Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
Organo del Ministero dell'Interno per la sicurezza cibernetica

Protocollo	RMPAC7/2025/002/0412	**Data**	17/10/2025
Destinatari	Enti destinatari delle informazioni riservate.		

Oggetto	**Phishing: campagna a tema PagoPA sfrutta il meccanismo di open redirect**
Data evento	Evento in corso
Descrizione Evento	Nell'ambito della propria attività istituzionale questo Centro è venuto a conoscenza che è stata tracciata in Italia una nuova variante della campagna di phishing a tema multe ai danni di PagoPA, che prevede lo sfruttamento di open redirect su domini legittimi di Google. Nel dettaglio, un URL malevolo inizia con un sottodominio Google (adservice[.]google.be) e sembrerebbe portare a un servizio del browser, ma in realtà il parametro finale sfrutta il meccanismo open redirect, effettuando il reindirizzamento verso una pagina intermedia ospitata su bio[.]site, piattaforma legittima che consente di creare pagine di presentazione con link personalizzati. Questa pagina fraudolenta riproduce il logo di PagoPA e fa riferimento a presunte infrazioni stradali non pagate. La potenziale vittima viene quindi indotta a cliccare su un pulsante riportante la dicitura "Accedi al servizio di regolamento", che conduce a una nuova pagina di phishing, graficamente imitante il portale ufficiale e ospitata su privatedns[.]org – un servizio legittimo che offre registrazioni gratuite di sottodomini a terzi. A questo punto, l'utente viene spinto a inserire i propri dati personali (nome e cognome, data di nascita, CAP e indirizzo e-mail) e i dettagli di carte elettroniche di pagamento. *Si allega alla presente un archivio zip cifrato con password "cnaipic", contenente gli indicatori di compromissione afferenti alla presente comunicazione.*
Note	Si prega di fornire riscontro a questa nota, facendo riferimento al nostro numero di protocollo, solo in caso di effettiva compromissione dei sistemi informatici.

ES/LC

IL DIRETTORE DEL CNAIPIC
V.Q.A. Riccardo CROCE

ORIGINALE FIRMATO AGLI ATTI

Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
Tel. +39-06-46530118 – Mob. +39-3138063547 - Fax +39-06-46530607
cnaipic@poliziadistato.it - - dipps037.0330@pecps.interno.it