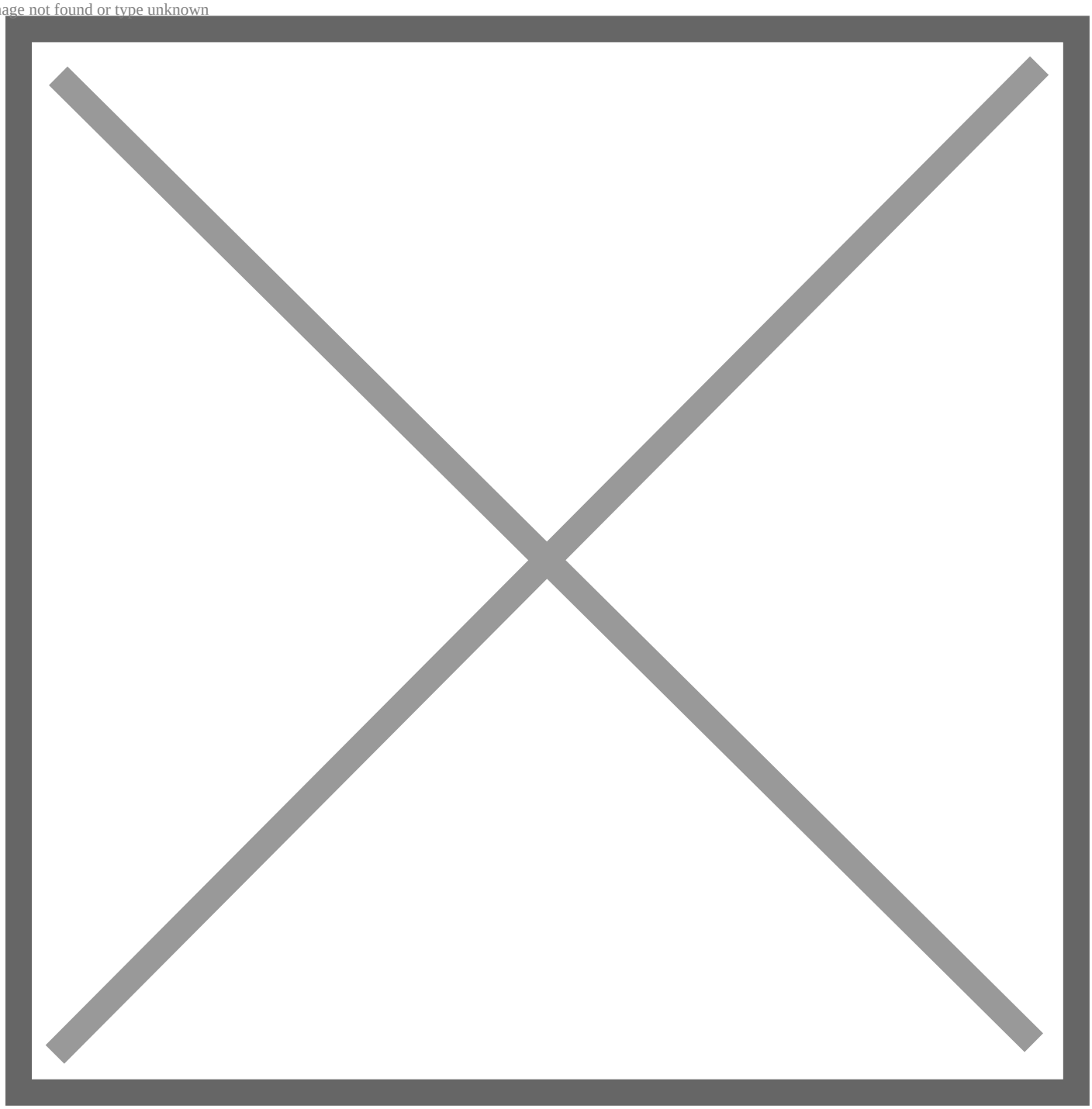
Image not found or type unknown



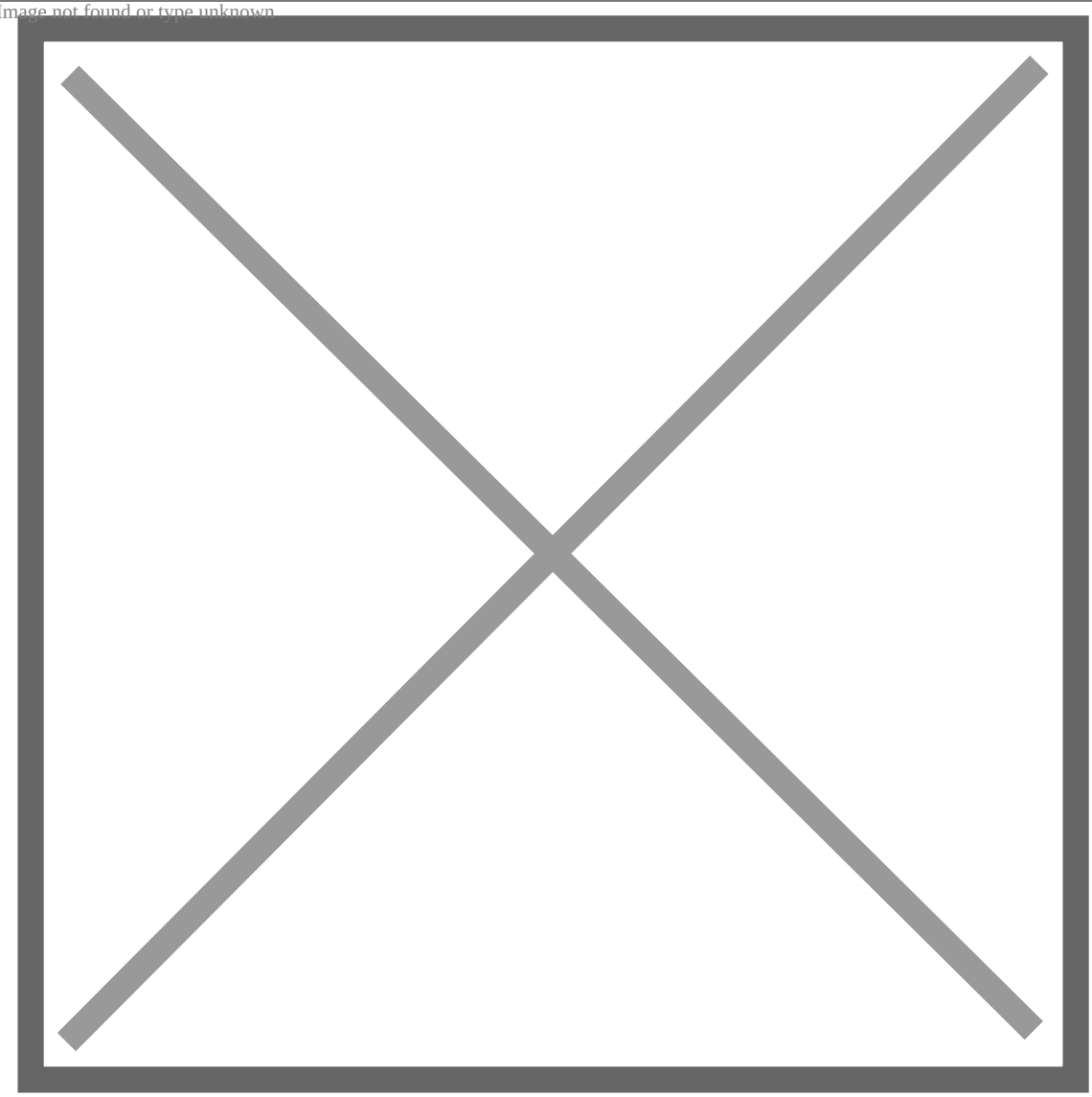
web & insidie

Cybercriminali sfruttano la morte di Francesco per lanciare truffe

CRONACA 30_04_2025

Image not found or type unknown

Daniele Ciacci



A seguito della morte di Papa Francesco, alcuni cybercriminali hanno lanciato numerose campagne malevole, sfruttando questo evento globale di grande risonanza per lucrare. Questa tattica non è nuova: gli hacker da tempo sfruttano eventi mondiali significativi, dalla scomparsa della Regina Elisabetta II alle catastrofi naturali e crisi come il COVID-19, per diffondere truffe, disinformazione e infezioni malware. La curiosità pubblica e le reazioni emotive rendono questi momenti delle opportunità ideali per gli attacchi informatici.

Tipicamente, queste campagne iniziano con disinformazione sui social media come Instagram, TikTok o Facebook, dove vengono caricate immagini false generate dall'intelligenza artificiale. Queste manovre mirano a catturare l'attenzione degli utenti, spingendoli a cercare ulteriori informazioni tramite motori di ricerca o a cliccare su link incorporati nelle immagini o nei post. Una volta coinvolti, gli utenti possono essere reindirizzati verso siti web fraudolenti che servono vari scopi malevoli, dal furto di dati

alle truffe finanziarie.

In questo caso, alcuni link nascosti veicolano il traffico verso siti web che promuovono fake news su Papa Francesco e relativo successivo Conclave. Quando un utente clicca su uno dei link, viene reindirizzato a una falsa pagina Google che promuoveva una truffa di carte regalo—una tattica comune usata per ingannare le persone e sottrarre informazioni sensibili o denaro attraverso il phishing, una tecnica fraudolenta che utilizza e-mail, messaggi o siti web contraffatti per ingannare gli utenti e indurli a rivelare informazioni sensibili come password, dati bancari o personali.

Un'altra minaccia significativa legata a questi eventi è il cosiddetto "SEO poisoning" (avvelenamento dell'ottimizzazione per i motori di ricerca). In questo caso, i cybercriminali pagano per posizionare i loro siti malevoli tra i risultati legittimi di ricerca, ingannando gli utenti che pensano di accedere a informazioni affidabili.

Il problema è aggravato dal fatto che molti di questi domini non appaiono negli strumenti di intelligence sulla reputazione. I domini potrebbero essere stati registrati recentemente o tenuti dormienti per mesi senza mostrare comportamenti malevoli, consentendo loro di eludere il rilevamento da parte della maggior parte dei sistemi di cybersecurity.

Per proteggersi, gli esperti consigliano di mantenere aggiornati browser e il sistema operativo, oltre a utilizzare strumenti di protezione della navigazione. Inoltre, val la pena essere cauti con titoli sensazionalistici, specialmente sui social media. È buona prassi evitare di cliccare su link da fonti sconosciute e invece verificare domini o file sospetti. Considerare l’acquisto della licenza di firewall e software di sicurezza avanzati che includano protezione contro il phishing può essere una buona opzione.