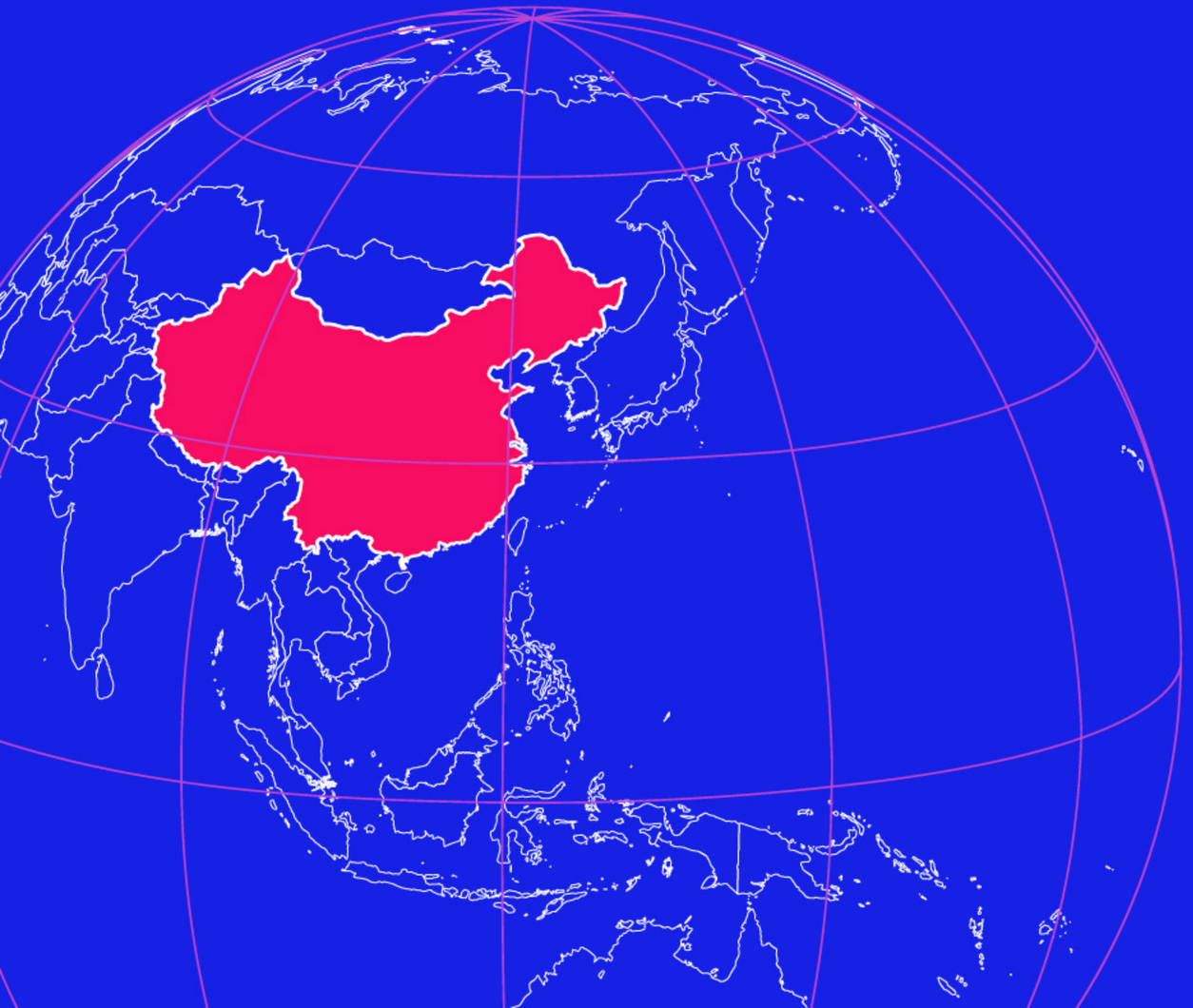
SecAlliance

Part of CSIS Security Group



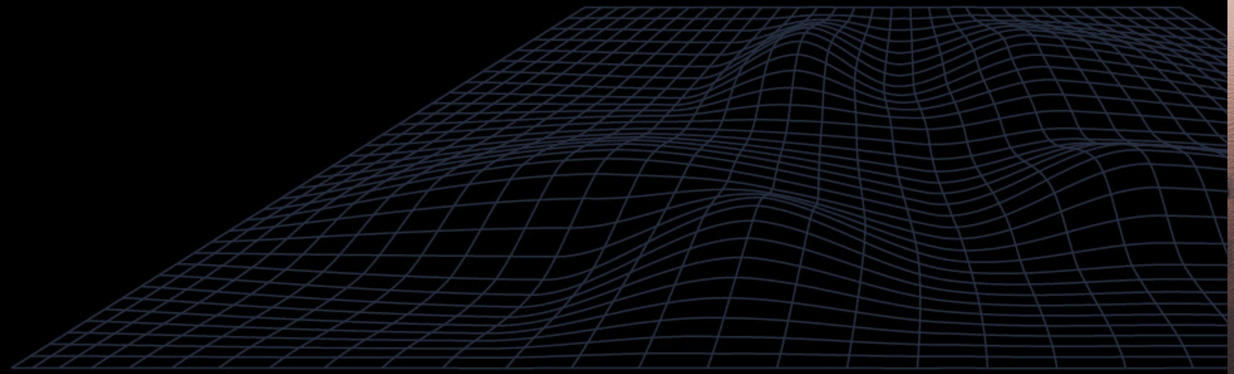
The Evolution of Chinese Smishing Syndicates and Digital Wallet Fraud

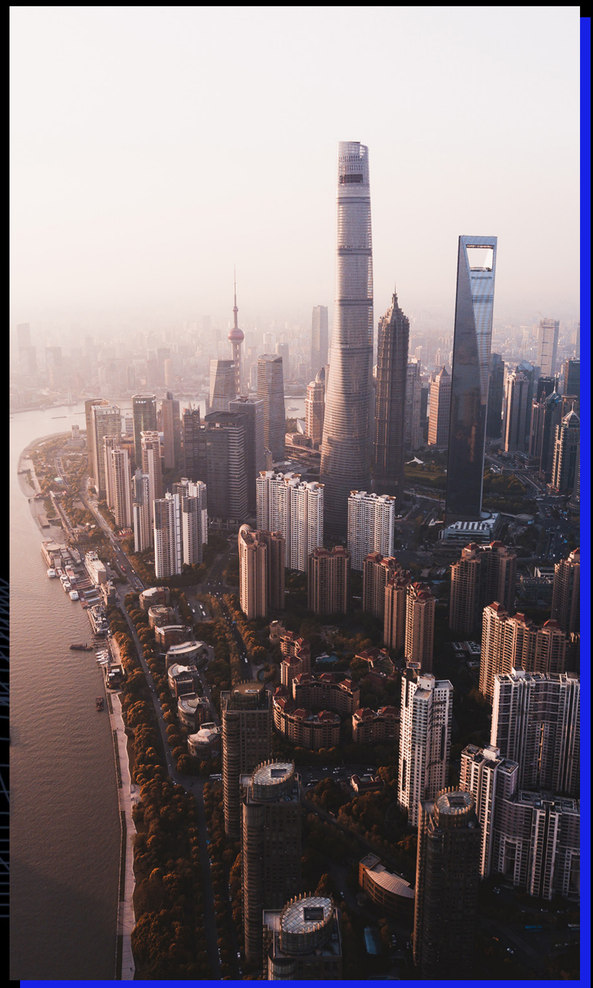
Contents

Executive Summary

This research presents an analysis of sophisticated smishing campaigns orchestrated by Chinese cybercriminal syndicates that have systematically targeted victims worldwide since early 2023. These operations represent a paradigm shift in payment card fraud, combining advanced SMS, RCS, and iMessage-based social engineering with sophisticated phishing infrastructure and real-time multi-factor authentication bypass techniques. The primary innovation lies in their strategic exploitation of digital wallet tokenization systems, particularly Apple Pay and Google Wallet, to circumvent traditional fraud detection mechanisms.

Our investigation reveals an extensive criminal ecosystem that may have compromised between 12.7 million and 115 million payment cards in the United States alone between July 2023 and October 2024, with estimated financial losses reaching into the billions of dollars. The research documents the operational evolution from simple package delivery scams to sophisticated phishing-as-a-service platforms, fake e-commerce operations, and most recently, brokerage account takeover schemes.



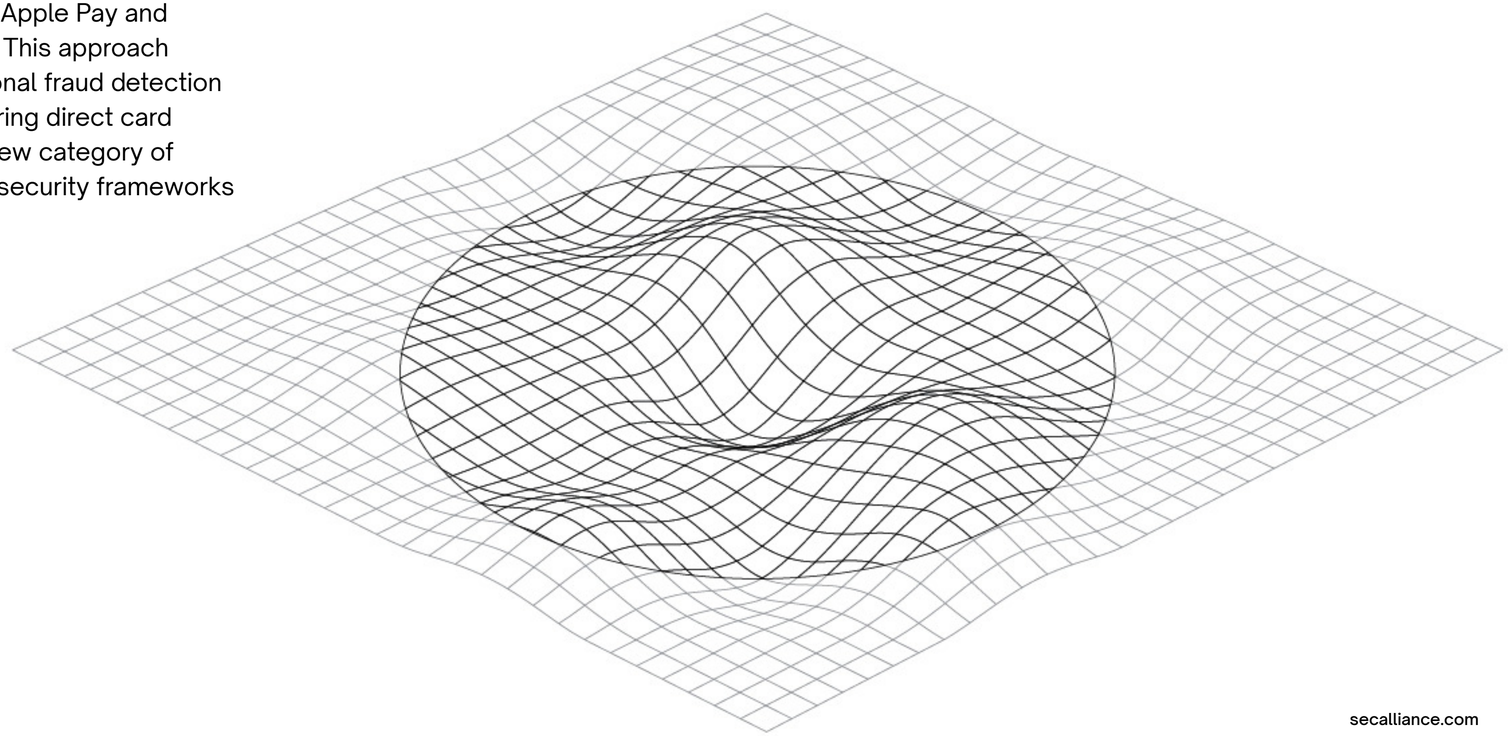


1. Introduction and Background

The landscape of SMS-based phishing attacks underwent a dramatic transformation in August 2023, marking the emergence of what we now believe is the most sophisticated and financially damaging smishing operation in recorded history. While SMS phishing has existed for years, and the COVID-19 pandemic initially created opportunities for package delivery scams targeting services like RoyalMail in the United Kingdom during 2020-2021, these early campaigns were relatively unsophisticated, short-lived, and didn't utilize digital wallet monetization.

The current wave of attacks, predominantly orchestrated by Chinese-speaking threat actors, represents a fundamental evolution in both technical sophistication and strategic approach. The defining characteristic of these operations is their deliberate and systematic exploitation of digital wallet provisioning processes, transforming stolen payment card credentials into tokenized assets within Apple Pay and Google Wallet ecosystems. This approach effectively bypasses traditional fraud detection systems that rely on monitoring direct card usage patterns, creating a new category of financial crime that existing security frameworks struggle to address.

Our investigation, spanning nearly two years of continuous monitoring and analysis, has uncovered a vast criminal infrastructure that operates with the efficiency and scalability of legitimate software-as-a-service businesses and whose implications extend far beyond individual financial losses.



2. Research Methodology and Data Sources

This investigation employed a multi-faceted research approach. Our methodology combined technical analysis of recovered phishing kits, further investigation of the phishing infrastructure, and analysis of advertising materials and tutorials created by the threat actors themselves.

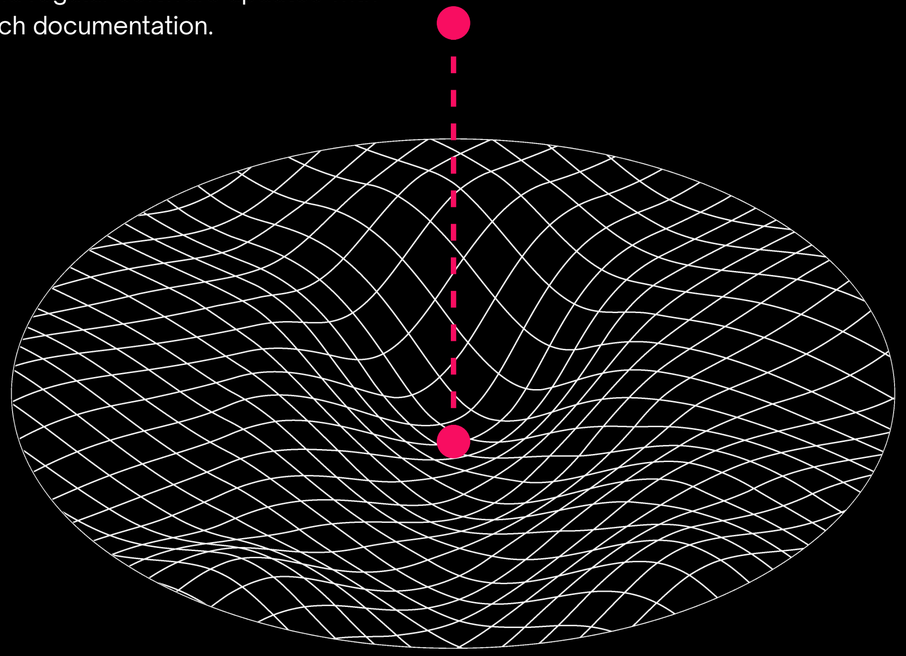
3. Primary Threat Actor Analysis: “Lao Wang”

Our investigation initially identified a Chinese-speaking developer operating under the pseudonym “Lao Wang,” or alternatively “Wang Duo Yu,” who appears to have established one of the first popular phishing-as-a-service operation with an integration to support digital wallet exploitation. Analysis of recovered phishing kit source code revealed extensive Chinese-language commentary and direct references to “Wang Duo Yu” within JavaScript files.

Further open-source intelligence analysis discovered advertisements for the service on Chinese-language forums, ultimately leading us to including the “dy_tongbu” Telegram channel operated by the same individual. This channel, established in February 2023, has evolved into a sophisticated marketplace for phishing services, demonstrating growth from approximately 2,800 members in August 2023 to over 4,400 members by early 2025.

Figure 1. *The dy_tongbu channel on Telegram where Lao Wang offers phishing kits, tuition, and guides.*

The channel operates exclusively in Chinese using mainland slang and serves as both a commercial platform and training center. The services ecosystem includes comprehensive ready-to-deploy subscription-based phishing kits targeting various brands priced at approximately $200 monthly, extensive educational resources including customization tutorials and operational guidance, and regular software updates with detailed patch documentation.



4. Technical Infrastructure and Attack Methodology

4.1 Phishing Kit Architecture

The phishing kits developed by these syndicates incorporate defensive capabilities. Geofencing mechanisms restrict access to targeted geographic regions, while mobile user-agent enforcement ensures that only mobile devices can interact with the phishing pages. We believe the mobile-user agent restriction serves two purposes, one to ensure that victims are being phished on the same mobile devices that will ultimately receive the OTP messages, and two to hinder security researchers from analyzing and categorizing these phishing pages.

The infrastructure also often employs IP blocking of known hosting providers, security vendor ranges, and Tor exit nodes, creating an additional layer of protection against detection and analysis. The distributed architecture separates front-end phishing interfaces from back-end data collection systems, providing resilience against takedown attempts. MySQL is used as a database to store victim data and configuration parameters.

```
$result = sql::$conn->query($sql);
if ($result->num_rows > 0) {
  header('location: https://usps.com/');
  exit;
}

$sql = "SELECT * FROM `config` LIMIT 1";
$result = sql::$conn->query($sql);
if ($result->num_rows <= 0) {
  header('HTTP/1.1 500 Forbidden');
  exit;
}
$res_arr = $result->fetch_array();
$country_whitelist = strtoupper($res_arr['country_whitelist']);
$allow_pc = (int)$res_arr['allow_pc'];
$is_tor = (int) $res_arr['is_tor'];
$is_ip_detection = (int) $res_arr['is_ip_detection'];

if ($allow_pc == 0) {
  if (!preg_match('/(phone|pad|pod|iPhone|iPod|ios|iPad|Android|Mobile|BlackBerry|IEMobile|MQQBrowser|JUC|Fennec|wOSBrowser|BrowserNG|WebOS|Symbian|Windows Phone)/i', $user_agent)) {
    header('location: https://usps.com/');
    exit;
  }
}
$country_whitelist_arr = $country_whitelist ? explode(',', $country_whitelist) : [];
$user_country_code = $checkData['location']['country']['code'];

if (count($country_whitelist_arr) && $user_country_code && !in_array($user_country_code, $country_whitelist_arr)) {
  header('location: https://usps.com/');
  exit;
}
$contype = $checkData["connection"]["type"];
$accepte_contype = ["cdn", "hosting", "education"];
if ($is_tor == 1) {
  if ($contype && in_array($contype, $accepte_contype)) {
    header('location: https://usps.com/');
```

Figure 2. *Part of the index.php file showing surveillance countermeasures such as geo-fencing and user-agent filtering from one of Lao Wang's original phishing kits "v1"*

4.2 Victim Targeting and Data Collection Process

Initial contact occurs through SMS, iMessage, or RCS messages employing social engineering lures related to package deliveries, toll road payments, tax refunds, vehicle registrations, or other urgent matters that require immediate attention.

Victims are directed to mobile-optimized phishing pages that have passed through the defensive filtering systems described above. The data collection process begins with personally identifiable information including full names, physical addresses, email addresses, and phone numbers, under the pretense of being required for service verification or delivery coordination.

The next step involves payment card information collection, typically justified by small fees for package redelivery, toll payments, or processing charges. The threat actors will enrich this card information using BIN (Bank Identification Number) databases to identify issuing banks and card types, as they will target specific banks based on several factors including the perceived value of the card and the strength of the bank's digital wallet security controls.

Finally, the phishing pages capture multi-factor authentication OTP codes from the victim, typically initiated when threat actors attempt to provision the stolen card information to digital wallets on attacker-controlled devices. This process requires sophisticated coordination between the attacker utilizing phishing infrastructure and the victim who will receive and enter the OTP code into the phishing page.

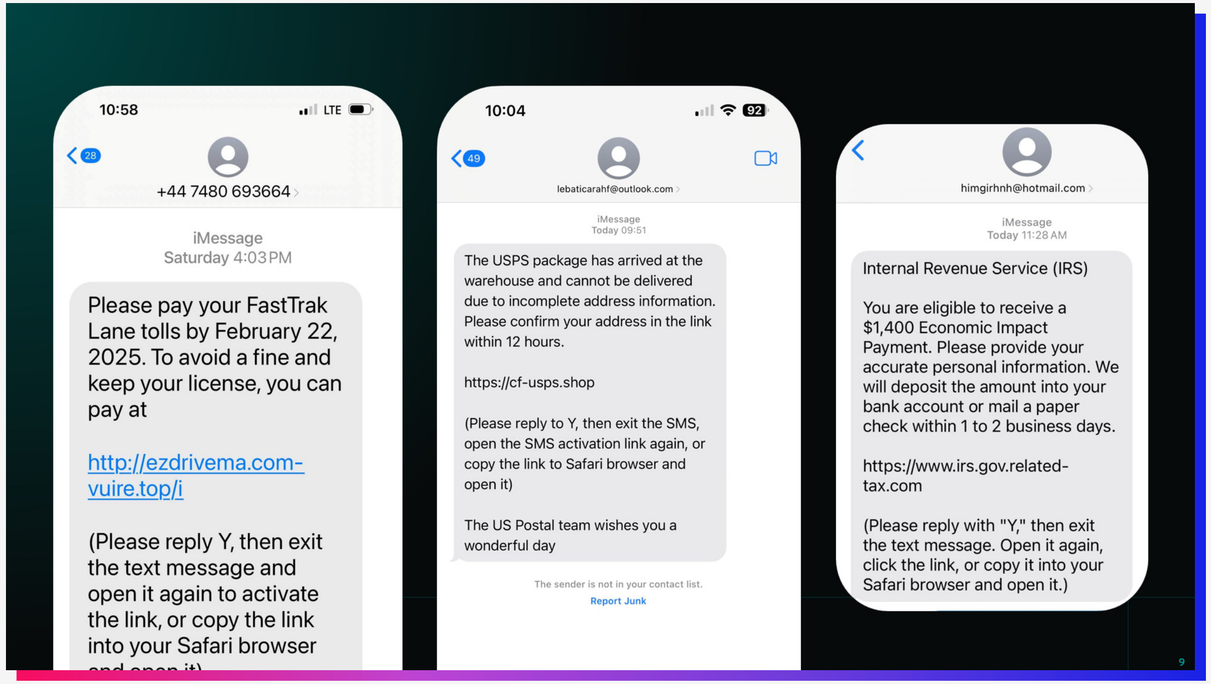


Figure 3. *Examples of common US based smishing lures. In these examples we see classic toll road, package redelivery, and tax refund/stimulus scams targeting American victims via iMessage.*

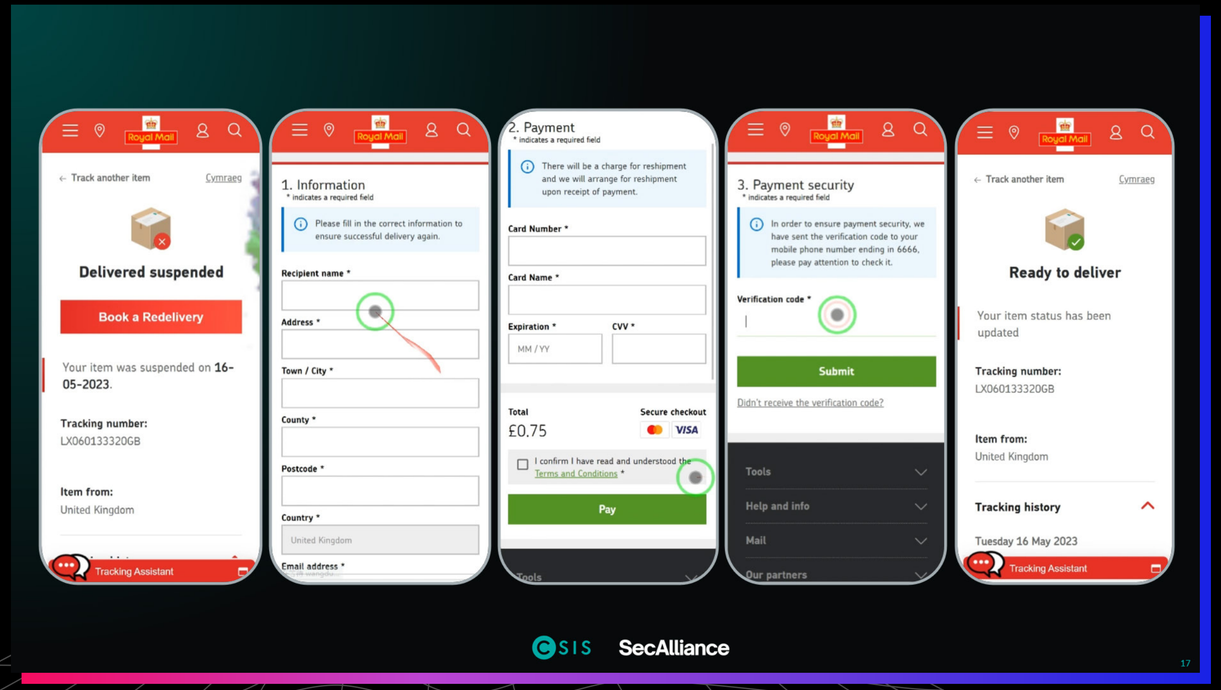


***Figure 4**. A RoyalMail example of the 5 stages of the phishing kits that a victim will go through, sourced from Lao Wang's own marketing videos in the dy_tongbu Telegram channel.*

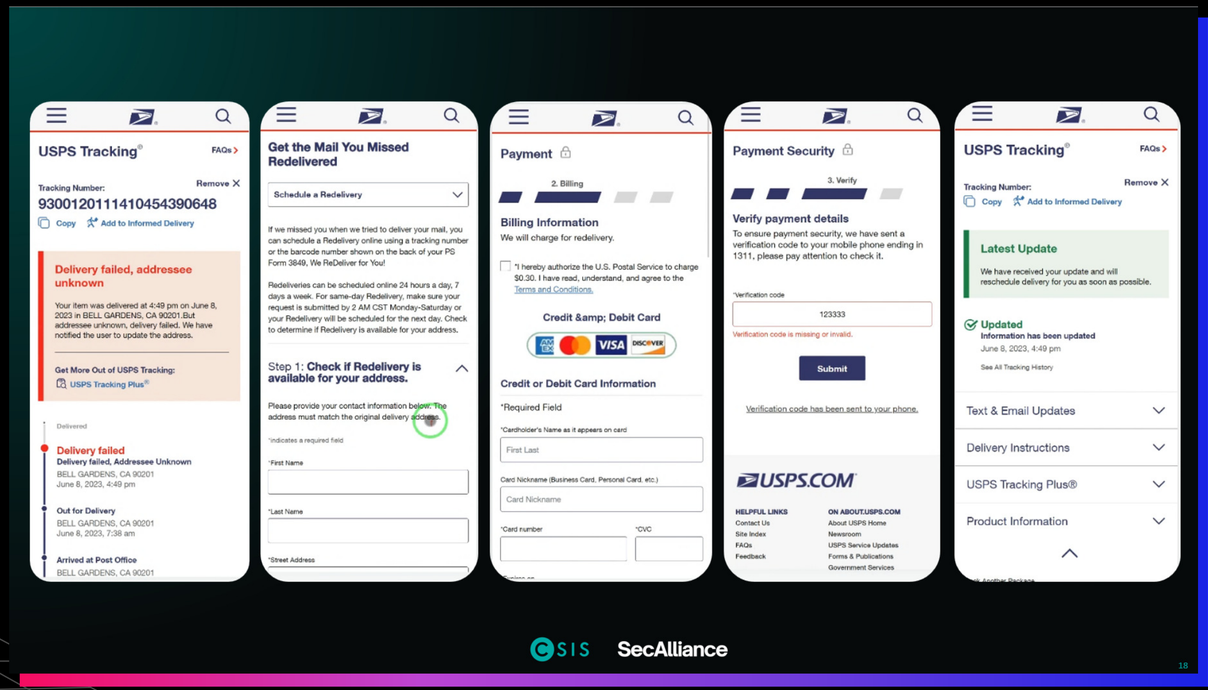


***Figure 5**. A USPS example of the 5 stages of the phishing kits that a victim will go through, sourced from Lao Wang's own marketing videos in the dy_tongbu Telegram channel.*

4.3 Evolution from “v1” to the “Lighthouse” Platform

August 2024 marked a significant technological advancement with the introduction by Lao Wang of the “Lighthouse” platform, representing a huge leap in phishing kit sophistication and operational capability. This platform features a unified back-end architecture with modular front-end components that enable rapid deployment across multiple brand targets without requiring painful code refactors.

The administrative interface of Lighthouse now supports multiple languages including Chinese, English, and Russian, indicating the global scope of operations and the diversity of customers. The platform provides comprehensive support for all major multi-factor authentication bypass techniques, including traditional SMS-based one-time passwords, time-based authentication tokens, email-based verification links, mobile application authentication, PIN code verification, and even card CVV codes used as secondary authentication factors.

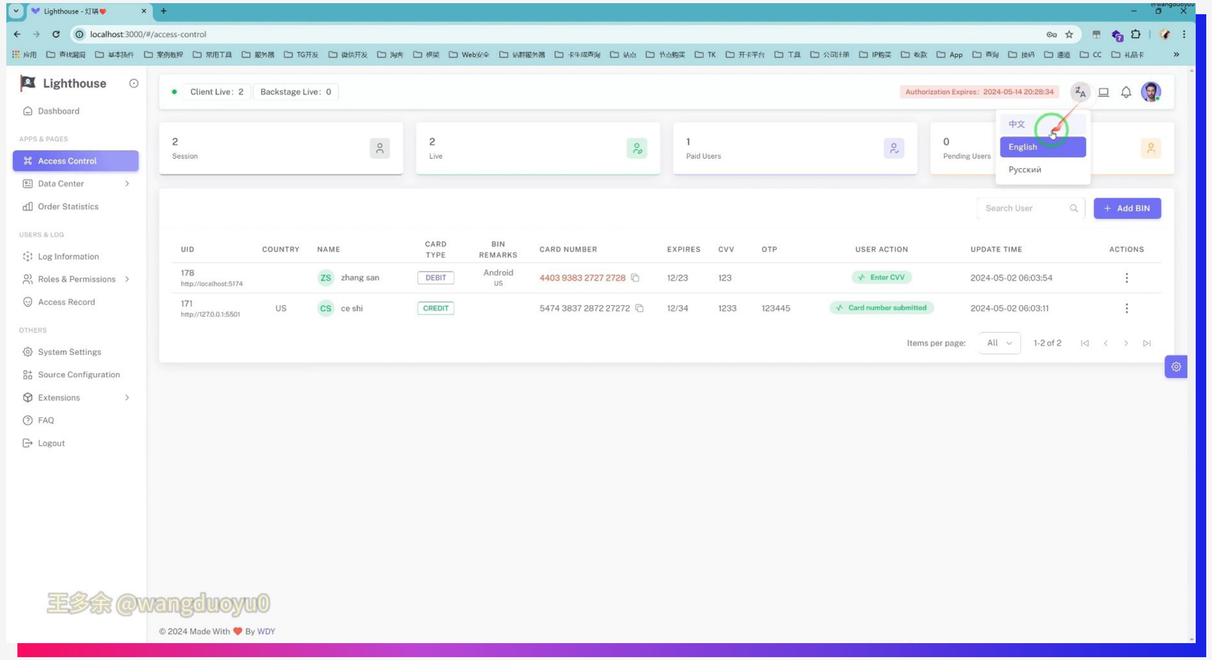


Figure 6. *A screenshot of the Lighthouse administrative backend interface from Lao Wang’s own marketing videos in the dy_tongbu Telegram channel.*

Technical enhancements include an integrated Bank Identification Number database that enables real-time card issuer enrichment, providing operators with immediate intelligence about card types and issuing banks (without needing to use an external BIN checking service or API). Role-based access control systems enable the platform to function as a true software-as-a-service offering, with detailed logging and audit capabilities that support reselling the platform.

The platform integration with WordPress and WooCommerce utilizing custom plugins represents a strategic expansion into fake e-commerce shops, while real-time data exfiltration via AJAX enables keystroke capture and immediate data transmission. These capabilities enabled rapid scaling from 17 supported brands in a handful of countries in the earlier “v1” kit to over 80 countries within months of deployment.

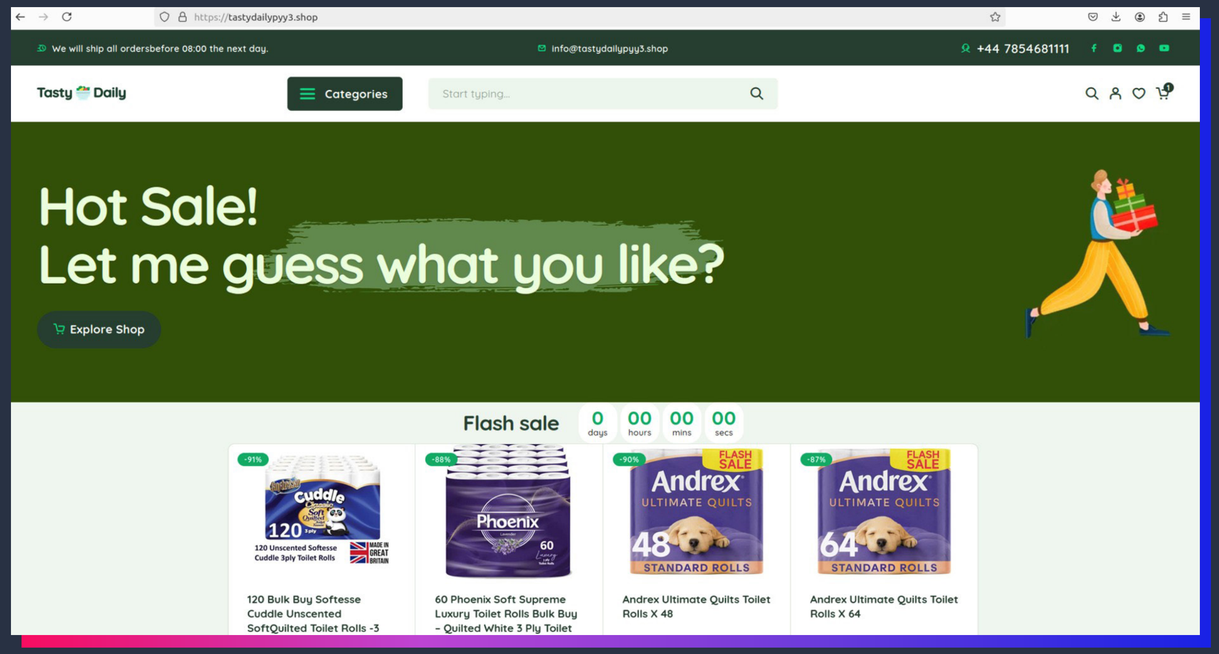


Figure 7. *A screenshot of a fake shop using the Lighthouse backend selling Toilet Paper and primarily targeting UK victims in late 2024.*

5. Digital Wallet Exploitation

The defining characteristic of these modern smishing operations lies in their strategic exploitation of digital wallet tokenization systems, representing a fundamental shift in payment card fraud methodology. Traditional card not present fraud relies on direct use of stolen card numbers, creating transaction patterns that existing fraud detection systems are designed to identify and prevent. Digital wallet tokenization creates an entirely different threat landscape that existing security frameworks struggle to address effectively.

Once threat actors successfully harvest payment card credentials through their phishing operations, they immediately provision these cards to digital wallets on attacker-controlled devices. This process creates several strategic advantages that traditional card fraud cannot achieve. Primary among these is the elimination of additional authentication requirements for individual transactions, as the initial provisioning process validates the card holder's identity through the multi-factor authentication bypass.

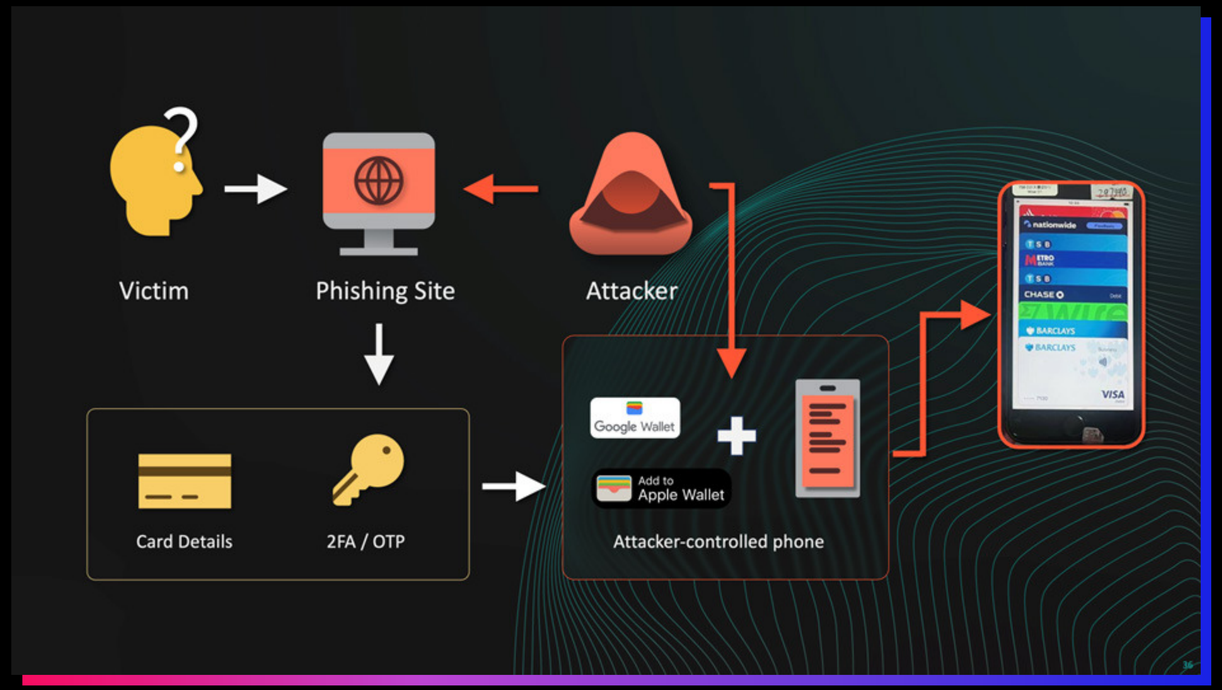


Figure 8. *A visual illustration of how threat actors use the captured card details and OTP to add victim cards to Apple Pay or Google Wallet on malicious devices.*

The monetization opportunities created by this approach are extensive. Contactless payments at physical point-of-sale terminals enable purchases via legitimate retail channels. Online purchases through applications that support digital wallet payments provide access to further goods and services. In some locations, tap-to-pay ATM withdrawals provide direct cash access without requiring physical card possession.

5.1 Device Management Strategies

Our research has identified device management strategies that demonstrate these operators' deep understanding of fraud detection systems and digital wallet provisioning policies. Initial operations showed a strong preference for older iPhone models, particularly the iPhone 6, 7, and 8 series, likely due to reduced security features and lower cost of acquisition for criminal operations.

Card provisioning strategies vary significantly based on target demographics and regional characteristics. For United States victims, operators typically provision 4 to 7 cards per device, while United Kingdom victims see 7 to 10 cards provisioned per device. These differences likely reflect variations in digital wallet provisioning controls and regional patterns that operators have identified through their operational experience.

The temporal aspects of these operations demonstrate remarkable sophistication and patience. Early operations employed waiting periods of 60 to 90 days between card provisioning and initial fraudulent use, likely designed to avoid triggering fraud detection systems that monitor unusual activity immediately following card provisioning. More recent operations have reduced this window to 2 to 10 days, suggesting an increased demand for rapid monetization.

When fraudulent activity begins, it typically follows a high-velocity pattern with multiple transactions occurring in rapid succession. This approach maximizes extraction before traditional fraud reporting systems or victim reports prevent further use.

5.2 Comprehensive Monetization Ecosystem

The monetization strategies employed by these syndicates demonstrate a sophisticated understanding of the digital payment ecosystem and exploit multiple vectors for converting stolen cards into usable assets. The creation of malicious merchant accounts with legitimate payment processors including Stripe, PayPal, HitPay, and Flutterwave enables operators to process fraudulent transactions through seemingly legitimate channels.

Physical point-of-sale terminal laundering represents another sophisticated monetization vector. Operators acquire legitimate business payment terminals and use them to process fraudulent invoices using contactless payments from provisioned digital wallets.

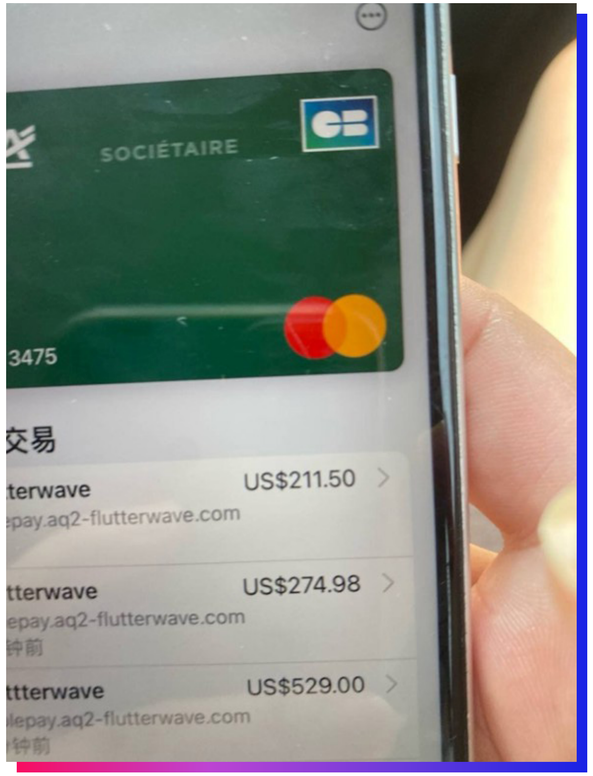


Figure 9. *A screenshot shared on a Chinese-speaking phishing Telegram group showing successful transactions against a tokenized Credit Agricole MasterCard using the Flutterwave merchant API.*

Figure 10. *An image sourced from Chinese-speaking phishing Telegram groups where an actor is advertising the ability to cash out stolen digital wallet provisioned cards via physical POS tap-to-pay terminals, along with around 100-120 phones.*

The criminal ecosystem has evolved to include wholesale operations that sell pre-provisioned devices loaded with multiple stolen cards. These operations typically require minimum orders of 10 devices or more and will ship the devices to their customers via air freight, indicating both the scale of the criminal infrastructure and the existence of downstream criminal networks that specialize in monetizing provisioned cards on devices.

NFC relay attacks represent a particularly sophisticated monetization technique that enables global usage of provisioned cards via a mule at the physical merchant location, effectively eliminating geographic constraints on fraudulent activity.

Further, PayPal account takeover operations demonstrate the versatility of these criminal networks and their ability to adapt existing techniques to new platforms. By compromising PayPal accounts and subsequently provisioning stolen cards to PayPal's digital wallet functionality, operators can conduct fraudulent activities without requiring physical devices for provisioning.

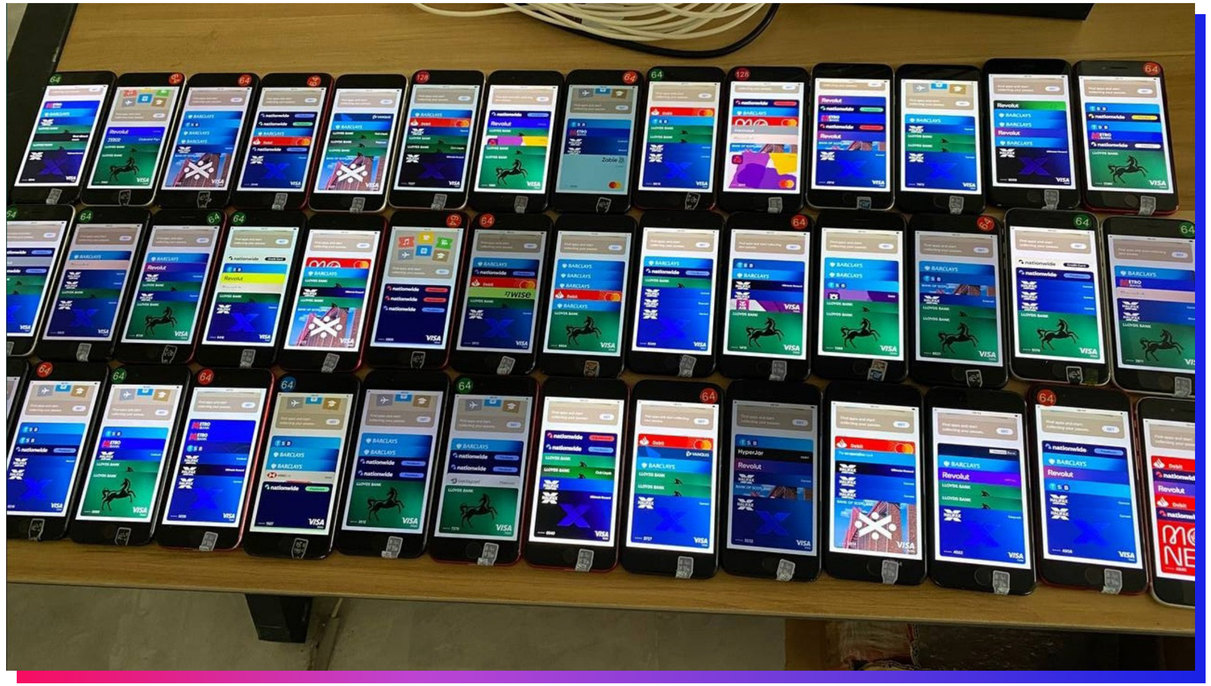


Figure 11. *A spread of older iPhones with stolen credit cards added to Apple Pay and offered for sale in a Chinese-speaking phishing Telegram group.*

6. Market Expansion and Major Threat Actors

While Lao Wang established the one of the first successful digital wallet-focused smishing platforms, the success of this approach has spawned a diverse ecosystem of threat actors, each contributing unique capabilities and targeting different market segments.

Chen Lun, operating under the aliases Sinking or Sinkinto, represents a significant evolution in the threat landscape. Intelligence suggests she initially trained under Lao Wang and was referenced as “The Young Lady” before establishing independent operations with a particular focus on European markets.

PepsiDog, also known as Xiū Gǒu, operates one of the more technically sophisticated platforms observed in our research. This actor employs Git branching methodologies to rapidly switch between different target brands and makes extensive use of GitHub infrastructure for operational management. This actor targets Japanese and European victims extensively.

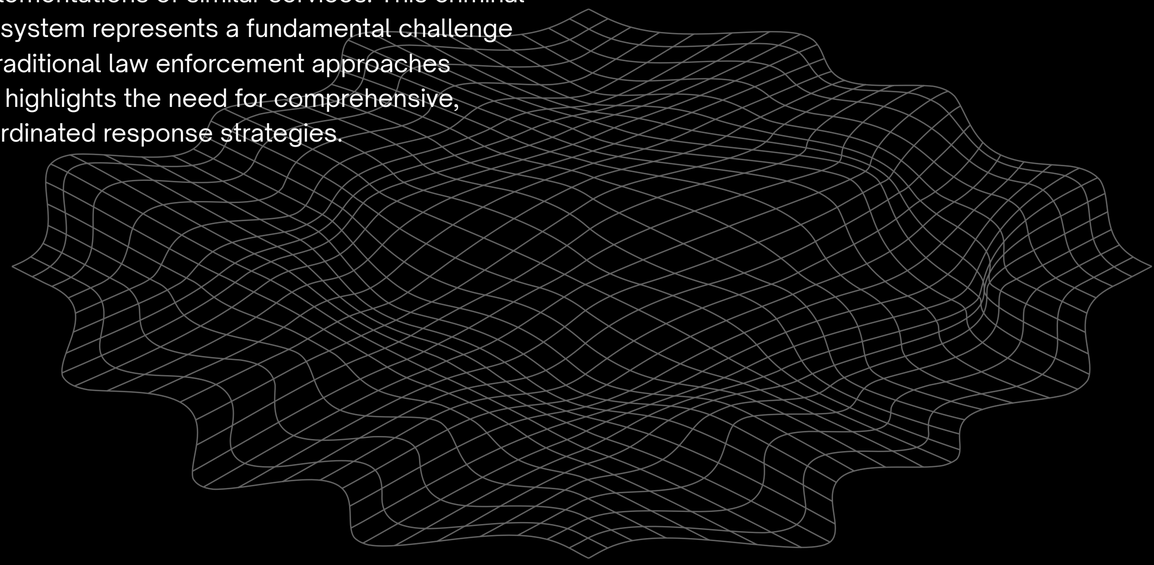
Darcula, whose phishing kit is also known as Magic Cat, appears to operate the most extensive infrastructure in the current threat landscape. With support for over 300 brands across nearly every country globally, this actor is responsible for an estimated 80 to 90 percent of smishing URLs we observed during late 2024 and early 2025.

XinXin, operating under the Lucid brand, provides another sophisticated phishing-as-a-service platform with global targeting capabilities and an extensive portfolio of targeted brands.

Panda Shop represents an interesting evolution in service delivery, making extensive use of Telegram bot automation to provide phishing-as-a-service capabilities to customers. This approach reduces operational overhead while maintaining service quality, indicating the continued evolution of these criminal business models.

Mouse, also known as Haozi, rounds out the major players with sophisticated phishing kits and broad brand targeting. The diversity of major actors, each with distinct operational characteristics and target preferences, indicates a mature criminal ecosystem with specialization and market segmentation.

Beyond these major operators, our research indicates the existence of hundreds, potentially thousands, of smaller operators who provide derivative services, direct copies, or specialized implementations of similar services. This criminal ecosystem represents a fundamental challenge to traditional law enforcement approaches and highlights the need for comprehensive, coordinated response strategies.



7. Impact Assessment and Scale

Quantifying the full impact of these sophisticated criminal operations presents significant methodological challenges due to the distributed nature of the infrastructure and the limited availability of comprehensive victim data. However, based on research conducted by independent security researchers and our own analysis of domain activity patterns, we can develop reasonable estimates for the scope of compromise.

Our analysis incorporates data from Grant Smith's comprehensive research, which identified 438,669 distinct compromised cards across 1,113 domains, yielding an average of 387 cards per domain. Additionally, Resecurity's research from August 31, 2023, documented 108,044 compromised cards across 31 domains, resulting in a significantly higher average of 3,485 cards per domain. The variation in these ratios likely reflects differences in operational sophistication, target selection, and campaign duration.

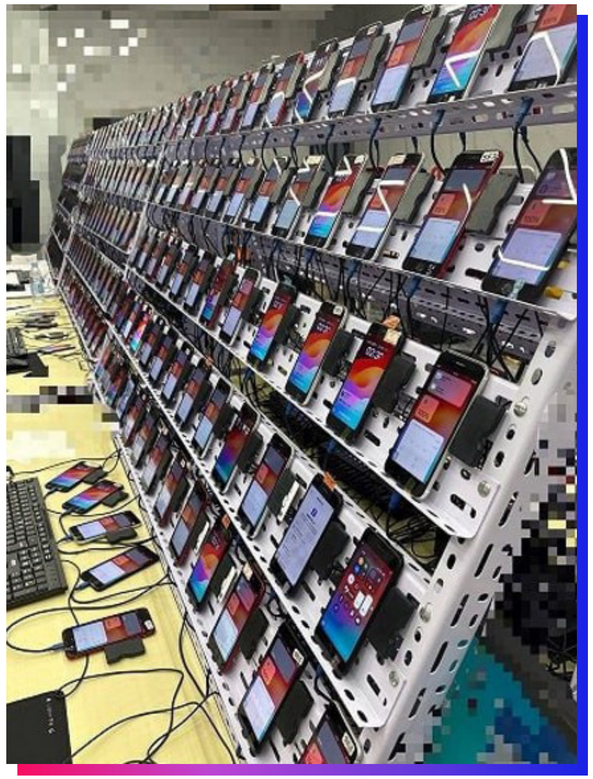


Figure 12. *A rack of phones with attached SIM card tray adapters, shared in a Chinese-speaking Telegram group related to SMS, RCS, and iMessage spam.*

Applying these ratios to the 32,094 distinct USPS-themed smishing domains identified during our monitoring period between July 2023 and October 2024, we estimate that between 12.7 million and 115 million distinct payment cards may have been compromised in the United States alone. This range reflects the uncertainty inherent in extrapolating from limited data sets, but even the lower bound represents an unprecedented scale of payment card compromise.

The financial implications of this scale of compromise extend far beyond direct fraudulent transactions. The costs associated with card replacement, fraud investigation, customer notification, and remediation create additional financial burdens for financial institutions. We acknowledge that the error bars for these estimates are extremely large, and the availability of additional comprehensive victimization data would improve the accuracy of impact assessments.

8. Evolution into Fake E-Commerce Operations

August 2024 marked another significant evolution in these criminal operations with the emergence of fake e-commerce websites that represent a fundamental shift in victim targeting methodology. Unlike traditional smishing campaigns that rely on unsolicited messages to drive traffic, these fake shopping operations target users who are actively seeking products and services through apparently legitimate channels.

These operations demonstrate remarkable technical sophistication by utilizing genuine WordPress and WooCommerce installations, creating websites that are functionally identical to legitimate e-commerce platforms. The critical difference lies in the payment processing integration, where the Lighthouse platform replaces legitimate payment processors such as PayPal, Stripe, or traditional merchant services.

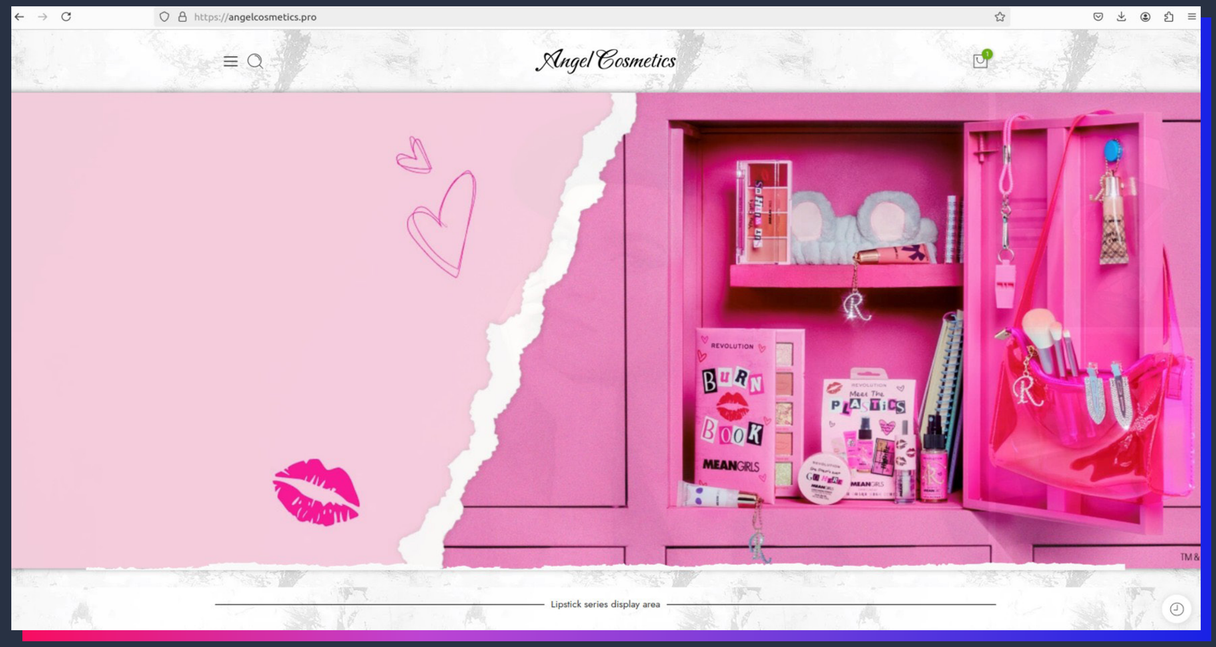


Figure 13. *A fake shop using the Lighthouse backend that targeted UK victims in late 2024, purportedly selling legitimate cosmetic products from Angle Cosmetics*

The advertising strategy for these fake shops demonstrates significant financial investment and operational sophistication. The operators purchase advertising space on major platforms including Meta, TikTok, and Google, reaching potential victims through the same channels used by legitimate businesses. The product catalogs feature seemingly legitimate items including cleaning supplies, cosmetics, electronics, and other consumer goods, complete with professional product photography and descriptions.

The checkout process appears entirely legitimate even during the final payment stage, where the Lighthouse platform captures payment card details, personally identifiable information, and conducts real-time multi-factor authentication bypass exactly as in package redelivery and toll-road smishing operations. Additional functionality via a custom module can also target PayPal credentials, enabling PayPal account takeover and expanding the scope of compromise beyond payment card theft.

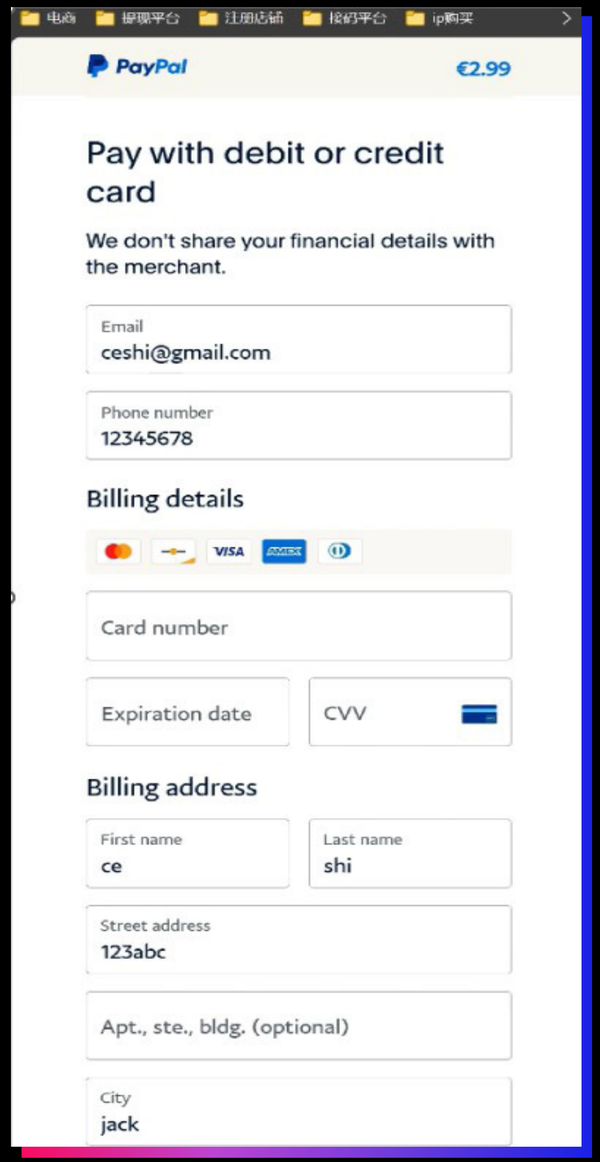


Figure 14. *An example of the checkout page on a fake shop using Lighthouse. The PayPal theming, look and feel, and animation is nearly identical to the real PayPal*

This evolution represents a particularly insidious threat because it fundamentally undermines traditional user education approaches. Standard security guidance advises users to avoid suspicious messages and unsolicited communications, but these fake e-commerce operations target users who are intentionally seeking products through channels they perceive as legitimate. The professional presentation and legitimate advertising channels create a false sense of security that makes detection extremely difficult for ordinary consumers.

9. Recent Expansion into Financial Services

The most recent evolution in these criminal operations, observed in May 2025, represents an expansion into financial services with specific targeting of major global brokerage firms. This development indicates the continued sophistication and adaptability of these criminal networks as they identify new opportunities for monetization.

The brokerage-focused phishing pages appear designed to facilitate account takeovers rather than card theft. We believe the actors may be targeting these accounts for use with two distinct monetization strategies. The first approach involves direct fund exfiltration through wire transfers, leveraging compromised account credentials to authorize large-value transfers to accounts controlled by the threat actors. This approach is likely less successful today due to brokerages implementing significant security controls around outbound wire transfers.

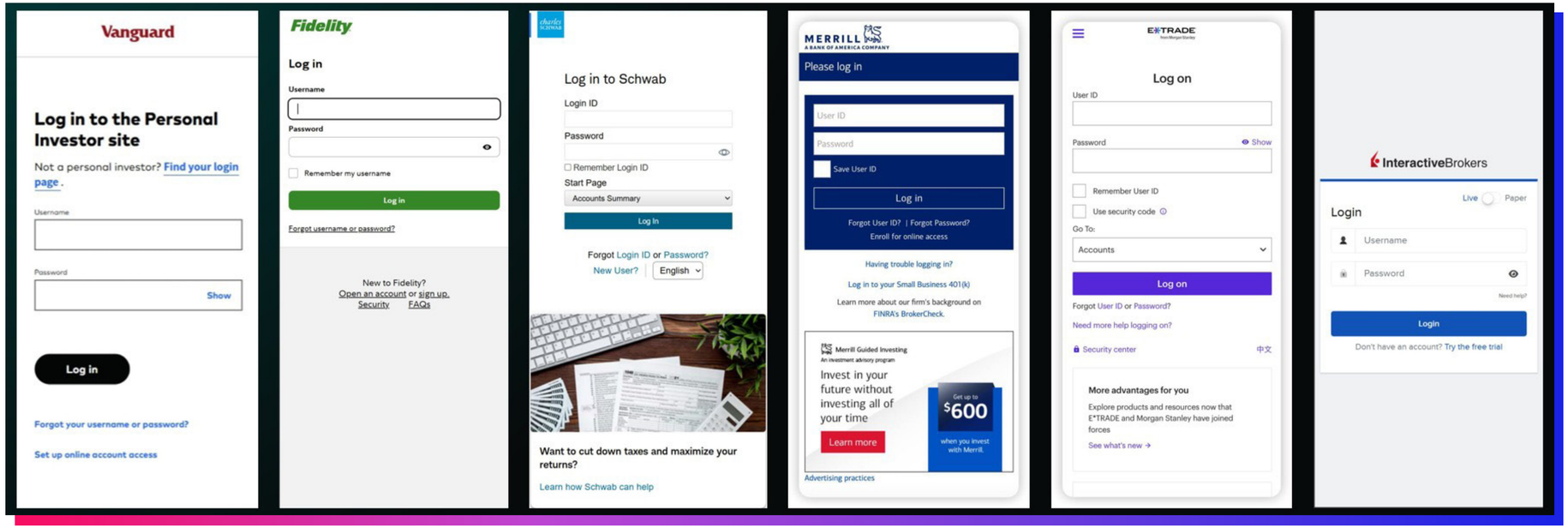


Figure 15. *An updated set of screenshots from Lao Wang showing Lighthouse support for phishing various brokerages*

The second approach represents an innovative adaptation of traditional pump-and-dump schemes to the digital age. Compromised brokerage accounts are used to liquidate existing holdings and purchase penny stocks or newly listed IPOs that are simultaneously held in accounts controlled by threat actors through separate brokerage relationships. This approach enables market manipulation while obscuring the connection between the original account compromise and the ultimate beneficiaries of fraudulent activity.

Both Darcula and Lighthouse platforms have integrated support for these brokerages, suggesting that this expansion represents a strategic priority for their customers.

10. Recommendations for Industry Response

10.1 Digital Wallet Security Enhancement

The fundamental security challenge posed by these operations requires comprehensive reform of digital wallet provisioning processes. Financial institutions, in partnership with major technology companies such as Apple and Google, must develop significantly enhanced capabilities for ingesting, tracking, and investigating digital wallet provisioning and transaction data. This includes implementing real-time monitoring systems that can identify suspicious provisioning patterns and flag potentially compromised cards before fraudulent activity begins.

The provisioning process itself requires additional security layers that go beyond traditional authentication mechanisms. Current systems rely heavily on SMS-based one-time passwords that these criminal organizations have demonstrated the ability to bypass systematically. Implementation of application-based authentication methods that clearly communicate the specific action being authorized would significantly improve security while maintaining user experience.

Device binding represents another security enhancement that would require users to have their financial institution's official mobile banking application installed on the same device attempting to provision a payment card and authorize the card add from the application on the same device. This approach would create an additional hurdle for attackers and provide institutions with enhanced visibility.

10.2 Cross-Industry Collaboration Framework

The sophisticated and distributed nature of these criminal operations requires a coordinated response that extends beyond individual organizational capabilities. Cross-industry collaboration cooperation remains essential, with organizations sharing information about emerging threats to identify patterns that may not be visible to individual organizations.

10.3 Consumer Education and Protection

Financial institutions should implement proactive monitoring and alert systems that notify customers immediately when their payment cards are provisioned to digital wallets, regardless of whether the provisioning appears legitimate. Further enhancements, such as the ability for customers to see all devices on which cards are provisioned, revoke provisioning on specific devices, and enact a "provisioning freeze" that would prevent any new provisioning attempts without explicit customer deactivation of the freeze (like a credit freeze) would significantly enhance consumer protection.

11. Conclusion

The sophisticated smishing operations orchestrated by Chinese-speaking criminal syndicates over the past two years represent a paradigm shift in payment card fraud that has fundamental implications for digital payment security globally. The strategic exploitation of digital wallet tokenization has created a new category of financial crime that bypasses traditional security controls and challenges existing fraud detection methodologies.

The continuous evolution of these operations, from simple package delivery scams to sophisticated phishing-as-a-service platforms, fake e-commerce websites, and financial services targeting, demonstrates the remarkable adaptability and technical sophistication of these criminal organizations. The estimated compromise of 12.7 to 115 million payment cards in the United States alone represents an unprecedented scale of financial crime with implications that extend far beyond direct monetary losses.

The response to these threats requires coordinated action across multiple stakeholders, including financial institutions, technology companies, telecommunications providers, and law enforcement agencies. Traditional approaches to fraud prevention are insufficient to address the sophisticated techniques employed by these criminal organizations, necessitating the development of new security frameworks specifically designed to address the unique challenges of digital wallet fraud.

Apple, Google, and financial institutions must prioritize the development of enhanced digital wallet security capabilities, including improved provisioning verification, real-time transaction monitoring, and comprehensive fraud detection systems designed specifically for tokenized payment environments. The failure to address these vulnerabilities effectively will likely result in continued growth of these criminal operations and increasing financial losses.

This research highlights the urgent need for continued investigation into these operations and enhanced collaboration between industry stakeholders. The sophistication and scale of these criminal operations represent one of the most significant challenges facing digital payment security today.

Acknowledgments

This research was conducted by SecAlliance, a CSIS Security Group company. We also acknowledge the valuable contributions of other security researchers whose work has provided critical insights into the scope and impact of these criminal operations.

References and Further Reading

- Resecurity. “Smishing Triad Targeted USPS and US Citizens for Data Theft.” Available at: https://www.resecurity.com/blog/article/smishing-triad-targeted-usps-and-us-citizens-for-data-theft
- Smith, Grant. “Hacking the Scammers: An Investigation into Cybercriminal Infrastructure.” Available at: https://blog.smithsecurity.biz/hacking-the-scammers
- Smith, Grant. “Systematic Destruction: Advanced Techniques in Criminal Infrastructure Analysis.” Available at: https://blog.smithsecurity.biz/systematic-destruction-hacking-the-scammers-pt.-2
- Smith, Grant (S1nn3r). “Smishing Smackdown: Unraveling the Threads of USPS Smishing and Fighting Back.” DEF CON 32 Presentation. Available at: https://www.youtube.com/watch?v=gLOv67LlIQs
- Netcraft. “Every Doggo Has Its Day: Unleashing the Xiū Gǒu Phishing Kit.” Available at: https://www.netcraft.com/blog/doggo-threat-actor-analysis
- ProDaft. “Lucid: Advanced Persistent Phishing Operations Analysis.” Available at: https://catalyst.prodaft.com/public/report/lucid/overview

SecAlliance

Part of CSIS Security Group

7th Floor, One Canada Square,
London, E14 5AA, United Kingdom.

+44 (0) 20 7148 7475

info@secalliance.com

@secalliance

www.secalliance.com