גאזט סייבר

שישי, י׳ בכסלו תשפ״ז · 20 בנובמבר 2026 · גיליון 7 · מגזין סוף השבוע

תחקיר השער · ארה״ב · תקלות או מתקפה

המיילים קרסו, המטוסים קורקעו, הבנקים נתקעו: יום הדין של הסייבר?

שבעה ימים, שבע קריסות, אף תוקף מוכח. מה באמת קרה לאמריקה, ולמה המתקפות האמיתיות של השבוע קרו דווקא במקום אחר

גאזט סייבר · תחקיר השער · כל עובדה מקושרת למקור · המקורות נבדקו מחדש ב־19.11.2026

הסיפור בקצרה

- בשבעה ימים קרסו מיקרוסופט, Workday, הבקרה האווירית בארה״ב, JPMorgan Chase, יונייטד, אפל והרשת המסווגת של NSA.
- אף אחת מהקריסות לא נקשרה לתוקף. כך אומרות החברות, ראשי המודיעין וה־FBI.
- ברוב המקרים שבהם נמסרה סיבה, הגורם הוא שינוי: עדכון, נתב חדש או מעבר בין מערכות. רק ב־NSA נקשרה התקלה לעדכוני אבטחה.
- מתקפות אמיתיות דווקא היו: ספקים של Chase נפרצו, מקפיאים באירופה הושבתו, וחברה ישראלית נסחטה בעזרת AI.

בגיליון · הקישו לקפיצה

תחקיר השער: התחקיר המלא ←

השבוע בסייבר · החדשות ←

תחקיר שני · סחיטה בידי AI ←

תחקיר שלישי · מתקפת המקפיאים ←

ב יום שישי בערב, 13 בנובמבר, קצת אחרי עשר וחצי בשעון ישראל, נעצרו כל ההמראות בארצות הברית. כ־3,500 מטוסים שכבר היו באוויר נחתו בבטחה, ואלפי טיסות בוטלו. יום קודם לכן קרס שירות הדואר של מיקרוסופט בעשרות מדינות, לכמעט יממה. בימים שאחרי נתקעו עסקאות בבנק הגדול באמריקה, מטוסים של חברת תעופה גדולה חיכו על הקרקע, שירותי הענן של אפל נפלו, ורשת המחשבים המסווגת של סוכנות הביון האלקטרוני האמריקאית התקשתה לעלות. ברשתות החברתיות נשאלה שאלה אחת: האם זו מתקפת סייבר מתואמת, יום הדין שמזהירים ממנו כבר שנים?

התשובה, לפי כל מי שחקר את האירועים עד עכשיו, היא לא. אף אחת משבע הקריסות לא נקשרה לתוקף. כך אומרות החברות עצמן, וכך אומרים ראשי המודיעין האמריקאי, ה־FBI וסוכנות הסייבר CISA. אבל התשובה המלאה מעניינת יותר מ"לא". מתחת לרעש יש דפוס: עדכונים, החלפות ציוד ומעברים בין מערכות שנעשו בלחץ, על מערכות ישנות או צפופות מדי. ובאותם ימים ממש התרחשו גם מתקפות אמיתיות. הן פשוט קרו במקום אחר.

ציר הזמן: שבוע של קריסות

- **12.11, 18:20** Microsoft 365 קורס בעולם, עד 18:10 למחרת (מיקרוסופט).
- **13.11, ערב** Workday: אתר הגיבוי מתחבר בטעות למסדי הנתונים החיים (DRJ).
- **13.11, 22:30** רשות התעופה FAA עוצרת את כל ההמראות בארה"ב. העצירה מוסרת ב־03:15 (FAA).
- **16.11, 18:30** עסקאות נתקעות אצל לקוחות JPMorgan Chase. הבנק: באג תוכנה, לא סייבר (CNBC).
- **16.11, 23:02** יונייטד איירליינס מעכבת המראות כשעה ו־40 דקות (AeroTime).
- **17.11, 18:45** שירותי אפל נופלים לכ־6 שעות. אפל: "עדכון פנימי" (TechCrunch).
- **17.11** הרשת המסווגת של NSA משובשת. מנהל המודיעין קושר את התקלה לעדכוני PHP (CBS).
- **19.11, 15:17** JPMorgan Chase: ספקים שלו נפרצו. "אין קשר" לתקלה (X).
- **20.11** המועד שקבעה מיקרוסופט לדוח הסופי. עד ערב 19.11 הוא לא פורסם.

השעות בשעון ישראל. מקורות: מיקרוסופט, FAA, DRJ, CNBC, AeroTime, TechCrunch, CBS, The Record, Reuters.

פרק 1 · מיקרוסופט: שלושה כשלים קטנים

הקריסה הגדולה הראשונה הייתה של מיקרוסופט. לפי הדוח המקדים של החברה, מ־18:20 ביום חמישי, 12 בנובמבר, ועד 18:10 למחרת, לא עבד השער שדרכו מגיעים משתמשים ל־Outlook ולשירותי Microsoft 365. לפי ה־BBC, נפגעו לפחות 74 מדינות. באוסטרליה נפגעו גם שירות הביטחון והמשטרה הפדרלית, ורשת בתי חולים בטורונטו הכריזה על "קוד אפור", כלומר כשל תשתית. לפי ה־Guardian, בתי חולים עברו לנייר. גם בישראל לא עבד Outlook במחשבים, לפי TheVerifier.

הקריסה חשפה גם כמה העולם תלוי בספק אחד. לפי ה־BBC, מפעילת הבורסות Euronext הנחתה חברות נסחרות להעביר מידע בטלפון. בגרמניה לא נפגעו רשויות המדינה, כי הן לא נשענות על Microsoft 365, כך אמרה ראש סוכנות הסייבר הגרמנית, קלאודיה פלטנר. לפי ישראל היום, מכון המחקר Anderson Economic Group מעריך את אובדן הפריון העולמי בלפחות 7 מיליארד דולר. זו הערכה ראשונית, לא נתון מדוד.

הסיבה, לפי מיקרוסופט, היא שלושה כשלים קטנים שנפגשו. הראשון: תיקון לשרתי השער, שהופץ כבר מיולי, ויצר באג רדום. תחת עומס מסוים נתקע תהליך פנימי בשרת, והשרת הפסיק להגיב. בבדיקות העומס במעבדה הבאג לא התגלה, כי הן נעשו בעיקר על חומרה חלשה עם פחות ליבות, שבה הוא כמעט לא מופיע. הבאג מחמיר דווקא בשרתים חדשים עם הרבה ליבות. השני: כ־15 שעות קודם לכן עבר Teams, כנוהל קבוע, לשער שמשרת גם את הדואר. השלישי: כמעט 14% משרתי השער כבר היו מושבתים בגלל תקלה אחרת מהיום הקודם.

מכאן התחיל אפקט דומינו. מערכות הניתוב האוטומטיות העבירו משתמשים משרת שנפל לשרת תקין, וכך העבירו אליו גם את העומס. בתוך פחות משעתיים נפגע רוב הצי, ובשיא לא הגיבו יותר מ־80% מהשרתים. המחיצות בין האזורים, שאמורות לעצור כשל כזה בגבולות אזור אחד, לא עצרו אותו. מנכ"ל מיקרוסופט

סאטיה נאדלה אמר ל־CNBC ב־18 בנובמבר: "היינו צריכים להבין איך לבנות את המחיצות כך שלא תהיה השבתה עולמית". לפי Ars Technica, הדוח הסופי, שתוכנן ל־20 בנובמבר, אמור להסביר למה המחיצות כשלו. עד ערב יום חמישי הוא לא פורסם.

ההתאוששות הייתה איטית במיוחד. לפי הדוח, שרתים שחזרו לפעולה הוצפו מיד בתנועה שחיכתה להם, ונפלו שוב. צ'ארלס למאנה, סגן נשיא בכיר במיקרוסופט, תיאר ב־X "כשלים מתגלגלים ועדרים רועמים", כלומר המוני משתמשים שמנסים להתחבר באותו רגע. הבאג היה בן חודשים, ולכן הכלים הרגילים להחזרת שינוי לאחור לא עבדו. ב־21:00 שעון ישראל עצרה מיקרוסופט כל פריסה ושינוי תצורה. המהנדסים כתבו עדכון ל־Windows שמחזיר את הקוד למצבו הקודם, ויישמו אותו על יותר מחצי אזור בכל פעם.

ומתקפה? "זו הייתה תקלה טכנית שאינה קשורה לסייבר או ל־AI ולסוכנים", כתב חשבון הסטטוס של מיקרוסופט ב־X. ערוץ טלגרם בשם Dark Storm Team פרסם צילומי מסך ו"לוח תקיפה", ונראה שניסה לקשור את עצמו לקריסה. לפי DarknetSearch, ההוכחה שפרסם מתוארכת כמעט חמש שעות אחרי תחילת התקלה, ורמת הראיות לייחוס "נמוכה". דווקא מתקפה אמיתית רכבה על התקלה: לפי צוות המודיעין של מיקרוסופט, מ־13 בנובמבר נשלחו הודעות פישינג, כלומר הודעות מתחזות, שציטטו את מספר האירוע האמיתי.

תחקיר השער

פרק 2 · מהשכר ועד השמיים

קריסה שנייה, כמעט נשכחת, הייתה של Workday, מערכת משאבי אנוש ושכר של חברות רבות. לפי DRJ, כתב עת לניהול המשכיות עסקית, ביום שישי, 13 בנובמבר, אתר הגיבוי של החברה "התחבר באופן בלתי צפוי" למסדי הנתונים החיים, במהלך בדיקה שבועית של חלון התחזוקה. הנתונים יצאו מסנכרון, וכל לקוחות הייצור באזור WD1 הועברו למצב תחזוקה עד שבת. לפי Niguro, עובדים לא יכלו להחתים שעון או לראות תלוש. כאן מערכת הגיבוי עצמה גרמה לנפילה.

ואז הגיעה רשות התעופה הפדרלית, FAA. לפי מסמך השאלות והתשובות שפרסמה, בסביבות 22:30 שעון ישראל הוצפה רשת התקשורת שלה ב־1,000 ניסיונות התחברות כל ארבע עד חמש שניות". הציוד הישן לא עמד בזה: 17 מתוך 22 מרכזי הבקרה האזוריים איבדו יציבות, והתקשורת עם המטוסים ותמונת המכ"ם נפגעו. ההמראות נעצרו בכל המדינה עד 03:15. לפי הרשות, כ־3,500 מטוסים נחתו בבטחה. לפי Reuters, נפגעו יותר מ־18,000 טיסות ומיליון נוסעים, בעצירה הארוכה ביותר מאז 11 בספטמבר 2001.

מה הציף את הרשת? לפי ה־FAA, שני מקורות אפשריים: אתר מכ"ם באמרילו שבטקסס, ואתר תקשורת באל דוראדו שבארקנסו, שם התקינה חברת L3Harris, הקבלנית שמפעילה את הרשת, נתב חדש. שר התחבורה שון דאפי אמר ל־ABC שזו הייתה ההתקנה ה־69 של הנתב, ו"68 עברו ממש טוב". לפי CNBC, הנתב התחיל לשדר יותר מדי נתונים בתוך שמונה דקות מההתקנה. הרשות כיבתה את פונקציית השידור בנתבי Juniper החדשים, וגם ביותר מ־60 נתבים נוספים, והקפיאה את ההתקנות.

כאן מתחילה המחלוקת. ה־FAA כותבת שהשדרוגים לא גרמו לתקלה, ומאשימה את רשת התקשורת הישנה שלה. ראש הרשות בריאן בדפורד אמר, לפי CRN, שהרשות מחליפה "כל הזמן 2,000 נתבים מדגם Cisco 600 בנתבי Juniper". מקור של TechTarget אומר שפונקציית השידור לא מופעלת כברירת מחדל, ושהפעלתה דורשת ידע בקוד. דאפי אמר ל־AP ש־L3Harris הייתה צריכה לאתר את הבעיה מהר יותר. ביום חמישי אמר בדפורד ל־Reuters שהממשל צפוי להודיע השבוע על שורש התקלה. עד כתיבת השורות האלה, ההודעה לא פורסמה.

ומתקפה? לפי ה־FAA, "אין שום אינדיקציה שזו הייתה מתקפת סייבר או גורם עוין מבחוץ". ה־FBI הצטרף לבדיקת הנתב במעבדה של L3Harris בפלורידה, לבקשת דאפי. סרטון ויראלי באורדו טען שאיראן הפילה את הבקרה האווירית. לפי בדיקת העובדות של האתר הפרסי Betacup, אין לכך ראיה.

"אנחנו לא תחת מתקפה מערכתית. לכל אחד מהאירועים האלה יש הסבר או סיבה שאין להם שום קשר לפושע סייבר, לגורם עוין או למדינה אחרת"

מזכיר המדינה מרקו רוביו, מנילה, 17.11 (בתרגום)

תחקיר השער

פרק 3 · בנק, חברת תעופה, אפל והסוכנות

שלוש הקריסות הבאות היו קצרות יותר. ביום שני, 16 בנובמבר, מ־18:30 בערך שעון ישראל, נתקעו עסקאות אצל לקוחות JPMorgan Chase, הבנק הגדול בארה"ב, לפי CNBC. הבנק כתב ב־X שמדובר ב"באג תוכנה במערכות חומרה מקומיות", ושאין "ראיה שזה קשור לסייבר". הנשיא טראמפ אמר במנילה, לפי NPR: "זה החיים. כשאתה גדול וחזק ויש לך את כל הכסף, דברים כאלה קורים".

באותו ערב, מ־23:02, עיכבה יונייטד איירליינס את ההמראות, כי הצוותים לא קיבלו נתוני משקל ואיזון סופיים. לפי AeroTime, 645 טיסות התעכבו ו־25 בוטלו. החברה לא פירטה מה נכשל, ואמרה ל־CNBC שאין סימן לבעיית סייבר. למחרת, מ־18:45 בערך, נפלו שירותי אפל: ההתחברות ל־iCloud, חנות האפליקציות, Apple Pay ואפילו הקופות בחנויות. אפל אמרה ל־TechCrunch ש"עדכון פנימי" גרם לתקלות, ושלא הייתה מתקפה. ניתוח מפורט היא לא פרסמה.

באותו יום התקשתה NSANet, הרשת המסווגת של NSA. הסוכנות מסרה, לפי CBS, שמדובר ב"פגיעה זמנית במהלך תחזוקה שגרתית מתוכננת". לפי The Record, הקמפוס נסגר לרוב העובדים ביום שלישי בערב, והעובדים התבקשו להגיע בהדרגה, כדי שלא כולם יתחברו בבת אחת.

רק כאן מופיע קשר ישיר לעולם האבטחה. מנהל המודיעין הלאומי ג'יי קלייטון אמר ל־Fox Business, לפי CBS, שהעדכונים שבאו אחרי חולשה ב־PHP, שפת התכנות שמריצה חלק גדול מאתרי האינטרנט, גרמו למערכות "לא לחזור כמצופה".

"זה מה שקרה ב־NSA היום", אמר. NSA עצמה מדברת רק על תחזוקה שגרתית. קלייטון דיבר על חולשה מלפני "כעשרה ימים", אבל PHP2Shell פורסמה ב־21 באוקטובר, כארבעה שבועות קודם.

תחקיר השער

פרק 4 · החוט המקשר: שינוי בלחץ

מה משותף לקריסות? לא תוקף, וגם לא סיבה אחת. מה שחוזר הוא שינוי. ברוב המקרים שבהם נמסרה סיבה, היא נוגעת לעדכון, להחלפת ציוד או למעבר בין מערכות: תיקון של מיקרוסופט מיולי, נתב חדש ברשת של ה־FAA, אתר גיבוי ב־Workday, "עדכון פנימי" באפל ועדכוני אבטחה ב־NSA. כמה מהשינויים פגשו מערכות ישנות או צפופות, שבהן תקלה מקומית מתפשטת לכל הרשת. אצל Chase ויונייטד לא פורסם מספיק כדי לשייך אותן לדפוס.

למה עכשיו? כאן נכנס הלחץ. ב־21 באוקטובר פרסמה CISA התרעה על שתי חולשות חמורות ב־PHP, שזכו לכינוי PHP2Shell. היא הורתה לתקן מיד, ואם אי אפשר, "להוציא מהרשת מערכות מבוססות PHP". לפי Nextgov, את החולשות מצאו בעזרת AI: חברת Calif בעזרת מודל של OpenAI, ו־Wiz בנפרד. ובישראל כבר ראינו מה קורה למי שלא עדכן. לפי צ'קפוינט, מ־30 באוקטובר פרצו תוקפים דרך PHP2Shell לשערי אבטחה שלה שלא עודכנו, ובחלק מהארגונים מחקו קבצים. לפרשה הזאת נחזור בשבוע הבא.

את הקשר הזה לא המציאו עיתונאים. קלייטון אמר, לפי הבית הלבן, ש"מוסדות רבים מתקנים" את החולשות, ו"הן לא חוזרות כמצופה בכל המקרים". הסנאטור מארק וורנר כתב ב־X ש־AI "מאפשר לזהות חולשות במספרים עצומים של מערכות במהירות חסרת תקדים", ויוצר לחץ לתקן "לעיתים קרובות הכול בבת אחת". דייוויד אגרנוביץ', לשעבר מנהל מודיעין במועצה לביטחון לאומי, כתב: "לקצב התיקון הידני יש מחיר, והמחיר הזה הוא אמינות".

אבל אסור למתוח את הקשר יותר מדי. רק התקלה ב־NSA נקשרה רשמית לעדכוני PHP, וגם זה בפי מנהל המודיעין ומקורות אנונימיים, לא בפי הסוכנות. הבאג של מיקרוסופט נולד ביולי, הרבה לפני PHP2Shell, והחברה שוללת מעורבות של AI. אצל ה־FAA מדובר בהחלפת ציוד שנמשכת שנים. בכיר אמריקאי אמר בתדרוך, לפי CNBC, שעל שאלת ה־AI "מאתגר לענות... בכל האירועים האלה". כלומר, יש דפוס משותף, אבל לא סיבה משותפת.

> **"יש סיבה טובה להאמין שהשיבושים האלה הם תוצאות לא מכוונות של מאמצים להפוך את המערכות שלנו לבטוחות יותר, ולא ראיה למתקפה רחבה יותר"**
>
> הסנאטור מארק וורנר ב־X, 18.11 (בתרגום)

תחקיר השער

פרק 5 · בינתיים, המתקפות האמיתיות

בזמן שאמריקה חיפשה האקרים בתקלות, האקרים אמיתיים עבדו במקומות אחרים. ביום חמישי, 19 בנובמבר, ב־15:17 שעון ישראל, פרסם JPMorgan Chase שספקים חיצוניים שנותנים לו שירות היו "יעד למתקפת סייבר". לדבריו, התוקפים ניגשו כנראה ל"נתוני שיווק מסוימים", ובהם שמות וכתובות מייל של לקוחות. לפי The Verge, הבנק הוסיף שאין "שום קשר" לתקלה של יום שני.

קבוצת הסחיטה N0n טענה ב־16 בנובמבר שיש בידיה רשומות של מחזיקי כרטיסים. לפי Reuters, בנתונים שפרסמה נמצאו יותר מ־16,000 כתובות מייל של לקוחות ו־124 של עובדי הבנק, אבל הסוכנות לא אימתה אותם. גם ויזה ומאסטרקארד אישרו אירועים אצל ספקים. לפי אותו דיווח, משרד האוצר והמפקח על הבנקים התקשרו לבנקים דקות אחרי התקלה של יום שני, כדי לוודא שאין מדובר באירוע סייבר. מתקפה אמיתית, אם כן, אבל לא זו שהפילה את הבנק.

ובאירופה: מקפיאים בסופרמרקטים. צרפת ייחסה למשמרות המהפכה האיראניים את המתקפה על בקרי הקירור בכ־700 אתרים באוקטובר, וגל שני פגע בתחילת נובמבר ברשתות בכמה מדינות. שר הפנים של איטליה, מתאו פיאנטדוסי, אמר ל־Reuters ב־19 בנובמבר שמתקפת הסייבר הגדולה היחידה שאושרה עד כה כוונה למערכות הקירור. באיטליה עצמה קיבלו כמעט 7,500 בתי ספר איומי פצצה במייל. בישראל, לפי חברת Gambit Security, סוכן AI ניהל סחיטה של חברה. שני הסיפורים מופיעים בהרחבה בהמשך הגיליון.

תחקיר השער

פרק 6 · המלחמה על האמון

הנזק הגדול של השבוע אולי לא היה טכני. פוסט של הפעילה הרפובליקנית ולנטינה גומז, "אין דבר כזה צירוף מקרים", נצפה יותר ממיליון פעם. לורה לומר כתבה ש"זו בבירור מתקפת סייבר מתואמת", ולפי NPR לא הציגה ראיות. לפי Deseret News, סרטון מזויף בטיקטוק הציג את טראמפ מכריז על הפסקת חשמל של 90 יום. וכשמערכת ההתרעה הלאומית נבדקה כמתוכנן, הופצה שמועה שהיא נפרצה. "הטענות האלה שקריות", כתבה FEMA, הסוכנות לניהול חירום.

הפחד לא נולד בחלל ריק. לפי Foreign Policy, כל האירועים האלה הגיעו מיד אחרי סדרה של "חשד למתקפות סייבר על מקפיאים בסופרמרקטים באירופה", ובתקופה שבה החרדה מ־AI הגיעה לשיא. גם הממשל לא התייחס לעניין כשגרה: סגן הנשיא ג'יי־די ואנס ביטל הופעה בכנס של ה־New York Times כדי להשתתף בדיונים על התקלות, לפי CNBC.

גם בוושינגטון לא כולם קונים את ההסבר. מנהיג המיעוט בסנאט, צ'אק שומר, אמר, לפי The Record, שזה "מקרי מדי שכל ההשבתות האלה קרו בתוך כמה ימים". הוא דרש "צוות אדום ייעודי" שיערער על ההנחה הרשמית. מנגד, בדיון בוועדה לביטחון המולדת ב־18 בנובמבר אמר קלייטון שהוא מבין ש"העיתוי של האירועים האלה יכול לעורר שאלות, וכך צריך להיות". סגן מנהל ה־FBI כריסטופר ראיה אמר, לפי CBS, שאין "שום אינדיקציה" לפעילות סייבר זדונית באף אחד מהאירועים.

ויש זווית ישראלית. שר ביטחון המולדת מרקוויין מולין כתב בעדות לקונגרס, לפי Zaobao, שיחידות סייבר של המדינה האיראנית והאקרים פרו־איראנים תוקפים בארה"ב תחבורה, פיננסים, אנרגיה, בריאות ומים. זה נמשך מאז פרוץ המלחמה עם איראן ב־28 בפברואר, עם נזק מוגבל עד כה. כלומר, האיום קיים. הוא פשוט לא מה שהפיל את המערכות השבוע.

תחקיר השער

פרק 7 · אז זה היה יום הדין?

איך מבדילים בין תקלה למתקפה? השבוע עזרו כמה סימנים. האם המפעיל מפרסם מנגנון וציר זמן, כמו מיקרוסופט וה־FAA, או רק "תקלה"? האם יש סימני מתקפה כמו דרישת כופר, דליפה או הצפנה? האם הכשל מתפשט לאורך תלויות, מ־Teams לשער הדואר, או מופיע בבת אחת אצל יעדים שאין ביניהם קשר? וטענת אחריות בטלגרם היא רמז, לא הוכחה.

ומה לומדים? לקוראים: לא ללחוץ על קישורים של "שחזור הדואר" או "תקלה בבנק", ולבדוק סטטוס רק באפליקציה או באתר הרשמי. לארגונים: להתייחס לכל שינוי כאל אירוע סיכון, להפיץ בהדרגה ולוודא שאפשר לחזור לאחור. לבדוק על חומרה שדומה לזו שבייצור. לבודד את אתר הגיבוי, כי גם הוא יכול להפיל. למפות את הספקים של הספקים. ולתקן מהר, אבל בשלבים.

אז האם זה היה יום הדין של הסייבר? לפי כל מה שידוע היום, לא. לא נמצא תוקף מאחורי אף אחת מהקריסות. אבל זה היה מבחן עמידות, וחלק מהמערכות לא עברו אותו. הן נפלו מהשינויים של עצמן, ובינתיים תוקפים ניצלו את הרעש לפישינג ולשמועות, והמשיכו לעבוד במקומות אחרים. מנהל CISA בפועל, ניק אנדרסן, דיבר השבוע, לפי CyberScoop, על חוסן מול "תיקון גרוע או עדכון מודרניזציה שהשתבש". הדוח הסופי של מיקרוסופט וממצאי ה־FAA יראו אם התמונה הזאת מחזיקה.

מה ידוע ומה לא

מה ידוע

- כל החברות שנפגעו שוללות מתקפת סייבר.
- המודיעין, ה־FBI ו־CISA לא רואים מתקפה או קשר.
- מיקרוסופט פרסמה מנגנון מפורט: באג מיולי ועומס.
- ב־FAA, נתב חדש הציף רשת ישנה.
- מנהל המודיעין קשר את התקלה ב־NSA לעדכוני PHP.
- ספקים של Chase נפרצו, בלי קשר לתקלה.

מה לא ידוע

- שורש התקלה ב־FAA: הגדרה שגויה או ציוד פגום.
- למה המחיצות של מיקרוסופט לא עצרו את הכשל.
- מה נכשל באפל, ביונייטד וב־Chase.
- אם התקלה ב־NSA קשורה דווקא ל־PHP2Shell.
- אם ל־AI היה תפקיד ישיר באחת התקלות.

מילון התחקיר

PHP
שפת תכנות שמריצה חלק גדול מאתרי האינטרנט וממשקי הניהול של מכשירים.

פישינג
הודעה מתחזה שנועדה לגרום לנמען למסור סיסמה או ללחוץ על קישור.

נתב
רכיב רשת שמעביר מידע בין רשתות. ב־FAA הוא חיבר קווי נחושת ישנים לסיבים אופטיים.

אתר גיבוי
מערכת משנה שאמורה להחליף את המערכת הראשית בזמן אסון.

מחיצה
הפרדה בין אזורים בענן, כדי שכשל באזור אחד לא יתפשט לאחרים.

דוח לאחר אירוע
מסמך שבו החברה מסבירה מה קרה, למה, ומה תשנה. מיקרוסופט פרסמה דוח מקדים, והסופי צפוי בקרוב.

צוות אדום
צוות שתפקידו לחשוב כמו תוקף ולערער על ההנחות הרשמיות.

מקור: הדוח המקדים של מיקרוסופט · BBC · Guardian · TheVerifier · נאדלה · CNBC · Ars Technica · מיקרוסופט · ב־X · למאנה ב־X · DarknetSearch · מודיעין מיקרוסופט ב־X · DRJ · Niguro · FAA · ABC · FAA · CNBC · Reuters · · AeroTime · NPR · CNBC · Chase · Chase ב־X 16.11 · Betacup · TechTarget · CRN · AP · FAA 19.11 · יונייטד · TechCrunch · NSA · CBS · The Record · קלייטון · CBS · CISA · Nextgov · צ'קפוינט · הבית הלבן · וורנר ב־X · אגרנוביץ' ב־X · תדרוך · CNBC · Chase ב־X 19.11 · The Verge · Chase · Reuters · איטליה · Reuters · גומז ב־X · לומר ב־X · Deseret News · FEMA ב־X · הדיון · CBS · Zaobao · CyberScoop · משרד החוץ האמריקאי · ישראל היום · Foreign Policy

חמישי, 19 בנובמבר · מה הגיע אחרי מהדורת הבוקר

עדכון **מאשר: ספקים JPMorgan Chase שלו נפרצו:** הבנק אישר שתוקפים ניגשו לנתוני שיווק אצל ספקים, כנראה שמות ומיילים של לקוחות, ויציע ניטור אשראי. לפי Reuters, בנתונים ש־N0n פרסמה יש יותר מ־16,000 מיילים של לקוחות. גם מאסטרקארד אישרה. הבנק: אין קשר לתקלה של יום שני. Reuters

הנציבות האירופית: הותקפנו בעזרת כלי AI: הנציבות אישרה מתקפה שזוהתה ב־22 באוקטובר ושיבשה לפי הדיווחים את מערכות כוח האדם שלה יותר מעשרה ימים. לפי Politico, CERT-EU זיהה שימוש ב־ARTEX, כלי ה־AI שה־FBI הזהיר ממנו. אין עדות לדליפה רחבה. The Record

מערך הסייבר: אפליקציה מתחזה לרשות המסים: הודעות מפנות לאתר שמתחזה לחנות Google Play ומציע אפליקציה בשם "רשות המסים" לאנדרואיד. היא עלולה לתת לתוקפים גישה להודעות, לקודי אימות ולמצלמה. מי שהתקין: לנתק את המכשיר מהרשת ולהחליף סיסמאות ממכשיר אחר. ynet

לונדון: פרטי 265 אלף מחזיקי כרטיס Oyster נחשפו: רשות התחבורה של לונדון גילתה ב־16 בנובמבר פריצה למערכת כרטיסי Oyster עם תמונה. נחשפו שמות, כתובות, תאריכי לידה ושאלות אבטחה, אבל לא סיסמאות ופרטי תשלום. כדאי להחליף שאלות אבטחה זהות באתרים אחרים. BleepingComputer

תוקפים ניצלו חולשה ב־Cisco Expressway: לפי F6, תוקפים פרצו לשרתי Expressway בארגון רוסי זמן קצר אחרי שפורסם קוד ניצול ל־CVE-2026-76466, ונעזרו בעוזר AI לכתיבת הכלים. החולשה מאפשרת הרצת פקודות כ־root, כלומר בהרשאות מלאות, רק במכשירים מקובצים. התיקון: גרסה X15.5.20. SecurityWeek

תחקיר · ישראל · AI בידי תוקפים

סוכן AI תמחר את הכופר: כך נסחטה חברה ישראלית

תוקף דובר רוסית פרץ דרך VPN, ונתן לכלי AI לקבוע כמה כופר לדרוש

גאזט סייבר · כמעט כל הפרטים מגיעים ממקור אחד, Gambit Security, ומסומנים כך

יש לא ישב מול המסך וקרא את הדוחות הכספיים של החברה. את זה עשה סוכן AI. לפי תחקיר שפרסמה חברת הסייבר הישראלית Gambit Security ב־18 בנובמבר, תוקף דובר רוסית פרץ לחברה ישראלית, העביר לכלי AI את המסמכים שגנב וקיבל ממנו הערכה כמה החברה יכולה לשלם. כשהחברה התמקחה, ה־AI כתב לו את התשובה.

את הפרשה חשפה חדשות 12 ב־16 בנובמבר. דרך הכניסה ושם הכלי הופיעו רק בבלוג של Gambit, ולא בדיווחים בעברית שמצאנו.

תחקיר · סחיטה בידי AI

איך זה עבד

לפי Gambit, הכניסה הייתה דרך חיבור VPN פרוץ לחומת אש מדגם FortiGate. VPN הוא "המנהרה" שדרכה עובדים מתחברים מרחוק לרשת הארגון. איך השיג התוקף את הגישה, Gambit לא מפרטת. משם הפעיל את PentestCode, כלי AI אוטונומי לבדיקות חדירה. "בתוך שעות ספורות" מיפה הכלי את המערכות הפנימיות, השתמש שוב בסיסמאות שמצא, השיג הרשאות של מנהל הרשת, ואיתר את שרתי האחסון, הווירטואליזציה והגיבוי.

PentestCode עצמו איננו נוזקה. לפי דף הפרויקט ב־GitHub, זהו כלי קוד פתוח, פיצול של OpenCode, שמיועד לבודקי חדירה מורשים. הוא לא היחיד שמנוצל כך. לפי CyberVeille, שסיכם מחקר של huntback מ־31 באוקטובר, מפעיל אחר הריץ את אותו כלי נגד 25 ארגונים, בעיקר באירופה, בין ספטמבר לאוקטובר. אין ראיה

שמדובר באותו תוקף. וזה אותו דפוס שה־FBI הזהיר ממנו בכלי ARTEX, לפי The Record.

התוקף העתיק כ־2 טרה־בייט: מסמכים כספיים, רשומות תאגידיות, מיילים של מנהלים וגיבויים של מכשירים, "כמעט 400,000 קבצים" לפי Gambit. בדיווחים בעברית, למשל ב־ערוץ 7, דובר על כחצי מיליון. ואז הגיע השלב החדש. התוקף הזין ל־AI דפי בנק, אישורי יתרה ורישומים חשבונאיים, וקיבל "הערכה פיננסית": הכנסות שנתיות של כ־57 מיליון דולר, רווח נקי שנתי של כ־2.8 מיליון ו־392,723 דולר במזומן. המסקנה: 500 אלף דולר הם בתוך היכולת של החברה.

תחקיר · סחיטה בידי AI

המשא ומתן

הדרישה, 500 אלף דולר תמורת אי־פרסום, נשלחה עם הוכחות לפריצה. החברה השיבה ש־500 אלף דולר הם כ־18% מהרווח השנתי, שעלות המתקפה לתוקף נאמדת ב־60 עד 80 אלף דולר, וששהנהלה לא תאשר תשלום כזה. התוקף העביר את התשובה ל־AI. ההצעה שחזרה: להציג את אותו סכום כ־0.88% בלבד מההכנסות השנתיות, "ביטוח מפני אסון, לא קנס".

> **"הם לא מסרבים לשלם, הם מתמקחים. אנחנו צריכים להוכיח ש־500,000 דולר מוצדקים"**
>
> סוכן ה־AI של התוקף, כפי שציטטה Gambit Security (בתרגום)

ה־AI גם מיין את השלל לארבע רמות של מנוף לחץ: נתוני בנק ואישורים פיננסיים ("איום מוות"), רשומות מסחריות חסויות ("גיהנום פיננסי"), מידע אישי של מנהלים ("פגיעות אישית") ושאר המסמכים. Gambit מודה שחלק מהעצות היו מובנות מאליהן, אבל לדבריה ה־AI חסך לתוקף זמן ומומחיות.

מי התוקף? Gambit מתארת אותו כ"דובר רוסית", ובכותרות בעברית הוא הפך ל"האקרים רוסים", צעד אחד מעבר למקור. Gambit לא פרסמה שם קבוצה או סימני זיהוי, ולא פירטה על מה מבוססת הקביעה. גם זהות הקורבן, הענף שלו, והאם שילם, לא פורסמו. Gambit מסרה שדיווחה ל"רשויות הרלוונטיות" לפני הפרסום, ומזהירה שחלק מהנתונים שונו מעט כדי להסתיר את זהות הקורבן.

גם התאריך שעל ההערכה הפיננסית, 28 ביולי 2026, אולי שונה. וכמעט כל מה שידוע מגיע ממקור אחד, חברה שמוכרת פתרונות התאוששות, ואיש לא אימת אותו באופן עצמאי.

תחקיר · סחיטה בידי AI

הלקחים

גיבויים לא עוזרים כאן, כי מדובר בגניבה ולא בהצפנה. גם Gambit כותבת שיכולת שחזור "לא מבטלת" חשיפה של מידע רגיש. לכן הלקח המעשי מתחיל בכניסה: אימות דו־שלבי לכל חיבור VPN, מעקב אחרי חשבונות מנהל חדשים וגישה לשרתי הגיבוי, וצמצום המסמכים הרגישים שיושבים פתוחים ברשת.

מה ידוע ומה לא

מה ידוע

- כניסה דרך חיבור VPN פרוץ ל־FortiGate (Gambit).
- כ־2 טרה־בייט, כמעט 400 אלף קבצים, נגנבו.
- ה־AI תמחר את הדרישה, 500 אלף דולר, והציע טיעוני מיקוח.

מה לא ידוע

- מי הקורבן ובאיזה ענף.
- אם שולם כופר ואם המידע דלף.
- איזה מודל AI הפעיל התוקף, ועל מה מבוססת הקביעה "דובר רוסית".

ציר הזמן

28.7.2026 התאריך שעל "ההערכה הפיננסית" שהכין ה־AI (ייתכן ששונה).

30.10–8.9 מפעיל אחר מריץ את PentestCode נגד 25 ארגונים באירופה (huntback, דרך CyberVeille).

18.11 Gambit מפרסמת את התחקיר הטכני: FortiGate, PentestCode והמשא ומתן.

מקורות: Gambit Security, חדשות 12, ערוץ 7, CyberVeille.

מקור: Gambit Security · חדשות 12 · Gambit · mako · ערוץ 7 · GitHub־ב PentestCode · CyberVeille · The Record

תחקיר שלישי · מתקפת המקפיאים

גאזט סייבר · 20 בנובמבר 2026

תחקיר · איראן · תשתיות

מתקפת המקפיאים: מי באמת עומד מאחורי "חזית האיסנאד"

צרפת ייחסה למשמרות המהפכה את השבתת הקירור בכ־700 סופרמרקטים. מפעל מזון בישראל ספג גרסה הרסנית יותר כבר במאי. כולם מסכימים שזו איראן, אבל לא על היחידה

גאזט סייבר · Profero, CERT-FR ו־FDD מובאים כמקורות, וכל טענה מיוחסת למי שאמר אותה

בלילה שבין 11 ל־12 באוקטובר שינה מישהו הגדרה אחת בבקרי הקירור של כ־700 סופרמרקטים בצרפת: מחזור הפשרת הקרח כוון לטמפרטורות גבוהות. הסחורה התקלקלה, ובלפחות 15 מקרים פרצה שריפה. לפי משרד החוץ הצרפתי, הנזק מגיע לעשרות מיליוני אירו. ב־9 בנובמבר ייחסה צרפת את המתקפה למשמרות המהפכה של איראן. אבל חמישה חודשים קודם לכן קרה משהו דומה, והרסני יותר, במפעל מזון בישראל.

תחקיר · המקפיאים

צרפת: הראיות

לפי הדוח של CERT-FR, מטעם מרכז תיאום משברי הסייבר הצרפתי, המבצעת הייתה "שהיד קאווה", יחידת סייבר התקפית במרכז הסייבר והלוחמה האלקטרונית של משמרות המהפכה. הדוח מונה "צבר ראיות": התשתית ששימשה לתקיפה שימשה באותה תקופה גם לסיור על ציוד Schneider Electric, בטכניקה שהיחידה מפעילה מאז אפריל 2026 לפחות. התוקפים השתמשו בכלי הסריקה FOFA, הכלי

הקבוע שלהם. ערוץ התעמולה CyberbanNews, שמזוהה עם היחידה, הפיץ את המתקפה כבר ב־13 באוקטובר. ובתשתית נמצאו עקבות של פרסית.

הדוח נוקב בשמות המפקדים, רזא סלרוונד ומהדי לשגריאן, ומונה את "האווטרים" של היחידה, כלומר הזהויות הבדויות שדרכן היא לוקחת אחריות, ובהם CyberAv3ngers ו"חזית האיסנאד" (Cyber Isnaad Front). לפי הדוח, היחידה גם לקחה אחריות למתקפה על ציוד קירור ישראלי במרץ ובאפריל 2026. צרפת פועלת לסנקציות של האיחוד האירופי עד אמצע דצמבר, לפי Politico. איראן דוחה את הייחוס, ודובר משרד החוץ שלה האשים את "מכונת הדיסאינפורמציה של ישראל", לפי Türkiye Today.

תחקיר · המקפיאים

ישראל: הגרסה המוקדמת

במאי 2026, לפי דוח של Profero, חברת תגובה לאירועי סייבר ישראלית שטיפלה באירוע, הוזעקו טכנאי קירור למפעל מזון שהמקררים שלו התחממו. הם גילו שמישהו תכנת מחדש את הבקרים: שינה את נקודות הכיוון ואת גבולות הבטיחות, העביר את השסתומים הממונעים למצב ידני והשאיר אותם פתוחים, והחליף את הסיסמה כדי לנעול את המהנדסים בחוץ. במערכת, שפועלת על פחמן דו־חמצני, הגיע נוזל למדחסים. שלושה מדחסים הושמדו, והמערכת חזרה לפעולה רגילה רק אחרי כמעט שבוע. לפי Profero, על הבקרים עצמם לא רצה שום נוזקה.

ברשת המחשבים של המפעל מצאה Profero נוזקה שהיא מכנה GRAT, שהתחזתה לעדכון של מיקרוסופט. יש בה מודול הצפנה לכופר בשם BigBang ופקודה שמוחקת את הדיסק ואת טבלת המחיצות, כלומר וייפר. לפי Profero, השילוב של חבלה בציוד פיזי ומחיקה ברשת באותו מבצע הוא העיקר. NPR סיקרה את הפרשה ב־3 בנובמבר, וציטטה את ראש Profero, עמרי שגב מויאל, שאמר שהוא בטוח שמאחורי המתקפה עומדים האקרים צבאיים איראניים.

תחקיר · המקפיאים

המחלוקת: איזו יחידה?

כאן מתחילה המחלוקת. Profero, בדוח מ־24 במאי, מעריכה "ברמת ביטחון גבוהה" ש"חזית האיסנאד" היא זהות בדויה שמופעלת בידי, או לצד, ASA (Aria Sepehr Ayandehsazan). לפי Profero, זו היורשת של Emennet Pasargad, שמשרד האוצר האמריקאי הטיל עליה סנקציות בגלל מבצעי השפעה בבחירות 2020. הבסיס, לדבריה: חפיפה בתשתיות, דפוסי פרסונה ובחירת קורבנות. CERT-FR, בדוח מ־9 בנובמבר, מונה את "חזית האיסנאד" דווקא בין האווטרים של שהיד קאווה. ואת Emennet Pasargad הוא משייך ליחידה אחרת, "שהיד שוסתרי".

קול שלישי מגיע מ־FDD, מכון מחקר בוושינגטון. ב־13 בנובמבר כתב שם ארי בן עם שצרפת אמנם טוענת ששהיד קאווה מפעילה את "חזית האיסנאד", אבל הניתוח של המכון קושר אותה יותר לשהיד שוסתרי. מנגד, לדבריו, הכלים במתקפה בצרפת דומים מאוד לאלה של CyberAv3ngers, ששהיד קאווה מפעילה. ההסבר שלו: היחידות חולקות אנשים וכלים. בן עם אינו מקור עצמאי לגמרי: לפי NPR, הוא ערך ניתוח מוקדם של הנתונים ש־Profero העבירה.

צרפת מול Profero: מה כל צד טוען

- CERT-FR, 9.11: אווטר של שהיד קאווה. הראיות נוגעות רק למתקפה בצרפת.
- Profero, 24.5: מופעלת בידי ASA או לצדה, ברמת ביטחון "גבוהה".
- FDD, 13.11: קרובה יותר לשהיד שוסתרי. היחידות חולקות אנשים וכלים.
- מוסכם: משמרות המהפכה. CERT-FR ו־Profero לא פירטו בפומבי ראיות לשיוך של "חזית האיסנאד".

תחקיר · המקפיאים

הגל השני

בלילה שבין 1 ל־2 בנובמבר נפגעו מקפיאים ברשתות בלפחות שבע מדינות באירופה, לפי ה־Guardian. בסניף של ICA בשוודיה כוונו המקררים ל־50 מעלות. אף מדינה לא ייחסה את הגל הזה, והמרכז הבלגי לסייבר אמר, לפי The Record, שייתכן ש"לעולם לא יהיה אפשר לזהות" את התוקפים. לכן אין לכתוב שגם הוא איראני. באותו יום הורה מערך הסייבר הלאומי לרשתות קמעונאות ומזון בישראל לבדוק את הבקרים בדחיפות, לפי כאן.

תחקיר · המקפיאים

למה למקפיא יש כתובת IP?

מקפיא בסופרמרקט מנוהל היום בידי בקר, מחשב קטן שמחובר לרשת כדי שקבלן הקירור יוכל לעקוב אחרי הטמפרטורות מרחוק. רבים נשארו חשופים לאינטרנט. לפי The Hacker News, Danfoss אמרה שרוב היחידות שנפגעו בצרפת היו דגמים ישנים שכבר לא מקבלים עדכונים, AK-SM 800 ו־AK-SC 355. "הפשרה" מחממת את סלילי הקירור כדי להמיס קרח. מחזור הפשרה שלא נגמר, עם התרעות מושתקות, הופך מקפיא לתנור איטי.

לפי Censys, מספר המכשירים החשופים של Danfoss ושל Copeland באירופה ירד ב־53%, מ־6,695 ל־3,124, בין 9 באוקטובר ל־5 בנובמבר. כלומר, אלפים עדיין חשופים. באמצע נובמבר פורסמו שש חולשות חדשות בדגם AK-SM800A, ולפי The Hacker News אין להן עדיין תיקון. הלקחים: להוציא ממשקי ניהול מהאינטרנט, לגשת רק דרך VPN, להחליף סיסמאות ברירת מחדל וציוד שהתמיכה בו נגמרה. לפי CERT-FR, כפי שציטט The Hacker News, איפוס להגדרות היצרן לבדו לא מספיק.

ציר הזמן

24.5.2026 Profero מפרסמת את דוח מפעל המזון בישראל.

12.10–11 המתקפה בצרפת: כ־700 אתרים, לפחות 15 שריפות.

2.11 הגל השני באירופה. מערך הסייבר מתריע בישראל.

9.11 צרפת מייחסת את המתקפה למשמרות המהפכה.

16.11 ערוץ בשם CyberAv3ngers טוען לדגל כוזב (Threat Beat).

מקורות: CERT-FR, Profero, FDD, Guardian, Censys, כאן, Threat Beat.

מה ידוע ומה לא

מה ידוע

- צרפת ייחסה רשמית את המתקפה של אוקטובר לשהיד קאווה, ופירטה חמש ראיות.
- במפעל בישראל הושמדו שלושה מדחסים, וברשת נמצא וייפר (Profero).

מה לא ידוע

- איזו יחידה מפעילה את "חזית האיסנאד".
- מי ביצע את הגל השני באירופה.
- אם ששת הפגמים החדשים ב־Danfoss כבר מנוצלים.

מקור: CERT-FR · משרד החוץ הצרפתי · Profero · NPR · FDD · CyberVeille · Guardian · The Hacker News · Danfoss · Censys · Türkiye Today · Politico · כאן · The Record · Threat Beat

גאזט סייבר · עיתון הסייבר היומי העברי הראשון · גיליון 7 · מגזין סוף השבוע · יום שישי, 20 בנובמבר 2026 · י׳ בכסלו תשפ״ז
כל עובדה מקושרת למקור. ציטוטים מאנגלית מובאים בתרגום, עם קישור למקור. ייחוס תקיפות מובא בזהירות, כפי שהמקורות עצמם מנסחים אותו. אין מדור סקופ השבוע: לא נמצא חומר חדש ומאומת שלא פורסם בעברית.

הבהרה

גאזט סייבר הוא שירות מידע חינמי לציבור הרחב. התוכן נכתב ונערך באמצעות כלי בינה מלאכותית, ועלולים להיות בו טעויות, השמטות, אי־דיוקים או מידע שאינו עדכני.

התוכן מובא למטרות מידע כללי בלבד. הוא אינו ייעוץ מקצועי, אבטחתי, משפטי או אחר, ואינו תחליף לייעוץ כזה. אין להסתמך עליו לבדו. לפני כל פעולה, ובכלל זה התקנת עדכון, חסימה, השבתה או שינוי של מערכות, יש לאמת את המידע מול המקור הרשמי (היצרן, הרשות המוסמכת או המקור המצוטט) ולהיוועץ בגורם מקצועי.

דיווחים על אירועי סייבר, פריצות ודליפות מבוססים על המקורות המצוינים לצדם, ומשקפים את מה שפורסם בהם במועד הכתיבה. טענה של גורם תוקף, או דיווח שלא אושר, מוצגים כטענה בלבד, ואין בהם קביעה שהארגון הנזכר נפרץ או פעל שלא כדין.

ככל שהדין מתיר, העורכים והמפרסמים לא יישאו באחריות לנזק, ישיר או עקיף, שייגרם משימוש בתוכן או מהסתמכות עליו. קישורים למקורות חיצוניים מובאים לנוחות בלבד, ואין לנו שליטה על תוכנם.

מצאתם טעות? אתם או הארגון שלכם מוזכרים ומבקשים תיקון או תגובה? כתבו לנו: editor@gazet.co.il או ב־X @Gazet_IL. נבדוק ונתקן בהקדם.