Resecurity | Smishing Triad Impersonates Emirates Post to Target UAE Citizens

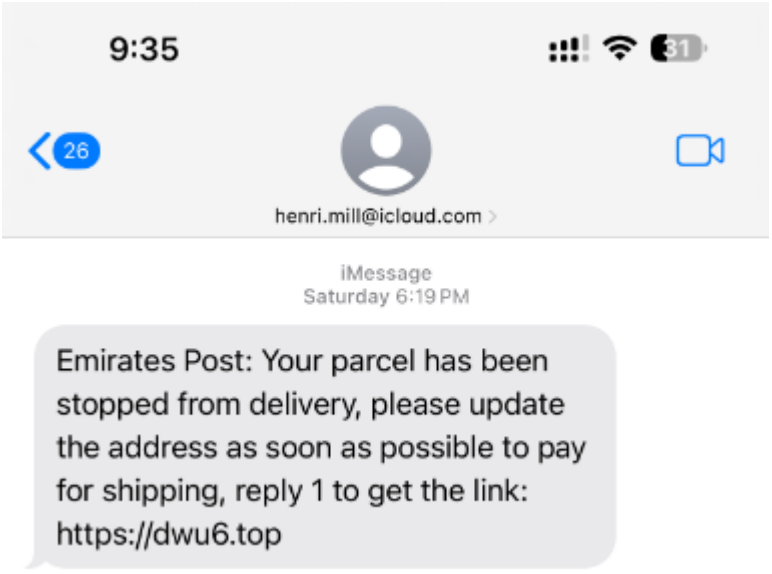
Published: 2023-09-25 · Archived: 2026-04-02 10:40:15 UTC

Introduction

This month, “Smishing Triad” has vastly expanded its attack footprint in the UAE. Resecurity, a leader in cybersecurity and threat intelligence, has identified domain names that closely resemble those used by the group in their previous campaigns. Threat actors registered the majority of these UAE-focused domains with Gname.com Pte. Ltd., a Singapore-based web registrar.

“Smishing Triad” fraudsters also listed various Chinese entities as registrant organizations, or the owners of the fraudulent domains. Similarities in domain signatures noted by Resecurity indicate a calculated and ongoing threat to the Emirates. The assessment that “Smishing Triad” is hyper-targeting victims in the Emirates is further supported by the group’s geo-filtering of smishing page access to UAE citizens only.

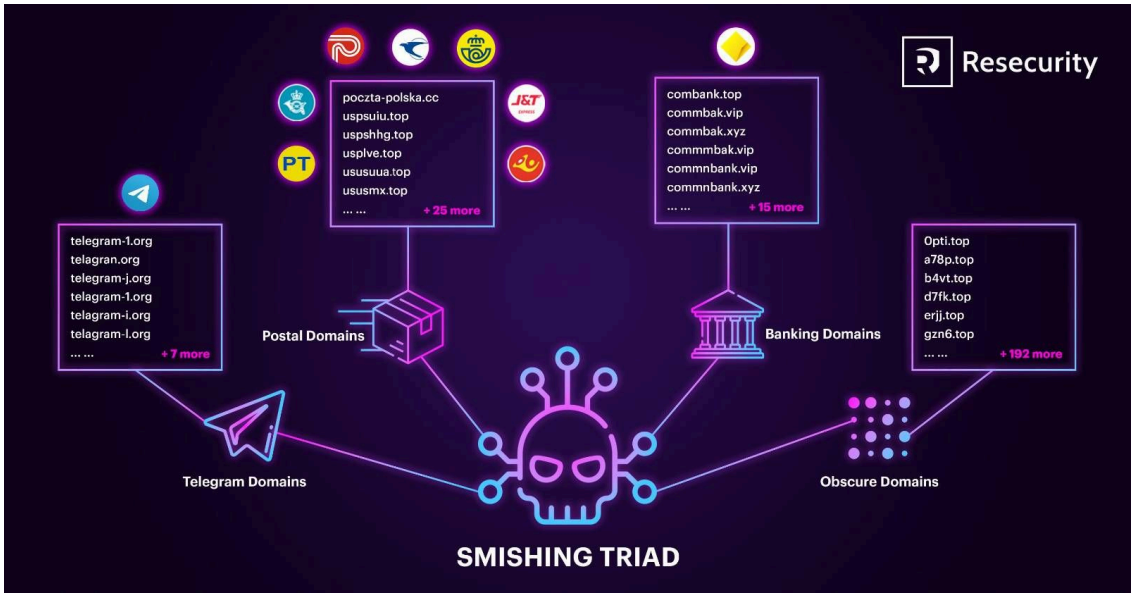
Resecurity specifically observed this geo-fencing of IP addresses in smishing lures cast out to impersonate the Emirates Post, the UAE’s official parcel delivery service. In fact, UAE-focused fraud campaigns imitating official Emirates Post communications were first confirmed in May, according to local news reports.



Example of 'smishing' text

Resecurity specifically observed this geo-filtering of IP addresses in smishing lures cast out to impersonate the Emirates Post, the UAE’s official parcel delivery service. “Smishing Triad” is also leveraging compromised Apple iCloud accounts and illegally obtained databases that contain the personally identifying information (PII) of UAE citizens to stage their attacks.

Specifically, the threat actor acquires UAE resident databases from the Dark Web and launches their smishing attacks from iCloud accounts they have previously compromised. Resecurity has already alerted and shared relevant information with the national Computer Emergency Response Team for the United Arab Emirates (AeCERT).



Resecurity's HUNTER (HUMINT) unit also blocked the majority of malicious domains that were flagged this week. But the battle against "Smishing Triad" threat actors continues.

Their Goal: To Defraud the Emirates Citizens

Their Objective

"Smishing Triad" has a singular, malign goal: to defraud Emirati citizens. By employing sophisticated tactics, the group aims to extract sensitive PII and financial data from unsuspecting victims.

Their Modus Operandi

The group typically sends out malicious text messages from iCloud accounts they have previously hijacked, while masquerading as reputable organizations like government agencies, financial institutions (FIs), and shipping firms.

These messages are designed to dupe people into divulging their PII and financial data. "Smishing Triad" then uses this stolen data to defraud individuals and businesses. To target prospective victims, "Smishing Triad" acquires geo-specific PII databases obtained from access brokers on the Dark Web.

Regarding the group's malicious infrastructure, Resecurity has observed "Smishing Triad" threat actors registering fraudulent domains through Singaporean website registrar Gname.com Pte. Ltd.

Technical Insights

Domain Details - Key Information

- **Domain Name**: dwu6.top
- **Registrar**: Gname.com Pte. Ltd.
- **Creation Date**: 2023-09-13
- **Registry Expiry Date**: 2024-09-13
- **Name Servers**: a.share-dns.com, b.share-dns.net

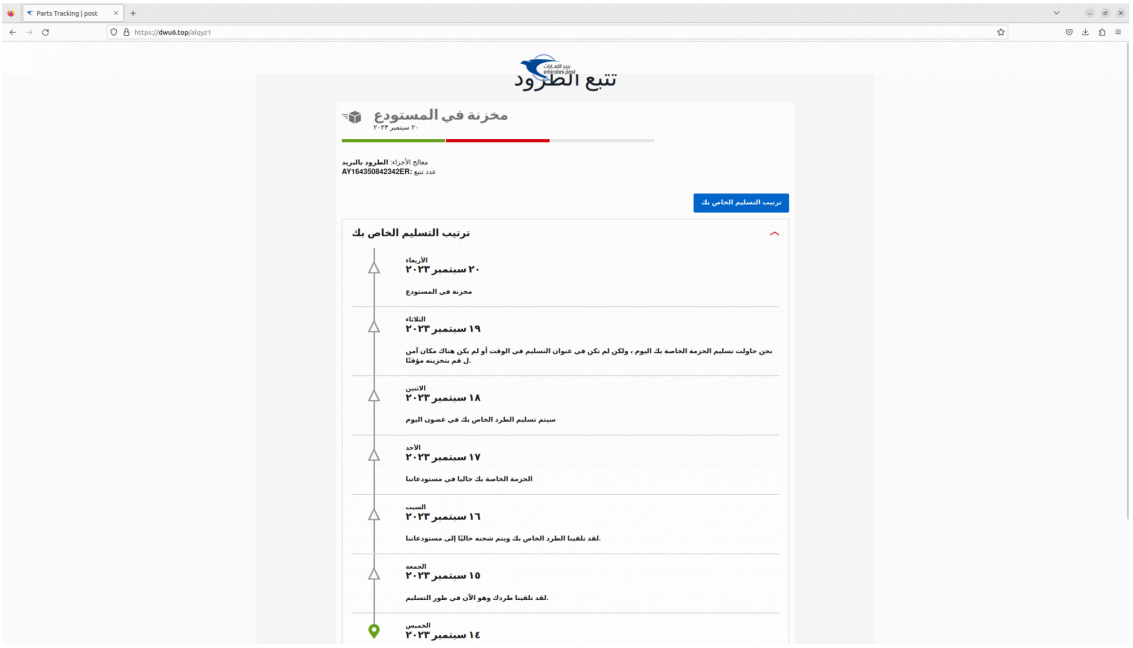
Analysis

The domain, dwu6.top, is a critical asset in “Smishing Triad's” campaign against the UAE. Its structure and registration details closely mirror those of domains used in earlier campaigns, suggesting a consistent and evolving modus operandi.

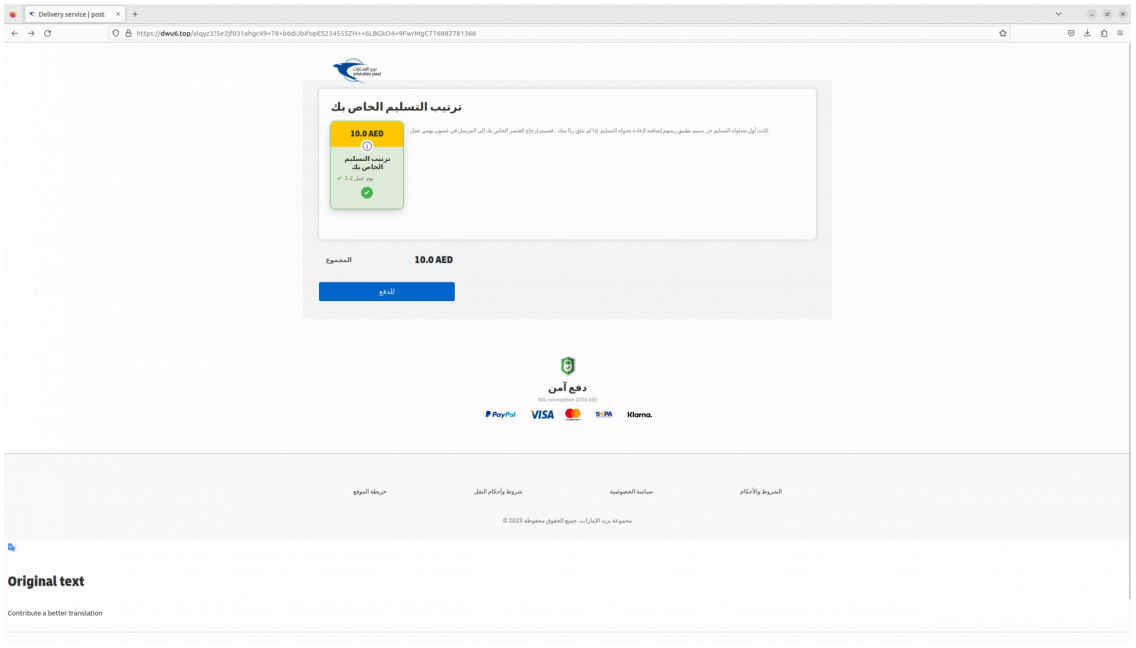
Tactics, Techniques, and Procedures

iMessage as a Delivery Method

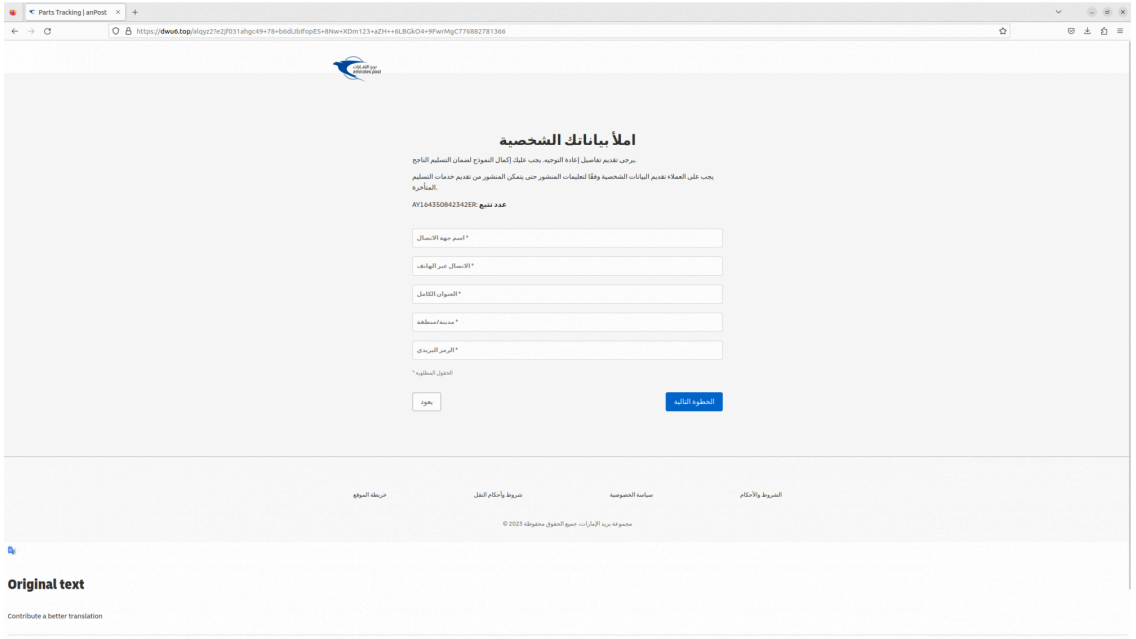
“Smishing Triad” is known to use compromised iCloud accounts to send iMessages, a tactic that makes their SMS scams more credible. The group is targeting UAE-specific users, while masquerading as the Emirates Post and other local organizations.

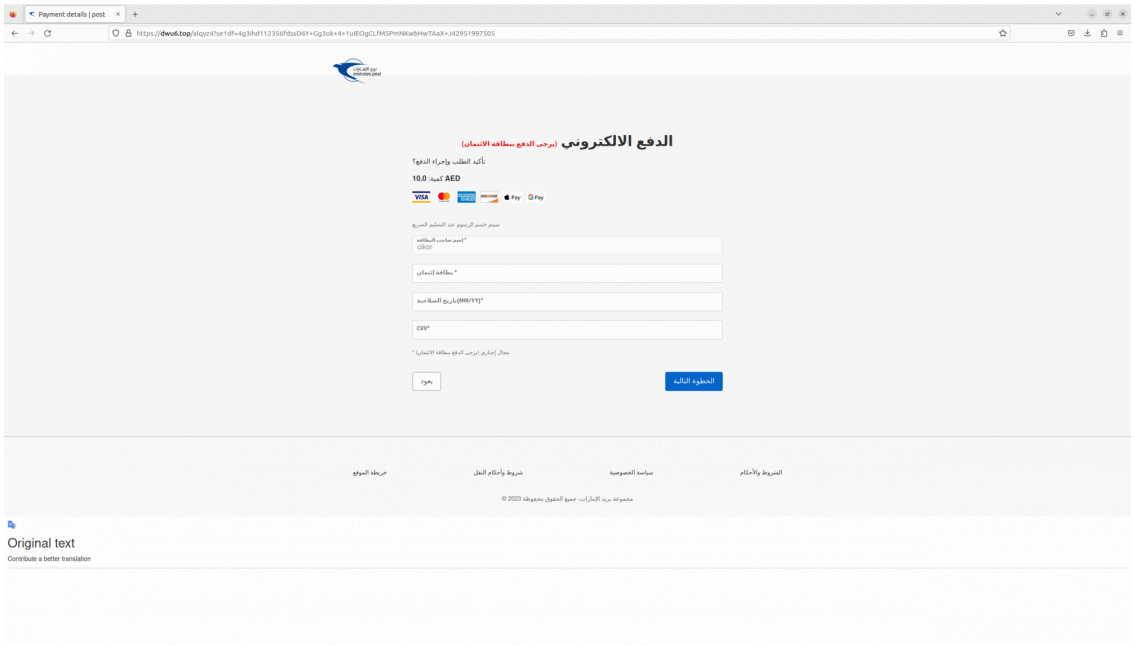


The victim will be asked to select the payment option, typically a small fee, then on the next page they're asked to enter personal and credit card information.



The next screen, the victim is asked to enter their personal information followed by the request to proceed with the payment (credit card) information.





Fraud-as-a-Service

Beyond proprietary smishing attacks, the group also offers 'smishing kits' for sale on platforms like Telegram. This fraud-as-a-service (FaaS) model enables “Smishing Triad” to scale their operations by empowering other cybercriminals to leverage their tooling and launch independent attacks.

Conclusion

The Need for Vigilance

As “Smishing Triad” expands its FaaS operations to target the Emirates, both cybersecurity agencies and UAE citizens must remain vigilant. Fraud awareness campaigns and educational programs are essential first lines of defense against these rapidly evolving threats.

Proactive Measures

Empowered by Resecurity’s discovery of the domain names and attack patterns associated with “Smishing Triad,” cybersecurity agencies are now capable of engaging in proactive monitoring, intervention, and mitigation. These measures could involve taking down malicious domains, tracking down threat actors behind them, and implementing more robust cybersecurity controls to protect UAE citizens.

Per Article 11 of the 2021 Emirates’ Cybercrime Law, “creating fake websites, email accounts, or impersonating someone else can lead to detention and fines ranging from AED 50,000 to AED 200,000. If these fabricated accounts are used to harm the victim, the perpetrator may face imprisonment for a minimum of two years.”

Penalties for cybercriminal offenses that harm UAE nationals or organizations become even harsher when “state institutions' websites or accounts are involved, leading to imprisonment for up to five years and fines ranging from AED 200,000 to AED 2,000,000.”

To assist victims of cybercrime, the government of the UAE has established multiple “easy reporting” services that include a dedicated ‘e-crime website,’ the Dubai Police website, and the ‘My Safe Society’ application. These user-friendly tools allow UAE residents to easily report cybercrime incidents.

The UAE has also established the ‘Cyber Pulse’ Initiative, an endeavor that “aims to encourage community members in the UAE to play a part in cybersecurity efforts. It seeks to enhance public awareness on suspicious online activities and the necessary steps to be taken from becoming a victim of ePhishing.”

To defend against the growing threat of “Smishing Triad” and other cybercriminal actors, UAE citizens and residents should consider the following best practices:

- Avoid publishing private contact information on unreliable online platforms
- Be cautious of unknown links sent through text messages or emails
- Only download apps from trusted sources
- Keep backup copies of personal data
- Regularly update smartphone operating systems
- Watch for signs of electronic fraud, such as abnormal battery consumption or slower processing speeds

IOC (Indicators of compromise)

Domains focusing on Telegram

telegram-1[.]org	telagran[.]org	telegram-j[.]org
telagram-1[.]org	telagram-i[.]org	telagram-l[.]org
telegram-1i[.]org	telegram-h[.]org	telegram-il[.]org
telegram-jl[.]org	telegram-jt[.]org	telegram-u[.]org
telegram-y[.]org	telagrem-l[.]org	

All Other Domains

0pti[.]top	comnmbak[.]vip	nl29s[.]xyz
15ip[.]top	comnmbank[.]vip	nml1[.]org
1hx0[.]top	comnmbnk[.]vip	nnu4l[.]top
1iw3[.]top	comnnbak[.]xyz	nudl0l[.]top
1lv0[.]top	comnnbank[.]vip	nv7d[.]top
1obs[.]top	conmmbak[.]vip	nyav[.]top
1oin[.]top	conmmbank[.]vip	o1z0[.]top

1yl[.]top	conmnbak[.]vip	odhb[.]top
1yll[.]top	conmnbank[.]vip	odl2[.]top
20in[.]top	connmbak[.]vip	og3u[.]top
2lfy[.]top	connmbank[.]vip	p1cz[.]top
2wao[.]top	cpiz[.]top	p1ml[.]top
2wgh[.]top	d7fk[.]top	pkaj[.]top
2x0o[.]top	df1u[.]org	qan1[.]top
2xlb[.]top	dkii[.]top	qq7t[.]top
3cqp[.]top	dly1[.]top	qrvk[.]top
3dal[.]top	edi8[.]top	r4lg[.]top
3guf[.]top	efij[.]top	ra1p[.]top
3gul[.]top	eha1[.]top	rij1[.]org
3l7xk[.]top	emtg[.]top	rs1u[.]top
4cel[.]top	erjj[.]top	rstv[.]top
4ece[.]top	f5pl[.]top	s9bj[.]top
4eyz[.]top	fbx8[.]top	sin3l[.]top
4jzo[.]top	fet4[.]top	suic[.]top
5a7p[.]top	ffm7[.]top	svq6[.]top
5fzx[.]top	gj9t[.]top	szp2[.]top
5iacc[.]top	gjeg[.]top	t2wr[.]top
5qfk[.]top	gzki[.]org	t78k[.]top
5ta1[.]top	gzn6[.]top	tga3[.]top
60xm[.]top	h14i[.]top	tnuk[.]top
6llp[.]top	hb06[.]top	ttp0[.]top
6pjj[.]top	hb1i[.]org	u4ae[.]top
7at3[.]top	i2lk[.]top	ueox5[.]top
7e3w[.]top	i2ro[.]top	uld3s[.]xyz

7pyi[.]top	i73o[.]top	un3ls[.]xyz
8h5c[.]top	ig3s[.]top	unfl3[.]top
8jcy[.]top	ikdle3[.]top	unfo3[.]top
8vei[.]top	iknv[.]top	unrpl[.]top
9cau[.]top	im3ls[.]top	ups1[.]top
9llu[.]top	inr3l[.]xyz	upsl[.]top
a1hr[.]top	irjy[.]top	us3ls[.]top
a1ic[.]top	itd1[.]org	uvm2[.]top
a4kh[.]top	ixva[.]top	uwqb[.]top
a78p[.]top	j7cp[.]top	uyb1o[.]top
abt7[.]top	jh0l[.]org	v0fj[.]top
aggq[.]top	jhi7[.]top	v6il[.]top
ai0y[.]top	jk1q[.]top	vgeq[.]top
ak3z[.]top	jlinx[.]top	vjya[.]top
akq4[.]top	jo3lk[.]xyz	vmn1[.]top
alpxm[.]top	juil[.]top	vp4f[.]top
aqty[.]top	jusl3[.]top	w0mq[.]top
atp2[.]top	kcns1[.]top	w3ot[.]top
auck[.]top	kcx1i[.]top	w3zx[.]top
auek[.]top	koxw[.]top	waxk[.]top
awx1[.]top	ku6t[.]top	wd9g[.]top
b4vt[.]top	kwl1[.]org	wu1rn[.]top
bfc1[.]top	l1sl[.]top	wvqc[.]top
bue9l[.]xyz	l3y[.]in	x4ld[.]top
bxav[.]top	l5gl[.]top	x6io[.]top
c6lm[.]top	l9mf[.]top	xs14[.]top
ccmmbank[.]vip	ldp8[.]top	xym3[.]top

cd1l[.]org	lr2k[.]top	yis3k[.]top
cdl6[.]top	ls9l[.]top	yjdo[.]top
cfqo[.]top	mg1a[.]top	yq0r[.]top
combank[.]top	mloe2[.]top	yqlo[.]top
commbak[.]vip	mu-2[.]top	ysio[.]top
commbak[.]xyz	myr7[.]top	yxw6[.]top
commmbak[.]vip	n30sk[.]top	z0mi[.]top
commnbank[.]vip	n3d8[.]top	z14r[.]top
commnbank[.]xyz	ncjg[.]vip	z4lg[.]top
commsbiz[.]top	nh2s[.]top	zirq[.]top
comnbank[.]vip	nisl0[.]top	zua9[.]top
comnbank[.]xyz	niss[.]top	zzg0[.]top

Source: https://www.resecurity.com/blog/article/Smishing-Triad-Impersonates-Emirates-Post-Target-UAE-Citizens