

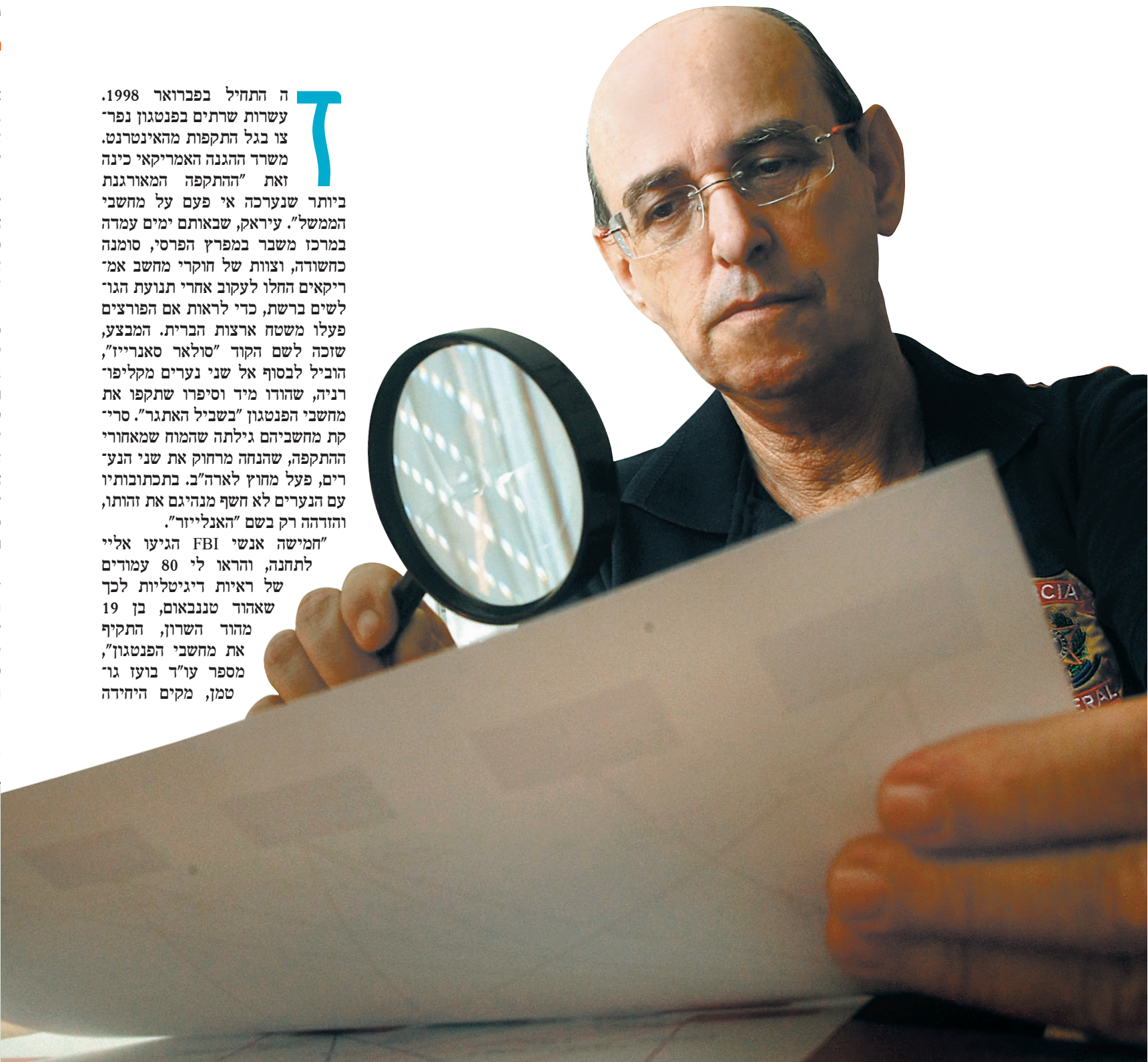


הצצה: כך חוקרים פשעי מחשב וחושפים רשתות טרור באינטרנט

עו"ד בועז גוטמן, שייסד את מפלג עבירות המחשב במשטרה, חושף את עולם הבילוש הדיגיטלי

צמרת פרוט

אבטי אבטי



לחקירת פשעי מחשב במשטרת יש ראל. בפברואר 1998 גוטמן שימש ראש מפלג תשאול ביחידה לחקירות הונאה במשטרה, והיה אחד השוטרים המעטים שהבינו באינטרנט. "עוד באותו ערב שלחנו שוטרת שתתקשר לטנבאום ותתחזה לבחורה צעירה שמתעניינת בו. היא קבעה לפגוש אותו בביתו למחרת בבוקר, ובשש בבוקר התייצבנו אצלו

”

היום עובדים בשיטה שבה מחברים למחשב דיסק און קי ששואב את המידע לבדו – בלי שהחוקר צריך לגעת במחשד. אבל האתגר הוא לא להשיג את המידע, אלא להבין מה רואים”

אנחנו, עם צו חיפוש. אני זוכר שישבתי בסלון שלו ושאלתי אותו באילו כינויים הוא משתמש ברשת. אחרי שציין שלושה, הבנתי שזה באמת הוא.”

ה"אנלייזר" היה מתוחכם מכפי שה"שבו החוקרים. לאחר השיחה מ"הבחורה הצעירה" הוא חשד שמשוה אינו כשורה, מחק את כל תכולת מחשבו ופרמט את הכונן הקשיח כדי לא להשאיר עקבות. "כשעצרנו אותו הוא אמר לנו שהוא פרמט את המחשב, ואין סיכוי שנוציא ממנו משהו", אומר גוטמן. "נאן נכנס לתמונה תהליך הויהו הדיגיטלי שלנו. בעודת תוכנה בשם 'מירור' שחורנו את תכולת הדיסק שנמחק. מול העיניים של סנבאום הרפסנו את כל מה שהיה במחשב, ראינו אחרי ראינו. לכתב האישור הוספנו אחר כך טעיף של השמרת ראינו. דרך אגב, אם הוא היה מפרמט את הכונן שלו פעמיים, התוכנה שלנו לא הייתה מצליחה לשחזר את הנתונים. זו הייתה תוכנה ישנה. אבל מאז השתכללנו".

על טנבאום נגזרו שישחודש עבודות שירות, שלאחר ערעור הפקליטות הומרו בשנה וחצי מאסר. שופטת בית משפט השלום בכפר סבא קלרה רג'ניאנו תיארה גנור דינו של טנבאום את הקושי שבאיתור עבדי יריני מחשב: "לאחר החרייה למחשב

לא נותרים סימנים כגון רסיסי זכוכית או מנעולים מעוקמים. גילוי עבירות כגון אלה מחייב מיומנות טכנית גבוהה ומוחות מתוחכמים לא פחות מאלה של מבצעי העבירה”.

משועים לכוח אדם

”התחלתי בזה בראשית שנות התש"ע, אומר גוטמן, שבסוף אותו עשור עזב את המשטרה, וכיום עובד כעורך דין המתמחה בעבירות מחשב. "שב" תי עם אוריאל שטרית, שהיה זוכרם היחיד בישראל שעבר קורס חקירות מחשב, ולמרותי ממנו. עד אז חקירות מחשבים טופלו על ידי סנ"צ מאיר זוהר – שלימים החליף אותי בפיקוד על מפלג עבירות המחשב. הוא טיפל בתחילת שנות התשעים עם מנהל רשת המחשבים של יאח"ה בכמה חקירות מחשב מעניינות. אחת היתה של נערה בת 17, בת של דמות ידועה מתחום המוזיקה בישראל, שפרצה לשרתים של בוק, התעשייה האווירית ובנק דיסקו נט. כמו האנלייזר, היא אמרה שעשתה את זה בשביל האתגר. סגרנו את זה בלי כתב אישום. היה גם האקר מטבעות

שפרץ למחשבים של 'דיעות אחרות נות' ושינה פרטים בכתבה של 'עקוב אילון, שהיה אז הכתב בניו יורק. הב' חור הזה גויס אחר כך ליחידת מחשבים מובחרת בצה"ל.

”הניסיון הראשון להרים יחידה רצינית לפשעי מחשב היה באמצע שנות התשעים. 30 שוטרים עברו קורס אצל חברת אבטחה ישראלית – אבל רובם נוצלו כסנ"צ לקצינים בכירים. לקחו אותם לבנות מצגות למפקדי מחוזות, או לתקן את מערכת ההפעלה במחשב של המפכ"ל יהודה וילק. את מפלג עבירות המחשב הקמתי רק אחרי פרשת האנלייזר. אז היו לי רק שני תקנים, ועד היום היחידה סובלת ממחסור בכוח אדם. היום, אחרי סיפוח מפלג המחשב, ליחידה הארצית ללוחמה בפשיעה, יש במפלג עשרה חוקרים בסך הכל. כמיפלג עבירות המחשב באיטליה, לשם השוואה, יש 800 חוקרים”.

”כנן, אנחנו משועים לכוח אדם”, אומר רב בנק מאיר חיון, ראש צוות במפלג עבירות המחשב. "יש לנו ארבעה חוקרים וקצין, ועוד מעברה עם שני שוטרים. בכל אחד ממחוזות המ' שטרה יש חמישה חוקרים שעברו הכשרה במחשבים. אנחנו מחפשים עוד עשרה חוקרים, אבל הבעיה היא לגייס

אותם. קשה לפתות אנשי מחשבים עם השכר משולם במשטרה, ומי שאין לו תואר ראשון צפוי להשתכר מעט מאוד. מה שיש לנו להציע זה האתגר והעניין שבמשרה”.

ההמחשה העיקרית למחסור בכוח אדם במפלג עבירות המחשב היא שא' פילו מפקד אין לו. החלפתו של מאיר אחוין ב'2005 על ידי סנן ניצב אבי

”

30 השוטרים הראשונים שעברו קורס בחקירת פשעי מחשב נהפכו לסנ"צים של קצינים בכירים. לקחו אותם לבנות מצגות ולתקן את המחשב של המפכ"ל יהודה וילק”

”

אביב זכתה לביקורת בגלל הרקע המורע של אביב בתחום עבירות המחשב והעובדה שאביב עצמו הורשע בעבר בהטרדה מינית של פקירתו. מאז פרישתו של סנ"צ אביב לגמלאות לא נמצאו מחליף.

CSI דיגיטלי

גוטמן מספר שחקירות פשעי מחשב – "קומפיוטר פורניקס" באנגלית – אינן הליך פשוט: "רוב החקירה היא שימוש בתוכנות מיוחדות כדי לאתר בהארד דיסק מילים וקבצים, ולנתח אותן כדי לגלות את היסטוריית הגליי צריכים לברוק הארד דיסקים שנמחקו, שיש של בעלי המחשב. לפעמים אנחנו צריכים להפיק מהם ראיות שיעזרו להוכיח אשמה בבית משפט.

”למשל ב'2005 ארה"ב הפציצה את הבית של אבו מוסב אל-זורקאווי מאל קאעידה. הם הוציאו את שאריות המחשב שלו מהיריסות הבניין, ושלוו אותן למכון לשחזור ראיות בקליפורניה. המ' כון הצליח להוציא מהמחשב מידע רדיעיני, כמו גם נתונים פיננסיים ומידע רפואי על ודקאווי, שחוסל ב'2006.

באילו כלים משתמשים חוקרי פשעי המחשב? "בעיקר בתוכנות", אומר דורי פישר מחברת חקירות המחשב We Secure, שעובדת עם חברות התקשורת והבנקים הגדולים בישראל. "התוכנה ששולטת היום בשוק היא Encase של חברת גיירנס. תוכנה נוספת היא FTK של אקסס דאטה, יש גם כלים חנימים שנמצאים על הרשת, וגם תוכנות שה' ברות אבטחה מייצרות ומספקות רק לכוחות הביטחון. באופן מזור, הממצאים של התוכנות מתקבלים כראיה משפ' טיית על בסיס הפופולריות של התוכנה בבתי המשפט. אם השתמשו בכלי הזה מאות פעמים במשפטים בעבר, הוא ית' קבל באמין גם הפעם”.

”זה עובר גם להפך”, אומר גוטמן. "כשלקחנו את האחים העיוורים באריר, לפסגו אצלם מחשב נייד עם אלפי מס' פרי כרטיסי אשראי, אבל ברקנו אותו עם תוכנה של נורטון, כי תוכנת השחזור שלנו נתקעה. השופטת סירבה לקבל את הראיות עד שלא יובא מומחה מנורטון שיעיד על מהימנות התוכנה. המומחה לא הגיע והראיות לא התקבלו”.

”תוכנה חדשה ששמעתי עליה אבל לא עבדתי איתה אישית היא תוכנה של מיקרוסופט בשם קופי COFEE – ראשי תיבות של Computer Online – Forensic Evidence Extractor – צ”ב”.

”אבל האתגר הוא לא רק להשיג את המידע, אלא להבין מה רואים”, ממשיך פישר. "חוקר ממשטרת לונ' דון סיפר לי איך לכד לפטופ של תא סטרויסטי שפעל בלונדון. אחד האת' רים בהיסטוריית הגלישה של לפטופ נראה כמו דף לכו, אבל בקוד המקור של האתר הם מצאו קישורים לתמונות של אנשים שצריך היה להכין עבורם דרכונים מווייטים”.

”שיטת החקירה משתנת כל הזמן”, אומר פישר. "פעם היה מספיק לתפוס מחשב, להוציא לו את הדיסק, לשכפל ולברוק. אבל בשנים האחרונות יש המון תוכנות הצפנה שמי ביאות לכך שבר' גע ששולפים את התקע, המידע עובר קיודר והחקירה נג' מרת. היום צריך לשלוף נתונים

שהו ניסה לגנוב מהבנק 220 מיליון דולר. המשטרה עצרה במרץ 2005 יש ראל בשם ירון בר' לונדי בחשד שהוא פתח את החשבון שדרכו ניסו לג' נוב את הכסף, אבל שחררה אותו אחרי שאיש לא הצ' ליה לתפוס את הנגבים עצמם. בסופו של דבר, מה שקובע במקרים האלה הוא התבונה של החוקר”.

פשעי מחשב בעולם

כל חוטי החקירה מובילים לארה"ב

פשעי המחשב בארצות הברית מסבים נוק של מאות מיליוני דול' רים. דו"ח של חברת CSI Computer Crime שנתעד בסיוע FBI מגלה שכל מחשב שני במגזר העסקי האמ' ריקאי הרבק בשנה האחרונה בוירוס או בתוכנת ריגול. חברות שנפלו קר רבן להונאה עסקית באמצעות הרשת ריווחו על נוק של חצי מיליון דולר בממוצע להונאה. לפי דו"ח של חברת האבטחה הבריטית גרילק, ב'2007 בוצעו בבריטניה יותר מ'3.5 מיליון הונאות מחשב ורבע מיליון ניסיונות לגניבת זהויות. הדו"ח מראה שמספר פשעי המחשב בבריטניה עולה בכ'7% בשנה. לפי הדו"ח ולפי נתוני FBI, ארה"ב היא המדינה שבה פועלים רוב עברייני הרשת בעולם: כ'63% מההונאות הרשת מקורן בארה"ב. אח' ריה בריטניה עם 15.3%, ניגריה עם 5.7%, קנדה עם 5.6% ורומניה עם 1.5% מסך הונאות הרשת.

המחשב כשהוא חי. צריך לשאוב מידע לא רק מההארד דיסק של המחשב אלא גם מהזיכרון הזמני שלו. אלה דברים שיחידות פשעי המחשב בעולם לומדות בשנתיים האחרונות”.

”כשמשטרה נתקעת, היא נעזרת הרבה פעמים בחברות אורחות”, אומר גוטמן. "כמו במקרה של דורי שטרנבי רג, שהורשע ב'2005 בפריצה למחשבי סניף בנק הדואר בחיפה. החוקרים לא הצליחו לפצח את ההצפנות במחשב, ורק חברה אורחית מצאה את הראיות”.

”יוצא לנו לעבוד בפרויקטים מות' פים עם המשטרה”, אומר ג'קי אלטל מח' ברית אבטחת המידע See Security. "נתנו לי פעם לפרוץ מחשב של עבריון, והייתי צריך לעבוד נגד השווחן כי עורכי הדין של העבריון רשעו את המחשב. בסופו של דבר הלחתי להוציא רישומים של העברות כספים, וזה היה מספיק”.

”היו ליחידה כישלונות”, אומר גר' טמן. "למשל – היחידה פספסה לגנ' רי את פרשת הסוס הטרויאני ב'2005. ראש יאח"ה מירי גולד, שלא היה לה מושג בנושא, נתנה לתלונה שהגיעה מפרטנר לשכב בארון. רק התלונה שה' גיש אמנון ז'קונט טופלה על ידי חזו תל אביב, והם הרימו את הפרשה. עוד כישלון היה ניסיון פענוח הפריצה לבנק סומיטומו היפני באנגליה. מ' שהו ניסה לגנוב מהבנק 220 מיליון דולר. המשטרה עצרה במרץ 2005 יש ראל בשם ירון בר' לונדי בחשד שהוא פתח את החשבון שדרכו ניסו לג' נוב את הכסף, אבל שחררה אותו אחרי שאיש לא הצ' ליה לתפוס את הנגבים עצמם. בסופו של דבר, מה שקובע במקרים האלה הוא התבונה של החוקר”.

מפלג עבירות מחשב תעודת זהות

היחידה	האתגרים	הכלים	הפרשות
מפלג עבירות המחשב הוקם בשנת 1999 כפוף כיום ליחידה הארצית להב' 443	מחסור בכוח אדם: ביחידה חמישה חוקרים בלבד אין ממקד: לא מונה מחליף לסנ"צ אבי אביב שפרש בשנה לגמלאות	תוכנות לשחזור מידע משמשות להפקת ראיות מהארד דיסקים שנמחקו, פורמטו או נמגמו גאדג'טים לחיפוש מידע מתחברים ליציאת USB של המחשב ובעצמם מעתיקים ממנו קבצים	לכידת האנלייזר, 1998: מבצע שניהל בועז גוטמן, ושזיזר את הקמת המפלג שוד בנק הדואר, 2004: לכידת הנוכל דודי שטרנברג, שפירץ לחשבי בנק הדואר בחיפה ונגב כספים לכידת אמנה מונג, 2001: המשטרה סייעה לשב"כ לאתר את המחבלת שפיתחה את אופיר רחום להגיע לרמאללה, שם נרצח

סנ"צ אבי אביב