מקרה מבחן

כאשר נמל התעופה של לונדון שימש כיעד להתקפת סייבר הרסנית, המדפסות של HP זיהו את האיום

דוח סיכום רשמי עבור הפריצה לנתונים

מגזר עסקי
תעופה

המטרה
זיהוי חוליות חלשות בשיטות אבטחת סייבר וטיפול בהן

הגישה
פיתוח תוכנית אבטחה מקיפה ביחד עם מומחי האבטחה של HP

IT קובע
- החלת אמצעי אבטחה על נקודות קצה של IoT
- הפיכת מאפייני אבטחה מובנים לזמינים במדפסות HP
- שיפור ניטור האבטחה ברשת

העסק קובע
שיפור אבטחת הסייבר להגנה על תשתית בינלאומית בסיסית ולשמירה על בטיחות הנוסעים

סקירה

נמל התעופה של לונדון* משרת יותר מ-300,000 נוסעים מדי יום בזמן שהם נוסעים ל-94 מדינות בכל רחבי העולם. קרוב ל-50,000 אנשים מ-300 חברות עובדים בנמל התעופה והופכים אותו למעשה לעיר צפופה.

כאשר נמל התעופה גדל, התשתית שלו הפכה יותר ויותר למחוברת ולאוטומטית. מערכות פנימיות, החל מחימום, אוורור ומיזוג אוויר, דרך תאורה וכלה במדפסות, נמצאות כעת ברשת של נמל התעופה. הדפסה, סריקה והעתקה מתבצעות על-ידי צי הכולל יותר מ-60 מדפסות רב-תכליתיות של HP המפוזרות בכל רחבי השטח.

ב-23 באפריל 2018, פושע הסייבר המוכר רק כ"הזאב" השתמש במערכות התאורה המקושרות של נמל התעופה כדי לקבל גישה ולהפיץ את התוכנה הזדונית שלו ברחבי הרשת. כיוון שהוא מפורסם בשימוש שלו לרעה בנקודות קצה שאינן מאובטחות דיין, מומחי אבטחת ה-IT פנו מיד ליומני אירועים ממדפסות HP Enterprise שלהם כחלק מהחקירה, כדי לבודד ולעצור את המתקפה. באופן מפתיע, יומני הרישום הכילו רמזים מ"הזאב" שיכלו לספק מידע על המיקום המקורי של החדירה. לאחר מכן, נמל התעופה של לונדון פנה ל-HP כדי לשפר עוד יותר את אבטחת נקודות הקצה שלו.

מה קרה

כאשר "הזאב" מצא נקודת תורפה, ככל הנראה על-ידי דיוג הודעות דוא"ל למשתמשים ברשת, הוא הצליח לזהם את מערכת התאורה של IoT בתוכנה זדונית. לאחר מכן הוא הצליח להפיץ את התוכנה הזדונית ברשת וקיבל דריסת רגל בהתקני נקודת קצה לא מנוטרים אחרים.

על-ידי הסתרת הנוכחות שלו בהתקני IoT לא

מנוטרים, הצוות של "הזאב" נשאר מוסתר ממערכות ניטור הרשת בזמן שפיתח נקודות הפעלה מרובות עבור התקפה הרסנית גדולה.

הנהלת נמל התעופה ניסתה נואשות לכבות מערכות מרובות תוך שמירה על תשתית בסיסית כגון המטוסים והנוסעים שעוברים שם.

התגובה למתקפה

"הזאב" נשכר כדי לתקוף את רשת נמל התעופה. צוות אבטחת ה-IT של נמל התעופה *האמין* שהרשת של נמל התעופה הייתה מוגנת היטב מפני פורצי מחשבים, אבל הייתה חסרה לו ניראות של האיומים המסתתרים בהתקני IoT.

למרבה המזל, מדפסות HP Enterprise של נמל התעופה כללו HP Connection Inspector, שעצר את התוכנה הזדונית כאשר היא ביצעה ניסיונות חשודים "להתקשר הביתה" לשרתי הפיקוד והבקרה של הפצחנים.

הפעולות תועדו ביומני הרישום של המערכת של המדפסת. כאשר צוות ה-IT הבין שמשהו לא בסדר, הוא בדק את יומני הרישום של המערכת וחיפש פרטים בנוגע למתקפה. אבל לזמן יש חשיבות עיקרית כאשר תוכנה זדונית מתפשטת ברשת. אם צוות אבטחת ה-IT היה מחבר את יומני הרישום של המערכת לזיהוי איומים של המדפסות למערכת אבטחת המידע וניטור האירועים (SIEM) שלו, הוא היה מקבל התראה מיידית כאשר אירעה החדירה.

אבטחה חזקה יותר מאי פעם

לאחר שאירעה הפרצה, צוות ה-IT סקר את נהלי האבטחה ביחד עם ספק שירותי ההדפסה המנוהלת ויועצי האבטחה של HP.

על-ידי התקנת מדפסות HP Enterprise, נמל התעופה של לונדון היה כבר במסלול הנכון. רק מדפסות HP Enterprise והמדפסות הרב-תכליתיות של HP מספקות זיהוי חדירה בזמן ריצה ואת HP Connection Inspector כדי לזהות ולעצור תוכנה זדונית במהלך פעולתה ולאכוף אתחול. בעת האתחול, HP Sure Start בודק את ה-BIOS ויכול לבצע תיקון עצמי אם הקוד נפגע, בעוד שיצירת הרשימות הלבנות בודקת את הקושחה.

ספק שירותי ההדפסה המנוהלת פרס את HP JetAdvantage Security Manager כדי לבדוק באופן אוטומטי הגדרות אבטחה בכל פעם שמדפסת מאותחלת ולאפס את כל ההגדרות שהשתנו.

צוות אבטחת ה-IT של נמל התעופה חיבר את יומני הרישום של המערכת של המדפסת לכלי SIEM שלהם. בניגוד למדפסות של יצרנים אחרים, ההתקנים של HP יכולים לספק יומני רישום ספציפיים לאיומים לכלי SIEM רבים כך שצוות ה-IT יכול לקבל התראות בזמן אמת על תקריות אבטחה אפשריות. זה הופך את המדפסות של HP ל"עיניים" חשובות לאין ערוך ברשת שלהן.

סוף דבר

בגלל מדפסות HP Enterprise של נמל התעופה והרמזים ש"הזאב" השאיר אחריו, צוות האבטחה הצליח לבודד את ההתקפה במהירות ומנע הפרעה לתפעול, פרסום שלילי, קנסות על אי ציות לתקנות ונזק למותג.

על-ידי שימוש בשיטות אבטחה חזקות יותר וניצול מלא של מאפייני האבטחה המובנים של מדפסות HP שלו, נמל התעופה הידק את האבטחה בכל רחבי הרשת.

**נמל התעופה של לונדון הוא ארגון בדוי ששימש כמטרה להתקפת סייבר גדולה בסרט של HP Studio, "THE WOLF": אלפא אמיתי."*

לקבלת מידע נוסף על פתרונות HP:
אבטחת הדפסה: hp.com/go/reinventsecurity
אבטחת מחשב: hp.com/go/ComputerSecurity

כדי לצפות בסרטי "The Wolf", בקר בכתובת:
hp.com/thewolf

הירשם לקבלת עדכונים
hp.com/go/getupdated

שתף עם עמיתיך

4AA7-3560HEE, אוגוסט 2018