סייבר

# רגע לפני: כיצד להיערך למתקפת הסייבר והאם עלינו להילחץ?

**עודכן 06/04/2016 22:21**
**יוסי לוי, נענע10 Online**

**ארגוני האקרים פרו פלסטינים חברו להם יחדיו למתקפת סייבר מתואמת ומתוכננת מראש שעתידה לצאת לפועל בשעות הקרובות. האם יש צורך להלחץ? הפרטים על #OpIsrael - בפנים**

**ביממה הקרובה (חמישי) אמורה לצאת לפועל מתקפת הסייבר ה"שנתית" של אנונימוס על ישראל. ה"מתקפה" המתוכננת, המכונה operation israel וקיבלה את ההאשטג #OpIsrael ברשתות החברתיות, מושכת האקרים פרו פלסטינים מרחבי העולם.**

**כמדי שנה גם הפעם הארגון מבטיח שישראל תימחק ממפת האינטרנט, וגם השנה מובטחת לנו "שואה דיגיטלית" עבור ישראל וכל הציונים. אז האם אנחנו צריכים להיבהל? לא, האם צריך להיערך לעניין? כן, בערך. לשם כך בדקנו כיצד החברות המובילות בשוק הסייבר נערכות, וכיצד צריך להיערך המשתמש הביתי למתקפה הקרובה.**

**קצת רקע: "מבצע OpIsrael", הינה פעילות התקפית אנטי-ישראלית מתואמת במרחב הסייבר, המתבצעת על-ידי מספר קבוצות האקרים מרחבי העולם בתאריך 7 באפריל (המועד עליו הכריזו בפומבי קבוצות אלו), כל שנה מאז שנת 2013. קבוצות אלו מזהות עצמן עם קהילת האקטיביסטים Anonymous ועל פי רוב, מעשי הפשיעה בסייבר שהן יוזמות במהלך פעילותן מיועדים ליצירת הד תקשורתי, הפחדת הציבור והעברת מסרים פוליטיים. לאור ניסיון העבר מהשנתיים האחרונות, פעילות זו התרחשה בימים שלפני ועדה הפומבי של התקיפה ב-7 באפריל, ולכן, לפיכך, עולה הסבירות כי גם השנה מתקפה זו תתפרס על פני מספר ימים.**

**אנונימוס צילום: גטי**

**אז בינתיים, כיצד ניתן להתגונן בפני המתקפה הקרבה? ובכן התשובה היא שעבור המשתמש הביתי לא מדובר ביום שונה מבכול יום אחר. אלו הם המלצות המומחים: לא להתפתות ולפתוח מיילים חשודים ולא צפויים ממקורות שאינכם מכירים (למרות שיתכן והמיילים יגיעו גם מחברים ומכרים). לא ללחוץ על לינקים חשודים בפייסבוק (בעיקר סרטוני סקס למינהם) ולא ללחוץ על כל מיני חלונות ושאר פופ אפים שומבקשים ממכם להקיש עליהם. לדאוג לרענן ולהחליף סיסמאות לתיבות הדואר ולפייסבוק שלכם, לעדכן את הגדרות תוכנות האנטי וירוס שלכם (ואם אתם לא משתמשים באחת - כדאי שתתחילו).**

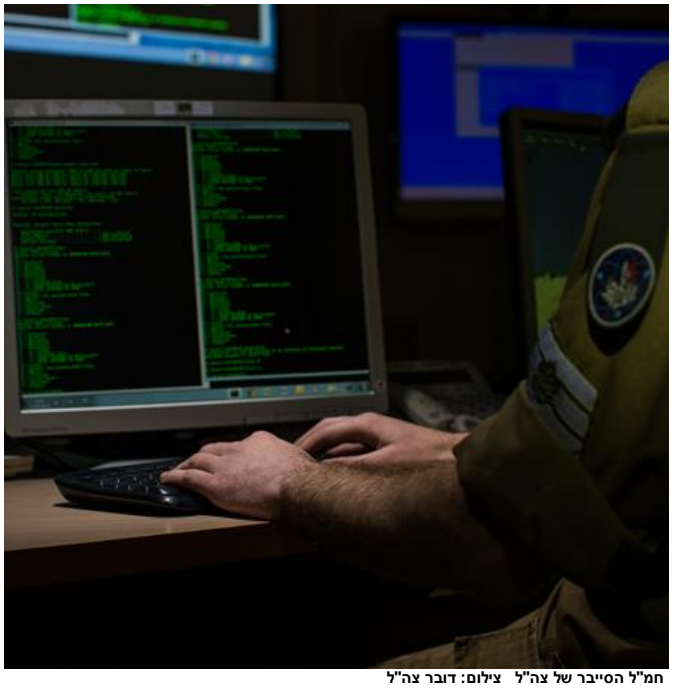
**במגזר העיסקי המצב קצת שונה, מרכז IL-CERT נערך במיוחד לארוע ופותח חמ"ל סייבר לתגובה בזמן אמת. המרכז הינו גוף מקצועי בלתי-תלוי, שמורכב ממומחי אבטחה בכירים במגזר הפרטי ובינהם עשרות מומחים, האקרים, חוקרי מתקפות סייבר, מנהלי אבטחה, אנשי אקדמיה ומנכ"לי חברות - מתכנסים מדי שנה לקראת המבצע, כדי לנטר מתקפות רשת ולספק מענה לחברות ומשתמשים שנפגעו מהן. מומחי IL-CERT סבורים כי 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 אלפי מתנדבים מרחבי הארץ, שמספקים מידע והתראות על תקיפות.**

האקר צילום: fotlia



במקביל, גם חברת הסייבר White-Hat, תקים ביום התקיפה, חמ"ל אזרחי עם מיטב מומחי החברה, אשר ינטרו את המרחב הקיברנטי, ידווחו על תקיפות בזמן אמת ויעניקו סיוע טכני לכל דורש. White-Hat תקים את החמ"ל בהתנדבות כמדי שנה, בשיתוף עם גופי משטרה וביטחון לאומי, כמו גם נציגים של חברות סייבר נוספות בתעשייה.

"מדי שנה המודעות לקראת יום זה גדלה והולכת. התוקפים מודעים לכך ולכן התקיפות מתחילות עוד הרבה קודם, עד מספר חודשים, כאשר למעשה ב-7 לאפריל נחשף "השלל" של אותן תקיפות", מספר שרון נימירובסקי מנכ"ל החברה. מהחברה נמסר כי "לקראת Opisrael 2016, עקבה יחידת המחקר של White Hat בשבועות האחרונים אחר קבוצות התקיפה ב-DarkNet ובערוצי ה-IRC המשויכים ל-Anonymous על מנת לספק מודיעין טקטי מהיר ואיכותי לארגונים הנמנים על לקוחות החברה וחשופים לתקיפה. עד כה זיהתה White Hat ארבע קבוצות הצפויות להשתתף בקמפיין השנה - AnonGhost, RedCult, Fallaga Team, Anonymous".



חמ"ל הסייבר של צה"ל צילום: דובר צה"ל

**"נשאלת השאלה מדוע מפרסם ארגון אנונימוס את התאריך המדויק שבו הוא יתקיף את מדינת ישראל?" שואל אלי כהן מנכ"ל Experis Cyber, המתמחה בשירותי soc, שירות מנוהל המעניק הגנה היקפית 24/7. "מדוע הוא לא שומר על אלמנט ההפתעה שכה חשוב בלחימה קונבנציונליות או דיגיטלית? התשובה היא", מספר כהן "שעצם ההכנה של המדינה כוחות הביטחון וארגוני התשתית הקריטית היא הפגיעה המשמעותית ההערכות אליה גורמת להשקעה של הון תועפות ברכישת מוצרים שיגנו מפני ההתקפה שתוצאותיה ברוב הפעמים מזעריות ובכך למעשה מצליחים לפגוע ולגרום נזק למשק הישראלי. אירועי סייבר קורים כל הזמן, רק בשבועות האחרונים משתוללים וירוסים של כופרות שפוגעות בעשרות אלפי מחשבים בישראל בכל יום, הנזק שנוצר בווירוסים הללו הוא פי כמה מהנזק שיוצר ב 7/4 לארגונים ולאנשים פרטים".**

אלי כהן צילום: חדר בקרה

**"בזמן צוק איתן היו למעלה ממיליון התקפות על מדינת ישראל ביום (לעומת כמאה אלף בזמן רגיל)", הוא אומר, "ארגונים פרטיים ואזרחים מהשורה כמעט ולא נערכים למתקפה ולכן הם אלו הפגיעים ביותר. סביר להניח שחלק מהארגונים הקטנים שלא יכולים להרשות לעצמם רכישת מוצרי אבטחה מתקדמים יתעוררו עם אתר אינטרנט עם כתובות נאצה, וירוס כופרה או מייל זדוני שנשלח לאנשי הקשר. כשבאמת רוצים לגרום נזק לתשתיות ולמדינה עושים זאת מתחת לראדר ולא מפרסמים זאת חודש לפני ב YouTube. וכרגיל מי שיסבול הם החברות הקטנות חסרות האמצעים".**

**"ספקיות האינטרנט הן בראש הכוונת של מתקפת ההאקרים השנתית ב-7 באפריל", אומר מהצד השני רוני בכר, סמנכ"ל חטיבת טכנולוגיות סייבר באבנת אבטחת מידע. "לאורך 3 שנים שמתקפות סייבר אלה מתקיימות, אנו רואים ניסיונות שונים**