עיתון הסייבר היומי העברי הראשון · חולשות, פריצות ותוקפים · שעון ישראל

גאזט סייבר

חמישי, ט׳ בכסלו תשפ״ז · 19 בנובמבר 2026 · גיליון 6 · מהדורת יום חמישי

סחיטה · כרטיסי אשראי

ויזה מאשרת פריצה אצל ספק, וכנופיה טוענת: גם JPMorgan

קבוצת הסחיטה N0n פרסמה את ויזה, מאסטרקארד ו־JPMorgan Chase ברשימת קורבנות. ויזה מאשרת פריצה לספק באסיה, ואומרת שמספרי כרטיסים לא נפגעו.

חברת כרטיסי האשראי ויזה אישרה השבוע שאחד מספקי השירות שלה באזור אסיה והאוקיינוס השקט נפרץ. האישור הגיע אחרי שכנופיית סחיטה חדשה פרסמה את ויזה ברשימת הקורבנות שלה, לצד מאסטרקארד, הבנק האמריקאי ג׳יי־פי מורגן ועשרות חברות מוכרות. לפי ויזה, המערכות שלה לא נפגעו, ואין סימן לכך שמספרי כרטיסים דלפו. הסכנה המיידית ללקוחות היא הונאות מותאמות אישית.

מה קרה? לפי BreachNews, ב־16 בנובמבר פרסמה הקבוצה, שקוראת לעצמה N0n, את שמותיהם של 59 ארגונים מ־11 מדינות באתר ההדלפות שלה, כלומר אתר שבו כנופיות מאיימות לפרסם מידע גנוב אם לא ישלמו להן. לפי הדיווח, 46 מהרשומות עמדו שם כבר מ־9 בנובמבר כמספרים אנונימיים, עד שהקבוצה החליפה אותם בשמות. לפי Cybernews, הקבוצה נתנה לחברות 48 שעות למשא ומתן.

מה הקבוצה טוענת שיש לה? לפי BreachNews, ברשומה של ויזה מדובר בנתוני מועדוני כרטיסים באסיה: שמות מלאים, כתובות מייל אישיות, מספרי טלפון,

הזמנות נסיעה ומסעדות של בעלי כרטיסי פרימיום ויותר מ־1.5 מיליון רשומות של פעילות בקמפיינים. ברשומה של ג׳יי־פי מורגן מדובר לפי הקבוצה ברשומות קמפייני מייל של תוכנית כרטיס Reserve, עם עשרות אלפי כתובות מייל. אף רשומה לא מזכירה מספרי כרטיסים, סיסמאות או יתרות. הקבוצה לא פרסמה דוגמה מהמידע, ואיש לא אימת את הטענות.

ומה אומרות החברות? ״המערכות של ויזה לא היו מעורבות ולא נפגעו. אין סימן לכך שנתוני תשלום כמו מספרי כרטיסים נפגעו״, מסר דובר החברה ל־Cybernews (בתרגום). ויזה לא מסרה מי הספק ולא קשרה את האירוע ל־N0n. ג׳יי־פי מורגן סבלה ב־16 בנובמבר מתקלה שהאטה חלק מהעסקאות של לקוחות פרטיים. הבנק אמר ל־CNBC ול־Reuters שמדובר בבאג תוכנה במערכות חומרה פנימיות, ושאין ראיה שזו מתקפת סייבר. מאסטרקארד לא הגיבה.

מי עוד ברשימה? לפי BreachNews, הקבוצה פרסמה גם את Walmart, Procter & Gamble, Airbnb, Pandora ו־Patagonia, ולגבי רובן היא טוענת לנתוני שיווק ואנליטיקה שחברות חולקות עם ספקים חיצוניים. הטענה הגדולה ביותר נוגעת לחברת התרופות Eli Lilly: כ־16 מיליון רשומות של מרשמים שנופקו ל־1,243,661 מטופלים. אדם שמכיר את הפרטים אמר ל־s’Barron שהחברה לא מצאה גישה לא מורשית למערכות שלה, ושהמידע קשור לספק נתונים חיצוני. הדפוס חוזר: Expedia אישרה ב־12 בנובמבר פריצה דרך ספק, אחרי ש־N0n טענה שיש לה את המידע שלה.

מי עומד מאחורי זה? N0n הופיעה בספטמבר 2026. לפי BreachNews, חוקרים ממליצים לא לקבל את המספרים שלה כפשוטם: Bitdefender מצאה בשרת קבצים חשוף של הקבוצה ראיות לקצת יותר מ־20 קורבנות בלבד, הרבה פחות ממה שהאתר מציג. SOCRadar קשרה את הקבוצה ל־23 ארגונים לפחות ב־14 מדינות. לדברי החוקרים, כל פריצה מתועדת שלה נשענה על סיסמאות חלשות או גנובות ועל מפתחות גישה לענן שנחשפו, והקבוצה כתבה את כלי התקיפה שלה בעזרת כלי AI לתכנות.

מה לעשות? מאחר שהמידע שנטען כולל שמות, טלפונים, כתובות מייל והזמנות, הסיכון הסביר הוא פישינג ממוקד (הודעות מתחזות שנראות אמינות כי הן מזכירות פרטים אמיתיים). לפי BreachNews, בעלי כרטיסי פרימיום צריכים לחשוד במייל, בהודעת טקסט או בשיחה שמזכירים הזמנה אחרונה או הטבת כרטיס ומבקשים לאשר פרטים, ללחוץ על קישור או למסור קוד חד־פעמי. מי שרוצה להיזהר יכול לבדוק עסקאות אחרונות ולהפעיל התראות כרטיס דרך הבנק.

מקור: BreachNews · Cybernews · TechRadar · The Paypers

בגיליון · הקישו לקפיצה

פריצות ואירועים ←	AI ואבטחה ←	סייבר ב־X ←
תוקפים וקמפיינים ←	כלים ומחקר ←	חולשות מנוצלות ו־KEV ←

פריצות ואירועים

גאזט סייבר · 19 בנובמבר 2026

MUFG: פריצה לספק חשפה 6.5 מיליון רשומות של לקוחות הבנק

הקבוצה הבנקאית הגדולה ביפן מדווחת על כ־8 מיליון רשומות בחמש חברות בנות. לפי הבנק, שמות וכתובות לא דלפו.

הקבוצה הפיננסית MUFG הודיעה ביום רביעי על דליפת מידע של כ־8 מיליון רשומות בחמש חברות בקבוצה, בהן בנק MUFG. הסיבה: גישה לא מורשית לשירות של PLAID, ספק טוקיואי שמנתח את השימוש של לקוחות באתרי הבנק.

לפי Sankei, בבנק עצמו דלפו כ־6.5 מיליון רשומות עם מגדר, גיל ואזור מגורים. לפי הבנק, שמות, כתובות, טלפונים וכתובות מייל לא נכללו, ולא זוהה שימוש לרעה. PLAID דיווחה לבנק על הפריצה ב־13 בנובמבר, והיקף הדליפה התברר ב־17 בנובמבר.

הבנק הפסיק את העברת הנתונים ל־PLAID, ולדבריו אין השפעה על עסקאות. גם חברות ניירות הערך והנאמנות של הקבוצה ו־WealthNavi אישרו דליפה.

מקור: MUFG · Sankei · BigGo Finance

כופרה עצרה ייצור מוני חשמל חכמים ביפן

Osaki Electric גילתה שרתים מוצפנים, ניתקה את הרשת והשביתה את קווי הייצור. מועד החזרה לפעילות לא ידוע.

יצרנית מוני החשמל היפנית Osaki Electric הודיעה שנפגעה ממתקפת כופרה, כלומר נוזקה שמצפינה מידע ודורשת כופר. לפי הודעת החברה לבורסה, ב־17 בנובמבר בבוקר היא גילתה שמידע בשרתים שלה הוצפן, ובצהריים ניתקה את המערכות מרשתות חיצוניות.

כדי למנוע נזק נוסף, החברה השביתה את מערכות הייצור במרכז הפיתוח והייצור בסאיטמה ובאתרים קשורים, ועצרה ייצור ומשלוח של מוני חשמל חכמים ומוצרים נוספים. היא בודקת עם מומחים חיצוניים אם מידע דלף, ודיווחה למשטרה.

לפי Cyware, בשוק כבר חוששים לעיכובים בפרויקטים של תשתיות חשמל שתלויים באספקה של החברה. Osaki לא מסרה מתי הייצור יחזור, ומה תהיה ההשפעה הכספית.

מקור: Osaki Electric · Cyware

בקונגרס: איראן תוקפת תשתיות בארה"ב, אבל לא הפילה את המערכות

ראשי DHS, המודיעין וה־FBI אמרו שהשיבושים בתעופה, בבנקים וב־NSA נבעו מתחזוקה. הם הזהירו שהאיום האיראני גדל.

שר ביטחון המולדת Markwayne Mullin, ראש המודיעין הלאומי Jay Clayton וסגן ראש ה־FBI Christopher Raia העידו ביום רביעי בוועדה לביטחון המולדת בבית הנבחרים. לפי CBS News, הם אמרו שאין ראיה שהשיבושים האחרונים, בחברות תעופה, בבנקים, בשירותי מיקרוסופט ובמערכות של NSA, קשורים זה לזה או נגרמו ממתקפת סייבר.

"אלה תקלות שירות נפרדות שקשורות לתחזוקה ולשינויים טכניים. הן לא מתקפה מתואמת או מתקפה של מדינה", אמר Clayton (בתרגום). Mullin אמר שהוא בטוח "ב־98%" שהתקלות אינן פעולה של יריב זר. עצירת הטיסות הארצית של ה־FAA נגרמה, לפי הפקידים, מנתב שהציף נתבים אחרים בזמן החלפת קווים אצל הקבלן L3Harris.

באותו זמן, לפי עדותו הכתובה של Mullin, גורמים הקשורים לאיראן תוקפים מאז פברואר תשתיות בארה"ב: תחבורה, בריאות, מים, אנרגיה ופיננסים. לפי העדות, הפעולות האלה גרמו עד כה לנזק מקומי ומזערי, בעיקר לרכיבי בקרה תעשייתיים שאובטחו גרוע. Clayton אמר שהאיומים האיראניים בתוך ארה"ב ומחוצה לה "גדלו בצורה דרמטית".

מקור: CBS News · DHS (עדות) · AP

אוקראינה וה־FBI עצרו כנופיית כופרה שגבתה 40.5 מיליון דולר

הכנופיה התחזתה לתמיכה טכנית בשיחות עם קולות שיוצרו ב־AI. לפחות 28 חברות שילמו לה כופר.

משטרת אוקראינה והתביעה הכללית, יחד עם ה־FBI, עצרו ארבעה חשודים בכירים בארגון כופרה בינלאומי. לפי התביעה, לפחות 28 חברות שילמו לארגון יותר מ־40.5 מיליון דולר. החקירה נמשכה כשנתיים.

לפי התביעה, הארגון מנה לפחות 27 אנשים מאוקראינה, מקזחסטן, מרוסיה וממדינות נוספות, והיה קשור לרשת של יותר מ־60 איש בשמונה מדינות, בהם חברים לשעבר בכנופיית Conti. החברים התחזו לאנשי תמיכה טכנית, השיגו סיסמאות ושכנעו עובדים להתקין תוכנות גישה מרחוק. את השיחות המתחזות הם הפעילו בעזרת AI.

במקרה אחד, לפי התביעה, נגנבו 1.4 טרה־בייט מחברה אמריקאית. הכנופיה דרשה 10 מיליון דולר וקיבלה 5 מיליון. בחיפושים ב־66 מקומות נתפסו כמעט 370 אלף דולר ו־20 אלף אירו במזומן. לפי BleepingComputer, רישומי בית המשפט מזהים את כופרת Chaos.

> **מה לעשות:** להנחות עובדים לא להתקין תוכנת גישה מרחוק לפי בקשה טלפונית, ולאמת כל פנייה של "תמיכה טכנית" בערוץ נפרד.

מקור: התביעה הכללית באוקראינה · BleepingComputer

האקרים רוסים פרצו לארגון אחד, ובעזרת המידע פרצו לשני

לפי גוגל, קבוצת הריגול Cold Relic השתמשה ברשימות עובדים ובזהויות גנובות כדי להתחזות לאנשי קשר מוכרים.

לפי Mandiant וקבוצת המודיעין של גוגל, קבוצת הריגול הרוסית Cold Relic, שנודעה בעבר בשם COLDRIVER, פרצה בסוף 2025 לסביבת הענן של ארגון אמריקאי. היא השתמשה בסיסמה גנובה של מנהל־על, והציפה אותו בבקשות אימות עד שאישר אחת.

לפי גוגל, הקבוצה רשמה מכשירים, מפתחות גישה (passkeys) וקודי גיבוי משלה כדי להישאר בפנים גם אחרי החלפת סיסמה. היא הורידה את כל כונן הענן של הארגון ומחקה התראות אבטחה כדי להסתיר את עקבותיה.

אחרי שגורשה, הקבוצה התחזתה לעובדי הארגון הראשון ופנתה באפליקציית מסרים לעובד בארגון אמריקאי שני. היא שלחה לו קישור פישינג, השיגה גישה לחשבון שלו והורידה קבצים.

> **מה לעשות:** לבדוק אילו מכשירים, passkeys וקודי גיבוי רשומים בחשבונות מנהלים, ולבטל את מה שלא מוכר.

מקור: The Hacker News

בקצרה

Scattered Spider: ההאקר הסקוטי Tyler Buchanan, בן 24, נידון בארה"ב לשש שנות מאסר. לפי BBC, הוא וחבריו שלחו הודעות פישינג לעובדי חברות וגנבו יותר מ־11.6 מיליון דולר בקריפטו. הוא האחרון מחמשת הנאשמים בתיק שנגזר דינו. BBC

AI ואבטחה

גאזט סייבר · 19 בנובמבר 2026

זיוף עמוק של מאסק בשידור חי, ו־AI שעצר 4.7 מיליון דולר

יותר מחצי מיליון צפו בשידור מזויף שהבטיח להכפיל קריפטו. לפי Coinbase, מערכת AI עצרה 91% מההעברות.

לפי Coinbase, נוכלים הקימו ביוטיוב שידור חי מזויף של אירוע "המכונית המעופפת" של טסלה, עם זיוף עמוק (deepfake), כלומר וידאו מזויף שנוצר ב־AI, של אילון מאסק. בשידור הופיעו כתובות ארנק וקוד QR, והבטחה להכפיל כל קריפטו שיישלח. יותר מחצי מיליון איש צפו.

לדברי Coinbase, בתוך כשעתיים ניסו מאות לקוחות שלה לשלוח כסף לנוכלים. מערכת ה־AI של החברה זיהתה את ההעברות, פתחה שיחה קצרה עם הלקוחות והסבירה להם את ההונאה. לפי החברה, נעצרו כ־91% מהכסף, 4.7 מיליון דולר, בלי מעורבות של אדם.

Coinbase מדגישה שאיש לא נפרץ: הלקוחות עצמם אישרו את ההעברות. את הנתונים מוסרת החברה עצמה, ואין להם אימות חיצוני.

> **מה לעשות:** אין גורם לגיטימי שמכפיל קריפטו. לא לשלוח כסף לכתובת או לקוד QR שמופיעים בסרטון או בשידור.

מקור: Coinbase · The Block · Bitcoin Magazine

כלים ומחקר

גאזט סייבר · 19 בנובמבר 2026

חולשה בת עשר שנים ב־NGINX מאפשרת הרצת קוד בלי סיסמה

החולשה nginx2root נמצאת בתמיכה ב־HTTP/2 מאז 2015. גרסאות מתוקנות יצאו ביום רביעי, ועדיין לא דווח על ניצול.

F5, החברה שמאחורי שרת האינטרנט NGINX, פרסמה ביום רביעי תיקון לחולשה CVE-2026-123007, שקיבלה את הכינוי nginx2root. לפי The Hacker News, החולשה מאפשרת לתוקף בלי סיסמה להריץ קוד על שרת שבו HTTP/2 מופעל. היא קיימת בקוד מאז גרסה 1.9.5 מספטמבר 2015.

לפי F5, הרצת קוד אפשרית כשההגנה ASLR, שמערבבת את מיקומי הזיכרון, כבויה או נעקפת. חוקרי Wiz עקפו אותה בניסויים, ו־Xint הריצה קוד כשרק פורט HTTP/2 היה נגיש. הקוד רץ בהרשאות של תהליך NGINX. ב־Xint הגיעו להרשאות root דרך באג נוסף בליבת לינוקס, גם בתוך קונטיינר Docker.

לפי The Hacker News, קוד הדגמה זמין ב־GitHub, אבל עד יום רביעי לא דווח על ניצול. הגרסאות 1.31.9 ו־1.30.7 מתקנות גם ארבע חולשות נוספות. Ubuntu

ו־Debian עוד לא הוציאו חבילות מתוקנות.

> **מה לעשות:** לעדכן ל־1.31.9 או ל־1.30.7 ולבצע הפעלה מחדש מלאה, לא רק reload. עד אז אפשר לכבות HTTP/2.

מקור: The Hacker News · X News

חוקרים איפסו את נעילת ה־TPM ופיצחו קוד PIN של BitLocker

באוניברסיטה הטכנית של ברלין הראו שמי שפותח את המחשב יכול לנחש PIN של Windows Hello ו־BitLocker בימים במקום בשנים.

לפי The Hacker News, חוקרים מהאוניברסיטה הטכנית של ברלין מצאו דרך לאפס את מונה הניחושים השגויים של ה־TPM, רכיב האבטחה שמגן על קוד ה־PIN, במחשבי AMD ובחלק ממחשבי אינטל. לשם כך צריך לפתוח את המחשב ולחבר לוח קטן לשבב הזיכרון.

בניסויים הם מצאו PIN בן ארבע ספרות של Windows Hello ו־PIN בן שש ספרות של BitLocker, בתוך 236 ניסיונות. לפי חישוביהם, PIN בן שש ספרות של BitLocker שהיה מחזיק 19 שנה מחזיק עכשיו 20 יום. AMD אישרה פגם בקושחה, CVE-2026-43613, ומתכננת תיקונים עד פברואר 2027.

> **מה לעשות:** להאריך את ה־PIN של Hello ושל BitLocker בשתי ספרות לפחות, ולא להשאיר מחשבים ניידים ללא השגחה.

מקור: The Hacker News

סייבר ב־X

גאזט סייבר · 19 בנובמבר 2026

על מה מדברים: השיבושים בארה"ב, NGINX ו־Fugaku

הסיפורים הבולטים ב־X News בסייבר, 18 עד 19 בנובמבר. חלקם לא אומתו.

הדיון על השיבושים בארה"ב מוביל, אחרי שבכירים אמרו בקונגרס שלא הייתה מתקפת סייבר. לצדו עולים החולשה ב־NGINX וההשבתה של מחשב העל Fugaku.

מפתחים מחכים גם לעדכוני האבטחה של PHP, שלפי סיכום X News אמורים לצאת היום, 19 בנובמבר, בכל הגרסאות הנתמכות. הסיכומים נכתבים בידי Grok ועלולים לכלול טעויות.

מקור: X News · The Hacker News · CBS News

חולשות מנוצלות ו־KEV

גאזט סייבר · 19 בנובמבר 2026

תוקפים מנצלים חולשה קריטית בפלטפורמת הבלוגים Apache Roller

החולשה מאפשרת להריץ קוד על השרת בלי הזדהות. גם תיקון קודם מספטמבר לא סגר אותה בכל הגרסאות.

קרן Apache הודיעה שתוקפים מנצלים את CVE-2026-129448 ב־Apache Roller, פלטפורמת בלוגים בג'אווה, בגרסאות 4.0.0 עד 6.1.4. לפי The Hacker News, ממשק XML-RPC מפענח בקשות לפני שהוא בודק מי שלח אותן, וכך תוקף בלי הזדהות יכול להריץ קוד. הקרן לא מסרה מי מנצל ונגד מי.

מה לעשות: לעדכן ל־6.1.6. עד אז לבטל את ממשק XML-RPC בקובץ web.xml; כיבוי בממשק הניהול לא מספיק.

מקור: The Hacker News

CISA מוסיפה ארבע חולשות מנוצלות, בהן LiteLLM

החולשה ב־LiteLLM מאפשרת לברוח מארגז החול של בדיקת קוד מותאם ולהריץ קוד על השרת.

CISA הוסיפה ביום רביעי לרשימת החולשות המנוצלות ארבע חולשות: CVE-2026-40217 ב־LiteLLM של BerriAI, CVE-2024-10441 ב־Synology DSM, CVE-2026-90436 ב־Apache Axis ו־CVE-2026-90817 ב־REDCap. לפי מאגר OSV, החולשה ב־LiteLLM נמצאת בממשק לבדיקת קוד מותאם, ומאפשרת לצאת מארגז החול ולהריץ קוד.

> **מה לעשות:** לעדכן את LiteLLM ל־1.83.11 ומעלה, או לחסום את הנתיב /guardrails/test_custom_code.

מקור: CISA · OSV