Attenti a quel pacco: come funziona la truffa degli SMS “in arrivo” e chi c’è dietro

Maria Cattini | 29/07/2025 | Sicurezza digitale

□□ Ti è arrivato un SMS su un pacco in arrivo?

“Il tuo pacco ha avuto un problema, clicca qui per sbloccarlo pagando una piccola somma”.
Se hai ricevuto un messaggio così, non sei solo. Sei potenzialmente uno dei **milioni di “pesci”** presi di mira da una delle truffe digitali più subdole e sofisticate degli ultimi anni.

Dietro queste trappole via SMS non ci sono hacker improvvisati. C’è un’organizzazione strutturata, un software chiamato *Magic Cat*, e un giovane sviluppatore cinese noto online con il nome di **Darcula**.

□□ Cos’è la truffa del pacco “bloccato”

□□ Il phishing dei pacchi

Il sistema sfrutta il meccanismo del **phishing**: un link che imita un sito ufficiale (di corrieri come GLS, UPS o Amazon), e una finta richiesta di pagamento per sbloccare una consegna. Il tutto con **l’unico scopo di rubare i dati della tua carta di credito**.

□□ “Pesci” e “gattini”: come parlano i truffatori

I truffatori definiscono le vittime “pesci”. Il nome del software che usano – *Magic Cat* – suona ironico, quasi infantile. Ma dietro quel “gattino magico” si nasconde un sistema industriale per truffare migliaia di persone in tutto il mondo.

□□ Il software della truffa: Magic Cat

Magic Cat è il cuore del sistema. Analizzato per un anno intero da NRK, Le Monde e Bayerischer Rundfunk con l’aiuto degli esperti di Mnemonic, è risultato essere un **servizio di truffa in abbonamento**.

□□ Come funziona

• I criminali acquistano una licenza su Telegram per poche centinaia di dollari al mese.
• Possono scegliere tra oltre 300 falsi siti clonati di corrieri e aziende internazionali.
• Il software invia automaticamente centinaia di SMS a potenziali vittime.
• Gli SMS contengono link a pagine false che imitano perfettamente quelle ufficiali.
• Quando una vittima inserisce i dati della carta, il sistema li registra in tempo reale.

□□ Chi è Darcula?

Dietro Magic Cat si cela **Yucheng C.**, 24 anni, provincia cinese di Henan. Online si fa chiamare

Darcula, e usa come immagine profilo gattini o personaggi dei cartoni animati.

Nonostante l’anonimato digitale, l’inchiesta è riuscita a rintracciarlo attraverso i **metadati dei file Word** che lui stesso condivideva su Telegram come manuali d’uso del suo software.

☎ La chiamata a sorpresa

Quando i giornalisti hanno provato a contattarlo, ha risposto un altro uomo: **Liao Liu**, che si è presentato come il suo “datore di lavoro”. Ha ammesso che Darcula è “quello che vende di più”, ma ha detto di non poter condividere informazioni sull’azienda.

□□ Una truffa industriale, non un gioco da ragazzi

□□ I numeri della frode

Solo in Norvegia, *Magic Cat* ha colpito **19.000 persone in sette mesi**. A livello globale, si parla di **centinaia di migliaia di vittime**.

Sui canali Telegram dei truffatori circolano prove di spese di lusso fatte con le carte rubate: **borse di alta moda, iPhone pieni di dati bancari, gioielli**.

□□ Il video virale degli SMS truffaldini

Darcula ha pubblicato un video dove si vedono **decine di telefoni accesi** che inviano SMS ininterrottamente. Una catena industriale della frode digitale. Ogni telefono un’arma. Ogni click, un potenziale furto.

□□ La struttura aziendale delle truffe

Quello che colpisce è il **modello organizzativo**: queste truffe funzionano come vere aziende. Con team tecnici, assistenza clienti, manuali, aggiornamenti. E con un **mercato globale su Telegram** dove il software viene venduto e distribuito con licenza.

□□ Come riconoscere e difendersi

□□ Segnali d’allarme

• Un messaggio che ti chiede di pagare per un pacco di cui non ricordi l’ordine.
• Un link che non corrisponde al sito ufficiale del corriere.
• Una pagina che ti chiede subito i dati della carta di credito.

□□ Cosa fare

• Non cliccare su link ricevuti via SMS se non sei assolutamente certo della provenienza.
• Controlla manualmente lo stato delle spedizioni dai siti ufficiali.
• Usa sistemi di verifica a due fattori per i tuoi pagamenti.
• Blocca e segnala il numero al tuo operatore.
• Denuncia il messaggio al servizio antiphishing nazionale o alla Polizia Postale.

□□ Giornalismo “satellitare” e nuove inchieste

L’inchiesta è parte della serie “Muckrakers”, che punta i riflettori su trame criminali digitali e frodi transnazionali. Come accade con le inchieste parallele di *Placemarks*, che usano strumenti satellitari per indagini su larga scala, anche in questo caso la collaborazione fra giornalisti e tecnologi ha permesso di **scoperchiare una rete criminale sofisticata**.

□□ Truffe sempre più globali, ma anche più

Questa vicenda ci insegna che le truffe digitali oggi **non sono più improvvisate**, ma costruite con cura, vendute come “servizi”, e gestite come imprese.

Ma ci dimostra anche che, con **indagini accurate, tecnologia OSINT, metadati e cooperazione internazionale**, è possibile risalire alle fonti. Anche quando si nascondono dietro a un gattino su Telegram.

□□ Ti è arrivato un SMS su un pacco in arrivo?

“Il tuo pacco ha avuto un problema, clicca qui per sbloccarlo pagando una piccola somma”.
Se hai ricevuto un messaggio così, non sei solo. Sei potenzialmente uno dei **milioni di “pesci”** presi di mira da una delle truffe digitali più subdole e sofisticate degli ultimi anni.

Dietro queste trappole via SMS non ci sono hacker improvvisati. C’è un’organizzazione strutturata, un software chiamato *Magic Cat*, e un giovane sviluppatore cinese noto online con il nome di **Darcula**.

□□ Cos’è la truffa del pacco “bloccato”

□□ Il phishing dei pacchi

Il sistema sfrutta il meccanismo del **phishing**: un link che imita un sito ufficiale (di corrieri come GLS, UPS o Amazon), e una finta richiesta di pagamento per sbloccare una consegna. Il tutto con **l’unico scopo di rubare i dati della tua carta di credito**.

□□ “Pesci” e “gattini”: come parlano i truffatori

I truffatori definiscono le vittime “pesci”. Il nome del software che usano – *Magic Cat* – suona ironico, quasi infantile. Ma dietro quel “gattino magico” si nasconde un sistema industriale per truffare migliaia di persone in tutto il mondo.

□□ Il software della truffa: Magic Cat

Magic Cat è il cuore del sistema. Analizzato per un anno intero da NRK, Le Monde e Bayerischer Rundfunk con l’aiuto degli esperti di Mnemonic, è risultato essere un **servizio di truffa in abbonamento**.

□□ Come funziona

• I criminali acquistano una licenza su Telegram per poche centinaia di dollari al mese.
• Possono scegliere tra oltre 300 falsi siti clonati di corrieri e aziende internazionali.
• Il software invia automaticamente centinaia di SMS a potenziali vittime.
• Gli SMS contengono link a pagine false che imitano perfettamente quelle ufficiali.
• Quando una vittima inserisce i dati della carta, il sistema li registra in tempo reale.

□□ Chi è Darcula?

Dietro Magic Cat si cela **Yucheng C.**, 24 anni, provincia cinese di Henan. Online si fa chiamare **Darcula**, e usa come immagine profilo gattini o personaggi dei cartoni animati.

Nonostante l’anonimato digitale, l’inchiesta è riuscita a rintracciarlo attraverso i **metadati dei file Word** che lui stesso condivideva su Telegram come manuali d’uso del suo software.

☎ La chiamata a sorpresa

Quando i giornalisti hanno provato a contattarlo, ha risposto un altro uomo: **Liao Liu**, che si è

presentato come il suo “datore di lavoro”. Ha ammesso che Darcula è “quello che vende di più”, ma ha detto di non poter condividere informazioni sull’azienda.

□□ Una truffa industriale, non un gioco da ragazzi

□□ I numeri della frode

Solo in Norvegia, *Magic Cat* ha colpito **19.000 persone in sette mesi**. A livello globale, si parla di **centinaia di migliaia di vittime**.

Sui canali Telegram dei truffatori circolano prove di spese di lusso fatte con le carte rubate: **borse di alta moda, iPhone pieni di dati bancari, gioielli**.

□□ Il video virale degli SMS truffaldini

Darcula ha pubblicato un video dove si vedono **decine di telefoni accesi** che inviano SMS ininterrottamente. Una catena industriale della frode digitale. Ogni telefono un’arma. Ogni click, un potenziale furto.

□□ La struttura aziendale delle truffe

Quello che colpisce è il **modello organizzativo**: queste truffe funzionano come vere aziende. Con team tecnici, assistenza clienti, manuali, aggiornamenti. E con un **mercato globale su Telegram** dove il software viene venduto e distribuito con licenza.

□□ Come riconoscere e difendersi

□□ Segnali d’allarme

• Un messaggio che ti chiede di pagare per un pacco di cui non ricordi l’ordine.
• Un link che non corrisponde al sito ufficiale del corriere.
• Una pagina che ti chiede subito i dati della carta di credito.

□□ Cosa fare

• Non cliccare su link ricevuti via SMS se non sei assolutamente certo della provenienza.
• Controlla manualmente lo stato delle spedizioni dai siti ufficiali.
• Usa sistemi di verifica a due fattori per i tuoi pagamenti.
• Blocca e segnala il numero al tuo operatore.
• Denuncia il messaggio al servizio antiphishing nazionale o alla Polizia Postale.

□□ Giornalismo “satellitare” e nuove inchieste

L’inchiesta è parte della serie “Muckrakers”, che punta i riflettori su trame criminali digitali e frodi transnazionali. Come accade con le inchieste parallele di *Placemarks*, che usano strumenti satellitari per indagini su larga scala, anche in questo caso la collaborazione fra giornalisti e tecnologi ha permesso di **scoperchiare una rete criminale sofisticata**.

□□ Truffe sempre più globali, ma anche più

Questa vicenda ci insegna che le truffe digitali oggi **non sono più improvvisate**, ma costruite con cura, vendute come “servizi”, e gestite come imprese.

Ma ci dimostra anche che, con **indagini accurate, tecnologia OSINT, metadati e cooperazione internazionale**, è possibile risalire alle fonti. Anche quando si nascondono dietro a un gattino su Telegram.