

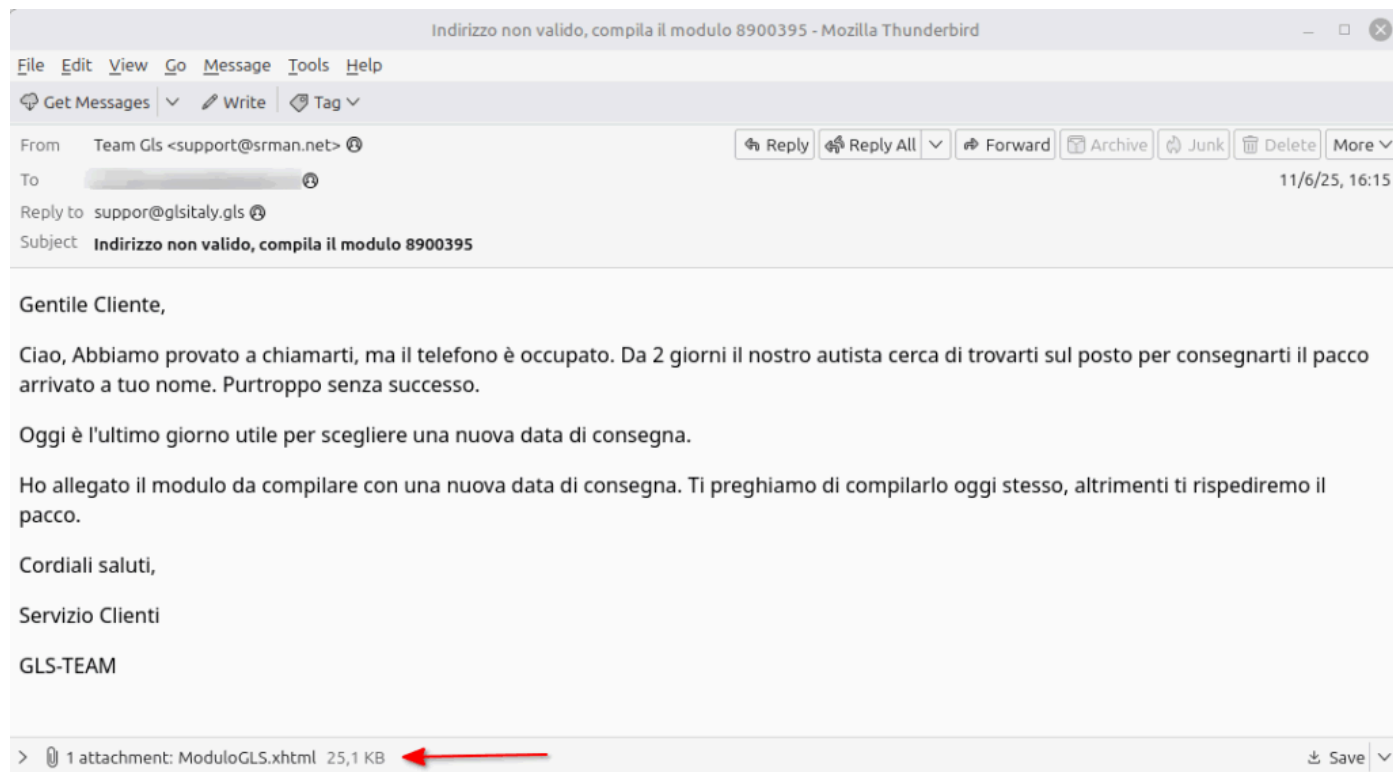
# Analisi di Remcos RAT diffuso in Italia con campagna ClickFix a tema GLS



cert-agid.gov.it/news/analisi-di-remcos-rat-diffuso-in-italia-con-campagna-clickfix-a-tema-gls

08/11/2025

## [ClickFix GLS remcos](#)

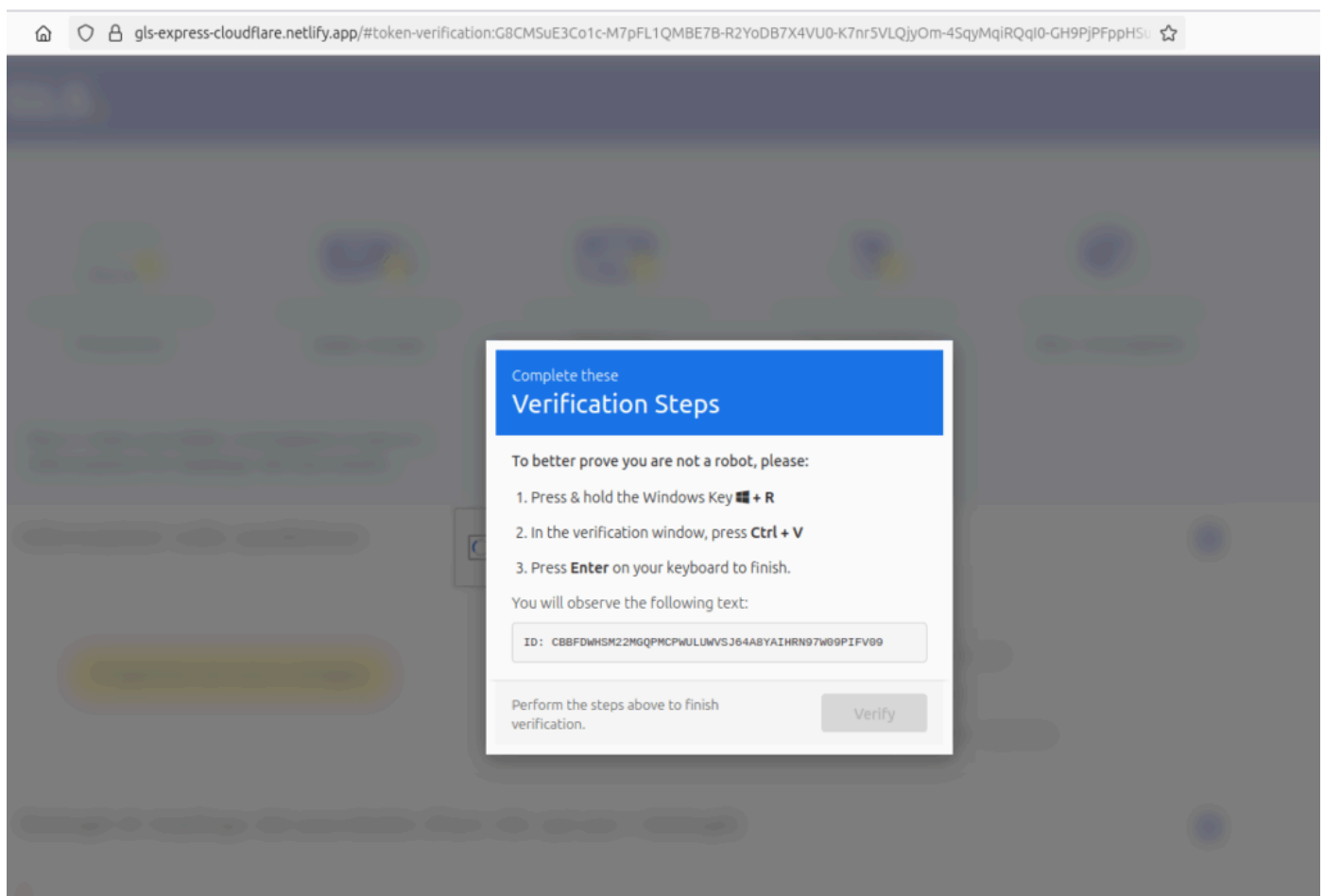
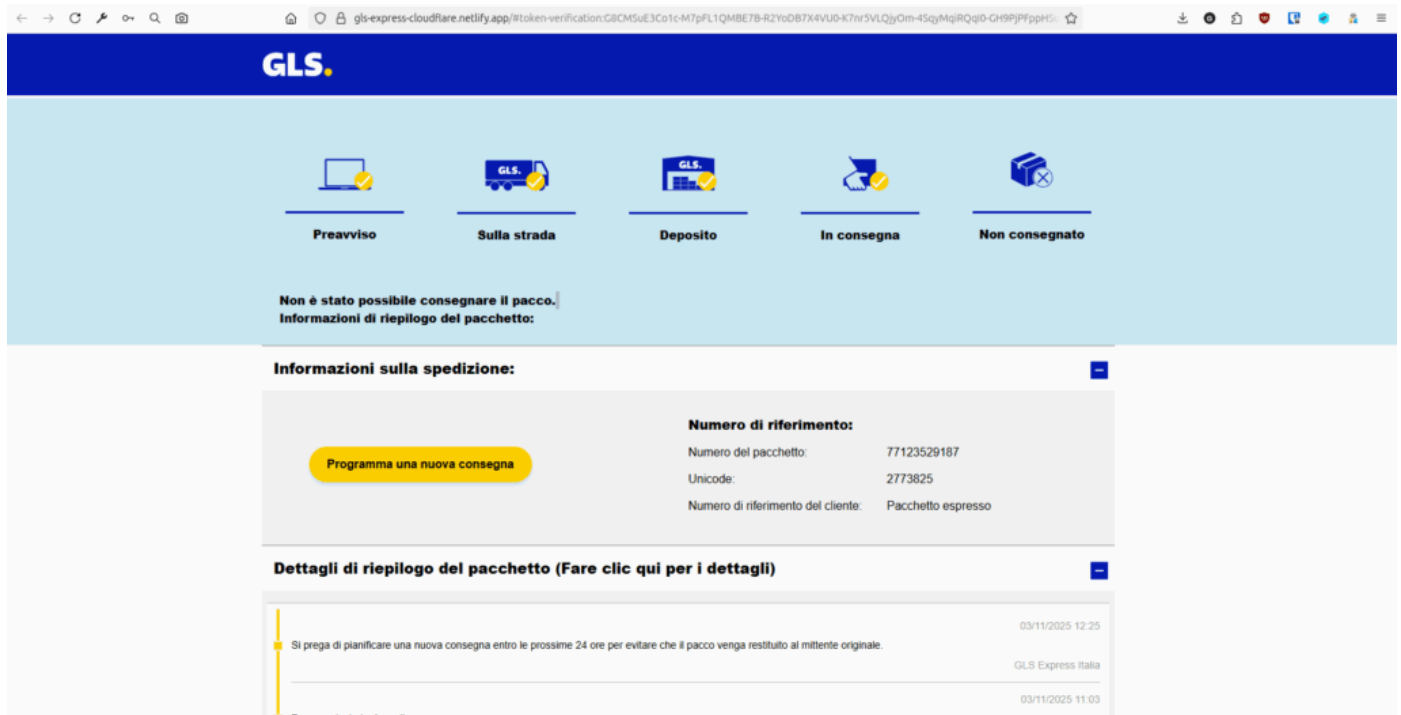


*Email utilizzata per la campagna malspam*

È in corso una campagna malspam, diffusa su larga scala, che utilizza il **brand GLS** come esca per indurre gli utenti a compilare un presunto modulo di riconsegna.

Le email presentano come oggetto “*Indirizzo non valido, compila il modulo 8900395*” e contengono un testo che simula una comunicazione del servizio clienti GLS, segnalando un problema nella consegna di un pacco e invitando a compilare un allegato.

L'allegato, un file **XHTML**, contiene codice JavaScript offuscato mediante operazioni **XOR** che, una volta decodificato, reindirizza l'utente verso il dominio malevolo ospitato sulla piattaforma *Netlify*.



Il sito replica l'aspetto del portale GLS e sfrutta la tecnica [ClickFix](#): tramite istruzioni di ingegneria sociale induce la vittima a copiare e incollare comandi nel terminale che scaricano o eseguono codice dannoso compromettendo il sistema.

Già osservata in campagne recenti, la tecnica usa un falso **CAPTCHA** per convincere l'utente a compiere azioni apparentemente legittime (incollare comandi o eseguire scorciatoie) che in realtà attivano codice dannoso. L'esecuzione manuale rende la campagna più difficile da intercettare e neutralizzare.

Seguendo le istruzioni del falso **CAPTCHA** viene eseguito un comando **mshta** che richiama un file **.hta** remoto passando un parametro che probabilmente funge da identificativo. Dall'analisi delle email, l'URL al file HTA rimane costante mentre il parametro varia puntualmente.

Il file HTA risulta totalmente offuscato. Il codice viene decodificato all'apertura tramite una funzione **XOR** con chiave inclusa nello script.

The screenshot shows the Cyberchef web application interface. On the left, the 'Recipe' panel is configured with 'From Base64' selected, 'Remove non-alphabet chars' checked, and 'Strict mode' unchecked. Below this, the 'XOR' panel is active, showing a key of 'fgTypHHvmuBddZ', 'UTF8' encoding, and 'Standard' scheme. The 'Input' panel on the right contains a long Base64-encoded string. The 'Output' panel displays the resulting JavaScript code, which is a Universal Downloader script. The code includes comments about its compatibility with Windows XP, 7, 8, 10, 11, and Server 2003-2022. It also includes a configuration section with a URL and filename generated using random strings.

*Codice deoffuscato con Cyberchef*

Il payload ha lo scopo di scaricare da un dominio secondario un file binario e avviarlo sul sistema.

All'analisi preliminare del file binario si rileva la presenza di una risorsa denominata **SETTINGS**, elemento tipico riscontrato nei sample di **Remcos RAT**. Questo suggerisce che il binario possa essere una build di Remcos e quindi finalizzato a controllo remoto, raccolta dati e caricamento/avvio di payload secondari.

Date	Time	Attr	Size	Compressed	Name
2025-10-11	13:20:23	.....	429056	429056	.text
2025-10-11	13:20:23	.....	135168	135168	.rdata
2025-10-11	13:20:23	.....	4096	4096	.data
2025-10-11	13:20:23	.....	24064	24064	.pdata
		.....	1150	1128	.rsrc/1033/ICON/1.ico
		.....	2462	2440	.rsrc/1033/ICON/2.ico
		.....	4286	4264	.rsrc/1033/ICON/3.ico
		.....	9662	9640	.rsrc/1033/ICON/4.ico
		.....	1303	1303	.rsrc/0/RCDATA/SETTINGS
		.....	62	62	.rsrc/1033/GROUP_ICON/123
2025-10-11	13:20:23	.....	3584	3584	.reloc
2025-10-11	13:20:23	.....	222	222	.rsrc 1

Dall'analisi della risorsa **SETTINGS** emerge chiaramente la tipica configurazione di **Remcos**, una tra le minacce più diffuse nel panorama italiano insieme a *Formbook*.

The screenshot shows a hex editor window titled "SETTINGS". The left pane displays hexadecimal data, and the right pane displays the corresponding ASCII text. Annotations include:

- A red box labeled "Key size" pointing to the value "A3" at offset 0x00000000.
- A green box labeled "Key RC4" pointing to the value "E6" at offset 0x000000A0.
- A pink box labeled "Data RC4" pointing to the value "7F" at offset 0x000000B0.

The hex data is as follows:

```

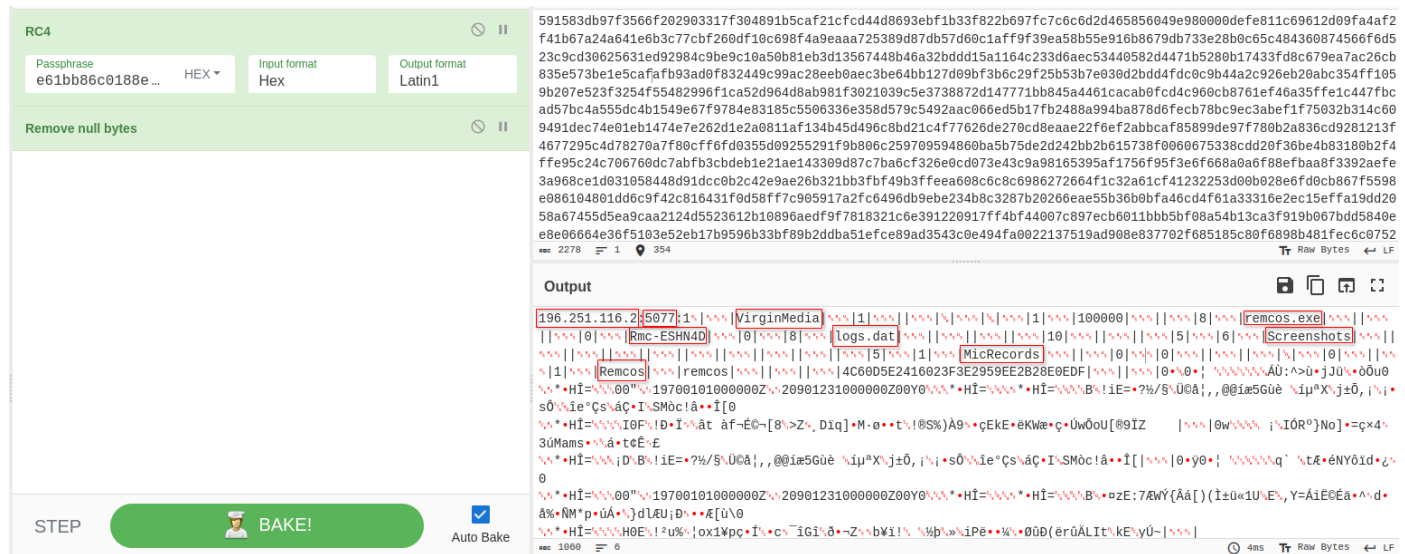
00000000 A3 E6 1B B8 6C 01 88 E4 BB 54 90 9C 82 F7 08 82
00000010 04 AE 9E 55 54 13 46 20 01 A1 CC 73 55 B8 41 8B
00000020 DE E3 E8 3F 26 14 CC 0A B9 A5 38 9E 0A 44 A6 C6
00000030 B2 12 F3 89 27 AB DB CE E1 DF 14 0B 98 43 81 98
00000040 06 EB 70 D4 4F 02 B6 23 17 ED 2C 65 C4 57 F7 9F
00000050 98 36 75 B9 7B AE CD AE C6 7A 8D 90 50 0A B6 2B
00000060 8E B9 2D 3D 9B A9 76 83 5A 29 2D 0E 24 BE A3 A8
00000070 A6 34 87 3D E0 3A 94 86 6E 8C A1 74 87 9F 8F 12
00000080 64 48 EB E1 F0 EA 50 E3 FB 13 CD D9 4A 8E E2 63
00000090 43 6B E3 0D 16 73 C1 7F 8C F5 8F 48 FA 16 50 02
000000A0 E6 D8 CF C6 59 15 83 DB 97 F3 56 6F 20 29 03 31
000000B0 7F 30 48 91 B5 CA F2 1C FC D4 4D 86 93 EB F1 B3
000000C0 3F 82 2B 69 7F C7 C6 C6 D2 D4 65 85 60 49 E9 80
000000D0 00 0D EF E8 11 C6 96 12 D0 9F A4 AF 2F 41 B6 7A
000000E0 24 A6 41 E6 B3 C7 7C BF 26 0D F1 0C 69 8F 4A 9E
000000F0 AA A7 25 38 9D 87 DB 57 D6 0C 1A FF 9F 39 EA 58
00000100 B5 5E 91 6B 86 79 DB 73 3E 28 B0 C6 5C 48 43 60
00000110 87 45 66 F6 D5 23 C9 CD 30 62 56 31 ED 92 98 4C
00000120 9B E9 C1 0A 50 B8 1E B3 D1 35 67 44 8B 46 A3 2B
00000130 DD D1 5A 11 64 C2 33 D6 AE C5 34 40 58 2D 44 71
00000140 B5 28 0B 17 43 3F D8 C6 79 EA 7A C2 6C B8 35 E5
00000150 73 BE 1E 5C AF AF B9 3A D0 F8 32 44 9C 99 AC 28
00000160 EE B0 AE C3 BE 64 BB 12 7D 09 BF 3B 6C 29 F2 5B
00000170 53 B7 E0 30 D2 BD D4 FD C0 C9 B4 4A 2C 92 6E B2
00000180 0A BC 35 4F F1 05 9B 20 7E 52 3F 32 54 F5 54 82
00000190 99 6F 1C A5 2D 96 4D 8A B9 81 F3 02 10 39 C5 E3
000001A0 73 88 72 D1 47 77 1B B8 45 A4 46 1C AC AB 0E CD
  
```

The ASCII representation on the right shows various characters, including "l...T...", "UT.F...sU.A.", "p.0...#...e.W...", "6u.{...z..P..+", "4.=...n..t...", "dH...P...J..c", "Ck...s...H..P.", "...Y...Vo ).1", ".0H...M...", "?..+i...e..I..", "...../A.z", "\$.A...|. &...i.J.", "..%8...W...9.X", ".^..k..y..s>(...\HC`", ".Ef...Data RC4", "...P...5gD.F.+ ..Z.d.3...4@X-Dq", ".(..C?...y.z.l.5.", "s...\...2D...(", ".....d...}...;l).[", "S..0.....J,.n.", "..50... ~R?2T.T.", ".o...-M.....9..", "s r Gw F F".

Offset: 0xA3; 0xA3 bytes from 0x1 to 0xA3 selected

Configurazione Remcos RAT cifrata

Una volta estratti tutti i valori utili, l'analisi tramite **CyberChef** consente di decodificare la risorsa **SETTINGS** e identificare i dettagli di configurazione rilevanti (C2, agent ID, intervalli, etc.), utili per il blocco tramite IoC e la correlazione degli incidenti.



Decodifica configurazione Remcos RAT

## Conclusioni

Le campagne basate sulla tecnica **ClickFix** sono ormai una tendenza consolidata: da circa un anno questo metodo viene sfruttato sempre più spesso per distribuire malware attraverso inganni che spingono l'utente a eseguire manualmente comandi dannosi.

In Italia la prima evidenza documentata risale al [gennaio](#) di quest'anno, quando la tecnica è stata utilizzata per diffondere [Lumma Stealer](#), uno dei principali infostealer in circolazione. Da allora, pur essendo stati osservati diversi tentativi, nel nostro Paese non si sono registrate campagne massive mirate, a differenza di quanto accade in altri contesti internazionali dove il fenomeno è molto più diffuso.

I malware writer prediligono questa tecnica perché consente di aggirare i sistemi di sicurezza automatici. Il codice malevolo non viene scaricato o eseguito direttamente, ma solo dopo l'intervento dell'utente. L'esecuzione manuale rende il rilevamento più difficile per antivirus, sandbox e sistemi EDR, offrendo un alto tasso di successo a fronte di uno sforzo tecnico relativamente basso.

ClickFix rappresenta quindi un'evoluzione dell'ingegneria sociale applicata al malware delivery. Non punta a sfruttare vulnerabilità del software, ma quella più semplice e sempre attuale: l'interazione umana.

## Indicatori di compromissione

---

Il CERT-AGID ha già condiviso i relativi IoC con le organizzazioni [accreditate al flusso](#) per favorirne la loro diffusione. Al fine di rendere pubblici i dettagli di questa campagna si riportano di seguito gli indicatori rilevati.

**Link:** [Download IoC](#)