

15 לפברואר 2022

ניצול של המערכת הפיננסית לטובת העברת תשלומים בגין מתקפות כופרה

תקציר מנהלים

מסמך זה מומלץ לקריאה בעיקר

עבור:

- גורמי הנהלה ומחלקות משפטיות בגופים פיננסיים
- קציני ציות
- גופים העוסקים בתחום הנכסים הווירטואליים
- חברות ניהול משברים
- מחלקות סייבר ואבטחה
- עו"ד, רואי חשבון ויועצי מס העוסקים בתחום הסייבר
- רגולטורים בתחום הפיננסי
- רשויות אכיפה
- מכוני מחקר בתחומי סייבר ובטחון לאומי

המעבר הגובר לשימוש באמצעים דיגיטליים ובתווך המקוון, אשר התעצם ביתר שאת בתקופת הקורונה, הביא בצידו גידול חד (בין 100% ל-300% לפי מרבית ההערכות) בהיקף מתקפות הסייבר, ובמתקפות הכופרה בפרט.

כופרה (Ransomware) מוגדרת כסוג של נזקה שמטרתה הדבקת מחשב/טלפון סלולארי של הקורבן וחסמת הגישה להפעלת/לנתונים שבו, אשר תוסר בתמורה לתשלום כופר (לרוב תשלום כספים).

אחד ממאפייני פשיעת הסייבר ככלל, ומתקפות הכופרה בפרט, בהקשר לפעילות פיננסית הוא, שהסתרת הפעילות הנעשית באמצעות שימוש בנכסים וירטואליים הינה חלק מביצוע עבירת הלבנת הון. לפי מחקרים בינלאומיים, כ-75% מהכספים המופקים מפשיעת סייבר מועברים באמצעות נכסים וירטואליים.

בהקשר זה יודגש כי ביום 14.11.2021 נכנס לתוקף צו איסור הלבנת הון המטיל חובות איסור הלבנת הון ומימון טרור על נותני שירות בנכס פיננסי (נש"פים), לרבות אלה המבצעים פעילות במטבעות ווירטואליים.

ישראל חשופה להיקף משמעותי של מתקפות כופרה. על פי הערכות שונות, מספר מתקפות הכופרה על גורמים ישראלים גדל בשיעור חד בשנה האחרונה (עד פי 7) ונאמד בין 5-11 מיליון תקיפות בשנה, הגם שחלק ניכר מן התקיפות נבלם. לפי סקרים עדכניים (לרבות של [הלמ"ס](#)) קרוב למחצית מהעסקים הגדולים בישראל חוו מתקפת סייבר (לרבות מתקפות כופרה).

מניתוח מאגר הנתונים של הרשות לאיסור הלבנת הון ומימון טרור (להלן - "הרשות"), עולה כי כלל תשלומי הכופר בישראל שדווחו לרשות מבוצעים בנכסים וירטואליים, בין השאר באמצעות נותני שירותים בנכסים וירטואליים (להערכתנו, חלק ניכר מכלל התשלומים מבוצע באמצעות נותני שירותים זרים, שאינם מדווחים לרשות). תשלומים אלו מבוצעים לעיתים ע"י/בתיווך חברות לניהול משברים (המייצעות לחברות באירועי משבר, דוגמת תקיפת סייבר). לעיתים, גם אזרחים זרים (ללא זיקה לישראל) משלמים תשלומי כופרה באמצעות נש"פים הרשומים בישראל. עוד עולה כי התוקפים מרבים להשתמש באמצעים לטשטוש יעד הכספים כגון מיקסרים¹ וארנקים "חד-פעמיים".

המסמך מציג גם דוגמאות לדיווחים של גופים פיננסיים לרשות בגין פעילות הנקשרת לתשלומי כופר, וכן פרשייה שהרשות הייתה מעורבת בחקירתה בהקשר של תשלום כופר ע"י גוף ישראלי שהגיע בסופו של דבר לנותן שירותים פיננסיים באיראן, ועשוי להצביע על טיב המתקפה. המסמך כולל רשימת "דגלים אדומים", אשר קיומם, לחוד או בצוותא, עלול להצביע על פעילות הנחזית כתשלום כופר.

¹ מיקסר (MIXER) - שירות מקוון שמטרתו לטשטש את מקורם של כספי קריפטו ע"י ביצוע מספר רב של העברות בפרק זמן קצר מאוד ("יערובל כספים").

רקע כללי

לפי משטרת ישראל², כופרה (Ransomware) מוגדרת כסוג של נזקה שמטרתה הדבקת מחשב הקורבן (לרבות מכשירים סלולריים) או רשת של מחשבים לטובת הצפנתו (נעילתו) או הצפנת קבצים המאוחסנים בו. לאחר ההדבקה, מוצגת הודעה על המסך המודיעה על חסימת הגישה למערכת ההפעלה או לקבצים במחשב ובה דורש התוקף כופר (לרוב תשלום)³ כתנאי לפתיחת ההצפנה. מדובר **בעבירה פשוטה לביצוע**, אשר ניתנת לביצוע מכל מקום ברחבי העולם סימולטאנית למספר רב של מחשבים בלחיצת כפתור ומאפשרת לתוקף לשמור על אנונימיות גבוהה. מצ"ב קישור להמלצות מערך הסייבר לדרכי התגוננות והתמודדות במקרה של תקיפה.

עוד עולה מסקירות מערך הסייבר הלאומי, כי גם משך הזמן שנדרש לשם ביצוע מתקפה מעין זו התקצר משמעותית, ממספר ימים לשעות בודדות, וניתן אף לרכוש ברשת האפילה "ערכות תקיפה" מוכנות אשר מאפשרות באמצעות "שירות מדף" לבצע תקיפות מתוחכמות גם עבור תוקפים בעלי רמת ידע טכנולוגי בסיסית, או לחלופין שירותי תמיכה בתקיפות כופרה (Raas) המסופקים ע"י גורמי מקצוע בעלי ידע טכנולוגי רב.

המעבר ההולך וגובר לשימוש באמצעים דיגיטליים ובתווך המקוון הביא במקביל למגמה ארוכת טווח של גידול משמעותי בפשיעת סייבר. כחלק ממגמה זו, ובשנים האחרונות ביתר שאת, חל **גידול חד בהיקף מתקפות הכופרה** בארץ ובעולם, ולפי הסוכנות האירופאית לאבטחת מידע, תחום פשיעה זה הפך למוביל עבור עברייני הסייבר.

למגמה זו תרמה גם **מגיפת הקורונה**, אשר עקב הצורך של ארגונים רבים לעבור לעבודה מהבית הביאה לגידול חד בהיקף השימוש במערכות גישה מרחוק לרשתות מחשב ארגוניות, וכפועל יוצא הגבירה את הפגיעות של ארגונים במגזרים הציבורי והפרטי למתקפות הכופרה.

כופרה הנה פשיעה חוצת-גבולות, אשר בחלקה מבוצעת על ידי גורמים מדינתיים או בגיבויים/סיועם ובחלקה ע"י גורמים פרטיים שאינם מדינתיים כאשר לתוקפים אין בהכרח עדיפות ליעד (מבחינה גיאוגרפית/אתנית/גיל), כל עוד מדובר במטרה קלה אשר טומנת בחובה פוטנציאל כספי גבוה. לפי הערכת המודיעין הלאומית של ארה"ב, חלק מן התקיפות מבוצעות על ידי קבוצות תקיפה הממוקמות באיראן, רוסיה, צפון-קוריאה וסין, ולפי מחקרים אחרים (כולל של האינטרפול) מעורבים בהן גם ארגוני פשיעה במדינות שונות שנכנסים לתחום עברייני זה מתוך הבנה כי הוא מניב רווחים קלים ומהירים ללא סיכון רב. ככלל, ישנן תקיפות אשר גלומים בהן סיכונים משמעותיים לפגיעה בתשתיות חיוניות ובהתנהלות הכלכלית בשגרה.

יצוין, כי חלק ניכר ממתקפות הכופרה מבוצעות על ידי קבוצות תקיפה מאורגנות אשר עושות שימוש בשם מסוים, אשר לרוב משמש גם כשם שהן נותנות לכלי התקיפה (Avaddon, Conti, Revil) נחשבות לשלוש הקבוצות המרכזיות מבחינת היקפי התקיפות) וכל קבוצה יכולה לבצע מאות מתקפות תחת אותו שם/עם אותו הכלי.

מדו"ח של FinCEN בנושא כופרה עולה כי התוקפים יעדיפו לכוון תקיפותיהם לארגונים עם אבטחה ברמה נמוכה, כמו גם ארגונים שמספקים שירותים חיוניים (דוגמת Colonial Pipe - אספקת דלקים בארה"ב) ולפיכך ייאלצו להעביר במהירות את הכופר.

ממסמך מדיניות של ממשלת אוסטרליה, עולה כי היקף התופעה העולמי המשוער **נאמד בכ-20**

מיליארד דולר במהלך 2021 ובכל 11 שניות מתרחשת מתקפת כופרה על ארגונים, חברות ויחידים ובעולם. לפי נתוני



² https://www.gov.il/he/Departments/Guides/police_cybercrime_ransomware?chapterIndex=1

³ ישנם מקרים מועטים בהם הכופר המבוקש הינו בדמות של דרישות אחרות (שאינן כספיות), דוגמת שחרור אסירים פוליטיים.

FinCEN, היחידה למודיעין פיננסי בארה"ב, במשך כשנה וחצי (ינואר 2020 - יוני 2021) שולמו בגין כופרה בארה"ב לבדה כ- 5.2 מיליארד דולר לפחות, כאשר סכום הכופר המבוקש במרבית התקיפות עמד על עשרות אלפי דולרים.

לפי מספר סקרים של חברות טכנולוגיה ואבטחת מידע, כ-80% מהארגונים שהחליטו לשלם את דרישת הכופר חוו מתקפת כופרה חוזרת.

מתקפות כופרה מאופיינות על פי רוב בכך שהסתרת הפעילות הפיננסית נעשית באמצעות שימוש בנכסים וירטואליים, כאשר בקשת ביצוע התשלום בנכס וירטואלי מהווה חלק ממתווה ביצוע הלבנת הון. נכסים וירטואליים מספקים במקרים רבים אנונימיות, רכישתם מבוצעת לא אחת בזירת מסחר בלתי מפוקחת והתקשורת הנלווית לפעולה מבוצעת באמצעות הרשת האפילה או באפליקציות כגון טלגרם. עוד עולה ממחקרים בינלאומיים כי למעלה מ-75% מהרווחים המושגים מפשיעת סייבר, ובייחוד רווחים שהופקו ממתקפות כופרה, מועברים בתווך המקוון באמצעות נכסים וירטואליים, כרטיסי גיפטקארד מקוונים או NFTs.⁴



אחת המתקפות הבולטות בעת האחרונה מיוחסת לקבוצת פצחנים רוסית ובוצעה מול חברת Colonial Pipeline האמריקאית (מאי 2021). החברה אחראית על אספקת כ-45% מהדלק בחוף המזרחי ומתקפת הכופרה אילצה את החברה להשבית את פעילותה למשך חמישה ימים, השבתה אשר הובילה לשיבושי אספקה ברחבי ארה"ב ולהכרזה על מצב חירום לאומי. החברה שילמה כופר בביטקוין (BTC) ומונרו (XMR) בסך השווה לכ-4.4 מיליון דולר בתמורה להשבת המידע והסרת ההצפנה. חודש לאחר התקיפה [הממשל האמריקאי הודיע](#) כי הצליח להשיב כ-90% מהתשלום הקונקרטי שבוצע באמצעות ביטקוין (כ-2.3 מיליון דולר) באמצעות ניטור הפעילות בבלוקצ'יין והעברת הכספים לארנק בשליטת ה-FBI (הכספים ששולמו באמצעות מונרו טרם הושבו).

מתקפות כופרה בישראל / "ישראל על הכוונת"

לפי [דו"חות](#) של גורמי טכנולוגיה מובילים בעולם ישראל נחשבת לאחד מהיעדים המועדפים על תוקפי הכופרה. היקפי המתקפות על ישראל גדלו בשיעורים חדים בשנה האחרונה (עד פי 7),⁵ כאשר, לפי מרבית ההערכות (של מערך הסייבר וחברות טכנולוגיה ואבטחת מידע), ישנן בין מיליון לחמש מיליון תקיפות שונות בשנה כנגד יעדים ישראלים (חלק ניכר מהן נבלם).

לפי [מערך הסייבר](#), לא רק שהיקף המתקפות גבר אלא שרמת התחכום והתוקפנות שלהן עלתה. כך, למשל, רמת התוקפנות מתבטאת ב"שיטת הסחיטה הכפולה" במסגרתה לאחר שארגון נתקף, התוקף מפרסם חלק מהפרטים הרגישים שהשיג כדי להביכו במקביל לדרישת הכופרה וכדי להמחיש לקורבן את רצינות האיום, בנוסף בחלק מהמתקפות כוללות יכולת מחיקה (WIPER) והן מוחקות את הגיבויים על-מנת להקשות על הגוף המותקף בפעולות השחזור.

⁴ Non fungible tokens –NFT, "טוקנים" יחודיים המסמלים בעלות חד ערכית ומאומתת על קובץ דיגיטלי ייחודי.

⁵ <https://storage.googleapis.com/vtpublic/vt-ransomware-report-2021.pdf>.



מערך הסייבר הלאומי עוד מציין במדריך התגוננות ממתקפות כופרה, כי מרבית המתקפות החלו בשליחת דואר אלקטרוני עם הודעת דיוג (Phishing) או בחזירה דרך ממשקים חשופים לרשת האינטרנט (בפרט ממשקי גישה מרחוק כגון RDP או ציוד VPN ארגוני ושרתי Web).

סקר עדכני של הלמ"ס ומערך הסייבר מיוני 2021 קבע, כי כ-42% מהעסקים הגדולים (250 עובדים ומעלה) בישראל חוו מתקפות סייבר (חלקן נהדפו). סקרים של חברות אבטחה מציגים תמונה ממנה עולה, כי כמחצית מהחברות בישראל חוו תקיפות כופרה וקרוב למחצית מאלו שלא חוו - סבורות כי ייתקפו בשנה הקרובה. יחד עם זאת, מדובר בתופעה אשר קיים קושי להעריך את היקפה האמיתי בשל תת-דיווח. מסקר בטחון אישי של הלמ"ס לשנת 2020, עולה כי 91% מנפגעי העבירות המקוונות אינם מדווחים על העבירה לרשויות האכיפה.

הנזקים הנגרמים ממתקפות כופרה הינם משמעותיים יחסית, כאשר לעתים חברות שהותקפו משלמות את דמי הכופר, אלא שכאמור גם לאחר מכן קיים סיכוי גבוה שיותקפו פעם נוספת. במקרים אחרים נאלצות החברות שהותקפו לתקן את נזקי המתקפה. עלות תיקון ממוצעת בישראל נאמדת בכחצי מיליון דולר למתקפה ונחשבת לנמוכה יחסית בהשוואה לעולם (על בסיס חישוב הכולל את עלות הזמן הנדרש להתאוששות ממתקפה, הנאמד בעולם בכ-21 ימים בממוצע). נוסף על נזקים אלו, ישנו הנזק הכרוך בפגיעה במוניטין (שאינה נכללת בחישוב לעיל) וכן האפשרות כי התוקפים לא יעמדו בהבטחתם וימכרו את המידע וכאמור לעיל שייתקפו שוב.

ביחס לסכומי הכופר המשולמים בישראל, מהנתונים שבידי הרשות עולה כי סכום הכופר אותו דורשים התוקפים מגורם נתקף פרטי נמוך משמעותית מהסכומים אותם דורשים התוקפים מחברות או גופים ממשלתיים. מבחינת המסגרת החוקית בתחום הלבנת הון הרלוונטית לפעילות הכלכלית סביב תשלום כופרה, נציין כי ביום 14.11.2021 נכנס לתוקף צו איסור הלבנת הון ומימון טרור המטיל חובות על נש"פים אשר מבצעים פעילות במטבעות ווירטואליים, לרבות חובות דיווח, רישום, זיהוי ואימות פרטי הלקוח (כולל בעת פתיחת חשבון מרחוק), כמו גם הוראות קונקרטיות לעניין העברה אלקטרונית של כספים ומטבעות ווירטואליים.

עוד יצוין, כי מתן שירות בנכס פיננסי (כגון: העברה, המרה, או שמירה עבור הלקוח), גם אם מבוצע במסגרת תשלום כופרה, מחייב דיווח, לרבות כאשר השירות ניתן לחברה לניהול משברים עבור צד שלישי (הנהנה).⁶

בין מתקפות הכופרה שאירעו השנה בלטה במיוחד התקיפה של בית החולים "הלל יפה" בחזרה, אשר סווגה ע"י מערך הסייבר כאירוע משבר לאומי וגרמה לחשש אמיתי ביחס להמשך התפקוד התקין של בית החולים, בין היתר בשל הנזק שנגרם למערכות המידע שלו. לפי מערך הסייבר הלאומי, אירוע זה היווה חלק מגל תקיפות על מוסדות רפואיים בישראל באותה עת. בשנה האחרונה בלטה גם המתקפה על חברת ביטוח ישראלית שהובילה לדליפה של מידע אישי רב של מבוטחיה. תקיפה זו בוצעה על ידי קבוצת פצחנים בשם BlackShadow המזוהה עם איראן, וזו הציבה לחברת הביטוח דרישה לשלם דמי כופר של 50 יחידות ביטקוין (שווה ערך בעת התקיפה לכ-2 מיליון דולר) בתמורה לכך שלא ימכרו את המידע החסוי שאספו.



בין מתקפות הכופרה שאירעו השנה בלטה במיוחד התקיפה של בית החולים "הלל יפה" בחזרה, אשר סווגה ע"י מערך הסייבר כאירוע משבר לאומי וגרמה לחשש אמיתי ביחס להמשך התפקוד התקין של בית החולים, בין היתר בשל הנזק שנגרם למערכות המידע שלו. לפי מערך הסייבר הלאומי, אירוע זה היווה חלק מגל תקיפות על מוסדות רפואיים בישראל באותה עת. בשנה האחרונה בלטה גם המתקפה על חברת ביטוח ישראלית שהובילה לדליפה של מידע אישי רב של מבוטחיה. תקיפה זו בוצעה על ידי קבוצת פצחנים בשם BlackShadow המזוהה עם איראן, וזו הציבה לחברת הביטוח דרישה לשלם דמי כופר של 50 יחידות ביטקוין (שווה ערך בעת התקיפה לכ-2 מיליון דולר) בתמורה לכך שלא ימכרו את המידע החסוי שאספו.

⁶ יצוין כי האמור לעיל מתייחס לחובות בתחום איסור הלבנת הון בלבד, ואין בו כדי למצות את כל הוראות הדין החלות על אירועי כופרה. כן, אין באמור כדי להוות אישור להעברת תשלום בגין מתקפת כופרה.

מגמות מרכזיות וטיפולוגיות להעברות כספים בגין מתקפות כופרה בארץ ובעולם

כאמור לעיל, חלק ניכר מתקיפות הכופרה מקורו בתוקפים מחוץ למדינה. לפיכך, הפצחנים המבצעים את התקיפה נדרשים להעברות כספים בינלאומיות, המבוצעות על פי רוב באמצעות נכסים וירטואליים. להלן יובאו דוגמאות לטיפולוגיות ודפוסים שזוהו בשנים האחרונות בתקיפות הכופרה שבוצעו בישראל ובעולם, הן על סמך ניתוח הדיווחים הבלתי רגילים שהתקבלו ברשות בחשד לפעילות הקשורה לתשלומים בגין כופרה והן על סמך מסמכים בינלאומיים בתחום. יצוין, כי חלק מטיפולוגיות אלו מאפיינות התנהלות פיננסית בהקשרי פשיעת סייבר ככלל ולא דווקא ייחודיות לתחום הכופרה.

1. שימוש בנש"פים המתמחים בתחום הקריפטו - מרבית הדיווחים הבלתי רגילים שהועברו לרשות בחשד לביצוע מתקפת כופרה, דווחו על ידי נש"פים המתמחים במסחר במטבעות וירטואליים, כאשר הקורבן ביקש לבצע באמצעותם את העברת המטבעות לתוקף.



2. שימוש של אזרחים זרים בנש"פים שאינם במדינת הקורבן - נוכח העובדה כי מדובר לרוב בפעילות מקוונת וניתן להעביר תשלומים מבלי הגעה פיזית לסניפים, אזי חלק מהקורבנות בעולם משתמשים בנש"פים ממדינות אחרות. כך, קונקרטיית בישראל, למעלה ממחצית מהדיווחים שהתקבלו ברשות בהקשרי כופרה עוסקים באזרחים זרים ממדינות שונות (לא זוהתה מדינה בולטת) אשר פנו לנש"פים ישראלים כדי לרכוש מטבעות קריפטו לשם העברתם לתוקפי כופרה (לרוב מדובר בסכומים קטנים של מאות עד אלפי שקלים בודדים).
3. שימוש בבלטפורמות בינלאומיות למסחר בקריפטו - להערכתנו, בדומה לנעשה בעולם, חלק ניכר מהתשלומים של קורבנות ישראלים מועברים לפצחן באמצעות גופים פיננסיים מחוץ למערכת הפיננסית הישראלית. הנתקף או מי מטעמו, רוכש נכסים וירטואליים באמצעות פלטפורמות מסחר בינלאומיות מקוונות ומעביר דרכן את

התשלום לפצחן. במקרים רבים הפלטפורמה הזרה אינה מפוקחת, ולפיכך הפעילות אינה מדווחת לרשות לאיסור הלבנת הון (FIU) במדינה בה פועלת הזירה. להבנתנו, ביצוע התשלום בפלטפורמה זרה נובע בין היתר מרצון הנתקף שלא לערב גורמים נוספים בישראל באירוע התקיפה ולפעול בפלטפורמה שאינה מדווחת כלל. לכך ניתן להוסיף מניעים כספיים, לאור עמלות נמוכות יותר בפלטפורמות זרות.

4. **שימוש בבלדרי כספים (Money Mules)** - כדי לטשטש את זהותו של מבצע העבירה, הפצחנים משתמשים לרוב בבלדרי כספים (כפי שפורט בהרחבה [בסקירת הרשות בנושא](#)). בחלק ניכר מהמקרים גורמים "משוטטים" (מקבלים עמלה בתמורה להעברה ואינם יודעים כי מדובר בכספי עבירה), אשר מקבלים את הכספים/ נכסים ווירטואלים, לעתים ממירים אותם, ומעבירים אותם ליעד הבא (לעיתים בלדר נוסף). זאת, כדי להקשות על הרשויות לאתר את נקודת היציאה של הכספים.

5. **תיווך באמצעות חברות לניהול משברים/ביטוח/עו"ד** - חלק מהנתקפים פונים לחברות ניהול משברים/הגנת סייבר, חברות ביטוח או משרדי עורכי דין (תוך ניצול החיסיון המשפטי בין עו"ד ללקוח) כדי שאלו יסיעו להם להיחלץ מתקיפת הכופרה באופן דיסקרטי. אותן חברות מסייעות במשא ומתן מול הפצחן (האקר) ולעיתים אף משלמות בשם הקורבן את תשלומי הכופרה למוסד הפיננסי ממנו נרכשים ומועברים תשלומי הכופרה. לפי [דו"ח FinCen](#), כ-63% מהדיווחים על כופרה הועברו על ידי חברות ניהול משברים,⁷ אשר סייעו לישויות אמריקאיות בהתמודדות עם תקיפת הכופרה, לרבות בהסדרת התשלום לפצחנים.

6. **שימוש בנכסים וירטואליים נפוצים אשר קל להמירם** - בכל הדיווחים הבלתי רגילים שהועברו לרשות התשלום לתוקף בוצע באמצעות ביטקוין. בפרסום של [FinCen](#) על מגמות בתחום הכופרה מציין הארגון, כי מרבית התשלומים שזיהו בוצעו באמצעות ביטקוין. במתקפות כופרה שבוצעו בעולם נעשה שימוש גם במטבעות וירטואליים המאפשרים אנונימיות גבוהה יותר ומקשים על התחקות אחר נתיב העברתם, כגון מונרו. מאידך, קיימת מגבלה בשימוש במטבעות אלו הכרוכה בזילות הנמוכה שלהם ובקושי להמירם למטבע פיזי בהשוואה לביטקוין. לפיכך תוקפים רבים מעדיפים לבקש מהישות המותקפת כי תבצע את תשלום הכופר בביטקוין. בד בבד, אנו מבחינים בניצנים ראשוניים בעולם של שימוש של פצחנים, לרבות בתחום הכופרה, ב-NFT⁸ כאמצעי נוסף להלבנת כספים שמקורם במתקפות כופרה.

7. **שימוש ב"מיקסרים", העברות מרובות ו-"Chain Hopping"** - על מנת לטשטש את נתיב העברת הכספים התוקפים מקפידים כי הכסף יעבור במספר "תחנות" עד לנקודת היציאה בה המטבעות הקריפטוגרפיים מומרים למטבע פיזי, על מנת להרחיק את הכספים מהתשלום המקורי בגין מתקפת הכופרה. פעילות זו מבוצעת בכמה דרכים: ביצוע העברות בין מספר רב של ארנקים באותו מטבע; העברת תשלום הכופר בין מספר מטבעות וירטואליים (Chain Hopping) עד לנקודת היציאה; העברת התשלום שהתקבל במטבע וירטואלי ב"מיקסר"⁹, במטרה לטשטש את מסלולו וייעודו.

8. **המרת הכספים למטבע פיזי בכופרה לא מפוקחת** - במקרים רבים נקודת היציאה בה נמשכו כספים ששולמו בגין מתקפת כופרה שבוצעה בישראל היא בורסת מסחר קריפטוגרפית הרשומה במדינה המוגדרת בסיכון גבוה להלבנת הון ומימון טרור, אשר הרגולציה בתחומה רופפת או בכופרה מסחר שאינה רשומה ואינה מפוקחת.

⁷ חברות ניהול משברים דיווחו ל-FINCEN כיוון שביצעו פעילות של המרת פיזי למטבע קריפטוגרפי (בשונה מבארץ, בה ביצוע פעילות כזו מצריך רשיון של נש"פ)

⁸ Non Fungible Token – NFT, "טוקן" ייחודי, לרוב בדמות קובץ דיגיטלי, שאין דומה לו בעולם וניתן להוכיח עליו בעלות בלעדית.

⁹ מיקסר (MIXER) - שירות מקוון שמטרתו לטשטש את מקורם של כספי קריפטו ע"י ביצוע מספר רב של העברות בפרק זמן קצר מאוד ("יערבו" שהכספים)."

9. העברה לארנקים "חד פעמיים" - כתובות הארנק אליהם מתבקשים הקורבנות להעביר את כספי הכופרה הינם עפ"י רוב חד פעמיים (Disposable) ומשמשים רק לצורך התקבול הספציפי עבור אותו אירוע כופרה ומשם המטבעות מועברות לארנקים נוספים.



10. שימוש של התוקף בבורסות מבוזרות (DeFi) - מניתוח שבוצע ברשות, כמו גם מניתוחים דומים בעולם, עולה כי תחנת המשיכה של כספי הכופרה הינה לעיתים תכופות בורסות מבוזרות¹⁰ (DeFi), אשר הפיקוח עליהם נוטה להיות רופף יותר.

11. שימוש בכרטיסי מתנה (Giftcards/Vouchers) - מחקר עדכני (2020) שנערך בהולנד תוך שימוש במידע ממשטרת הולנד על תקיפות כופרה שבוצעו במדינה, מעלה שימוש ניכר של הפצחנים בכרטיסי מתנה לשם הלבנת הכספים שהתקבלו ממתקפת הכופרה. במסגרת זאת, הפצחנים מבקשים מהקורבנות להעביר את התשלום באמצעות כרטיסי מתנה שניתן לרכוש באופן מקוון, אותם הפצחנים מוכרים, או לחלופין ממירים בחזרה בחנות המקוונת לכספים שמועברים לארנק דיגיטלי, או לעיתים מנצלים את היתרות בכרטיסים לרכישות של מוצרים ברי קיימא.

דוגמאות לדיווחים ופרשיות שנבדקו ע"י הרשות לאיסור הלבנת הון

ניתוח הדיווחים הבלתי רגילים שהועברו לרשות בהקשרי כופרה מעלה כי קיימת עירנות של המוסדות הפיננסיים לתופעה ולבעייתיות העולה ממנה. מוסדות פיננסיים רבים נוקטים משנה זהירות בנוגע למתן שירות בגין כופרה ואינם מאשרים ביצוע פעולות פיננסיות לצורך תשלום כופרה ומדווחים לרשות הן אם ביצעו את הפעולה והן אם סירבו לבצעה. להלן, דוגמאות למספר דיווחים שהועברו לרשות:

- לקוח זר ביצע רכישה של ביטקוין בסכום של כ-10,000 ₪ באמצעות כרטיס אשראי. מבדיקה שביצע המדווח עולה כי מכתובת הארנק שנתן הלקוח על מנת לקבל את המטבע הוירטואלי הועברו בעבר מטבעות וירטואליים לכתובת אחרת באירלנד, אשר ידועה ככתובת המעורבת בפעילות כופרה.
- מחשבון בנק של חברה המתמחה בניהול משברים בוצעה העברה של עשרות אלפי שקלים לחשבון נש"פ לצורך רכישת ביטקוין. לדברי הנש"פ, נציג חברת ניהול המשברים ציין כי חברה שהעסיקה את שירותיו הותקפה על ידי פצחן והביטקוין שנרכש ישמש לתשלום בגין מתקפת כופרה.
- עמותה הפקידה בחשבון אצל נש"פ עשרות אלפי שקלים. מבירור שערך הנש"פ מול נציג העמותה עלה כי מדובר באירוע כופרה עקב פריצה לאחד משרתי העמותה והיא מעוניינת לבצע רכישה של ביטקוין לצורך התשלום, לאחר שלדברי הנציג היא הונחתה לעשות כן ע"י המשטרה. הנש"פ לא אישר את הפעולה והכסף הוחזר לחשבון העמותה.
- בחשבון בבעלות בני זוג מבוגרים עלתה פעילות חריגה של העברות בסך עשרות אלפי שקלים מגורמים שונים ומשיכות מזומנים בסכומים דומים. בבירור מול בעלי החשבון עולה כי הם הופעלו כבלדרי כספים (Money Mules) על ידי האקרים רוסים שדרשו מהם למשוך את הכספים שמתקבלים לחשבונם ולהפקידם אצל נש"פ שירכוש מטבעות וירטואליים עבורם.



¹⁰ טכנולוגיה המספקת מגוון של מכשירים ושירותים פיננסיים אשר מבוצעים באמצעות בחוזים חכמים על גבי רשת הבלוקצ'יין ולא נסמכים על מתווכים פיננסיים "קלאסיים" דוגמת בנקים, נש"פים, חברי בורסה וכו'.

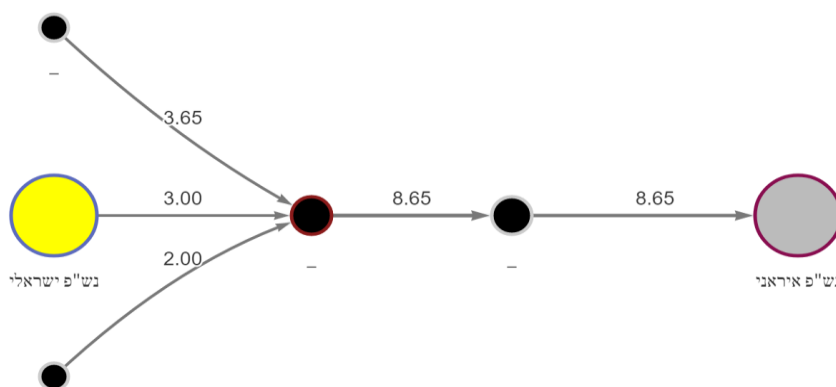
- לקוח (חברת ניהול משברים) ביצע רכישה של מטבע וירטואלי בעשרות אלפי שקלים. מבירור של הגוף הפיננסי מול הלקוח עלה כי הרכישה בוצעה לצורך תשלום עבור אנשים שנפגעו מכופרה ולעסקים שרוצים להחזיק מטבעות וירטואליים כאמצעי התגוננות למקרה שיעברו מתקפת כופרה.
- אזרח זר שמערכות המחשב שלו הותקפו על ידי האקרים ביצע מספר רכישות של מטבעות וירטואליים בסך של כ-100,000 ש"ח באמצעות כרטיס האשראי שלו לצורך תשלום כופר. הגוף המדווח ביצע בירור מול המשטרה על מנת לוודא את אמיתות המקרה וכן פנה לגוף בו מועסק האזרח הזר בכדי לקבל מכתב רשמי המאשר את העסקתו והצהרה לגבי מקור הכספים.

תשלום כופרה מיישות ישראלית לארנק דיגיטלי בבעלות גורם איראני

ברשות לאיסור הלבנת הון התקבל דיווח בלתי רגיל אודות חברה ישראלית שפנתה לצד שלישי במטרה שזה יסייע לה להיחלץ מאירוע כופרה אליו נקלעה. אותו צד שלישי רכש שלוש יחידות ביטקוין (בשווי של עשרות אלפי דולרים בעת הרכישה) אותם העביר לארנק הדיגיטלי של התוקף באמצעות נותן שירותים פיננסיים ישראלי.

בבדיקה שבוצעה ברשות לאיסור הלבנת הון עלה, כי הארנק אליו הועברו הכספים מוכר כקשור לאירועי כופרה. לאחר מכן (כפי שמופיע בתרשים) הועברו הכספים לארנק "צינור" (ארנק שמשמש אך ורק לקבלת כספים והעברתם לארנק אחר), אשר שימש גם כיעד לקליטת כספים נוספים בסך של 5.65 מטבעות ביטקוין החשודים כתשלומים בגין כופרה שבוצעה מחוץ לישראל. מארנק הצינור הועברו כלל הכספים לארנק שזוהה כזה המצוי בבעלותו של נש"פ איראני.

יצוין, כי פרטי האירוע הועברו לגופי הבטחון הרלבנטיים בישראל לשם המשך בדיקה.



דגלים אדומים - איתור ומניעת הלבנת הון באמצעות תשלומי כופרה

RISK



הדגלים האדומים המפורטים מטה נועדו לאפשר לזהות פעילות אשר יתכן והיא קשורה לתשלומים בגין כופרה ולהעביר דיווח בגינה לרשות. כמו כן, דגלים אדומים אלו נועדו לחזק את ההיכרות והמודעות הציבורית לתופעה ומאפייני הפעילות הפיננסית הקשורים עמה.

יובהר, כי דגל אדום בא להצביע על אפשרות קיומה של פעילות כופרה, אך **אין בקיומו כדי להעיד כי בהכרח מבוצעת פעילות זו**. ככל שקיימים דגלים רבים יותר כן גובר החשש כי מדובר בפעילות בעלת זיקה לאירוע כופרה. יודגש, כי הרשימה שלהלן אינה מהווה רשימה מלאה או סגורה.

כתובת ארנק חשודה - הלקוח מבקש להעביר את המטבע שרכש לטובת ארנק המסומן במערכות ככזה המעורב בפעילות כופרה (רשימות סנקציות, מאגרי מידע של חברות מודיעין עסקי וכו').

העברה לארנק "חד-פעמי" - כפי שעולה גם **מדו"ח FATF**, העברה לארנק שבניתוח פרופיל הפעילות שלו לא נצפו עד כה העברות יכולה להיות אינדיקציה לכך כי מדובר בארנק שנפתח לשם קבלת כספי כופרה.

שימוש במתווך:

- פניה של חברת ניהול משברים/חברת סייבר/משרד עו"ד/חברת ביטוח לצורך רכישת מטבע קריפטוגרפי עבור צד ג'. קיים חשש כי הרכישה מבוצעת עבור קורבן מתקפת כופרה (עם/בלי הצהרה בדבר מהות הפעולה ו/או הגורם עבורו מבוצעת הפעולה).
- עסקה חריגה בין ארגון לחברות לניהול משברים, משרד עו"ד או חברות המתעסקות בטיפול באירועי סייבר אשר עשויה להעיד כי הארגון הותקף בכופרה.
- חברת סייבר/ניהול משברים מבצעת העברה יוצאת למוסד פיננסי אשר מבצע תשלומי קריפטו זמן קצר לאחר שקיבלה לחשבונה סכום זהה/דומה.

מידע שנמסר ע"י הלקוח - לעיתים הלקוח מספק למוסד הפיננסי מידע המרמז כי פעולותיו בחשבון מבוצעות בגין תשלום עבור כופרה. בהקשר זה, FINCEN ממליץ לבקש מהלקוחות פרטים רבים ככל הניתן במסגרת ה-KYC (הכר את הלקוח) בבואם לבצע העברות במטבעות קריפטו (בייחוד אם זו עסקה ראשונה שלהם).

חוסר היכרות של הלקוח עם מטבעות וירטואליים - לקוח שנראה כבעל ידע מוגבל בכל הקשור למטבעות וירטואליים מבקש לבצע רכישה בסכום גבוה.

שימוש באמצעים טכנולוגיים לביצוע פעולה באופן אנונימי - לקוח אשר מבקש לדוגמא לבצע פעולה ומעביר את ההוראה באמצעות רשת מקוונת מוצפנת (TOR וכו').

תחושת לחץ/דחיפות של הלקוח - לקוח לוחץ על נותן השירות להשלים את ההעברה באופן מיידי ומוכן לשלם עמלות גבוהות יחסית יותר בגין ביצועה המהיר.

עסקה חריגה/חד-פעמית - הלקוח מבצע רכישה חריגה או חד פעמית במטבעות וירטואליים.

העברות במטבעות קריפטוגרפיים למדינות בסיכון גבוה - ניטור בדיעבד של ההעברה בבלוקצ'יין מראה כי הכספים הגיעו לארנקים המנויים **בפרסום הרשות** כמדינות בסיכון או למדינות נוספות הנחשבות למובילות בעולם בביצוע תקיפות כופרה.

העברות למדינות שללקוח אין קשר פיננסי עימן - דו"ח FATF מציינ כדגל אדום העברת כספים לנותן שירותים פיננסיים בנכסים דיגיטליים במדינה שללקוח אין קשר אליה (פעילות עסקית, משפחה וכו').



- 🚩 **שימוש במיקסרים** - כאשר ניטור בדיעבד של ההעברה ברשתות מבוזרת (דוגמת הבלוקצ'יין) מראה כי הכספים מועברים דרך מיקסרים.
- 🚩 **העברות מרובות בפרק זמן קצר של מטבעות וירטואלים לארנק** של לקוח בלא הסבר למקור הכספים (למשל במקרים בהם הלקוח מובטל, או בעל הכנסה נמוכה).
- 🚩 **"ריקון חשבון"** - כאשר לקוח חדש מעביר את כלל יתרת הנכסים הדיגיטליים בחשבונו ליעד אחר.
- 🚩 **שימוש/המרה למטבעות בעלי אנונימיות גבוהה** - לקוחות המבקשים לרכוש, ללא סיבה נראית לעין, מטבעות פחות סחירים המתאפיינים באנונימיות גבוהה דוגמת מונרו.
- 🚩 **שימוש במילים חשודות בתיאור ההעברה** - כאשר הלקוח מבקש להוסיף למלל המצורף לתיאור ההעברה מילים המרמזות על אפשרות לאירוע החשוד כמתקפת כופרה (לדוגמא - בעבור מידע במחשב, הסדרת/השבת מאגרי מידע וכו').