GROUP-IB

← Blog

Vlada Govorova
CERT-GIB Head, Latam

Hans Figueroa
Senior CERT Tier 2 Analyst, Latam

GTFire Phishing Scheme: Avoiding Detection Using Google Services

How GTFire abuses Google Firebase and Google Translate to scale global phishing campaigns

February 26, 2026 · min to read · Scam & Phishing

Brand Abuse Credential Harvesting Google Firebase Phishing Scam Campaigns Threat Intelligence

Introduction

Over the past several years, phishing campaigns have evolved beyond simple spoofed emails and low-effort fake login pages. Modern threat actors increasingly rely on legitimate cloud services, trusted domains, and well-known technology platforms to blend malicious activity into normal internet traffic. One such campaign, tracked as GTFire, demonstrates how attackers can systematically abuse Google-owned infrastructure to distribute phishing pages, evade security controls, and harvest credentials from thousands of victims worldwide.

The GTFire scheme relies heavily on Google Firebase (web.app) for hosting phishing pages and Google Translate as an intermediary layer that disguises malicious URLs to be capable of bypassing email and web security filters. By chaining these services together, the attackers create phishing links that appear benign, leverage Google's reputation, and dynamically redirect victims to brand-impersonating login pages. Once credentials are submitted and harvested, victims are often redirected back to the legitimate website of the targeted organization, reducing suspicion and delaying incident response.

This campaign is notable not only for its technical sophistication, but also for its scale. Analysis of exposed command-and-control (C2) infrastructure reveals thousands of stolen credentials

associated with more than a thousand organizations, spanning over a hundred countries and hundreds of industries. The attackers demonstrate strong operational discipline; reusing phishing templates across brands, enforcing multi-step credential collection, and maintaining centralized servers that store harvested data in an organized manner.

From a defensive perspective, GTFire highlights several uncomfortable truths. Trusted services can be weaponized with minimal effort, traditional URL-based detection is insufficient, and brand abuse remains one of the most effective social engineering vectors.

This blog aims to document the GTFire phishing scheme in detail, outline its modus operandi, map victimology, and provide actionable recommendations for defenders, CERT teams, and law enforcement.

Key Discoveries

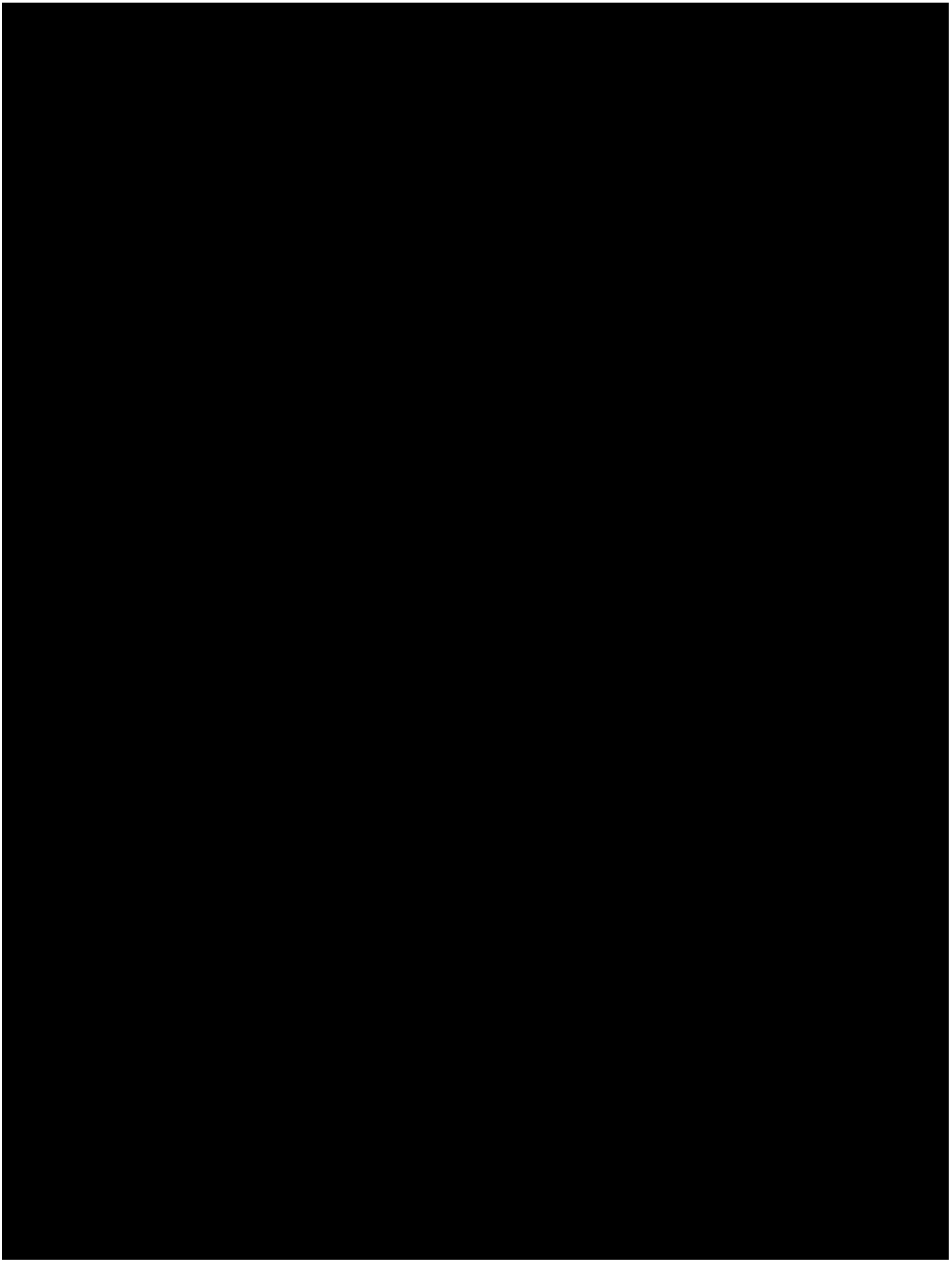
- GTFire abuses Google Firebase (web.app) to host phishing pages at scale.
- Google Translate is used as a phishing shield to evade detection and filtering.
- Over 120 unique phishing domains and more than 1,000 organizations are observed to be impacted.
- Redirection from fake login pages back to legitimate brand sites often leave victims none the wiser that their credentials have already been stolen.
- Victims span 100+ countries and over 200 industries globally.

Who May Find This Blog Interesting

- Cybersecurity analysts and corporate security teams
- Malware analysts
- Threat intelligence specialists
- Cyber investigators
- Computer Emergency Response Teams (CERT)
- Law enforcement investigators
- Cyber police forces

Group-IB Threat Intelligence Portal: GTFire

Group-IB customers can access our Threat Intelligence portal for more information about the GTFire threat actor and phishing scheme.



Victimology

Country (Top 5)	Industries Targeted	Total Victims
Mexico	Manufacturing, Education, Government	385
United States	Multiple	101
Spain	Multiple	67
India	Multiple	54
Argentina	Multiple	50

Figure 1. GTFire phishing scheme global victimology.

Infrastructure and Techniques

Abuse of Google Firebase Hosting (web.app)

GTFire relies on Google Firebase's free and fast hosting infrastructure to deploy phishing pages at scale. The threat actor registers large volumes of randomly generated *.web.app subdomains, allowing rapid rotation of infrastructure and minimizing operational costs. Because Firebase domains are widely trusted and frequently used by legitimate developers, these phishing pages often bypass reputation-based security controls.

Firebase-hosted pages dynamically load brand-specific login templates, displaying logos and visual elements of the targeted organization. The same phishing framework is reused across multiple brands, with only minor changes to URL paths and visual assets, enabling efficient scaling across regions and industries.

Domain Generation Patterns

Despite these characteristics, Firebase domains observed by Group-IB researchers in this campaign follow predictable, high-volume naming patterns, including:

- Randomized alphabetic strings of 6-10 characters
- Alphanumeric combinations designed to evade simple blocklists

These patterns enable defenders to build proactive hunting rules rather than relying on static domain lists.

Google Translate as a Phishing Shield

A defining feature of the GTFire campaign is the systematic abuse of Google Translate's website translation functionality. Phishing links are distributed to victims in the form of *translate.goog* URLs, which act as an intermediary redirect layer between the victim and the malicious Firebase-hosted phishing page.

Google Translate – Website Translation Mode

These links use Google Translate's website translation feature. Google loads the original website through a translation proxy and dynamically replaces the visible text with the translated version, while preserving the original site structure and navigation. The original website itself is not modified; only the content rendered in the victim's browser is translated.

The first screenshot below demonstrates Google Translate's *Websites* feature, where a full website URL (in this case, *group-ib.com*) is submitted for automatic translation into another language (Spanish).

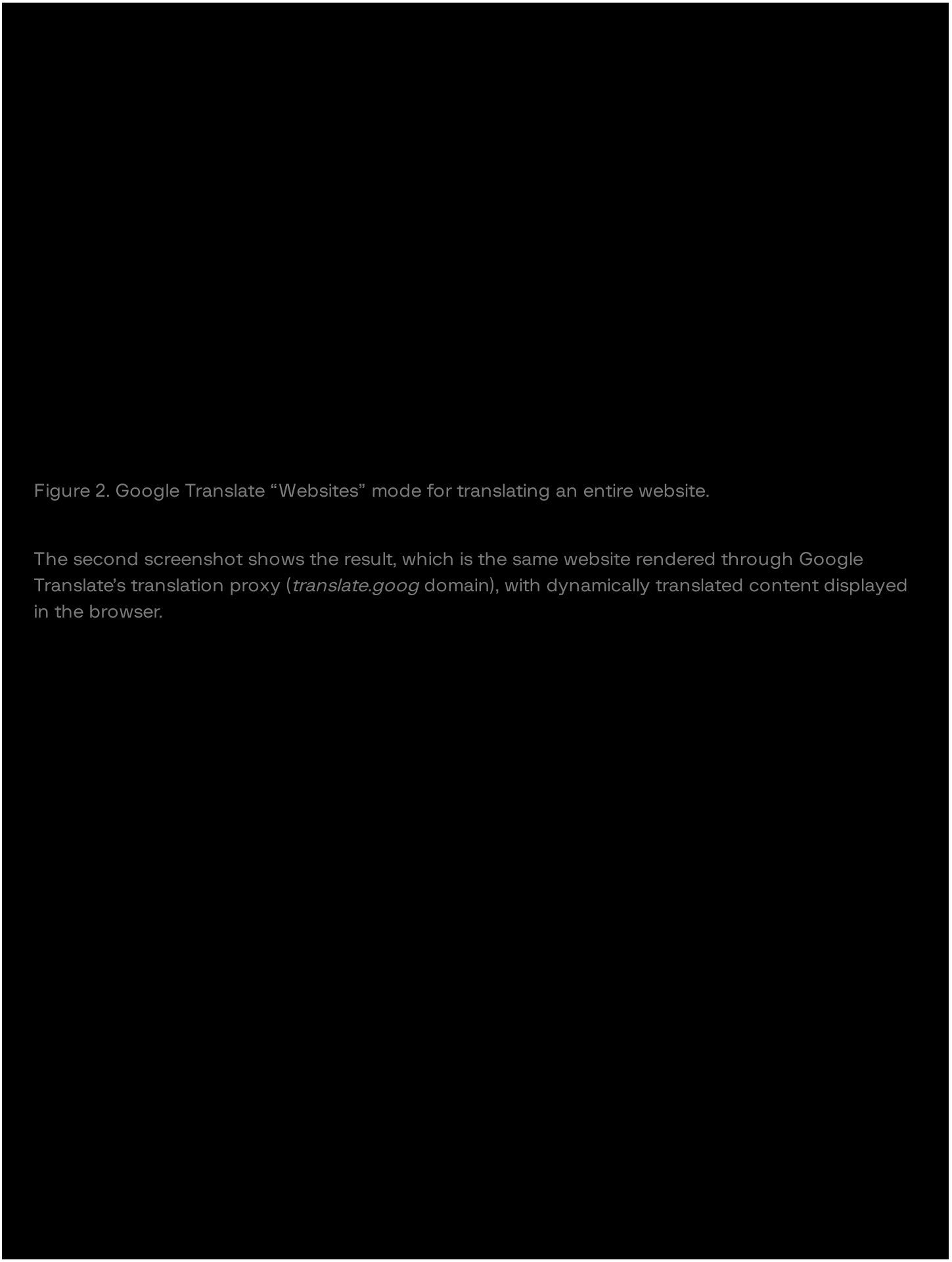


Figure 2. Google Translate “Websites” mode for translating an entire website.

The second screenshot shows the result, which is the same website rendered through Google Translate’s translation proxy (*translate.goog* domain), with dynamically translated content displayed in the browser.

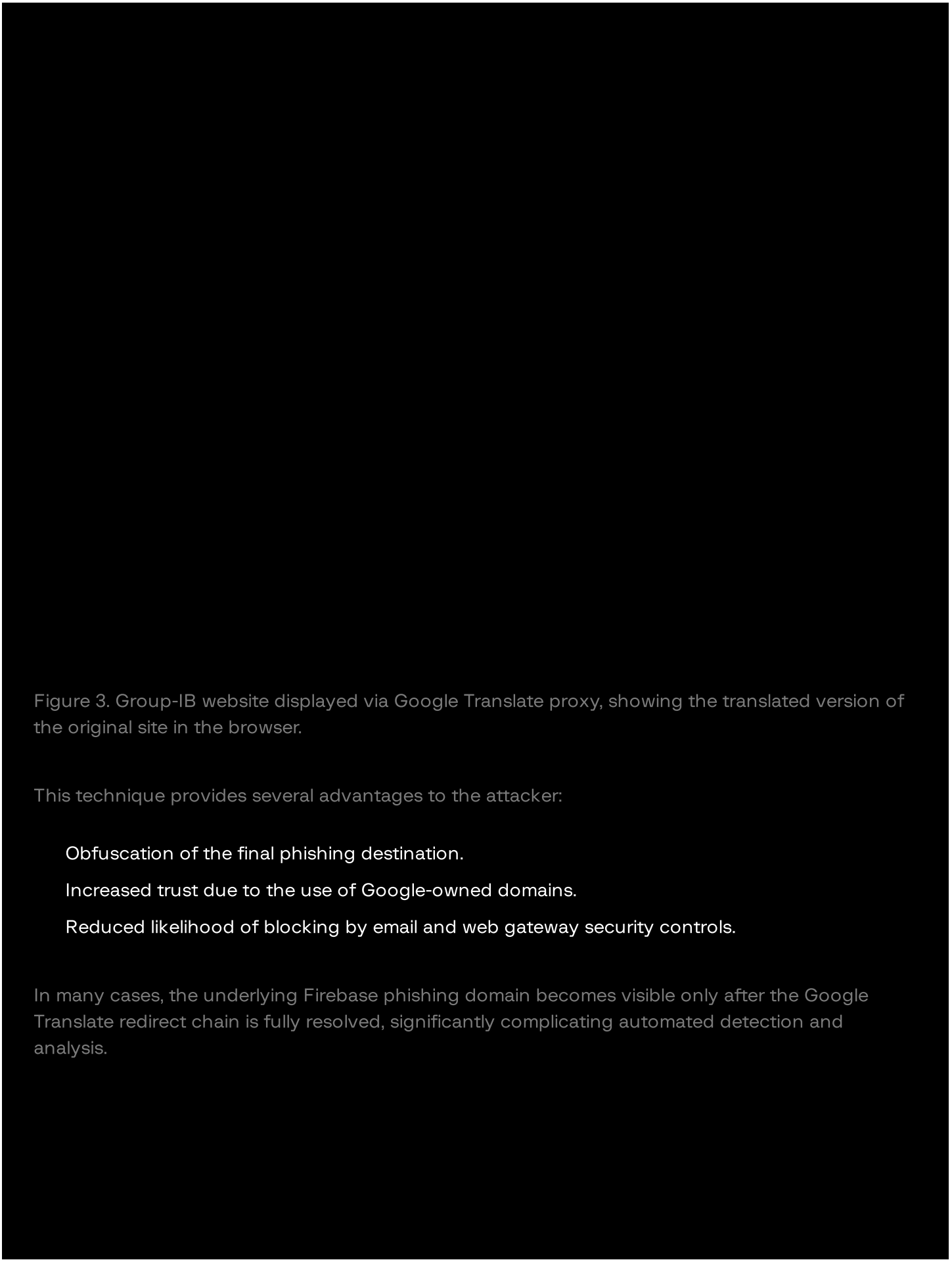


Figure 3. Group-IB website displayed via Google Translate proxy, showing the translated version of the original site in the browser.

This technique provides several advantages to the attacker:

- Obfuscation of the final phishing destination.
- Increased trust due to the use of Google-owned domains.
- Reduced likelihood of blocking by email and web gateway security controls.

In many cases, the underlying Firebase phishing domain becomes visible only after the Google Translate redirect chain is fully resolved, significantly complicating automated detection and analysis.

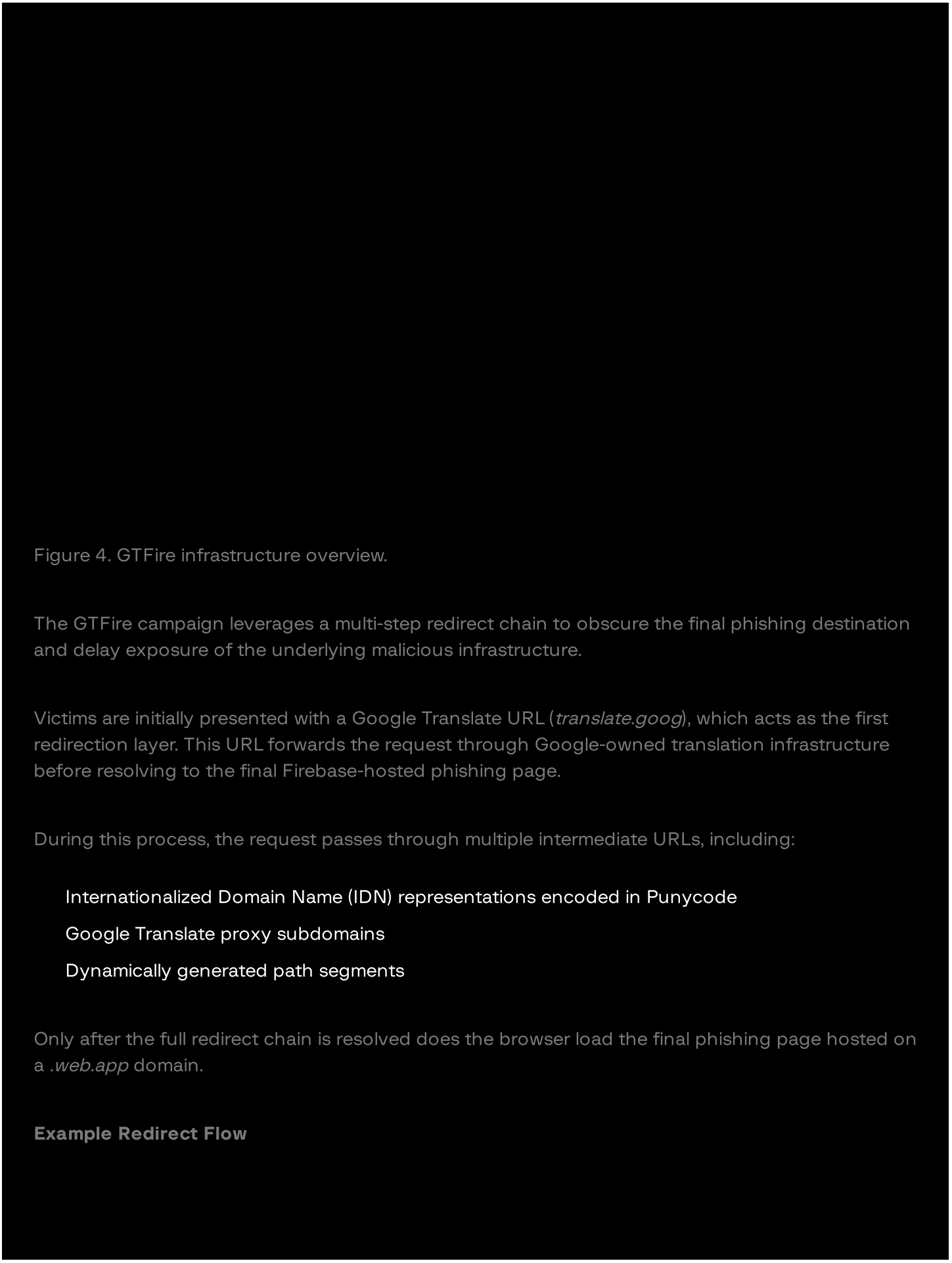


Figure 4. GTFire infrastructure overview.

The GTFire campaign leverages a multi-step redirect chain to obscure the final phishing destination and delay exposure of the underlying malicious infrastructure.

Victims are initially presented with a Google Translate URL (*translate.goog*), which acts as the first redirection layer. This URL forwards the request through Google-owned translation infrastructure before resolving to the final Firebase-hosted phishing page.

During this process, the request passes through multiple intermediate URLs, including:

- Internationalized Domain Name (IDN) representations encoded in Punycode
- Google Translate proxy subdomains
- Dynamically generated path segments

Only after the full redirect chain is resolved does the browser load the final phishing page hosted on a *.web.app* domain.

Example Redirect Flow

Figure 5. How legitimate Google Translate and Firebase domains are used to mask and host malicious webpages.

1. **The initial link**
   Victim clicks a *translate.goog* URL distributed via phishing messages.
2. **Google Translate proxy layer**
   The request is processed by Google Translate's web translation service, which rewrites the URL and forwards the request through Google-controlled infrastructure.
3. **Intermediate translated domain**
   The browser resolves encoded and translated domain names (including IDN/Punycode variants), further obscuring the true destination.
4. **Final destination on Firebase (Primary Request)**
   The request ultimately resolves to the phishing page hosted on Firebase (see below). Even at this stage, the Firebase domain only becomes visible in network traffic or browser developer tools, not necessarily in the address bar during earlier steps.

```
Google Translate URL
https://gxvv3mrr1-xn--wtsyr9q6-xn----c1a2cj-xn----p1ai[.]translate.goog/mon9K20E/KvQkJ/Y6l

Intermediate Translated Domain
https://gxvv3mrr1-xn--wtsyr9q6-xn----c1a2cj-xn----p1ai-translate.xn--c1a2cj[.]xn--p1ai/Czl
```

```
Primary Request on Firebase https://it1lhz.web[.]app/host:-%20%20login.:4592?+&_x_tr_sl=p
```

URL Obfuscation and Encoding

The phishing URLs frequently contain Base64-encoded parameters that embed victim-specific information, such as email addresses, language preferences, and targeted brands. In some cases, parameters are double-encoded to further hinder analysis and signature-based detection.

Figure 6. Double base64 decoding the url parameter: WTJGc2JDNTJhWEowZFdGc09VQmlZVzV2Y25SbExtTnZiUT09OkI0STNY

Credential Harvesting Workflow

Once a victim lands on the phishing page, the credential harvesting process follows a consistent and deliberate workflow:

1. The victim enters their username and password.
2. The phishing page displays an “incorrect password” message.
3. Credentials from the first attempt are silently exfiltrated.
4. The victim is prompted to re-enter their password.
5. Credentials from the second attempt are also harvested.
6. The victim is redirected to the legitimate website of the impersonated brand.

This design increases the attacker's chances of capturing valid credentials while minimizing user suspicion.

Figure 7. Phishing pages use fake error prompts and retry attempts to hide credential exfiltration in the background.

Data Exfiltration

Captured credentials are transmitted via HTTP GET requests to attacker-controlled command-and-control (C2) servers. Passwords are Base64-encoded and accompanied by metadata such as:

- Victim email address
- Country of access
- Browser language

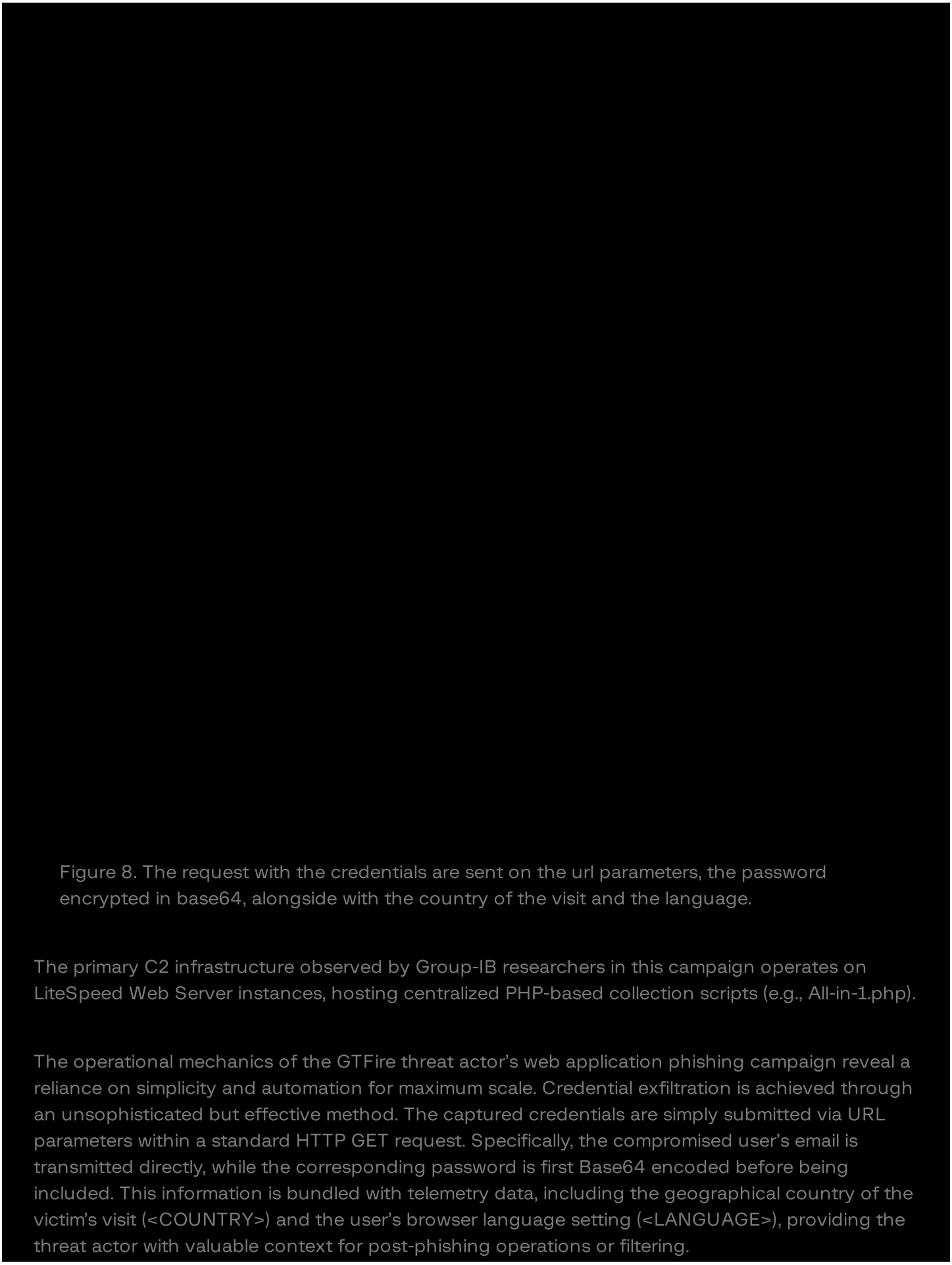


Figure 8. The request with the credentials are sent on the url parameters, the password encrypted in base64, alongside with the country of the visit and the language.

The primary C2 infrastructure observed by Group-IB researchers in this campaign operates on LiteSpeed Web Server instances, hosting centralized PHP-based collection scripts (e.g., All-in-1.php).

The operational mechanics of the GTFire threat actor's web application phishing campaign reveal a reliance on simplicity and automation for maximum scale. Credential exfiltration is achieved through an unsophisticated but effective method. The captured credentials are simply submitted via URL parameters within a standard HTTP GET request. Specifically, the compromised user's email is transmitted directly, while the corresponding password is first Base64 encoded before being included. This information is bundled with telemetry data, including the geographical country of the victim's visit (<COUNTRY>) and the user's browser language setting (<LANGUAGE>), providing the threat actor with valuable context for post-phishing operations or filtering.

The structure of the exfiltration request is as follows:

```
GET /myown/All-in-1.php=user=&pass=&pass2=&visit=&lang= HTTP/1.1
```

Once again, the cornerstone of the GTFire campaign's success is its strategic utilization of readily available tools such as commercialized All-in-1 PHP phishing scripts. This tactical choice dramatically reduces the operational overhead and speeds up the deployment cycle. These pre-packaged scripts are highly efficient, simplifying the creation of sophisticated, convincing phishing pages and automating the critical backend logic required for credential harvesting and exfiltration. This changes an attack that is typically complex, multi-stage, and highly customized per target, into a readily available plug-and-play operation.

By building their infrastructure on common, legitimate software components, such as the ubiquitous PHP scripting language and the high-performance LiteSpeed Web Server, the GTFire actor minimizes the need for specialized custom development and reduces the risk of being associated with maintaining unique, easily fingerprinted infrastructure. This commitment to automation enables GTFire to instantly replicate and deploy new credential harvesting pages across their continually rotating network of domains. all while maintaining minimal resource investment.

Command-and-Control (C2) Infrastructure

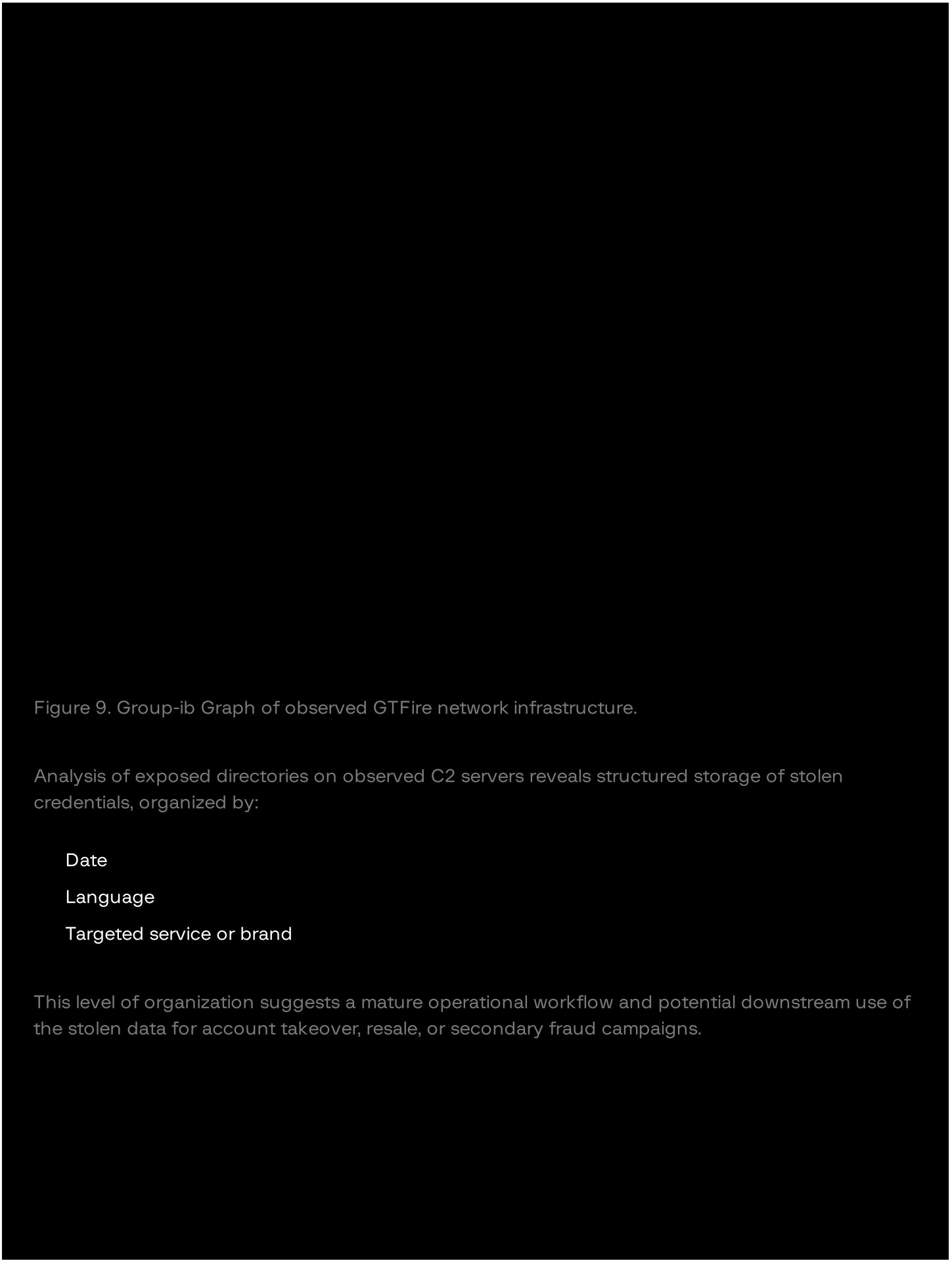


Figure 9. Group-ib Graph of observed GTFire network infrastructure.

Analysis of exposed directories on observed C2 servers reveals structured storage of stolen credentials, organized by:

- Date
- Language
- Targeted service or brand

This level of organization suggests a mature operational workflow and potential downstream use of the stolen data for account takeover, resale, or secondary fraud campaigns.

Figure10. Litespeed Web Server where the harvested credentials and phishing scripts are stored.

Conclusion

The GTFire phishing scheme demonstrates how modern threat actors can effectively weaponize trusted platforms to conduct global, large-scale credential harvesting campaigns. By abusing Google Firebase and Google Translate, GTFire significantly reduces detection rates while maintaining operational efficiency. The observed use of other legitimate services and tools such as LiteSpeed Web Server and All-in-1 PHP scripts further enhances the scalability and rapid deployment capability of this phishing campaign. The campaign's longevity and scale highlight the urgent need for defenders to rethink trust models and improve detection strategies around legitimate service abuse.

Recommendations

For Organizations

- Implement phishing-resistant MFA
- Monitor for brand impersonation on trusted cloud platforms
- Educate employees about Google-based phishing techniques

For Security Teams

- Correlate URL patterns involving translate.goog and web.app
- Share IOCs across industry and CERT communities

Frequently Asked Questions (FAQ)

What makes GTFire different from typical phishing campaigns?

Its systematic abuse of trusted Google services and global scale.

Why is Google Translate used in this scheme?

Are only Latin American companies targeted?

How does redirection to the real brand website reduce suspicion?

Group-IB Fraud Matrix

Indicators of Compromise (IOCs)

Network IOCs

- jnhwzs[.]fyi
- gnpnia[.]lat

Network Indicators

- *.web.app with Google Translate redirects

File Indicators

- All-in-1.php credential collection scripts

DISCLAIMER: All technical information, including malware analysis, indicators of compromise and infrastructure details provided in this publication, is shared solely for defensive cybersecurity and research purposes. Group-IB does not endorse or permit any unauthorized or offensive use of the information contained herein. The data and conclusions represent Group-IB's analytical assessment based on available evidence and are intended to help organizations detect, prevent, and respond to cyber threats.

Group-IB expressly disclaims liability for any misuse of the information provided. Organizations and readers are encouraged to apply this intelligence responsibly and in compliance with all applicable laws and regulations.

This blog may reference legitimate third-party services such as Telegram and others, solely to illustrate cases where threat actors have abused or misused these platforms.

This material is provided for informational purposes, prepared by Group-IB as part of its own analytical investigation, and reflects recently identified threat activity.