Polizia di Stato

Genova: attraverso lo “Smishing-Vishing” svuotavano i conti in tutt’Italia, quattro denunciati

Scoperto dalla Polizia postale di Genova un gruppo criminale specializzato in phishing bancario di ultima generazione.

Al termine dell’indagine gli agenti hanno denunciato a piede libero quattro persone responsabili di frodi ai correntisti in tutt’Italia, sottraendo cifre da un minimo di 300 fino a 55.000 euro.

Le frodi venivano messe in atto con lo “Smishing-Vishing” ovvero attraverso l’invio di comunicazioni che sembrano provenire dalla propria banca, nelle quali si invitano i correntisti ad accedere al proprio conto on-line mediante un web-link.

Lo “smishing” in particolare si concretizza attraverso messaggi sms malevoli che, per una mera affinità semantica, si collocano in coda ad altri messaggi autentici ricevuti dalla banca; tali sms contengono link di rinvio a pagine di phishing dove l’utente, ritenendo di operare sulla pagina veritiera, è indotto ad inserire le proprie credenziali bancarie consegnando così i propri dati ai cyber-criminali.

La tecnica del vishing invece consiste nel contattare la potenziale vittima tramite una chiamata telefonica nella quale un finto operatore di banca, attraverso raggiri ed argomentazioni capziose, la persuade a fornire i codici dispositivi del proprio rapporto finanziario; è frequente, nel corso delle chiamate, che il truffatore chiede alla vittima la necessità di ottenere il suo codice al fine di bloccare alcuni tentativi illeciti di prelievo da parte di terzi. Sfruttando questo momento di incertezza e utilizzando numeri telefonici che sembrano arrivare dalla propria banca, i criminali ottengono le credenziali di accesso ai conti correnti che subito dopo provvedono a svuotare.

Queste frodi hanno avuto un incremento notevole dall’inizio della pandemia a causa delle limitazioni a poter andare fisicamente in filiale, con il conseguente aumento dei rapporti telefonici con le banche.

L’inchiesta ha fatto emergere anche la sicurezza con cui agivano gli indagati i quali pensando di farla franca in alcuni cassi hanno apostrofato e insultato le vittime con frasi del tipo: “Ti abbiamo fregato” o “Sei stato un ciambellone”.

La Polizia Postale e delle Comunicazioni attraverso le Sezioni Financial Cyber Crime si è prefissata l’obiettivo di colpire in maniera selettiva questa specifica attività criminale denominata “ Alias “, che sta mietendo numerose vittime in ogni contesto sociale e geografico, provocando danni per milioni di euro

Alcuni consigli per difendersi da queste frodi

I numeri verdi per loro natura sono numeri che funzionano in ricezione e non vengono utilizzati per effettuare chiamate verso gli utenti e quindi la Banca mai contatterà i propri clienti attraverso un numero verde.

Anche i numeri territoriali assegnati alla banca possono essere nascosti quindi nel dubbio è meglio concludere la chiamata e telefonare direttamente alla propria filiale.

Inoltre è bene ricordare che nessuna banca richiede i dati di accesso al proprio conto via email o via SMS.

Qualora si sia caduti nella trappola fornendo i propri dati, contattare immediatamente il numero verde

della propria banca e bloccare l’accesso al conto ed eventuali pagamenti fraudolenti già effettuati.

In autonomia si può procedere immediatamente al cambio della password per accedere al conto.

Nel caso si siano forniti codici dispositivi necessari per utilizzare l’applicazione della banca installata sul proprio telefono, riutilizzare immediatamente l’applicazione: in questo modo verrà inibita la possibilità al truffatore di utilizzarla.

Concludendo:

- Non “cliccare” sui link inviati tramite e-mail o sms sospetti.

- Verificare sempre l’autenticità della pagina dell’istituto bancario.

- Non fornire alcuna credenziali di accesso/codice otp via telefono o sms.

- Effettuare la scansione del dispositivo con un antivirus aggiornato.

- Modificare le credenziali di accesso ai servizi on-line in caso di accessi sospetti.

Vincenzo M. Recchiuti

26/11/2020