מבט על, גיליון 561, 15 ביוני 2014

מבצע ריגול איראני בסייבר – חשיפה נוספת ומטרידה

גבי סיבוני וסמי קרוננפלד

כל העוקב אחרי התפתחות יכולות הפעולה של איראן במרחב הסייבר, לא מופתע לראות כיצד זו הופכת לאט למעצמה בתחום זה. במהלך הימים האחרונים נחשפה בארצות הברית מערכת ריגול סייבר איראני ארוכת-טווח שבמהלכה נעשה שימוש בטכניקות של "הנדסה חברתית" ו"דיוג" (social engineering & phishing) כדי לשאוב מידע מגורמי מפתח בארצות הברית, ישראל, בריטניה ומדינות אחרות. אף אם הפרטים שנחשפו אינם מצביעים על שימוש איראני בכלים טכנולוגיים מתקדמים, הרי שהם חושפים את היכולת המבצעית המתפתחת של איראן להוציא לפועל מבצעים מורכבים במרחב הסייבר תוך איסוף מודיעיני והפעלת תשתית מבצעית מורכבת ורחבת היקף.

המתקפה שזכתה לכינוי newscaster החלה ככל הנראה כבר ב-2011. בהנחה שמועד זה מדויק הרי שהמתקפה החלה סמוך לחשיפת מתקפת סטקסנט, שפעלה לפגוע בסרקזות באיראן. התוקפים אספו מודיעין ובנו פרופילים אנושיים באמצעות שימוש ברשתות חברתיות. זאת כדי ליצור מארג מורכב ומתואם של זהויות וירטואליות בעלות קשרים פיקטיביים לגורמי תקשורת, אנשי צבא וממשל אמריקניים, דיפלומטים וחברי קונגרס, קבלני בטחון ועוד. הפרופילים החברתיים של זהויות פיקטיביות אלו, נוצרו על גבי רשתות חברתיות דוגמת: Facebook, Linkedin, Twitter ו+Google ונבנו באופן מעמיק ומפורט תוך מתן תשומת לב ליצירת כיסוי "היסטורי" אמין ומשכנע לדמויות. התוקפים אף הקימו מערך וירטואלי התומך את סיפורי הרקע של הזהויות וכולל אתר חדשות פיקטיבי תחת השם newsonair.org, אשר בו עובדים לכאורה שש מהזהויות. השימוש בזהויות פיקטיביות אינו חדש בעולם הריגול והסייבר. אולם, היכולת לייצר מערך זהויות בדויות, הנתמך על ידי מערך תחזוקה וניהול זהויות הפועל לתחזק את הזהות בצורה שתשכנע את הקורבנות לאורך זמן שהזהות הנה זהות חיה ואמתית, מראה על שאיראן שידרגה את יכולות הפעולה המבצעית שלה במרחב הסייבר.

לאחר שנוצרו, החלו האיראנים לנהל את הזהויות וליצור קשר עם אישים, אשר נתפסו בעיני התוקפים כמקורבים לממשל וכמקורות פוטנציאלים למידע בעל ערך. בין המטרות היו בכירי ממשל בהווה ובעבר, עיתונאים, עובדי מכוני מחקר ואנשי תעשיות ביטחוניות. יצירת הקשר ובניית האמון עם המטרות נעשתה באופן סבלני ומתוחכם תוך שימוש במעגלים החברתיים של הקורבנות וניצול יעיל של הפלטפורמות השונות שמציעות הרשתות החברתיות. המטרה הייתה לייצר אמון שיספיק כדי לאפשר משלוח דואר אלקטרוני הכולל קוד זדוני. ואכן, כאשר הצליחו התוקפים לבסס מידה מספקת של אמון בין הקורבן לבין הזהויות הווירטואליות הם הוציאו אל הפועל את המתקפה ושלחו הודעות דואר אלקטרוני הכוללות קוד שהתקין עצמו על מחשב הקורבן או על קישורים לדפי מידע הדורשים הזנת פרטים אישיים ומעבירים אותם לתוקפים.

על-פי המידע שנחשף, התוקפים הצליחו לייצר רשת הכוללת יותר מ-2000 בני אדם, בהם מאות "יעדי איכות". במידע שנחשף לא צוין סוג המידע שנגנב ואלו אישים ומוסדות נפלו ברשת, אך מהזהות הכללית של היעדים ניתן ללמוד כי התוקפים חיפשו אחר מידע רגיש הנוגע לטכנולוגיות ביטחוניות ולפעילות הצבאית והדיפלומטית של ארצות הברית, בריטניה, ישראל וערב הסעודית. החיפוש אחר מידע מסוג זה, מעיד על אופייה הפוליטי-מדיני של המתקפה וכי ככל הנראה אין מדובר בפשיעת סייבר או בריגול תעשייתי שגרתי.

שיוך המתקפה הזו לאיראן נשען על כמה ראיות: אתר החדשות המזויף newsonair.com נרשם בטהראן, שרתי השליטה באמצעותם הפעילו התוקפים את הקוד הזדוני מתארחים על שרתים בתוך איראן, בשורות הקוד של התוכנות התגלו מילים איראניות והזמנים בהם פעלו התוקפים תואמים את שעות העבודה במדינה. עם זאת, לא ברור האם המתקפה בוצעה באופן

ישיר על גורמי ממשל איראניים, על ידי קבוצה הקשורה לשלטון או על ידי האקרים פרטיים התומכים בממשל או המופעלים על ידי הממשל.

תקיפה זו מהווה חוליה נוספת בקמפיין לוחמת הסייבר שמנהלת איראן כנגד יריבותיה במערב ובמזרח התיכון. היא מצטרפת למתקפות איכותיות נוספות אשר יוחסו לגורמים איראניים במהלך השנים האחרונות ביניהן מתקפת DDoS רחבת היקף על אתרי האינטרנט של בנקים ומוסדות פיננסיים מרכזיים בארצות הברית וגל תקיפות כנגד מערכי בקרה של חברות תשתית ואנרגיה אמריקאיות. עם זאת, במתקפה הנוכחית יש בכדי ללמדנו על רוחב היריעה והגיוון הרב שבפעילות הסייבר האיראנית. בעוד שמתקפות קודמות התמקדו בגרימת נזק והתאפיינו בפרופיל גבוה הרי שהמתקפה הנוכחית כוונה להשגת נגישות ביעדי איכות והתנהלה בחשאיות ולאורך זמן.

השימוש במרחב סייבר למטרות איסוף מידע ומעקב אינו זר לאיראן, אשר עושה שימוש רב בטכניקות של "דיוג" ו"הנדסה חברתית" לשם ניטור פעולותיהם ודעותיהם של אזרחים איראניים ואיתור מתנגדי שלטון ופעילי אופוזיציה. ביוני 2013, מועד הבחירות לנשיאות, פרסמה חברת גוגל כי אנשיה איתרו ובלמו מתקפת "דיוג" ששוגרה על ידי גורמים בתוך איראן וכוונה כנגד עשרות אלפי חשבונות דואר-אלקטרוני של אזרחים איראניים. המתקפה כללה שליחה של מייל המוסווה כמייל אחזקתי של מערכת Gmail ומבקש את הגולש להזין את שם המשתמש וסיסמת הדואר האלקטרוני שלו. המידע המוזן הועבר ישירות לתוקפים ואפשר להם גישה חופשית לתיבות הדואר האלקטרוני של המשתמש. עם זאת, חשיפת המתקפה הנוכחית הינה החשיפה המשמעותית הראשונה של פעילות ריגול איראנית במרחב הסייבר הבינלאומי, תחום אשר בו פועלות כיום בעיקר רוסיה וסין.

החשיפה הנוכחית מצטרפת לרשימה ארוכה של פעולות במרחב הסייבר, המיוחסות לאיראן ואשר מטרתן לפגוע בארצות הברית, בישראל ובמדינות מערביות נוספות. אף שהחשיפה הזו אינה מצביעה על קפיצת מדרגה טכנולוגית ייחודית ביכולת לוחמת הסייבר האיראניות, היא מעידה על רמת ארגון מבצעי ומודיעיני גבוהה ועל קיומם של יעדים אסטרטגיים ארוכי טווח לאיראן בשנים האחרונות.