גאזט סייבר
CYBER GAZETTE

ראשון, ה׳ בכסלו תשפ״ז · 15 בנובמבר 2026 גיליון 2 · מהדורת יום ראשון

בינה מלאכותית · אזהרת FBI

ה־FBI מזהיר: כלי AI פתוח מנהל פריצות כמעט לבד

לפי הבולשת, תוקפים משתמשים בכלי ARTEX מאוגוסט, ולפעמים מגיעים להרשאות גבוהות בפחות משלוש שעות. המפתח מחק את הקוד, אבל עותקים עדיין מסתובבים.

הבולשת האמריקאית, ה־FBI, פרסמה ב־13 בנובמבר אזהרה על כלי פריצה מבוסס בינה מלאכותית, שתוקפים מכל הסוגים הפכו לנשק. הכלי מבצע לבד את רוב שלבי הפריצה, מהסריקה הראשונה ועד הוצאת המידע, ואדם צריך רק להגדיר לו מטרה. לפי הבולשת, מאוגוסט לפחות הוא שימש נגד ארגונים בעולם כולו: בנקים, ממשלות, ביטחון, אנרגיה, בריאות ומשרדי עורכי דין.

למה זה חשוב? לפי ה־FBI, בחלק מהמקרים עברו פחות משלוש שעות מהבחירה במטרה ועד שהתוקף החזיק בהרשאות גבוהות ברשת. הכלי מאפשר גם לתוקפים עם ידע טכני מועט להריץ כמה מתקפות מורכבות במקביל. הוא מייצר הרבה רעש שעלול להפעיל התרעות, אבל המהירות שלו משאירה למגינים מעט זמן להגיב.

הכלי נקרא ARTEX. לפי ה־FBI, הוא פורסם בגלוי ב־GitHub ביולי 2026 בידי מפתח בכינוי Autumn-27, ככלי לבדיקות חדירה, כלומר פריצות מורשות שארגונים מזמינים כדי לבדוק את עצמם. המשתמש כותב מטרה במילים, והכלי מתרגם אותה לפקודות שמבצעים כמה סוכני AI: תוכנות שמקבלות משימה

ומבצעות אותה צעד אחר צעד. לכלי אין מודל שפה משלו, והוא מתחבר למודלים חיצוניים כמו Claude, GPT, DeepSeek ו־Grok.

לפי ה־FBI, במופעים שבשליטת תוקפים בולטים דווקא המודלים הסיניים, ובעיקר משפחת DeepSeek Flash. הסיבה: יכולת טובה, מחיר נמוך והיעדר מגבלות נראות כשהבקשה מוצגת כבדיקת חדירה. ב־8 באוקטובר הוריד המפתח את המאגר אחרי דיווחים על שימוש לרעה. לפי The Record, הוא זוהה כמהנדס סייבר סיני והכחיש אחריות לפשעים שבוצעו בכלי. זה לא עצר את ההתפשטות: הכלי ממשיך לעבור בעותקים, בגרסאות מקומיות ובגרסה מסחרית בשם ARTEX PRO.

איך זה נראה בשטח? בטבלת הטכניקות של ה־FBI מופיעים ניחוש תיקיות באתרים ביותר מ־500 בקשות, ניצול טפסים להעלאת קבצים בלי הזדהות, וסיסמאות מנהל שנכתבו בתוך קוד JavaScript של אתרים. הכלי השתיל webshells, קבצים קטנים בשרת שדרכם התוקף שולח פקודות מרחוק. בתוך הרשת הוא מיפה יותר מ־110 אלף אובייקטים ב־Active Directory, מערכת ניהול המשתמשים של הארגון, וחיפש מחשבים שאין בהם תוכנת הגנה.

מי נפגע? לפי ה־FBI, תוקפים עם מניע כספי פגעו במוסדות פיננסיים בדרום קוריאה וגנבו פרטים אישיים של כ־67 אלף בני אדם. במקרה אחר, תקיפת שרשרת אספקה, כלומר פריצה לספק כדי להגיע ללקוחות שלו, פגעה בלקוחות שירות הגיבוי בענן של ConnectWise ופתחה גישה ליותר מ־2,250 ארגונים. לפי The Record, מיקרוסופט קשרה את המתקפה הזו לשחקנים שנתמכים בידי המדינה הסינית. גם חברת Amazon פרסמה ביום שישי מחקר על קבוצות שקשורות לסין, שגנבו מפתחות גישה למודלי AI ומימנו בהם את המשך הציד.

הכלי גם קל למצוא. לפי ה־FBI, חוקרי Censys ספרו בתחילת נובמבר יותר מ־1,600 לוחות בקרה של ARTEX שחשופים לאינטרנט, ומספר ההתקנות האמיתי כנראה גבוה בהרבה. הבולשת פרסמה רשימת כתובות IP ודומיין שקשורים למתקפות, אבל מזהירה שכתובות בענן מתחלפות. לכן צריך לבדוק כל כתובת מול נתונים עדכניים לפני שחוסמים אותה.

מה לעשות. ה־FBI ממליץ למפות את כל המערכות שחשופות לאינטרנט, גם השוליות: פורטלים לספקים ולשותפים, אפליקציות עובדים ומערכות ישנות, כי שם הכלי מצליח במיוחד. ממשקי ניהול, גיבויים ושרתי וירטואליזציה צריכים להיות נגישים רק מרשתות מהימנות. כדאי לבדוק קריאות יוצאות לא צפויות לשרתי מודלים, כמו api.deepseek.com, לצד פעילות חשודה אחרת. מי שחיבר אפליקציות של ConnectWise ל־Microsoft 365 צריך לבדוק יומנים מ־1 באוקטובר לפחות, ולא למחוק את האפליקציות לפני ששמר ראיות.

מקור: FBI FLASH · The Record · TSN

בגיליון · הקישו לקפיצה

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

חולשות מנוצלות ו־KEV

גאזט סייבר · 15 בנובמבר 2026

PostgreSQL סוגרת 52 חולשות ונפרדת מגרסה 14

כמה מהחולשות מאפשרות למשתמש מחובר להריץ קוד על השרת. אחרי העדכון יש צעדים נוספים.

ב־12 בנובמבר שחררו מפתחי PostgreSQL את הגרסאות 18.7, 17.12, 16.16, 15.20 ו־14.25. העדכון סוגר 52 חולשות אבטחה ויותר מ־140 באגים. כמה מהחולשות, בדירוג CVSS 8.8, מאפשרות להריץ קוד, למשל CVE-2026-6460: בלבול סוגים אחרי SET DATA TYPE ... ALTER.

זו הגרסה האחרונה של PostgreSQL 14. מעכשיו היא לא תקבל תיקוני אבטחה. לפי הפרויקט, חלק מהתיקונים דורשים צעדים נוספים אחרי העדכון, והם מפורטים בסעיף Updating בהודעה.

מה לעשות: לעדכן לגרסה המתוקנת, לבצע את צעדי ההמשך שבהודעה, ולתכנן שדרוג לשרתים שעדיין על גרסה 14.

מקור: PostgreSQL

בקצרה

VS Code: חולשת הזרקת קוד בדירוג 9.6, CVE-2026-120779, מאפשרת לתוקף להריץ קוד דרך הרשת, אם המשתמש מבצע פעולה. מתוקן בגרסה 1.145.3. רשומת CVE

מועדי KEV: SonicWall SSLVPN עד 20 בנובמבר. Outlook, Chromium, Cisco BroadWorks ו־Openwave עד 24 בנובמבר. צ'קפוינט ו־UnrealIRCd כבר מחר, 16 בנובמבר. CISA

פריצות ואירועים

גאזט סייבר · 15 בנובמבר 2026

ספק שירות הלקוחות של Coinone נפרץ

מתוך שיחות התמיכה עלולים לדלוף מספרי זהות, חשבונות בנק וסיסמאות של לקוחות הבורסה הקוריאנית.

לפי Coinone, תוקף חדר בסביבות 4:00 לפנות בוקר, ב־12 בנובמבר, לשרת של MetaM, הקבלן שמפעיל את שירות הלקוחות של בורסת הקריפטו. הוא צפה ברשומות של שיחות תמיכה והוציא אותן. Coinone הודיעה ללקוחות ב־15 בנובמבר.

המידע שעלול לדלוף הוא מה שלקוחות מסרו בצ'אט או בטלפון: שמות, טלפונים, מספרי זהות, חשבונות בנק, סיסמאות, כתובות וארנקי קריפטו. לפי החברה, החשבונות, המסחר והארנקים מופרדים משרת הקבלן, ולא נמצאה חדירה אליהם. מי שלא פנה לשירות הלקוחות לא נפגע.

מה לעשות: לקוחות שפנו לתמיכה: להחליף סיסמה, ולא להיענות לפניות שמבקשות כסף או פרטים.

מקור: Chosun Biz · Seoul Economic Daily

אוסקה: מיליון כתובות מייל דלפו דרך ספק דיוור

הפריצה לשירות הדיוור Arara ממשיכה לגלגל נזק ביפן.

לפי העירייה, התוקפים חדרו לשירות הדיוור Arara, שמשמש את TKC, החברה שמתחזקת את מערכת השירותים המקוונים של העיר. כל מי שקיבל מייל מהמערכת בין יולי ל־31 באוקטובר נחשף. לפי The Record, מדובר ביותר ממיליון כתובות.

לפי Arara, הפריצה ב־2 בנובמבר חשפה 77 מיליון כתובות מייל של כמעט 400 לקוחות, והתוקפים שלחו דרך השירות מיליוני מיילים שהתחזו לחברות אשראי ולמוסדות פיננסיים.

מה לעשות: לא לפתוח קישורים או קבצים במיילים שנראים כאילו נשלחו מהעירייה.

מקור: The Record

בקצרה

Unocoin: הבורסה ההודית אישרה ב־14 בנובמבר גניבה של כ־200 אלף דולר משלושה ארנקים חמים, בעזרת מפתחות גיבוי שהודפסו על נייר לפני כשמונה שנים. גם מיילים, כתובות וסיסמאות מוצפנות של לקוחות עלולים להיחשף. Bitcoin.com

ActiveCloud: כופרה הצפינה חלק מתשתית ספק הענן הבלארוסי ושיבשה אתרים, מייל ושרתים וירטואליים לכמה ימים. זה המקרה השלישי החודש אצל ספקי אחסון ברוסיה ובבלארוס. The Record

יפן AXA: חברת הביטוח דיווחה על גישה לא מורשית לפורטל MyAXA. כ־597 אלף חשבונות אולי נפגעו, עם שמות, כתובות, תאריכי לידה, מיילים וטלפונים. החברה אישרה דליפה של חלק מהמידע. Alias Fleet

תוקפים וקמפיינים

גאזט סייבר · 15 בנובמבר 2026

אין היום ידיעות חדשות ומאומתות על ישראל ואיראן.

צפון קוריאה הקליטה מצלמות רשת של יותר מ־900 קורבנות

ה־FBI השבית תשתית של קמפיין FaceStealer, שגנב יותר מ־400 מיליון דולר בשיחות וידאו מזויפות.

לפי ה־FBI, התוקפים משתלטים על חשבון של אדם מוכר, שולחים הזמנה לשיחת וידאו בכתובת מזויפת של Zoom או Teams ומקליטים את המצלמה של הקורבן. בשיחה מוצג סרטון מוקלט של מי שכביכול הזמין, בלי קול. בתיבת הטקסט מופיעה הנחיה להתקין "תיקון" לשמע, והוא הנוזקה.

ה־FBI מייחס את הפעילות לקבוצה הצפון קוריאנית שמכונה Sapphire Sleet או BlueNoroff. לדבריו, הקבוצה מכוונת יותר ויותר למפתחי קוד פתוח, כדי להגיע למאגרים שלהם ומשם לשרשרת האספקה. נתפסו יותר מ־900 סרטונים.

> **מה לעשות:** כשמגיעה הזמנה לשיחה עם בקשה להתקין משהו, לאמת בערוץ אחר. לא להתקין "תיקוני שמע" מקישור.

מקור: FBI · The Register

AI ואבטחה

גאזט סייבר · 15 בנובמבר 2026

Darktrace: הזיכרון של Claude כערוץ שליטה חשאי

במעבדה הפכו החוקרים סוכן Claude Code לכלי בידי תוקף, דרך ערוץ שנראה כמו תעבורת AI רגילה.

חוקרי Darktrace Signal Labs הראו שתוקף שכבר חדר למחשב ומחזיק בפרטי ההתחברות של המשתמש ל־Claude Console יכול להוסיף "מאגר זיכרון" לסביבת

העבודה. הסוכן קורא משימות מקובץ זיכרון אחד וכותב את התוצאות לקובץ אחר, כך שכל התקשורת עוברת לשרתי Anthropic.

בניסוי הסוכן מיפה את הרשת, ריסס סיסמה על שרת הדומיין והוציא קובץ של 1 GB דרך Files API. לפי Darktrace, השיטה לא מנצלת חולשה בפלטפורמה ולא נראתה בשטח.

> **מה לעשות:** להתייחס למפתחות API של כלי AI כמו לפרטי גישה מרחוק, ולנטר כמה מידע סוכנים מעלים.

מקור: Darktrace

בקצרה

לוורדפרס MCP: בתוסף MCP Server for WordPress, עד גרסה 2.0.1, משתמש מחובר עם הרשאות נמוכות יכול להעלות את עצמו להרשאות גבוהות (CVE-2026-121576). גרסה 2.0.2 לא מושפעת. רשומת CVE

כלים ומחקר

גאזט סייבר · 15 בנובמבר 2026

Mior: מארח זדוני שובר את הגנת הענן של AMD

חוקרים מ־ETH ציריך עקפו את SEV-SNP, הטכנולוגיה שאמורה להגן על מכונה וירטואלית גם מפני ספק הענן.

SEV-SNP מצפינה את הזיכרון של מכונה וירטואלית ומגינה עליה מפני ה־hypervisor, התוכנה שמנהלת את המכונות בשרת. ב־Mior החוקרים משנים את ניתוב הזיכרון במעבד, כך שהבדיקות הראשוניות עוברות אבל ההגנות לא מופעלות. מנהל וירטואליזציה זדוני יכול אז לקרוא ולשנות את הזיכרון של המכונה, ואף לזייף דוחות אימות.

המתקפה הודגמה על מעבד EPYC 9135 Zen 5, ולפי החוקרים גם Zen 3 ו־Zen 4 אולי מושפעים. החולשה קיבלה את CVE-2026-0462, ו־AMD פרסמה קושחה מתוקנת. המחקר יוצג בכנס ACM CCS.

> **מה לעשות:** מי שמריץ מכונות וירטואליות חסויות בענן: לשאול את הספק מתי הקושחה המתוקנת תגיע.

מקור: Mior

סייבר ב־X

גאזט סייבר · 15 בנובמבר 2026

על מה מדברים: ARTEX, ספרד ושיחות וואטסאפ

הסיפורים הבולטים ב־X News בסייבר, 14 עד 15 בנובמבר. חלקם לא אומתו.

אזהרת ה־FBI על ARTEX מובילה את הדיון. מוכר בפורום טוען שבידיו מאגר של 46.3 מיליון ספרדים. האמינות לא אומתה. סוחר קריפטו מספר שאיבד את חסכונותיו אחרי שתוקף השתלט על המחשב שלו דרך קובץ בוואטסאפ. גם זה לא אומת.

כל ידיעה מקושרת למקור. סיכומי X News נכתבים בידי Grok ועלולים לכלול טעויות.