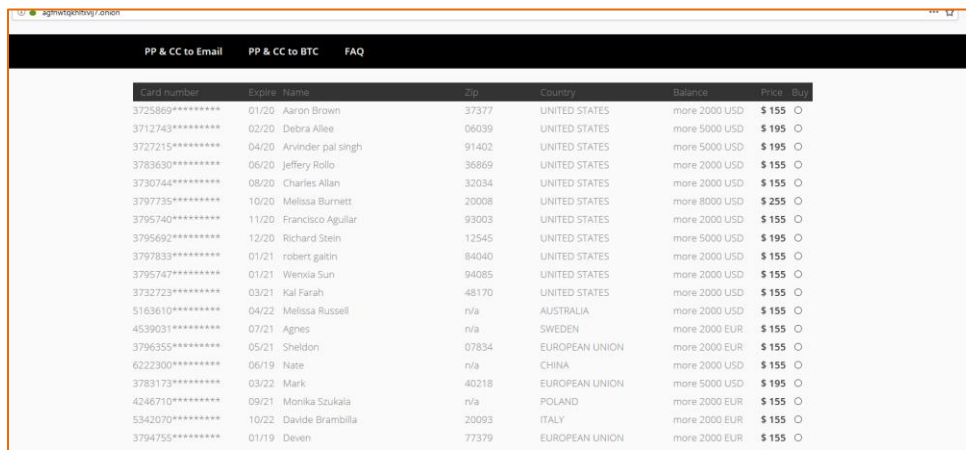


מהי הונאת SIM Swap?

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 פשיגן מוצלחת או על ידי רכישת הפרטים באחד השווקים המחתרתיים ב – Dark Web.



Card number	Expire	Name	Zip	Country	Balance	Price	Buy
3725869*****	01/20	Aaron Brown	37377	UNITED STATES	more 2000 USD	\$ 155	○
3712743*****	02/20	Debra Allee	06039	UNITED STATES	more 5000 USD	\$ 195	○
3727215*****	04/20	Arvinder pal singh	91402	UNITED STATES	more 5000 USD	\$ 195	○
3783630*****	06/20	Jeffery Rollo	36869	UNITED STATES	more 2000 USD	\$ 155	○
3730744*****	08/20	Charles Allan	32034	UNITED STATES	more 2000 USD	\$ 155	○
3797735*****	10/20	Melissa Burnett	20008	UNITED STATES	more 8000 USD	\$ 255	○
3795740*****	11/20	Francisco Aguilar	93003	UNITED STATES	more 2000 USD	\$ 155	○
3795692*****	12/20	Richard Stein	12545	UNITED STATES	more 5000 USD	\$ 195	○
3797833*****	01/21	robert gaitin	94040	UNITED STATES	more 2000 USD	\$ 155	○
3795747*****	01/21	Wenxia Sun	94085	UNITED STATES	more 2000 USD	\$ 155	○
3732723*****	03/21	Kal Farah	48170	UNITED STATES	more 2000 USD	\$ 155	○
5163610*****	04/22	Melissa Russell	n/a	AUSTRALIA	more 2000 USD	\$ 155	○
4539031*****	07/21	Agnes	n/a	SWEDEN	more 2000 EUR	\$ 155	○
3796355*****	05/21	Sheldon	07834	EUROPEAN UNION	more 2000 EUR	\$ 155	○
6222300*****	06/19	Nate	n/a	CHINA	more 2000 USD	\$ 155	○
3783173*****	03/22	Mark	40218	EUROPEAN UNION	more 5000 USD	\$ 195	○
4246710*****	09/21	Monika Szukala	n/a	POLAND	more 2000 EUR	\$ 155	○
5342070*****	10/22	Davide Brambilla	20093	ITALY	more 2000 EUR	\$ 155	○
3794755*****	01/19	Deven	77379	EUROPEAN UNION	more 2000 EUR	\$ 155	○

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 ביזוק.

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 למערכת. 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 למערכת הארגונית עד שלא אושר על ידי העובד עצמו ומנהל נוסף בארגון.

מוביסק טכנולוגיות עוסקת משנת 2011 בתכנון, יישום ותחזוקת מערכות לניהול והגנה של התקני קצה בארגונים, החברה מימשה עד כה מאות מערכות ניהול והגנה בארגונים המובילים בישראל ומיישמת הגנה מוחלטת מפני תקיפה מסוג זה.

לפרטים נוספים: info@mobisec.co.il