06 מרץ 2020
י' אדר תש"פ
סימוכין:ב-ס-1030

קמפיין סחיטה רחב היקף הנשלח בדוא"ל לאזרחים בישראל

פרטים

החל מיום חמישי, ה-6.3.2020, מתקבלות במערך הסייבר הלאומי פניות רבות מאזרחים אשר קיבלו הודעת סחיטה בדוא"ל.

ההודעות נשלחות כביכול מכתובת הדוא"ל של האזרח, ותוכנן זהה: התוקף טוען כי פרץ למכשיר הטלפון או לתיבת הדוא"ל, ואף מפרט כיצד עשה זאת.
לאחר מכן, מאיים על הקורבן כי ברשותו תכנים אישיים שלו, ובמידה ולא ישלם, הם יופצו לרשימת אנשי הקשר שלו.
את הכסף מתבקש הקורבן להעביר לארנק ה-Bitcoin של התוקף.

להלן תוכן ההודעה:

מאת: [redacted]
<[redacted]>
תאריך: 6 במרץ 2020 בשעה 4:57:17
GMT+2
אל: [redacted]
<[redacted]>
נושא: בדוק את סודיות הנתונים שלך (חשבונך נפרץ על ידי האקרים).

שלום!

כפי ששמת לב, שלחתי לך דוא"ל מחשבונך.
המשמעות היא שיש לי גישה מלאה למכשיר שלך.

אני צופה בך כבר כמה חודשים.
העובדה היא שנדבקת בתוכנה זדונית דרך אתר ו שביקרת בו.

אם אינך בקיא בזה, אסביר.
נגיף הטרויאני נותן לי גישה ושליטה מלאה במחשב או במכשיר אחר.

אם אתה רוצה למנוע זאת,
העבר את הסכום של 950 דולר ארה"ב לכתובת הביטקוין שלי (אם אינך יודע כיצד לעשות זאת, כתוב לגוגל: "קנה ביטקוין").

ארנק הביטקוין שלי:
12Ss927B28nrmC617J4kxCC3Yc3t18M9Hd

לאחר קבלת התשלום, אני מוחק את הסרטון ואתה תשכח מהמקרה הזה.
אני נותן לך 50 שעות (יותר מיומיים) לשלם.
ברגע שתפתח את המכתב הזה התוכנה שלי תגלה על זה והטיימר יעבוד.

הגשת תלונה במקום כלשהו אינה הגיונית, מכיוון שלא ניתן לעקוב אחר אימייל זה כמו כתובת הביטקוין שלי.
אני לא עושה טעויות.

אם אגלה ששיתפת את ההודעה הזו עם מישהו אחר, הסרטון יופץ מייד

כל טוב!

חשוב להבהיר כי מדובר בקמפיין רחב היקף, אשר במסגרתו נשלחת אותה הודעה גנרית למאות אזרחים ברחבי הארץ. הדבר בכל הנראה מעיד על אמינות ההודעות.

כמו כן, גם אם ברשות התוקף התכנים המצוינים לעיל, העברת דמי הסחיטה אינה מבטיחה כי הוא לא יעשה בהם שימוש לאחר מכן.

התרעות קודמות של המערך בנושא סחיטה בערוץ הדוא"ל, ניתן לראות בקישור.

דרכי התמודדות

- יש לשנות סיסמאות לדוא"ל ולאתרים רגישים לעיתים קרובות.
- אין להשתמש בסיסמה זהה באתרים שונים.
- ההודעה נשלחה אליכם מהכתובת שלכם? ייתכן ומדובר בהתחזות ולא בפריצה. במקרה זה, מומלץ לשנות סיסמה לדוא"ל ולהגדיר אימות דו-שלבי.

במידה והתוקף מוכיח כי בידיו תכנים אישיים שלכם, יש לפנות לתחנת המשטרה הקרובה אשר תפנה אתכם ליחידת הסייבר שלה.

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו.
המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.