Come funziona Anubis, il malware che sfrutta l'INPS come esca

I Criminal Hacker stanno prendendo di mira l'**INPS**. Ma non riguarda il sito ufficiale dell'ente nazionale italiano, ma vere e proprie truffe utilizzando l'ente previdenziale italiano come esca.

La denuncia dell'INPS

Due giorni fa, l'Istituto guidato da **Pasquale Tridico**, ha comunicato ai propri utenti che si sono verificato sospetti **tentativi fraudolenti** di richiesta di **dati sensibili**.

In particolare, spiega l'INPS, sarebbe in atto una massiccia campagna malware attraverso l'invio di **SMS** che invitano a cliccare su un link per aggiornare la propria domanda **COVID-19** e inducono a installare una app malevola.

"*Questi SMS,* conferma l'ente previdenziale, ***non sono inviati dall'INPS.*** *Eventuali SMS che l'Istituto dovesse inviare non conterranno link a siti web, l'unico accesso ai servizi INPS è tramite il sito istituzionale*".

Il CERT-PA conferma la denuncia dell'INPS

La conferma della campagna malevola in atto arriva anche dal **CERT-PA**, la struttura che opera all'interno dell'**Agenzia per l'Italia Digitale** e preposta al trattamento degli incidenti di sicurezza informatica dei domini della pubblica

amministrazione.

“La campagna malevola denunciata dall’INPS si appoggia al dominio inps-informa.online, un dominio palesemente falso, ha comunicato il Cert-PA. *La homepage contiene un link per il download di una fantomatica applicazione per richiedere un bonus in denaro, se installata l’applicazione è in grado di infettare il telefono. L’applicazione,* continua la struttura*, è diffusa anche tramite QR code che rimandano al link per il download.*

Il CERT-PA ha quindi analizzato l’applicazione e provveduto a diffonderne gli indicatori di compromissione alla constituency tramite il Canale Nazionale di Trasmissione IoC (CNTI).

Il malware Anubis

L’applicazione, spiega il CERT-PA, *è un derivato del* ***malware Anubis****. Il codice di Anubis è così riusato per l’infezione di dispositivi Android da essere stato impiegato anche in precedenti campagne FTCODE, con cui condivide buona parte delle funzionalità*“.

Il malware Anubis è in grado di:

- di leggere gli SMS ed occultare gli SMS ricevuti;
- mutare tutti i volumi del cellulare e bloccare lo schermo come forma di riscatto;
- rubare informazioni come numero di telefono, operatore e modello di cellulare;
- disinstallare applicazioni, mostrare pagine di phishing all’apertura di determinate applicazioni (di home banking, IM e client e-mail);
- impedire la propria disinstallazione (chiudendo la finestra di sistema ogni volta che ci si prova)

Cosa difendersi

- Se ricevete sms dall’INPS NON aprite nessun link
- Non installate mai programmi scaricati fuori dagli store ufficiali
- Ignorate email, sms o altre comunicazioni che ci chiedono di compiere una qualsiasi azione (download allegato, clic su link)
- Se siete stati truffati denunciate subito l’accaduto alla polizia locale con più dettagli possibili
- Comunicate la frode alla vostra banca e tenete sotto controllo il vostro conto

https://www.key4biz.it/come-funziona-anubis-il-malware-che-sfrutta-linps-come-esca/299611/