אל : בית משפט השלום בראשל"צ **1/5/18**

דוח סודי פרשיית "מכפלת אשראי" - הארכת מעצר שנייה

החשוד:

1. חלמי גית ת"ז 946945300 יליד 1985, תושב חברון (רש"פ).

פרטי החשדות:

1. מתן אמצעים לביצוע פשע ס' 498 לחוק העונשין תשל"ז-1977.
2. קבלת דבר במרמה ס' 415(1) לחוק העונשין תשל"ז-1977.
3. קשירת קשר לעשות פשע ס' 499(א)(1) לחוק העונשין תשל"ז-1977.
4. הונאה בכרטיס חיוב ס' 17 בחוק כרטיסי חיוב 1986.
5. כתיבת תוכנה שתוצאתה מידע כוזב ס' 3(א)(2) לחוק המחשבים תשנ"ה 1995

רקע:

ביחידת הסייבר להב 433 מתנהלת פרשיה בשיתוף עם מספר מדינות נוספות בעולם אודות אתר ברשת האינטרנט שעיקר עיסוקו בהונאות כרטיסי אשראי מסוגים שונים, לרבות, הפצת פרטי כרטיסי אשראי, מכירת פרטי כרטיס או רשימות פרטי אשראי, מכירת פרטי פסים מגנטיים לטובת זיוף כרטיסים, הונאות גולשים ושלל עברות סייבר נלוות. **מדובר באחד האתרים המשמעותיים והגדולים ביותר ברשת באינטרנט בשפה האנגלית בתחום הונאות כרטיסי אשראי שגורמות נזקים לחברות אשראי במדינות רבות בעולם. באתר רשומים כיום מעל ל- 1,300,000 חברים מהארץ ומחו"ל. כתובת האתר המדובר היא www.altenen.com שבעבר נוהל תחת השם www.alboraaq.com (כיום סגור ומפנה לאתר הנוכחי altenen). מי שהקים ומנהל את האתר הוא חשוד 1 תושב חברון. מעבר לעברות המבוצעות על ידי חשוד 1 והחברים בפורום, נמצאו לא אחת טענות של גולשים כלפי חשוד 1 בעצמו על כך שרימה והונה אותם.**

במהלך שנת 2016 התפרסמה כתבה ברשת האינטרנט באתר בשם "פוסטה" אודות אתר Altenen.com והעומד בראשה חשוד 1. הכתבה התפרסמה לאחר שאדם בשם עדן חן (מבעלי חברת פרוגינטר) "נעקץ" ע"י חשוד 1 והמטרה שלו הייתה לפרסם את פרטיו של בעל האתר (חשוד 1) ואת המניעים שלו בניהול האתר וזאת כדי

להזהיר גולשים אחרים לבל "יעקצו" ע"י חשוד 1. **<u>עדן טען כי הסיר את הכתבה מהאתר "פוסטה" כי הוא ושותפו פחדו שחשוד 1 יאתר אותם ויהרוג אותם בגלל הכתבה</u>**.

במהלך חודש ינואר 2017 התפרסם מאמר מחקרי בנוגע לאתרים העוסקים בהונאות בכרטיסי אשראי ברשת האינטרנט ואתר Altenen, היה בין אחד האתרים המפורסמים ביותר.

במהלך שנת 2014-2015 התנהלה במחלק הנוער של ימ"ר ת"א פרשיה גדולה בשם "רכישה אנונימית". במסגרת הפרשיה התקבלה תלונה מקב"ט חברת לאומי קארד על רכישות של פיצות מ-"פיצה דומינוס" בהיקף של 80,000 ₪. **נחקרו כ- 40 חשודים רובם קטינים כאשר 25 מהם הודו שעשו שימוש בפרטי כרטיסי אשראי גנובים שהגיעו אליהם מפורום Alboraq.com (האתר שקדם ל-Altenen.com) . אחד מהחשודים מסר שדיבר עם חשוד 1. חשוד 1 אמר לו שהוא בן 23 או 30 ומתגורר בחברון ושלא נותנים לו להיכנס לארץ. לציין כי לחשוד 1 אין היתר להיכנס לשטח מדינת ישראל כי הוא מנוע שב"כ מתאריך 29.11.2009 עד לתאריך 30.1.2103 (ראה מזכר של שושן מתאריך 28.2.18).**

<u>ידיעות מודיעיניות</u>

1. מידיעות מודיעיניות בשנים האחרונות עולה כי אתר Alboraq ואתר Altenen משמשים להעברה ומכירה של כרטיסי אשראי ישראלים וכרטיסי אשראי מחו"ל וחשוד 1 הינו פלסטיני אשר מנהל ובעלים של אתרים אילו . חשוד 1 הוא בעל מספר כינויים שעימם הוא עושה שימוש ברשת האינטרנט. הנ"ל משתמש במספר תיבות מייל של yahoo, Hotmail, gmail.
2. בתאריך 26.3.18 התקבלה ידיעה (326-0165-18) כי **חשוד 1 עוסק בעבירות מחשב, פריצות לאתרים וגניבת כסף. את הכסף מעביר לחשבונות של חלפנים תושבי חברון ומקבל מהם כסף במזומן בתמורה. ברשותו מספרי טל"ס ישראלים והוא מחליף סימים מעת לעת בכדי לא להשאיר עקבות שיובילו להפללתו..... בערך אחת לחודש חשוד 1 יוצא לישראל ללא היתר עם מסמכים מזוייפים. חשוד 1 מחזיק ברשותו רובה M16.** בנוסף, בתאריך 26.3.18 התקבלה ידיעה (329-0183-18) כי **חשוד 1 מסתובב עם דיסק און קי על גופו באופן קבוע ויתכן ומצוי עליו מידע או שמשמש אותו לאינטרנט. כמו כן, בזמן עבודתו של חשוד 1 בחדר העבודה הוא מוציא סוללה מהטלפון הנייד שלו.**

<u>פעולות החקירה שהתבצעו בשלב החקירה הסמויה:</u>

1. צילום מסך מתאריך 2.9.15 מאתר בשם http://www.sharwat.con (אתר ברשות הפלשתינאית למכירה של מוצרים, נדלן ומכוניות) בו משתמש בעל כתובת מייל **helmegith@gmail.com**ומספר טלפון **059-8481404 מחברון** מפרסם מודעה למכירת רכב מסוג קאיה.

2. בקבלת המענה לצו המצאת מסמכים לפייסבוק אודות פרופיל הפייסבוק HLBoRaaQ.Hackers התקבל מענה כי החשבון נפתח בתאריך 9/9/2010. **בעל החשבון הוא חשוד 1. טלפון המקושר לחשבון הוא: 059-8481404 (טלפון בבעלות חשוד 1).** הכניסות לחשבון התבצעו **מכתובות IP מהרשות הפלשתינאית.**

3. דוח פעולה של השוטר יונתן בר לב מתאריך 20.9.15 אשר **פרסם הודעה באתר altenen.com שהוא מחפש אחר פרטי כרטיסי אשראי ו/או מאגרי מידע הקשורים לישראל למטרות שיווק. זמן קצר לאחר מכן פנה אליו משתמש בפורום בשם "CAL LOON" אשר הציע לו מאגר של 100 כרטיסי אשראי ישראלי בסכם של 16 דולר לכל כרטיס.**

4. בדוח של השוטר ג'רמי מקובסקי מתאריך 9.3.17 **אותר משתמש בשם Helmi בפורום Grandtheftarma. בפרטי המשתמש כפי שמילא אותם בעצמו, מכריז חשוד 1 שעיסוקיו הם משחקים וקארדינג ושהוא חלק מקבוצת שחקנים הנקראת ATN Team , בנוסף הוא מוסר שכינויו במשחק הוא T3es. בנוסף, בקבוצת המשחק הוא מצהיר שהוא המוביל של החבורה ששמה altenen.**

5. דוח מתאריך 19.4.17 של השוטרת לימור נבו בנוגע **לביסוס הקשר בין חשוד 1 לאתר altenen.com ולאתר alboraaq.com:**

- **חשוד 1 מופיע כאיש הקשר לאתר altenen.com . בנוסף, המייל שלו webmaster@altenen.com מעיד על תפקידו כמנהל האתר** (מסמך 1).
- **באתר altenen.com נכתב שאם אדם רוצה לפרסם בפורום עליו ליצור קשר עם מייל helmigith@gmail.com . בנוסף, רשום באתר כי האדמין (חשוד 1) משתמש בכינוי T3es** (מסמך 2א+2ב).
- **בתאריך 22.12.2015 פרסם גולש בבלוג כי רימו אותו באתר altenen.com ויש להיזהר מהאדמין של האתר שהפרטים שלו הם: Helmi Gheith והשם משתמש שלו T3es והכתובת שלו בחברון ברחוב בילאל** (מסמך 3).
- באתר http://otx.alienvault.com **חשוד 1 מופיע כאיש הקשר לדומיין alboraaq.com** (מסמך 4).
- באתר centralops.net **חשוד 1 מופיע בתור האדמין של אתר alboraaq.com** (מסמך 5).

- בחיפוש ברשת האינטרנט אותרו תלונות רבות של גולשים ש"נעקצו" בסכומי כסף גבוהים ע"י חשוד 1 (מסמך 6).
- **משתמש T3eS (חשוד 1)** העלה מספר סרטונים ל youtube , אחד מהסרטונים הוא תחת הכותרת **Hacked Bank by T3eS** (מסמך 7).
- באתר בשם ahrefs.com שתפקידו לנתח אתרים, **הועלה לינק לדומיין altenen.com. בדיקה באתר הובילה למסך Altenen-Card the world בו נרשם כי בהרשמה לאתר ניתן להפוך לחבר מלא ב-ATN ונרשם כי ה-Head Admin הינו (חשוד 1) T3eS** (מסמך 8 ומסמך 9).

6. דוח של השוטר ג'רמי מקובסקי מתאריך 24.4.17- חיפוש ברשת האינטרנט מידע אודות Helemi Gaith (חשוד 1) והכינוי T3es:

- אותר עמוד פייסבוק בשם alburaqbuilding – עסק של חשוד 1. בעמוד הפייסבוק ניתן לראות פרטים אודות החברה ואת כתובת המייל של חשוד 1 **helmegith@gmail.com.**
- **אותר ברשת האינטרנט פרסום לגבי פריצה והשחתת אתרים אשר ביצע T3es** (חשוד 1). **<u>חשוד 1 פרסם כי הוא האקר פלסטיני המשתמש בכינוי T3es אשר ביצע פריצה והשחתה של כמה אתרי אינטרנט וכתב בדף הראשי של כל אתר שפרץ " HACKED Owned BY T3ES".</u>** בנוסף, **קשר חשוד 1 את המייל שלו שהינו t3ys@hotmail.com.**

7. דוח של השוטר ג'רמי מקובסקי מתאריך 16.5.17 – בדיקה אודות דף הפייסבוק ואתר העסק של חשוד 1. תרגום הכותרת מערבית של דף הפייסבוק הינה Al Buraq for construction. האתר כתוב בערבית ומסביר על עסק הבניה של חשוד 1. מבדיקה של הדומיין עולה כי האתר רשום על שם חשוד 1 ומופיעים בו פרטים הקושרים את חשוד 1 לאתר כדון: שמו הפרטי, כתובתו בחברון, מספר הטלפון שלו וכתובת המייל שלו helmegith@gmail.com.

8. בקבלת המענה לצו המצאת מסמכים למייקרוסופט בנוגע לכתובת המייל helmegith@gmail.com נכתב כי מכיוון שהתיבה ופעילותה היא מחוץ לתחום השיפוט של ישראל, בעיקר בתחום ירדן והסביבה, החברה לא מספקת את הנתונים המבוקשים.

9. בקבלת מענה לצו בימ"ש 17159-06-17 ע"ש משתמש סקייפ ABH-T3eS, עלה כי **דוא"ל מקושר הוא: helmegith@gmail.com. בוצעו שיחות מהמספר 059-8481404 המקושר לחשוד 1.**

10. בקבלת המענה לצו המצאת מסמכים למייקרוסופט בנוגע לכתובת המייל t3ys@hotmail.com עלה כי החשבון נפתח בתאריך 2.5.2008 , **שם החשבון הרשום הוא: T3es, החשבון נפתח מכתובת IP פלסטינאית.**

11. דוח פעולה של השוטר אריה אחישר מתאריך 25.6.17, בכניסה לאתר בכתובת http://uniqueway.net/mnf/altenen.com אותר חשוד 1 כאיש הקשר לאתר.

12. זכ"ד של השוטר מתאריך 31.7.17 בנוגע למידע אודות פוסטים של משתמשים ישראלים ומשתמשים מחו"ל שהורדו מאתר Altenen וכמות של **947,710 מספרי כרטיסי אשראי שהועתקו מאתר Altenen.**

13. דוח של השוטר יצחק ברומי מתאריך 16.10.17- קבלת 6 קבצים **המכילים 947,710 מספרי כרטיסי אשראי שהורדו מאתר Altenen**, מתוכם 3013 כרטיסי אשראי ישראלים.

14. דוח של אביטל גיגי מתאריך 12.2.18 בו בוצע סינון ל-947,710 מספרי כרטיסי אשראי **ולאחר סינון של כפילויות התקבלו 835,397 כרטיסי אשראי.**

15. דוח מתאריך 6.2.18 של השוטר יצחק ברומי שביצע סינון ל- 3013 כרטיסי אשראי ישראלים וקיבל **לאחר סינון כפילויות 2584 מספרי כרטיסי אשראי ישראלים**.

16. **סודי ביותר---** דוח של מעיין שרעבי ואורטל סלמן מתאריך 18.2.18- **יחידת הסייבר בנתה אתר דמה של חברת השקעות ומלכודת IP. מלכודת ה-IP הושתלה כפיקסל במסמך וורד. האתר הועלה בתאריך 7.2.18. בתאריך 16.2.18 בבוקר נשלח לחשוד 1 מייל עם כלי מלכודת ה-IP וקישור האתר. באותו היום (16.2.18) נכנס חשוד 1 למייל וכתובת ה-IP שלו נחשפה (217.21.6.174). מבדיקת כתובת ה- IP עולה כי מדובר ISP פלסטינאי. בדוח המשך מתאריך 14.3.18 בו בצעו בדיקות עלה כי פרטי רישום לדומיין של אתר Altenen מוסתרים באמצעות שירות proxy והדומיין מאוחסן בהולנד ע"י חברה בריטית. בכניסה אתר Altenen ניתן לצפות בשמות משתמש כולל Administrators ובעמוד ה-Administrators מופיע משתמש אחד תחת הכינוי t3es. תחת קטגוריית "Core Members" באתר Altenen נמצא משתמש אחד בעל הכינוי "prince" (עם תווים מיוחדים). בחיפוש בגוגל נמצאו קישורים לאתרים שונים המדווחים על משתמש זה כספאם והמקשרים אותו אל שם המשתמש t3es.**

17. דוח פעולה של השוטר יניב חסון מתאריך 27.2.18- **קישור ארנק הביטקויין המפורסם באתר Altenen.com לחשוד1:**

- **המשתמש המכונה בפורום T3eS המשמש באתר זה כ-Admin (חשוד 1) , הוא הכתובת לשדרוג מעמד המנויים באתר, ממעמד מנוי חינמי רגיל למעמד משתמש VIP, וכל זאת לאחר תשלום ושליחת הודעה פרטית (Private Message.**

- התשלום עבור שדרוג מעמד המנוי, ל-VIP, יתבצע ע״י העברת Bitcoin לארנק שכתובתו 1FHJpzzPs6Tcqb1PuyFUicSqdYu3gikCmB.
- **כתובת הדוא״ל Helmegith@gmail.com (נפתחה ומשויכת לחשוד 1) הינה הכתובת לפנייה עבור כל משתמש בפורום אם רצונו לשכור שטח פרסום תמורת תשלום חודשי קבוע ולברורים נוספים בנושא.**
- ישנה הודעת אזהרה באתר Altenen כי יש להיזהר מפני זייפנים ו/או מתחזים למנהלי הפורום ושאין לעשות איתם שום עסקה ו/או לשלם להם עבור כל שירות, הכתובת היחידה ליצירת קשר הינה המשתמש T3eS, ע״י שליחת הודעה פרטית.

18. דוח פעולה של השוטר יניב חסון מתאריך 27.2.18- **שירותים בתשלום באתר Altenen:**

- באתר ישנם מס׳ שירותים שאותם ניתן לקבל תמורת תשלום, התשלום יתבצע אך ורק ע״י מטבע וירטואלי מסוג Bitcoin את כמות ה- Bitcoin נדרש להעביר לכתובת ארנק FHJpzzPs6Tcqb1PuyFUicSqdYu3gikCmB1 שמפורסמת באתר.
- מבדיקה באתר Blockchain.com עבור כתובת הארנק עולים הנתונים הבאים: מס׳ הטרנזקציות שבוצעו בארנק הם 2348, הסכום הכולל שהתקבל בארנק זה במטבע הוא 1,068.12441894BTC, הפעולה האחרונה שבוצעה בארנק היא קבלת BTC בתאריך 26/2/2018.
- על פי הנתונים המוצגים באתר Altenen, כמות המשתמשים הרשומים בו נכון לתאריך 27.2.18 הוא 1,352,258 כמות זו כוללת את כל סוגי המשתמשים: חינמיים, VIP . ולא ניתן לדעת כמה מהם משתמשי VIP וכמה מהם חינמיים.
- באתר Altenen ניתן לקבל שירותים בתשלום כגון: שדרוג משתמש חינמי למשתמש VIP. שדרוג המשתמש מקנה גישה לכל מדריכי VIP, התאמה אישית של האתר מבחינת צבעים והרשאות וגישה לכל הפורומים באתר. המחיר 30$ לחודש או 200$ לכל החיים. בנוסף, ניתן לקנות שטח פרסום בראש האתר בעלות של 500$ עד 4000$ תלוי בזמן ובגודל שטח הפרסום. בנוסף, באתר מפורסם כי נתן לרכוש Accounts and

Database Dumps ב-200$ לשבוע או ב-750$ לחודש, Verified Carders ב-300$ לשבוע או ב-500$ לחודש וניתן לשלוח הודעת דוא"ל לכלל משתמשי הפורום בעלות חד פעמית של 10,000$ או שליחת הודעה פרטית בממשק ההודעות בפורום לכלל המשתמשים בעלות חד פעמית של 5,000$.

19. דוח של השוטר שושן בנימין מתאריך 28.2.18-שיחה עם מש"ק מת"ק חברון בנוגע לחשוד 1. הנ"ל מסר כי **לחשוד 1 אין היתר להיכנס לשטח מדינת ישראל כי הוא מנוע שב"כ מתאריך 29.11.2009 עד לתאריך 30.1.2103.בנוסף, חשוד 1 מנוע משטרה ועל סמך שתי המניעות הללו המנהל האזרחי בחברון לא יכול לספק לו אישור כניסה לארץ.** חשוד 1 יוצא ממעבר אלנבי והיציאה האחרונה הייתה בתאריך 3.1.18 וחזרה בתאריך 4.1.18.

20. **בתאריך 7.3.18 הועברו לחברות האשראי 12 מספרי כרטיסי אשראי ישראלים נוספים שפורסמו באתר Altenen ע"י שני משתמשים ישראלים. במענה שהתקבל מחברות האשראי עלה כי רוב כרטיסי האשראי נחסמו ע"י חברות האשראי ביום בו הם פורסמו באתר Altene** (ראה שני דוחות של השוטר ליאור רוטנברג מתאריך 11.3.18).

21. דוח פעולה של השוטר יניב חסון מתאריך 11.3.18 בנוגע להיקף השימוש והפרסום של כרטיסי אשראי של 11 חשודים ישראלים החברים בפורום השייך לאתר Altenen.com.

22. דוח של השוטר ליאור רוטנברג מתאריך 11.3.18. **אבירם מלאומי כארד ביצע סינון ל-2584 מספרי כרטיסי אשראי ישראלים שהוא קיבל מיחידת הסייבר ולאחר הסינון 669 כרטיסי אשראי שייכים לחברת ישראכרט, 488 כרטיסי אשראי שייכים לחברת לאומי כארד, 939 כרטיסי אשראי שייכים לחברת ויזה כאל ו-79 כרטיסי אשראי זרים. <u>ממענה של חברות האשראי עולה כי ברוב מספרי כרטיסי האשראי ביצעו הונאות אשר הוכחשו ע"י בעלי הכרטיס. בנוסף, רוב הכרטיסים נחסמו באותו היום או מספר ימים לאחר שהם פורסמו באתר Altenen.com</u>.**

23. דוח של השוטר ברומי יצחק מתאריך 12.3.18 בנוגע לבדיקת משתמשים באתר Altenen- אותרו מספר משתמשים ישראלים אשר פרסמו מספרי כרטיסי אשראי ופרסמו פוסטים בנוגע לרכישות במספרי כרטיסי אשראי בשנים 2016-2018.

24. דוח של השוטר יניב חסון מתאריך 18.3.18- איתור נתונים המבססים שליטה וניהול ע"י המשתמש T3eS:

- לאחר הרשמה לאתר Altenen בכניסה לפרופיל המשתמש הבחין החוקר בדירוג המשתמש שקיבל, Starter, דהיינו משתמש מתחיל, מבדיקה שערך לא ניתן לשנות את מעמד המשתמש אלא רק מנהל הפורום. בעת הרישום לאתר התקבל מספר יחודי ID (1392150) מס' המראה את כמות המשתמשים שנרשמו לפורום עד לאותו רגע. **בעת הכניסה לפרופיל המשתמש בכינוי T3eS הבחין החוקר כי המספר ID של משתמש T3es הינו 1, דהיינו משתמש T3eS הינו המשתמש הראשון שנוצר בפורום ובDataBase- המשתמשים של הפורום.**
- **מכניסה לתיבת ההודעות של המשתמש T3eS עלו הממצאים הבאים: המשתמש T3eS הוא בדרגת Administrator, המשתמש T3eS קיבל 131 הודעות מכלל חברי הפורום, בדף הפרופיל של האדמין T3eS ביקרו 18,746 משתמשים.**
- להלן מקבץ הודעות ששלחו משתמשים באתר Altenen את משתמש T3eS:

1. המשתמש kosova מבקש לחדש את פעילות השם משתמש הקודם שלו, בשם At0m, ועוד מסביר כי ניסה לשכנע ע"י כך שהוא זוכר את הסיסמא האחרונה שלו ואת התשובות לשאולות המופיעות במנגנון שיחזור סיסמא. ע"פ בקשה זו ניתן להבין כי המשתמש At0m יודע כי יש ביכולתו של חשוד 1 (האדמין T3eS) לעזור לו מכיוון שהוא זה שמנהל את האתר Altenen.com.
2. **המשתמש Smewds מודה לאדמין T3eS על שייצר את הפורום Altenen.com.**

3. הודעות של משתמשים שונים, על כך שמודים לחשוד 1 (לאדמין T3eS) שביצע את השנוי בסוג החשבון שלהם, והפך אותם במערכת ממשתמשים רגילים למשתמשי VIP, לאחר ששילמו על כך.
4. הודעות של משתמשים שונים, על שמתלוננים בפני חשוד 1 (אדמין T3eS) שהם לא מבחינים בשום שינוי מהותי לאחר שבוצע השנוי בסוג החשבון שלהם, והפכו במערכת ממשתמשים רגילים למשתמשי VIP, לאחר ששילמו על כך.
5. הודעות של משתמשים שונים, על שמתלוננים בפני חשוד 1 (אדמין T3eS) שלא ביצע את השנוי בסוג החשבון שלהם, ולא הפך אותם במערכת ממשתמשים רגילים למשתמשי VIP, לאחר ששילמו על כך.
6. הודעות של משתמשים שונים, על שמבקשים מחשוד 1 (האדמין T3eS) לצרף אותם ולתת להם גישה לאחד מהפורומים המתמקדים בכרטיסי אשראי גנובים.
7. הודעה מהמשתמש GoDevilX ששואל למה הכתובת IP שלו חסומה באתר altenen.com ועל כך שלא מצליח להיכנס לפורום, וגם מבקש מחשוד 1 (אדמין T3eS) פתרון לבעיה שלו.
8. הודעות של משתמשים שונים, על שמבקשים מחשוד 1 (אדמין T3eS) לשנות את שם המשתמש שלהם, פעולה זו מצריכה הרשאות מנהל וכניסה ל- DataBase המשתמשים.
9. הודעה מהמשתמש Sopped ששואל את חשוד 1 האם המשתמש The Big Father, שתפקידו לנהל את הפורום אמין ואפשר לסמוך עליו. חשוד 1 (אדמין T3eS) עונה לו תשובה חיובית.
10. הודעות ממשתמשים שונים, על שמבקשים מחשוד 1 את הקרדיט (דירוג משתמש) שהיה לו בעת שהיו חברים בפורום ABH עבור המשתמשים הנוכחיים שלהם בפורום Altenen.com. פעולה זו מצריכה הרשאות מנהל וכניסה ל- DataBase המשתמשים.

11. **הודעות ממשתמשים שונים, על כך ששואלים את חשוד 1 (אדמין T3eS) מתי הפורום ABH חוזר לאוויר.**
12. **הודעה ממשתמש rileyman0000, על שמברך את חשוד 1 (אדמין T3eS) בנוגע לפתיחת הפורום החדש שלו Altenen.com לאחר שנסגר הפורום ABH.**
13. מחיפוש הודעות שכתב חשוד 1 (אדמין T3eS), עולה ההודעה הבאה שפורסמה בתאריך 6.2.17, שאומרת שהוקם ונפתח אתר פורום חדש www.altenenS.com, ושכולם מוזמנים להירשם אליו. עוד מצרף האדמין לינק לאתר החדש. אתר www.altenenS.com, ששמו השני הוא " Card The World" ("עולם הכרטיסים" הכוונה לאשראי), וגם הוא מתמקד בפרסום וסחר בפרטי כרטיסי אשראי גנובים של אחרים מהארץ ומחו"ל. ע"פ הודעה שכתב חשוד 1 (האדמין T3eS) הפורום הוקם בתאריך 4.2.17.
14. מחיפוש הודעות שכתב חשוד 1 (אדמין T3eS) עולה ההודעה הבאה, שאומרת כי האתר החדש בכתובת www.altenenS.com שופץ ותוקן, כל המשתמשים שהיו קיימים לפני שקרתה הבעיה עדיין יכולים לגלוש שם ללא כל בעיה.
15. **מחיפוש הודעות שכתב חשוד 1 (אדמין T3eS) עולה ההודעה הבאה שבה מודיע כי ישנה בעיה זמנית בפורום ATN עקב ביצוע גיבוי שנעשה לאתר יומיים לפני כן. בהודעה אחרת כותר חשוד 1 כי הייתה בעיה זמנית בפורום ATN, וכעת הבעיה טופלה ותוקנה.**
16. **מחיפוש הודעות שכתב חשוד 1 (אדמין T3eS) עולה ההודעה הבאה שבה הוא מבקש ומחפש לשכור שירותים מהאקרים לטובת שיפור מנגנון האבטחה באתר www.altenen.com היות וכמות החברים בו גדלה בצורה ניכרת. עוד מציין חשוד 1 בפוסט כי כל המעוניין להגיש מועמדות יצטרך להוכיח את רמת מיומנותו ע"י פריצה למחשב/אתר/שרת אחר. לבסוף, חותם את הפוסט עם הכינוי שלו T3eS ומוסיף "מייסד ATN".**

17. מחיפוש הודעות שכתב חשוד 1 (T3eS), אותרה הודעה שהיא תגובה למשתמש ghettomain על שטען שפורום ABH חזר ועלה לאוויר. **חשוד 1 (T3eS) ענה בתגובה שהפורום ABH נסגר והוא פותח אותו לפעמים.**

18. מחיפוש הודעות שכתב חשוד (T3eS), עולות ההודעות הבאות שהן תגובות למשתמשים שונים על שטענו שפורום ABH שוב נפל. **חשוד 1 (T3eS) ענה בתגובות שונות שהפורום ABH יעלה בקרוב ו/או עלה לאוויר.**

25. בתאריך 19.3.18 התקבל מענה לצו המצאת מסמכים למייקרוסופט בנוגע לכתובת המייל t3ys@hotmail.com. מהמענה עולה כי תיבת המייל נפתחה בתאריך 2/5/2008. **שם החשבון הרשום הוא: T3es.** דואר חלופי לכתובת המיל הוא: nana_s1@hotmail.com וכתובת ה-IP עימה נפתחה התיבה היא **כתובת IP מהרשות הפלשתינאית.**

26. דוח של השוטרת רחל אפריאט מתאריך 19.3.18- איתור פרטים אודות חשוד 1:

- בחיפוש באתר "altenen.com" בהקשת מילת החיפוש "T3es"", נמצא פוסט אחד מיום 10/02/14 ובו הפרטים הבאים: Name: Helmi ,Nickname: T3es,Te3s ,Address: Bilal street city Hebron, Pin-00970, Isreal ,Gheith Email: helmegith@gmail.com, t3ys@hotmail.com , owner_abh@yahoo.com, Phone: 970598432751
- בבדיקת הכינוי "t3es" נראה בין היתר סרטון ביוטיוב בשם " Hacked bank by T3es" שפורסם על ידי המשתמש בעל חשבון ב-google plus בשם "helme gith" בחשבון זה מופיעים שני תצלומים שהועלו בשנת 2013 תחת הכותרת "t3es" ובו נראה גבר בעל שיער קצוץ משקפי שמש וחולצה קצרה. בנוסף , מופיע חשבון twitter ע"ש " t3es" עם השם "alboraaq_owner".
- בחיפוש כתובת הדוא"ל helmegith@gmail.com נמצא כמקושר למשתמש בשם "t3es11" עם תמונה ובה כיתוב "alboraaq team". בנוסף, כתובת הדוא"ל מקושרת לחשבון פייסבוק על שם "חילמי ג'ית"(כתוב בשפה הערבית) המציג עצמו מחברון. בתוך הפרופיל תמונות ובהן הכיתוב "t3es big boss alboraaaq" , "t3es".
- בבדיקת חשבון ה-630593739 " ICQ", נמצא שם המשתמש "T3eS ALBoRaaq".
- בבדיקת מספר 059-8432751 במערכת המשטרתית, נמצא כמשויך לחילמי ג'ית , ת.ז: 946945300 מחברון. תאריך לידה: 19/01/85.

27. דוח של השוטר יניב חסון מתאריך 19.3.18- איתור נתונים אודות המשתמש –
•™_prince_™• :

- בחיפוש באתר Altenen אותר משתמש שמספר ה-ID שלו הינו 2 והוא בדרגת ATN-TeaM ושם המשתמש שלו הינו –•™_prince_™•–.
- לאחר בדיקה שמטרתה להבין את מיקום הדרגה ATN-TeaM בסולם הדרגות הכללי של אתר Altenen.com, נמצא כי קיים משתמש אחד בלבד בדרגה זו (–•™_prince_™•–) והנ"ל דרגה אחת מתחת לדרגת Administrator בה מכהן מייסד ומקים האתר המשתמש T3eS שהינו חשוד 1.
- בחיפוש במידע הגלוי על השם –•™_prince_™•– אותרה כתובת המייל topwuprince@gmail.com.

28. דוח פעולה של השוטר תמיר סנבטו מתאריך 3.4.18 בנוגע לסריקת רשתות: **בתאריך הנ"ל בוצעה סריקת רשתות בסמוך לביתו של חשוד 1 בחברון. במהלך הסריקה בסמוך לביתו של חשוד 1 אותרה רשת מוצפנת וסגורה בשם ANT office 2. מכשירים שנצפו על הרשת: Sumsung electro-mechanics (Thailand) ,LG Electronics (mobile).**

29. דוח של השוטר יניב חסון מתאריך 9/4/18- **איתור Post מאתר Altenen.com המדבר על יום הולדתו של חשוד 1 המכונה באתר T3es: משתמש בשם JulleD רושם לחשוד 1: " Happy Birthday Admin T3es". משתמש נוסף רושם לחשוד 1 " Happy Birthday Administrator..Love you and ATN too much". משתמש נוסף רושם לחשוד 1 "Happy birthday T3es! We are glad that we have Admin like uou". עוד משתמש כותה לחשוד 1 "happy birthday boss". חשוד 1 עונה לכולם "thanks all".**

30. בתאריך 16.4.17 נחקר באזהרה (בתיק אחר של יחידת הסייבר) עדן חן ת"ז 311290076 מסר כי **לפני כשנתיים נעקץ ב-500 דולר ע"י חשוד 1 (בעל אתר ATN), עדן רכש מהאתר אייפון 7 או אייפון 6 והאייפון היה אמור להגיע אליו, וכעבור מספר ימים המשתמש שלו נחסם והטלפון לא הגיע ובעקות זאת הוא ביצע פעולות שונות ואיתר את הפרטים האישיים של חשוד 1 תושב חברון והתכתב איתו דרך האתר. חשוד 1 סיפר לו שהוא מיליונר, הוא עושה הרבה כסף אבל הוא לא אמר דרך מה הוא עושה את הכסף. בנוסף, לקראת סוף ההתכתבויות עם חשוד 1 עדן**

הגיע לחשבון שלו ב-ATN ואז נשלחה לחשוד 1 התראה שעדן שניסו להיכנס אליו לחשבון ואז חשוד 1 שאל את עדן בהתכתבות אם זה הוא שניסה להיכנס אליו לחשבון והוא חסם את החשבון של עדן. בעקבות זאת, התפרסמה כתבה באתר "פוסטה" על חשיפת חשוד 1 כבעל אתר ATN בנוגע לעבירות הונאה שמבצע חשוד 1 כלפי משתמשים. עדו מסר עדן כי חשוד 1 עושה את הכסף שלו ממכירת מכשירים סלולאריים. חשוד 1 מפרסם ברשת האינטרנט בכל מיני אתרים וקבוצות מכירה של מכשירי טלפון חדשים בחצי מחיר והתשלום רק בביטקויין. לאחר התשלום החשבון של אותו משתמש שהעביר כסף לקניית מכשיר נחסם ואז חשוד 1 מגיב בשמו שהוא קיבל את המוצר ומעלה תמונה של המוצר שכביכול נשלח וזהו. עדן מסר כי לאחר 3 ימים שהכתבה פורסמה הוא הוריד את הכתבה מהאתר כי הפרטים שלו נחשפו ולכן הוא <u>חשש לחייו ועדיין חושש לחייו.</u>

<u>חקירת משתמשים ישראלים באתר Altenen.com</u>

במהלך החודשים האחרונים נאספו ראיות מאתר Altenen.com כנגד 10 משתמשים ישראלים שפרסמו מספרי כרטיסי אשראי ורשמו פוסטים באתר Altenen אודות שימוש בכרטיסי אשראי. להלן תקציר חקירותיהם:

1. **בתאריך 14.3.18 נחקר ברנדון דין אלוני ת"ז 313296345** בוצע חיפוש בביתו ונתפסו מספר מחשבים וטלפונים ניידים. הודה כי יש לו חשבון באתר Altenen.com פרסם כרטיסי אשראי באתר וביצע קניות בכרטיסי אשראי שפורסמו באתר. בנובמבר 2014 חבר שלו הכיר לו את אתר Alboraq שבהמשך נהפך לאתר בשם Altenen. מסר כי אח של חבר שלו שעבד במוקד הזמנות של רשת מסעדות "ג'ירף" העביר לו מספרי כרטיסי אשראי של לקוחות שבאמצעותם הוא הזמין נסיעות דרך get taxi ולאחר מכן הוא פירסם את הכרטיסי אשראי באתר Altenen. נשאל לגבי בעל האתר ומסר כי אם משלמים לבעל האתר בביטקוין, הוא נותן דרגת משתמש, הדרגה נותנת הרשאה לפרסום של נתונים למי שרוצה למכור באתר Altenen ואם לא רוכשים דרגה לא יכולים להרוויח כסף ולמכור באתר, רק לפרסם בחינם. מסר כי זוכר ששם המשתמש של בעל האתר הוא prince. מסר כי באתר Altenen יש סחר בחשבונות פרוצים במידע פרוץ, זה אתר לא חוקי לגמרי מבחינת המהות שלו, השימושים של האתר זה חקר ושימוש, גם סיסמאות השייכים לאתרים פרטיים נמצאים באתר מפרסמים שם מספרי כרטיסי אשראי בכמויות.
בתאריך 29.3.18 נחקר שוב ברנדון אלוני ומסר כי בתקופה בה התעסק בקארדינג הוא שם במתנ"ס בבית דגן פעמיים Keylogger, על מחשב אחד, המחשב הראשי של המזכירה, הוא

עשה את זה במשך 3 ימים וכל הנתונים עברו לכונן חיצוני שחיבר לצד האחורי של המחשב שאף אחד לא ראה. מסר כי רוב כרטיסי האראי שאותרו אצלו במחשב הם מקבוצות באיסיקיו או מאתר altenen. החשוד נתן את הסכמתו בכתב שיחידת הסייבר תוכל להשתמש בחשבון שלו באתר Altenen ובחשבון המייל שלו המקושר ל-Altenen. במהלך החקירה החשוד ביחד עם החוקר נכנסו לאתר Altenenולחשבון המייל כדי לוודא שהם תקינים. בנוסף, הראה לחוקר היכן מפרסמים באתר Altenen את מספרי כרטיסי האשראי.

2. **בתאריך 21.3.18 נחקר באזהרה אבירם אברהם דהן ת"ז 208207902** בוצע חיפוש בביתו ונתפסו מספר מחשבים וטלפונים ניידים. הודה כי יש לו חשבון באתר altenen.com . מסר כי בעבר האתר נקרא albooraq אבל הוא נסגר והפך ל- altenen . הודה כי ביצע שימושים במספרי כרטיסי אשראי שפורסמו באתר Altenen. הכחיש כל קשר לשם משתמש kolmns22 וטען כי לא פרסם כרטיסי אשראי ובמיוחד לא כרטיסי אשראי ישראלים.
בתאריך 4.4.18 נחקר בשנית וזאת לאחר שאותרו במחשביו ראיות לכך שהוא פתח 3 חשבונות באתר Altenen והוא רכש מוצרים רבים בכרטיסי אשראי. בנוסף, אותרו שיחות רבות בהם הוא מדבר עם משתמשים רבים בנוגע לכרטיסי אשראי גנובים. טען כי זה לא הוא כי פרצו לו למחשב והוא היה בצבע ו/או בעבודה בשעות המדוברות.

3. **בתאריך 21.3.18 נחקר באזהרה אדר קציר דהן ת"ז 209502293.** הודה כי לפני 3 או 4 שנים פתח חשבון באתר albooraq שלאחר מכן נהפך ל- altenen.com . לאחר שחשבון הראשון נחסם, הוא פתח חשבון נוסף בעל שם משתמש adarkatzir. מסר כי עשה העתק הדבק באתר Altenen למספרי כרטיסי אשראי שפורסמו שם כי צריך מכסה של פוסטים שצריך לכתוב על מנת להיכנס לכל מיני פורומים באתר. ביצע בסביבות 30 -40 ניסיונות במספרי כרטיסי אשראי שונים רק של חו"ל שפורסמו באתר Altenen, בחלק הצליח לרכוש מוצרים. לא השתמש בכרטיסי אשראי ישראלים כדי לא לפגוע באנשים בישראל. בנוסף, פרסם באתר Altenen שירותי פוטושופ ועשה 3 כרטיסי אשראי מזוייפים לשלוש משתמשים שפנו אליו באתר Altenen ושילמו לו כסף.

4. **בתאריך 21.3.18 נחקר באזהרה ברק מרציאנו דהן ת"ז 319130225**. הודה כי פתח חשבון בשנת 2015 בעל שם משתמש baracuda153 באתר Altenen שלאחר מכן נהפך ל- albooraq . הוצג לו מסמך ובו הכחשות עסקאות בכרטיס אשראי שהוא פרסם באתר Altenen ובעל הכרטיס הכחיש, ברק איתר מספר עסקאות שהוא ביצע בכרטיס אשראי זה.

5. **בתאריך 21.3.18 נחקר באזהרה לירון מובשוביץ ת"ז 318324381.** מסר כי אולי פעם ראה את אתר altenen או alboraq. הכחיש כל קשר לשם משתמש שהוצג לו שכביכול הוא פתח וטען כי לא יודע אם יש לו שם משתמש באתר Altenen ולא זכור לו אם יש דבר כזה. בחלק מהתשובות שמר על זכות השתיקה.

6. **בתאריך 28.3.18 נחקר באזהרה סהר אברהם מנע ת"ז 207580515**. הכחיש קשר לאתר Altenen. מסר כי לא מכיר אתר בשם זה.
7. **בתאריך 29.3.18 נחקר באזהרה רון ישראל בן סימון ת"ז 318401577.** מסר כי את פרטי כרטיסי האשראי הוא הביא מאתר בשם Altenen ואת הרכישות שלו לפני כחודש וחצי ביצע דרך אתר amazon וקנה נעליים של ניו בלאנס, ועוד ג'ל לשיער שתי המשלוחים הגיעו אליו הביתה. עוד מסר כי המשתמש שלו באמזון חסום בגלל שהשתמש באשראי לא שלו. אישר כי שם המשתמש שלו באתר Altenen הוא ron1561. מסר כי כדי להיכנס לאתר Altenen צריך VPN, אבל בתקופה של לפני שנתיים וחצי הוא נרשם בלי VPN כי לא היה צריך. בנוסף, לפני שנתיים וחצי זה היה גם נקרא אתר alboraq היה אפשר להיכנס גם וגם עד שאתר alboraq נסגר.
8. **בתאריך 29.3.18 נחקר באזהרה אלמוג סלגניק ת"ז 207580515.** מסר כי הכול התחיל בגיל 16 או קצת לפני, תקופה בה הוא נחשף לאתר בשם alboraq ואחרי זה שהפילו את האתר או שינו אותו, הוא המשיך באתר שנקרא altenen. שם המשתמש שלו באתר altenen הוא almog290. מסר כי ביצע מאות נסיונות וגם רכישות בכרטיסי אשראי שלקח מאתר alboraq ואתר altenen . פירט את תהליך ההרשמה לאתר alboraq ולאתר altenen . מסר כי בין היתר באותה קטגוריה של כרטיסי אשראי שהיו מפרסמים באתר altenen היו גם מפרסמים חשבונות פייפל. **מסר שהתחילו להיכנס לאתר altenen עם כתובת IP לא מישראל כי כנראה זה אתר של ערבים כי באתר היה מלא כיתוב בערבית, ב-altenen יש אפשרות לכתוב מאיפה אתה והיה הרבה תורכיה, ערב הסעודית הרבה, מצרים בעיקר ערבים היה שם, פחות אירופה, בעיקר ערבים.**

<u>החקירה הגלויה</u>

מדובר בחקירה המתנהלת ביחידת הסייבר בלהב 433 בשיתוף פעולה בין לאומי בין גורמי אכיפה שונים ברחבי העולם. בשעות הקרובות ייעצר במדינת קנדה חשוד תושב קנדה שפרסם והשתמש בכרטיסי אשראי באתר Altenen.com.

היום החלה החקירה הגלויה בישראל. לפנות בוקר נכנסו ברכבים מוגנים שוטרי יחידת הסייבר של להב 433 עם חיילים מחטיבה מרחבית יהודה וחיילים מגדוד 101 של חטיבה 35 לחברון לביתו של חשוד 1. בנוסף, הוכנס לביתו של חשוד 1 כלב המתמחה באיתור אמל"ח. במהלך החיפוש נתפסו מחשבים, טאבלטים, מדיה נתיק, טלפונים ניידים, כרטיסי אשראי, צ'קים ומכונית מסוג קאיה בצבע שחור. לציין כי בתוך כספת שאותרה בביתו של חשוד 1 נמצא התקן נייד-ארנק דיגיטלי למטבעות וירטואליים.

1. התקבלה עדות עצמית מאבירם אברהמי מחברת לאומי כארד. **מהעדות עולה כי ב-486 כרטיסי אשראי אשר פורסמו באתר Altenen והועברו ללאומי כארד בוצעו 48,998 נסיונות לביצוע הונאות בסך כולל של 31,286,155 ₪ כאשר מתוכם צלחו 2945 פעולות בסך כולל של 892,312 ₪.** בנוסף, **אבירם ציין בעדותו כי מדובר ב"קצה הקרחון" של הפרשה כיוון שבפרשה מעורבים אלפי כרטיסי אשראי אשר הונפקו בחו"ל ואין יכולת לחברות האשראי בארץ, לראות עסקאות הונאה בכרטיסים אלו באתרי אניטרנט בחו"ל----לכן צוות החקירה שלח כ-6000 מספרי כרטיסי אשראי לחברות אשראי בחו"ל על מנת לקבל מהם נתונים אודות הונאות שבוצעו בכרטיסים אילו.**

2. התקבל מייל מסוכן ה-FBI כי התקבלו נתונים של כרטיסי האשראי מחו"ל שפורסמו באתר והשייכים לחברת אמריקן אקספרס העולמית. **הנתונים נמצאים אצלו והוא יעביר אותם לידי צוות החקירה בהקדם.**

3. במהלך חיפוש בביתו של חשוד 1 נמצאו בביתו מספר מחשבים דלוקים/פתוחים. מסכי המחשב תועדו. **מתיעוד מסכי המחשב עולה באופן ברור ביותר כי חשוד 1 הוא משתמש T3es והבעלים והמנהל של אתר Altenen.com ואתר Alboraq.com**. בנוסף, **לחשוד יש ארנק דיגיטלי שבתוכו כ-5 מטבעות ביטקויין השווים כיום כ-40,000 דולר---לציין כי האפשרות היחידה לשלם באתר Altenen.com היא רק באנצעות מטבע דיגיטלי מסוג ביטקויין** (ראה מזכר של השוטר סנבטו תמיר מיום 24.4.18).

4. במהלך חיפוש בביתו של חשוד 1 בוצעה סריקת רשתות בבית החשוד על מנת לאתר את הרשת בביתו. **אותרה רשת חשודה בשם Office ATN (שם הקיצור של אתר Altenen.com הוא ATN).**

5. דוח פעולה של השוטר יצחק ברומי מיום 24.4.18-חיפוש בביתו של חשוד 1- במהלך החיפוש בביתו של חשוד 1 בקומה ק+1 (משרדו של חשוד 1) **היה מחשב נייח אשר היה פתוח על עמוד הפייסבוק של קבוצת Alboraq Hackers. כמו כן במועדפים של דפדפן האינטרנט היו קיצורי דרך לאתר Altenen / ATN. במחשב הנ"ל הייתה מותקנת תוכנת ICQ אשר פעלה ברקע והקפיצה הודעות שונות אודות קבוצת ATN ובקשות שונות בנוגע לכרטיסי אשראי. לאחר מכן נמצא מחשב נייח HP בקומה ק -1 – במחשב הנ"ל דפדפן האינטרנט היה פתוח על הפורום של Altenen. במהלך החיפוש נמסר לחשוד 1 מחשב נייד משטרתי בו מבוצע תיעוד מסך, לצורך כניסה שלו ל Altenen**

<u>משום שעלתה טענה מצד החשוד שמדובר באתר הכרויות. החשוד נכנס לאתר הכרויות (ללא קשר ל Altenen) שם ניסה להיכנס אך ללא הצלחה</u>. בנוסף, מבדיקת כתובת ה-IP בביתו של חשוד 1 עלה שכתובת ה- IP החיצונית של הנתב היא: 217.21.6.174

6. מדוח פעולה של השוטר סאפי כרים עולה כי בתשאול חשוד 1 בביתו הוא טען כי הוא השתמש בעבר באתר Alboraq ובאתר Altenen הוא משתמש אך ורק לקשקוש עם נשים כי הוא אוהב נשים. בנוסף, הנשים שלו תושאלו ומסרו כי רק חשוד 1 משתמש במשרדים ובמחשבים בבית.

7. מדוח פעולה של השוטר רן פלייסיגר מתאריך 24.4.18 עולה כי חשוד 1 **החשוד ניסה מספר פעמים לדבר באנגלית. <u>חשוד 1 נשאל מה הקשר שלו לאתר Altenen והחשוד ענה " its my site"</u> בהמשך טען כי הוא התכוון שהוא רק רשום כמשתמש באתר והאתר לא שלו. לשאלת השוטר מי זה משתמש T3es וחשוד 1 ענה שהוא לא יודע השוטר הטיח בפניו שזה שם המשתמש בכל המחשבים בבית וחשוד 1 ענה שאולי השוטרים שמו לו את זה במחשבים שלו, לאחר מכן טען כי אתר Altenen זה אתר הכרויות עם נשים. תוך כדי חיפוש שביצע החשוד בגוגל הוא נכנס לאתר הכרויות (ששמו לא דומה בכלל לאתר Altenen) וניסה להתחבר עם שם משתמש וסיסמא ללא הצלחה.**

8. חשוד 1 נחקר (במהלך החקירה נוכח מתורגמן) ומסר כי **מספר הטלפון 059-8481404 הוא בשימושו. מכחיש כל קשר לאתר Altenen וטען כי "אני לא מכיר את האתר הזה, רק מכיר אתר Altenen שיש בו צ'ט". בנוסף טען כי " אלבורק זה אתר לפני 8 שנים, הוא אתר להתקשרויות פלסטינאיות, ויש שם גם צ'ט".**

<u>פעולות חקירה מיום 25/4/18</u>

אותרה במחשבו של חשוד 1 גישה לניהול אתר Altenen.com

1. בתאריך 25.4.18 נחקר חשוד 1 ומסר כי לפני שלושה שבועות הוא ירד לשוק הישן, וראה מישהו שיש לו מחשבים, בן אדם בערך בן 31. חשוד 1 רצה לקנות 3 לפטופים לנשים שלו ולפטופ בשבילו. חשוד 1 מסר כי הוא לקח משם 4 מחשבים ולאחד מהמחשבים הקופסה שלו הייתה שבורה ואותו אדם אמר לו אתה והמזל שלך אם המחשבים עובדים אז עובדים ואם לא אז לא. חשוד מסר כי הוא נתן לכל אישה מחשב והוא בדק את המחשב הראשון והתפלא שהוא עובד, כולם עבדו חוץ מאחד. בנוסף, חשוד 1 מסר כי כאשר הוא פתח את המחשב לא היה עליו שום סיסמה. **הכחיש קשר לאתר Altenen ומסר כי אינו יודע מה זה מטבעות ביטקויין. לרוב שאלות החוקר ענה " אמרתי את כל מה שיש לי" ובחלק נכבד מהשאלות שתק.**

2. חשוד 1 נחקר בתאריך 25.4.18 בשנית. **בנוכחותו במהלך החקירה הוצג בפניו מסמך. מסמך זה הוא קובץ שנקרא server NL(1).txt. קובץ זה אותר בפריט מספר 80621493 . מחשב נייח גלקסי אשר נתפס אצל חשוד 1 בביתו. <u>במסמך זה רשומה הכתובת של אתר altenen עם הפורט 2082 שזה פורט ניהול האתר</u>. בנוכחותו של חשוד 1 הופל אתר Altenen.com על מנת להפסיק את העבירות שמתבצעות באתר בכל רגע נתון- <u>החשוד שתק לכל אורך החקירה וברגע שהצלחנו להיכנס לפאנל ניהול האתר הוא צחק.</u>**

3. בחודשים האחרונים הועברו לחברת ישראכרט נתונים אודות 669 מספרי כרטיסי אשראי אשר פורסמו באתר Altenen.com. **בתאריך 25/4/18 התקבלה עדות עצמית ונתונים מחברת ישראכרט כי ב-282 כרטיסי אשראי מתוך ה-669 כרטיסים אשר פורסמו באתר התבצעו <u>1014 עסקאות הונאה</u> בסך כולל של <u>161,982.90</u> דולר.**

4. בבדיקה של פריט מספר 80621638 (מחשב נייד) אשר נתפס בביתו של חשוד 1, **אותרה תיקייה בשם T3eS בתוך תקיית User של Windows. כלומר ישנו משתמש (User) במחשב זה בשם T3eS.**

פעולות חקירה מיום 26/4/18

1. בתאריך 26.4.18 נחקר חשוד 1. **לאורך כל החקירה הוא אמר " אמרתי את כל מה שיש לי" וגם בחלק נכבד של השאלות הוא שתק.**

2. דוח פעולה של השוטר יצחק ברומי מיום בתאריך 26.4.18 **במהלך חקירתו של החשוד בתאריך 25.4.18 ובנוכחותו נכנסנו לממשק ניהול altenen בכתובת altenen.com:2082- אשר אותרה במחשבו של חשוד 1**. לאחר מכן נכנסנו למנהל הקבצים ושם נכנסנו להרשאות התקייה – public_html, **והסרנו הרשאות קריאה והפעלה מ- Group כך שהמשתמשים אשר ינסו להיכנס לאתר Altenen.com לא יוכלו לצפות בדף האינטרנט של האתר ובכך תחסם הגלישה לאתר וכל זאת על מנת להפסיק את העברות המתבצעות באתר altenen.com עד לרגע חסימת הגלישה לאתר.**

פעולות חקירה מיום 27/4/18

1. דוח פעולה של השוטר שושן בנימין מיום 26.4.18- בדיקת מכשיר galaxi lg gsm k520dy stylus2 מספר פריט 80621312- **במהלך הבדיקה התגלתה התחברות ל wireless בשם ATN office 2- שם זה הוא שם הרשת בביתו של חשוד 1.** לציין, **כי בטלפון הנ"ל ישנן הודעות sms בשפה הערבית, הודעות whatsup בשפה הערבית, הודעות פייסבוק בשפה הערבית, ותמונות עם כיתוב בערבית**.

2. דוח פעולה של השוטר יניב חסון מתאריך 27.4.18- איתור פרטי ארנק ווירטואלי במהלך בדיקת פריט 80621523. במהלך בדיקת פריט שמספרו 80621523 (HD פנימי) שנתפס בביתו של חשוד 1, **אותר קובץ מסוג TXT, בשם Bitcoin.txt שנמצא בנתיב " NEWS format/goo format/new [root]/(I:)NONAME.**
לציין כי כתובת הארנק המצויה בקובץ זה, זהה לכתובת הארנק שמפורסמת באתר altenen.com לטובת העברת תשלומים עבור שטחי פרסום ושדרוג משתמשים. ראה דוח "קישור ארנק הביטקויין המפורסם באתר Altenen.com לחשוד חילמי גית."מתאריך 27/02/18).

3. דוח פעולה של השוטר שושן בנימין מתאריך 27.4.18-

פעולות חקירה מתוכננות לימי החקירה הבאים:

1. המשך חקירת החשוד- מדובר בחקירות רבות שיש להטיח בפני החשוד את חומר הראיות ואת התוצרים שיופקו מהמחשבים ומהציוד הדיגיטלי שנתפס.
2. תישקל האפשרות להכניס מדובב לתאו של חשוד 1.
3. מיצוי וחקירה פורנזית לכלל המחשבים והציוד הדיגיטלי והסלולאר (בהתאם לטבלת מוצגים) שנתפסו בביתו של החשוד- מדובר בעבודה מורכבת הדורשת ימים רבים על מנת למצות את החומרים.בנוסף, **מדובר בהודעות והתכתבויות רבות מאוד בשפה הערבית, דבר שמצריך תרגום מהשפה הערבית לשפה העברית.**
4. כלל הנתונים (Data Base) של אתר Altenen.com נמצאים בשרתים מרוחקים ולכן יש חשש כי החשוד ימחק את כל הנתונים מרחוק כולל הורדת האתר- בשלב זה צוות החקירה לא יודע היכן ממוקמים שרתי האתר מכיוון שהחשוד השתמש בשירותי בידול ומיסוך.
5. בדיקת תוכן ענני גיבוי השייכים לכל תיבות הדוא"ל בהם משתמש החשוד.
6. קבלת חומר ראיות רשמי מהבקשה לעזרה משפטית שהופנתה לארה"ב.
7. חקירת יעקב חסקל- בעבר מסר ביחידת הונאה ת"א כי דיבר עם חשוד 1.
8. חקירת חירות זלטקה- העביר לגולש ישראלי מספרי כרטיסי אשראי אשר פורסמו באתר Altenen.
9. חקירת דוד גולצמן- משתמש ישראלי שפרסם כרטיסי אשראי באתר- לא נחקר עדיין בשל החשש כי ישבש הליכי חקירה בשל העובדה כי לנ"ל ר"פ מגוון בעבירות שונות.
10. קבלת נתונים מחברות האשראי בחו"ל בנוגע להונאות שבוצעו באלפי כרטיסי האשראי שהועברו להם.
11. בדיקת הארנקים הדיגיטלים שאותרו ויואתרו ברשות חשוד 1 והשוואתו/התאמתו לארנק הדיגיטלי המפורסם באתר Altenen.
12. מיצוי המוצגים שאינן מוצגי מחשב בדגש על בדיקת מקרם לרבות צ'קים, כרטיסי אשראי וכו'.

כבוד בית המשפט, החקירה בעיצומה. מדובר בחשוד שהקים ומנהל את אחד האתרים הגדולים והנפוצים ביותר בעולם לעבירות סייבר בכלל

ולהונאות בכרטיסי אשראי בפרט. האתר גורם נזק כלכלי רב ביותר לחברות האשראי בעולם כולל ישראל ובאופן ישיר לקרבנות תמימים בארץ ובעולם. אותרו הודעות והתכתבויות רבות בכל המוצגים שנתפסו מחשוד 1 דבר שמצריך זמן כדי לתרגם ולאחר מכן להטיח בפני החשוד. שחרור החשוד בשלב זה של החקירה עלול לשבש את החקירה ולהקשות על צוות החקירה באיסוף הראיות והגעה לחקר האמת. בנוסף, החשוד שלפינו יוצא חדשות לבקרים דרך מעבר אלנבי ולכן יש חשש רב להימלטות מהדין. על כן, מתבקש בית המשפט הנכבד להיעתר לבקשה במלואה.

רס"מ ליאור רוטנברג

חוקר סייבר

להב 433