18 פברואר 2019
י"ג אדר תשע"ט
סימוכין: ב-ס-843

מתווה הונאות חדש באמצעות היישומון WhatsApp

תקציר

1. בשנה החולפת זוהה מתווה הונאה חדש המבוצע באמצעות היישומון WhatsApp.
2. עד כה, נצפו שתי גרסאות של אותו מתווה, אשר האחת כוללת שימוש בתא הקולי של המכשיר הנייד והשניה מובילה לעמוד דיוג.
3. טרם ידועה מטרת התוקפים, מעבר להשתלטות על מספר רב של חשבונות WhatsApp.
4. מטרת המסמך שלהלן היא חשיפה למתווה והעלאת מודעות הציבור להונאות מסוג זה.

רקע

מתווה חדש זה, אשר הפך שכיח בשנה האחרונה, מזכיר מתווה הונאה מוכר אשר פורסם בעבר על-ידי ה-CERT הלאומי. המתווה הקודם כלל התחזות טלפונית לחברה גדולה (מיקרוסופט בדרך כלל), במטרה להשיג פרטים אישיים או אחיזה במחשב.

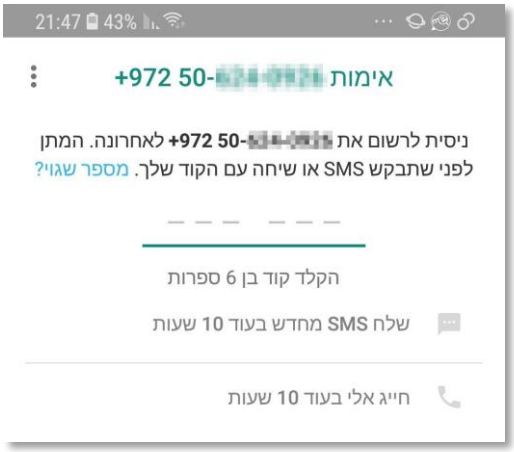
המתווה הנוכחי כולל התחזות ליישומון WhatsApp בשתי דרכים שונות, כאשר המטרה של שתיהן היא השגת קוד האימות של המשתמש, ובסופו של דבר השתלטות על חשבונות רבים ככל האפשר. נכון לכתיבת שורות אלה, לא ידוע על פעולות נוספות המבוצעות בחשבון ה-WhatsApp או במכשיר הטלפון, מלבד ניסיון גישה לחשבונות WhatsApp נוספים, ולכן טרם ידועה מטרתם הסופית של התוקפים.

פרטי אירוע

כאמור, במתווה ההונאה הנוכחי זוהו עד כה שתי דרכים שונות להשתלטות על חשבונות WhatsApp:

- <u>השתלטות באמצעות התא הקולי</u>

במתווה זה, התוקף מוריד את היישומון ומזין מספר טלפון ישראלי. על מנת להפעיל חשבון קיים הוא מתבקש לבחור בזיהוי באמצעות שיחה טלפונית או באמצעות מסרון. הוא בוחר באימות באמצעות שיחה, בדרך-כלל בשעות הלילה, בתקווה שבעל החשבון לא יענה לשיחה. במידה והשיחה לא נענית, קוד האימות נשמר בתא הקולי. בשלב זה התוקף מתקשר לתא הקולי של בעל החשבון ומנסה להזין סיסמת ברירת מחדל (1234 או 0000), ובמידה וזו הסיסמה התוקף מצליח להשיג גישה לחשבון ה-WhatsApp.



- <u>השתלטות באמצעות מסרון המתחזה ל-WhatsApp</u>

בתחילת התקיפה התוקף שולח למשתמשי WhatsApp אותם רוצה לתקוף מסרונים בהם נכתב כי משתמש אחר טוען לבעלות על החשבון. במסרונים מתבקש בעל החשבון להזין קוד אימות אשר לקישור המצורף למסרון על-מנת להוכיח שהחשבון שייך לו. כאשר המשתמש עושה זאת הוא

למעשה שולח לתוקף את קוד האימות המאפשר הפעלת האפליקציה על המכשיר ומקנה לו גישה לחשבון.







לאחר שהתוקף השיג גישה לחשבון ה- WhatsApp של המשתמש באחת משתי הדרכים, הוא שולח לכל רשימת אנשי הקשר בחשבון הפרוץ בקשה, כביכול מבעל החשבון, לשלוח לו את קוד האימות של חשבון ה- WhatsApp שלהם. בחלק מהפניות, אזרחים דיווחו כי התוקף הצליח להשתלט להם על החשבון ולחסום להם את הגישה אליו.



ניתן לשתף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים

דרכי התמודדות

1. מומלץ לשנות את סיסמת ברירת המחדל למענה הקולי, או לבטלו במידה ואין בו צורך. ניתן לבדוק האם קיים מענה קולי באמצעות לחיצה ארוכה על הספרה "1" במכשיר הטלפון.
2. מומלץ להגדיר אימות דו-שלבי ביישומון WhatsApp, כמו גם בשירותים חשובים נוספים. אימות דו שלבי הוא אמצעי אבטחה שעובד באמצעות הזנת קוד זמני שיתקבל ב-SMS לטלפון הנייד בעת כניסה לחשבונכם ממכשיר חדש, בנוסף להזנת הסיסמה הרגילה. בחשבון ה-WhatsApp ניתן להגדיר אימות דו שלבי באמצעות כניסה לתפריט הגדרות-> חשבון-> אימות דו-שלבי-> הפעל.
3. קוד האימות של WhatsApp הוא אישי ואין לשתפו, אפילו לא עם חברים או בני משפחה, ייתכן שגם להם פרצו ומשתמשים בחשבונם.

שיתוף מידע עם הCERT הלאומי איננו מחליף חובת דיווח לגוף מנחה בלשהו, במידה שהתגלה צורך כזה