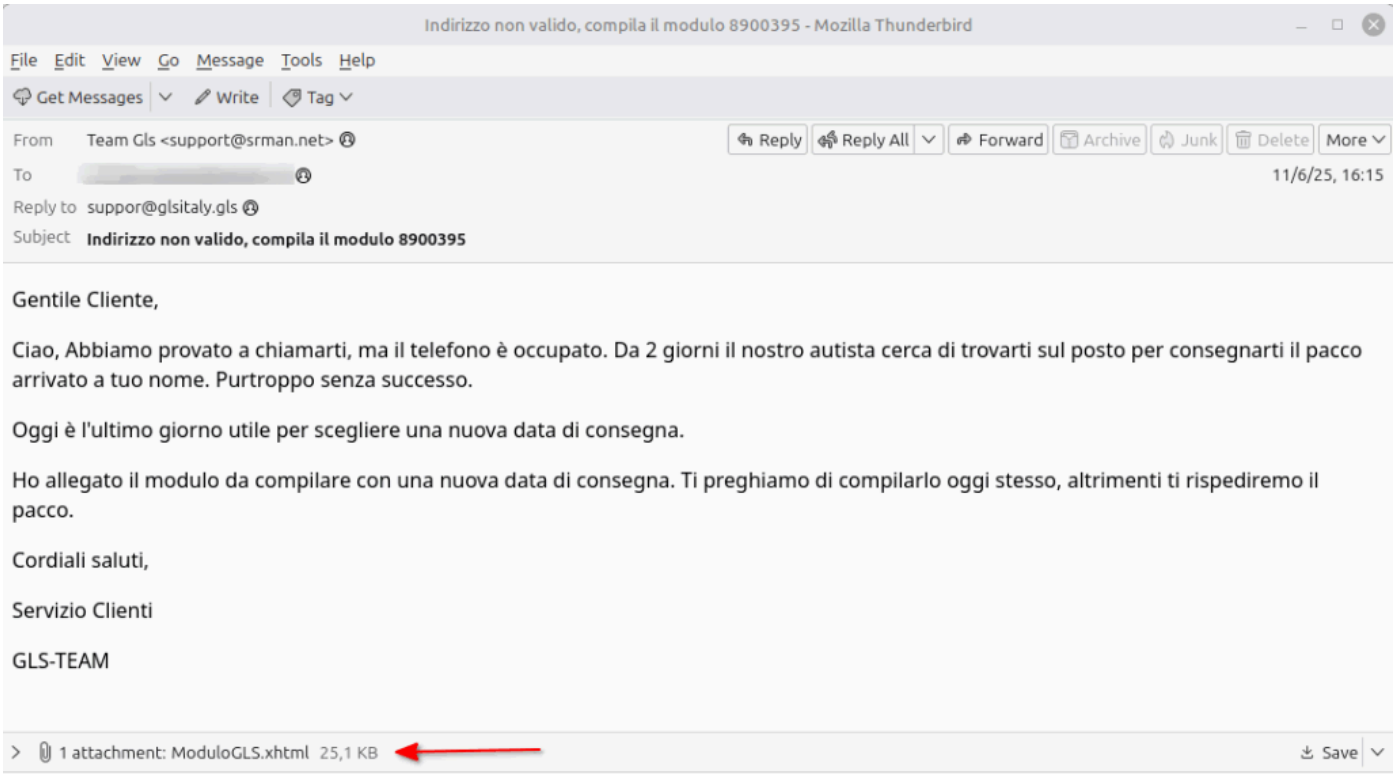
Analisi di Remcos RAT diffuso in Italia con campagna ClickFix a tema GLS

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

08/11/2025

ClickFix GLS remcos

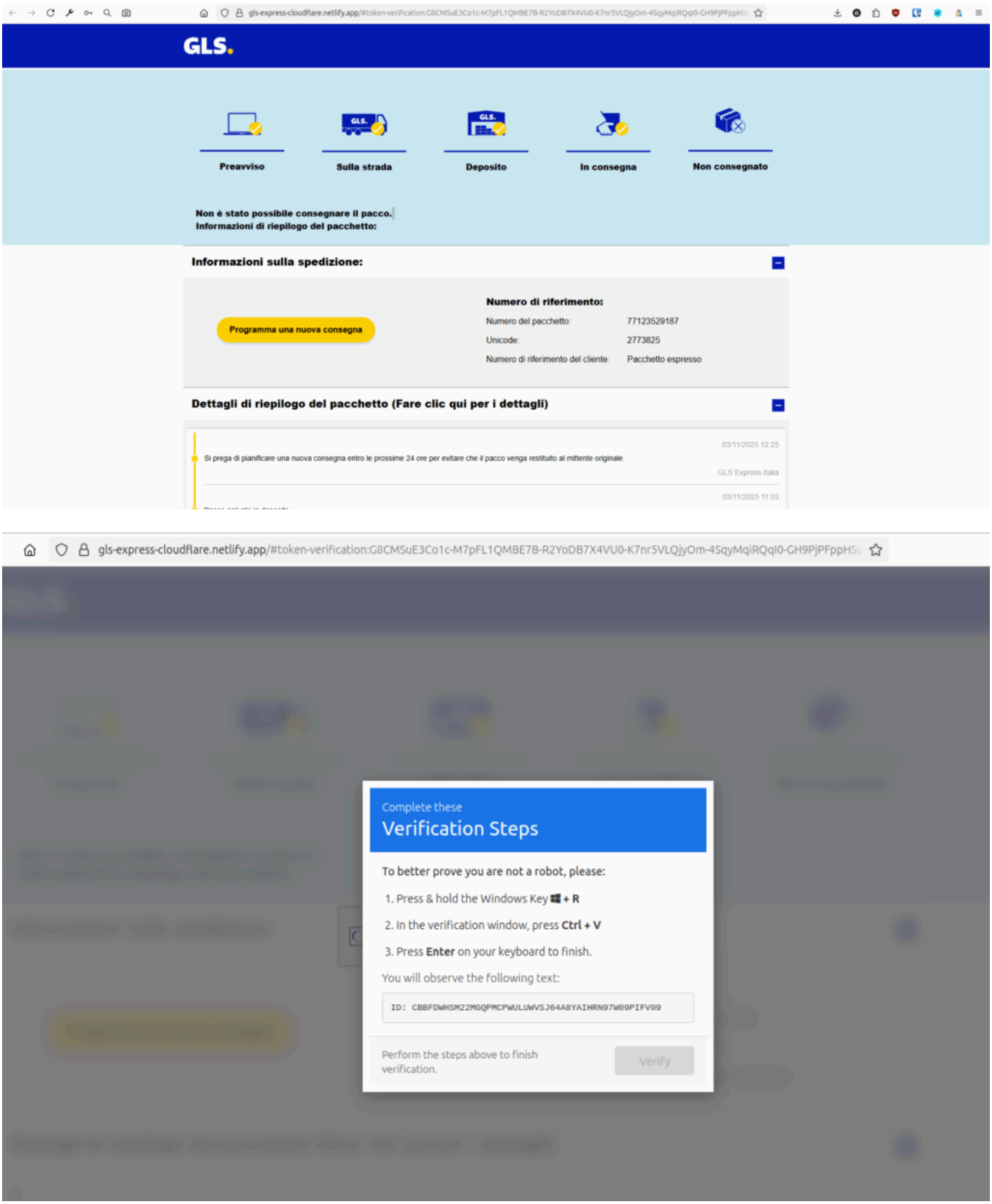


Email utilizzata per la campagna malspam

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*.

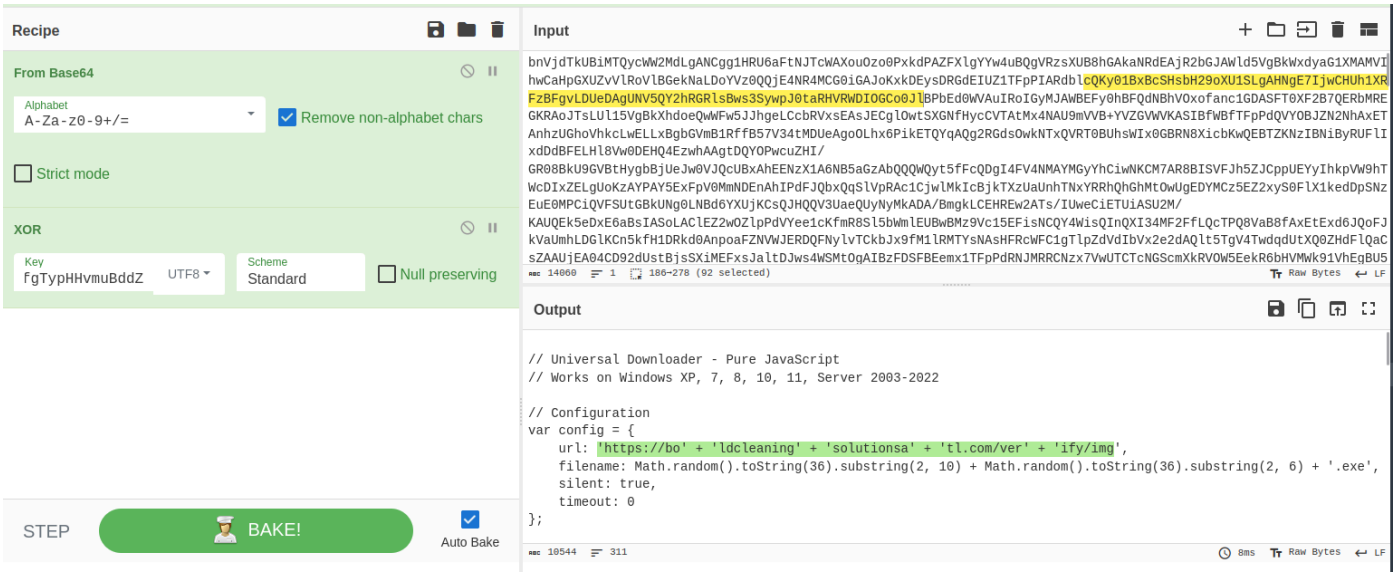


Il sito replica l’aspetto del portale GLS e sfrutta la tecnica **ClickFix**: tramite istruzioni di ingegneria sociale induce la vittima a copiare e incollare comandi nel terminale che scaricano o eseguono codice dannoso compromettendo il sistema.

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.



Codice deoffuscato con Cyberchef

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

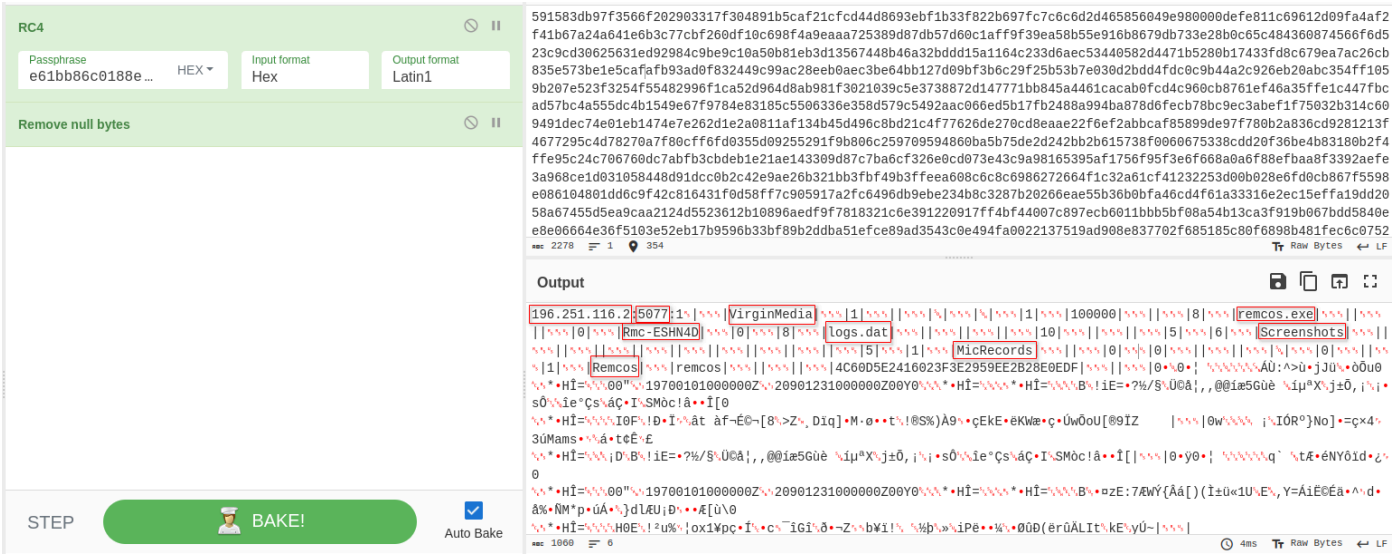
All'analisi preliminare del file binario si rileva la presenza di una risorsa denominata `SETTINGS`, elemento tipico riscontrato nei sample di **Remcos RAT**. Questo suggerisce che il binario possa essere una build di Remcos e quindi finalizzato a controllo remoto, raccolta dati e caricamento/avvio di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

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