גאזט סייבר

שני, ו׳ בכסלו תשפ״ז · 16 בנובמבר 2026 · גיליון 3 · מהדורת יום שני

קריפטו · מתקפה בעזרת בינה מלאכותית

השתלטו על מכונות כרייה, והמנכ״ל מאשים את ה־AI

חברת Luxor מאשרת שתוקפים הפנו את כוח החישוב של יותר מתריסר לקוחות לבריכה אחרת. הפרצה תוקנה בתוך שעתיים, ואיך היא עבדה עדיין לא פורסם.

תוקפים השתלטו לפנות בוקר ביום ראשון, שעון ישראל, על מערכת לניהול מרחוק של מכונות לכריית ביטקוין, והפנו את כוח החישוב של המכונות לעבוד בשבילם. החברה שמפעילה את המערכת אישרה שנפגעו יותר מתריסר חשבונות של לקוחות, ושהפרצה תוקנה בתוך שעתיים. המנכ״ל שלה אומר שהתוקפים נעזרו בבינה מלאכותית, ומזהיר שמתקפות כאלה רק יתרבו.

למה זה חשוב? כריית ביטקוין היא תחרות חישוב: מכונות ייעודיות פותרות חידות מתמטיות, ומי שתורם כוח חישוב מקבל חלק מהתגמול. מי ששולט בתוכנה שמנהלת את המכונות יכול לשנות לאן הן שולחות את העבודה, ולקחת את הרווח בלי לגעת בחומרה. פריצה אחת לתוכנת ניהול מרכזית פוגעת בבת אחת בציים של כמה לקוחות.

החברה היא Luxor, והתוכנה היא Commander, שבה לקוחות מנהלים את צי המכונות שלהם. לפי Luxor, מערכת הניטור שלה זיהתה בלילה שינוי לא מורשה בהגדרות בריכת הכרייה, כלומר השרת שאליו המכונות שולחות את העבודה ושמחלק את התגמול. המכונות של הלקוחות שנפגעו הופנו לבריכה אחרת לזמן

מוגבל. המהנדסים תיקנו את הפרצה בתוך שעתיים, ואז התחילו להחזיר את המכונות להגדרות המקוריות.

המנכ"ל, ניק הנסן, כתב שהלקוחות נפגעו דרך "וקטור מתוחכם מבוסס AI", כלומר שיטת חדירה שנעזרה בבינה מלאכותית. החברה לא פרסמה איך בדיוק זה עבד. לדבריו, כל מי שמנהל עסק משמעותי, ובעיקר בקריפטו, מוצף היום במתקפות כאלה, והקצב עולה ככל שהמודלים משתפרים. הוא תיאר מודלים שהוסרו מהם המגבלות, שרצים מסביב לשעון ומחפשים סדק קטן.

כמה מכונות נפגעו? עדיין לא ברור. לפי הערכות שפורסמו בשבת בלילה, כ־64 אלף מכונות, עם כוח חישוב של כ־13 אקסה־האש לשנייה, הופנו לבריכת הכרייה OCEAN. החברה לא אישרה את המספרים, ואמרה רק שנפגעו "קצת יותר מתריסר חשבונות לקוחות". לפי Bitcoin.com, מספר החשבונות לא מלמד כמה מכונות נפגעו בסך הכול.

והתוקף הרוויח משהו? לפי Cointelegraph, כתובת ביטקוין שחברת CoreX קשרה לאירוע קיבלה שני תשלומים מ־OCEAN, בסך כ־0.162 ביטקוין, כ־10,500 דולר. החברה התחייבה לפצות כל לקוח שנפגע במלואו, "כאילו המכונות כרו כרגיל", ולפרסם תחקיר. לפי החברה, לא דלף מידע מהמערכות שלה, והפריצה נשארה בתוך Commander: בריכת הכרייה שלה ומערכת ההפעלה LuxOS לא נפגעו.

המקרה מצטרף לשורה של פריצות לעסקי קריפטו שבהן, לפי הדיווחים, נעזרו התוקפים ב־AI. הנסן אמר שהחברה הקפיאה את רוב עבודת הפיתוח כדי לחזק את האבטחה, וקנתה מעבדים גרפיים כדי להריץ בעצמה מודלים פתוחים לשיפור ההגנה. מה לעשות: מי שמנהל מכונות דרך שירות כזה צריך לבדוק בלוח הבקרה של הבריכה שהמכונות שלו מדווחות לחשבון שלו, ושכתובת התשלום לא שונתה.

מקור: Bitcoin.com · Cointelegraph

בגיליון · הקישו לקפיצה

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

חולשות מנוצלות ו־KEV

גאזט סייבר · 16 בנובמבר 2026

מפתחות פרטיים ביומני ניטור: 870 ארנקים רוקנו

פלטפורמת המסחר Proxima, שפועלת ברשת סולנה, כתבה בטעות מפתחות של ארנקים ליומנים. שרת ניטור לא מעודכן וכלל חסימה שנמחק השלימו את השרשרת.

לפי התחקיר של Proxima, תוקף רוקן ב־14 בנובמבר, בין 05:22 ל־07:42 שעון ישראל, 5,324.2 SOL מ־870 ארנקים של 181 משתמשים. השורש: בין 3 ל־10 בנובמבר הורידה החברה את רמת הרישום בשרתים כדי לנטר ביצועים, ושורת קוד ישנה כתבה ליומנים מפתחות פרטיים של ארנקים.

היומנים נשמרו 15 יום בשרת SigNoz, כלי ניטור בקוד פתוח, שרץ על גרסה ישנה עם חולשה ידועה שמאפשרת גישה בלי הזדהות. כלל ב־Cloudflare, שאמור היה להסתיר את השרת מהאינטרנט, נמחק בטעות. החברה לא ציינה איזו חולשה נוצלה. באתר AltcoinReporter מציינים כאפשרות את CVE-2026-97055, שתוקנה בגרסה 0.143.0, אבל זה לא אושר.

לפי החברה, כל ההפסדים כוסו מהקופה שלה, והארנקים שנחשפו הוחלפו בחדשים.

> **מה לעשות:** לעדכן את SigNoz לגרסה 0.143.0 ומעלה, להגדיר סוד חתימה, ולוודא שמפתחות וסודות לא נכתבים ליומנים.

מקור: AltcoinReporter · SolanaHub · OSV

דרום קוריאה: 300 תיבות מייל ממשלתיות נפרצו

התוקפים נכנסו דרך רשתות חלשות של רשויות מקומיות וניצלו חולשה במערכת הכניסה האחידה. שירות הביון מצטרף לחקירה.

משרד הפנים והביטחון של דרום קוריאה הודיע ב־16 בנובמבר שתוקפים חדרו למערכת המייל של עובדי המדינה, שמפעיל מרכז ניהול משאבי המידע הלאומי. נמצאה גישה חריגה לכ־300 חשבונות. המשרד קיבל הודעה על הפריצה מגופים אחרים ב־9 בנובמבר.

לפי הממצאים הראשונים, התוקף עבר דרך רשתות פגיעות של כמה רשויות מקומיות וניצל חולשה ב־SSO, מערכת הכניסה האחידה: התחברות אחת שפותחת את המייל, את האישורים הממוחשבים ומערכות עבודה נוספות. המשרד דיווח לרשות להגנת המידע האישי ועדכן את מי שהמידע שלו דלף.

החיבורים המיותרים בין שרתי הרשויות למערכת המייל נחסמו, והניטור הוגבר. חקירה משותפת עם שירות הביון הלאומי ו־KISA תבדוק את נתיב החדירה, והאם נשארה נוזקה במערכות. המשרד לא אמר מי עומד מאחורי הפריצה.

> **מה לעשות:** מי שמפעיל כניסה אחידה: לבדוק אילו רשתות חיצוניות מחוברות לשרת ההזדהות, ולנתק כל חיבור שלא נחוץ.

מקור: Yonhap · Newsis · Aju Press

רשת Tor תחת מתקפת הצפה, ועדכון חירום לממסרים

רוב מפעילי הממסרים נפגעו. בעדכון הוסרו גם המפתחות של שרת סמכות, בגלל פריצה אפשרית.

פרויקט Tor שחרר ב־13 בנובמבר את גרסה 0.4.9.17, עדכון חירום שמיועד בעיקר לממסרים: השרתים שמתנדבים מפעילים, ושדרכם עוברת התעבורה האנונימית.

לפי הפרויקט, מתקפת מניעת שירות מתמשכת פוגעת ברוב המפעילים. הממסרים מוצפים במבול של מעגלים, כלומר נתיבי חיבור שלקוחות פותחים דרך הרשת.

התיקון המרכזי: הממסרים יזהו לקוחות IPv6 לפי קידומת /64 ולא לפי כל כתובת בנפרד, כך שכתובות רבות מאותו טווח ייספרו כלקוח אחד. בעדכון הוסרו גם המפתחות של bastet, אחד משרתי הסמכות של הרשת, בגלל פריצה אפשרית. הפרויקט בוחן הגנות נוספות ומצפה לעדכונים נוספים בקרוב.

מה לעשות: מפעילי ממסרים: לעדכן מיד לגרסה 0.4.9.17.

מקור: Tor Forum · tor-announce

בקצרה

Coles: רשת הסופרמרקטים האוסטרלית חוקרת אירוע סייבר יחד עם מרכז הסייבר האוסטרלי. לפי החברה, אין עדות לפגיעה במידע של לקוחות, עובדים או ספקים, והחנויות פועלות כרגיל. היא בודקת תקלות באיסוף הזמנות של Liquorland. SBS

N0n: קבוצת הסחיטה פרסמה ב־14 בנובמבר טענה שבידיה מידע של עובדים ולקוחות מ־Gap. הרשומה באתר הדליפות לא כוללת שום הוכחה, ו־Gap לא אישרה אירוע. Cypro

תוקפים וקמפיינים

גאזט סייבר · 16 בנובמבר 2026

אין היום ידיעות חדשות ומאומתות על ישראל ואיראן.

התחזו לעוזר של חבר פרלמנט, ושלחו את הקובץ רק כשביקשו

Genians: קבוצה שכנראה קשורה לצפון קוריאה תקפה משתתף בסמינר בפרלמנט הקוריאני, ושלטה בנוזקה דרך אתר פתקים ציבורי.

לפי חברת האבטחה הקוריאנית Genians, בין 12 ל־18 בספטמבר קיבל משתתף בסמינר בפרלמנט מייל מ"עוזר בכיר" של חבר פרלמנט, עם בקשה למלא טופס לתשלום שכר טרחה. במייל הראשון לא היה קובץ, וזה היה מכוון. כשהקורבן השיב שהקובץ חסר, הגיע קובץ ZIP עם קיצור דרך שהתחפש למסמך.

הקובץ פתח טופס אמיתי והריץ ברקע סקריפטים. הנוזקה קראה פקודות מדף בשירות פתקים ציבורי, כך שהתוקף החליף כלים רק בעריכת הפתק. בחודש שעבר הותקן דרכו NodeLinkRAT, כלי שליטה מרחוק שרץ על Node.js, גונב קבצים וצופה במסך בזמן אמת.

החברה מייחסת את הפעילות לקבוצה Kimsuky ברמת ביטחון בינונית, בגלל חפיפה בחשבונות, במבנה עמודי ההתחזות ובטווחי הכתובות של השרתים. החברה לא שוללת שקבוצה אחרת מחקה את השיטה.

> **מה לעשות:** לחשוד בקובץ שמגיע אחרי "שכחתי לצרף", ולבדוק אם "מסמך" הוא בעצם קיצור דרך.

מקור: Genians · Korea JoongAng Daily

AI ואבטחה

גאזט סייבר · 16 בנובמבר 2026

גוגל מקצרת את הזמן לתיקון חולשות, בגלל AI

Project Zero תפרסם פרטי חולשות 90 יום אחרי הדיווח, גם אם לא תוקנו. ב־2028 החלון יירד ל־30 יום.

צוות Project Zero של גוגל, שמחפש חולשות במוצרים של חברות אחרות, הודיע על מדיניות חשיפה חדשה. עד עכשיו ספקים קיבלו 90 יום לתיקון ועוד 30 יום להפצת העדכון. מעכשיו הפרטים יתפרסמו 90 יום אחרי הדיווח, בלי קשר למצב התיקון. ב־2 בפברואר 2027 החלון יירד ל־60 יום, וב־3 בינואר 2028 ל־30 יום.

הסיבה, לפי הצוות: מודלי שפה מאפשרים לתוקפים למצוא ולנצל חולשות מהר יותר, ולהבין חולשה מתוך העדכון שלה כמעט מיד. הצוות עצמו מוצא היום כמה חולשות בשבוע במוצרים שבהם מצא פעם כמה בשנה. רוב החריגים, כמו תקופת החסד, בוטלו. חולשות שכבר מנוצלות בשטח יטופלו לפי מדיניות נפרדת של גוגל.

מה לעשות: לקצר את הזמן מפרסום עדכון אבטחה ועד התקנתו, כי פרטי החולשות יתפרסמו מהר יותר.

מקור: Project Zero · SecLog

סייבר ב־X

גאזט סייבר · 16 בנובמבר 2026

על מה מדברים: מכונות הכרייה, Tor ו־Kava

הסיפורים הבולטים ב־X News בסייבר, 15 עד 16 בנובמבר. חלקם לא אומתו.

ההשתלטות על מכונות הכרייה מובילה את הדיון, עם המספר 64 אלף שעדיין לא אושר. סביב מתקפת ההצפה על Tor יש משתמשים שמשערים שמדינות עומדות מאחוריה. אין לכך ראיה. לפי הסיכום, תוקף ניצל פרצה במודול ההלוואות של Kava ושאב כ־55 מיליון אסימוני KAVA. גם זה לא אומת.