SANS SECURITY AWARENESS

אאוץ! | יוני 2018

עלון מודעות אבטחת מידע למשתמשי מחשב

עצור את התוכנית הזדונית

סקירה כללית

בטח שמעתם על מונחים כגון וירוסים, סוסים טרויאנים, כופרה או rootkit כאשר אנשים מדברים על אבטחת סייבר. אלה סוגים שונים של תוכניות זדוניות, המכונות נוזקה, פושעי סייבר משתמשים בהן כדי להדביק מחשבים והתקנים. לאחר ההתקנה, הם יכולים לעשות מה שהם רוצים. נלמד מה היא תוכנה זדונית, מה הסכנה שהיא מציבה, והכי חשוב מה אתה יכול לעשות כדי להגן על עצמך מפניה.

מהי תוכנה זדונית?

במילים פשוטות, תוכנה זדונית היא תוכנה - תוכנית מחשב - המשמשת לביצוע פעולות זדוניות. מונח נוזקה הוא משחק מילים של המילים נזק ותוכנה. פושעי סייבר מתקינים תוכנות זדוניות על המחשבים או ההתקנים שלך כדי לקבל שליטה עליהם. לאחר ההתקנה, תוכנות זדוניות עלולות לאפשר לפושעים לרגל על הפעילות המקוונת שלך, לגנוב את הסיסמאות או הקבצים או להשתמש במערכת שלך כדי לתקוף אחרים. נוזקה יכולה אפילו להשתלט על הקבצים שלך, בדרישה לשלם כופר כדי לקבל אותם בחזרה. אנשים רבים מאמינים כי תוכנה זדונית היא בעיה רק עבור מחשבי Windows. למרבה הצער, תוכנות זדוניות יכולות להדביק כל מכשיר, ממחשבי Mac וטלפונים חכמים למצלמות DVR ולמצלמות אבטחה. ככל שפושעי הסייבר מדביקים יותר מחשבים והתקנים, כך הם יכולים להרוויח יותר כסף. לכן, כל אחד הוא יעד, כולל אתה.

להגן על עצמך - עצור תוכנות זדוניות

אתה יכול לחשוב בטעות שכל מה שאתה צריך לעשות הוא להתקין תוכנית אבטחה כמו תוכנת אנטי וירוס ותהיה בטוח מפני הדבקות. למרבה הצער, אנטי וירוס לא יכול לעצור את כל התוכנות הזדוניות. פושעי סייבר מפתחים כל הזמן תוכנות זדוניות חדשות ומתוחכמות יותר, שיכולות להתחמק מזיהוי. במקביל ספקי תוכנות אנטי וירוס, כל הזמן מעדכנים את המוצרים שלהם עם יכולות חדשות כדי לזהות תוכנות זדוניות. במובנים רבים יש כאן מרוץ חימוש, והרעים בדרך כלל נמצאים צעד אחד קדימה. מכיוון שאינך יכול לסמוך על אנטי וירוס בלבד, הנה צעדים נוספים שעליך לנקוט כדי להגן על עצמך:

פושעים באינטרנט פוגעים לעתים קרובות במחשבים או בהתקנים על-ידי ניצול פגיעויות בתוכנה המותקנת. ככל שגרסת התוכנה הנוכחית שלך עדכנית יותר, מספר הפגיעויות נמוך יותר, וקשה יותר עבור פושעי הסייבר להדביק את המחשבים וההתקנים. ודא שההתקנים, מערכות ההפעלה, היישומים, הדפדפן והרחבות הדפדפן שלך תמיד מעודכנים ועדכניים. הדרך הקלה ביותר להבטיח זאת היא לאפשר עדכון אוטומטי בכל הזדמנות אפשרית.

דרך נפוצה לפושעי סייבר היא להדביק מחשבים או התקנים ניידים היא על ידי יצירת תוכניות מחשב או יישומים ניידים מזויפים, לפרסם אותם באינטרנט, ולאחר מכן לפתות אותך להוריד ולהתקין אותן. הורד והתקן תוכניות או אפליקציות מחנויות מקוונות מהימנות בלבד. כמו כן, התרחק מיישומים יחסית חדשים, בעלי מספר מועט של ביקורות חיוביות, אשר מתעדכנים לעיתים רחוקות או הורדו על ידי מספר קטן של אנשים. הפסקת להשתמש בתוכנת מחשב או באפליקציה לנייד? מחק אותה.

פושעי סייבר לעיתים קרובות מטעים אנשים להתקין תוכנות זדוניות עבורם. לדוגמה, הם עשויים לשלוח לך הודעת דוא"ל שנראית לגיטימית ומכילה קובץ מצורף או קישור. ייתכן שהדוא"ל מגיע מהבנק או מחבר. כאשר תפתח את הקובץ המצורף או תלחץ על הקישור, תפעיל קוד זדוני שמתקין תוכנות זדוניות על המערכת שלך. אם נשלח אלייך מסר שיוצר תחושה חזקה של דחיפות, או נראה טוב מכדי להיות אמיתי, תחשוד שמדובר בהתקפה. הייה חשדן, השכל הישר הוא לעתים קרובות ההגנה הטובה ביותר שלך.

בצע גיבוי קבוע של המערכת והעברת קבצים לשירותים מבוססי ענן, או אחסון הגיבויים במקום לא מקוון, כגון כוננים חיצוניים מנותקים. פעולה זו מגינה על הגיבויים שלך במקרה שתוכנות זדוניות ינסו להצפין או למחוק אותן. גיבויים הם קריטיים, הם בדרך כלל הדרך היחידה שאתה יכול לשחזר מזיהום שנגרם עקב תוכנה זדונית.

בסופו של דבר, הדרך הטובה ביותר להתגונן מפני תוכנות זדוניות היא לשמור את כל התוכנות והתקנים שלך עדכניים, להתקין תוכנות אנטי וירוס מהימנות ולהיות ערני ככל האפשר לאפשרות שמנסים לפתות אותך לפעילות שתדביק את המערכת שלך. כאשר כל השאר נכשל, גיבויים קבועים הם בדרך כלל הדרך היחידה שאתה יכול לשחזר במקרה והותקפת.

עורך אורח

לני זלצר נלחם בתוכנות זדוניות על ידי פיתוח מוצרי אבטחה לתחנות קצה במעבדות מינרבה ומלמד במכון SANS. לני פעיל בטוויטר כ- @lennyzeltser *וכותב בלוג אבטחה ב* zeltser.com.

מקורות

תוכנות כופר: https://www.sans.org/u/Edl

גיבויים: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201708_he.pdf

עצור את הדייג: https://www.sans.org/sites/default/files/2018-04/201804-OUCH-April-Hebrew.pdf