אאוץ! | דצמבר 2018

SANS SECURITY AWARENESS

OUCH!

עלון מודעות אבטחת מידע למשתמשי מחשב

כן, אתה מטרה

סקירה כללית

אנשים רבים לא מאמינים שהם מטרה עבור תוקפי סייבר: כי הם, המערכות שלהם או החשבונות שלהם לא מכילים ערך. מחשבה זו רחוקה מאוד מן האמת. אם אתה משתמש בטכנולוגיה בכל צורה שהיא, בעבודה או בבית, סמוך עלינו - יש לך ערך עבור הרעים. אבל, יש לך מזל. כי כבר יש לך את ההגנה הטובה ביותר שיש נגד התקפות סייבר - אתה.

למה אתה יעד

יש היום הרבה תוקפים מקוונים שונים באינטרנט, ולכולם יש מניעים שונים. אז למה שמישהו מהם ירצה לתקוף אותך? כי על ידי פריצה אליך הם עוזרים להשיג את מטרתם. הנה שתי דוגמאות נפוצות של התוקפים הקיברנטיים ומדוע הם יכוונו אותך.

⚠ **פושעי סייבר**: מטרת החבר'ה האלה היא לעשות כסף רב ככל האפשר. מה שהופך את האינטרנט לכל כך יקר ערך עבורם, הם יכולים בקלות להתמקד על כל אחד בעולם בלחיצת כפתור. ויש הרבה דרכים שהם יכולים להרוויח ממך כסף. דוגמאות לכך כוללות גניבת כסף מהבנק או מחשבונות אחרים, יצירת כרטיס אשראי בשמך וחיבורו לחשבונך, שימוש במחשב שלך כדי לפרוץ לאנשים אחרים, או לפרוץ למדיה החברתית או לחשבונות המשחקים שלך ולמכור אותם לעבריינים אחרים. הרשימה כמעט אינסופית איך החבר'ה הרעים יכולים להרוויח כסף מניצולך. ישנם מאות אלפי רעים כאלה שמתעוררים כל בוקר במטרה לפרוץ לאנשים רבים ככל האפשר בכל יום, כולל אותך.

☆ **תוקפים ממוקדים** : אלה תוקפי סייבר מאומנים היטב, לעתים קרובות עובדים עבור ממשלות, אירגוני פשיעה או מתחרים שלך בעבודה. אתה עלול לחשוב שעבודה שלך לא תמשוך תשומת לב רבה, אבל אתה תהיה מופתע מאוד.

- למידע שאתה מטפל בעבודה יש ערך עצום לחברות או ממשלות שונות.
- תוקפים ממוקדים יכולים לכוון אליך בעבודה לא מפני שהם רוצים לפרוץ אליך, אלא להשתמש בך כדי לפרוץ אחד מעמיתיך לעבודה או למערכות אחרות.
- התוקפים עשוים לכוון אליך בעבודה בגלל חברות אחרות שאתה עובד או שותף עמם.

יש לי אנטי וירוס, אני בטוח

אוקיי, אז אני מטרה, לא בעיה. אני אתקין אנטי וירוס וחומת אש במחשב שלי ואני מוגן, נכון? ובכן, לצערי, לא. אנשים רבים מרגישים שאם הם התקינו מספר כלי אבטחה ואז הם בטוחים. למרבה הצער, זה כלל לא נכון. תוקפי סייבר משיכים להש־תפר, ושיטות ההתקפה רבות יכולות בקלות לעקוף טכנולוגיות אבטחה.לדוגמה, לעתים קרובות הם יוצרים תוכנות זדוניות מיוחדות שהאנטי-וירוס שלך לא יכול לזהות. הם עוקפים את מסנני הדוא"ל עם התקפת דיוג מותאמת אישית או מתקשרים אליך לטלפון או בדרכי הונאה גורמים לך לתת את כרטיס האשראי שלך, כסף או סיסמה. הטכנולוגיה משחקת תפקיד חשוב בהגנה עליך, אבל בסופו של דבר אתה ההגנה הטובה ביותר.

למרבה המזל, להיות מוגן לא כל כך קשה, בסופו של דבר השכל הישר וכמה התנהגויות בסיסיות הם ההגנה הטובה ביותר שלך. אם אתה מקבל דוא"ל, הודעה או שיחת טלפון דחופה, מוזרה או חשודה, זה עלול להיות התקפה. כדי להבטיח שהמחשבים וההתקנים שלך מאובטחים דאגו שישארו מעודכנים, אפשרו את העדכון האוטומטי. ולסיום, השתמשו בביטוי סיסמה חזק, ייחודי לכל החשבונות שלכם. עדכניות מודעות הסייבר היא בסופו של דבר ההגנה הטובה ביותר שלך. לא בטוח איך להתחיל? שקול להירשם ל- OUCH החודשי! ידיעון ב - sans.org/ouch

עורך אורח

מאט ברומיילי (@mbromileyDFIR) נותן מענה לאירועי סייבר ומומחה ניתוח דיגיטלי משפטי עם מעל 8 שנות ניסיון. הוא עבד עם ארגונים והשתתף באירועים ברחבי העולם. מאט הוא גם מדריך ניתוח דיגיטלי משפטי ותגובות לאירועים, ומלמד את קורסי SANS FOR508 ו-FOR572.

SANS SECURITY AWARENESS

מקורות

עצור את התוכנה הזדונית: https://www.sans.org/sites/default/files/2018-06/201806-OUCH-June-Hebrew.pdf
הנדסה חברתית: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_he.pdf
התקפות בשיחות טלפון והונאות: https://www.sans.org/sites/default/files/2018-07/201807-OUCH-July-Hebrew_0.pdf
משפטי סיסמה: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201704_he.pdf
פוסטר - אתה יעד: https://www.sans.org/security-awareness/resources/posters/you-are-target

OUCH! יוצא לאור ומפורסם על ידי חברת SANS Security Awareness, הפצתו ברישיון Creative Commons BY-NC-ND 4.0 license, הנך רשאי להפיץ או להשתמש בעלון זה כעזר לתוכנית מודעות המשתמשים, כל עוד לא בצעת שינויים בעלון זה. לתרגומים או מידע נוסף, אנא פנה www.sans.org/security-awareness/ouch-newsletter. עורכי המערכת: וולט סקריוונס, פיל הופמן, בוב רודיס, שריל קונלי | תורגם על ידי: גדי מרגלית ודרור ענבר