



2012: מלחמת הסייבר בעיצומה

בשנה החולפת עבדו אנשי אבטחת המידע שעות נוספות: החל מדליפת כרטיסי האשראי, דרך פרשת וובגייט ועד גאוס Flame-1 - נראה שהסייבר היה אחד התחומים הבולטים של השנה ♦ בעולם שבו אפילו מחשבי המשטרה אינם בטוחים, קשה לצפות מה תביא עמה השנה הבאה

יוסי הטוני

על פי פרסומים זרים, ישראל היא שביצעה את הפעולה. אתר נוסף שנפרץ הוא זה של ועידת נשיא המדינה, **שמעון פרס**, אלא שהוא לא כולל פרטים אישיים. כמו כן, פרצו ההאקרים לאתר רשות השידור וגנבו מידע ממנו.

כמה ימים מאוחר יותר נפגעו עשרות אלפי מחשביה של סעודי ארמקו - חברת הנפט הסעודית, על ידי נזקה. עם זאת, על פי החברה, למרות שהוירוס השפיע על פעולת כמה מחשבים, הוא לא השפיע בצורה כלשהי על פעילות רשת תקשורת המחשבים בחברה וגם הייצור שלה לא נפגע. החברה הותקפה על ידי הנוזקה שאמון (Shamoon), שהייתה מסוג "מתקפת יום אפס" ותקפה ב-16 באוגוסט השנה - היום האחרון של חג הרמאדאן. הנוזקה הייתה נטולת חתימה, עירבה פשיג עם מתקפה ממוקדת והייתה בעלת יכולות להשמדת מידע והצפנה עצמית. הנוזקה פגעה במגוון הגרסאות של מערכת ההפעלה חלונות של מיקרוסופט וגרמה לשיתוקם של יותר מ-35 אלף מחשבי תאגיד הנפט הענק.

המתקפה על סעודי ארמקו התגלתה כשבוע לאחר שחוקרים של קספרסקי חשפו את קיומה של גאוס - תוכנת ריגול למגזר הבנקאי, שחדרה בעיקר למחשבים של בנקים בלבנון, אולם נתגלתה גם בישראל וברשות הפלסטינית. על פי ההערכות של חוקרי קומסק, שבדקו אותה, מדובר באחת מסדרה שלמה של נזקות שנועדו לריגול בין מדינות, בעיקר במזרח התיכון.

בגאוס, מפתח ההצפנה של המידע מוחזר מהשרת באמצעות XOR - הצפנה חלשה, שניתנת לפענוח בנקל - ומפתח במיקום OxACDC, ציינו החוקרים. לדבריהם, "מצחק לראות שהוא המפתח, משום שזה מזכיר את הדיווח שהיה באחרונה לגבי מחשבים במעבדות באיראן שהיו נגועים בוורוס ופתאום החלו להשמיע מוזיקה של להקת AC/DC". חוקרי קספרסקי בטוחים שיוצרי גאוס יצרו גם את Flame, שנתגלתה בחודש מאי ותקפה מחשבים במדינות שונות במזרח התיכון, ובעיקר באיראן. נטען עליה, כי מדובר ב"אחת התוכנות הזדוניות המתוחכמות והמורכבות ביותר שנתגלו עד כה, הרבה יותר מתוחכמת ממה שראינו עד כה". היא אף כונתה על ידי החוקרים "נשק-על קיברנטי", עקב "ההיבט הגיאוגרפי, הבחירה הדקדקנית של יעדי התקיפה והשימוש המתוחכם בנקודות תורפה".

פגיעה בתאגידי אנרגיה

בספטמבר, ימים אחדים אחרי שסעודי ארמקו דיווחה שבשל המתקפה נפגעו כ-35 אלף תחנות עבודה, דיווח תאגיד האנרגיה הקטארי RasGas, שגם מחשבים שלו נפגעו. RasGas מפעילה מתקני ייצור לטיפול, זיקוק וייצוא של גז טבעי נוזלי למדינות ברחבי אסיה, אירופה ואמריקה. מתאגיד הענק נמסר, כי הייצור של הגז שלו לא נפגע בשל המתקפה. עם זאת, המתקפה אילצה את מנהלי ה-IT שלו לסגור את אתר האינטרנט ומערכות הדואר אלקטרוני של החברה.

באוקטובר הורה הפיקוד הבכיר של משטרת ישראל על ניתוק כלל המחשבים המחוברים לרשת האזרחית שלה בשל התרעה על מתקפה שעלולה להפיל את רשת תקשורת המחשבים שלה או להשתלט עליה. כמו כן, החליטו ראשי המשטרה בעקבות אותו חשש לאסור על הכנסת

גם של מנוחה לא היה באבטחת מידע השנה: כבר ב-2 בינואר דלפו והועלו לרשת פרטי כרטיסי האשראי של אלפי ישראלים, על ידי חבורת האקרים סעודים שטענו שהם משתייכים לארגון אנונימוס. ההאקרים פרצו לאתר הספורט ONE ובמשך זמן מה, הגולשים שנכנסו אליו הופנו לקובץ שההאקרים הסעודים טענו שמצויים בו פרטיהם האישיים של 400 אלף ישראלים, בהם מספרי כרטיסי אשראי ופרטים מזהים נוספים. המפקח על הבנקים בבנק ישראל הודיע, כי "מדובר בפרטיהם של כ-15 אלף כרטיסים פעילים, בשלוש החברות יחד - כ.א.ל, ישראלכרט ולאומי קארד". הפריצות נעשו בטכניקת הזרקת SQL על ידי שלושה האקרים.

מי שכונה "ההאקר הסעודי", OxOmar - והדליף את פרטי כרטיסי האשראי, הבטיח כי קבוצת האקרים פרו-פלסטינים המכנה את עצמה "סיוט", תפיל אתרים ישראליים. ואכן, כשבועיים לאחר מכן, נפלו האתרים של אל-על ושל הבורסה לניירות ערך. עוד הותקפו האתרים של קבוצת הבנק הבינלאומי - אתר האינטרנט של הבנק הבינלאומי ואתרי האינטרנט של בנק מסד ובנק אוצר החייל, שבבעלותו.

זה לא נגמר שם: בהמשך ינואר הותקפו אתרי בתי החולים שיבא ואסותא ואתר הארץ. ימים אחדים לאחר מכן הגיע תורו של אתר ynet.

"ארה"ב אינה ערוכה"

ביולי השנה אמר הגנרל **קית אלכסנדר**, ראש הסוכנות לביטחון לאומי של ארצות הברית (NSA) ומפקד פיקוד הסייבר שלה, כי "בסולם של 1 עד 10, המוכנות של ארצות הברית להתמודד עם מתקפת סייבר גדולה על התשתיות הקריטיות שלה עומדת על הציון העגום 3". לדברי אלכסנדר, המדבר בפומבי לעתים רחוקות, מאז שנת 2009 גדלה כמות מתקפות הסייבר שחוו ארגונים של תשתיות קריטיות בארצות הברית פי 17. "אני מודאג ביותר לגבי מערכי ה-IT של תחנות כוח וחברות חשמל ולגבי חברות שמספקות מים", הוסיף אלכסנדר. "אני חושב שהארגונים הללו זקוקים לעזרה בהגנה ברמה הגבוהה ביותר". הוא ציטט מחקר של מק'אפי, שלפיו העלות של אובדן מידע בשל ריגול תעשייתי עומדת על טריליון דולרים. באותו החודש אמר **שון הנרי**, לשעבר עוזר בכיר לראש ה-FBI וראש החטיבה לאבטחת הרשת ולמלחמה באיומים קיברנטיים, כי "מלבד נשק להשמדה המונית, איומי הסייבר הם האיומים המשמעותיים ביותר שיש לפעול נגדם".

מלחמת הסייבר נמשכת

באוגוסט נמשכה מלחמת הסייבר בין ישראל לעולם הערבי: האקרים, שמקורם ככל הנראה מארצות ערב, פרצו לשרת אינטרנט ופרסמו את פרטיהם האישיים של כמה אלפי ישראלים, ובכלל זה את מספרי כרטיסי האשראי שלהם. הפרטים היו מאוחסנים בשרת של חברת אחסון השרתים וובגייט, שהתוקפים חדרו אליו. ההאקרים מסרו את דבר הפריצה בהודעה שפרסמו באתר "זוכרים את עימאד", כאשר כוונתם הייתה לעימאד מורנייה, קצין המבצעים של החיזבאללה, שחוסל בדמשק ב-2008, כאשר פוצצה מכוניתו ליד ביתה של המאהבת שלו.