

Κατά την ανάλυση των πληροφοριών που λαμβάνει η Αρχή για την Καταπολέμηση της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες, εντόπισε εκτεταμένη χρήση της απάτη της μορφής "Phishing, Pharming και Cracking" σε συνδυασμό με την απάτη "Sim Swapping".

Πιο συγκεκριμένα, οι δράστες σε αρκετές περιπτώσεις αποκτούσαν παράνομη πρόσβαση στους ηλεκτρονικούς υπολογιστές των θυμάτων και υπέκλεπταν τα ονόματα χρήστη και τους κωδικούς πρόσβασης των θυμάτων στις διαδικτυακές τραπεζικές πλατφόρμες τους. Εν συνεχεία με τη χρήση των στοιχείων αυτών εξέδιδαν εξουσιοδοτήσεις, μέσω υπηρεσιών της ηλεκτρονικής διακυβέρνησης δήθεν για λογαριασμό των. Αφού κατάφερναν να εκδώσουν όλα τα απαραίτητα έγγραφα, οι δράστες χρησιμοποιούσαν «αχυράνθρωπους» για να εκδώσουν νέες κάρτες SIM για λογαριασμό των θυμάτων. Με τον τρόπο αυτό κατάφερναν να παρακάμψουν τις διαδικασίες ασφαλείας του e-banking (αποστολή SMS ή VIBER κειμένου στους πελάτες με μοναδικό κωδικό για κάθε συναλλαγή) και να αφαιρέσουν μεγάλα χρηματικά ποσά από τα θύματα, στέλνοντάς τα σε τραπεζικό λογαριασμό νομικού προσώπου συμφερόντων τους ως δωρεές. Από αυτόν τον τραπεζικό λογαριασμό, τα κλεμμένα χρήματα προωθήθηκαν σε τραπεζικούς λογαριασμούς των δραστών ή δευτερεύοντα μέλη της Εγκληματικής Οργάνωσης ως «βοήθημα για οικογένειες σε ανάγκη».

Κατόπιν αυτού καλούμε το κοινό να παρακολουθεί καθημερινά της κινήσεις των τραπεζικών του λογαριασμών προς αποφυγή μεγάλης ζημιάς.