06 אוגוסט 2019
ה' אב תשע"ט
סימוכין:ב-ס-980

# התמודדות עם נוזקה מסוג כופרה - Ransomware

## תקציר

1. כופרות הן נוזקות המונעות מהמשתמש גישה לקבצים או ציוד שברשותו, בדרך כלל באמצעות הצפנת המידע, ודורשות מהמשתמש לשלם דמי כופר תמורת החזרת היכולת להשתמש בקבצים או בציוד.
2. מטרת מסמך זה לסקור את נושא הכופרות, להמליץ כיצד להיערך טרם אירוע כופרה, ולסקור את האפשרויות העומדות בפני משתמש או ארגון שהותקפו באמצעות כופרה.

## פרטים

### מה היא כופרה?

1. כופרה (Ransomware) היא סוג של נוזקה המשמשת לסחיטת המשתמש לתשלום כסף (דמי כופר), בדרך כלל באמצעות הגבלת גישה למערכות מחשב או לקבצי מידע. חלק מתוכנות הכופרה מבצעות הצפנה לקבצים על הכונן הקשיח, ובכך הופכות את תהליך הסרת ההצפנה שלא בדרך של תשלום הכופר, לקשה. תוכנות כופרה אחרות נועלות את המערכת ומציגות הודעת שווא כי לא ניתן לגשת לקבצים, על מנת לתעתע במשתמש ולהמריצו לשלם. בנוסף, קיימים סוגי כופרה שמטרתם למנוע גישה לציוד קצה מסוים (טלפון נייד, מחשב).
2. תוכנות כופרה יכולות להצפין בנוסף לקבצים בתחנת העבודה המותקפת, גם כל קובץ שנמצא בכונן משותף מחלקתי או ארגוני ברשת הארגונית, וכן בהתקן אחסון המחובר למחשב. חלקן יודעות לבצע תנועה רוחבית בין עמדות ברשת.

3. לאחר תהליך ההצפנה, תוצג למשתמש הודעה כי עמדתו הותקפה והקבצים הוצפנו. בנוסף יוצג מידע כיצד ניתן ליצור קשר עם התוקפים, לטובת תשלום דמי הכופר באמצעות מטבעות וירטואליים, וקבלת אמצעי הפענוח. התוקפים מבטיחים לבעלי המידע כי יעבירו לידיהם את האמצעי לשחזור הקבצים (מפתח הפענוח או תוכנת פענוח), תמורת תשלום דמי כופר.

## וקטור כניסה

1. דואר אלקטרוני - השיטה הנפוצה ביותר היא שימוש בדואר אלקטרוני המכיל צרופה שנראית תמימה, או קישור לאתר המתחיל את תהליך ההדבקה בכופרה.
2. הורדת קבצים - הפניה לאתר אינטרנט שמכיל נוזקות המנצלות פרצות אבטחה בדפדפנים להדבקת העמדה בכופרה.
3. תוכנות חינמיות - הצעת תוכנות חינמיות, אשר הפעלתן על ידי המשתמש תגרום להדבקת העמדה בכופרה.
4. RDP - חיבור מחשב מרחוק - השתלטות על מחשב אשר פתוח לחיבור מרחוק והדבקתו בכופרה באמצעות חיבור זה.

## מאפייני הדבקה בכופרה

להלן מספר מאפיינים עיקריים המצביעים על הדבקות בכופרה:

1. אין אפשרות לפתוח קבצים ובעת פתיחת קובץ מתקבלת הודעת שגיאה על כך שהקובץ פגום או שהסיומת שלו שגויה.
2. תמונת הרקע של שולחן העבודה מוחלפת בהודעת איום עם הנחיות לתשלום דמי הכופר לטובת שחרור הגישה לקבצים. לעתים בהודעה מופיעה ספירה לאחור עד המועד בו דמי הכופר יגדלו או המועד שלאחריו לא ניתן יהיה לשחזר הקבצים כלל.
3. נפתח חלון שהמשתמש אינו יכול לסגור.
4. בספריות שונות מופיעים קבצים בעלי שמות כגון "כיצד לפענח הקבצים" או "הוראות לפענוח הקבצים".

## דרכי התמודדות עם כופרה

במקרה שזוהתה התקפת כופרה, מומלץ לפעול על פי ההמלצות הבאות:

1. ניתוק המחשב הנגוע מכל הרשתות שאליהן הוא מחובר, כולל רשתות קוויות ואלחוטיות כגון Wi-Fi או Bluetooth. ניתוק כל הרכיבים החיצוניים המיועדים לאחסון קבצים או התקני זיכרון נייד. המטרה היא למנוע ככל האפשר התפשטות של הכופרה באמצעות רשתות אלו לעמדות נוספות.
2. הימנעות מביצוע פעולות כלשהן על המחשב הנגוע- בשלב זה אין למחוק קבצים, להפעיל כלי ניקוי דיסק או סריקות אנטי-וירוס.
3. הבנת היקף הפגיעה - ביצוע סריקה לבירור כמות הקבצים שהוצפנו וסוגיהם. מומלץ לבדוק ב-Registry, או בקבצים מסוימים שם הכופרה שומרת בדרך כלל את רשימת הקבצים שהוצפנו על ידה.

   בדקו האם לעמדה שהותקפה יש גישה ל:

   - תיקיות משותפות (Shared Folders)
   - כוננים קשיחים חיצוניים
   - אמצעי אחסון רשתיים
   - התקני זיכרון נייד (Disk On Key)
   - אמצעי אחסון בענן ( DropBox, Google Drive, Microsoft OneDrive/Skydrive וכד')

   והאם קבצים על אמצעים אלו הוצפנו.
4. בדקו באיזה סוג של כופרה מדובר- במידה וקיימים פרסומים ברשת לגבי סוג הכופרה, ניתן ללמוד מהם את היקף התקיפה הצפויה ומאפייני ההתפשטות השונים כגון:
   - סוגי קבצים מוצפנים
   - האם מבוצעת תנועה רוחבית והצפנת קבצים ברשת או באזורי אחסון משותפים
   - האם מבוצעת גישה לשירותי ענן

עבור משפחות מסוימות של כופרות, קיימים כלי פענוח או שמפתח פענוח פורסם על ידי גורמים שונים, כגון סוכנויות אכיפת חוק או חברות אבטחה שחקרו כופרות אלו. ניתן לחפש מידע זה באתרים שונים המרכזים מידע

על כופרות, ואף עשויים להציע אפשרויות שונות לשחזור קבצים מוצפנים. ניתן לחפש אחר הנחיות באתר אשר הוקם בשיתוף משטרת ישראל: https://www.nomoreransom.gov.il.

יש לשים לב כי משפחות כופרה מתעדכנות באופן תדיר, כך שתוכנה או מפתח פענוח שהיו זמינים עבור גרסה מסוימת, עלולים לא להועיל לגרסאות מתקדמות יותר.

אם הדבר אפשרי, מומלץ לבצע פענוח קבצים במערכות הארגוניות, משום שפענוח הקבצים באמצעות שירותים חיצוניים, יחשוף את תוכן הקבצים לספק השירות.

5. החליטו על צעדי המשך- לאחר שידועים סוג הכופרה, סוגי הקבצים שהוצפנו וכמה קבצים נפגעו, ניתן לבחון את האפשרויות העומדות בפניכם:
   1. שחזור הקבצים מגיבוי- במקרה שקיימים קבצי גיבוי עדכניים, מומלץ לבחון האפשרות לשחזר את הקבצים מגיבוי.
      בדקו בנוסף גם את ה- Shadow Copies (העתקי צל) שיוצרת מערכת ההפעלה. כאשר מערכת ההפעלה Windows יוצרת Restore Point לצורך שחזור, היא מייצרת Snapshot (תמונת מצב) של הקבצים ב-Volume. קיימות תוכנות ייעודיות היודעות לקרוא העתקים אלו ולשחזר מהם קבצים.
   2. ניסיון לפענוח הקבצים המוצפנים, על ידי שימוש בתוכנה או שירות צד ג'-
      עדיף להשתמש בכלי כזה רק לאחר בדיקה באמצעות מספר מנועי אנטי-וירוס שהכלי אינו מכיל בעצמו נוזקה. בנוסף, מומלץ לבצע הפענוח באופן עצמאי במערכותיכם, על מנת למנוע הגעת העתק מפוענח של הקבצים לספק השירות.
   3. לא לעשות דבר- לוותר על גישה ושימוש בקבצים בשלב זה, לגבות את הקבצים המוצפנים ולקוות כי בעתיד יימצא עבורם מפתח הפענוח או יפורסם כלי המאפשר את פענוחם.

בכל המקרים המתוארים לעיל, יש להסיר את נוזקת הכופרה עצמה. לשם כך ניתן להשתמש בתוכנות אנטי-וירוס המזהות את הכופרה על

מנת להסירה, אך עדיף לפרמט ולהתקין מחדש את העמדה, זאת על מנת לוודא כי הנוזקה הוסרה לחלוטין.
בנוסף, יש לנסות ולאתר את וקטור התקיפה, ולטפל בו למניעת תקיפה חוזרת.

ראו רשימת תיוג לפעולות השונות בנספח א'.

## כיצד למנוע הדבקה?

1. מומלץ להתקין בהקדם האפשרי עדכוני אבטחה שמפרסמים יצרני מערכות ההפעלה והיישומים השונים הפועלים במערכותיכם. התקנת העדכונים, מפחיתה את אפשרויות התקיפה של נוזקות הכופרה (Surface Of Attack), ומקטינה את היכולת שלהן להצליח בשלב ההדבקה הראשוני.
2. מומלץ להסיר תוכנות שאינן בשימוש, זאת על מנת למנוע שימוש בחולשות בתוכנות אלו לצורך תקיפה.
3. מומלץ לגבות באופן קבוע את קבצי המידע, רצוי ביותר משיטה אחת (כונן חיצוני, התקן נייד, גיבוי לענן, גיבוי רשתי וכד'). מומלץ לוודא כי מעת לעת חלק מקבצי הגיבוי נשמרים באופן שאינו מקוון (Offline), כך שאינם נגישים לכופרות.
4. מומלץ להגביל את סוגי הצרופות שניתן לשלוח אל משתמשי הארגון, למינימום הנדרש לפעילות העסקית התקינה של הארגון (Whitelist). ניתן לבחון שימוש בעמדות הלבנה המנטרלות קוד עוין אם קיים בקבצים, או בודקות באמצעות מספר שיטות הימצאות קוד מסוג זה. אם נעשה שימוש בעמדות אלו, יש לוודא כי כל קובץ המוכנס לרשת הארגון, ללא תלות באופן הכניסה (דוא"ל, הורדה מהרשת, החסן נייד, DVD/CD וכד'), עובר דרכן טרם הגעתו לרשת הפנימית.
5. מומלץ להפעיל שיקול דעת לפני פתיחה של צרופה או הפעלת קישור בהודעות דוא"ל, וכן במסרים ברשתות חברתיות, אתרים מקצועיים וכד'. במקרה של הודעה ממקור בלתי צפוי, או אף הודעה בלתי צפויה ממקור מוכר, מומלץ לא לפתוח את הקישור/ צרופה,

ולוודא מול הגורם השולח, בערוץ תקשורת שונה, האם אכן שלח את ההודעה.

6. במקרים בהם מופיעה התרעה ממקור כלשהו (מערכת ההפעלה, יישום, אנטי-וירוס וכד') לגבי חשד לשימוש לא ראוי בצרופות, מומלץ לא לאשר את פתיחת הקובץ ויש לדווח לגורמי אבטחת המידע הארגוניים.
7. מומלץ לפתוח מסמכי Office מרשת האינטרנט רק כאשר הפעלת Macros מנוטרלת, ותחת Protected View. יש לחשוד בכל מסמך או הודעה המנסים לשכנע את המשתמש להסיר אמצעי הגנה אלו.
8. אם הדבר אפשרי מבחינה עסקית, מומלץ לנטרל הפעלת קוד JavaScript בקורא קבצי PDF.
9. אם אינכם עושים שימוש בסקריפטים שונים מבוססי VBS או JavaScript, ניתן לשקול לנטרל את רכיב ה-Windows Scripting Host. **יש לבחון הגדרות אלו בסביבת ניסוי טרם הטמעה בסביבת ייצור.**
10. מומלץ לשקול להתקין כלים העושים שימוש בשיטות הונאה (Deception), אשר עשויים להסיט את פעולת הכופרה אל מטרה שהוכנה לשם כך מראש, ובכך לזהותה.
11. מומלץ להימנע מלתת למשתמשים הרשאות מנהלן מקומי (Local Administrator).
12. מומלץ לעשות שימוש במערכות כגון LAPS, המנהלות את חשבונות המנהלן המקומי בעמדות בצורה מרוכזת, מגדירות סיסמה שונה לכל אחת מהעמדות, ומחליפות את הסיסמה באופן אוטומטי מעת לעת. לפרטים נוספים ראו את פרסומנו בנושא https://www.gov.il/he/Departments/publications/reports/campaignil
13. מומלץ להגדיר את ארכיטקטורת הרשת כך שעמדות קצה יוכלו לתקשר אך ורק עם שרתים ושירותי רשת מרכזיים, ולא ישירות עם עמדות קצה אחרות ברשת. **יש לבחון ארכיטקטורה זו בסביבת ניסוי טרם הטמעה בסביבת ייצור.**

14. מומלץ לבחון את הצורך העסקי בגישה מרחוק למערכות ארגוניות, ולאפשר זאת רק עבור עמדות או משתמשים אשר זקוקים לכך. מומלץ לא לחשוף עמדות נגישות מרחוק ישירות לרשת האינטרנט, אלא לאפשר גישה אליהן באמצעות תשתית VPN ארגונית הכוללת הצפנה מתאימה והזדהות חזקה.
15. מומלץ לעשות שימוש במנגנונים שונים של מערכת ההפעלה, כגון Application Whitelisting, Attack Surface Reduction (ASR), Exploit Guard וכו', על מנת למנוע הרצת והפעלת תוכנות לא מוכרות בעמדות הקצה. יש לבחון הגדרות אלו בסביבת ניסוי טרם הטמעה בסביבת ייצור.
16. מומלץ להעביר הכשרות מתאימות למשתמשים מהי כופרה ומהם הסימנים המעידים על הימצאותה. בנוסף, מומלץ לבחון שימוש בתוכנה או שירות המדמים התקפת כופרה, על מנת לתרגל את המשתמשים בפועל.
17. מומלץ לבחון ולעדכן את מסמכי הארגון בנושא המשכיות עסקית והתאוששות מאסון, וכן לתרגל תרחישים בנושא זה באופן עיתי.

## מקורות

1. https://nomoreransom.gov.il/
2. https://www.nomoreransom.org/

לכל מידע נוסף ניתן לפנות אלינו. במידה שעלו ממצאים בבדיקתכם, נבקש לקבל היזון חוזר.

שיתוף מידע עם הCERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כלשהו, במידה שהתגלה צורך כזה

בברכה,
CERT-IL

## נספח א' - רשימת תיוג להתמודדות עם התקפת כופרה (Checklist)

1. ניתוק

☐ נתק את המחשב מהרשת

☐ נתק את כל הרשתות האלחוטיות: Wi-Fi, Bluetooth, NFC

2. בדיקת היקף ההדבקה

בדקו האם קיימים קבצים מוצפנים, בכל אחד מהמיקומים הבאים:

☐ כוננים מקומיים (אם נגישים)

☐ כוננים ממופים או משותפים

☐ התקני אחסון רשתיים

☐ כוננים חיצוניים

☐ התקני זיכרון נייד מכל סוג שהוא (DOK, טלפונים, מצלמות וכד')

☐ אחסון מבוסס ענן

☐ אם ניתן, אתרו את הקובץ בו הכופרה רושמת את רשימת הקבצים שהוצפנו

3. זיהוי סוג הכופרה

☐ זהו את סוג הכופרה באמצעות מידע זמין ברשת ובאתרים ייעודיים כגון NoMoreRansom

4. בחירת תגובה

4.1. שחזור מגיבויים

מצאו את כל צורות הגיבוי של הציוד הזמינים לשימוש

☐ גיבוי חיצוני

☐ גיבוי רשתי

☐ גיבוי ענן

☐ העתקי צל (Shadow Copies)

☐ וודאו כי הגיבויים תקינים והמידע עדכני

- ☐ גבו את הקבצים המוצפנים (למקרה של שיבוש בתהליך השחזור)
- ☐ הסירו את הכופרה ושחזרו המידע באמצעות גיבויים
- ☐ זהו את וקטור התקיפה וטפלו בו, למניעת תקיפה חוזרת

4.2. שחזור באמצעות תוכנת פענוח/מפתח פענוח

- ☐ זהו את סוג הכופרה באמצעות מידע זמין ברשת ובאתרים ייעודיים כגון NoMoreRansom
- ☐ בדקו האם פורסם לכופרה זו מפתח או תוכנת פענוח
- ☐ גבו את הקבצים המוצפנים
- ☐ שחזרו את המידע בעזרת מפתח או תוכנת פענוח, תוך שימוש במחשב שונה ובגיבוי הקבצים המוצפנים לביצוע השחזור
- ☐ אם השחזור הצליח, הסירו הכופרה והחזירו הקבצים המפוענחים למחשב המקורי
- ☐ זהו את וקטור התקיפה וטפלו בו, למניעת תקיפה חוזרת

4.3. המתנה לפרסום מפתח תוכנת פענוח

- ☐ גבו את הקבצים המוצפנים
- ☐ הסירו את הכופרה
- ☐ זהו את וקטור התקיפה וטפלו בו, למניעת תקיפה חוזרת