17/07/2024
077-5006206
052-6885006

סחיטה באמצעות וירוס כופר (Ransomware) – כיצד מתמודדים?

דמיינו לכם מצב בו אתם מנסים לפתוח את קבצי התמונות שהעלאתם לאחרונה למחשבכם האישי, תמונות שתיעדו את הרגעים החשובים בחייכם, אך במקום זאת אתם מקבלים הודעה המבשרת לכם את הגרוע מכל – כי הקבצים הוצפנו ועליכם לשלם כופר בתמורה לפתיחתם. למרבה הצער, גולשים רבים ברחבי הגלובוס נפלו קורבן לעוקץ תוכנות הכופר המתגנבות בחשאי למחשב או לנייד, ומצפינות את הקבצים הנמצאים בתוכם ולוקחות אותם כ"בני ערובה". בכדי לזכות בהם בחזרה, על הקרבנות לשלם כופר, אומנם הדבר לצערנו לא מבטיח את שחזורם או את הסרת מפתח ההצפנה. עו"ד אסף דוק מסביר מהי תוכנת כופר, כיצד ניתן להתגונן בפניה וכן מה כדאי לעשות מיד לאחר שהמחשב או הטלפון הנייד מותקפים על-ידי וירוס מצפין קבצים.

תוכנות כופר הפכו לנפוצות בשנים האחרונות אך ניכר כי הן מתחדשות מרגע לרגע עם גרסאות מתוחכמות הרבה יותר אשר מצפינות מגוון של קבצים החשובים למשתמשים ועם סיכויים אפסיים לשחזור. וירוסי הכופר הנפוצים כיום הינם: **CryptoWall**, **CTB-torrentLocker**, **Locker** ו-**Cryptolocker**.

תוכנת כופר היא למעשה וירוס המצפין את הקבצים במחשבו של המשתמש ולמעשה לוקח אותם כ"בני ערובה". בכדי לזכות בהם בחזרה – יש לשלם את הכופר, למרות שאף זה לא מבטיח בוודאות את שחזורם ו/או הסרת הצפנתם. תופעת תקיפות באמצעות תוכנות כופר זולגת גם לסמארטפונים אט אט ולא רק למחשבים. למרבה הצער, משטרות העולם לרוב חסרות אונים מול התופעה ובמרבית המקרים הנסחטים נאלצים לשלם בעבור שחרור הקבצים באמצעות מטבע וירטואלי – הביטקוין (Bitcoin).

תוכנות כופר (Ransomware) – נעשות מתוחכמות מיום ליום

תוכנות הכופר הן נפוצות ואינן חדשות. אופן פעולתן תועד ברוסיה כבר מעל לעשור; סוס טרויאני המכונה Gpcode ניסה לסחוט מהמשתמשים כספים לאחר שהצפין במחשבם האישי מספר קבצים. למרבה המזל, כותב הנוזקה עשה מספר טעויות שהובילו לפיענוח ההצפנה בידי חוקרי אבטחה, מה שאפשר את השבת הקבצים לבעליהן. תוכנת ה – CryptoLocker, היא למעשה תוכנה הממשיכה את אופן הפעולה של ה – Gpcode אך טרם הצליחו לפענח את אופן ההצפנה שלה.

אופן הפעולה של וירוס כופר

וירוס כופר חודר לתיקיות המחשב ומחפש אחר קבצים כמו PDF, OFFICE או כל קובץ שיכול להכיל מידע רגיש וחיוני למשתמש. יש לציין שהוירוס יצפין גם קבצים אשר שמורים ב – USB המחובר למחשב. עוד חשוב לדעת כי ככל שמספר ההרשאות למשתמש שלכם גבוה יותר כך הנזק הוא גדול יותר.

כשההצפנה מסתיימת הוירוס מעלה לשולחן העבודה את הודעת הכופר. ההודעה מפרטת אודות הסכום של הכופר שבדרך כלל נע בין 300-400 יורו לצד אופן התשלום, שנעשה בעיקר באמצעות המטבע הווירטואלי – ביטקוין. ההודעה בנוסף מתריעה כי כל ניסיון להסיר את התוכנה יגרום להשמדתו של מפתח ההצפנה היחידי שלמעשה יכול לפענח אותה ובכדי להגביר את הלחץ על הקרבן – הוסיפו התוקפים שעון עצר המכוון בדרך כלל ל-72 שעות שזה פרק הזמן שעל הקרבן לשלם את הכופר טרם הקבצים החשובים לו ביותר יימחקו לצמיתות.

הווירוס כאמור בנוי באופן בו אין אפשרות לפענח את ההצפנה, דבר שלמעשה מאפשר את שיחזור הקבצים. המידע הדרוש לכך,

17/07/2024

077-5006206

052-6885006

נמצא רק אצל יוצר התוכנה הזדונית. אלגוריתם ההצפנה בנוי ממפתח הצפנה ציבורי ופרטי. הצפנת הקבצים בתחילה נעשית במפתח הציבורי ובמקביל תוכנת הכופר יוצרת מפתח הצפנה פרטי, אשר נשמר על שרת התוקפים ונשלט על ידיהם.

האם הסרת וירוס כופר יכולה למנוע את הסרת הקבצים?

הסרת הווירוס לא מועילה לקרבן ובמידה ומשביתים את השרת המחזיק במפתח ההצפנה הדבר יוביל לאבדן הכלי שבאמצעותו ניתן להציל את הקבצים. על כן, האופציות היחידות שנשארו לקרבנות הן: או לאבד את הקבצים או לשלם את הכופר. כמו כן, חשוב לציין כי למרה הצער, תשלום הכופר אינו מבטיח את שחזור הקבצים או את הסרת מפתח ההצפנה.

כיצד ניתן להתגונן מפני סחיטה וירטואלית באמצעות תוכנות כופר? זכרו את אלה: הגנה, גיבוי ושחזור;

1. גיבוי הקבצים

חשוב לגבות את הקבצים החשובים לכם בכדי להגן מפני תוכנות זדוניות למיניהם המאיימות על השמדתם. ניתן לגבות את הקבצים און-ליין כמו ב – Google Drive או Drop Box אך יש לשים לב כי תוכנות הכופר יודעות להצפין קבצים המגובים לרשת. יחד עם זאת, שירותי הגיבוי המקוונים מאפשרים את שיחזור הקבצים על כן יש להקפיד על גיבוי תקופתי. כמו כן, בלא מעט מקרים, גם משתמשים שבחרו לשלם את הכופר גילו שאין הבטחה שהמידע יוחזר אליהם ונותרו חסרי אונים.

2. עדכון מערכת הפעלה

תוכנות הכופר למעשה מנצלות פירצות אבטחה במערכות הפעלה על מנת ולפרוץ פנימה ולהחדיר את הוירוס הזדוני. בכדי להיות מוגנים, יש לעדכן באופן קבוע את מערכת ההפעלה.

3. סוף מעשה במחשבה תחילה – אל תלחצו על קישורים המגיעים בדואר האלקטרוני

הודעות אימייל הן דרך ההפצה העיקרית של תוכנות הכופר. הודעות עשויות להיראות אמתיות וכאילו הן הגיעו מגופים רשמיים כאלו ואחרים כמו קופת חולים או ביטוח לאומי. אל תפתחו את הקבצים המצורפים ואל תלחצו על הקישורים הנמצאים בהודעות האימייל טרם וויאדאתם במלוא הביטחון כי הודעת האימייל אכן מיועדת לכם והקבצים המצורפים אינם מסכנים אתכם.

4. עשו שימוש בחוסמי פרסומות בדפדפנים

לא מעט וירוסים של כופר מגיעים באמצעות גלישה ברחבי האינטרנט ולחיצה של גולשים על פרסומות במסגרת שיטוט באתרים שונים.

5. התקינו תוכנת אבטחה חדשה ועדכנית

מרבית תוכנות האבטחה מזהות את וירוס הכופר, על כן רצוי להתקין תוכנת אבטחה טובה על מחשבכם. יחד עם זאת, דרך הפעולה של תוכנות הכופר מתעדכנת מעת לעת וכך מקשה על החברות הללו את הזיהוי. לכן יש להקפיד להישמע לשאר ההוראות והמלצות האבטחה.

17/07/2024

077-5006206

052-6885006

קיבלת דרישת תשלום בעקבות התקפת כופר?

הנך זקוק/ה לעורך דין פלילי מנוסה המתמחה בעבירות מחשב וסייבר שיסייע לך להשיב את המידע והשליטה חזרה על המחשב או הטלפון הסלולרי שלך. בלא מעט מקרים, ניתן להציל את הקבצים במחשב או בטלפון החכם מבלי להיכנע לסחטנות. משרדנו מספק ייעוץ וייצוג משפטי למטופלים שנפלו למעשי נוכלות, איומים וסחיטה ברשת מזה תקופה ארוכה ובכך שומר נאמנה על הזכויות והאינטרסים שלהם תוך לחימה עיקשת, רציפה ובלתי מתפשרת בגורמים השונים עד לכיבוש היעד לשביעות רצונם. במידה ומצאת עצמך נסחט באמצעות וירוס כופר פנה ללא דיחוי להתייעצות עימנו בטלפון **052-6885006** או השאר/י פרטים ונשמח לסייע ולהציע לך מענה ופתרונות מקצועיים בהתאמה אישית. הפניה אינה כרוכה בהתחייבות כל שהיא מצדך. סודיות מלאה מובטחת.