המשרד להגנת הסביבה
الوزارة لحماية البيئة
Israel Ministry of Environmental Protection
המערך הלאומי לחומרים מסוכנים וחירום

סייבר בתעשייה
המשרד להגנת הסביבה

# פעולות ראשוניות לטיפול

# בנוזקת כופרה

## 1. מבוא

לאחרונה אנו עדים להתגברות תקיפות כופרה (RANSOMEWARE) בקרב עסקים בישראל בכלל ובקרב מפעלי חומרים מסוכנים בפרט.

תקיפת כופרה יכולה להתממש על רשת ה-IT (הרשת המנהלתית של העסק) המטפלת במידע של העסק אך גם על רשת ה-OT (הרשת התפעולית של העסק) בתוכה נמצאות מערכות הבקרה התעשייתיות (ICS) אשר במפעלי חומרים מסוכנים הם גם מנהלות / מבקרות טיפול בחומרים מסוכנים.
במסגרת תקיפות כופרה שחוו מפעלי חומרים מסוכנים גם עמדות HMI (עמדת אדם – מכונה) חוו הצפנות. תקיפות על עמדות HMI ועל מערכות בקרה תעשייתיות יכולה להתרחש במקרים שבהם התקיפה החלה מרשת ה-IT (אשר חשופה בצורה כזו או אחרת אל רשת האינטרנט או רשת אחרת הנגועה בנוזקה), ו / או עקב אי בידוד בין רשת ה-IT לרשת ה-OT (רשת שטוחה) שאיפשרה זליגה של הנוזקה אל רשת ה-OT והצפינה רכיבים במערכות ICS . תקיפה כזו יכולה גם להתבצע ישירות על רשת ה-OT במידה ורשת זו פתוחה ישירות לעולם באמצעות פורטים פתוחים של בקרים או רכיבי בקרה אחרים (סנסורים, רכיבי שטח) או תוכנות השתלטות מרחוק כגון TEAM VIEWER , ANY DESK ודומיהם העובדים בתווך ה-WEB.
תקיפת כופרה על עמדות HMI בעסק משביתות את יכולת העסק לשלוט בתהליכים התפעוליים ואף לגרור אירוע חומרים מסוכנים אשר עלול לפגוע בבריאות הציבור ובסביבה.

## 2. מטרה

מטרת מסמך זה, מתן הנחיות ראשוניות לעסק המותקף בכופרה. מסמך זה איננו נותן מענה מלא להתאוששות מתקיפה זו ואינו משחרר את העסק משימוש בצוותי תגובה (צוותי IR ) בטיפול בנוזקה או כל פעילות אחרת להרחקת הנוזקה וניקוי הרשת. ההנחיות המופיעות במסמך זה הן בגדר המלצות בלבד, ולא בהכרח שימנעו את הנזק שעלול להגרם ממתקפת כופרה בעסק . יודגש כי הנחיות אלה אינן באות במקום טיפול של העסק בתקיפה אלא כהנחיות עזר בלבד.

ניהול גרסאות

| גרסה | כתב | אישר | מהות השינוי | תאריך |
|---|---|---|---|---|
| 1.0 | יוסי שביט<br>ר' יחידת הסייבר בתעשייה | | כתיבת המסמך | 18.5.2023 |

## 3. <u>פעולות ראשוניות לביצוע עם זיהוי תקיפת כופרה</u>

במידה וזוהתה תקיפת כופרה בדמות קבצים מוצפנים, חוסר אפשרות להגיע למידע בארגון או הזדהות לתחנות עבודה יש לנקוט בפעולות הבאות:

א) יש לעדכן את יחידת הסייבר של המשרד להגנת הסביבה באמצעות מוקד החירום של המשרד להגנת הסביבה בטל: 073-2733200 או: 6911*.

ב) יש לנתק (ככל שהדבר מתאפשר מבחינה עסקית וללא פגיעה בתהליכים העסקיים) את רשת ה-IT ממעבר תעבורת תקשורת אל רשת ה- OT זאת על מנת למנוע אפשרות זליגת הנוזקה מרשת ה-IT לרשת ה-OT. במידת האפשר וללא פגיעה בתהליכים העסקיים של העסק יש לבצע את הניתוק בין רשתות ה-IT לרשת ה-OT פיסית. במידה ולא ניתן לבצע ניתוק כזה בין רשתות ה- IT וה-OT (עקב חשש פגיעה בתהליכים עסקיים) יש לצמצם לוגית את התעבורה בין הרשתות למינימום האפשרי תוך מתן תשומת לב יתרה ללוגים המתקבלים מתעבורה המאופשרת בין 2 רשתות אלה בדגש על מעבר מידע מרשת ה-IT לרשת ה-OT. יש לוודא מראש שאין לניתוק כזה השפעה שלילית על פעילות העסק.

ג) במידה וניתן להמשיך לעבוד ידנית ברצפת הייצור ללא מערכות המנהלות / מבקרות חומרים מסוכנים, מומלץ מאד לנתק את מערכות המחשוב ולעבור לעבודה ידנית (מומלץ מאד להכין נוהל מראש המתאר כיצד עוברים מעבודה באמצעות בקרים תעשייתיים לעבודה ידנית. רצוי שהנוהל יכלול את כל השלבים הנדרשים והאנשים המעורבים בפעילות בפירוט רב ככל האפשר).

ד) במידה וזוהה המחשב / המערכת / הרכיב שנמצא בו הנוזקה (שהקבצים בו הוצפנו) – יש לנתק את המחשב / מערכת / רכיב הנגוע באותה נוזקה מכל הרשתות אליהן הוא מחובר, כולל רשתות קוויות ואלחוטיות כגון Fi-Wi או Bluetooth.

ה) על מנת למנוע התפשטות הכופרה גם לעבר מערכות אחסון או גיבוי, יש לבצע ניתוק של כל הרכיבים החיצוניים המיועדים לאחסון קבצים או התקני זיכרון נייד או רכיבי גיבוי.

ניהול גרסאות

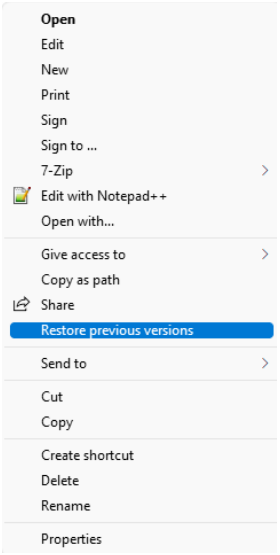
| גרסה | כתב | אישר | מהות השינוי | תאריך |
|---|---|---|---|---|
| 1.0 | יוסי שביט<br>ר' יחידת הסייבר בתעשייה | | כתיבת המסמך | 18.5.2023 |

ו) יש לבדוק אם הגיבויים נגישים. במידה וכן יש לבצע גיבוי לכל הגיבויים לפני כל שימוש בהם. מומלץ להחזיק גם גיבויים "קרים" קרי גיבויים שלא מחוברים שום צורה לרשת המותקפת שמהם ניתן יהיה לשחזר את הקבצים המוצפנים.

ז) יש לנסות לשחזר מדגמית מספר קבצים מגיבוי. יתכן מצב שקבצים שמשוחזרים מגיבוי יתגלו כמוצפנים . במקרה כזה יש להמתין עם שחזור מלא אד לאחר איתור וקטור התקיפה.

ח) במידה ומבצעים שחזור מלא רצוי לבצע את השחזור על עותק נקי של מערכת הפעלה שהותקנה מחדש , במידה ומדובר במכונה וירטואלית יש להקים את המכונה הוירטואלית מחדש.

ט) במידה והשחזור מביא קבצים מוצפנים, יש לנסות לבצע שחזור הקבצים לגירסא קודמת ע"י קליק ימני על הקובץ -> אפשרויות -> שחזר גירסאות קודמות. ראה תמונה מס' 1 .




תמונה מס 1 : שחזור גירסאות קודמות של קובץ

י) ניתן גם לנסות לבצע שחזור של המערכת (system restore) למועד שלפני זיהוי התקיפה.

ניהול גרסאות

| גרסה | כתב | אישר | מהות השינוי | תאריך |
|---|---|---|---|---|
| 1.0 | יוסי שביט<br>ר' יחידת הסייבר בתעשייה | | כתיבת המסמך | 18.5.2023 |

יא) במידה והקבצים עדיין מוצפנים ניתן להעזר בכלים לפתיחת הצפנות כופרה שנמצאים באתר הבא: https://www.nomoreransom.org/he/decryption-tools.html לפני שימוש בכל כלי כזה יש לבדוק אותו באתר של וירוס טוטאל כדי לוודא שהכלי אינו נגוע בנוזקה. הלינק לאתר של וירוס טוטאל: https://www.virustotal.com/gui/home/upload

## 4. פעולות לביצוע כהכנה להגעת צוות תגובה IR

כדי לחסוך זמן השבתה ולהגיב מהר נדרש לאסוף מידע אשר ישמש את צוותי התגובה. המידע יכלול את הנתונים הבאים:

א) לנסות לתזמן ככל האפשר את הזמן המדויק בו קרה האירוע

ב) לתעד את גירסאות מערכות ההפעלה ומצב העדכונים של אותם מחשבים שנפגעו

ג) לתעד את גירסאות האנטי-וירוס / EDR או כל אמצעי הגנה על עמדת הקצה הקיימת בתחנה ומצב העדכונים של אותה הגנה.

ד) לתחקר את משתמש הקצה של המחשב הנגוע, האם צפה באירועים מוזרים / תגובות מוזרות מהמחשב שלו לפני קרות האירוע?

ה) לשמור עותק של יומן האירועים (Event Viewer) של אותו מחשב שנפגע

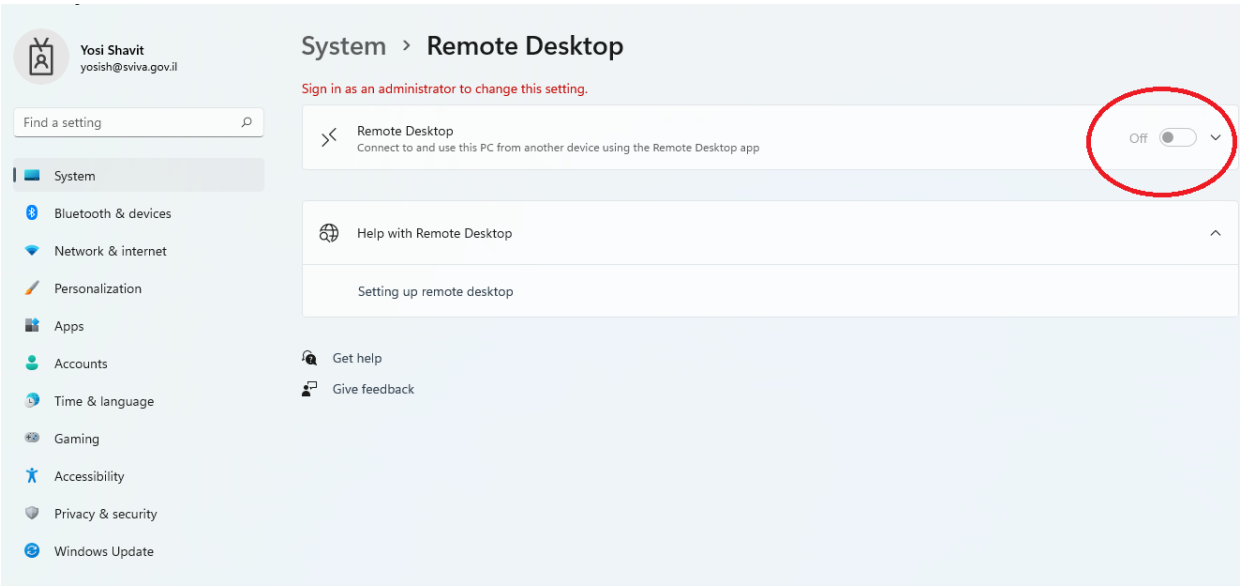
ו) לבדוק עם משתמש המחשב הנגוע אם ביצע את הפעולות הבאות:

- הורדת קבצים
- הכנסת DOK או כל מדיה אחרת ליציאת ה-USB
- גלישה לאתרים שלא נוהג לגלוש בד"כ
- קבלת מייל שיש בו הורדת קובץ או לחיצה על לינק (גם אם המייל ממקור ידוע!)
- מתן גישה מרחוק כלשהיא למחשב הנגוע (תוכנות כגון Team Viewer, Any Desk ודומיהם)
- מתן פרטי הזדהות שלו לגורם כלשהוא

ניהול גרסאות

| גרסה | כתב | אישר | מהות השינוי | תאריך |
|---|---|---|---|---|
| 1.0 | יוסי שביט<br>ר' יחידת הסייבר בתעשייה | | כתיבת המסמך | 18.5.2023 |

בדיקה אם יש אפשרות להשתלטות מרחוק ב-Remote Desktop – ראה תמונה מס' 2




תמונה מס' 2: ביטול אפשרות להתחברות מרחוק

## 5. פעולות להמשך על מנת למזער את האפשרות לאירוע דומה

מומלץ לבצע יישום כל הבקרות החסרות מרשימת הבקרות הכתובות במדריך הסייבר לתעשייה גירסא 2.0 בנספח ג' המופיע בלינק הבא:

https://www.gov.il/he/departments/publications/reports/cyber_industry_toxins_permit

בנוסף לשים דגש על הדברים הבאים:

א) עדכון מערכות הפעלה למערכות הפעלה נתמכות יצרן כולל כל עדכוני האבטחה

ב) עדכון הגנה על תחנות הקצה – לעדכונים האחרונים הקיימים

ג) מתן סיסמאות מורכבות ושינוי סיסמא בתדירות של אחת לרבעון.

ניהול גרסאות

| גרסה | כתב | אישר | מהות השינוי | תאריך |
|---|---|---|---|---|
| 1.0 | יוסי שביט<br>ר' יחידת הסייבר בתעשייה | | כתיבת המסמך | 18.5.2023 |

ד) עדכון דפדפן הקיים בתחנה לגירסא האחרונה עם עדכוני האבטחה האחרונים

ה) חסימת חלונות קופצים ( Pop-Up) בגלישה

ו) ביטול האפשרות להוריד שורת משימות לדפדפן (Task Bar)

ז) ניטרול הרצת פקודות מקרו בקבצי אופיס

ח) ניטרול פתיחת לינקים מתוך קבצי PDF

ט) ביצוע גיבויים "קרים" – קרי גיבויים שלא מחוברים לרשת (למשל דיסק חיצוני)

י) הטמעת סינון תוכן למערכת המייל הארגונית

יא) ביצוע קמפיין מודעות עובדים נרחב

ניהול גרסאות

| גרסה | כתב | אישר | מהות השינוי | תאריך |
|---|---|---|---|---|
| 1.0 | יוסי שביט<br>ר' יחידת הסייבר בתעשייה | | כתיבת המסמך | 18.5.2023 |