מבט על, גיליון 867, 13 בנובמבר 2016

איום של צבא התקנים-מקושרים לרשת

גבי סיבוני, טל קורן

לפחות שלושה גלים רצופים של התקפות מקוונות מורכבות כוונו לשרתי הקצאת שמות לכתובת אינטרנט (DNS) שמפעילה ספקית תשתיות האינטרנט האמריקאית Dyn. הייתה זו תקיפת מניעת שרות (DDoS), שבוצעה ב-21 באוקטובר 2016. התקיפה גרמה לחסימה של הגישה לאלפי אתרי אינטרנט, ביניהם Twitter, Amazon, Netflix, PayPal, *New York Times*, Airbnb. החשד המידי לביצוע התקיפה נפל על רוסיה וסין, כמי שלכאורה יש להן הן מניע והן יכולת ליזום אותה ולהוציאה לפועל. אולם נכון לזמן כתיבת שורות אלו, כלל לא ברור האם המניע לתקיפה אכן היה מדינתי. אחרי התקיפה דווח כי קבוצת האקרים סינית ורוסית בשם New World Hacker נטלה אחריות לביצועה וטענה כי מדובר בתקיפה מתוחכמת, שעשתה שימוש ב-botnets ובתעבורה בקצב גבוה יותר ממה שהיה ידוע עד כה, של 1.2 טרה ביט לשנייה.

בתקיפה זו נעשה שימוש במספר רב של התקנים מקושרים (חברת Dyn הודיעה לתקשורת כי כ-100,000 התקנים היו מעורבים בה). התקנים אלה, הקרויים "אינטרנט של דברים" (IoT – Internet of Things), כוללים מצלמות רשת, מערכות אזעקה, חיישנים לחדרי ילדים, מצלמות אבטחה מבוססי אינטרנט, מערכות הקלטה (DVRs) ונתבים (routers) — כולם מחוברים לרשת האינטרנט. התוקפים הצליחו לשתול בהתקנים אלה רכיב תוכנה שיכול לקבל פקודה משרת שליטה ולפנות לגורם המותקף באופן מסונכרן, יחד עם עשרות אלפי התקנים אחרים, ולשתק את יכולת התפקוד של השרת המותקף על ידי הצפתו בפניות. רובם המכריע של ההתקנים האלה נעדרים כל מנגנוני הגנה משמעותיים, כשהגישה לרוב המערכות הנה באמצעות שמות וסיסמאות ברירות מחדל, המותקנות על ידי היצרן. למעשה, לא קיימת כל תפיסה עדכנית אפקטיבית להתמודדות מול האיום הזה.

האיום הגלום בנחילי התקנים-מקושרים איננו חדש. חברת האבטחה סימנטק דיווחה עוד בשנת 2013 על תולעת בשם Linux.Darlloz, אשר הדביקה, לפי הערכות, כחמישים אלף התקני IoT, כגון נתבים והתקני STB (Set-Top-Box) או מחשבים מבוססי ארכיטקטורת אינטל (X86). המטרה הייתה להתקין תוכנה המאפשרת לכרות (Mine) מטבעות וירטואליים – Crypto currencies. בשנת 2015 הוציאה אותה חברה דו"ח מפורט על אודות הקלות שבה ניתן לפרוץ ל-50 התקני "בית חכם" (Smart Home Devices). בדו"ח מאפריל השנה דיווחה החברה, כי מכשירים רפואיים (כגון: משאבות אינסולין, מערכות רנטגן וסורקי CT), אף הם חשופים לתקיפה, וכן מערכות טלוויזיה חכמה, ועוד עשרות מכשירים מסוגים שונים.

אף שהיכולת לחדור להתקנים האלה ולבצע באמצעותם תקיפות מניעת שרות רחבות לא הפתיעה, הרי שעוצמת המתקפה הדגימה את יכולת ההרס של שימוש במספר רב של התקנים פשוטים, המופעלים באופן מסונכרן. תקיפה זו שברה את השיא של מתקפת ה DDoS הגדולה ביותר, שהתרחשה בספטמבר 2016, אשר בוצעה נגד חברת OVH הצרפתית בהיקף של 1Tbps, ובה נעשה שימוש בסוכני תוכנה (Bots) שניצלו מצלמות CCTV נפוצות. זוהי הסלמה מסוכנת המציבה רף חדש לאיום קיברנטי שאין לו מענה נאות, וזאת ממספר היבטים.

הראשון נוגע להיקף תפוצתם של ההתקנים הללו. בארצות הברית יש כ-25 התקנים מקושרים לכל 100 תושבים, וזאת רק ההתחלה. חברת Gartner מעריכה כי במהלך 2016 ייספרו בעולם 6.4 מיליארד התקנים-מקושרים, ועד שנת 2020 יגיע מספרם לקרוב ל-21 מיליארד. מספר התקנים רב שכזה יוצר ברשת האינטרנט רכיב של חולשה ניכרת, ומאפשר שימוש בהם למגוון צרכים

של תוקפים למיניהם. החידוש בתקיפה הנדונה הוא הפשטות שבביצועה. מיליוני התקנים יכולים להיות אמצעי פוטנציאלי למתקפות סייבר DDoS, שביצוען קל יחסית. כל זאת, משום שההתקנים יוצרים נקודות כניסה חדשות לרשת, ולכן היקף האיום גדול. סיכון זה גדל עוד יותר בשל השימוש במכשירי קצה, דוגמת טלפונים חכמים ומחשבים, לצורך שליטה על ההתקנים המקושרים.

ההיבט השני נוגע לחולשת ההגנה. לרוב התקני IoT חסרים אמצעי אבטחה נאותים ולכן ההתקפות יכולות לנצל חולשות במערכות המפעילות את ההתקנים. לא קיימת עדיין מסגרת תקינה ואבטחה שאומצה על ידי מירב היצרנים והם עושים בדרך כלל שימוש בקוד ציבורי פתוח המאפשר להתקנים לתקשר עם מכשירים אחרים בסביבתם, אולם בה בעת יוצר חולשות אבטחה חמורות. צעדים חיוניים בכיוון זה כבר החלו להתבצע בשיתוף פעולה בין חברות אבטחה, איגודי יצרנים ואף גורמים ממשלתיים בארצות הברית. אולם, אלה רחוקים עדיין מלהבשיל לכדי תפיסת הגנה מספקת.

ההיבט השלישי נוגע להיקף ולעוצמת הנזק. המתקפה על חברת Dyn היא תמרור אזהרה משמעותי מאחר שיכולת התקיפה שהודגמה אינה נשענת על יכולות מתוחכמות במיוחד, ואילו עוצמת הפגיעה הייתה משמעותית. העובדה שהקוד המפגע פורסם ברבים מכשירה את הקרקע לתקיפות נוספות שיסתמכו על קוד זה או דומה לו, ומעלה את האפשרות שלכותבי הקוד יש כבר גרסה משופרת שלו. לכן ניתן להניח ששימוש בשיטות תקיפה דומות עתיד לחזור, ואף בעוצמות גדולות יותר.

לבסוף, נושא הפרטיות. אחת הבעיות המרכזיות של התקנים-מקושרים הנה הבטחת פרטיות המשתמשים. התקנים מחוברים אוספים דרך קבע מידע רב על מגוון פרמטרים של השימוש בהם, בבית המגורים ובמשרד, כולל מאפייני שימוש בציוד ומכשירי חשמל, וכן שימוש בהתקנים לבישים (Wearable Devices), שעתידים להיות נפוצים עוד ועוד. חולשות ההגנה המובנות בהתקנים אלו עלולות לאפשר למידע להיות זמין לתוקפים שונים, שיעשו בו שימוש שאינו ראוי.

החולשה שהודגמה בתקיפה האחרונה אינה יכולה להישאר נחלת המגזר הפרטי שהותקף. השימוש בצבאות של התקנים-מקושרים מהווה אתגר גם ברמה המדינתית, שכן באפשרותו לפגוע בתפקוד המדינתי בשגרה, וחמור מכך - בזמן חרום ומלחמה. משום שהסיכון ממשי, ההגנה על התקנים-מקושרים היא אתגר משמעותי. בעקבות התקיפה הנדונה שבה ועלתה קריאה לממשלת ארצות הברית להסדיר על ידי רגולציה את אבטחת מוצרי IoT. נראה שזה המקום למיקוד המאמץ, בדומה לצעדים שננקטו במגזר הפיננסי. אף שהבעיה הנה כלל עולמית, טוב יהיה אם גם הגורמים האמונים על ביטחון הסייבר בישראל יפנימו את עוצמת החשיפה למתקפות כאלו ויפעלו כדי להיות שותפים למאמצים הבינלאומיים בהקשר זה, ובמקביל יפעלו לשכלל את מנגנוני ההגנה והמשך התפקוד המתאימים להתמודדות מול סוג זה של תקיפות.

ד״ר גבי סיבוני הוא חוקר בכיר וראש תכנית ביטחון סייבר.
ד״ר טל קורן הוא חוקר בתכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.