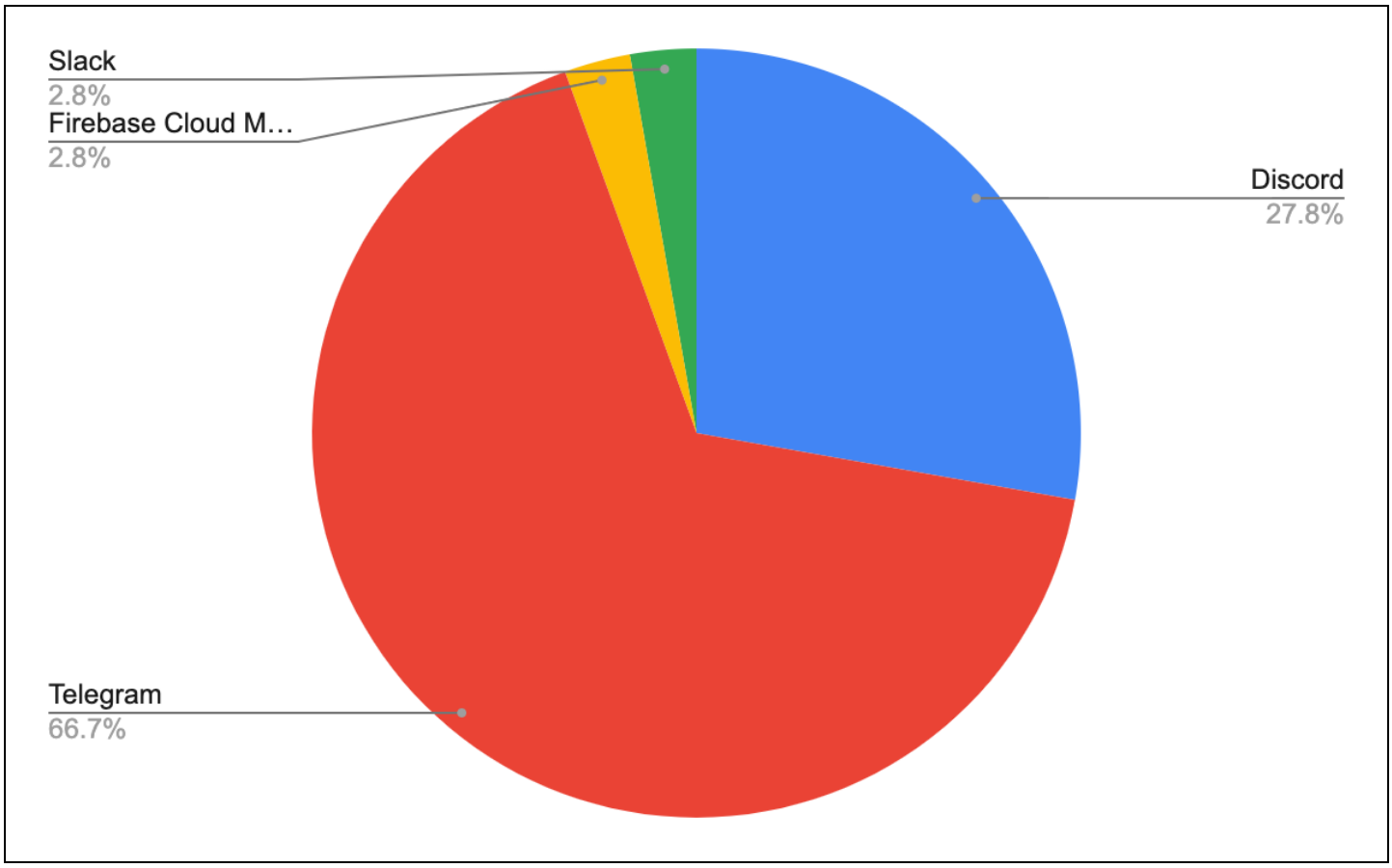

Figure 8: *Proportion of specific LIS abused for C2 among all messaging instances (Source: Recorded Future)*

Interestingly, the vast majority of cases involving Telegram (87.5%) and Discord (80%) are associated with infostealers (see **Figure 9**). Instances of non-infostealers leveraging Telegram or Discord for malicious purposes are rare — examples of this include PrivateLoader, which used Discord for final payload delivery until mid-2022, as well as the aforementioned use of Discord in the WhisperGate attacks against Ukraine. It is not clear why other malware categories are not equally abusing Telegram and Discord, but it is suspected that these services cater exceptionally well to the requirements of infostealers in providing simple exfiltration capabilities.

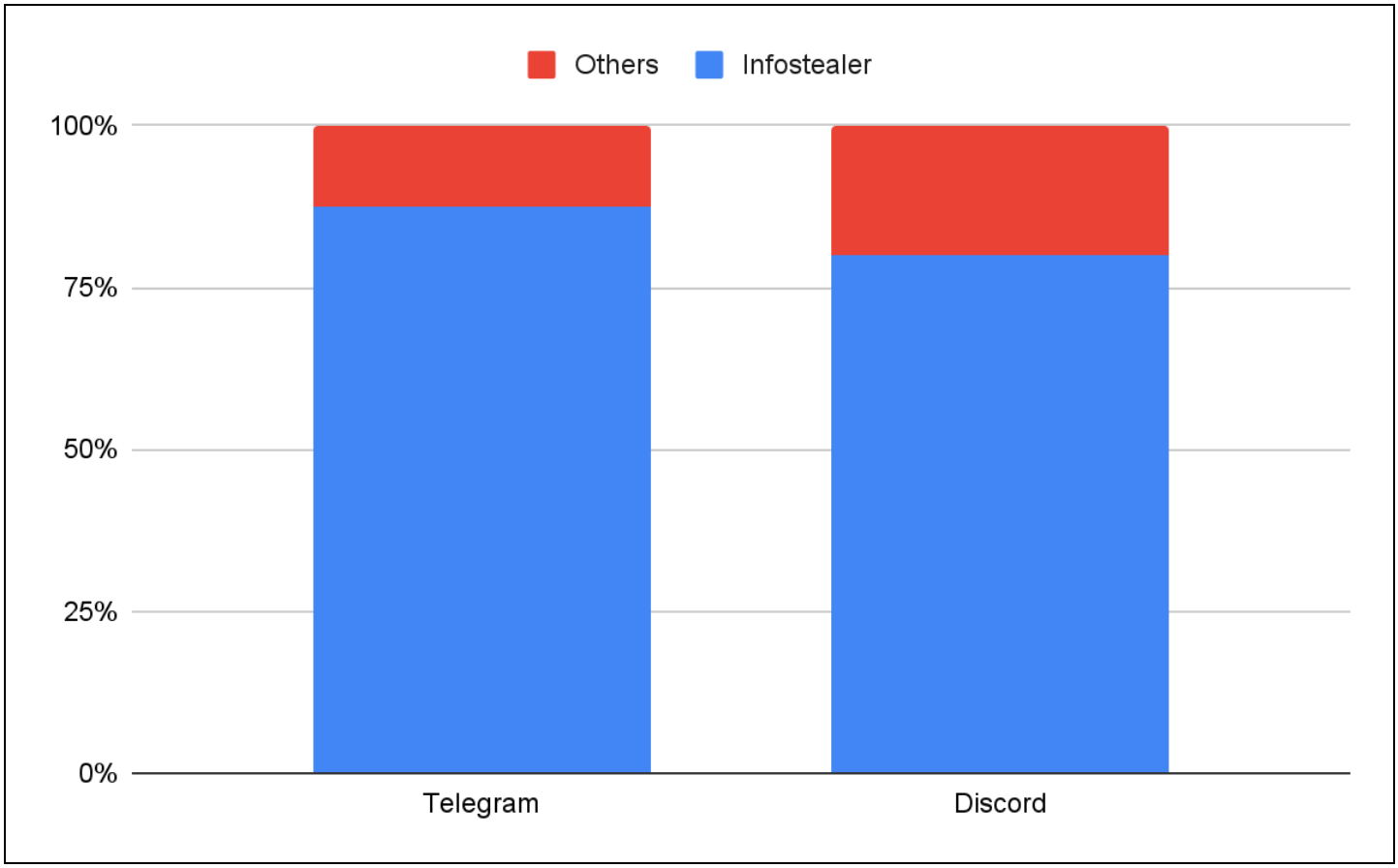

Figure 9: *Telegram and Discord abuse split by infostealers and other malware categories (Source: Recorded Future)*

A Diverse Range of Social Media Services Are Abused for C2

Among the various types of LIS susceptible to abuse, social media platforms are the fourth-most commonly targeted type. This type of LIS is highly diverse, with a total of 14 distinct, observed services. Steam Community and YouTube are the most common services, with both of them accounting for 14.3% of abuse instances (see **Figure 10**). In addition to its ease of use, one of the probable factors contributing to the widespread abuse of Steam Community is the lenient approach of its parent company, Valve, toward content takedowns. According to Emerging Threats, Steam Community was contacted regarding a C2 distribution method observed in relation to Vidar, but the platform determined that the importance of enabling its users to share information through their profiles outweighed the need to take any action against allegedly abusive accounts.

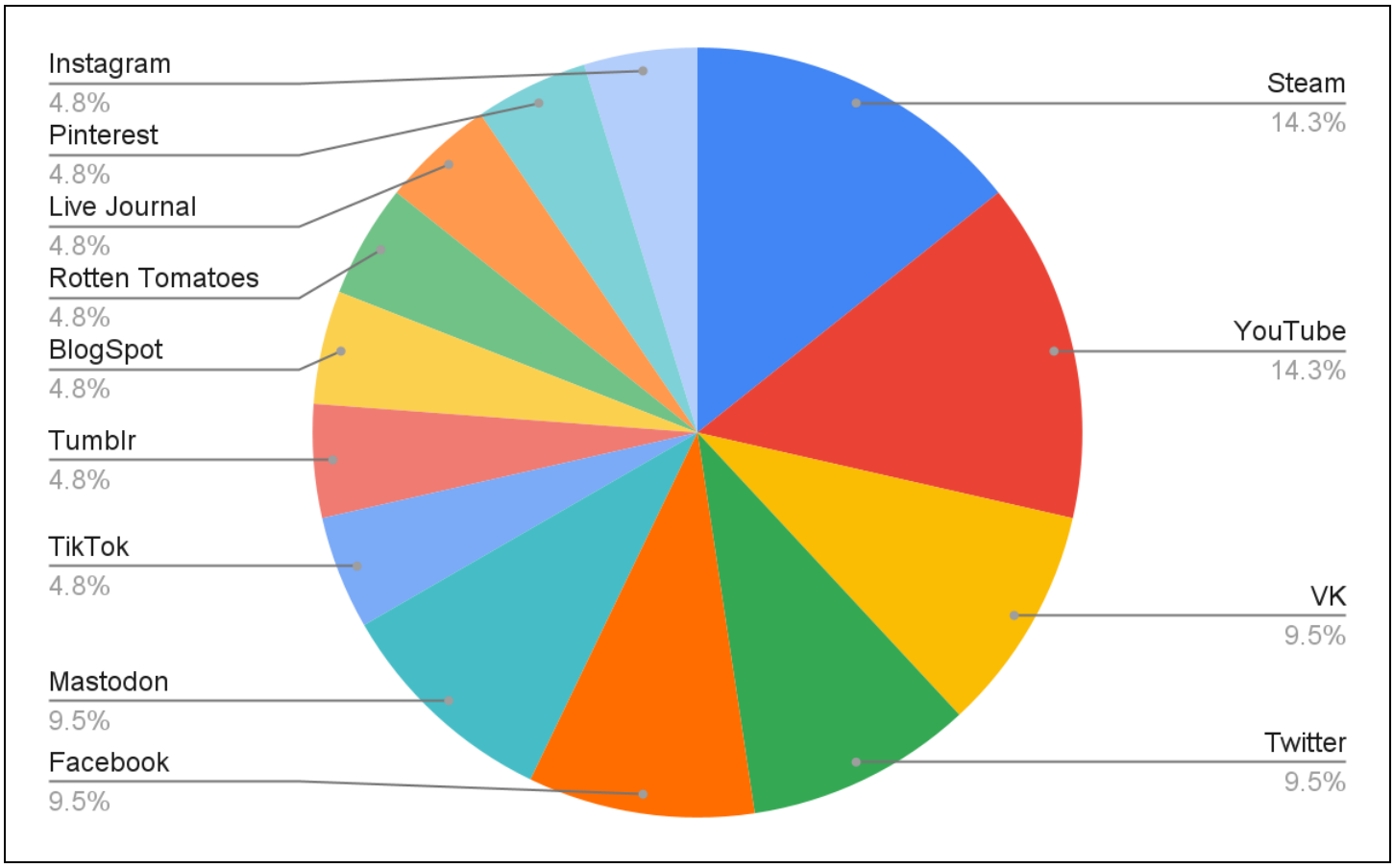

Figure 10: *Proportion of specific LIS abused for C2 among all social media instances (Source: Recorded Future)*

Mitigations and Recommendations

- **Consider blocking the use of specific LIS on your corporate network** if not required for legitimate purposes. Findings from this report about the most abused LIS combined with knowledge about employees' usage and requirements can help to prioritize which services to block. Network defenders must strike a balance between mitigating C2 communication via LIS and excessively restricting access to services that are allowed or necessary on their network.
- **Flag and investigate the use of specific LIS** while taking into account particular circumstances such as the nature of LIS usage (API vs. non-API, for example), details about the subnetwork where the communication occurs (such as the specific corporate department), and the communicating process (such as browser vs. non-browser), among others.
- **Use detection types including YARA and Sigma rules** to search your network for potential infections and to account for the missing visibility on the network level. Prioritize orchestration of the "triangle of detections" consisting of network-, file-, and log-based approaches.
- **Implement TLS network interception to improve visibility** in the face of widespread encryption adoption within LIS environments.
- **Implement more advanced detections** that involve behavioral aspects of malware activity (for example, requests to an LIS such as Telegram directly followed by a connection to an IP address by the same process, or possibly high certificate exchange frequencies to LIS).
- **Perform proactive threat hunting to detect novel instances of LIS abuse** or to identify LIS with potential for abuse. Recorded Future clients can search and alert on specific patterns associated with malware activity observed on a selection of LIS (such as Pastebin sites hosting base64-encoded payloads).
- **Integrate scenarios of LIS abuse into routine attack simulations** to continually assess the effectiveness of your infrastructure's detection capabilities.
- **Consider contacting LIS vendors** for their assistance in disabling/thwarting known malicious activity on their platform, since they alone have the capability to effectively stop the abuse from taking place.

Outlook

This report addresses a critical gap in current knowledge by providing a comprehensive and systematic overview of how LIS are abused for malicious purposes across various malware categories. While quantifying trends in LIS abuse is challenging due to the lack of comparable industry reporting, there are strong indicators suggesting that this kind of abuse is increasing. These indicators include the rapid pace of innovation by APT groups that constantly explore new LIS, the increasing adoption of LIS by malware families in updated versions, and the fact that LIS abuse support is increasingly becoming standard for certain malware categories such as infostealers.

Considering the advantages enjoyed by threat actors and the corresponding challenges faced by defenders inherent in using LIS, we anticipate a further rise in the abuse of LIS over the next few years. More specifically, from a quantitative perspective, we expect an increase not only in the proportion of

malware families and threat actors abusing LIS but also in the number and types of LIS being abused. From a qualitative perspective, we anticipate increased sophistication (in infrastructure and methods) and the continuation of APT groups leading the way in this domain, causing trickle-down effects to less-sophisticated groups over time.

While defenders face significant challenges in mitigating the abuse of LIS, there are some effective mitigations. These include implementing measures to block or flag the malicious usage of specific LIS within corporate environments, engaging in proactive threat-hunting practices or using threat-hunting-based intelligence, and focusing on other components of the "triangle of detections" to compensate for difficulties on the network level. To enhance protection against the abuse of specific LIS, however, it's imperative that defenders develop a deeper comprehension of 1) how certain services are legitimately engaged by an organization's users, and 2) how they are maliciously used. This knowledge will further enable the development of effective detection mechanisms and bolster overall protection. The next report in this series will analyze one specific LIS category abused for malicious infrastructure.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased and actionable intelligence.

Learn more at recordedfuture.com.