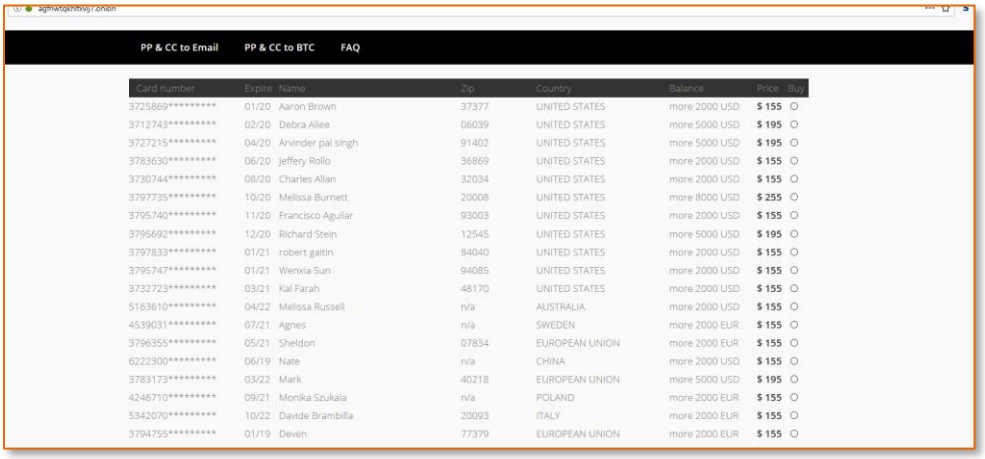
מהי הונאת SIM Swap?

הונאת SIM Swap הנה הונאה מורכבת המאפשרת באמצעות התחזות לבצע פעולות בחשבונות בנק של קורבנות ולהתגבר על השימוש של גופים פיננסיים בפין קוד והודעות SMS על מנת לאמת את זהות המשתמש.
הונאה מסוג זה, מחייבת עבודת מודיעין מקדימה של התוקף ולכן תבוצע בדרך כלל מול קורבן ספציפי ולא אקראי.

בשלב הראשון התוקפים ישימו ידיהם על פרטי חשבון בנק של הקורבן, לפרטים אלה ניתן להגיע באמצעות מתקפת פישינג מוצלחת או על ידי רכישת הפרטים באחד השווקים המחתרתיים ב – Dark Web.



דוגמה לחשבונות בנק הנמכרים ב Dark Web

כעת, התוקפים פותחים חשבון בנק עסקי נוסף על שם הקורבן ובאותו בנק, כשהם מנצלים את העובדה שיש פחות בדיקות אבטחה כשמדובר בלקוח קיים.
התוקפים מבצעת עבודת איסוף מודיעין אודות הקורבן ברשתות החברתיות, מידע זה מאפשר להם לענות על שאלות האבטחה (שנת לידה, שם הילד הבכור, שם חיית המחמד) של ספק השירותים הסלולאריים של הקורבן ולעדכן אותו שהנייד שלהם אבד או ניזוק.
לאור היכולת שלהם להזדהות מול ספק השירותים הסלולאריים, כרטיס הסים של הקורבן מבוטל והתוקף מקבל כרטיס סים חדש ומאוקטב.
כעת, כשהתוקף מחזיק בזהות הקורבן ואף מחזיק את מכשיר הטלפון המזהה של הקורבן, הוא יכול לבצע כל פעולה, לקבל שיחות ומסרונים ואף לבקש לשנות את הגדרות האבטחה כך שהקורבן ינעל מחוץ למערכות.
בנוסף למכשיר המזהה יש לתוקף גם גישה לחשבון הבנק של הקורבן וכעת הוא יכול לבצע פעולות על חשבון זה.

כמובן שלא מדובר בתקיפה פשוטה, מבחינת התוקף נדרשת עבודת הכנה ומודיעין שלפעמים אינן פשוטות, אך מתקפות כאלה ישימות, קיימות ומתרחשות באופן קבוע.
המסר החשוב מתקיפות אלה זו ההבנה שכל אחד יכול להיות קורבן למתקפה כזאת, לפעמים בגלל חשבון בנק שמפתה את התוקפים, ולפעמים לאור מקום העבודה שלו ותפקידו בארגון.
ולכן ארגונים חייבים להבין שמכשירי הטלפון החכמים של העובדים שלהם יכולים להוות תשתית פריצה למידע הארגוני ללא ידיעתו של העובד ולכן הארגונים חייבים ליישם מערכות ניהול ארגוניות, מערכות שימנעו אפשרות ממכשיר שהוחלף להתחבר למערכות הארגוניות עד שלא אושר על ידי העובד עצמו ומנהל נוסף בארגון.