22.3.2020

פוטין מאדים בכיכר האדומה: שירות הביון הרוסי נפרץ

מאת יוסי הטוני 22במרץ 2020
נחשפו מסמכים של תכנית פרונטון של הפס"ב, המחליף של הקג"ב מטרתה של התכנית היא לנצל פגיעויות אבטחה מרובות בהתקני אינטרנט של הדברים - טכנולוגיות פחות מאובטחות מההתקנים המחוברים האחרים.

קבלן משנה של **הפס"ב** ,שירות הביטחון הפדרלי הרוסי, או אולי השירות עצמו – נפרץ, כך דיווח **פורבס** בסוף השבוע. הפריצה חשפה כלי נשק חדש, שהוזמן על ידי שירות הביון ושנועד לבצע מתקפות סייבר ברכיבי האינטרנט של הדברים. התכנית של הפס"ב שנחשפה מכונה "תכנית פרונטון", ומטרתה לנצל פגיעויות אבטחה מרובות בהתקני IoT – טכנולוגיות פחות מאובטחות מההתקנים המחוברים האחרים בבתים ובמשרדים. אחד המסמכים הטכניים שנגנבו, שעליו דיווחה BBC רוסיה, הסביר כי "האינטרנט של הדברים פחות בטוח מאשר מכשירים ושרתים ניידים". מקצועני אבטחה ציינו שהפריצות העתידיות נועדו להתבסס על החולשה המובנית בסמאות ברירת המחדל של אותם רכיבים, שקל לנצל אותן.

ייעודה של התכנית שנפרצה ונחשפה אינו להשיג גישה לבעלי המכשירים הללו, אלא לנצל את היותם נקודות קצה של מחשוב ולהפוך אותם לרשת בוטים, שניתן להשתמש בהם כדי לתקוף יעדים גדולים – פלטפורמות אינטרנט גדולות בארצות הברית ובאירופה, או תשתית רשתית של מדינות שלמות, דוגמת אלה שגובלות ברוסיה.

במסמכים המאובטחים שחשפה קבוצת ההאקרים שפרצה מצוטטים קבלני המשנה של פס"ב כי "מתקפה עוצמתית של כמה מאות אלפי מכונות יכולה להפוך אתרי רשתות חברתיות או שירותי אירוח לקבצים לבלתי נגישים למשך כמה שעות.

מתקפה על שרתי DNS ארציים עלולה להביא למניעה של שירותי האינטרנט למשך כמה שעות במדינה קטנה."

עוד מציינים קבלני המשנה של ארגון הביון הרוסי את מתקפת – Miri עם שגיאת כתיב. הכוונה היא למתקפת הענק שערכו האקרים באוקטובר 2016, שהביאה לנפילה ארוכה של מאות אתרים, עם מתקפת מניעת השירות המבוזרת) ה-DDoS) הגדולה ביותר אי פעם. הם הפיצו את הקוד הזדוני Mirai למכשירי אינטרנט של הדברים ועל בסיסו התוקפים ערכו מתקפות מניעת שירות מבוזרת. מתקפת הענק, שהביאה לנפילות ולשיבושים קשים ורבים של מאות אתרים בארצות הברית, נמשכה כחצי יממה ומאות אתרי אינטרנט נפגעו ממנה, ביניהם רבים וגדולים בעולם, דוגמת **אמזון**, **טוויטר**, **נטפליקס**, **אי-ביי**, **Airbnb**, **ספוטיפיי**, וכן אתרי מדיה וחדשות. יעד המתקפה היה **דיין** (Dyn), חברת תשתיות אינטרנט וספקית שירותי DNS. המתקפה הסבה נזק רב יחסית, בכך שהתמקדה בחברת תשתיות אינטרנט ולא בלקוחותיה. Mirai ניצלה את התקני האינטרנט של הדברים כדי לבצע את המתקפה הגדולה ביותר בהיסטוריה מסוג מניעת שירות מבוזרת ופגעה בכ-600 אלף מחשבים בעולם.
על פי המדווח, לא היה קשה לעקוב אחרי מי עקבו אותם קבלני משנה: אב הטיפוס של כלי הנשק שהוזמן פותח על ידי – **InformInvestGroup CJSC** בהוראת יחידה צבאית מספר 64829. יחידה זו ידועה יותר בשם "מרכז אבטחת המידע של הפס"ב."
המכשירים שנועדו להיות מנוצלים על ידי כלי הפריצה שפותחו הם מצלמות ו-NVR – מערכות ההקלטה שלהן. "אם הם משדרים וידיאו", מסבירים הקבלנים, "יש להם ערוץ תקשורת גדול מספיק כדי לבצע מתקפת מניעת שירות מבוזרת ביעילות."

תקיפה זו באה יותר שמונה חודשים לאחר שדווח על פריצה ל-SyTech, קבלן משנה של הפס"ב, שעובד על טכנולוגיית מעקב באינטרנט.

שירות הביון הרוסי לא הגיב לדיווח.