SILENT PUSH

SMISHING TRIAD

CHINESE ECRIME GROUP TARGETS 121+ COUNTRIES, INTROS NEW BANKING PHISHING KIT

TABLE OF CONTENTS

KEY FINDINGS

- Smishing Triad, a Chinese eCrime group, has systematically targeted organizations in at least 121 countries across numerous industries, including postal, logistics, telecommunications, transportation, finance, retail, and public sectors, with SMS phishing "smishing" campaigns.
- Silent Push analysts have acquired Smishing Triad server log data and determined that portions of the group's infrastructure generated over one million page visits within a period of only 20 days, averaging 50,000 per day. Based on this data, we believe the actual number of messages sent may be significantly higher than the current public estimates of 100,000 SMS messages sent per day.
- On March 18, 2025, the developer behind the phishing kit used by Smishing Triad released a new Telegram channel detailing his new "Lighthouse" kit. Details suggest that sophisticated bank phishing efforts are being set up, with the initial phishing kit targeting major Western financial organizations and banks in Australia, as well as the broader Asia-Pacific (APAC) region.
- Smishing Triad boasts it has "300+ front desk staff worldwide" supporting the Lighthouse kit. The staff is apparently used to support various aspects of the fraud and cash-out schemes. Smishing Triad continues to sell its phishing kits to other threat actors via Telegram and likely other channels.
- Domains used by Smishing Triad are rotated frequently. Silent Push researchers have seen approximately 25,000 domains online during any 8-day period—and expect to see tens of thousands of the group's websites live on any given day. More than half of phishing sites were hosted by two Chinese hosting companies: Tencent (AS132203) and Alibaba (AS45102).

EXECUTIVE SUMMARY

Smishing Triad is an advanced e-crime group from China that has been in operation since 2023, with criminal affiliate partners operating in multiple countries. Silent Push has found evidence of this group, known primarily for its SMS phishing ("smishing") campaigns that use postal delivery and government services as lures. These campaigns have targeted at least 121 countries and numerous industries with up to 100,000 texts daily.

In a new twist first seen in March 2025, Silent Push has discovered Smishing Triad appears to be working on new phishing kits focused on banks and financial organizations. The kits were initially focused on Australian financial institutions, but several major global financial brands have also been included.

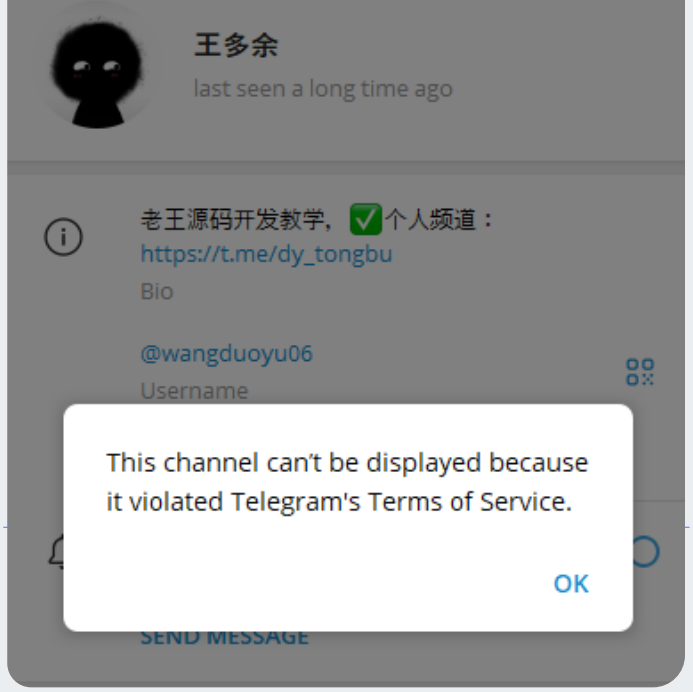
Smishing Triad is also selling its phishing kits to other maliciously aligned threat actors via Telegram and likely other channels. These sales make it difficult to attribute the kits to any one subgroup, so the sites are currently all attributed here under the Smishing Triad umbrella. As of this writing, Silent Push Threat Analysts have seen roughly 25,000 Smishing Triad domains in use within the last 8 days, and currently over 90,000 domains across the observed lifetime of this campaign.

BACKGROUND

Resecurity first wrote about the "Smishing Triad" in August 2023, with a substantial follow-up in August 2024. Their research helped provide context that this SMS phishing campaign was targeting multiple countries. It initially used compromised Apple iCloud accounts to send spam over iMessage and then later used local phone numbers. Resecurity confirmed that the SMS phishing kit was being sold to other threat actors, and they were able to acquire details to map 36 domains being used for the attacks.

In October 2023, Krebs on Security reported that a phishing campaign was targeting USPS and 12 other national postal services. These included services in Australia, Ireland, Spain, Costa Rica, Chile, Mexico, Italy, Netherlands, Denmark, Norway, Sweden, and Finland. This phishing effort appeared to be an early Smishing Triad campaign.

In 2024, security researcher Grant Smith hunted the same threat actors due to them scamming his wife with one of the USPS package scams, covered by Wired. Smith wrote up his efforts to compromise their phishing kits. He confirmed the creator of the kit was someone named "王多余" (Wang Duo Yu) who used the Telegram account "wangduuoyu0" (t[.]me/wangduoyu06). The creator originally communicated with buyers on the t[.]me/dy_tongbu channel. It was later shut down by Telegram due to Terms of Service violations. Resecurity confirmed similar details.



Screenshot of the wangduoyu06 Telegram account, accessed March 2025

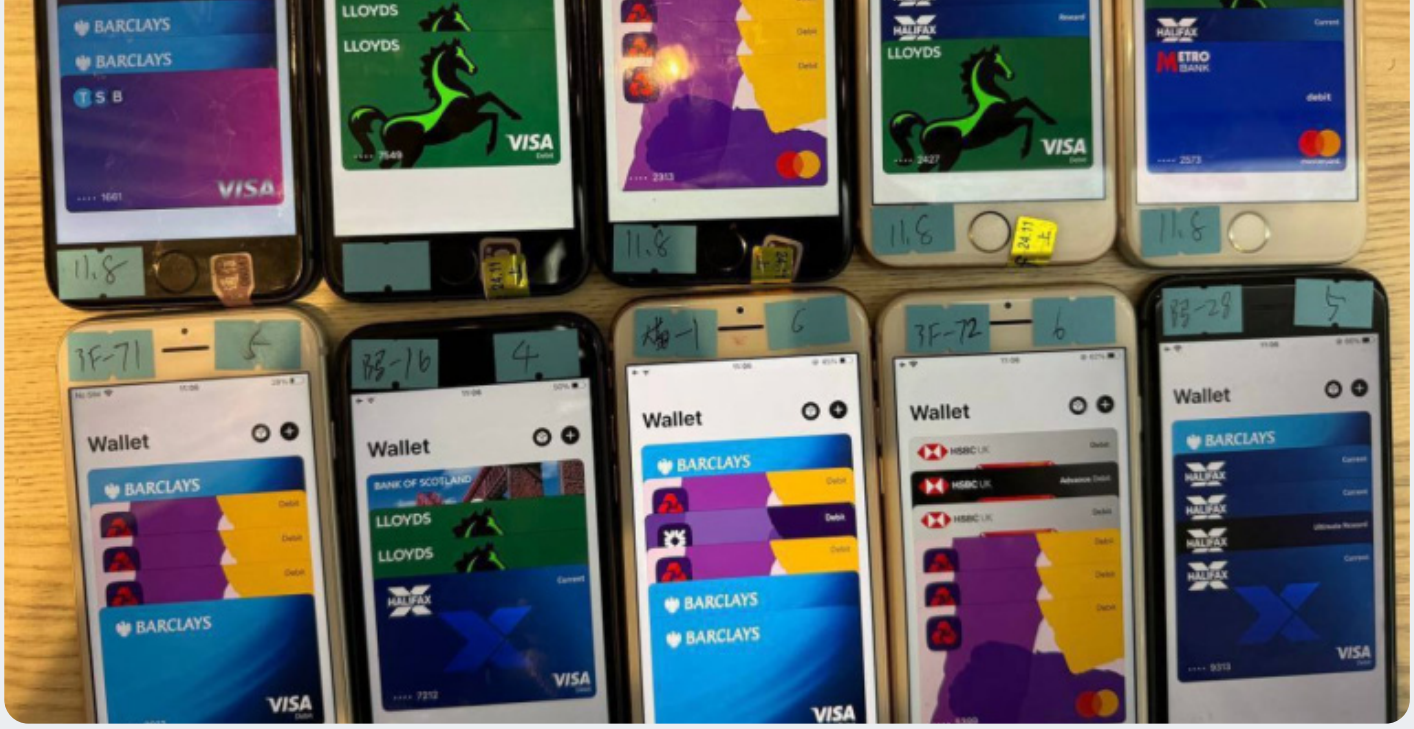
In April 2024, the FBI Internet Crime Complaint Center (IC3) noted it had received over 2,000 complaints about smishing texts related to fake toll road collection efforts, a primary lure from Smishing Triad.

In June 2024, the U.S. Postal Inspection Service issued a warning about package tracking text scams, reminding readers, "USPS utilizes the 5-digit short codes to send and receive SMS to and from mobile phones."

In July 2024, Fortinet released a blog on Smishing Triad and helpfully noted that Apple ID allows the use of third-party email addresses. This helped explain why many of the "email-to-SMS" examples we've seen don't use iCloud email addresses. The blog described the process: "We have observed third-party email addresses such as Hotmail, Gmail, or Yahoo being used in phishing emails on iMessage. Apple allows users to create an Apple ID using these third-party email addresses as the primary email associated with their Apple ID. Once the Apple ID is created and configured for iMessage, the sender can use that third-party email address to send messages through iMessage."

Following these initial reports, there have been hundreds of significant local news reports about smishing campaigns – the vast majority do not name "Smishing Triad," but they do mention toll road lures (aka E-ZPass phishing), USPS lures, and other government services that we've seen targeted via Smishing Triad domains.

In a new twist first seen in March 2025, Silent Push Threat discovered Smishing Triad appears to be working on new phishing kits to target banks and financial organizations. As mentioned in our key findings, these kits focus primarily on Australian and APAC-based financial institutions.



Telegram channel for a popular Chinese smishing kit vendor shows 10 mobile phones for sale, each loaded with 4-6 digital wallets from different U.K. financial institutions (Krebs article)

NEW BANKING FOCUS

In January 2025, Brian Krebs from Krebs on Security was the first to cover the new "Lighthouse" branding being used by the Smishing Triad phishing kit backend software, based on his tracking of its Telegram marketing.

In February 2025, Krebs continued his publishing on Smishing Triad and highlighted their cash-out schemes and new methods for loading stolen credit cards onto iPhone digital wallets in "How Phished Data Turns into Apple & Google Wallets." It's important to note that while images of devices found on Telegram being used in the attacks are exclusively Apple iPhones, this is just one of the cash-out schemes to load mobile Apple wallets with stolen credit cards, and is not an indication that only Apple devices are targeted.

On March 18, 2025, the developer behind the Smishing Triad phishing kit released a new Telegram channel about the creation of his new "Lighthouse" kit. Details allude to extremely sophisticated bank phishing efforts being set up. One video featured in the channel also included details of the USPS phishing template.

The new Lighthouse kit targets dozens of financial brands, many with a focus on Australia, including PayPal, Mastercard, Visa, Stripe, HSBC, Bendigo and Adelaide Bank, Bank of Sydney, Bank Australia, Bank of Queensland, Bank of Nova Scotia, Australia and New Zealand Banking Group, CitiGroup, Commonwealth Bank of Australia, Cuscal LTD, HSBC Bank Australia, ING Bank (Australia), National Australia Bank, Newcastle Permanent Building Society, Police Bank, George Bank, Westpac Banking Corporation, and Macquarie Bank.

SMISHING TRIAD TARGETING DIVERSE INDUSTRIES IN OVER 121 COUNTRIES

Smishing Triad has systematically targeted organizations in at least 121 countries across numerous industries, including postal, logistics, telecommunications, transportation, finance, retail, and public sectors.

Our team has constructed the extensive lists below to show the scope of targeting, including only those countries explicitly mentioned by name in a Smishing Triad domain. Some country codes in observed domains alluded to other countries, but have been left off until stronger confirmation is found.

With nearly two-thirds of all countries in the world targeted by Smishing Triad, it's safe to say they are essentially targeting every country with modern infrastructure outside of Iran, North Korea, and Russia. Our team has observed some potential targeting in Russia (such as domains that mentioned their country codes), but nothing definitive enough to indicate Russia is a persistent target.

Interestingly, even though these are Chinese threat actors, we have seen instances of targeting aimed at Macau and Hong Kong, both special administrative regions of China.

GEOGRAPHIC SCOPE INCLUDES 2/3 OF THE WORLD'S COUNTRIES

- **North America:** United States, Canada, Mexico, Guatemala, Costa Rica, Dominican Republic, Bahamas, Belize, Cuba, El Salvador, Honduras, Jamaica, Nicaragua, Panama, and St Lucia
- **South America:** Argentina, Brazil, Chile, Colombia, Ecuador, Peru, Uruguay, Bolivia, Guyana, Paraguay, and Venezuela
- **Europe:** Austria, Belarus, Belgium, Bulgaria, Croatia, Czech Republic, Finland, France, Germany, Greece, Ireland, Italy, Lithuania, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Spain, Switzerland, United Kingdom, Ukraine, Albania, Cyprus, Denmark, Estonia, Hungary, Kosovo, Latvia, Luxembourg, Macedonia, Malta, Monaco, Slovenia, Sweden
- **Middle East:** Egypt, Georgia, Israel, Kazakhstan, Libya, Saudi Arabia, Turkey, United Arab Emirates, Bahrain, Iraq, Jordan, Kuwait, Kyrgyzstan, Oman, Qatar, and Turkmenistan
- **Africa:** South Africa, Angola, Botswana, Congo, Ghana, Kenya, Mali, Mauritius, Morocco, Namibia, Nigeria, Seychelles, Togo, Tunisia, and Uganda
- **Asia-Pacific:** Australia, Hong Kong, India, Indonesia, Japan, Malaysia, China, New Zealand, Pakistan, Philippines, Singapore, Sri Lanka, Thailand, Armenia, Brunei, Cambodia, Fiji, South Korea, Laos, Maldives, Mongolia, Taiwan, and Vietnam

BROADLY TARGETED INDUSTRIES

- **Postal & Logistics:** National postal services, private couriers, and global shipping firms (USPS, Royal Mail, La Poste, DHL, FedEx, and UPS)
- **Telecommunications:** Providers in Thailand, Indonesia, Mexico, Guatemala, Malaysia, and the Dominican Republic
- **Transport & Toll Systems:** Electronic toll systems in California, Hong Kong, and Spain
- **Finance, Banking & Retail:** Banking institutions and multinational retail corporations
- **Government & Public Services:** Law enforcement, energy infrastructure (Tokyo Electric Power), and labor ministries

TARGETED BRANDS

Numerous organizations outside of the shipping, postal, and logistics industries are being targeted, with a secondary focus on toll road brands and financial organizations. These organizations include:

- CitiGroup, HSBC, Mastercard, Visa, PayPal, Stripe, Australia and New Zealand Banking Group, LATAM Airlines (South America), Commonwealth Bank of Australia, National Australia Bank, Westpac Banking Corporation, Claro Cloud (Latin America), ING Bank (Australia), Macquarie Bank, Bank of Nova Scotia, Dirección General de Tráfico (DGT) (Spain), East Nippon Expressway Company (E-NEXCO) (Japan), Maxis Telecom (Malaysia), Bendigo and Adelaide Bank, HSBC Bank Australia, Bank of Queensland, Dubai Police, Bank Australia, Bank of Sydney, Cuscal LTD, George Bank, Newcastle Permanent Building Society, Police Bank, Altice Dominican Republic (Dominican Republic), M360 SMS Send (Philippines), Airpaz (Indonesia), and Macau Pass (China)

DOZENS OF SHIPPING AND MAIL COMPANIES TARGETED

- **North America:** Amazon (U.S.), Bay Area FasTrak (California, U.S.), Canada Post, Correo El Salvador, Correos de Costa Rica, Correos de Guatemala (Guatemala Post), DHL (U.S.), Estafeta (Mexico), FedEx (U.S.), Telcel (Mexico), Telefónica México, The Toll Roads (California, U.S.), Tigo Guatemala, UPS (U.S.), and USPS (U.S.)
- **South America:** 4-72 Shipping (Columbia), Agencia Nacional de Infraestructura (ANI) (Columbia), Correo Uruguayo (Uruguay), Peruvian Ministry of Labor, Servicios Postales del Ecuador, and Servientrega Post (Columbia)
- **Europe:** An Post (Ireland), Aramex (Bulgaria), BelPost (Belarus), Chronopost France, Czech Posta (Czech Republic), DPD Parcel (France), Evri (U.K.), Hellenic Post (ELTA) (Greece), InPost (Poland), La Poste (France), Lietuvos Paštas (Lithuania), Mondial Relay (France), myHermes Konto (Germany), Obrasci Posta (Croatia), Post AG (Austria), Poșta Moldovei (Moldova), Poșta Română, Posten Norway, Posti Group (Finland), Poste Italiana (Italy), Public Enterprise "Pošta Srbije" (Serbia), Posturinn (Iceland), Royal Mail (U.K), Slovenská Pošta (Slovakia), Swiss Post (Switzerland), and Ukraine Post
- **Middle East:** Georgian Post (Georgia), Israel Post, Qaz Post (Kazakhstan), SMSA Express (Saudi Arabia), SPL Express (Saudi Arabia), Turkish Post (PTT) (Turkey), and Yurtiçi Kargo (Turkey)
- **Africa:** Algeria Post, Egypt Post, Libyan Post (Libya), and South African Post Office
- **Asia-Pacific:** AIS Thailand, Australia Post, HKeToll (China), India Post, J&T Express (Asia), New Zealand Post, Pakistan Post (EP), Philippine Postal Corporation, Singapore Post, SMBC Card (Japan), Sri Lanka Post, Telkomsel (Indonesia), TEPCO (Japan), Thailand Post, and Yamato Transport (Japan)

It should be noted that all phone numbers include a country code. This makes it easy for a threat actor to send geo-targeted phishing messages even to relatively small countries like Iceland, Kosovo, or Jamaica.

In some countries, such as the U.S. and Canada, mobile phone numbers even include an area code, making regional targeting of victims (for example, when impersonating toll operators) more effective.

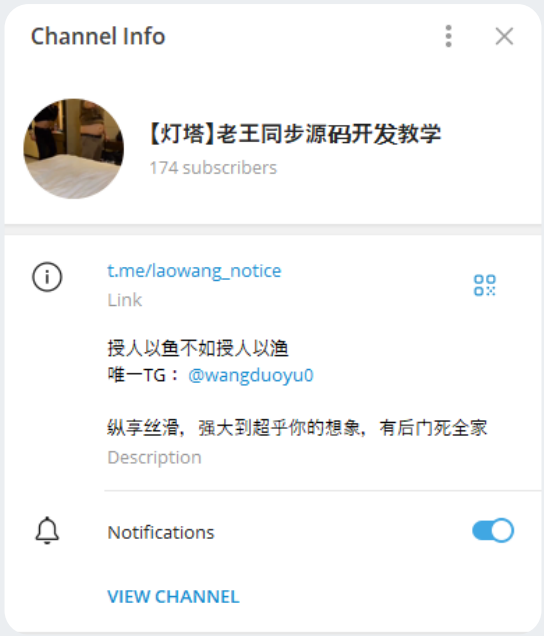
MARCH 2025: NEW TELEGRAM CHANNEL FROM SMISHING TRIAD KIT DEVELOPER WANG DUO YU

Silent Push analysts discovered a new Telegram channel (t[.]me/laowang_notice) created on March 18, 2025, being used by Smishing Triad developer “Wang Duo Yu” to communicate with buyers of the smishing kit.

This access helped us better understand some of the new Smishing Triad kit’s features, targeting details, and the lures they are planning to use. A partially translated capture of the developer’s handle is:

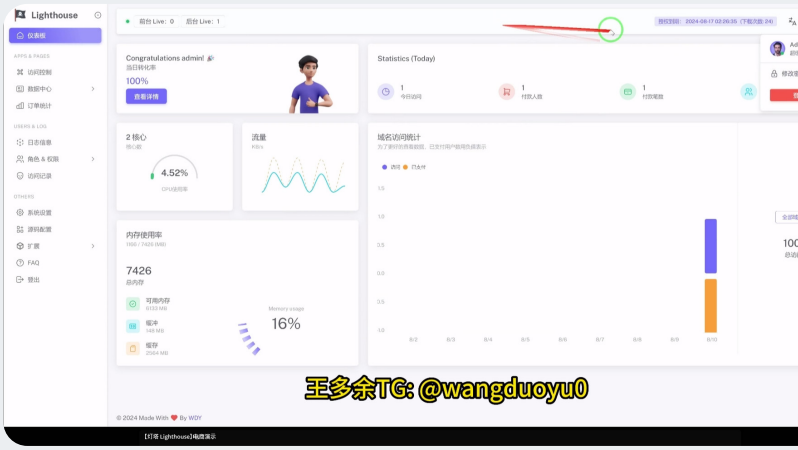
“It is better to teach a man how to fish than to give him a fish. The only TG: @wangduoyu0”

The most recent message also explains why Wang Duo Yu created a new one, “The old channel has been blocked, so I will use this channel to release the latest news in the future.”



“Wang Duo Yu” Telegram channel

Access to this Telegram channel confirmed the name of the Smishing Kit as “**Lighthouse**.” Readers can see the Lighthouse interface here in this screenshot from one of the videos posted on Telegram in March 2025:



Screenshot of the Lighthouse interface from Telegram

The Lighthouse description alludes to the sophistication of the bank phishing features, directly calling out how they have “300+ front desk staff worldwide”:

”【Lighthouse】E-commerce Demo

The most powerful synchronization backend: supports real-time synchronization, one-click setup, one-click update, automatic diversion, card header notes, OTP verification, APP verification, PIN verification, 3DS verification, code scanning verification, contacting banks, card replacement payment, online banking verification, points customized products, multiple customized verifications, etc., with a real interface, high bit rate, and stable operation

300+ front desk staff worldwide

Enjoy the silky smoothness, powerful beyond your imagination, with a backdoor to kill your whole family!”

The Lighthouse footer also includes a reference to the creator Wang Duo Yu with the reference, “Made with <heart> By WDY”

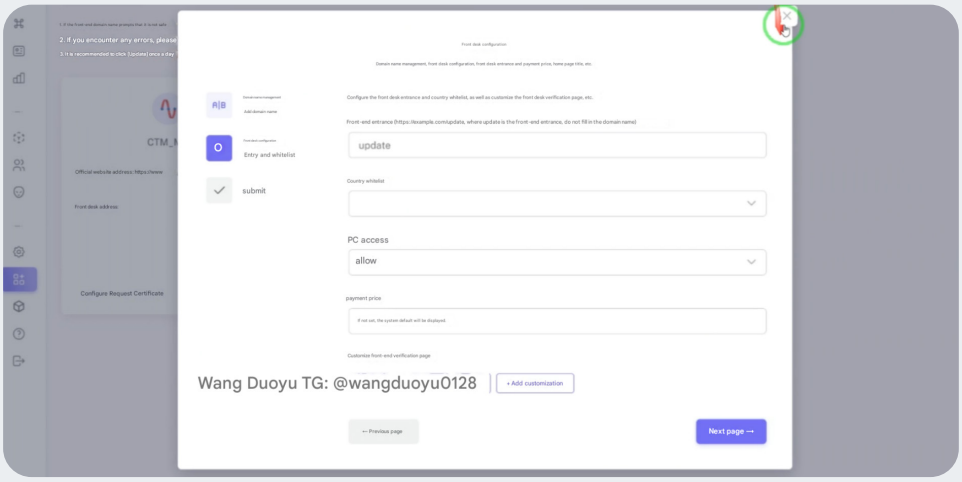
Screenshot of the Lighthouse footer on Telegram

Other details within the Telegram channel align with past attacks and provide context for current targeting.

SMISHING TRIAD PHISHING KIT FEATURES

The new Lighthouse phishing kit promoted on Telegram featured several options for threat actor groups that buy the tool. A translated version of the interface confirmed these options were available for admins:

1. Customizing the directory of the “Front-end entrance” where content is shown.
2. A country whitelist so that the page can likely only load for people on specific IP addresses
3. A toggle to allow desktop access (most pages only render to mobile user agents)
4. Payment price (amount charged to victim)
5. Customized front-end verification page



Screenshot of Lighthouse Interface from Telegram

You can watch a full video walkthrough of the Lighthouse app from the creator himself—although it is in Mandarin—at https://youtu.be/o6lNR7zfwZ8*.

FURTHER CONFIRMATION OF CHINESE DEVELOPERS

The developer of the Smishing Triad kit communicates with potential affiliate partners in Mandarin, and the text on the phishing kit’s JavaScript also contains Chinese text. The ties to China are significant and were relatively easy to confirm.

“当前正在首页” -> “Currently on the home page.”

“当前已填写完成” -> “Currently completed filling out.”

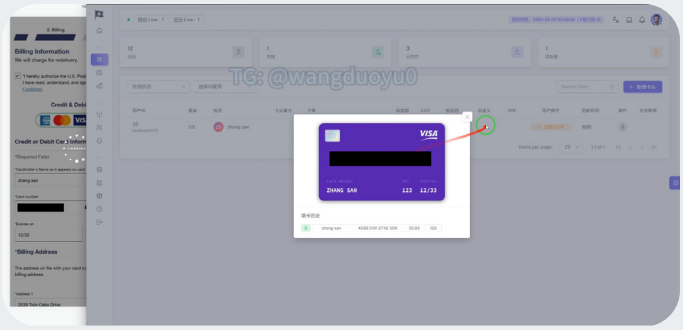
“当前正在填卡页面” -> “Currently on the card filling page.”

“当前正在地址页面” -> “Currently on the address page.”

Phishing kit text example

USPS PHISHING KIT

The USPS phishing kit was one of the first launched by Smishing Triad, but it continues to see updates. The kit provides a real-time sync between the front-end phishing pages and the back-end database with features for easy viewing of victims' data:



Screenshot of the Lighthouse interface, from Telegram by @wangduoyu0

There is also a feature to support real-time purchasing so that if a threat actor is stopped from using a victim's credit card, they can direct victims to a QR code to get a code from a mobile app.

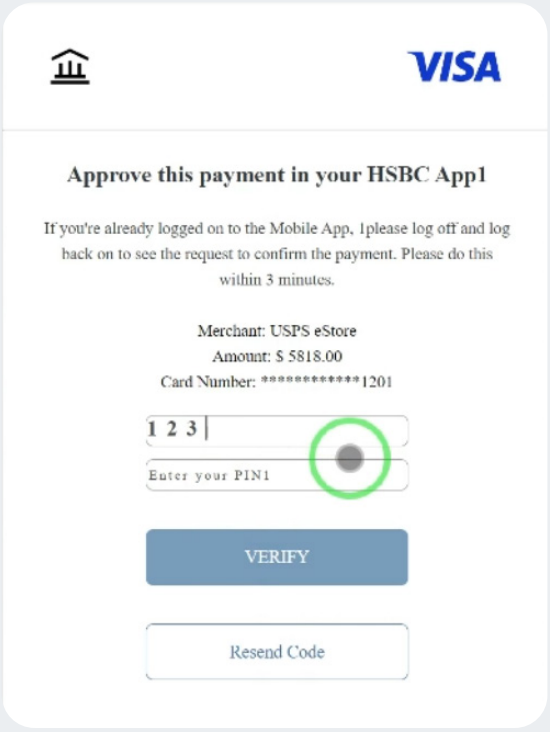
Screenshot of the QR code on the USPS phishing page

PAYMENT TACTICS: CREDIT CARD CVV VERIFICATION & QR CODES FOR MOBILE APPS

Depending on the type of card entered in the form, an additional verification can be triggered to ensure the card can be used. You can see the Card Verification Value (CVV) prompt here:

Screenshot of Lighthouse interface from Telegram

There are also screens encouraging victims to approve payments within the HSBC mobile app and requesting their transaction's personal identification number (PIN):



One of the USPS Phishing Kit features targets Visa and HSBC users from Telegram

This triggers a screen based on the type of credit card used (American Express is featured in the USPS Phishing Kit on Telegram, example below):

Screenshot of American Express CVV phishing prompt from the USPS Phishing Kit via Telegram

Watch the full video promoting the USPS kit from the Smishing Triad developer here: https://youtu.be/307WeScSBc4.*

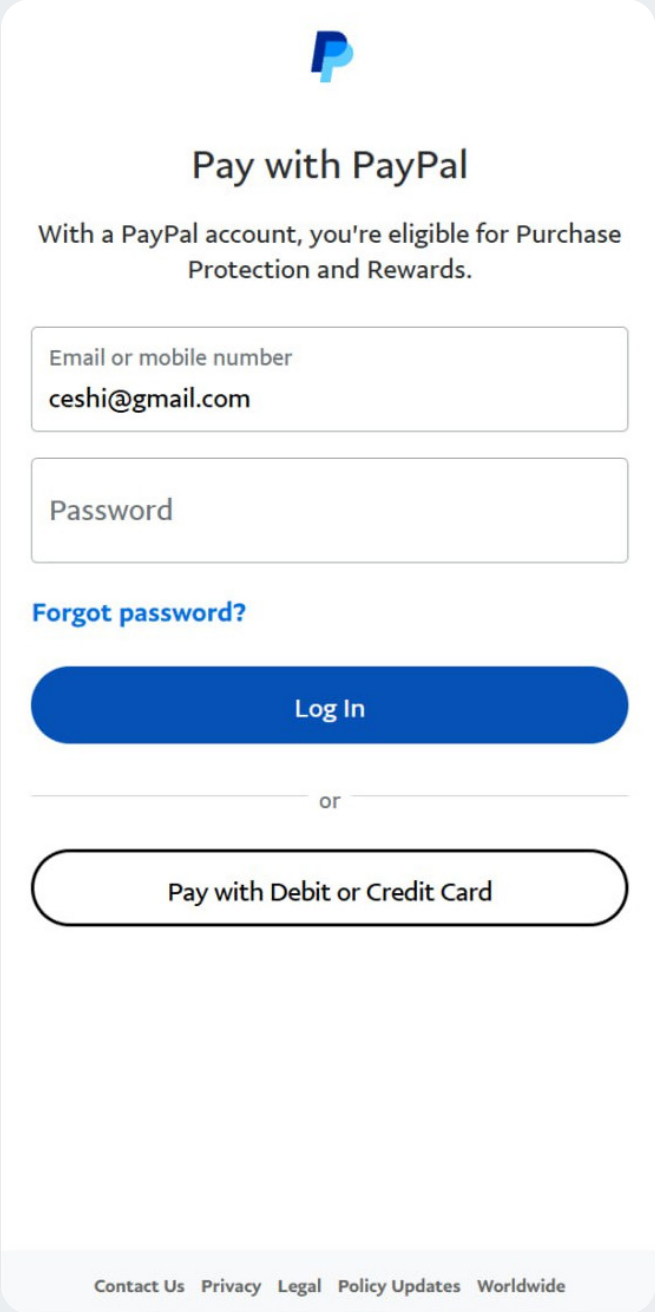
NEW PAYPAL PHISHING KIT

The threat actor group's Telegram channel describes the PayPal phishing kit as:

"【Lighthouse】E-commerce PayPal Update

Supports simultaneous fishing of accounts and cards"

Screenshots of the phishing pages look like this:

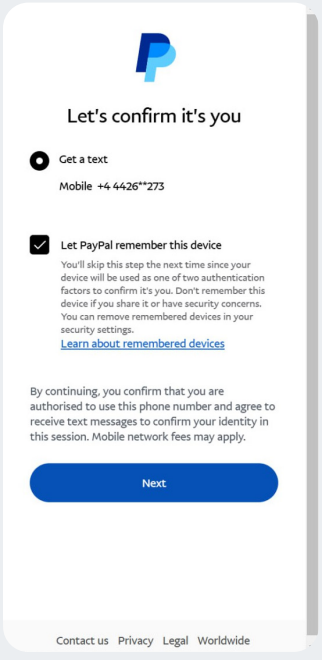


Screenshot of the mobile-optimized PayPal phishing kit includes the email "ceshi@gmail[.]com"

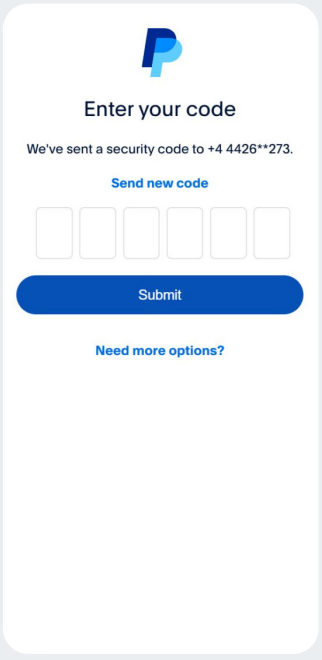
The ceshi@gmail[.]com email address may actually be the personal email of the threat actor. It has been seen in breach files from Shein[.]com, Youku[.]com, and hiapk[.]com – all Chinese brands. It's also been seen in some stealer logs, with one unique hand-created password being "wuppypuppy1," which could be a pivot point into other accounts controlled by this same threat actor.

In other parts of the phishing kit infrastructure, there are references to "ceshi" like in one of the C2 subdomains, which you can see in this screen capture of the video from the Telegram channel:

Screenshot of the Lighthouse interface, highlighting a C2 domain of "ceshi.appexpress[.]top"



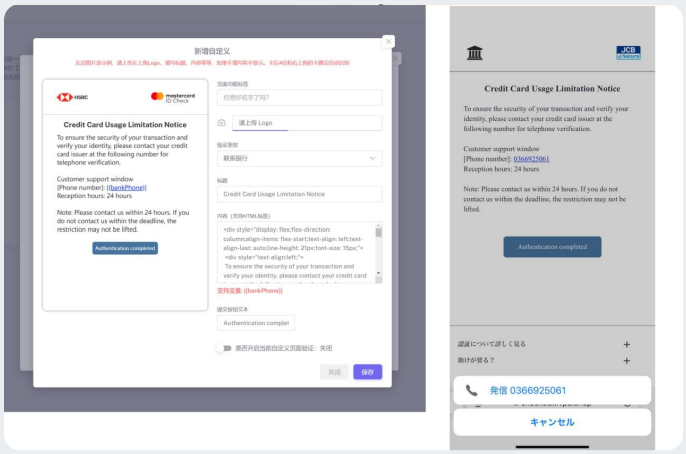
Smishing Triad PayPal phishing kit includes a realistic SMS request page



Smishing Triad PayPal phishing page for acquiring 2-factor codes

NEW HSBC MASTERCARD PHISHING KIT

The Telegram channel promoting the Lighthouse tool also featured new templates for phishing HSBC Mastercard users. For unknown reasons, multiple new layouts and features were made to target HSBC customers.



HSBC Mastercard phishing template from Telegram

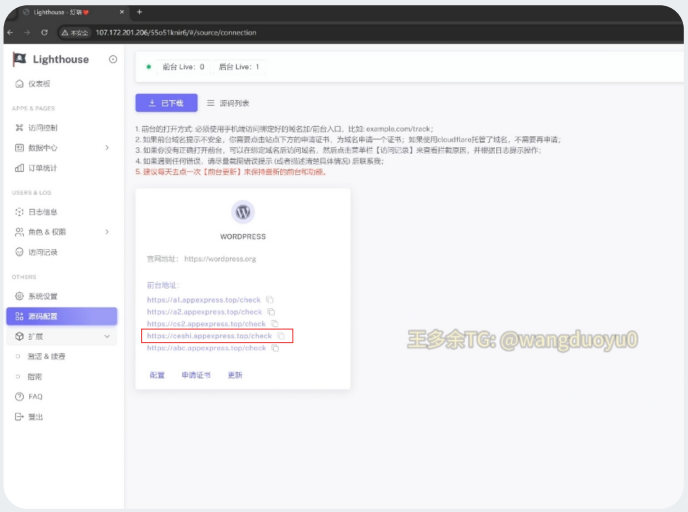
TRACKING MULTIPLE SERVER VARIATIONS

Silent Push's Threat Analysts have developed extensive fingerprints that enable our team to track the various server setups being used by Smishing Triad threat actors. The diversity in server setups hosting their phishing kits further confirms that multiple threat actors are using similar TTPs and code kits, while making their own deployment decisions.

For operational security reasons, we can't make the queries used to track Smishing Triad public, but we are sharing 50 **IOFA™** domains at the bottom of this report to support external research.

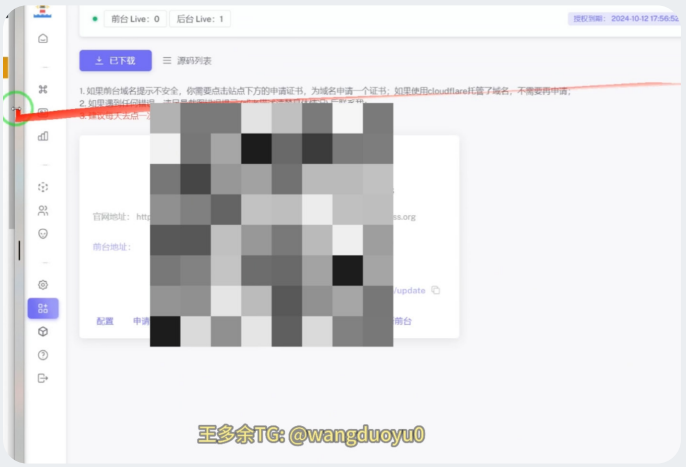
SMISHING TRIAD LIGHTHOUSE C2 DOMAINS

Within the Telegram channel, the admin recorded a video showing the testing domain they had set up, "appexpress[.]top," which appeared to be a C2 where credentials would be sent from phishing pages.



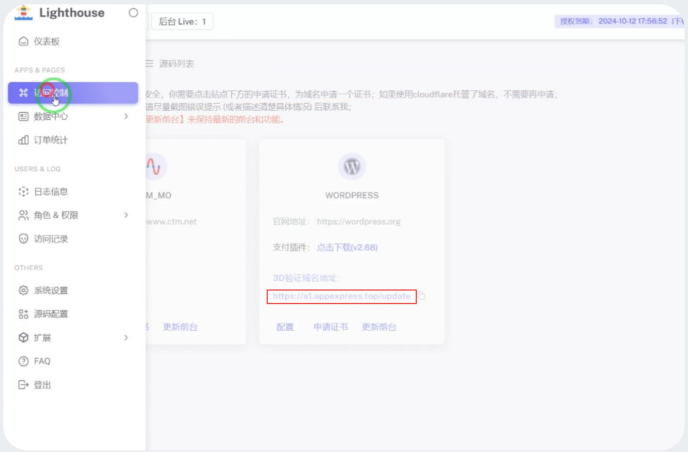
Screenshot of the Lighthouse walkthrough from Telegram

It appears this detail was inadvertently included, as it was blurred out in previous sections of the video:



Screenshot of the Lighthouse walkthrough from Telegram

Even in that section, however, the admin messed up the blurring, and it was briefly visible in the video:



In the video screenshot, it appeared the admin revealed the testing domain they had set up, "appexpress[.]top," by mistake

Silent Push analysts found a JavaScript file connected to this C2 in a phishing kit. The file references a wide variety of banks and financial institutions, including several Australian finance organizations.

- index-D76-mPwS[.]js

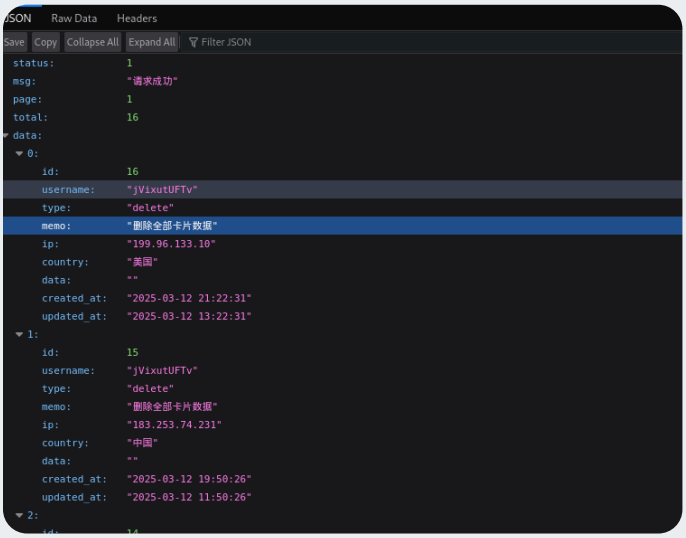
We believe this file showcases early targets of the threat actor's new bank phishing template, and expect this group to expand targeting beyond this initial list:

- PayPal
- Mastercard
- Visa
- HSBC
- Bendigo and Adelaide Bank
- Bank of Sydney
- Bank Australia
- Bank of Queensland
- Bank of Nova Scotia
- Australia and New Zealand Banking Group
- CitiGroup
- Commonwealth Bank of Australia
- Cuscal LTD
- HSBC Bank Australia
- ING Bank (Australia)
- National Australia Bank
- Newcastle Permanent Building Society
- Police Bank
- George Bank
- Westpac Banking Corporation
- Macquarie Bank
- Stripe (brief reference, likely leftover code from the Stripe template)

SMISHING TRIAD WEAK SERVER CONFIGURATIONS

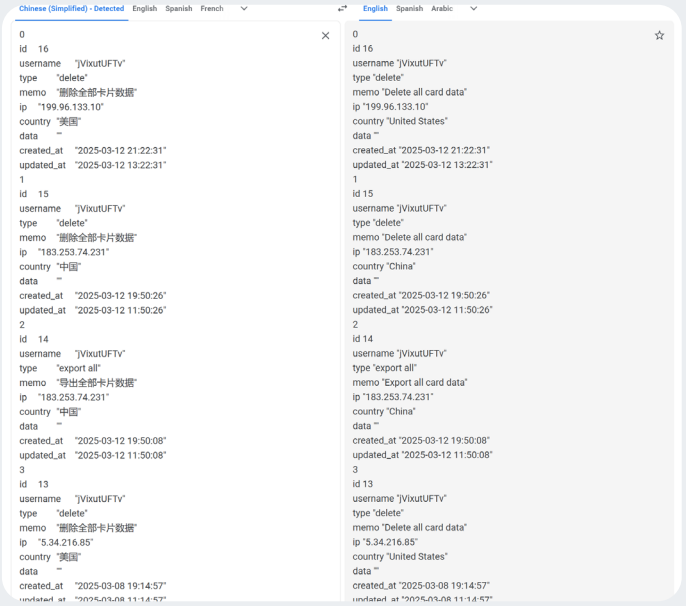
Silent Push Threat Analysts also discovered a vulnerability that led to an information leak from one of Smishing Triad's phishing pages. For operational security reasons, we can only share a limited view of the findings.

Here you can see a JSON file with log records:



Log records from a Smishing Triad phishing page

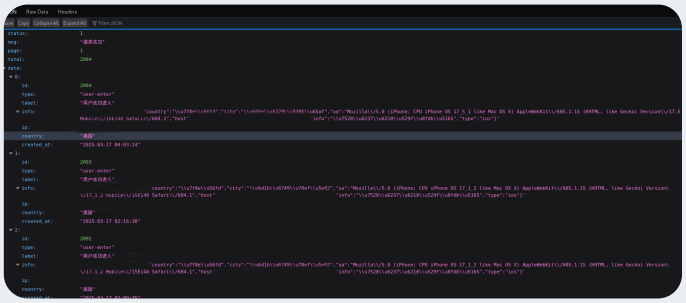
When translating this information, it was noted that the logs included the text "Delete all card data" and "Export all card data." This indicated these logs were actual phishing log records from Smishing Triad. Additional data showed that this was a log from a website user.



Brief translation reveals the memo's meaning

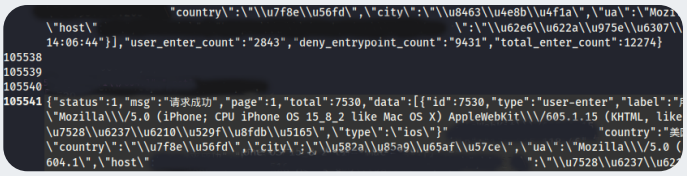
Based on the information found, Silent Push Threat Analysts scanned 9,270 unique domains and narrowed the list to 450 IP addresses—all likely controlled by Smishing Triad.

Another leak revealed page visits from victims and the specific phishing page they had visited.



Log showing details of phishing page visits

Silent Push Threat Analysts scanned all 9,000+ unique domains for the specific attributes used here and were left with a file containing 105,500 lines of output.



A small snippet of the output

This information served as the basis for the million+ page visits referenced in the earlier section in our report. Based on the data we gathered, our team has calculated that the total number of phishing page visits was well over 1,000,000 potential victims within a 20-day time span.

BREAKDOWN OF SMISHING TRIAD INFRASTRUCTURE

Approximately 200,000 domains have been used by Smishing Triad threat actors.

Tens of thousands of Smishing Triad domains are live within any 8-day period.

The infrastructure has been hosted across over 8,800 unique IP addresses, across more than 200 different ASNs.

Notably, more than half of the phishing sites were hosted by two Chinese hosting companies: Tencent (AS132203) and Alibaba (AS45102).

Based on analysis of these results, Smishing Triad is targeting at least 121 countries (or about two-thirds of the world). This information was constructed using the domain names and favicons.

Additionally, across all of the Smishing Triad campaigns our team has been tracking, we saw about 187 top-level domain (TLD) suffixes being used. The most popular TLDs were: “.top,” “.xin,” “.vip,” “.world,” “.cc,” “.com,” “.xyz,” “.icu,” “.cfd,” and “.ink”.

Below is a small sample of impersonated companies and organizations and the relevant countries, intended to further illustrate the global reach of this campaign and the scope of the organizations being targeted:

TARGETED ORGANIZATION	LEGITIMATE WEBSITE	TARGETED COUNTRY	FAVICON MD5 HASH	PHISHING SITE
USPS	usps[.]com	United States	3f0f72ed57a54b97c da500bcf0545efb	info-trackingcoi[.]cc
Evri	evri[.]com	United Kingdom	7d0229599d942f4c ef13e6412fe18723	evriuk[.]top
Estafeta	estafeta[.]com	Mexico	bf0b6949346d4fe16 8245aa2bfc61cfc	estafetau[.]shop
Turkish Post (PTT)	ptt[.]gov[.]tr	Turkey	7bb31b9ef5f35d816 f9bc7a816c800d7	tuyrepost[.]cc
La Poste	laposte[.]fr	France	2e7b6d178a0468f6b eaf184e854d773e	posten[.]top
Correos Post	Correos[.]es	Spain	349246ee336d8b298 6e584a4fa436128	busine[.]cfd
India Post	Indiapost[.]gov[.]in	India	d6d9ecedd59f3418a 8425ce5e61e5695	indiapost[.]top
Amazon Post	amazon[.]com	Global	ca6619b86c2f6e606 8b69ba3aaddb7e4	ewdfb[.]top
Canada Post	canadapost-postescanada[.]ca	Canada	b97eafae41beb90b3 c3279fb07fdbc45	canadaapoost[.]com
Servientrega Post	servientrega[.]com	Colombia	f264619a74d8b662e 7a695c2563a9bcf	btyzywlp[.]top
Australia Post	auspost[.]com[.]au	Australia	5848f96af0da17512 255e056da67263d	auspoust[.]cc

Royal Mail	royalmail[.]com	United Kingdom	3b1e1a3f7ea2c1ae 22748f963728cba6	psocygb[.]xin
DHL	dhl[.]com	Global	d8106bf3a1d00ab43 b01e6e3c92500eb	post-isl[.]sbs
Poste Italiana	poste[.]it	Italy	3cbac548d46ec7b77 94ec1d1ba11ff08	posteit[.]cfd
An Post	anpost[.]com	Ireland	9a59afcbfc57b19ae 71413f2b2d950a0	chamge-a[.]top
Yurtiçi Kargo	yurticikargo[.]com	Turkey	eac1870faf46ea45a 318c20563d3cf8f	yurticikargoy[.]cyou
SMBC Card	smbc-card[.]com	Japan	67ac939271735622 b07d41dbcc90300b	smbc-card[.]shop
InPost	inpost[.]pl	Poland	c98cb827ea0cc793 9a9083ecd833410e	inposttrack[.]click
CTT Correios	ctt[.]pt	Portugal	782c9d4b134c4e0b 632b67970d23287e	cttpacks[.]click
Correos El Salvador	correos[.]gob[.]sv	El Salvador	87eebd70b533b24b 2c127e7d113c3b88	slvpostgob[.]ccsv
AIS Thailand	ais[.]th	Thailand	e9c703a4188c3c83 55c1529caa76eb1a	aiisoi[.]top
South African Post Office	postoffice[.]co[.]za	South Africa	c1dd8d14493c54a6 75ac29031713bfc0	za-post-word[.]top
Slovenská Pošta	posta[.]sk	Slovakia	34541285068a8cab e10d7393ea68704d	shant[.]fun

DPD Parcel	dpd[.]com	Global	d6e8d97ca54021f4 6aae3e4b5fbf3208	dpd-pack[.]xyz
Philippine Postal Corporation	phlpost[.]gov[.]ph	Philippines	5e56f6ac37123d15 2c4f477e40a1a92d	phlppovd[.]top
Swiss Post	post[.]ch	Switzerland	f6e7b043a102b271 d898072e24227356	post-track[.]help
Czech Posta	Postabo[.]cz	Czech Republic	4053dfb4509b7c2d 5a3596e2875caab1	ceska-post-a[.]blog
4-72 Shipping	4-72[.]com[.]co	Colombia	12a853f2e837b036a c706f3d5160aea5	address-4-72[.]top
Israel Post	israelpost[.]co[.]il	Israel	aa8806968a55f7e5e 5202cb59f8b0318	isr-aelpost[.]sbs
Qaz Post	post[.]kz	Kazakhstan	ed9cb0beb42ed449 75095a4f2ca5cf86	wbduvn[.]com
Peruvian Ministry of Labor	trabajo[.]gob[.]pe	Peru	1965fef6225a1639b 0919581e37ab5cf	fwedsfg[.]top
Yamato Transport	kuronekoyamato[.] co[.]jp	Japan	9e83ad80e466873a 9acc652c194fa5bd	whetf[.]xin
FedEx	fedex[.]com	Global	a53129769d15f251d 4e5c5cb966765b4	fexpres[.]lol
J&T Express	jtexpress[.]ph	Southeast Asia	b3eae70fa423635b4 359de4bd9b59b00	mys-jtexpres[.]cyou
Claro Cloud	clarocloud[.]com	Latin America	1a4f0664da92aa9ca 994296084d46e9e	www-claro[.]top

Lietuvos Paštas	post[.]lt	Lithuania	d06cf67753097487e2b29d3d0cb47ae7	lietuvospost[.]help
Singapore Post	singpost[.]com	Singapore	3ea19204ea4c75da2cff7aff54135c09	singpposts[.]top
Servicios Postales del Ecuador	serviciopostal[.]gob[.]ec	Ecuador	aa568cd0fc3e7c8c6d34511d0dd4e641	serviciopostalgobec[.]pics
Maxis Telecom	maxis[.]com[.]my	Malaysia	38cce9d714010a3e43132f1348454461	mapxis[.]ink
Chronopost France	chronopost[.]fr	France	cdf92e329cc12fa614a9b706250d8498	chroonopostfrr[.]click
Poșta Moldovei	posta[.]md	Moldova	2326ee2db9d78be59257b9d08be1507a	business-poste[.]top
Egypt Post	egyptpost[.]gov[.]eg	Egypt	44fff7ded89e2c97b6b3797550a69a75	egiuw[.]top
Public Enterprise “Pošta Srbije”	posta[.]rs	Serbia	8f69a8995d3eb92cb0a35b07d05659e3	postah[.]cc
Correos de Costa Rica	pagos[.]correos[.]go[.]cr	Costa Rica	f6a5c39822bebd1071a30d77b02ca0fd	cootrut[.]site
Aramex	aramex[.]bg	Bulgaria	bd668e3a554306b020c5670b02e70586	aramexaene[.]com
Ukraine Post	ukrposhta[.]ua	Ukraine	a3765a9d883516fbf9992fb368ab4a45	ukrspack[.]click
SPL Express	splonline[.]com[.]sa/ar	Saudi Arabia	0d738b9111bf58499f057e84b0d6c0f4	spl-express[.]help

Poșta Română	posta-romana[.]ro	Romania	f0806fd528a615d2 86a7f3398be0a002	posta-romanam[.]cc
Posten Norway	Posten[.]no	Norway	1fa4c9a05aae4399 c4ae72eab37a5cd0	unogmu[.]icu
Post AG	post[.]at	Austria	e219d187a2e604c4 feb65b4c8e838ba1	at-post[.]icu
myHermes Konto	myhermes[.]de	Germany	47c30669b590c553 9b01c28f1203dbcc	myhermes-at[.]bond
Autopistas	autopistas[.]com	Spain	386464fffd1b5b5d e12fa217fb4c8962	autopistes[.]asia
Telkomsel	telkomsel[.]com	Indonesia	762c0117f77fc03c6 66586ca8920f5e4	telkomssel[.]ink
Obrasci Posta	posta[.]hr	Croatia	a054771f947814ce d1668f9056dda56d	post-word[.]top
TEPCO	tepco[.]co[.]jp	Japan	454357104cfcc4afb d9f4274b755bab2	tepco-co-jp[.]online
Georgian Post	gpost[.]ge	Georgia	998950a66034565a fde5b38b16a2c848	geopostl[.]cfd
Hellenic Post (ELTA)	elta[.]gr	Greece	a2dcaabb983ac9e0 0cd561dba81e63f6	eltade[.]cc
The Toll Roads	thetollroads[.]com	United States	b77c325bbed7cde9 ed764e39301a0dfa	thetollroadsll[.]lol
Pakistan Post (EP)	ep[.]gov[.]pk	Pakistan	977c05b3d421bc68 473bbd5dbf85578e	epgovc[.]top

Telcel	telcel[.]com	Mexico	b211f84b21ccbb8 65ff13decfccfdb3f	ttspost[.]sbs
Guatemala Post (Correos de Guatemala)	correos[.]gob[.]gt	Guatemala	a20e946cd5fc459b 3fc24aac7ba63f76	coeetrttgroup[.]cfd
SMSA Express	www[.]smsaexpress[.] com	Saudi Arabia	63c8ae68ffc88607 adcb991403aac338	smseexpress[.]cfd
Posti Group	posti[.]fi	Finland	9f18375658005abf 5ea3ca68bba84fd1	posti-fifi[.]top
UPS	ups[.]com	Global	afd13e52f285793f 5eaa266c12a19abe	mxups[.]me
Tigo Guatemala	tigo[.]com[.]gt	Guatemala	6da0a1b3f14c594c a59b2d0f5cbba8c4	tigo-gtmc[.]top
Mondial Relay	mondialrelay[.]com	France	cdc89ea9ddff2fac d9df0854165e0dc1	mondialrellay[.]live
Telefónica México	telefonica[.]com[.]mx	Mexico	0ffe21b6f2306750e 5dac33036a72cb0	entelclws[.]top
Sri Lanka Post	slpost[.]gov[.]lk	Sri Lanka	727dba352808dbac f07c64665221a63a	slpostgovls[.]xyz
HKeToll	hketoll[.]gov[.]hk	Hong Kong	8617548fca9c0056 70313f8199c91b54	hketoll-etc-hk[.]top
Correo Uruguayo	correo[.]com[.]uy	Uruguay	64c6903fded3bcab 9fa069e0a8510868	uypos[.]xyz
M360 SMS Send	m360.com[.]ph	Philippines	f5aa2599540f5470c 5c6db0a9a816988	globeefd[.]top

Thailand Post	thailandpost[.]com	Thailand	e7a779b2a78738e30ce2056417615a4f	thposto[.]vip
BelPost	belpost[.]by	Belarus	b69b0e9972eb5cd55852c5c4ad86f270	belpost-by[.]lol
Libyan Post	libyapost[.]ly	Libya	e021fa39a227f70c7d74ebc1397ff555	hanypost[.]top
Agencia Nacional de Infraestructura (ANI)	ani[.]gov[.]co	Colombia	a003e0a196f18d56b5b4ef9622ab8b60	adffew[.]top
New Zealand Post	nzpost[.]co[.]nz	New Zealand	5b8f637a20a50f9e5de34bf4fd923e3b	nzposst-co[.]top

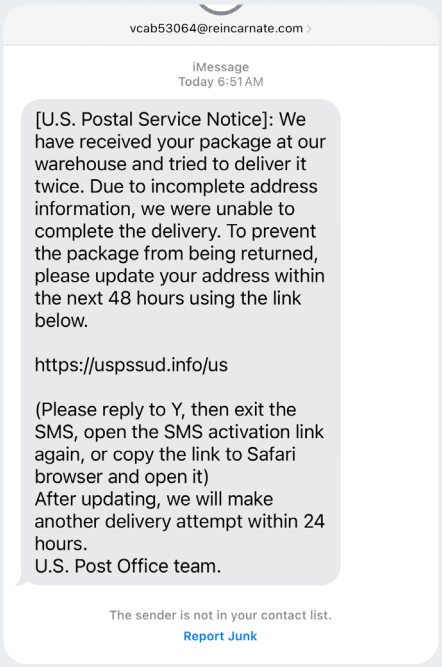
CONTINUING TO TRACK SMISHING TRIAD, WORKING ON TAKEDOWNS

Silent Push analysts will continue to track Smishing Triad and its infrastructure. We appreciate any additional leads or research tips. We believe collaboration is key to disrupting this globe-spanning effort and welcome any additional leads. In the spirit of that:

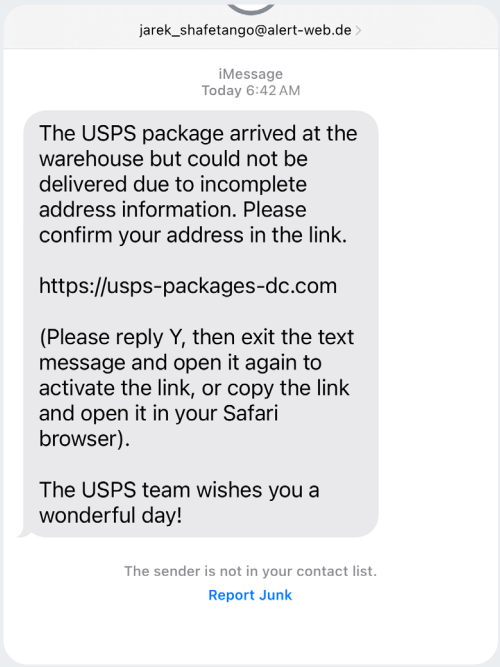
SHARING (SMISHING MESSAGES) IS CARING

Multiple research partners supported our research into the Smishing Triad at Silent Push by sharing the targeted smishing messages they were receiving. These collaborative efforts helped us confirm many new domains and also better informed our understanding of how these messages and their delivery mechanisms have evolved over time.

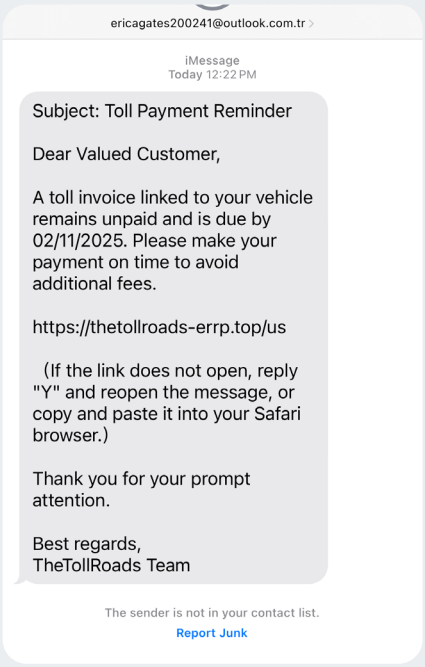
A small sample of what we have analyzed is included below:



Smishing message example: "USPS package address incomplete"



Smishing message example: "USPS package delivery incomplete"



Smishing message example: "Toll payment due"

MITIGATION

Silent Push believes all domains associated with Smishing Triad phishing campaigns represent some level of risk. This campaign is primarily a consumer-focused phishing threat, which abuses the trademarks of major brands and organizations.

Our analysts have constructed a series of Silent Push **Indicators Of Future Attack™ (IOFA™)** on these types of phishing efforts.

Silent Push **IOFA™** Feeds are available as part of an Enterprise subscription. Enterprise users can ingest **IOFA™** Feed data into their security stack to inform their detection protocols or use it to pivot across attacker infrastructure using the Silent Push Console and Feed Analytics screen.

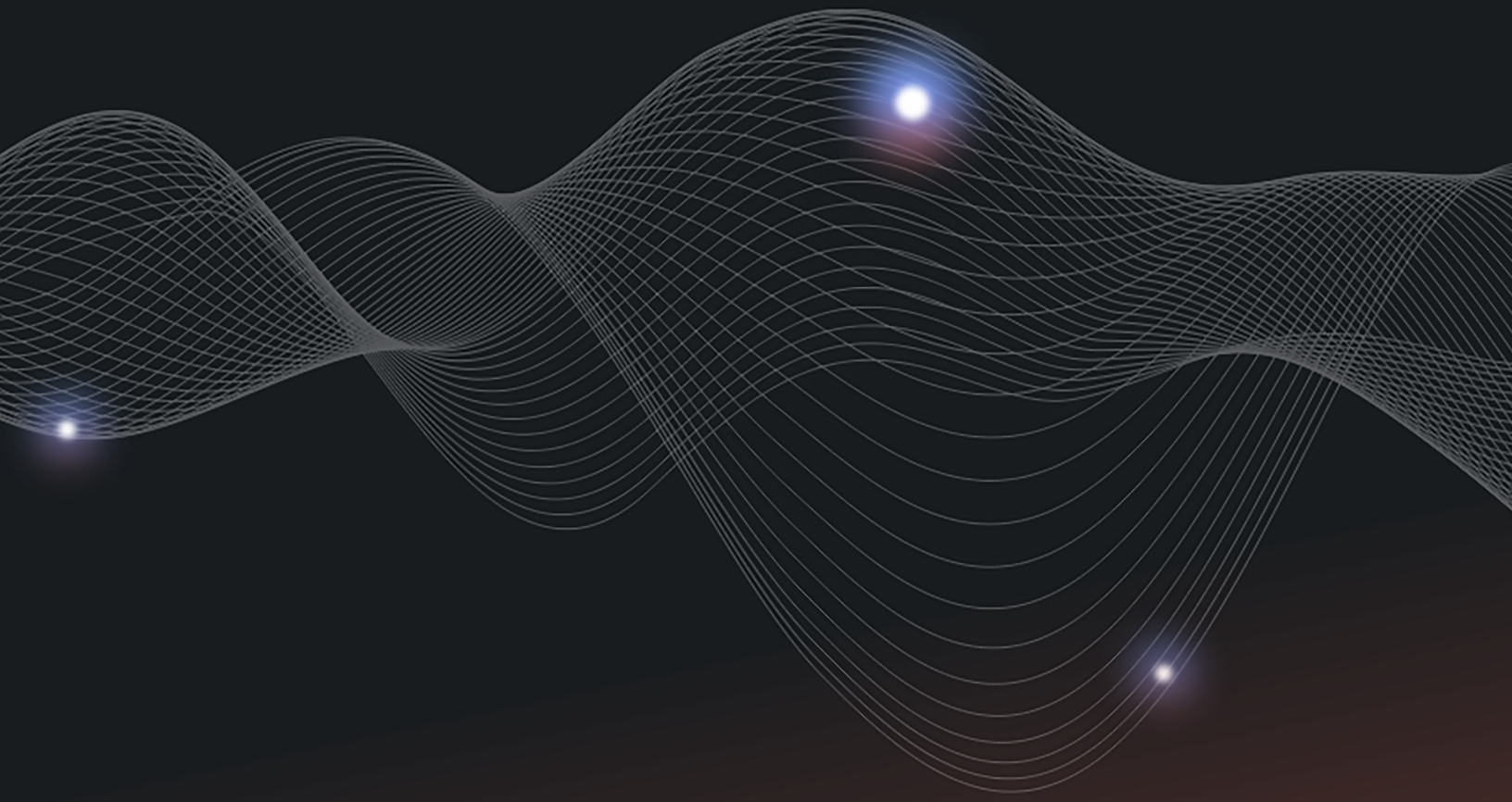
REGISTER FOR COMMUNITY EDITION

Silent Push Community Edition is a free threat-hunting and cyber defense platform featuring a range of advanced offensive and defensive lookups, web content queries, and enriched data types, including Silent Push Web Scanner and Live Scan.

SAMPLE IOFA™ LIST FROM THIS CAMPAIGN

Silent Push is sharing a sample **Indicators Of Future Attack™ (IOFA™)** list we have associated with the Smishing Triad campaign to support ongoing efforts within the community. Our enterprise users have access to an **IOFA™** feed currently containing significantly more indicators from this campaign.

- address-4-72[.]top
- adffew[.]top
- aiisoi[.]top
- appexpress[.]top
- aramexaene[.]com
- at-post[.]icu
- auspoust[.]cc
- autopistes[.]asia
- belpost-by[.]lol
- btyzywlp[.]top
- busine[.]cfd
- business-poste[.]top
- canadaapoost[.]com
- ceska-post-a[.]blog
- chamge-a[.]top
- chroonopostfrr[.]click
- com-billsgowkx[.]xin
- cootrut[.]site
- cttpacks[.]click
- dpd-pack[.]xyz
- egiuw[.]top
- eltade[.]cc
- entelclws[.]top
- epgovc[.]top
- estafetau[.]shop
- evriuk[.]top
- ewdfb[.]top
- fexpres[.]lol
- fwedsfg[.]top
- globeefd[.]top
- geopostl[.]cfd
- hanypost[.]top
- hketoll-etc-hk[.]top
- indiapost[.]top
- info-trackingcoi[.]cc
- inposttrack[.]click
- isr-aelpost[.]SBS
- lietuvospost[.]help
- mapxis[.]ink
- mndot.us-etce[.]cc
- mondialrellay[.]live
- myhermes-at[.]bond
- mys-jtexpres[.]cyou
- mxups[.]me
- telkomssel[.]ink
- post-word[.]top
- tepco-co-jp[.]online
- thetollroadsll[.]lol
- ttspost[.]sbs
- coeetrttgroup[.]cfd
- nzposst-co[.]top
- phlppovd[.]top
- postah[.]cc
- posta-romanam[.]cc
- post-isl[.]sbs
- post-track[.]help
- posteit[.]cfd
- posten[.]top
- posti-fifi[.]top
- psocygb[.]xin
- serviciopostalgobec[.]pics
- shant[.]fun
- singpposts[.]top
- slpostgovls[.]xyz
- slvpostgob[.]ccsv
- smbc-card[.]shop
- spl-express[.]help
- smseexpress[.]cfd
- tigo-gtmc[.]top
- trackwpwy[.]top
- thetollroads-errp[.]top
- thposto[.]vip
- tuyrepost[.]cc
- ukrspack[.]click
- unogmu[.]icu
- usps-packages-dc[.]com
- uspssud[.]info
- uypos[.]xyz
- wbduvn[.]com
- whetf[.]xin
- www-claro[.]top
- yhvxm[.]icu
- yurticikargoy[.]cyou
- za-post-word[.]top



SILENT PUSH

PREEMPTIVE CYBER INTELLIGENCE WITH
INDICATORS OF FUTURE ATTACK

Silent Push provides preemptive cyber intelligence exposing threat actor infrastructure as it's being set up. Our industry-leading Indicators of Future Attack (IOFA) act as an early warning system to defend against threats. We go beyond stale IOCs and create a unique digital fingerprint of adversary behavior enabling you to proactively block hidden attacks before they're launched.

Get started today.

silentpush.com