daily maily
עמוד 8 , 07/04/2016 , 17.11 x 26.23
כתבים: יוסי הטוני
52702769

המדריך למותקף הישראלי

מאת יוסי הטוני On 6 באפריל 2016 @ 15:12 In אבטחת מידע,אינטרנט,בראש הכותרות,חדשות | No Comments

החגיגה תיכף מתחילה. אנונימוס. צילום: BigStock

מחר (ה'), ה-7 באפריל הוא מועד ה-"OPIsrael" היום בו **אנונימוס** (Anonymous) והאקרים אנטי-ישראלים ובתוכם פרו-פלסטינים, צפויים לתקוף, או לנסות לתקוף, אתרים ישראליים.

ד"ר **גבי סיבוני**, חוקר בכיר וראש תכנית הסייבר במכון למחקרי ביטחון לאומי (INSS), אומר כי "המודעות לכללי היגיינת רשת בסיסיים – הינה כלי ההגנה המרכזי בכל הקשור למתקפות הסייבר. אלו הולכות ומשתכללות משנה לשנה, ולכן מתקיימים יותר ויותר שיתופי פעולה בין ארגונים ממשלתיים וגופים עסקיים".

"כדאי מאוד קודם כל להגן על המכשור הביתי שלכם ולהתקין את עדכוני האבטחה העדכניים ביותר שקיבלתם ואשר טרם הותקנו", אמר. "יש לגבות מידע חשוב שברשותכם – כמו גם את המערכות הקריטיות".

בנוסף, אמר ד"ר סיבוני, "מומלץ לרענן ולהקשיח סיסמאות ופרטי כניסה קיימים למכשירים שלכם, לתוכנות, מיילים, אפליקציות, ובחשבונות ברשתות החברתיות".

לדבריו, "על מנת להגן מפני מתקפות סייבר, יש להימנע מלפתוח קישורים והזמנות חשודים במייל, בפרופיל האישי ברשתות החברתיות או בתוכנות ובאפליקציות בנייד. כדאי להימנע מהתקנת תוכנות ואפליקציות לא מוכרות ביום המתקפה".

"אסור לפתוח מיילים משולחים שאינם מזוהים או אינם מוכרים – אלה עלולים להכיל סוסים טרויאנים", אמר ד"ר סיבוני. "יש לחשוד גם במיילים מאנשים מוכרים, שהגיעו עם קבצים או קישורים מצורפים – חשודים ולא מזוהים".

"אנשי אנונימוס מתמקדים גם בגופים לאומיים, משרדי ממשלה וארגונים ממלכתיים", הוסיף. "על גורמי אבטחת הסייבר בארגונים הללו לשדרג שרתים, להקפיד לגבות את המידע החשוב, ולתדרך את עובדי הארגון בנוגע לכללי האבטחה המקוונת ביום המתקפה".

למנהלים שביניכם, סיכם ד"ר סיבוני, "חשוב לתדרך את העובדים על היתכנות המתקפה, לחזק את ההיכרות שלהם עם כללי אבטחת המידע המקוון ולרתום אותם למאמץ ההתגוננות, עם דיווח על אירועים חריגים ביום המתקפה".

IL-CERT פותח חמ"ל סייבר

IL-CERT, המרכז לתיאום אירועי אבטחת מידע, פותח מחר (ה') מרכז מבצעים מיוחד לרגל מתקפת הסייבר OPIsrael. המרכז הינו גוף מקצועי בלתי תלוי, שמורכב ממומחי אבטחה במגזר הפרטי. עשרות מומחים – האקרים, חוקרי מתקפות סייבר, מנהלי אבטחה, אנשי אקדמיה ומנכ"לי חברות – מתכנסים מדי שנה לקראת המבצע, כדי לנטר מתקפות רשת ולספק מענה לחברות ומשתמשים שנפגעו מהן.

לדעת מומחי IL-CERT, ניתן להתמודד בהצלחה עם האיום, לתקן נזקים ולהימנע מהם כליל. להערכתם, התוקפים לא יצליחו להפיל אתרים חיוניים, או להשפיע על שגרת החיים בארץ. את פעילות המרכז מלווים דרך **פייסבוק** (Facebook) אלפי מתנדבים מרחבי הארץ, שמספקים מידע והתראות על תקיפות.

תומכי דאעש יתקפו את ישראל

קבוצת ההאקרים תומכי **דאעש**, **AnonGhost**, הודיעה ברשתות הפנימיות שלה – כי תתקוף משרדי ממשלה, מוסדות חינוך אקדמיים, רשויות לאומיות, משפטיות ופיננסיות, בנקים, ספקיות אינטרנט ושגרירויות של ישראל סביב העולם; כך מסר צוות מודיעין הסייבר של MadSec.

על פי החוקרים, האתרים והרשתות הפנימיות של המטרות יסבלו ממתקפות מניעת שירות, DDoS, הנדסה חברתית ומתקפות אחרות ושונות לפני מתקפת OpIsrael, הכוללות "ניסוי כלים", איסוף מידע ותצוגת יכולות. קבוצות נוספות של האקרים שמשתתפות במבצע, כוללות את קבוצת האקטיביסטים **Red Cult** שהשתתפה בעבר בהתקפות כנגד דאעש, וקבוצות תוניסאיות, דוגמת **Fallaga Team**.

קבוצת טלגרם סודית הוקמה על ידי AnonGhost Team לקראת OpIsrael. בקבוצה יעבירו התוקפים בזמן אמת מידע על המתקפות: Telegram.me/OpIsrae [1]

דורון סיון, בעלי **MadSec** אמר כי "ישראל תיאלץ להתמודד השנה מול גל נרחב של מתקפות שונות נגד הרשתות והתשתיות שלה. ההאקרים משדרגים השנה את טכניקות התקיפה ומשתמשים בכלים חדשים שלא נראו במבצעים הקודמים. על מנת להגדיל את יעילות המבצע, האקרים מפרסמים מדריכים טכניים לשימוש בכלים, עם רשימה של מטרות תקיפה. ארגונים נדרשים להתכונן מראש ולבחון את מוכנותם".

סיון הוסיף כי "על חברות וגופים ממשלתיים לשקול הקשחה של מערכות ההגנה המקיפות שלהם, על מנת לזהות סוגי תקיפה שונים, מתקפות מניעת שירות (DDoS) ומתקפות על שירותי אחסון אתרים (Web Application). לעסקים קטנים ומשתמשים בסיסיים מומלץ ליצור קשר עם ספקית האינטרנט שלהם ולוודא כי מדיניות אבטחת המידע בארגון מעודכנת וכי ה-Group Policy מוגדר כראוי".

פריצה לרשתות אינטרנט ביתיות

חוקרי חמ"ל הגנת הסייבר של **רדוור** (Radware) הישראלית, זיהו את הפצתו של כלי התקיפה RouterHunter 2.0. הכלי מיועד לפרוץ לנתבים ביתיים, ולהשתלט על רשתות Wi-Fi ביתיות.

הפריצה מתאפשרת על ידי ניצול חולשות באבטחת המידע של הנתב והשתלטות עליו מרחוק. לאחריה, מתבצעת גניבת נתונים העוברים ברשת הביתית, או השתלטות על ציוד הקצה המחובר אליו – מחשבים, טלפונים חכמים, טאבלטים, טלוויזיות חכמות, מצלמות, מדפסות ועוד. אחת הסכנות המרכזיות, מציינים חוקרי רדוור, "היא ביכולת להשתמש בנתבים שנפרצו כדי להפוך אותם לכלי תקיפת סייבר".

חמ"ל אזרחי

חברת מודיעין הסייבר **White-Hat** תקים מחר (ה') חמ"ל אזרחי, בו מומחי החברה ינטרו את המרחב הקיברנטי, ידווחו על תקיפות בזמן אמת ויעניקו סיוע טכני לכל דורש. White-Hat תקים את החמ"ל בשיתוף גופי משטרה וביטחון לאומי, ונציגי חברות סייבר נוספות. צוות חוקרי המודיעין של החברה אסף ב-2015 מידע שכלל יותר מ-400 כתובות מייל ממשלתיות, פרטים של עשרות כרטיסי אשראי, יותר מ-10,000 כתובות דוא"ל, מגורים ומספרי טלפון, ופרטים דיגיטליים נוספים, כמו גם עשרות פרופילים בפייסבוק של עסקים ואנשים פרטיים שהכילו סיסמה. אנשי החברה התריעו על הפרצות בפניהם.

לדברי **שרון נימירובסקי**, מנכ"ל White-Hat, "מדי שנה המודעות לקראת יום זה גדלה והולכת. התוקפים מודעים לכך ולכן התקיפות מתחילות עוד הרבה קודם. ב-2015 היינו עדים למספר כלים וטכניקות התקפות סייבר שונות כנגד רשתות ותשתיות. למרות שההתקפות היו צנועות בהיקפן ובמידת הנזק שגרמו, ההאקרים עדיין הצליחו למנוע שירות באתרים של גופים מרכזיים, להשחית אתרים ולהדליף נתונים. מודעות לנושא ונקיטה במספר צעדים בסיסיים יכולים לסייע במזעור הנזקים".

עד כה זיהו אנשי החברה ארבע קבוצות הצפויות להשתתף בקמפיין השנה: AnonGhost, RedCult, Fallaga Team, Anonymous.