שלום רב,

בתקופה האחרונה אנו שומעים על ריבוי "התקלויות" בתוכנות זדוניות, רוגלות(Malwares), המכונות כופרות (Ransomware).

אז מהי בעצם כופרה?

- כופרות הן תוכנות שמתוכננות למנוע ממשתמשים להשתמש במחשב שלהם, אלא אם ישלם כופר לתוקף שהפיץ את הכופרה.
- ישנן כופרות שעושות זאת בעזרת נעילת המחשבים ע"י כלים שונים שמונעים התחברות למחשב.
- כיום כופרות רבות מקצינות עוד יותר וגם מצפינות את קבצי המשתמש, דוגמאות לכך הן cryptolocker, cryptowall ודומות.
- ההצפנות של הקבצים הן הצפנות חזקות כך שהאפשרות היחידה שנותרת עבור משתמשים שנפגעו היא לשלם את הכופר(תשלום גבוה - במקרים רבים מעל 500$, שבד"כ משולם בBitCoin), ובתמורה (במקרים מסויימים, אך ממש לא תמיד!) התוקף מסיר את ההצפנה.

איך הכופרות מפיצות את עצמן?

- ישנן כמה דרכי הפצה לתוכנות אך רובן מבוססות על דיוג(Phishing) של המשתמש, וביצוע פעולה ע"י המשתמש שתפעיל את הכופרה על המחשב שלו.
- התוקף יכול להפיץ מייל זדוני, המבקש מהמשתמש להכנס לאתר מסויים, לעיתים אם כתובות דומה מאוד, לאתר אחר מפורסם לדוג'(www.gooogle.com - שימו לב לאות o המיותרת, במקרה הזה ספציפית גוגל התגוננה ורכשה גם כתובת זאת על מנת למנוע דיוג משתמשים).
- התוקף יכול להתחזות למכר של המשתמש ולשלוח קובץ שהמשתמש יוריד למחשב שלו.
- התוקף יכול לשלוח מייל למשתמש, שבתוך ההודעה עצמה מוחבא קוד זדוני הגורם להורדה של התוכנה למחשב המשתמש מבלי שהמשתמש ידע על כך!
- בעקבות פגיעת אבטחה ב**Microsoft Outlook** התוקף יכול לשלוח מייל, אשר יפעיל תוכנת **Ransomware** מבלי שהמשתמש יפתח את המייל אפילו!! הפגיעות אותרה בתחילת חודש דצמבר, ובתאריך 8.12 יצא תיקון אבטחה עבורה.(מקור:https://blog.kaspersky.com/bad-badwinmail/10868/)

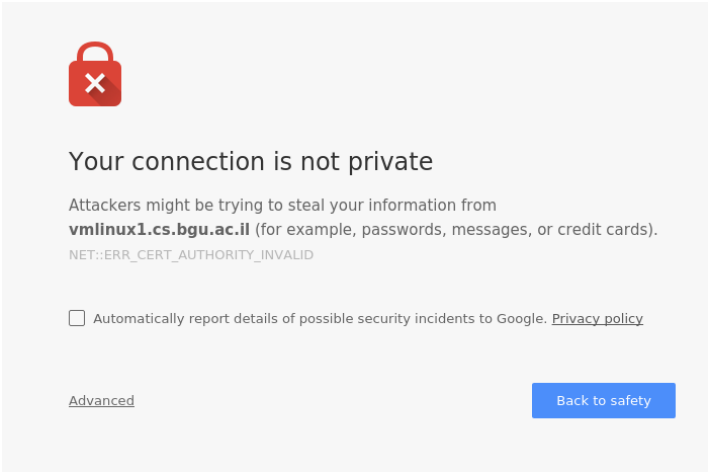
<u>אז איך ניפטר מכופרה?</u>

- במקרים רבים לא ניתן להיפטר מהכופרה ללא תשלום השוחד (מדובר בד"כ בסכומים גבוהים באזור ה500$) , במקרים מסויימים גם כאשר השוחד משולם התוקף לא שולח את המפתח.
- ישנם כלים (לדוג' Kaspersky Ransomware Decrypter) אך הם אינם עומדים על 100% הצלחה ומתאימים רק לסוגים מסויימים של כופרות (Kaspersky לדוגמא עובד רק על כופרות מסוג Coinvault ו(Bitcryptor

<u>אם לא ניתן להסיר את ההצפנה, אז מהו הפתרון?</u>

- הפתרון הכי אפקטיבי לבעיה מחולק לשני חלקים:
  - גיבוי! גיבוי! וגיבוי של החומר החשוב - חשוב שהחומר החשוב לנו (תמונות, מסמכים וכו') יעברו גיבויים תכיפים, כך שבמידה ונפגע נוכל לשחזר את החומר בקלות, מומלץ מאוד לגבות את החומר לכמה מקומות שונים (לדוג' לשירות ענן - Dropbox וכו' וכונן נייד), זאת מכיוון שאם אחד מנתיבי הגיבוי שלנו יפגעו(או באמצעות ה Ransomware או סתם מפדיעה אחרת).
    - בנוסך מומלץ מאוד שתוכנת הגנה(Anti-virus) כלשהי תהיה מותקנת, במקרים מסויימים התוכנה תוכל לזהות את המתקפה ולמנוע אותה(חשוב להדגיש כי לא בכל המקרים! ולכן גיבוי! גיבוי! גיבוי!)
  - <u>אסור!!!</u> לפתוח הודעות ממקור לא מוכר/ להכנס ללינקים לא מוכרים!!!
    - יש לשים לב שבכתובות האתרים שאליהם אנו נכנסים אין שגיאה(אות נוספת, טעות באות וכו').
    - במקרים רבים אתרים מוכרים משתמשים בחיבור מוצפן על מנת לתקשר עם המחשב (HTTPS), ברגע שאתר משתמש בחיבור מוצפן ניתן לוודא (בסבירות מסוימת) כי אנו אכן מדברים אם האתר הנכון ע"י מבט לשורת הכתובת וזיהוי שהמנעול בצבע ירוק

    - במידה והדפדפן מתריע על שגיאה בכניסה לאתר: (לדוג')



יש להימנע מכניסה לאתר.

בנוסף, חשוב מאוד להתקין את עדכוני האבטחה שמשוחררים עבור התוכנות המותקנות במחשב שלנו.

מה לעשות במידה ו"נדבקנו"

- במידה והופיע לנו הודעה הדורשת כופר ו/או זיהינו קבצים שאין לנו גישה אליהם יותר/השתנה להם השם/נוספה סיומת לא מוכרת:
  - יש לכבות במהרה את המחשב, לנתק כל אמצעי אחסון חיצוני שמחובר אליו, לנתק את המחשב מהרשת ולפנות במהרה לאיש מקצוע שיוכל לנסות ולטפל בבעיה.

למידע נוסף

https://en.wikipedia.org/wiki/Ransomware
https://en.wikipedia.org/wiki/CryptoLocker
http://www.pcworld.com/article/2901672/how-to-prevent-ransomware-what-one-company-learned-the-hard-way.html
http://us.norton.com/ransomware/article