Digital Whisper
Technologic Papers

על אבטחת מידע, עבר, הווה ועתיד

מאת חץ בן חמו (hetz@hetz.biz)

הקדמה

בין קוראי המגזין Digital Whisper ישנם רבים שמבינים באבטחת מידע, יש המבינים ברמה של Overview ויש מומחים המבינים עד רמת ה-packet בתקשורת ועד ה-Buffer overflow באפליקציות ובקוד. במאמר זה אנסה להתייחס ברמה שדי כללית, אולם אנסה "לנגוע" קצת יותר לעומק (עם הסברים) היכן שניתן.

תחום אבטחת המידע עובר טלטלה בשנים האחרונות, ומנהלים רבים עדיין לא מבינים זאת. תחושת ה"יש לנו חומת אש יקרה ומעולה" אופפת אותם, בו בזמן שחומת אש, כמה שתהיה משוכללת **אינה רלוונטית** במקרי פריצה רבים.

בשנים האחרונות מעבר לרמת ה-Firewall הבסיסי שנתן לנו הגנה ברמה של חסימת/פתיחת פורטים בצורה זו או אחרת, נכנסו חומות אש מסוג שונה, הלו הם ה-WAF (ר"ת Web Application Firewall) שחלקם הוטמעו במוצרי Firewall כמו Checkpoint, Fortinet ואחרים, ואילו חברות אחרות בנו WAF שיושב "מאחורי" ה-Firewall של החברה וכל מטרתו היא לנתח את התעבורה ולמצוא נסיונות פירצה, החל מ-SQL Injection, נסיונות כניסה מרובים מכתובת IP אחת ועד נסיונות התקפת DDoS (כאן המקום להזכיר שעם כל הכבוד לכל פתרון שנקנה ספציפית נגד DDoS, הפתרון לא יספק מכיוון שהתקשורת אל האתר כבר תהיה פקוקה ויש לפתור זאת ברמת ה-ISP). פתרונות ה-WAF עושים את עבודתם בצורה לא רעה וחוסמים חלק ניכר מה"האקרים" שברובם הם מה שנקרא "Script Kiddies" (אגב, בניגוד למה שרבים חושבים, Script Kiddies אינם ילדים שכותבים סקריפטים, רובם פשוט מורידים סקריפטים מוכנים ומשתמשים בהם, ותעיד העובדה שבפורומים רבים שאותם סקריפטים ניתנים להורדה, ישנם הרבה תלונות של אותם Kiddies על כך שזה "לא עובד" - מה שמראה שאותו Kiddie אפילו לא יודע את שפת הסקריפט).

כל הדברים שציינתי אינם חדשים לא לקוראים ולא למנהלי אבטחה. הבעיות מתחילות ברמה מעבר, ברמה ששום Firewall **לא עוזר**. ברמה של פריצה למחשב בודד אחד.

תכירו את שוקי

לשם המאמר, נכיר את שוקי, אדם שנשכר כדי לפרוץ לארגונים ולדלות מידע. שוקי הוא דמות פיקטיבית שמומצאת לצורך מאמר זה, ואני אציין ברמה עקרונית כיצד שוקי פורץ ובהמשך המאמר אסביר מה מחלקת האבטחת מידע צריכה לעשות כדי להתגונן נגד שוקי. (אגב, אני אינני שוקי, ואינני פורץ, גם לא בתשלום או בחינם).

הלקוחות של שוקי הם בד"כ ארגונים שפונים דרך צד שלישי כדי להסתיר עקבות. נניח שחברת התוכנה (הפיקטיבית) Micro Code 2000 נמצאת בקשיים ואילו המתחרה שלה Server Code מציגה בדוח"ות הרבעוניים רווחים נאים ועליה של עשרות אחוזים במכירות מדי רבעון. ב-Micro Code ניסו הכל, החל בהעתקת המוצר של המתחרה, שיווק אגרסיבי, הנחות ענק לעוברים מהמוצר המתחרה ועוד, אולם בינתיים רווחים גדולים עדיין לא הגיעו ל-Micro Code ובהנהלה החליטו שהם מעוניינים במידע "מבפנים" מה קורה אצל המתחרים. הם ניסו לעבוד בשיטה הידועה של "חטיפת" עובדים בכירים מהמתחרים, אולם הנסיונות כשלו ואותם אלו שקיבלו פניה מ-Micro Code "לערוק" - סירבו בנימוס.

מישהו מההנהלה מחליט לפנות לבחור שהוא מכיר (נקרא לו יקי) כדי שימצא מישהו ש"יציץ" ויעביר מידע רגיש של המתחרים ל-Micro Code. סוג המידע? פרטים על לקוחות של Server Code, מחירים לא רשמיים, תוכניות עתידיות של החברה, אסטרטגיות שיווקיות. קוד מקור של Server Code אינו כל כך חשוב אבל אם גם זה יגיע לידי Micro Code הם לא יתלוננו על כך. יקי שומע, ומבקש סכום התחלתי כדי למצוא מישהו ולשלם לו. מתבצעת העברה כספית בצינורות אחוריים של כמה עשרות אלפי דולרים. יקי גוזר קופון שמן ופונה לשוקי עם ההוראות.

עתה נמנה אותך, קורא יקר, למנהל האבטחת מידע של Server Code. שוקי **הולך לפרוץ ולגנוב מידע ממך**. איך הוא הולך לעשות זאת? או, טוב ששאלת. ישנם מספר דרכים.

הדבר הראשון ששוקי יעשה הוא מחקר מקיף לגבי מי האנשים שנמצאים בחברה, מה תפקידם ומה כתובת המייל שלהם. לשם כך הוא ישתמש בגוגל, יוטיוב, לינקדין ואתרים אחרים - הכל על מנת לדלות את המידע ולבנות לעצמו מעין עץ של בעלי תפקיד ב-Server Code. לאחר שהוא בנה, הוא ישיג את כתובות המייל שלהם.

מכיוון ששוקי קיבל כמות כספים רצינית, הוא יכול לפנות לכל מיני אתרים ב"שוק שחור" (רבים חושבים שמדובר ב-Dark Web אבל במקרים רבים באתרי אבטחה רבים ניתן ליצור קשר פרטי ו"חברי" עם כל מיני פורצים כדי לרכוש מהם פריצות למוצרים שונים, כל עוד הפריצות לא דווחו ואינם מפורסמים בשום מקום. ביטקוין היא צורת התשלום הרצויה. מה לעשות, יש עדיין כאלו שחושבים שביטקוין הוא אנונימי) כדי לרכוש פירצה. הוא יוצא מתוך הנחה שבחברה מותקן אצל אותם מנהלים ה-Adobe Reader והוא יוצר

קובץ PDF מיוחד שמשתמש באותה פירצה לא ידועה כדי לשתול Loader קטנטן במחשבו של אותו מנהל. אותו Loader מהרגע שהוא יופעל (בכך שאותו מנהל יפתח את קובץ ה-PDF הנגוע) יטען כבר את החלקים האחרים של האפליקציה ששוקי כתב/גנב/השאיל/שינה כדי להקים מעין Shell קטנטן בתוך אותו מחשב.

מהרגע שאותו Shell רץ, לשוקי יש גישה למחשבו של אותו מנהל. מה עם ה-Firewall של החברה או כל משהו באמצע? הם **לא רלוונטיים** כי שוקי משתמש באותם הגדרות שאותו מנהל גולש (לדוגמא - אם יש Proxy באמצע, גם ה-Shell של שוקי ישאב מידע דרך הפרוקסי). שוקי מספיק חכם כדי למצוא מה הפורטים הפתוחים וכיצד הוא יכול לבנות Tunnel בינו לבין מחשבו של המנהל (סביר להניח שיהיה מעורב שרת באמצע שנמצא באמזון או אצל כל ספק שרותי VPS/ענן כלשהו כדי לטשטש עקבות).

מכיוון ששוקי פרץ למחשבו של המנהל, יש לו מיידית גישה לקבצים שיווקיים, כך שאסטרטגיות שיווקיות, מבצעים ומידע על מוצרים עתידיים זמין לו כבר עכשיו והוא יכול בשמחה להוריד אותם ולמסור אותם ליקי, אבל שוקי לא עוצר כאן, הוא רוצה להיות "מגובה" כך שאם המחשב שהוא פרץ אליו הוא Laptop שהמנהל לוקח הביתה ומנותק מה-LAN של החברה, שוקי יוכל לגשת גם ממחשב אחר בחברה. לשם כך הוא רוכש עוד פרצה שעדיין לא פורסמה ל-Windows והוא פורץ לעוד 3-4 מחשבים ומתקין גם שם את אותו Shell. שוקי עכשיו לא צריך לשבור את הראש על ה-Firewall הארגוני או כל כלי הגנה אחר שמגן על התנועה מבחוץ. **הוא כבר בפנים** וכל מה שהוא צריך לעשות הוא להעביר את המידע בצורה שלא תגרום לאחת ממערכות ה-IPS/IDS לחשוד. איך עושים זאת? די פשוט: שותלים Header ("ראשן") כאילו מדובר בקובץ וידאו קובץ של תמונה גדולה ובמשכו ה-DATA בצורה מוצפנת (ה-Shell יכול להצפין). מבחינת מערכות ה-IPS/IDS, המנהל שולח תמונות שהוא צילם או מעלה וידאו. הן **לא תתרענה** על בעיות.

שוקי לא עוצר כאן, שוקי **רוצה לראות קוד**, אבל איך הוא יוריד קוד? למנהלי שיווק והנהלה בכירה בד"כ אין שום נגיעה לקוד, בוודאי שלא ל-Source Repository כלשהו (Source Safe, SVN, GIT וכו'). אז מה הוא יעשה?

הוא יתחיל לסרוק את מחשבי החברה. הוא לא יעשה זאת בצורה גורפת (שוב, הוא לא מחפש "להעיר" את שרת ה-IPS/IDS), אלא לאט לאט. אם לדוגמא מוצר החברה רץ על לינוקס, הוא יחפש מכונות שיש להן Port-22 פתוח. המוצר מבוסס על Windows? הוא ינסה לפרוץ למכונות Windows אחרות תוך חיפוש קוד בהן ואם מנהל הרשת היה עצלן ולא הגדיר הרשאות מוגבלות למחלקות שונות, אז הוא בכלל "יחגוג" על ה-File Servers השונים ויוריד כמה שיותר.

וכאן נמצאת חולשה שקיימת **בחברות רבות** אך לא תמיד זוכה ליחס מצד אבטחת המידע (שוב, אשליית ה-Firewall "החזק" שמגן): במחלקות R&D רבות שמשתמשות לדוגמא בלינוקס, המפתחים מבטלים מנגנוני אבטחה כמו חומת אש פנימית (iptables) או מנגנוני אבטחה מבוסס Kernel (כדוגמת SELinux),

מה שאומר שכל מה ששוקי צריך לעשות זה לפרוץ למכונת Windows אחת שרץ עליה Putty עם מפתחות או SecureCRT, להעתיק את הפרופיל **ובמכה אחת יש לו גישה להרבה מכונות לינוקס בלי לשבור את הראש על סיסמא**. לפעמים הוא כלל לא יצטרך זאת אם המשתמש שומר קבצי מקור בכונן C מקומי ואז לשוקי יש בכלל חיים קלים.

זו היתה השיטה הראשונה. נעבור לאופציה אחרת ששוקי לא מצליח לפרוץ למחשב דרך שליחת קובץ PDF נגוע (מה לעשות, המנהל שהוא שלח אליו את המייל כבר לא נמצא ב-Server Code או שאשכרה מישהו עושה צעדי מנע כדי לתקוף את הבעיה של חולשות בקבצי PDF). איך שוקי יצליח לחדור?

כאן אנחנו מגיעים ל"מימד האנושי". שוקי יתחיל לחפש עבודות באותה חברה. לא משנה מה העובדה, העיקר שהוא יוזמן לראיון עבודה. לא, בזמן הראיון הוא לא יגע במחשב. כל מה שהוא עושה הוא שולח קורות חיים (מפוברקים כמובן) למנהלת כח האדם בחברה (לא קובץ נגוע).

סביר להניח ששוקי יזומן לראיון. הוא יגיע לחברה, ישב וישוחח עם החברה ובמהלך השיחה הוא יזכיר בהתלהבות אתר חדש שהוא "שמע" עליו. אתר מ-ה-מ-ם שהיא ח-י-י-ב-ת לראות אותו! מנהלת כח האדם סקרנית והיא פותחת דפדפן. שוקי מכתיב לה את שם הדומיין ואכן יש אתר. מהמם? שאלה טובה, אבל אם נסתכל על שוקי, נראה שהוא מחייך. מדוע שוקי מחייך?

כי את אותו אתר "מהמם" בנה שוקי. כשמנהלת כח האדם נכנסה אליו, היא נכנסה לאתר שסורק בעצם את הדפדפן ומנסה עליו פריצות שונות, הכל לפי הידע והפריצות ששוקי קנה. השרת של שוקי לא מצליח לפרוץ? אז הוא יתן למנהלת כח האדם הודעה שנגן ה-Flash שלה ישן ויש להתקין את הקובץ הבא. מה לכל הרוחות מבינה מנהלת כח אדם בגרסאות Flash? כלום, אבל שוקי כבר יעודד אותה להוריד ולהריץ. תודות לתמימותה של המנהלת, לשוקי יש עכשיו גישה מרחוק.

הדבר הראשון ששוקי יעשה לאחר שיגיע לביתו ויתחבר מרחוק (דרך אותה אפליקציה שהמנהלת התקינה) הוא לשאוב את ה-Contact List כדי שידע בדיוק למי לגשת. אם הוא רוצה לפרוץ לשאר המחשבים, הוא יכול לשלוח דרך כתובת המייל שלה **בשימוש בשרת הפנימי** אימייל עם אותו פריצת PDF שאינה ידועה עדיין ובכך להשיג השתלטות על מחשבים אחרים וכך הוא יוכל לגנוב מידע וקוד.

נעזוב עתה את שוקי ונחזור למציאות שלנו. אומר לכם משהו פשוט: **רוב החברות עדיין לא יודעות להתמודד מול שוקי**. אנשי אבטחת מידע רבים, לצערי, מנסים לחשוב על אבטחת מידע באופן סיסטמתי בשעה שמחשבה נכונה על אבטחת מידע צריכה להיות **הכל חוץ מסיסטמתי**. שוקי נשכר לפרוץ אליכם והוא מעוניין להרוויח כסף, לא להחזיר אותו. Micro Code תשכור דרך יקי מישהו אחר אם שוקי לא יצליח כי הם רוצים בכל דרך לעקוף את Server Code.

עניין ה-R&D שהזכרתי לעיל, לדוגמא, הוא עניין שאישית ראיתי בחברות קטנות וגדולות כאחד. מפתחים רוצים לנסות משהו ומעיפים כל הגנה בסיסית. קבצים נכתבים עם מקסימום הרשאות (כי ה-Apache לא נותן כתיבה אז פותחים הכל ל-777!), אין הפרדת משתמשים והסיסמאות הן מגוכחות בפשטותן ואינן מוחלפות. עדכוני אבטחה שאמנם מיושמים על שרתי פרודקשן **במקרים רבים כלל לא מיושמים** על מכונות D&R וכך לאותו שוקי תהיה עבודה מאוד קלה בשאיבת הקוד ואם הוא ירצה - בגרימת נזק.

איך מתגוננים? נתחיל בעניין חולשות ה-PDF וחולשות קבצים אחרים. רובם בד"כ מגיעים דרך האימייל.

אז מה ניתן לעשות?

איך מטפלים בכך? אם לדוגמא יש לכם שרת Exchange אז כדאי שתשתמשו במוצר כזה או כזה שמתחבר ל-Exchange ושומר את ה-Attachments בתיקיה נפרדת כך שהמייל מגיע למשתמש ללא ה-Attachment, רק HTML של המייל.

כאן אני ממליץ להרים שרת לינוקס פשוט ולהתקין עליו ImageMagick ולבצע "חיבור" בין אותה תיקיית Attachment לבין הלינוקס, ובעזרת סקריפט פשוט להריץ Convert **לכל קובץ** שמגיע והוא ברמת סיכון שהוא כולל פירצה. כך לדוגמא קובץ PDF אפשר לבצע לו convert ל-PNG או לבצע המרה לאותו פורמט ומכיוון שהלינוקס יוצר את הקובץ, הוא אינו כולל קוד זדוני (קבצי אופיס ניתן להמיר עם ooo-thumbnail של Open Office או Libre Office), ולאכסן את הקובץ שנוצר במקום הקובץ המקור. את הקובץ המקורי נעביר לתיקיה אחרת כך שאם המשתמש ירצה, הוא יוכל בעזרת קישור במערכת להגיע אליו. בעזרת מערכת פשוטה כזו גם אם שוקי ישלח קובץ PDF (או קובץ וורד/אקסל/פאואר-פוינט) נגוע, המשתמש יראה במייל טקסט כלשהו כתמונת PNG או כקובץ PDF רגיל. אם שוקי שלח שטויות ב-PDF, אז אותו מנהל יגחך ויזרוק את המייל, לא בוצעה חדירה. את הקבצים המקוריים ניתן יהיה להשמיד לאחר מספר ימים או לפי הנוהלים של החברה. מבחינת אחסון ושרת, אין צורך במשהו עוצמתי, תספיק מכונת לינוקס פשוטה ו-RAID של מספר דיסקים גדולים עם חיבור SATA הואיל ואין צורך כאן בכתיבה/קריאה מהירה.

מבחינת הורדת קבצים ע"י המשתמשים, כדאי לארגן את התצורה כך שהם ירדו לתיקיית רשת עם עדיפות שיראו ב-Viewer פנימי. לכרום ופיירפוקס ישנו Viewer של PDF כך שהם אינם צריכים את התוסף של אדובי מותקן בדפדפן (אפשר, שוב, לחבר את אותו שרת לינוקס לעיל כדי שימיר אוטומטית קבצים שיורדים בפורמטים פופולריים לתמונות או שיצור אותם מחדש - ויתן למשתמש את הגירסה המומרת ורק אם צריך - את קבצי המקור). קבצי EXE או כל קובץ שהוא מסוג Executable שיורדו ע"י משתמש יעברו אישור של אבטחת מידע או כל גורם מוסמך אחר בחברה.

בשיטות אלו אנו מונעים משוקי גישה. השיטה היא כמובן אינה Bullet Proof (שוקי עדיין יכול לקבוע פגישה ולתת Disk On Key לאחד המנהלים ולהדביק את מחשבו של המנהל לדוגמא), אבל היא חוסכת למנהלי המערכת הרבה כאב ראש.

ועכשיו אשאל אותך קורא יקר שאלה: כיצד הינך יודע ששוקי (או דומים לשוקי) לא קיימים אצלך במערכת? כל מנגנוני האנטי וירוס למינהם עובדים בתצורה של חתימות או זיהוי סוגים שונים של תולעים ונוזקות אחרות, אך הם אינם יודעים להתמודד עם פריצות שלא פורסמו, שבוודאי עדיין לא ננעלו ע"י יצרן התוכנה.

הטריק שאני משתמש הוא טריק פשוט: קח סופ"ש או חג וקבע אותו כיום שהמשתמשים **לא מכבים** את המחשבים שלהם. הם עושים Logout וזהו ואם אפשר, אנשים שמשתמשים במחשבים ניידים, שישאירו אותם בחברה במצב **פעיל**. למשך החג או לילה או סופ"ש שמור את הטראפיק שיוצא ונכנס (או לפחות את הלוגים שלו) וכשתחזרו לעבודה, עברו על הלוגים, תראו מי נכנס ומי יצא ובמיוחד מאלו מחשבים/שרתים. חלק מהתעבורה הוא "כשר" (כמו עדכונים שיורדים) אולם יכול להיות שחלק מהתעבורה מגיע למקומות שאתה לא בטוח שהם "כשרים". לכתובות האלו תבצע בדיקת PTR (כדי להמיר כתובת IP לכתובת DNS שמית) ואז יהיה יותר קל לבדוק זאת. פורצים רבים מנצלים את סופ"ש/חג/לילה כדי לבצע העברות, וכך תוכל לדעת אם יש דברים לחקור.

והנה נקודה שאני חוזר ואומר שוב ושוב: מצאת טראפיק חשוד? **אל תתקוף את הפורץ בחזרה**. לפעמים אותו שוקי נעקב בעצמו ע"י גורמי בטחון שונים מהארץ ו/או מחו"ל ותקיפה שלך רק תדפוק עבודות מעקב שונות. אם אתם ארגון גדול, פנה למחלקת הבטחון ושהם יפנו למז"פ/עבירות מחשב במשטרה. אם אתם ארגון קטן, פנו ישירות למשטרה. חשוב שתשמור כל לוג או כל טראפיק שיש לך ואם אתה יודע מהו המחשב הנגוע, שמור את הטראפיק ממנו/אליו. אני יודע שרבים צוחקים על מחלקת פשעי המחשב של המשטרה (ללא הצדקה, אגב, המצב שהיה בעבר הרחוק השתנה לגמרי כיום, ואני מדבר ספציפית על המחלקה הזו ולא על פדיחות שנעשים ע"י מחלקות אחרות בתביעות של פורצים) אבל בכל זאת - לכו by the book.

העתיד בכל הקשור לפריצות אינו מביא בשורות טובות. אדרבא, הוא מביא כאב ראש לא קטן למחלקות הסיסטם ואבטחת המידע יחד. בסוף מאי eBay, חברה שיש לה נסיון גדול מאוד באבטחת מידע - הודיעה שפרצו לבסיסי הנתונים שלה. אמנם הפורץ לא הצליח להשיג את המפתחות לפתיחת ההצפנה וקיבל ג'יבריש בתור dump, אבל עדיין - פורצים מצליחים להגיע למקומות רבים באותם שיטות ששוקי לעיל השתמש.

"הדור הבא" של פריצות, לדעתי, יהיה יותר מוטה חומרה. כיום ישנן מערכות לינוקס משובצות בגודל של קופסת סיגריות (כולל סוללה) עם חיבורי RJ45 פנימה והחוצה, כך שניתן לחבר אותן מתחת לשולחן לכניסת הרשת של PC, אותו ציוד יתחזה מבחינת MAC Address כ-PC (כך שלא תוכלו לדעת דרך ה-Switch בדיוק מה קורה אלא אם תבצעו Sniffing) כך שהפריצה מרחוק תהיה יותר קלה לפורצים. כל מה שצריך זה לתפוס עמדת מידע כלשהי שמחוברת ל-LAN, להתקין את הקופסא ולחבר לחשמל (ולהטעיה יש כאלו שאפילו ישימו מדבקה עם לוגו של החברה הנפרצת על מנת להטעות עובדים שאינם מבינים בנושא). חושבים ש-Offline מוגנים? תחשבו שוב: ישנן קופסאות לינוקס (עדיין לא יצאו רשמית, אגב) שלא רק מציעות 2 חיבורי רשת אלא גם חיבור WIFI בתדר 2.4 או 5 ג'יגהרץ, השידור יקלט ע"י מודם סלולרי שמוחבא מחוץ לדלת החברה (ה-SSID חבוי והתקשורת מוצפנת) והמודם הסלולרי מחובר ל-G3 כך שכל מה שהפורץ צריך לעשות זה להתחבר למודם הסלולרי שמתחבר לקופסא - ומשם לעשות כרצונו.

מי המטרה של פריצות עתידיות כאלו? כל חברה גדולה שיש לה מתחרים מאוד שאפתניים **וגם חברות ביטוח ובנקים**. המחיר של הציוד זול, זול מאוד אפילו: קופסא כזו יחד עם מודם סלולרי לא יעלו יותר מאלפי שקלים בודדים והפיתוי לפורצים הוא גדול, מה שיצריך מחשבה מחדש מבחינת מחלקות אבטחת מידע כיצד ניתן להגן על התשתית והמידע, ואם מישהו חושב שהוא מוכן, שיזכר בבקשה מתי הוא עבר על שקעי ה-RJ45 וראה מה מחובר למה ומתי הוא עשה סריקה של תדרים 2.4 ו-5 ג'יגהרץ לאחרונה.

לסיכום

עולם ה-Cyber Crack **רק גודל**. זה מגיע אלינו מאוחר, אבל הגיע. שום ארגון שהכניס לתוכו כל מיני "קופסאות פלא" **אינו מוגן** כפי שהוא חושב, ועם מזעור חומרות פריצה ומערכות משובצות, גילוי הפרצות יהיה יותר מורכב ויצריך מחשבה מחוץ לקופסא. לא חסרים גורמים שירצו את המידע שיש ברשותכם, החל ממתחרים מקומיים ועד חברות ענק בינלאומיות וכלה במדינות שבהן ה"ספורט הלאומי" הוא פריצות כדי להשיג מידע (סין, NSA בארה"ב וכו'), ואם אתם רוצים להגן, תחשבו בצורה יצירתית.

על המחבר

שמי חץ בן חמו, אני פרילאנסר ואני עוסק בתחומי לינוקס, וירטואליזציה ואבטחת מידע. ניתן ליצור איתי קשר במייל hetz@hetz.biz ובטלפון: 054-5297156. בנוסף, אני כותב בבלוג "כמה מילים, ברשותכם".