אאוץ! | יוני 2017

מרכז סליקה בנקאי בע"מ שירותי בנק אוטומטיים בע"מ

עלון מודעות אבטחת מידע חודשי לכולם

OUCH!

בגיליון זה...

- סקירה כללית
- עדכוני אבטחה
- גיבויים
- התחזות / דיוג

לקחים בעקבות מתקפת WannaCry

סקירה כללית

בזמן האחרון, סביר להניח שראיתם או שמעתם בתקשורת ובחדשות על התקפת סייבר חדשה בשם"WannaCry"."WannaCry" הדביק למעלה מ-200,000 מחשבים, תוכנת הכופר הצפינה לארגונים רבים את המידע, כולל בתי חולים בבריטניה. ישנן מספר סיבות לכך שההתקפה זכתה לכל כך הרבה תשומת לב. ראשית, היא התפשטה במהירות ממחשב למחשב על ידי תקיפת חולשה ידועה במחשבי Windows. שנית, ההתקפה הייתה סוג של תוכנת כופר זדונית בשם "Ransomware", כלומר בעת הדבקת המחשב התוכנה מצפינה את כל הקבצים שלך ונועלת לך את הנתונים. הדרך היחידה שאתה יכול לשחזר את הנתונים שלך הוא לשחזר את המידע מגיבויים או על ידי תשלום סכום של 300 $ לתוקף כדי שיאפשר לך לפענח את הנתונים. הסיבה השלישית, והכי חשובה, התקפה זו מעולם היתה צריכה להתרחש. החולשה ש-"WannaCry" נצלה במחשבי Windows הייתה ידועה היטב על ידי מיקרוסופט שפרסמה תיקון לפני מספר חודשים. אבל ארגונים רבים לא הספיקו להתקין את התיקון בזמן, או שעדיין משתמשים במערכות הפעלה ישנות כמו Windows XP, שהן כה ישנות, שלא משוחררים להן תיקונים. הנה שלושה צעדים פשוטים שניתן לבצע על מנת לוודא שהתקפות כמו "WannaCry" לא ידביקו אותך.

עורך אורח

בירלוא סנהוי ר"ד הוא דיקן המחקר של המכון לטכנולוגיה SANS ומייסד DShield.org. הוא אחראי על **Internet Storm Center** של SANS , אשר עוקב אחר איומי האבטחה הקברטית. הוא מלמד יישומי אינטרנט ואבטחה קורס (**DEV522**), איתורי פריצה קורס (**SEC503**) וקורס (**SEC546**) IPv6.

עדכוני אבטחה

בראש ובראשונה, חשוב לוודא שכל המחשבים, נייחים וניידים, תוכנות וכל דבר אחר המחובר לאינטרנט יהיה מעודכן. פושעי הסייבר מחפשים כל הזמן נקודות תורפה חדשות בתוכנה של המכשירים שלך. כאשר הם מגלים פגיעויות, הם משתמשים בתוכניות מיוחדות אשר נועדו לפרוץ למכשירים שבהם אתה משתמש. בינתיים, החברות שיצרו את התוכנות עבור המכשירים שלך עובדות קשה על מנת לתקן פגיעויות אלו על ידי הפצת עדכונים. כאשר אתה שומר על המכשירים שלך מעודכנים, אתה מקשה על פושעי הסייבר להצליח בהתקפה שלהם. זה מה שכל כך מתסכל

לקחים בעקבות מתקפת WannaCry

בהתפשטות של WannaCry. העדכונים שסוגרים את הפרצה של ההתקפה שוחררו כמעט חודשיים קודם לכן על ידי מיקרוסופט. אילו ארגונים היו מעדכנים את המחשבים שלהם, ההתקפה הזאת לא הייתה עובדת. כדי להבטיח שההתקנים שלך יישארו מעודכנים, יש לאפשר עדכונים אוטומטיים בכל עת. כלל זה חל על כל טכנולוגיה אשר מחוברת לרשת, לא רק את המחשבים הנייחים והניידים, גם טלוויזיות חכמות, נתבים, קונסולות משחקים או יום אחד אולי אפילו את המכונית שלך. במידה ומערכות ההפעלה שלך ישנות עד שהן אינן נתמכות עוד עם עדכוני אבטחה, כגון Windows XP, החלף אותם במערכות חדשות אשר מקבלות עדכוני אבטחה.

המפתח להגנה על עצמך מפני התקפות כמו WannaCry הם שלושה שלבים פשוטים; לשמור על המחשבים שלך מעודכנים, להיות זהירים מהתקפות פישינג וגיבוי המערכות שלך.

גיבויים

במקרים מסוימים, התקפות סייבר כמו Ransomware עשויות להדביק מערכות עדכניות. דרך נוספת להגן על עצמך היא גיבוי הנתונים. גיבויים הם עותקים של המידע המאוחסן במקום אחר מאשר במחשב. כאשר אתה מאבד נתונים בעלי ערך, תוכל לשחזר את הנתונים מהגיבויים. למרבה הצער, יותר מדי אנשים נכשלים לבצע גיבויים סדירים, למרות שזה תהליך פשוט ולא יקר. קיימות שתי דרכים לגיבוי הנתונים: מדיה פיזית או אחסון מבוסס ענן. לכל גישה יש יתרונות וחסרונות. ניתן להשתמש בשתי הגישות בו-זמנית, אם אינך בטוח באיזו שיטה להשתמש.

מדיה פיזית אלו התקנים שאתה שולט בהם כגון כונני USB חיצוניים או כוננים המחוברים לרשת בבית או במשרד. היתרון של שימוש במדיה הפיזית הוא שהם מאפשרים לך לגבות ולשחזר כמויות גדולות של נתונים מהר מאוד. החיסרון של גישה כזו הוא שאם אתה נגוע בתוכנה זדונית, כגון תוכנת כופר, הזיהום עלול להתפשט לגיבויים. אם אתה משתמש במדיה פיזית עבור גיבויים, עליך לאחסן עותקים של הגיבויים במקום בטוח. ודא שכל הגיבויים שאתה מאחסן מסומנים כהלכה. פתרונות מבוססי ענן הם שירותים מקוונים לגיבוי ושמירת הקבצים באינטרנט. בדרך כלל, אתה מתקין תוכנה במחשב אשר דואגת להכל. היתרונות של פתרונות ענן היא הפשטות שלהם. בנוסף, אם אתה נגוע בתוכנת כופר, הזיהום בדרך כלל לא יכול לגשת לגיבוי מבוסס ענן, ולעיתים נשמרות גרסאות ישנות של אותם קבצים

לקחים בעקבות מתקפת WannaCry

שגיבית. החסרונות הם כי זה יכול לקחת זמן רב כדי לגבות או לשחזר כמויות גדולות מאוד של נתונים. הקפד לחקור את הפרטיות והאבטחה של גיבויי ענן. האם שירות הגיבוי מספק אבטחה חזקה כגון הצפנת הנתונים ואימות חזק?

התחזות / דיוג

לבסוף, הרעים תמיד מעדכנים ומשנים את שיטות ההתקפה שלהם. פושעים סייבר לעתים קרובות ישתמשו בשיטת התקפה נוספת בשם דיוג או התחזות על מנת לתקוף ולהדביק קורבנות. התחזות היא כאשר פושעי סייבר שולחים אליך הודעת אימייל שמנסה לפתות אותך לפתוח קובץ מצורף נגוע או לבקר באתר זדוני. אם תעשה זאת, המחשב עלול להידבק. בעוד "WannaCry" לא השתמשה בשיטת תקיפה זו, זה נפוץ עבור סוגים רבים של התקפות, כולל רוב סוגי תוכנות הכופר. בנוסף, פושעי סייבר שפיתחו את WannaCry יאלצו ללא ספק לעדכן את שיטות ההתקפה שלהם בחודשים הקרובים ולהשתמש בטכניקות חדשות כגון התחזות על מנת להדביק עוד מחשבים. המפתח להגנה על עצמך מפני התקפות מבוססות דואר הוא השכל הישר. אם דוא"ל או הודעה נראה מוזר, חשוד או טוב מכדי להיות אמיתי, סביר להניח כי זו התקפה.

למד עוד

הרשם לעלון OUCH! המפורסם אחת לחודש, עלון זה מתמקד במודעות אבטחת המידע, ניתן לקרוא עלונים קודמים וניתן ללמוד על מודעות אבטחת המידע של SANS באתר securingthehuman.sans.org/ouch/archives.

מקורות

מהי תוכנה זדונית:	https://securingthehuman.sans.org/ouch/2016#march2016
תוכנות כופר:	https://securingthehuman.sans.org/ouch/2016#august2016
גיבויים:	https://securingthehuman.sans.org/ouch BehaAugust2015
דיוג:	https://securingthehuman.sans.org/ouch BehaDdember2015
שימוש בענן מאובטח:	https://securingthehuman.sans.org/ouch/2016#november2016

עורכי המערכת: ביל ויימן, וולט סקריוונס, פיל הופמן, בוב רודיס, שריל קונלי
תורגם על ידי: גדי מרגלית ודרור ענבר