**דף פתיחה :**

**שמות מלאים :**

1. אריאל קרביצקי , מס ת.ז : 039678024.
2. יובל חשמונאי , מס ת.ז : 204404669.
3. גיא כהן , מס ת.ז : 313189466.

**נושא :**

**"ווירוס כופר"**

****

**מקורות מידע :**

1. ויקיפדיה
2. <https://www.eset.co.il/support/kb/ransomware-protection-home-guide>
3. <https://www.ransomware.co.il/>
4. <https://www.webfocus.co.il/%D7%95%D7%99%D7%A8%D7%95%D7%A1-%D7%9B%D7%95%D7%A4%D7%A8.html>
5. <https://www.y4pc.co.il/04-16-news/new-ransomware-locky.html>

**ווירוס כופר**

**התופעה מוכרת שנים רבות, אך רק לאחרונה, (החל מ- 2014 ואילך) התופעה החלה לצבור תאוצה והפכה למכה של ממש.  
מהי תוכנת כופר?  או וירוס כופר?  כיצד אפשר להימנע מלהיפגע?   כיצד ניתן לשחזר ולהציל קבצים שנדבקו והוצפנו ?   ומה זו בכלל הצפנה ?**  
האקרים יוצרי הווירוסים, כדוגמת CryptoWall 3.0 virus ואחרים)  ידרשו מהנפגע כסף, ולא מעט).   הכופר מתחיל ממאות דולרים, ולאחר זמן קצוב, מוכפל...  
תשלום להאקרים, שמתבצע באמצעות המטבע הווירטואלי ביטקויין, לא מבטיח שתקבלו את קוד השחרור, לרוב כן נשלח קוד לשחרור ההצפנה, אך במקרים לא מועטים, הקוד לא נשלח כלל.  
יתרה מכך ויש לקחת בחשבון - אישית כשעזרתי לנפגעים (מקרב מכריי) נתקלתי לא פעם במצב שתוכנת ההצפנה לאחר הכנסת הקוד הנכון, פתחה את ההצפנות מהקבצים, אך קבצי WORD, EXCEL ואחרים, הפכו לבלתי קריאים, בשפת העם... הפכו לג'יבריש.  
יותר ויותר משתמשים, פרטיים, עסקים וחברות נפגעים, וכבר בתחילת המאמר - אין בפי בשורות "טובות" למי שנפגע מווירוס כופר, אך יש אור בקצה המנהרה.

**מהו ווירוס כופר**

וירוס כופר הינה תוכנה זדונית שהגיעה ונכנסה אל המחשב שלכם, ומרגע שהיא הופעלה, התוכנה סורקת אחר תיקיות הקבצים במחשב, ומצפינה את הקבצים, בדר"כ ברמת הצפנה גבוהה במיוחד - 2048 ביט.  
ברגע שקובץ הוצפן, לדוגמא:  קבצי WORD, תמונות, מצגות POWER POINT, קבצי OFFICE שונים, קבצי מוזיקה MP3 וכ"ו.. אין אפשרות לפתוח אותם אלא אם כן יש ברשותכם תוכנה לפתיחת ההצפנה וכמובן, הקוד לשחרור.  (קוד שחרור נקרא גם מפתח הצפנה)  
הצפנה ברמה של 2048 ביט, כמעט ובלתי ניתנת לפריצה, ורק מעט ארגוני ממשל בעולם, מחזיקים בכלים שמסוגלים לפרוץ הצפנה ברמה של 2048 ביט.  
וירוס הכופר, יצפין קבצים בתיקיות שונות במחשב ובכוננים המחוברים למחשב, לרבות כוננים בחיבור USB, התקני DISK ON KEY ואף כונני רשת.

**כיצד הווירוס עובד?**

מיד עם ההדבקה, הווירוס ייצר 3 קבצים בסיומת EXE (קובץ תוכנה) וישתול את הקבצים במספר תיקיות במחשב. תחת( %user% ) כולל גם ב Startup של מערכת ההפעלה.  וזאת ע"מ שאם תכבו את המחשב, מיד בהדלקה הווירוס יחזור לחיים וימשיך להצפין תיקיות וקבצים נוספים.  
הווירוס בנוסף מבטל ופוגע ב- Windows system restore - תוכנת (קבצי) הגיבוי והשחזור של ה Windows.

**כיצד הגיע ווירוס כופר למחשב שלי?**

תוכנת הכופר לרוב תופעל במחשב הנגוע עקב טעות אנוש של המשתמש!   הדרכים שבהם נדבקים לרוב בווירוס כופר, הן:

1. כניסה לאתר אינטרנט נגוע, וביצוע פעולה באתר, לחיצה על קישור, על כפתור, על פרסומת - שמבצעת הורדה של קובץ הווירוס כופר למחשב והפעלתו.  
   בשנת 2015 ידוע על מעל 40,000 אתרים ודומיינים נגועים שמפיצים את הווירוס כופר
2. קבלת קובץ וירוס באמצעות הודעת דוא"ל, תפתה אתכם לפתוח את הקובץ שיראה כמו עוד מצגת טיולים לחו"ל או סרטון מצחיק אחר.
3. המחשב פתוח להתחברות מרחוק ( Remote Desktop Connection )  ללא הצפנה מספקת או רמת אבטחה מספקת, מאפשר לאותם מפיצי הווירוס השתלטות מרחוק על המחשב ושתילת הקובץ.
4. הורדה של תוכנה פיראטית, או קבצי CRACK - תוכנות קטנות שנועדו לפרוץ לתוכנות אחרות ע"מ לא לשלם עבורן...  
   לדוגמא: גולש רוצה להתקין על המחשב את Adobe Photoshop - תוכנת עיבוד תמונה וגרפיקה יקרה - הפתרון הקל והמסוכן - הורדת התוכנה המלאה מאתר חברת Adobe, תוכנה שמאפשרת 30 ימי התנסות... ולאחר ההתקנה, הורדת תוכנת Crack - תוכנה שמפצחת את מנגנון ההגנה של ה Photoshop ופותחת את התוכנה כזו ללא תקופת ניסיון.  כאילו נרכשה במלואה.  
   קבצי ה Crack שמופצים באלפי אתרים, חלקם הגדול נגוע בווירוסים, לרבות וירוס כופר.
5. במחשב אין תוכנת אנטי וירוס או שיש תוכנת אנטי וירוס ישנה ולא מעודכנת.
6. גלישה ל[אתר פישינג](https://www.webfocus.co.il/%D7%90%D7%AA%D7%A8-%D7%A4%D7%99%D7%A9%D7%99%D7%A0%D7%92.html), שהגולש חשב לתומו שמדובר באתר שאליו הוא רגיל לגלוש, לחיצה על קישור / הפעלה של אופציה באתר, תדביק את המחשב בתוכנת כופר.
7. גלישה לאתר לא מוכר, ולחיצה על חלון הודעה שמודיע לדוגמא:  "לחץ כאן לעדכון תוכנת ה FLASH"... או "הורד עדכון למערכת ההפעלה" וכ"ד....(כמובן, שההודעות יהיו באנגלית(.

# ווירוס הכופר **Locky** :

## מי הוא ווירוס הכופר Locky ולמה הוא גורם:

Locky התגלה לראשונה בפברואר 2016 והיוצר של הווירוס הצליח עד עכשיו להפיץ אותו ברחבי העולם בהצלחה רבה. הפצת הווירוס נעשית על ידי שליחת אימייל אשר מושך את המשתמש לפתוח קובץ מסוים (בדרך כלל זה הוא קובץ מסוג Word), או דרך כל מיני אתרים מפוקפקים שקיימים ברשת.

חברות אבטחה גדולות כמו: נורטון Norton ומקאפי McAfee אשר מספקות מגוון תוכנות הגנה למחשב, מעידות על כך שמחודש פברואר 2016 יש עלייה במתקפות כופר של וירוס הכופר Locky. החברות טוענות שמספר רב של מחשבים נלקחים כבני ערובה והן מתאמצות לאסוף את כל החומר והמידע שיש להן על הווירוס החדש. כל זאת נעשה בכדי לפתח כמה שיותר מהר פתרונות ואמצעי מניעה לווירוס הכופר.

בגרף הבא של חברת נורטון, ניתן לראות את מהירות ההתפשטות של וירוס הכופר Locky לאחר שהתגלה בחודש פברואר 2016. אפשר לראות שיש עלייה חדה בגרף הנפגעים מחודשים פברואר, מרץ והלאה.

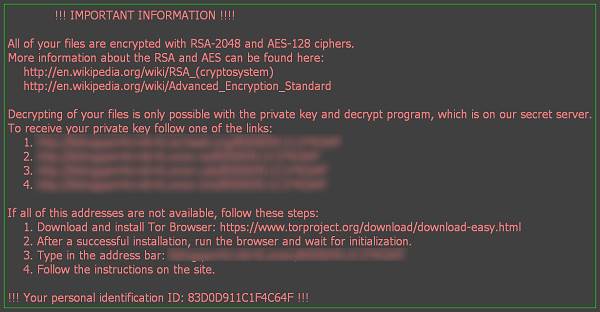


וירוס הכופר Locky מצפין (נועל) את הקבצים אשר נמצאים במחשב ומשנה את הסיומת שלהם ל- **Locky.** לאחר מכן הם דורשים מהמשתמש לשלם בין 0.5 ל- 1 [ביטקוינים](https://www.y4pc.co.il/bitcoin.html) (שזה יוצא בערך בין 200$ ל- 400$) רק בכדי לשחרר את הקבצים שננעלו ולהחזיר אותם להיות תקינים כבעבר

נכון לעכשיו, אין שום דרך אחרת להסיר את הווירוס מהמחשב ולהחזיר את הקבצים לקדמותם. כנראה שהנפגע יצטרך לשלם את דמי הכופר, מפני שאם הוא לא ישלם את דמי הכופר אז הוא יסתכן בכך שכל המידע שלו יימחק (אם הוא לא גיבה את הקבצים לפני כן) והוא אינו יוכל [לשחזר את הקבצים](https://www.y4pc.co.il/deleted-files-restore.html).

וירוס הכופר אינו מצפין רק את הקבצים שנמצאים בכונן C (הכונן בו מותקנת מערכת ההפעלה), אלא הוא גם מצפין את כל הכוננים החיצוניים והזיכרונות הניידים (Disk On Key) אשר מחוברים למחשב באותו זמן. הווירוס גם תוקף את כל המחשבים אשר נמצאים ברשת של המחשב המותקף, כלומר: אם המחשב שלכם נמצא בתוך רשת משרדית או ביתית ובתוכה ישנם 5 מחשבים, אז יש סיכוי גבוה שכל חמשת המחשבים יידבקו בווירוס.

הווירוס יודע ויכול להתקיף מחשבים אשר מריצים מערכות הפעלה מסוג ווינדוס Windows, לינוקס Linux ואפילו גם OS x של אפל. כך שאין ספק שהוא נחשב לאיום גדול לכל המשתמשים הביתיים, לעסקים הקטנים וגם לעסקים הגדולים.



**דוגמא להודעה שנשלחה למשתמש אשר נפגע מווירוס הכופר Locky**

## האם יחזירו לי את הקבצים כאשר אשלם את הכופר ?

אם הקבצים שלכם באמת חשובים ולא גיביתם אותם לפני כן, אז כנראה שאין ברירה אחרת. אך שימו לב **שאנו לא ממליצים לשלם את דמי הכופר** מפני שמהלך זה יעודד את יוצרי הווירוס להמשיך ולהפיץ אותו שוב ושוב. קחו גם בחשבון שאם תשלמו את דמי הכופר, ישנה אפשרות גדולה שיגנבו לכם את פרטי החשבון אשר שילמתם דרכו.

אם הקבצים שהצפינו לכם, אינם חשובים כל כך אז אתם יכולים להיפטר מהווירוס בכך שתפרמטו את המחשב ולאחר מכן תתקינו מחדש את כל [התוכנות המומלצות](https://www.y4pc.co.il/format-softwares.html) למחשב לאחר פרמוט.

## כיצד להימנע ולהגן על המחשב מפני וירוס הכופר החדש Locky

בכדי להגן על הקבצים החשובים לכם מפני וירוס הכופר החדש, אנו ממליצים לבצע מספר פעולות:

**1.** התקינו תוכנת [אנטי וירוס](https://www.y4pc.co.il/anti-virus.html) במחשב והקפידו שהיא תהיה תמיד מעודכנת.

**2.** מומלץ להתקין במחשב [תוכנת אנטי רוגלה](https://www.y4pc.co.il/malwarebytes.html) ומידי פעם לבדוק שהיא מבצעת עדכונים כנדרש.

**3.** מומלץ להתקין במחשב תוכנת חומת אש.

**4.** אל תפתחו ותקראו אימיילים ממקורות שאינכם מכירים, פשוט אל תתפתו לפתוח מיילים שמתחילים במילים כמו **"קבלה על הרכישה שביצעת"** או **"מצורף למייל הקובץ שביקשת"**. בדרך כלל, וירוס הכופר Locky מפיץ את עצמו דרך מסמך וורד Word שמצורף למייל. מעבר לכך, יכול לקרות מצב שבו מפיץ הווירוס מתחזה למישהו אחר וכתובת האימייל שלו תהיה דומה לכתובת אימייל של אתר מוכר, כמו פייסבוק או גוגל.

**5.** גבו מידי יום את הקבצים שלכם ! אנו מאוד ממליצים לגבות תמונות, מסמכים, שירים וסרטונים לכונן אחסון חיצוני. לאחר שסיימתם לגבות את כל הקבצים החשובים, נתקו את הכונן מהמחשב. כמו שאמרנו קודם לכן, הווירוס יודע גם לתקוף כונני גיבוי חיצוניים אשר מחוברים למחשב.

**6.** תמיד תהיו זהירים וחשדניים כאשר אתם גולשים באינטרנט. וירוס הכופר מושתל גם בתוך פרסומות שמגיעות ממקור לא אמין וכאשר תקליקו עליהן, אתם עלולים להידבק בווירוס.

## כיצד ניתן להסיר מהמחשב את ווירוס הכופר Locky

לא התגלתה עד עכשיו תוכנה או שיטה יעילה להסרת תוכנת הכופר. אך תמיד אפשר לנסות ולסרוק את המחשב באמצעות תוכנת האנטי רוגלה.