Digital Security
Progress. Protected.

המדריך המלא להתגוננות מפני כופר בארגונים

כיצד להתגונן מפני התקפת כופר ברשת הארגונית?

1. יש לוודא שעובדי החברה מכירים את הסכנות ברשת.
חשוב מאוד לפני הכול להפנים שהעובדים הם חלק בלתי נפרד ממערך ההגנה על הארגון. יש ליישם תוכנית מודעות אבטחת מידע לעובדים בארגון באמצעות הדרכות, מבחנים ועדכונים המתריעים על התקפות נפוצות על מנת לוודא שכל העובדים מכירים את כללי אבטחת המידע ומודעים לסכנות ברשת.
הנה לכם **מצגת שתוכל לסייע לכם בהדרכות.**

2. יש לוודא שקיים מנגנון אנטי-פישינג ואנטי-ספאם ברשת.
איומים רבים כמו ניסיונות דיוג (פישינג) נשלחים בהודעות דוא"ל למשתמשים בארגון. יש לוודא שקיימים מנגנוני הגנה כמו אנטי-פישינג ואנטי-ספאם שמסוגלים לעצור מיילים מסוג זה ולמנוע מהם להגיע לעובד.

3. יש להגדיר עדכוני מערכת הפעלה אוטומטיים בשרתים ובתחנות.
מומלץ להשתמש במערכת כמו WSUS להפצה ובקרה על העדכונים, כדי לוודא שהעדכונים יתבצעו באופן אוטומטי. מומלץ גם לוודא שמערכות הפעלה מסוג לינוקס ו-MacOS מקבלות עדכונים באופן שוטף.

4. יש לוודא התקנה של תוכנת אבטחה מעודכנת וחוקית בכל התחנות והשרתים ברשת.
- יש לוודא שלתוכנת Endpoint Security בה משתמשים קיימת מערכת קדם-פגיעה.
מערכות מסוג זה מגנות על העמדה בהקדם האפשרי נגד איומים חדשים (Zero Day), לרוב על ידי מנגנונים שמאפשרים הגנה עוד לפני שיוצא עדכון למערכת.
- יש להשתמש בתחנות בחומת אש מתקדמת, במיוחד במחשבים ניידים שיוצאים מהרשת ואינם מוגנים ע"י חומת האש הארגונית.
- יש להגדיר ניקוי אוטומטי לנוזקות שאותרו.
במקרים רבים, ברירת מחדל של סריקות המתבצעות על ידי תוכנות אבטחה היא להציע למשתמש אפשרויות ניקוי. לרוב, משתמשים פשוט יסגרו חלונות מסוג זה מבלי לבצע כל ניקוי – פעולה זו תשאיר את האיום במערכת.
- יש לוודא כי הוגדרה סריקה אוטומטית של כל המחשבים והשרתים בארגון, בתדירות של לפחות פעם בשבוע
- להגדיר סיסמת הגנה לתוכנת האבטחה בתחנות ובשרתים על מנת למנוע הסרה ידנית, שינוי הגדרות או נטרול שלה.
ברוב המקרים בהם חודרת תוכנת כופר למערכת, היא תנסה להסיר או לנטרל את תוכנת האבטחה כדי שלא "תפריע" לה. סיסמה זו תגן גם מפני כיבוי מוצר ההגנה על ידי העובד, בין אם מסיבות תמימות ובין אם מסיבות זדוניות (איום פנימי).
- להגדיר זיהוי **של תוכנות לא רצויות / לא בטוחות.**
- יש לוודא שתוכנת ההגנה ברשת מזהה גם תוכנות מסוג זה.
- יש להגדיר דו"חות והתראות על איומים ברשת.
חשוב תמיד להישאר בבקרה על איומים שנמצאים ברשת, לכן חשוב להגדיר דו"חות והתראות אוטומטיים ומותאמים לאיומים שזוהו. יחד עם זאת, חשוב לשים לב לאיומים שחוזרים על עצמם – גם אם הם מנוקים מהמערכת. לדוגמא, אם נוזקה אותרה על ידי תוכנת האבטחה ונמחקה, אך מזוהה כל פעם מחדש, יש לחקור זאת לעומק כדי לוודא שלא קיים מנגנון של Presistance, כחלק ממתקפה מתקדמת - APT.

5.מומלץ להטמיע פתרון זיהוי, תחקור ותגובה Endpoint Detect & Response (EDR)
מערכת הזיהוי ותגובה (EDR) לתחנות קצה מאפשרת נראות יוצאת מן הכלל של הרשת הארגונית המשקפת למשתמש איומים בזמן אמת, ניתוח מעמיק של תהליכים חשודים ותגובה מידית וטיפול באירועי אבטחה.
פתרון ה-EDR בשילוב פלטפורמת ההגנה על תחנות הקצה, מעניק מענה מקיף למניעה, זיהוי ותגובה למתקפות סייבר:
- זיהוי איומים מתמשכים
- חסימת מתקפות נטולות-קבצים
- חסימת איומי Zero Day
- הגנה מפני כופרות
- מניעת הפרות של מדיניות החברה

6. במידה ונעשה שימוש בשירות Remote Desktop (RDP) יש להקפיד לפעול על פי ההמלצות הבאות:
- יש להשתמש ב VPN או באימות דו-שלבי (2FA) או שילוב של שניהם.
- יש להגדיר סיסמה מורכבת, מומלץ להשתמש ב- Passphrase (ביטוי המורכב ממספר מילים) ולא Password (אותיות ומספרים).
משפטים שמשמשים כסיסמאות הם הרבה יותר בטוחים וקשים לפריצה.

7. יש להגדיר גיבוי חיצוני למסמכים והקבצים החשובים ברשת.
במהלך ניסיון הצפנה של תוכנת כופר, התוקפים ינסו גם להצפין גיבויים שמאוכסנים על התקנים שמחוברים פיזית לשרתים (NAS, קלטות, התקנים חיצוניים ניידים וכו'), לכן חשוב לגבות על התקנים שאינם מחוברים באופן רציף לשרתים.

8. לבצע עדכונים של תוכנות צד שלישי כמו Java ו – Adobe Flash/Reader.
ברשתות גדולות מומלץ להתקין מערכת משלימה של Patch Management.

9. מומלץ לבצע מבדקי חדירות חד פעמיים או תקופתיים באמצעות חברות המתמחות בנושא.

כיצד לטפל ברשת שנפגעה מתוכנת כופר?

יש לעבוד על פי סדר הפעולות <u>ולא לדלג על סעיפים</u>.

1. לבדוק מהו המחשב הנגוע שממנו קודדו הקבצים.
- יש לאתר את קובץ ה – TXT או HTML המכיל את ההנחיות לתשלום "How to decrypt" בתיקיות המשותפות / כוננים שהוצפנו.
- יש ללחוץ לחיצה ימנית על הקובץ > Properties > לשונית Details ולאתר בשדה Owner את המשתמש שממנו בוצעה ההצפנה.
- במידה וה – Owner הוא Administrators, זה לרוב יצביע על פריצה דרך RDP או Privilege Escalation.

2. לנתק את המחשב של המשתמש מסעיף 1 מהרשת - פיזית.

3. יש לוודא שה - RDP סגור בכל הרשת, במידה ויש צורך בגישה מרחוק יש להשתמש ב – VPN עם אימות דו-שלבי.
סגירת ה – RDP ברשת תנתק חיבור פעיל של תוקף במידה ועדיין מחובר.

4. במידה ועדיין לא הוצפנו, מומלץ לבודד שרתים קריטיים מהרשת הנגועה.
- לדוגמא שרתי קבצים, SQL, דואר, IIS וכו'.
- חשוב לשים דגש מיוחד על שרתי גיבוי, גיבויים שרצים לענן, או NAS הקיימים ברשת, ולנתקם, או לבטל את הגיבוי האוטומטי כדי שלא יסונכרנו קבצים מוצפנים.

5. לוודא התקנה בגרסה עדכנית של תוכנת אבטחה בכל התחנות ברשת.
- גם אם התחנה הבעייתית נותקה מהרשת, עדיין ייתכן מצב בו הנוזקה הדביקה תחנות אחרות. לכן יש לוודא שמותקנת גרסה עדכנית ומעודכנת של תוכנת האבטחה בכל התחנות.
- במידה וקיימת גרסת עדכנית של תוכנת אבטחה במערכת אותה ניתקתם, יש לבצע סריקה מלאה כדי לוודא שלא קיימים רכיבים נוספים מהנוזקה שעלולים לגרום להדבקה נוספת.
- במידה ואין גרסה עדכנית או אין חתימות עדכניות, מומלץ לבצע סריקה עם כלי ניקוי משלימים (לדוגמא סריקת אבטחה במצב בטוח או סריקה מתוך התקן USB Bootable עליו שמים סורק כלשהו).
- יש לשלוח סריקות מלאות לכל התחנות והשרתים ברשת דרך ממשק הניהול.

6. לשחזר את הקבצים מגיבוי
רק לאחר השלמת סעיפים 1-5, שמטרתם לוודא שלא קיימת נוזקה פעילה במחשב או ברשת, ניתן לשחזר את הקבצים מגיבוי.

7. אם לא היה גיבוי מסודר, או שהגיבוי הוצפן, ניתן לנסות לשחזר את הקבצים מתוך Shadow Copy.
ניתן להיעזר **במדריך של Bleeping Computer**, זאת בתנאי שתוכנת הכופר לא הצליחה למחוק את ה – Shadow Copy.

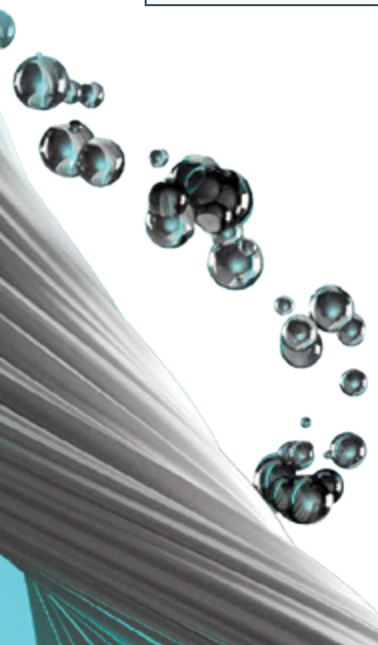
8. בזמן עבודה לפי התהליכים המתוארים למעלה, מומלץ להקפיד לפעול לפי קווי המנחה הכלליים:
- ברגע שהמתקפה אומתה, יש ליידע את הגורמים הרלוונטיים (מנהל הרשת, CISO, צוות Incident Response).
- אתרו ונתחו את המחשבים הנגועים.
- התריעו למחלקה המשפטית בנושא המתקפה.
- צרו קשר עם ספקים שיכולים לסייע בתהליך (חברת הגיבוי, תוכנת ההגנה ברשת, פיירוול וכו').
- יש להזכיר לעובדים שלא לפרסם ולהדליף פרטים על המתקפה לרשתות חברתיות או לתקשורת.
- צרו קשר עם מערך הסייבר הלאומי.
- בדקו האם הקבצים שהוצפנו זמינים לשחזור מגיבוי.
- במידת הצורך יש להפעיל את תוכניות ההמשכיות העסקית.

9. בסיום האירוע יש לתחקר את הגורמים והפרצות שהובילו למתקפה, להסיק את המסקנות הנדרשות וליישם נהלים, אמצעים והגנות שהיו חסרים לפני כן.

10. מומלץ להירשם להתראות של מערך הסייבר ולפעול בהתאם להנחיות שמתפרסמות.

Checklist
להתגוננות מפני נוזקות כופר

משימה	מי אחראי	בוצע/לא בוצע
הדרכות מודעות אבטחת מידע לעובדים בארגון		☐
מנגנון אנטי-פישינג ואנטי-ספאם ברשת		☐
הגדרת עדכוני מערכת הפעלה אוטומטיים בשרתים ובתחנות		☐
התקנה של תוכנת אבטחה מעודכנת וחוקית בכל התחנות והשרתים ברשת		☐
וידוא שימוש נכון ובטוח בשירות Remote Desktop		☐
הגדרת גיבוי חיצוני למסמכים והקבצים החשובים ברשת		☐
עדכונים של תוכנות צד שלישי		☐
מבדקי חדירות חד פעמיים או תקופתיים באמצעות חברות המתמחות בנושא		☐



Checklist
במידה והארגון נפגע מנוזקת כופר

משימה	מי אחראי	בוצע/לא בוצע
איתור המחשב הנגוע שממנו קודדו הקבצים		☐
ניתוק המחשב הנגוע מהרשת – פיזית		☐
סגירת RDP בכל הרשת		☐
בידוד שרתים קריטיים מהרשת הנגועה (אלו שלא הוצפנו)		☐
ידוע המחלקה המשפטית על המתקפה		☐
עדכון העובדים ודרישה לשמירה על דיסקרטיות		☐
יצירת קשר עם מערך הסייבר הלאומי		☐
ווידוא עדכון תוכנת האבטחה על כל התחנות ברשת		☐
שחזור הקבצים מגיבוי		☐
שחזור קבצים מתוך Shadow Copy		☐
תחקיר האירוע והסקת מסקנות		☐

Digital Security
Progress. Protected.

ESET היא חברת אבטחת המידע מס' 1 באיחוד האירופי הנחשבת לחלוצת תחום האנטי וירוס עם למעלה מ-30 שנות ניסיון.

אנחנו מפתחים פתרונות הגנה המצטיינים במניעה, זיהוי ותגובה לאירועי סייבר, המאפשרים לארגונים להתמקד במטרותיהן מבלי לעצור ותוך מינימום צריכת משאבים.

יש לנו יותר 1 מיליארד משתמשים מוגנים ומעל 400 אלף עסקים מוגנים במעל ל- 200 מדינות ברחבי העולם.
בין לקוחותינו ניתן למנות משרדי ממשלה ועיריות, מוסדות חינוך ובריאות, חברות היי-טק ועסקים במגוון תחומים רחב.

הפתרונות שלנו המיועדים למגזר העסקי כוללים:

- Endpoint Protection Platform
- Endpoint Detection & Response
- Cloud Sandbox
- Data & Identity Protection
- Data Loss Prevention
- Threat Intelligence