הניוזלטר החודשי למודעות אבטחת מידע למשתמשי המחשב

OUCH!

בגליון זה...

- סקירה
- מדוע אתם מטרה
- להגן על עצמכם

כן, אתם למעשה מטרה

סקירה

לאנשים רבים יש תפישה שגויה שהם לא מטרה לפשעי סייבר, שלהם או למחשבים שלהם אין שום ערך. שום דבר לא יכול להיות רחוק יותר מהאמת. אם יש לכם מחשב, מכשיר נייד, חשבון מקוון, כתובת דואר אלקטרוני, כרטיס אשראי או קשורים לסוגים אחרים של פעילות מקוונת, אתם שווים כסף לפושעי סייבר. בניוזלטר זה אנו מסבירים למה אתם מטרה, איך תוקפים אתכם ומה אתם יכולים לעשות כדי להגן על עצמכם.

עורך אורח

אריק קונרד הוא נשיא ו CTO של Backshore Communications והכותב הראשי של הספרים CISSP – מדריך הלמידה, מהדורה שניה ו CISSP – השעה האחת עשרה, מהדורה שניה. הוא גם הכותב השותף של הקורס SANS, Continuous Monitoring and Security Operations (SEC511).

מדוע אתם מטרה

פשעים כמו הונאה, גניבת זהות וסחיטה קיימים מאז שקיימות ציביליזציות, הם חלק מחיי היומיום. מטרתו של פושע היתה תמיד זהה: להרוויח כמה שיותר כסף, בקלות ככל שניתן, ובסיכון הנמוך ביותר. מסורתית זה היה קשה כי פושעים היו מוגבלים על ידי המיקום שלהם, והיו צריכים להיות במגע פיזי עם הקורבן שלהם. זה לא רק הגביל את מי שהפושעים ראו כמטרה, אלא גם חשף את הפושעים לסיכון גבוה. לעומת זאת, הפשע השתנה בקיצוניות עם ההופעה של האינטרנט וטכנולוגיות מקוונות. כעת, פושעי סייבר יכולים לתקוף בקלות כמעט כל אחד ברחבי העולם בעלות אפסית או נמוכה מאוד ובסיכון נמוך. בנוסף, פושעי סייבר הפכו למאוד מאורגנים ויעילים, דבר המאפשר להם להיות אפקטיביים יותר מתמיד.

לבסוף, פושעי סייבר יודעים שככל שהם גונבים יותר כרטיסי אשראי, ככל שהם פורצים ליותר חשבונות בנק, או יותר סיסמאות שהם מגלים, כך הם מרוויחים יותר כסף. הם ינסו בפועל לתקוף כל אדם המחובר לאינטרנט, כולל אתכם. תקיפת מיליוני אנשים מסביב לעולם עלולה להישמע כעבודה רבה, אך באופן מפתיע זו משימה קלה מאחר שהם משתמשים בכלים אוטומטיים שעושים את כל העבודה עבורם. לדוגמא, הם עלולים לבנות בסיס נתונים של מליוני כתובות דואר אלקטרוני ולהשתמש בכלי אוטומטי לשלוח הודעות דיוג לכל אחת מכתובות אלו. שליחת הדואר האלקטרוני עולה כמעט כלום: הם פשוט משתמשים במחשבים פרוצים אחרים, אולי אפילו שלכם, לעשות עבורם את העבודה המלוכלכת. זוהי דוגמא נוספת מדוע המכשיר שלכם

© The SANS Institute 2014

כן, אתם למעשה מטרה

הוא בעל ערך אפילו רק כדי לתקוף ולפגוע באחרים. לבסוף, הפושעים לא יודעים מי יהיה הקורבן למתקפות הדואר האלקטרוני שלהם, אך הם כן יודעים שככל שישלחו יותר דואר אלקטרוני, יותר אנשים ייפלו לבסוף קורבן למתקפותיהם. ייתכן שהפושעים יסרקו בפועל כל מחשב באינטרנט (שוב כאמור באמצעות מחשבים נגועים) בחיפוש אחר מחשבים ומכשירים שניתן לפרוץ אליהם. זכרו, אתם לא נבחרים כי אתם מיוחדים, אלא פושעים אלו תוקפים את כל מי שהם יכולים וזה כולל גם אתכם.

אתם אולי לא תבחינו בכך, אך למכשיר שלכם ולמידע שלכם יש ערך בל יתואר לפושעי סייבר ברחבי העולם

להגן על עצמכם

כאשר פושעי סייבר מנסים לתקוף אנשים מסביב לעולם, הם בדרך כלל משתמשים בשיטות פשוטות. למזלנו, ע»י נקיטת מספר צעדים פשוטים אתם יכולים להתקדם קברת דרך ארוכה לקראת הגנה על עצמכם. הצעדים שאנו ממליצים עליהם כוללים:

- **אתם עצמכם**: לבסוף, אתם קו ההגנה הראשון כנגד מתקפת סייבר כלשהי. מתקפות רבות מתחילות עם נסיון של פושע סייבר להערים עליכם או לשטות אתכם, כמו לגרום לכם לפתוח דואר אלקטרוני נגוע או לגרום לכם למסור את הסיסמה שלכם בטלפון. הגיון בריא הוא ההגנה הטובה ביותר שלכם: אם משהו נראה מוזר, חשוד או יותר מדי טוב כדי להיות אמיתי, רוב הסיכויים שזוהי מתקפה.

- **לעדכן**: וודאו שכל מחשב או מכשיר נייד שאתם משתמשים בו מעודכן באופן מלא ומותקנים בו כל העדכונים והטלאים האחרונים. זהו צעד חשוב לא רק לגבי מערכת ההפעלה שלכם, אלא לגבי כל אפליקציה או התקן (plugin) שאתם משתמשים בהם. על ידי שמירת המערכת והאפליקציות עדכניים תמיד אתם מסייעים לשמור על עצמכם מוגנים מפני מרבית המתקפות הנפוצות.

- **סיסמאות**: השתמשו בסיסמה חזקה וייחודית לכל אחד מהחשבונות שלכם. כך כאשר אתר שאתם משתמשים בו נפרץ, וכל הסיסמאות באתר נגנבות (כולל שלכם), שאר החשבונות שלכם מוגנים. כמוכן וודאו שכל המכשירים השונים שלכם מוגנים על ידי סיסמא חזקה וייחודית, PIN או על ידי מנגנון נעילה חזק אחר. על מנת לעקוב אחרי כל הסיסמאות השונות שלכם, אנו ממליצים להשתמש במנהל סיסמאות (Password Manager).

© The SANS Institute 2014

כן, אתם למעשה מטרה

- **כרטיסי אשראי**: בידקו את חשבון כרטיס האשראי שלכם בתדירות גבוהה, אנו ממליצים לפחות פעם בשבוע (פעם בחודש אינו מספיק). ברגע שאתם מבחינים בפעולה לא מאושרת בכרטיס האשראי שלכם, דווחו מיידית למחלקת האבטחה של מנפיק הכרטיס. אם חברת האשראי או הבנק מאפשרים לכם להגדיר קבלת דואר אלקטרוני או הודעת טקסט עבור עסקות חריגות, השתמשו בשירות זה על מנת לקבל הודעה במהירות הגבוהה ביותר על כל פעילות חריגה.

- **הרשת שלכם**: אבטחו את הרשת האלחוטית הביתית שלכם באמצעות סיסמת אדמיניסטראטור חזקה וודאו שהרשת האלחוטית שלכם דורשת סיסמה מכל מי שמעוניין להתחבר אליה. כמו כן ודאו כי אתם יודעים אילו מכשירים מחוברים לרשת הביתית שלכם ושכל המכשירים האלו מעודכנים.

- **מדיה חברתית**: ככל שאתם מפרסמים יותר מידע במדיה חברתית כך אתם מסכנים את עצמכם יותר. לא רק שמידע כלשהו שאתם מפרסמים עלול לסייע לפושעי סייבר להתמקד בכם, להערים עליכם או לשטות אתכם, אלא שכל מידע שתעלו עלול לזהות אתכם כמטרה בעלת ערך.

למדו עוד

הרשמו ל OUCH! הניוזלטר החודשי למודעות אבטחת מידע, גשו לארכיון OUCH!, בקרו אותנו ב http://www.securingthehuman.org ולמדו עוד על פתרונות מודעות אבטחת מידע של SANS.

מקורות

OUCH! Password Managers:
http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Securing Your Home Network:
http://www.securingthehuman.org/ouch/2014#january2014
OUCH! Phishing Attacks:
http://www.securingthehuman.org/ouch/2013#february2013
Poster: You Are A Target:
http://www.securingthehuman.org/resources/posters

OUCH! מפורסם ע»י SANS Securing The Human ומופץ תחת רשיון Creative Commons BY-NC-ND ۳,۰. אתם חופשיים להפיץ את הניוזלטר הזה או להשתמש בו בתוכנית העלאת המודעות שלכם כל עוד שאינכם עורכים שינויים בניוזלטר. לתרגום ומידע נוסף אנא צרו קשר ב ouch@securingthehuman.org

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
צוות העורכים: ביל ווייימן, וולט סקריבנס, פיל הופמן, בוב רודיס.