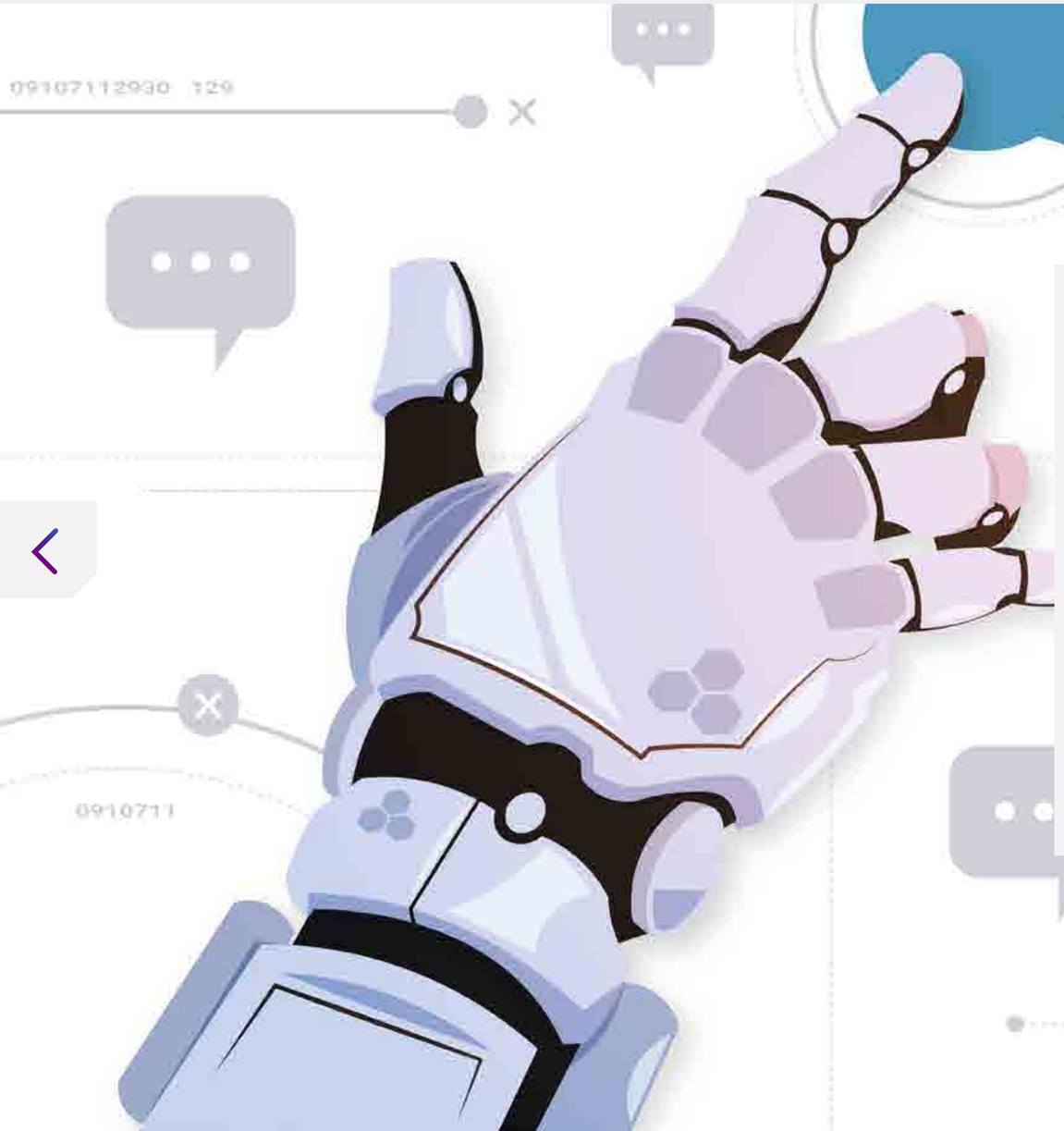
הראל
ביטוח ופיננסים

מאי 2021 //

מגזין הסייבר



תוכן עניינים

מאמר מערכת

חולשה בשרתי דוא"ל של מיקרוסופט אפשרה למודיעין הסיני לרגל אחרי ארגונים מסביב לעולם

בחודשים האחרונים הממשל הפדרלי בארה"ב מתמודד עם מתקפות חוזרות ונשנות מצד הביון הרוסי והסיני. לאחר מתקפת שרשרת אספקה שניצלה את המוצר של חברת Solarwind (מוצר IT נפוץ בארה"ב ובעולם), גילו במיקרוסופט חולשות בשרתי הדוא"ל הנפוצים של החברה - Microsoft Exchange Server. הפעם, אלו הסינים שניצלו את החולשות. בייג'ינג מצידה מכחישה את ההאשמות.

היות וחלק מהקורבנות היו משרדי ממשל אמריקאים, עולה השאלה מדוע מיקרוסופט התעכבה בשחרור הטלאי לחולשות. בעוד חוקרי אבטחה טוענים שהם שיתפו את החברה בממצאים כבר בסוף דצמבר 2020, טלאי פורסם לציבור רק בתחילת מרץ 2021. כחודשיים לאחר מכן. זהו פרק זמן ארוך מאד, אותו ניצל הביון הסיני לטובת ריגול אחרי מטרות אמריקאיות.

האירוע של Microsoft Exchange חשף מעל מאה אלף שרתים ברחבי העולם למתקפות. חלקם חשופים עד כתיבת שורות אלו. מסתבר שלא פשוט לארגונים לעדכן טלאי אבטחה, בעיקר ארגונים עם רשתות של אלפי מחשבים. מערך הסייבר של ממשלת ארה"ב מיהר להזהיר בעלי עסקים בעולם, וכך עשו גם גופי סייבר דומים בעשרות מדינות.

על פי האזהרה של ממשלת ארה"ב, לפחות אחת החולשות יכולה לאפשר לתוקף לגנוב את כל התוכן של תיבות הדואר האלקטרוני בארגון. תנו לזה לשקוע. דמיינו תוקף שנכנס לשרת הדוא"ל של הארגון בו אתם עובדים ומוריד את כל תוכנו. כן, כל הודעות הדוא"ל של כלל העובדים, לכל התקופה ששמורה בשרת. עכשיו תחשבו שזה שירות ביון זר. ועכשיו תכפילו את זה בעשרות אלפי ארגונים באותה מדינה.

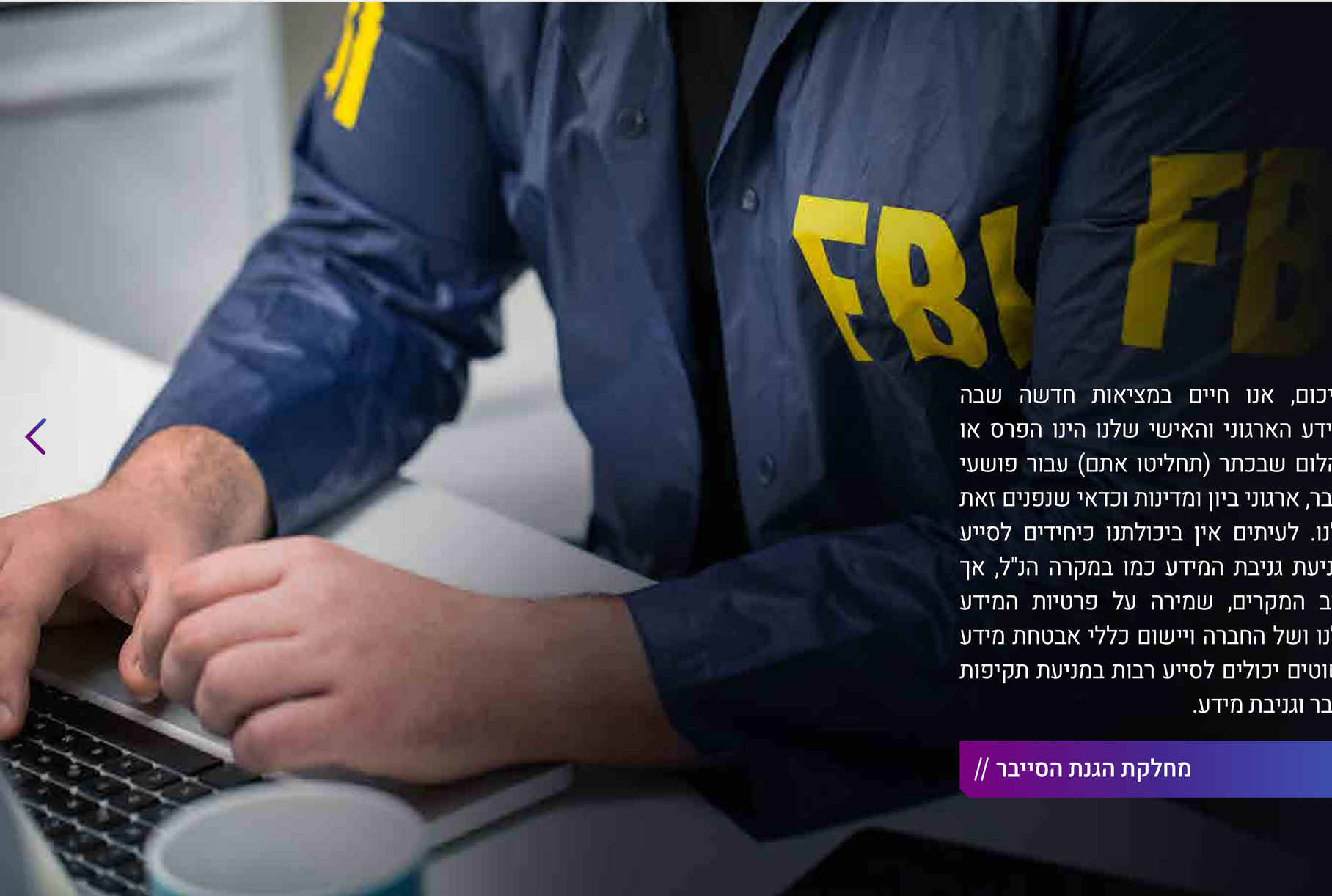
האירוע כה מכונן, עד אשר בית משפט בטקסס, ארה"ב, אפשר לשירות החקירות הפדרלי (ה- FBI), להיכנס לארגון פרטי ולעדכן עבורו את שרת הדוא"ל. בעולם הסייבר האמריקאי מדובר ב "רעידת אדמה". עד היום, ההנחה הייתה שכל ארגון דואג לעצמו והמדינה לכל היותר ממליצה לעסקים איך להגן על עצמם. במקרה זה מדובר במעבר מעמדה פאסיבית של הממשלה - לאקטיבית.

monticello / Shutterstock.com

"הסרת הקוד הזדוני שהוסמכה היום על ידי בית המשפט מדגימה את מחויבות מחלקת המשפטים לשבש את פעילות הפריצה באמצעות כל הכלים המשפטיים שלנו, ולא רק העמדה לדין", אמר העוזר היועץ המשפטי לממשלה ג'ון סי. דמרס באגף לביטחון לאומי במשרד המשפטים האמריקאי.

"בשילוב עם מאמצי המגזר הפרטי וגופים ממשלתיים אחרים עד כה, כולל שחרור כלי איתור ותיקונים, אנו מראים יחד את העוצמה ששותפות ציבורית-פרטית מביאה לאבטחת הסייבר של מדינתנו."

למרות אישור בית המשפט, מומחים טוענים שבפועל, המעורבות של ה FBI, היא אצבע בסכר. זאת, מכיוון שמאז דצמבר האחרון ועד אפריל, הביון הסיני כבר הצליח לגנוב מידע מכל הארגונים שמצא בהם עניין וניתן היה לנצל את החולשה לשרת הדוא"ל. במציאות כזו, גם אם הממשלה תעשה את העבודה של העסקים ותתקין טלאים, המידע כבר בחוץ.



לסיכום, אנו חיים במציאות חדשה שבה המידע הארגוני והאישי שלנו הינו הפרס או היהלום שבכתר (תחליטו אתם) עבור פושעי סייבר, ארגוני ביון ומדינות וכדאי שנפנים זאת כולנו. לעיתים אין ביכולתנו כיחידים לסייע למניעת גניבת המידע כמו במקרה הנ"ל, אך ברוב המקרים, שמירה על פרטיות המידע שלנו ושל החברה ויישום כללי אבטחת מידע פשוטים יכולים לסייע רבות במניעת תקיפות סייבר וגניבת מידע.

מחלקת הגנת הסייבר //

טיפ מודעות

האקרים מנצלים מידע סינטטי למתקפות סייבר

על פי חוזר עדכני של שירותי החקירות הפדרלי בארה"ב (ה- FBI), פושעים בסייבר משתמשים במידע סינטטי לטובת מתקפות סייבר. מהו מידע סינטטי? קשת רחבה של תוכן דיגיטלי שנוצר או מנוהל, הכולל תמונות, וידאו, שמע וטקסט. בעוד שניתן להשתמש בטכניקות מסורתיות כמו פוטושופ ליצירת תוכן סינתטי, ניתן להשתמש גם באלגוריתמים מתחום הבינה המלאכותית לצורך כך.

מטרת השימוש בתוכן סינטטי הינה לבסס אמון בין התוקף לקורבן במטרה לנצל את אמון זה. בחלק מהמקרים, התוקפים משתמשים בתוכן סינטטי לייצר פרופילים של מובילי דעה ברשתות החברתיות על מנת להשפיע על השיח באותן רשתות. בין שמדובר בפייסבוק, טוויטר, ווטסאפ, אינסטגרם או כל רשת אחרת.

כאמור, אחת הדרכים לממש תוכן סינטטי היא לזייף פרופילים ברשתות החברתיות. באמצעות יכולות כאלו, תוקף יכול לייצר כל פרופיל שהוא רוצה - גבר, אישה, נער, נערה ולשטות בקורבנות פוטנציאליים. תוקף יכול גם

מקור | FBI

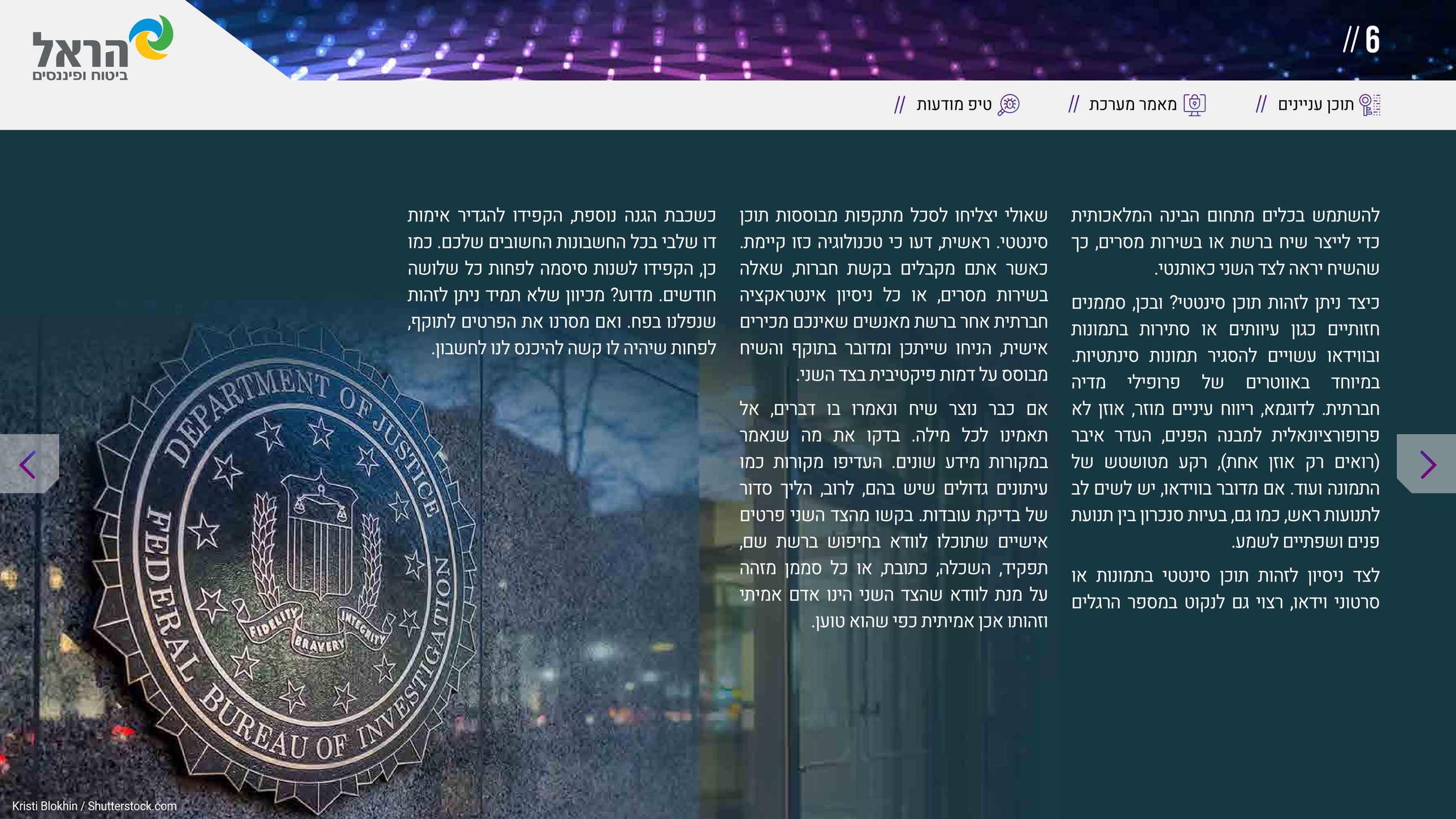
להשתמש בכלים מתחום הבינה המלאכותית כדי לייצר שיח ברשת או בשירות מסרים, כך שהשיח יראה לצד השני כאותנטי.

כיצד ניתן לזהות תוכן סינטטי? ובכן, סממנים חזותיים כגון עיוותים או סתירות בתמונות ובווידאו עשויים להסגיר תמונות סינתטיות. במיוחד באווטרים של פרופילי מדיה חברתית. לדוגמא, ריווח עיניים מוזר, אוזן לא פרופורציונאלית למבנה הפנים, העדר איבר (רואים רק אוזן אחת), רקע מטושטש של התמונה ועוד. אם מדובר בווידאו, יש לשים לב לתנועות ראש, כמו גם, בעיות סנכרון בין תנועת פנים ושפתיים לשמע.

לצד ניסיון לזהות תוכן סינטטי בתמונות או סרטוני וידאו, רצוי גם לנקוט במספר הרגלים שאולי יצליחו לסכל מתקפות מבוססות תוכן סינטטי. ראשית, דעו כי טכנולוגיה כזו קיימת. כאשר אתם מקבלים בקשת חברות, שאלה בשירות מסרים, או כל ניסיון אינטראקציה חברתית אחר ברשת מאנשים שאינכם מכירים אישית, הניחו שייתכן ומדובר בתוקף והשיח מבוסס על דמות פיקטיבית בצד השני.

אם כבר נוצר שיח ונאמרו בו דברים, אל תאמינו לכל מילה. בדקו את מה שנאמר במקורות מידע שונים. העדיפו מקורות כמו עיתונים גדולים שיש בהם, לרוב, הליך סדור של בדיקת עובדות. בקשו מהצד השני פרטים אישיים שתוכלו לוודא בחיפוש ברשת שם, תפקיד, השכלה, כתובת, או כל סממן מזהה על מנת לוודא שהצד השני הינו אדם אמיתי וזהותו אכן אמיתית כפי שהוא טוען.

כשכבת הגנה נוספת, הקפידו להגדיר אימות דו שלבי בכל החשבונות החשובים שלכם. כמו כן, הקפידו לשנות סיסמה לפחות כל שלושה חודשים. מדוע? מכיוון שלא תמיד ניתן לזהות שנפלנו בפח. ואם מסרנו את הפרטים לתוקף, לפחות שיהיה לו קשה להיכנס לנו לחשבון.



Kristi Blokhin / Shutterstock.com

האקרים הקימו חברת אבטחת מידע מזויפת בכוונה להונות חוקרי אבטחה

ככל הנראה, המטרה הייתה לגנוב חולשות וקטעי קוד שישמשו את התוקפים בעתיד

גוגל חושפת כי קבוצת האקרים הנתמכת על ידי ממשלת צפון קוריאה הקימה חברת אבטחת סייבר מזויפת בשם SecuriElite הממוקמת בטורקיה כדי לפתות מומחי אבטחה באמצעות חשבונות מדיה חברתית מזויפים (טוויטר ולינקדאין). חוקרי גוגל גילו כי התוקפים רימו את מומחי האבטחה באמצעות חשבונות ואתרים מזויפים. בסך הכול זוהו על ידי גוגל כשמונה חשבונות טוויטר וכשבעה פרופילי לינקדאין.

לאחר יצירת תקשורת ראשונית, התוקפים שאלו את החוקרים אם הם רוצים לשתף פעולה במחקר חולשות. אם כן, התוקפים סיפקו לחוקרים פרויקט בשפת תכנות Visual Studio הכולל קוד זדוני. המטרה, ככל הנראה, הייתה לגנוב מהחוקרים **חולשות יום-אפס** או קטעי קוד אחרים במטרה לעשות בהם שימוש בקמפייני תקיפה של צפון קוריאה.

לטענת גוגל, כל החשבונות בלינקדאין וטוויטר המשויכים לקמפיין ההונאה הושבתו מיד לאחר שדיווחו עליהם. פרופילים מסוימים היו של אנשים שהתחזו כמנכ"לים של החברה הטורקית המזויפת. כאמור, כל החשבונות הושעו וגוגל הוסיפה את הקישור של האתר המזויף לרשימת החסימה שלה כדי למנוע ממשתמשים לבקר בו בטעות.

מה ניתן ללמוד מהמקרה?

לא כל מה שנוצץ זהב. אם פניה מסוימת טובה מידי להיות אמיתית, כדי לבחון האם מדובר בהונאה. לא משנה אם זה מנכ"ל, יו"ר, או סלבריטי - אם מישהו פונה אליכם עם הצעה או בקשה חריגה (גם חריגה לטובה), תחשדו. חפשו פרטים אודות אותו אדם או חברה. באם הנושא קשור לעבודתכם, התייעצו עם אבטחת המידע. בנושאים אישיים, התייעצו עם חברים או משפחה טרם שיתוף פרטים או מסמכים.

דו"ח: האקרים איראנים פרצו למכוני מחקר רפואיים בישראל וארה"ב

הפריצה נעשתה באמצעות דוא"ל זדוני והודעות המתחזות לדף של חברת מיקרוסופט

מוסדות רפואיים וחוקרים בכירים בישראל וארה"ב הותקפו בחודשים האחרונים על ידי קבוצת האקרים הנתמכת ומזוהה עם המשטר באיראן. בדו"ח שחיברה חברת הסייבר Proofpoint, נמצא כי קבוצת ההאקרים ניסתה לפרוץ לחשבונותיהם של לפחות 25 מומחים בעלי שם עולמי בתחומי גנטיקה, נוירולוגיה, אפידמולוגיה ואונקולוגיה. התקיפה החלה בחודש דצמבר 2020.

הדו"ח מספר כי הפריצה נעשתה באמצעות דוא"ל זדוני והודעות המתחזות לדף של חברת מיקרוסופט. לא נאמר מה הייתה מידת ההצלחה של ניסיונות הפריצה, אך החברה מעריכה כי מדובר במבצע מקיף לאיסוף מודיעין.

הניסיון לפרוץ למוסדות רפואיים ולחשבונותיהם של חוקרים בכירים הוא חדש עבור הקבוצה המתמקדת באיסוף מידע אחר אקדמאים, עיתונאים ודיפלומטים, בהם מתנגדי המשטר האיראני בחו"ל.

מה ניתן ללמוד מהמקרה?

כל אחד מאיתנו יכול להפוך למטרה רק מהיותו עובד ארגון המושך עניין של מדינות זרות. הקפידו לבחון כל הודעת דוא"ל או SMS בצורה קפדנית. המנעו מלחיצה על קישורים או הורדת צרופות משולחים שאינכם בטוחים בזהותם.

תוכנות זדוניות משתמשות במוקדים טלפוניים זדוניים כדי להדביק קורבנות

האקרים עושים שימוש במוקדים טלפוניים להפצת מסמכי אקסל המתקינים תוכנות זדוניות

בחודשיים האחרונים מומחי אבטחה מנהלים מאבק מקוון נגד תוכנה זדונית חדשה בשם BazarCall המשתמשת במוקדים טלפוניים כדי להפיץ תוכנות זדוניות. קמפיין התקיפה מתחיל בדוא"ל **דיוג** (Pishing), אך משם הוא חורג לשיטת הפצה חדשנית - שימוש במוקדי שיחות טלפון להפצת מסמכי אקסל זדוניים. כאלו המתקינים תוכנות זדוניות.

במקום לצרף קבצים לדוא"ל, ההודעות של BazarCall מעודדות את המשתמשים להתקשר למספר טלפון מסוים כדי לבטל מנוי לפני שהם מחויבים אוטומטית. לאחר מכן, המוקדן מפנה את המשתמש לאתר מיוחד להורדת "טופס ביטול". מדובר בהורדה של קובץ אקסל, כאשר נציג השירות נשאר על הקו להנחות את הקורבן כיצד לפתוח את הקובץ ולאפשר פקודות **מאקרו**. הפעלת המאקרו מתקינה תוכנה זדונית במחשב הקורבן.

לדברי מספר מומחי וחוקרי אבטחה, קבוצת האקרים מנהלת את המוקדים הטלפוניים. לדעתם, שירות ההפצה מנוהל כמו חברה רגילה, תוך הקפדה על שעות העבודה בימי שני עד שישי. למרות המאמצים המשולבים של קהילת אבטחת הסייבר, שיטת הפצה זו מצליחה מאוד.

מה ניתן ללמוד מהמקרה?

קיבלתם דוא"ל מאיים עם הוראות לביצוע בדחיפות? עצרו ונשמו עמוק. בררו אם התוכן נוגע אליכם. אם קיבלתם שיחת טלפון, פעלו בצורה דומה. אם אתם מקבלים הוראות טלפוניות מוזרות, תחשדו לפני שאתם לוחצים על קישור או מורידים קובץ. נסו לברר מי עומד מהצד השני של הקו טרם ביצוע פעולה שיכולה להזיק לכם.

ענקית הביטוח CNA נפגעה על ידי תוכנת כופר חדשה

להתקפה זו עלולה להיות השפעה על חברות שרכשו פוליסת ביטוח סייבר ב CNA

ענקית הביטוח CNA נפגעה מתוכנת כופר בסוף חודש מרץ האחרון שהשפיעה על שירותי האון-ליין שלה ועל הפעילויות העסקיות שלה. חברת CNA אישרה כי אכן נפגעה ממתקפת סייבר מתוחכמת שפגעה גם בדוא"ל של בכירי החברה.

מסתבר כי תוכנת הכופר הותקנה ברשת חברת CNA ב- 21 במרץ והצפינה מעל 15,000 התקנים ברשת שלהם וכן את מחשבי העובדים. גם כאלו שעובדים מרחוק. טרם ברור האם CNA תצליח לשחזר את הקבצים מתוך גיבויים.

להתקפה על CNA עלולה להיות השפעה עצומה על חברות אחרות, במיוחד על אלו שיש להן פוליסות ביטוח כנגד מתקפות סייבר באמצעות חברת CNA. מתקפה זו יכולה ליצור רשימה של חברות מבוטחות ומגבלות הפוליסה שלהן. מפעילי תוכנות כופר, כמו קבוצת REvil, יוכלו אזי לדרוש דרישות כופר המותאמות לכיסוי הביטוחי של הקורבן המסוים.

מה ניתן ללמוד מהמקרה?

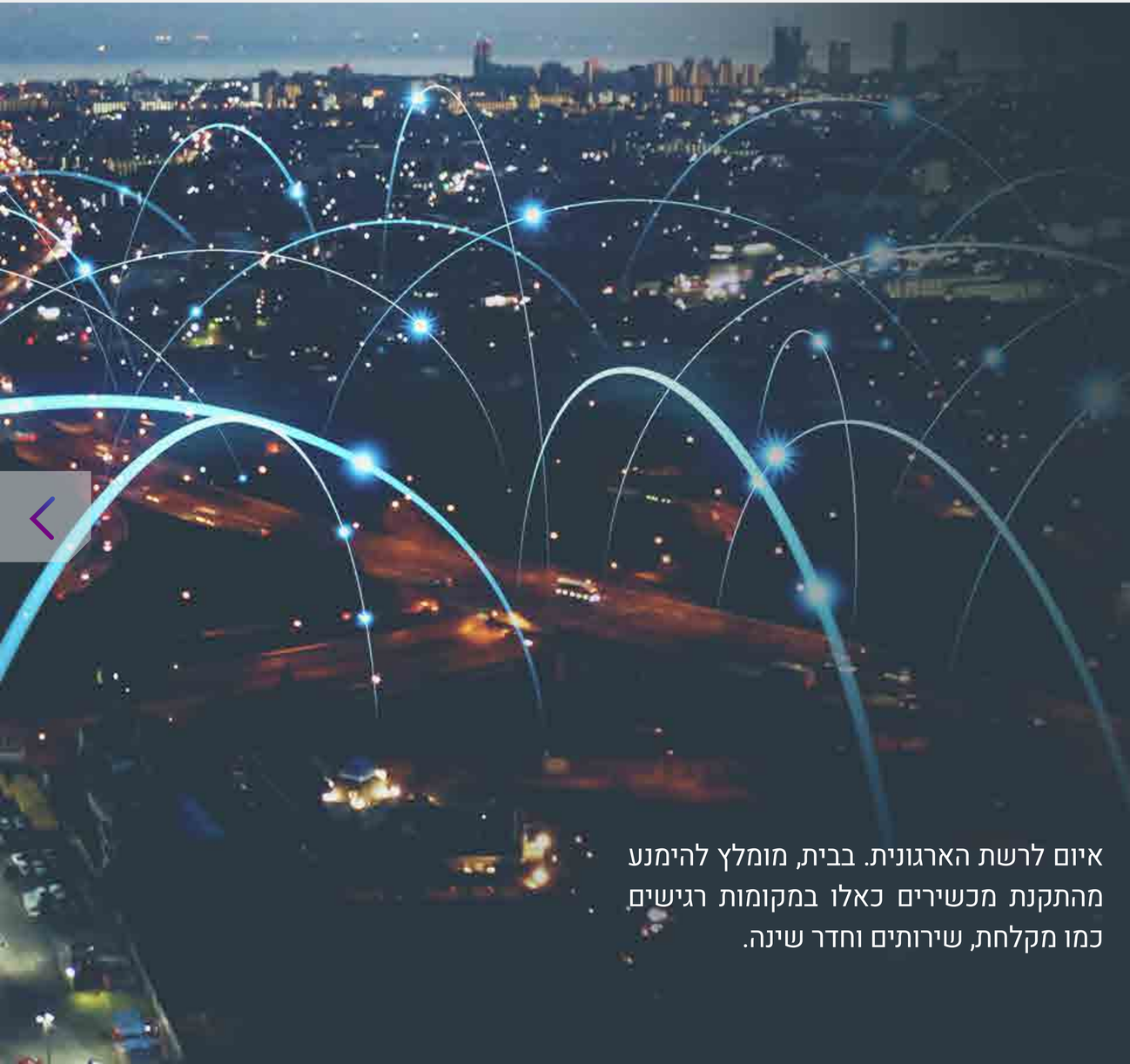
ההאקרים מחפשים ארגונים גדולים, כאלו עם כסף לשלם כופר או כאלו המחזיקים במאגרי מידע גדולים אותם אפשר למכור. במציאות כזו, כל אחד מאיתנו הופך להיות מטרה. היו ערניים לקישורים וצרופות שאתם מקבלים בדוא"ל, ברשתות חברתיות או בשירותי מסרים מיידים.

rarrarorro / Shutterstock.com

100 מיליון מכשירי IoT חשופים למתקפות

נקודות תורפה שאותרו על ידי חברות Forescout ו-JSOF כבר חשפו למתקפה מאות מיליוני התקנים ברחבי העולם

מערך חדש של תשע נקודות תורפה בקוד התקשורת בין התקני IoT ובין רשת האינטרנט חושף למתקפות כ- 100 מיליון מכשירים ברחבי העולם. "זו בעיה נרחבת. זו לא רק בעיה עבור מכשיר מסוג מסוים", מסבירים החוקרים שמצאו את הכשל. "וזה לא רק מכשירי IoT זולים. יש יותר ויותר עדויות עד כמה הכשל נפוץ. זו הסיבה שאנחנו ממשיכים לעבוד כדי להעלות את המודעות."



הכשל שהתגלה נובע מפרוטוקולי התקשורת המשמשים את המכשירים לתקשר עם השרת ששולט עליהם באמצעות רשת האינטרנט. האקרים יכולים להשתלט על ערוץ תקשורת זה על מנת לפרוץ לרשת הארגונית או הביתית. כמו גם, התוקף יכול לנצל את הכשל לטובת הרס ההתקן המחובר או כדי להשתלט עליו.

כאשר מדובר בתשתיות קריטיות, מוסדות רפואה או ארגונים תומכי חיים, הסכנה מכיוון התקנים מחוברים גדולה אף יותר. למרות האיום שחשפו החוקרים, טרם נמצא פתרון. מדובר בשוק מכשירים רווי יצרנים, שלא כולם ממהרים להוציא עדכוני תוכנה. ארגונים יכולים להיעזר בכלים שונים לאיתור התקנים הכוללים את הכשל המדובר.

מה ניתן ללמוד מהמקרה?

במידה ומדובר ברשת ארגונית, אין לחבר התקנים שאינם מאושרים על ידי הארגון לרשת אלחוטית. כל התקן כזה יכול להוות איום לרשת הארגונית. בבית, מומלץ להימנע מהתקנת מכשירים כאלו במקומות רגישים כמו מקלחת, שירותים וחדר שינה.

קזינו נפרץ באמצעות מדחום באקווריום

באמצעות המדחום באקווריום הצליחו התוקפים לגנוב מסד נתונים

גם זה קרה. קזינו בצפון אמריקה נפרץ דרך מד-חום באקווריום הנמצא בקזינו. ההאקרים השתמשו במד-חום המקושר לאינטרנט כדי להשיג דריסת רגל ברשת הקזינו. הם הצליחו להגיע למסד נתונים הכולל מידע אודות מהמרים כבדים בקזינו, ובאמצעות הקישור של המדחום לרשת, הצליחו לגנוב את הנתונים לענן בשליטתם.

הסיבה להצלחת המתקפה נעוצה באינטרנט של הדברים (IoT). מעליות, מנועים, מכונות, משאיות, טלפונים, מערכות השקיה, וכן, אפילו מדחומים לאקווריומים. כל אלו מצוידים בחיישנים מחוברים לרשתות, מאגרי מידע ומערכות תקשורת. הצפי הוא שעד שנת 2025 יהיו עשרות מיליארדי מכשירים מחוברים ברחבי העולם.

המכשירים המחוברים הללו יוצרים הזדמנויות עבור האקרים מכיוון שרבים ממכשירים אלו אינם מצוידים בהגנות אבטחה. המשמעות היא שחובה להעריך סיכונים המגיעים ממכשור כבקרות חימום בניינים, רמקולים חכמים, גלאי עשן, מערכות אזעקה, תאורה עילית ואפילו מכונות הקפה. אה, ולא לשכוח את האקווריום.

מה ניתן ללמוד מהמקרה?

כל התקן מחובר לרשת יכול להוות נקודת כניסה להאקרים. הקפידו להתקין רק מכשירים חכמים שאתם באמת חייבים לטובת צמצום משטח התקיפה.

קרדיט סוויס: מידע אודות עובדים לשעבר דלף לרשת

הנתונים כללו את כתובות העובדים לשעבר, מספרי ביטוח לאומי ופרטי חשבון בנק

חברת-הבת למסחר בניירות ערך בארה"ב של קרדיט סוויס גרופ חשפה כי הנתונים האישיים של עובדים לשעבר הודלפו וכי היא הגישה תביעה בנושא. קרדיט סוויס תבעה לפחות אדם אחד (לא ברור האם היה עובד חברה או פלוני אחר) בגין שליחת מידע פרטי אודות עובדים לשעבר לכלי תקשורת ורשויות אכיפת חוק באמצעות הודעת דוא"ל.

הנתונים נשלחו מחשבון ג'ימייל מזויף על שמו של תומאס גוטשטיין, מנכ"ל קבוצת הבנקאות השוויצרית. הוא כלל בין השאר את כתובות העובדים לשעבר, מספרי ביטוח לאומי ופרטי חשבון בנק. מהתביעה לא ניתן היה להבין כמה עובדים לשעבר הושפעו מהנתונים שהודלפו. בתביעה, שהוגשה לבית משפט פדרלי בסן פרנסיסקו, הואשמו האלמונים גם באיום לחשוף נתונים חסויים אחרים.

מה ניתן ללמוד מהמקרה?

במקרה זה לא ידוע כיצד ההאקרים השיגו את המידע או מה הקשר שלהם לחברת קרדיט סוויס. עם זאת, ידוע כי מרבית תקיפות הסייבר נגד ארגונים מתחילות ב**בפישינג**. הקפידו לבחון כל הודעת דוא"ל שאתם מקבלים והמנעו מלחיצה על קישור או הורדת צרופה במידה והשולח אינו מוכר לכם. בנוסף, מכיוון שבמקרה זה הייתה לתוקפים ככל הנראה עזרה מבפנים, אנו שבים ומזכירים לכם שאם אתם רואים משהו לא תקין - עשו את הדבר הנכון - דווחו על כך.

Novikov Aleksey / Shutterstock.com

איראן ניסתה לפתות ישראלים לצאת לחו"ל לצורך פגיעה בהם או חטיפתם

שירות הביטחון הכללי והמוסד הודיעו כי גורמי מודיעין מאיראן פעלו לפתות ישראלים לצאת למדינות שונות בחו"ל לצורך פגיעה בהם או חטיפתם.

בפעילות משותפת של שירות הביטחון הכללי והמוסד, נחשפה שיטת פעולה של גורמי מודיעין איראנים, באמצעותה פעלו לפתות ישראלים לצאת למדינות שונות בחו"ל, לטובת פגיעה בהם או חטיפתם.

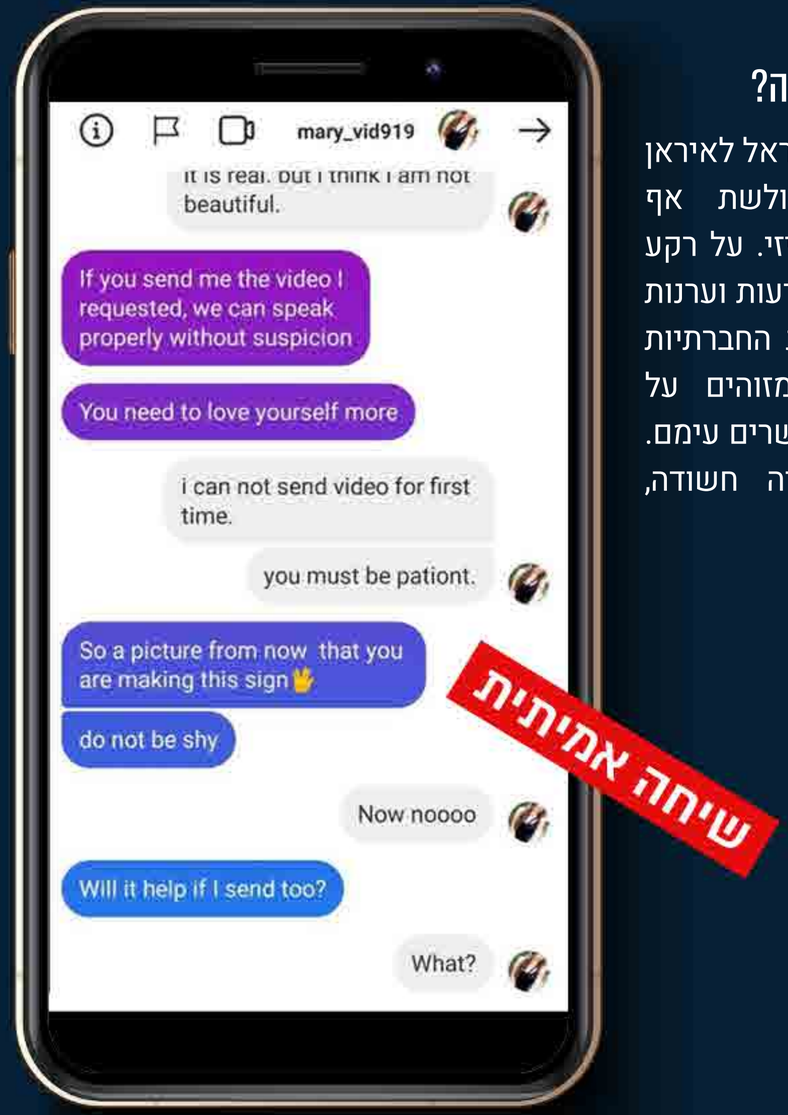
השיטה מבוססת על שימוש בפרופילים פיקטיביים ברשת חברתית ויצירת קשר עם ישראלים העומדים בקשרים עסקיים עם גורמים בעולם ונוהגים לצאת לחו"ל.

השיטה פעלה באופן הבא: הגורמים האיראנים פתחו פרופילים פיקטיביים של אנשים שעוסקים בתחום העסקים והתיירות, ברשת החברתית אינסטגרם. פרופילים אלו יצרו קשרים עם אזרחים ישראליים, תיאמו עמם מפגשים בחו"ל וניסו "למשוך" אותם למפגשים בתואנות עסקיות שונות. מפרסומים עולה כי המאמץ האיראני מתקיים כבר מעל לחצי שנה. מדובר בדפוס פעולה מוכר ודומה לזה אשר בוצע בעבר על ידי איראן מול מתנגדי משטר באירופה.

מהשב"כ נמסר כי "קיים חשש ממשי כי פעילות זו של גורמים איראניים תוביל לניסיונות פגיעה בישראלים או חטיפתם באותן מדינות בהן פועלים האיראנים". עד עתה לא ידוע על אזרח ישראלי שנפגע מפעילות זו.

מה ניתן ללמוד מהמקרה?

מלחמת הסייבר בין ישראל לאיראן הולכת ומחריפה וגולשת אף לפעילויות במרחב הפיזי. על רקע זה, על כולנו לגלות מודעות וערנות ביחס לפניות ברשתות החברתיות מפרופילים שאינם מזוהים על ידנו, ולמניעת יצירת קשרים עימם. באם נתקלתם בפנייה חשודה, דווחו עליה מייד.



מקור | YNET | צלום : שב"כ

הראל

ביטוח ופיננסים