

# "האיראנים משתפרים בצורה מדהימה, אמנות ההסתרה בתמונה עוד חדשה להם"

הארץ

ניווט 🔍 חיפוש

קיומם, ומחבר זאת למאבק בין ישראל לאיראן בשדה הסייבר

🖨️ קריאת זן | 📖 שמרו | 💬 10

✉️ 📧 📱 📘



ד"ר גיל דוד. לימד באוניברסיטה בפינלנד ובין תלמידיו היו גם סטודנטים איראניים צילום: עומר הכהן

בפיגוע הכפול שהתרחש בירושלים לפני כשבועיים, ובו נרצחו אריה שצ'ופק וטדסה טשומה, היה גם אלמנט של ניצחון תודעתי לאיראן, שכמעט ולא נדון בתקשורת. יממה לאחר הפיגוע הפיצה קבוצת פצחנים (האקרים) בשם "מטה משה" (Moses Staff), המזוהה עם המודיעין האיראני, צילומים ממצלמת



יוסי מלמן

התראות במייל 🔔

06 בדצמבר 2022

אבטחה שהתקין גוף ביטחוני גדול בצומת בכניסה לעיר, סמוך לאחת הזירות. מסיבה לא ברורה המצלמה לא נבדקה, או שנבדקה אך התייעוד שנאסף בה לא הוצא לתקשורת. מי שעשו זאת הם אנשי "מטה משה" ובכך נוצר הרושם כאילו הפיגוע הכפול הוא בעצם מבצע איראני נועז. שב"כ, אנב, ממשיך לחפש אחר מבצעי הפיגוע הכפול. זהותם והשתייכותם הארגונית טרם פורסמו.



**Local Focus - Security Alerts**

עקוב @LocalFocus1

The Iranian hacker group "Moses Staff" leaked a video showing the bombing attack at western Jerusalem City entrance.

צפה בטוויטר

@LocalFocus1 **Local Focus - Security Alerts**

Explosion took place in the area between Givat Sha'ul and Begin Road at Jerusalem City Western entrance. Fatalities reported among Israelis.

"החדירה למצלמת אבטחה - אחת מיני רבות במרחבים הציבוריים בישראל - היא פעולה קלה לביצוע. כל פצחן חובב יכול לבצע אותה. לא צריך בשביל זה מנגנון

של מדינה. זה לא שבוקר אחד קם הצבא הווירטואלי של איראן ויוצא למלחמה", מעיד ד"ר גיל דוד, מומחה בינלאומי לסייבר, בינה מלאכותית (AI), הסתרת מידע ואבטחת מידע, ומחבר הספר "אמנות ההסתרה" שראה אור באחרונה. "חברות וארגונים מדינתיים שמתחקים אחרי קבוצות הפצחנים הללו מעניקים להן שמות לפי הקודים וצורת התכנות. 'מטה משה' היא דוגמה לקבוצת סייבר מזו. לרוב הקבוצות יש מעין טביעת אצבע. אם המסר המקודד נראה כמו נחש, למשל, החוקרים יעניקו לקבוצה את הכינוי 'סנייק'. זהו קוד משותף או פעולה משותפת תקל מאוד לאורך הזמן על המנינים".

## האם הקבוצות האלה הן עצמאיות או חלק ממערך סייבר גדול יותר של המודיעין האיראני?

"הן חלק ממערך הסייבר האיראני. הכול מוכוון מלמעלה".

## נגד מי מכוונות התקיפות האלה?

"הקבוצות האלה, והן לא רק איראניות כמובן, תוקפות אנשים בודדים, קבוצות, ארגונים ממשלתיים, כולל גופי ביון ומודיעין וממשלות. כפי שאנו יודעים ממקורות נלווים, גם ישראל מותקפת כל הזמן בידי האיראנים".



זירת הפיגוע בצומת רמות בירושלים, בחודש שעבר צילום: אוהד צוינגברג

## לשם מה?

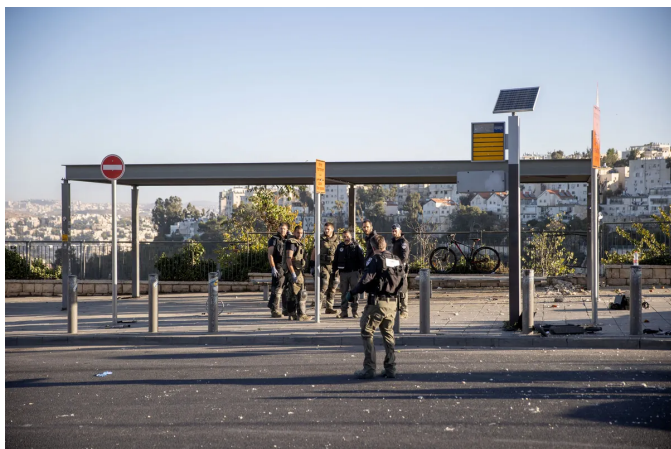
"בעיקר לאיסוף מידע. מה שאני מזהה הוא שימוש גובר של האיראניים בשיטות להסתרת מידע ולתקשורת חשאית. הם תוקפים תוך כדי מאמץ להסתיר את התקשורת שלהם עם הכלי התוקף".

השימוש שעליו מדבר דוד מכונה בשפה המקצועית "סטגנוגרפיה", נגזרת של המילה היוונית "סטגנו" שפירושה "חבוי" או "מכוסה". או במילים אחרות: הסתרת מסרים כך שאף אחד זולת המקבל לא יוכל לדעת על קיומם. חשוב להבחין בהקשר זה בין סטגנוגרפיה ל"קריפטוגרפיה", שהיא תורת כתיבת הסתרה וההצפנה, שבה עצם קיום המידע אינו מוסתר, אלא רק תוכנו.

בספרו מציג דוד שורה של דוגמאות מההיסטוריה ועד העידן הדיגיטלי בהן ניסו בודדים (אסירים למשל), קבוצות, חברות, ארגוני ביון ומדינות, להסתיר את סודותיהם בלי שיתגלו ומזמין את הקורא - גם אם לא תמיד בשפה המובנת להדיסו - לעולם שבו הגיבורים הם סוכני חרש, מרגלים, בוטים ואלגוריתמים מתמטיים. דוגמה: "כשיושבים במסעדה ומתלבטים מה להזמין מהתפריט באמצעות קוד סריקה (QR), מישהו יכול להסתיר שם מידע ואף אחד חוץ ממקבל המסר לא ידע זאת. עשיתי ניסוי כזה והצלחתי להסתיר את המידע. גם סריקת הקוד או הצילום שלו לא יאפשרו את גילוי המסר החשאי".

## להסתיר את הכל

דוד, בן 48, התחנך בנימנסיה העברית בירושלים ולאחר שירותו הצבאי (מפקד טנק) למד מדעי המחשב באוניברסיטה העברית. את הדוקטורט שלו בזיהוי תקיפות ברשת באמצעות למידת מכונה עשה באוניברסיטת תל-אביב. בהמשך ערך באוניברסיטת ייל האמריקאית מחקר על בינה מלאכותית. נוסף על כך, במשך שבע שנים הוא שימש כראש ענף מחקר ופיתוח ביחידת סייבר של אחד מגופי משרד ראש הממשלה. באותה תקופה, כך לפי פרסומים בארה"ב, היו אנף המודיעין בצה"ל והמוסד מעורבים בפיתוח והפעלה של וירוס המחשבים "סטוקונט". הווירוס הדביק בשנים 2004-2009 את המחשבים שהפעילו ופיקחו על הסרזות באתר להעשרת אורניום בנתאנו וכתוצאה מכך ניווקו כשליש מהן. דוד מסרב לדבר בנושא זה מעבר למה שפורסם בתקשורת.



זירת הפינוע בתחנת האוטובוס בכניסה לירושלים, בחודש שעבר צילום: אוהד צויגנברג

למרות שמנהליו ביחידת הסייבר באחד מגופי משרד ראש הממשלה ניסו לשכנעו להישאר, דוד העדיף לפנות למחקר אקדמי ולייעוץ למערכת הביטחון ולחברות ההיי-טק העוסקות בפיתוח אלגוריתמים לבינה מלאכותית. בין היתר, לימד באוניברסיטה בפינלנד ובין תלמידיו היו גם סטודנטים איראניים. "האיראנים משתפרים בצורה מדהימה מקמפיין לקמפיין", הוא מעיד. "לאחרונה הם החלו לפעול בשיטה של הסתרה בתמונה. זה משהו חדש עבורם. הם עדיין לא עושים זאת בצורה מושלמת, אך יש להם נוכחות בולטת ברשת. ארגוני ביון מערביים השתמשו בשיטה זו כבר לפני כמה שנים".

### מה זו הסתרה באמצעות תמונה?

"נניח שאיראן רוצה לתקוף מטרה בישראל כמו מתקני המים של 'מקורות' שהתוקפו בעבר. התוקפים בדרך כלל מוצאים איוושהי חולשה ונכנסים דרכה לארגון. זה יכול להיות ששיחזו משהו מתוך ארגון או שהצליחו לחדור אליו באופן עצמאי. התוקף שולח פקודות כמו 'תאסוף את כל הסיסמאות, האימיילים והמסמכים מהמחשבים האלה והאלה'. זה מה שנקרא שו"ב - שליטה ובקרה. השאלה היא איך אתה שולח את הפקודות והעדכונים בלי להתגלות. לכן רוב השו"ב בשנים האחרונות מבוסס על הסתרה. הסתרת מידע".

**כלומר המטרה היא לשלוח הודעות שייראו לצד השני כתימומת ולא**

## כהודעות מוצפנות.

"נכון. לשלוח לצד השני משהו כמו תמונה שתראה תמימה לנתקף, לצד שמקבל את ההודעה, והוא לא יחשוד בכוונותיו של השולח".

## איך זה פועל?

"תיקח כל תמונה, לדוגמה תמונה של מזוודה שהתוקף שולח באימייל כקובץ מצורף - מי שמסתכל רואה תמונה תמימה של מזוודה ואומר לעצמו 'זה לא משהו חריג'. אבל בפועל, השולח, נניח התוקף האיראני, מעביר דרך תמונת המזוודה הודעות מוסתרות, כמו הוראות להפעלה, לתקיפה כזו או אחרת או לאיסוף מידע.

"כשאתה מסתיר מידע בתמונה אתה מנסה ליצור בה שינויים קטנים שלא ירגישו שהיא חריגה. אבל האיראנים טעו בכל מיני מבצעי סייבר שלהם ושינוי את התמונה באופן מודגש. הם גם שלחו כל פעם את אותה התמונה, אבל בכל פעם הוסתרה בה מידע אחר. כלפי חוץ, לעין האנושית, היא נראתה זהה, אבל בפועל, אם תשווה בין התמונות באמצעות מחשב - תזהה שהתמונות שונות במקצת. זה מעורר חשד כי ברור שמישהו ביצע בכל פעם מניפולציה שונה באותה תמונה".

## אתה כותב בספרך שקשה לגלות את הסתרת מידע באמצעות תמונה.

"נכון. זה לא פשוט לחשוף את ההסתרה, אבל יש פתרונות המבוססים לא על זיהוי ההסתרה אלא על ביצוע שינויים בתמונה, כגון שינוי פורמט או שינוי גודל. פתרונות אלה נמצאים בעיקר בשימוש של ארגונים גדולים, כמו ארגוני ביון או חברות ביטחוניות".

למרות כל הכלים הטכנולוגיים המשוכללים שעומדים לרשות משטרים, ועל אף שמדינות מנסות יותר ויותר להצר את חופש זרימת המידע, דוד מסכם את ספרו באמירה שלאנשים מן השורה עדיין עומדת היכולת להתגבר ולעקוף כל סוג של פיקוח. "אם יעמדו לרשות האזרחים כלי סטנוגרפיה מתקדמים", הוא אומר, "הם יוכלו להעביר ביניהם 'מידע אסור' ולהתגבר גם על הצנזורה הנוקשה. כלים כאלה יאפשרו ליצור אינטרנט חופשי או לכל הפחות להפיץ ולהעביר מידע בחופשיות, במסווה של אינטרנט מפוקח".

בניסיון לעורר עניין נוסף, מציג דוד בפני קוראיו חידות - בדומה לאלה שניסחו  
בעבר המוסד ושבי"כ. ביכולתי הדלה הצלחתי לפצח רק שתיים מהן ונחלתי כישלון  
חרוץ גם בניסיון להחדיר לכתבה זו מסר מוסתר.



### יוסי מלמן | חשאי

עיתונאי ופרשן לענייני מודיעין וביטחון כל חיי המקצועיים - 45 שנים.  
מחברם של עשרה ספרים בנושאים אלה בארץ ובעולם, ובערוב ימי גם יוצר  
דוקומנטרי.

ושכחתי את הדבר הכי חשוב - למרות נילי המופלג (71), התקף לב ושבץ  
מוחי קל, אני ממשיך לרוץ (באישור הרופאים עמם אני מתלוצץ).