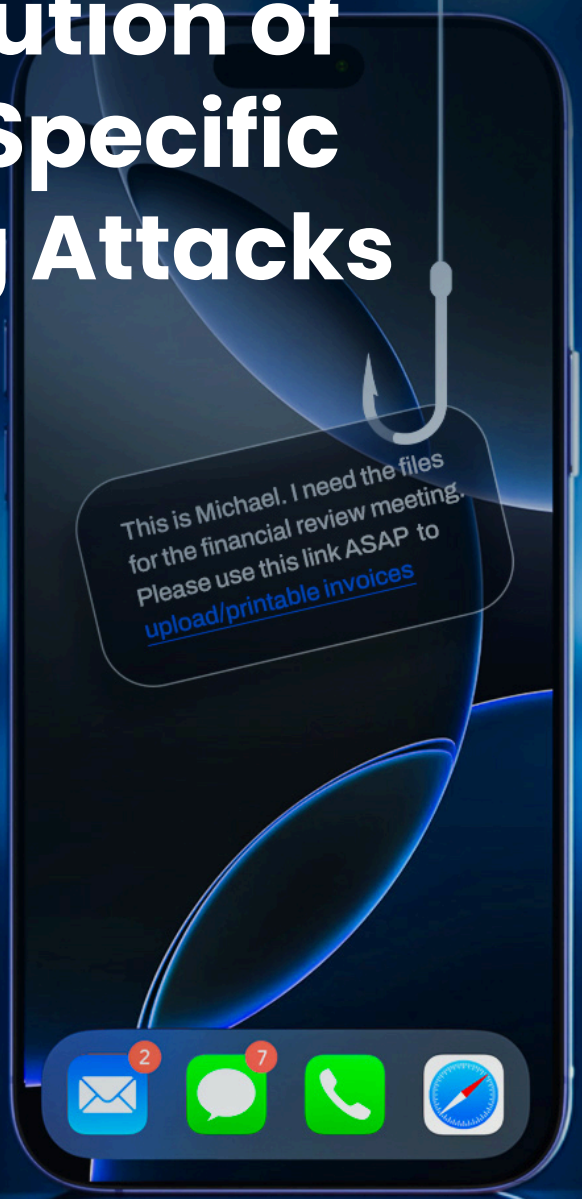
zLabs Mishing Report:

The Evolution of Mobile-Specific Phishing Attacks



Understanding Mishing Attack Vectors in 2024

ZIMPERIUM®

As cybercriminals have moved to a “mobile-first” attack strategy, they have discovered an insidious new attack vector: the pairing of social engineering with mobile devices. Our recent analysis reveals concerning trends in mobile-specific phishing attacks – known as "mishing" – that leverage unique platform characteristics to execute targeted campaigns. These attacks exploit mobile-specific features, vulnerabilities and user behaviors, making both detection and analysis significantly more challenging than phishing on a traditional work desktop or laptop.

Beyond just traditional banking/payment fraud, mishing campaigns have been observed executing much more treacherous actions, including the downloading of malware capable of hijacking OTP (one-time-passwords) and verification codes, mimicking screen interfaces and the ability to steal enterprise application credentials. An interesting example of this is the SMS stealer campaign discovered by zLabs. The blogpost describes a large-scale Android-targeted SMS stealer campaign, distributing more than 100,000 malware samples across 113 countries. Attackers employ deceptive ads and Telegram bots to trick users into installing malicious apps that intercept SMS messages, including one-time passwords, compromising accounts on more than 600 global services.

The Rising Threat of Mishing

The convergence of personal and professional activities on mobile devices has created an ideal landscape for a new generation of targeted phishing campaigns. Unlike traditional phishing attacks, mishing exploits mobile-specific weaknesses:

- **Limited screen size,** which makes suspicious URLs harder to detect
- **Touch-based interfaces,** reducing users’ ability to carefully inspect URLs
- **Mobile-specific messaging channels,** such as SMS, messaging apps, QR codes, which are often trusted and commonly used in our every day interactions.
- **Users’ inherent trust in mobile devices,** lowering user’s vigilance and increasing the likelihood of deception

These factors highlight a critical shift: mishing is not just a mobile adaptation of traditional phishing—it is a distinct category of threats engineered specifically for (and often only for) mobile environments.

The Strategic Significance

The rise of mishing attacks coincides with several key developments in enterprise mobility, including:

- **The normalization of BYOD (Bring Your Own Device) policies**, blurring the lines between personal and corporate data.
- **Greater reliance on mobile devices for multi-factor authentication**, making them a prime target for credential threat.
- **The growing adoption of cloud & mobile business applications**, expanding the attack surface, specifically data leakage of both private and corporate data.
- **The blurred lines between personal and professional device usage**, creating security gaps that can be easily exploited by threat actors.

This convergence has created an environment where a successful mishing attack can compromise both personal and enterprise security, potentially providing attackers with a direct access to critical corporate infrastructure and data.

Understanding the Mobile Phishing Ecosystem

Our research has identified primary attack vectors that define the current mobile phishing landscape:

1. **Mobile-targeted Email Phishing** -A standard email attack that only executes from a mobile device.
2. **Smishing** - a targeted phishing attack that is delivered by text/SMS.
3. **Quishing** - Utilizing QR codes, which obfuscate the destination.
4. **Vishing** - Voice call-based phishing attacks using social engineering through phone communication to manipulate targets into taking unsafe actions, such as clicking on an SMS link or divulging sensitive information such as credentials, OTP codes.

Figure 1 summarizes our analysis of mobile phishing attack vectors during 2024, revealing a diverse threat landscape where SMS-based attacks (**smishing**) and messaging apps are the predominant attack vector. Our data places **email vectors** in a second place, closely followed by PDF-based attacks. While **QR codes** represent a small percentage, their unique evasion capabilities and growing adoption rates make them vectors with huge latent potential.

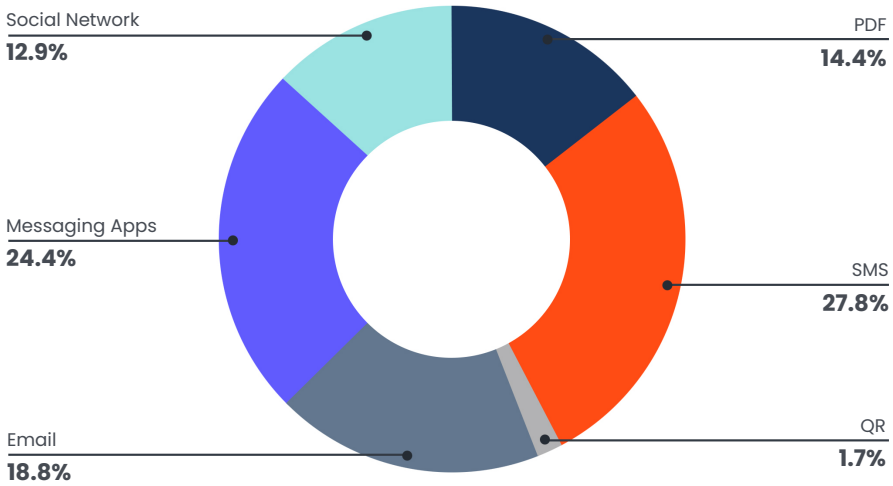


Figure 1.
Mobile phishing entry points during 2024.

Mobile Targeted Email Phishing

The emergence of device-aware email attacks allows campaigns specifically targeted to mobile users through seemingly standard email messages in which the malicious payload only executes when accessed from a mobile device. When the same link is accessed from a desktop environment, the attack chain is terminated, making detection and analysis significantly more challenging. This is a unique and clever tactic for bypassing standard email and network security solutions, as few enterprises and users employ security on the mobile device.

As shown in a previous blogpost, mobile specific phishing attacks usually originated as an email.

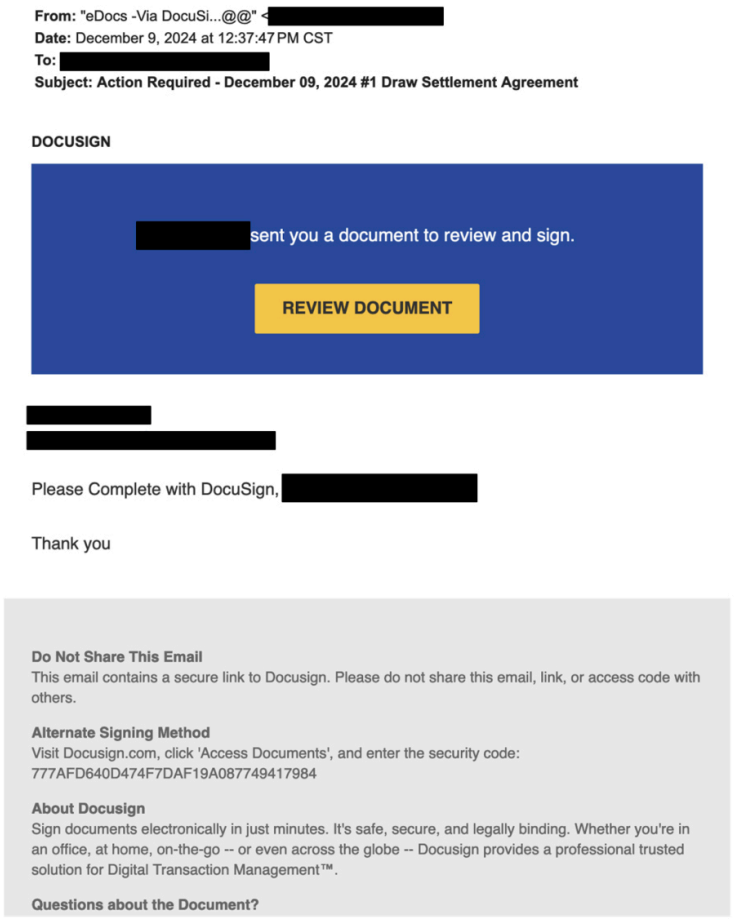


Figure 2.
Phishing email trying to get user credentials via a fake document from Docusign.

Figure 2 shows the phishing email, in which the attack originates. The final phishing site is only accessible via mobile devices.

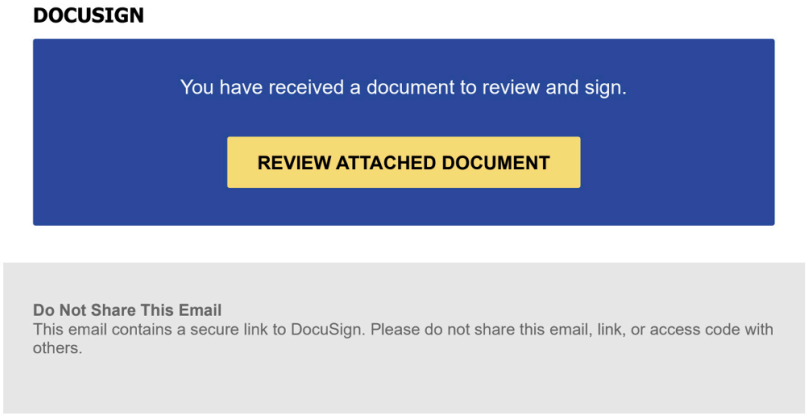


Figure 3.
Fake Docusign PDF containing phishing link, the final phishing site is only accessible via a mobile device.

The referenced blogpost also describes an attack with the phishing link embedded into a PDF file (Figure 3). Usually those files are harder to analyze, or give people a false sense of security.

Smishing: SMS-Based Attack

Smishing continues to show concerning growth rates, with particularly high impact in specific geographical regions. As shown in Figure 4, our data indicates that India leads in smishing susceptibility at 37%, followed by the United States at 16%, and Brazil at 9%.

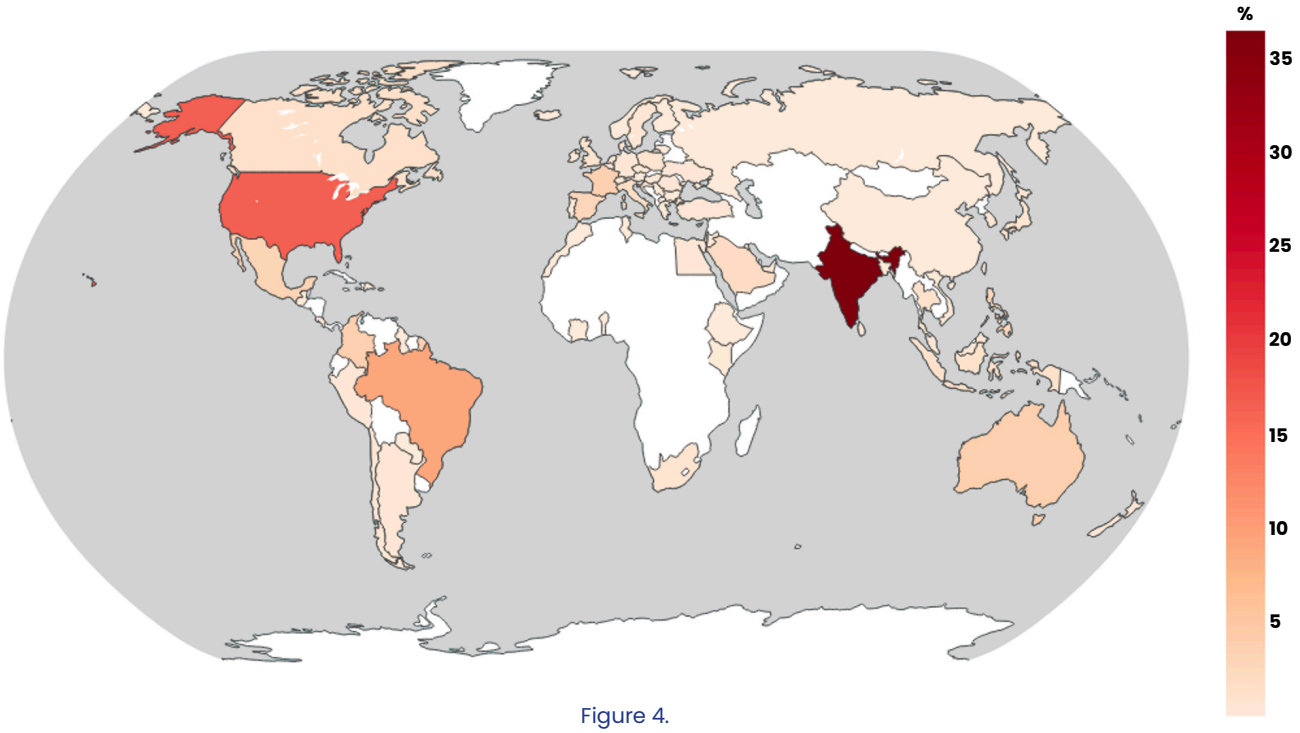


Figure 4.
Distribution of detected Smishing attacks by country.

Taking advantage of both the short nature of SMS texts and a sense of urgency, threat actors frequently employ URL shorteners and redirect chains to obscure their attack infrastructure. Figure 5 shows examples of blocked mishing attacks received via SMS by our clients. It can be seen that it is common to use short links, or URL shortening services in case of long final URL.

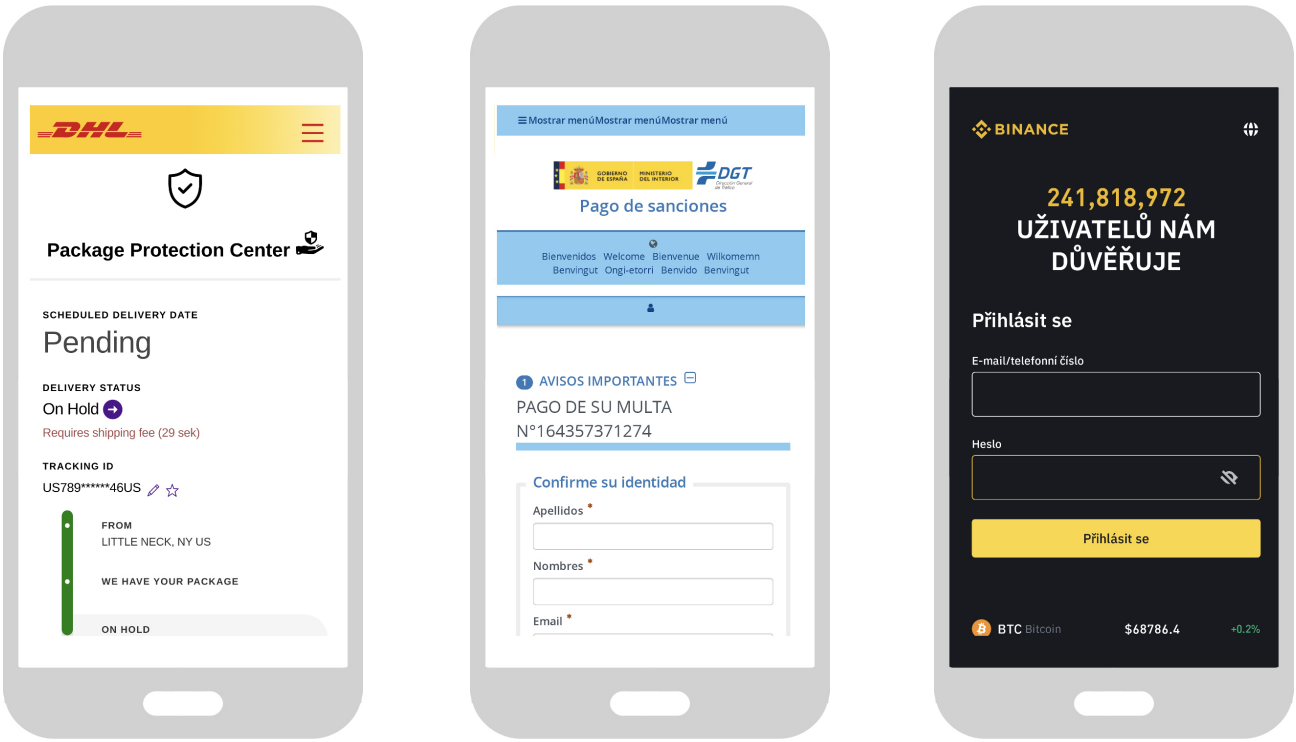


Figure 5.
Spoofed trusted brands detected and blocked via smishing attacks.

On the left, a targeted attack trying to deceive the victim to pay to complete a delivery package. Blocked URL: **https[://]2h[.]ae/dhl[redacted]**. On the center, another targeted attack trying to get information from a user, related to a traffic fine. After the form, the attacker is trying to get a payment from the victim. Attack using a shortened URL: **https[://]u[redacted]A** redirecting to: **https[://]eeu[.]wek[.]mybluehost[.]me/website_c9d63928/wp-admi[redacted]o**. On the right, a URL: **https[://]binan[redacted]** received via SMS, trying to get credentials from a crypto exchange.

Quishing: QR Code-Based Phishing

QR code-based phishing, or "quishing," represents an emerging threat vector that exploits the inherent trust users place in QR codes, which obfuscate the destination. As shown in Figure 6, the geographical distribution of detected Quishing attacks by Zimperium shows significant concentration in Japan (17%), the United States (15%), and India (11%).

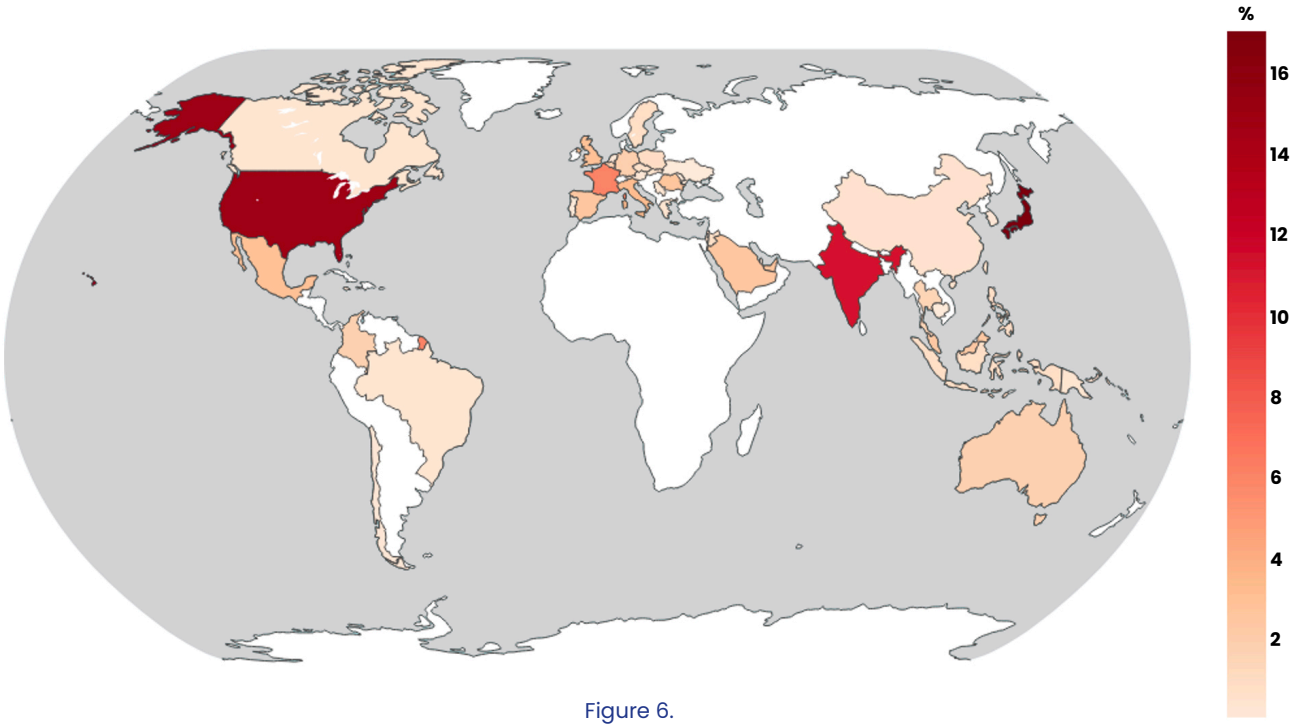


Figure 6.
Geographical distribution of Quishing attacks.

We've observed two primary quishing deployment strategies:

1. **Public Space Deployment:** Attackers place malicious QR codes in high-traffic areas, often disguised as legitimate promotional materials or utility services. Examples of these detections are shown in Figure 7.
2. **Targeted Mail Campaigns:** Physical mail containing QR codes purporting to be from legitimate services, particularly effective for package delivery and financial service scams. A couple of examples are shown in Figure 8.

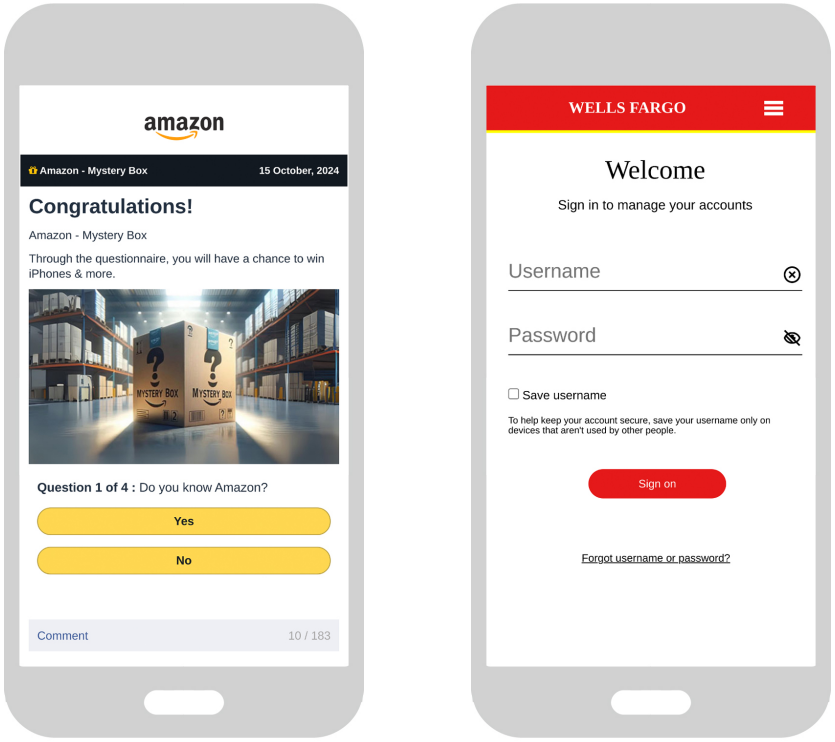


Figure 7.

Figure 7. On the left, QR phishing targeting a shopping site. A public sign on the street can have a message to scan the QR code to win a prize and get private information from the victim. Final URL is: **https[://]amazon.com@sroff[.]cyo[redacted].** On the right, QR phishing targeting homebanking. A public sign next to the bank's door can have a message to scan the QR code to get a number for the bank queue, stealing the victim's homebanking credentials. Final URL is: **http[://]abdrsd[.]github[redacted]**

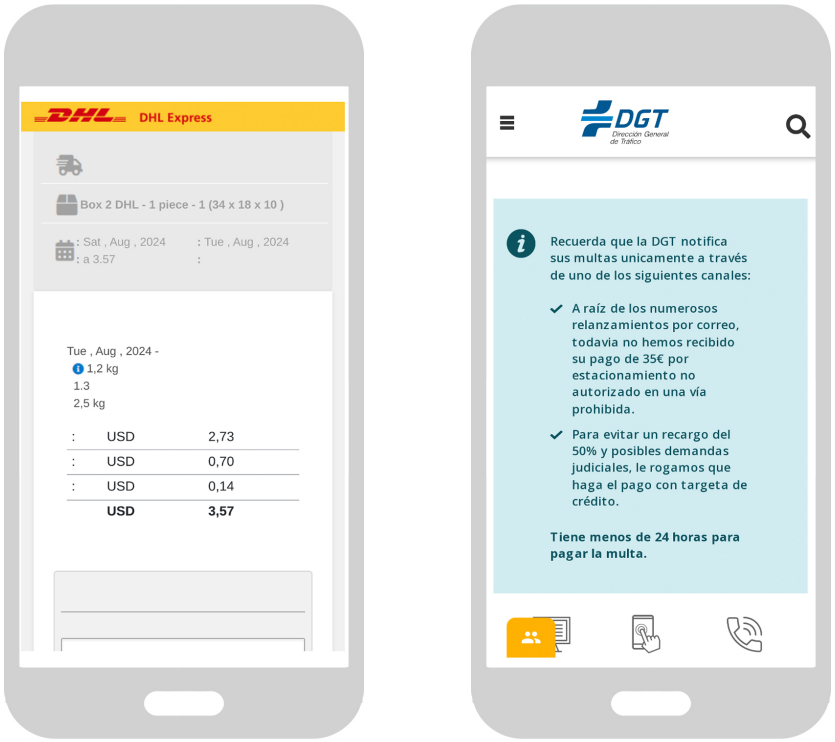


Figure 8.

Figure 8. On the left, a phishing site trying to get a payment from the user to receive a package. Final URL: **`http[://]hej[.]rnz[.]mybluehost[.]me/wp-admin/folder/dh`**[redacted] . On the right, a phishing site trying to get a payment from the user for a traffic fine. In both cases, an attacker can leave a paper in a mailbox to deceive a victim to complete a pending order. Final URL: **`https[://]ume[.]la/`**
`Vb`[redacted]

Technical Analysis: Advanced Evasion Techniques

In our analysis of mobile phishing campaigns throughout 2024, we've observed an increasing sophistication in evasion techniques. Threat actors are implementing multi-layered detection bypass mechanisms (smart redirections) that leverage device fingerprinting, conditional execution paths, and legitimate service impersonation. Our research has identified several advanced evasion techniques commonly employed in mishing campaigns.

Device-Specific Redirection

Approximately 3% of analyzed phishing sites implement different redirection paths based on the user's device type. This technique serves multiple purposes:

1. **Evasion of Security Analysis:** Desktop-based security tools often fail to detect mobile-specific attack chains
2. **Enhanced Targeting:** Allows attackers to deliver device-optimized payloads
3. **Improved Campaign Longevity:** Reduces detection rates by serving benign content to non-targeted devices

Our analysis of verified phishing sites reveals a sophisticated pattern of desktop redirection to legitimate services as an evasion technique (Figure 9) wiith Google and Facebook being the primary destinations. When accessed from desktop devices, these malicious sites redirect users to legitimate platforms – a technique that significantly complicates automated analysis and detection. This evasion tactic allows attackers to maintain prolonged campaign effectiveness by appearing benign to security tools while still targeting mobile users with malicious content.

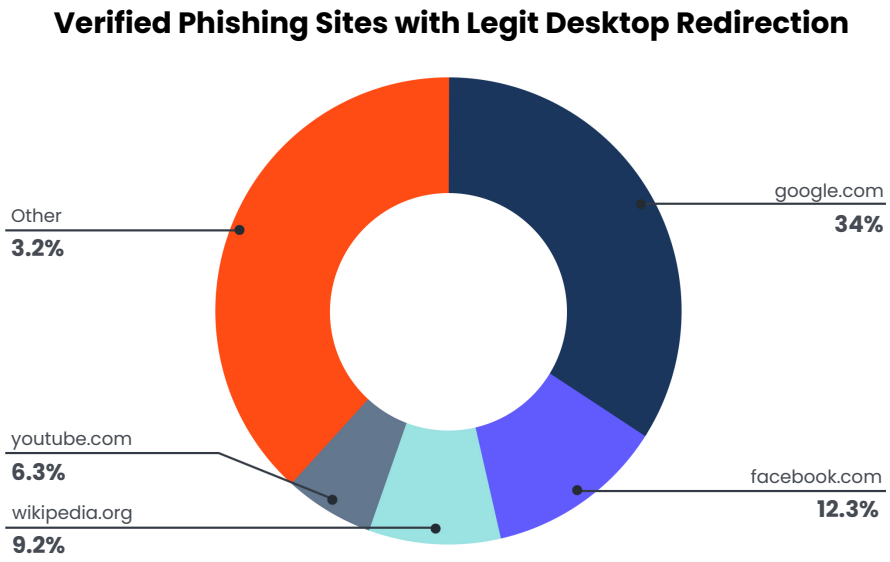


Figure 9.
Popular websites used by phishing sites for redirection when accessed via a desktop.

Figure 10 shows a detected phishing attack targeted for mobile devices. The redirection can also be configured for a specific device, not just mobile, multiplying the combinations for a detailed analysis.

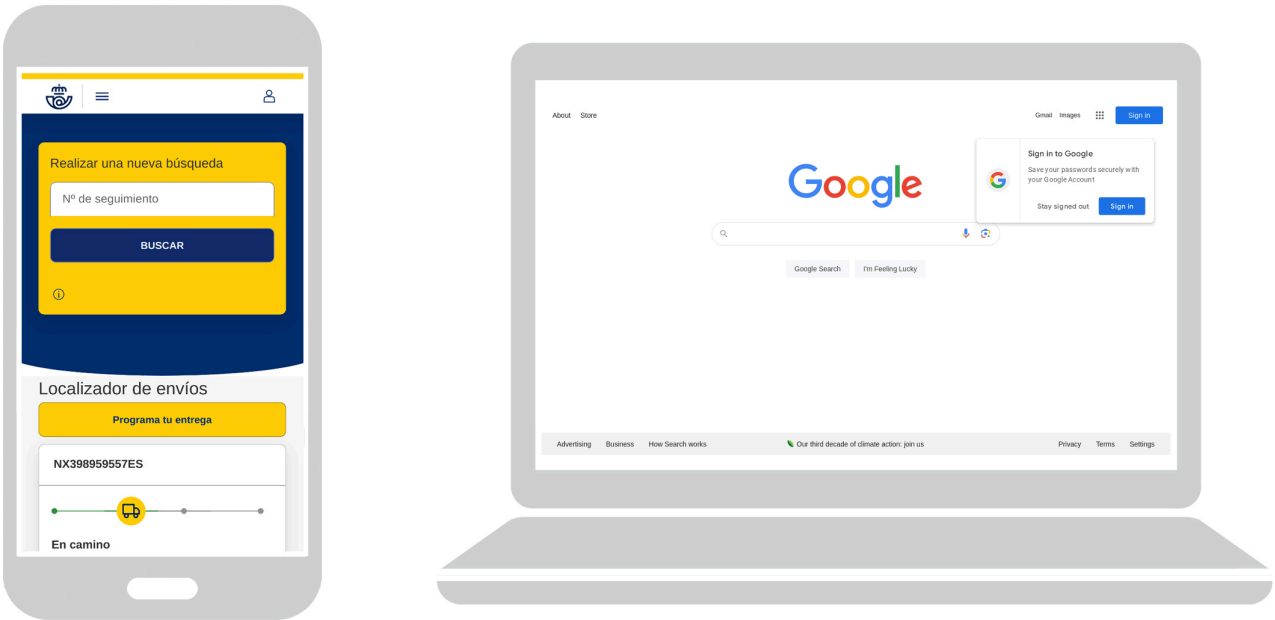


Figure 10.

Figure 10. A phishing campaign targeting specific mobile devices. URL: **http[://]itsssl[.]com/gru[redacted]** . On the left, the site is rendered on mobile. On the right, redirection to google.com when accessed using desktop.

Geolocation-Based Attack Distribution

Modern mishing campaigns frequently employ geolocation-based redirection at country or even at the city level, allowing for highly targeted attacks. This technique:

- Enables precise targeting of specific regions or organizations
- Complicates detection by security researchers
- Increases campaign effectiveness through localization
- Reduces detection rates by serving legitimate content to non-targeted regions

Detected Phishing Campaign Sharing Infrastructure

Our investigation into a large-scale phishing operation revealed sophisticated infrastructure sharing patterns across multiple targeted brands. The campaign, initially identified through a Chase-targeted phishing site, demonstrated advanced evasion techniques through selective desktop redirection.

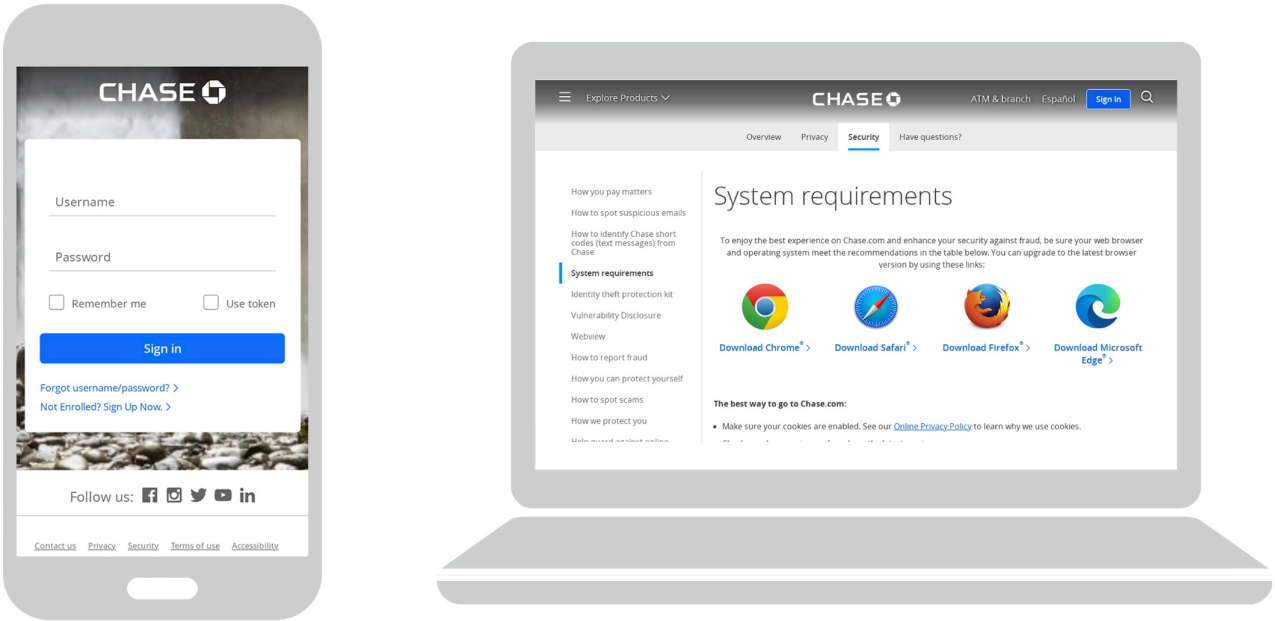


Figure 11.

Figure 11. URL: **http[://]svdiipla[.]com/[redacted]/** . On the left, spoofed phishing site rendered on mobile. On the right, redirection to the legit chase.com site when accessed using a desktop.

Infrastructure Analysis

A significant portion of the attack infrastructure was traced to a specific CIDR block apparently owned by Unified Layer, a web hosting provider. This hosting infrastructure exhibited several notable characteristics:

1. **Adaptive Redirection Patterns:** When accessed via desktop browsers, the malicious domains consistently redirected to legitimate websites of the targeted brands. For example, the analyzed URL **`http[://]svdiipla[.]com/[redacted]/`** redirected desktop users to chase.com while serving phishing content to mobile visitors.
2. **Infrastructure Reuse:** The campaign demonstrated systematic reuse of the same CIDR block across multiple phishing sites targeting different financial institutions and brands. This pattern suggests a coordinated operation rather than disparate individual attacks.
3. **Hosting Provider Abuse:** The attackers leveraged legitimate hosting infrastructure through Unified Layer, potentially exploiting the provider's scale and reputation to enhance attack persistence and credibility.

Our analysis uncovered an extensive phishing operation leveraging shared infrastructure across the CIDR block 162.241.124.0/22. Network analysis revealed a sophisticated campaign utilizing multiple IP addresses within this block to host phishing domains targeting a diverse range of financial institutions and technology companies.

Infrastructure Analysis and Campaign Scope

The campaign infrastructure, visualized in Figure 12, demonstrates a hierarchical attack structure:

- Central CIDR block (162.241.124.0/22) distributing traffic across distinct IP addresses.
- Several unique domains targeting different brands.
- Primary targets include financial institutions (Chase, Brookline Bank, Credit Agricole), technology companies (Apple, Microsoft), and financial technology services (PayPal, Square).

Domain naming patterns suggest intended social engineering with domains crafted to impersonate legitimate services (e.g., **`care-apple.info, chaseistonthecase.com`**) and technical support platforms (**`fyndsupports.info`**).

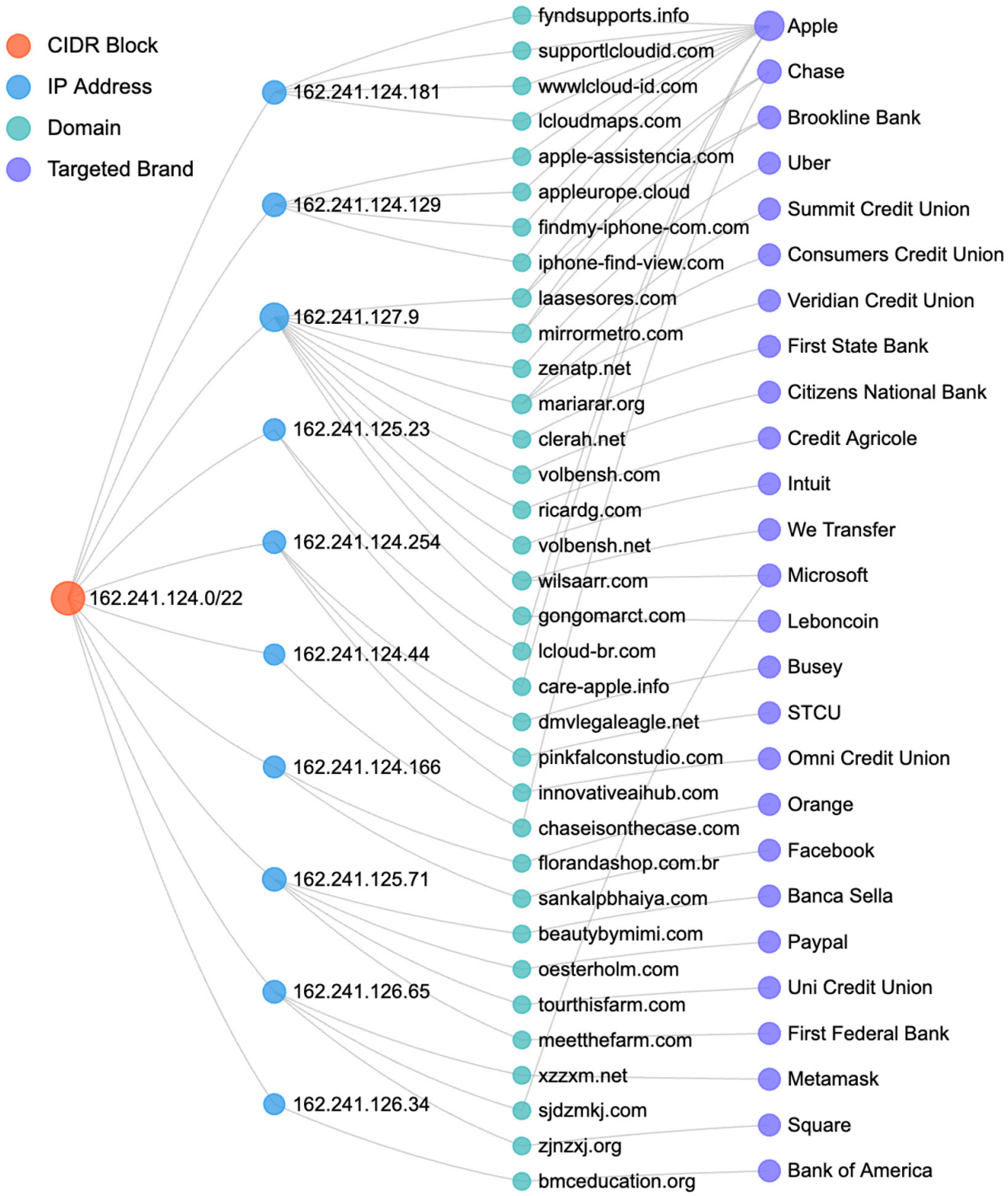


Figure 12.
Mobile phishing campaign network infrastructure.

Temporal Analysis and Campaign Evolution

The campaign's operational timeline, shown in Figure 13, reveals strategic patterns in infrastructure deployment:

- Initial infrastructure deployment identified in January 2024.
- Significant escalation in mid-2024, peaking in August with over 1,000 daily records.
- Sustained operational presence through October, indicating robust infrastructure resilience.
- Periodic activity spikes suggesting coordinated deployment of new attack vectors.

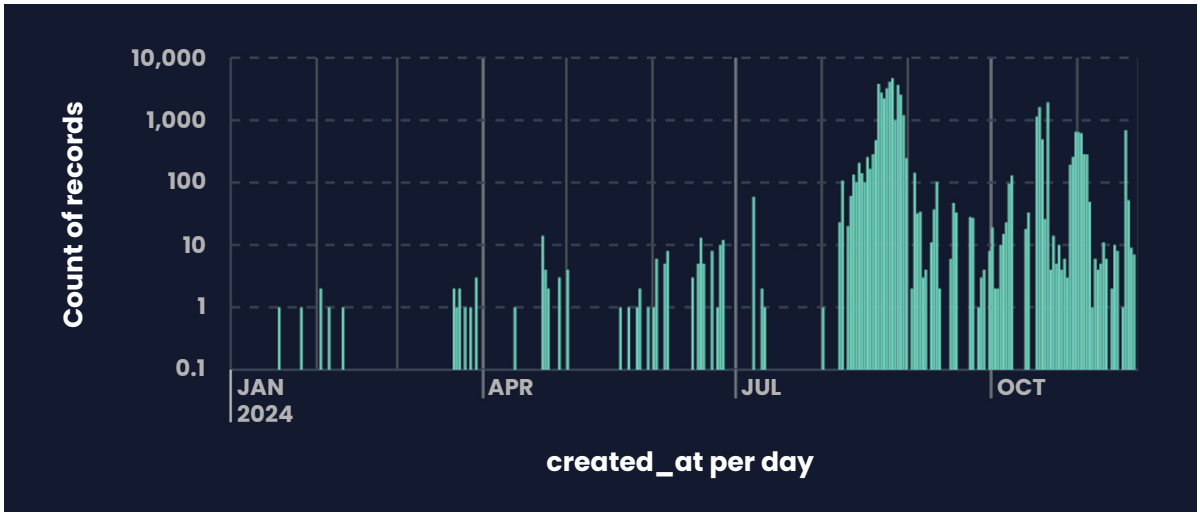


Figure 13.
Timeline of detection for mobile phishing campaign sharing network infrastructure.

Conclusion: The Evolving Mishing Threat Landscape

Our analysis of mobile-targeted phishing campaigns throughout 2024 reveals a continuous evolution in attack sophistication and scale. The emergence of mishing as a distinct attack methodology represents a significant shift in the threat landscape with attackers leveraging mobile-specific vulnerabilities and user behaviors to execute increasingly effective campaigns.

Key Research Findings

The data presents compelling evidence of systematic changes in phishing tactics:

- Device-aware attacks leverage sophisticated fingerprinting to selectively target mobile users while evading desktop-based security controls
- Infrastructure sharing patterns indicate coordinated campaign operations, with single CIDR blocks supporting diverse targeting across multiple sectors
- Geolocation-based targeting enables precise attack delivery, complicating detection and analysis efforts
- Cross-channel attack vectors (SMS, QR codes, mobile email) demonstrate attackers' adaptability to mobile user behaviors

Strategic Security Implications

Organizations must recognize that traditional anti-phishing measures, designed primarily for desktop and enterprise network environments, are increasingly inadequate against mobile-specific attack vectors. The convergence of personal and professional mobile device usage, combined with sophisticated evasion techniques and infrastructure sharing, creates complex security challenges that require mobile-specific defensive strategies.

Effective mishing protection requires a multi-layered approach combining:

- On-device behavioral analysis to detect device-aware attacks
- Real-time URL analysis with device-context awareness
- AI-based detection of infrastructure patterns
- Cross-channel threat correlation and analysis

As mobile devices continue to become primary targets for sophisticated mishing campaigns, organizations must evolve their security frameworks to address these emerging threats effectively. The technical sophistication demonstrated by observed campaigns suggests this trend will continue to accelerate, demanding continued innovation in mobile-specific security controls.

About Zimperium

Zimperium is the world leader in mobile security. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging AI-driven, autonomous security to counter evolving threats including mobile-targeted phishing (mishing), malware, app vulnerabilities and compromise, as well as zero day threats. As cybercriminals adopt a mobile-first attack strategy, Zimperium helps organizations stay ahead with proactive, unmatched protection of the mobile apps that run your business and the mobile devices relied upon by your employees. Headquartered in Dallas, Texas, Zimperium is backed by Liberty Strategic Capital and SoftBank. Learn more at www.zimperium.com and connect on LinkedIn and X (@Zimperium).

www.zimperium.com

Author: Santiago A. Rodriguez

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244