קמפיין תקיפה באמצעות שרשרת האספקה כנגד ספריות ב-NPM

31/03/2026
י"ג ניסן תשפ"ו

[תקציר]

1. לאחרונה התפרסמו ידיעות בנוגע לקמפיין תקיפה המבוצע באמצעות ספריות ב-NPM (מאגר חבילות תוכנה הכתובות ב-JavaScript) המהוות שרשרת אספקה למספר רב של חבילות תוכנה ותוכנות מסחריות ואחרות.
2. מספר הספריות המותקפות גבוה, וחלקן בשימוש מספר רב של תוכנות ומשתמשים, או מטפלות בשמירה מאובטחת של פריטי מידע סודיים ורגישים המשמשים מערכות פיתוח כגון API Keys, Session Tokens וכד'.
3. מדובר בקמפיין פעיל ומתפתח. מערך הסייבר הלאומי יעדכן מסמך זה בהתאם לצורך.

[פעולות מידיות לביצוע]

- בכל מקרה של חשד כי במערכות הארגון פעלו או פועלות חבילות תוכנה שהודבקו במזיד במהלך הקמפיין, יש לפעול מיידית על פי הנוהל הארגוני לחשד לאירוע סייבר.
- מומלץ למשתמשים בחבילות תוכנה שפורסמו שהותקפו, לנטרל עד לסיום בדיקתם כל אפשרות ממוכנת לעדכון החבילות ללא אישור של מנהלן, ולוודא מיידית האם הגרסה שבשימושם הודבקה או לא.

[פרטים]

1. במהלך השבועיים האחרונים זוהה קמפיין תקיפה מתמשך הכולל תולעת ב-NPM, אשר הדביקה וממשיכה להדביק מספר רב של חבילות פיתוח. התוקפים ניצלו publish tokens (מפתחות המאפשרים עדכון ופרסום הקוד של חבילות תוכנה) שנגנבו, כדי להפיץ נוזקות גם ב-PyPI, מאגר המידע העיקרי של חבילות תוכנה בשפת Python, באמצעות חבילות קוד פתוח פופולריות.
2. התוקף מזוהה בדיווחים ברשת כ-TeamPCP.
3. להלן דרכי הפעולה העיקריות של התולעת, המוכרת בשם Canister Worm:
   1. ככל הנראה, התקיפה החלה בפריצה של GitHub Actions (ובפרט trivy-action ו-setup-trivy של Aqua Security), דרכה הושגו Publish Tokens ל-NPM. התולעת הפיצה עצמה גם באמצעות github actions: checkmarx/kics-github-action and checkmarx/ast-github-action.
   2. התולעת מנצלת Tokens שמצאה במהלך פעילותה, אשר נאספים מ-CI/CD runners, כדי להתפשט לחבילות נוספות השייכות למשתמש שנפגע, באמצעות פרסום גרסאות חדשות הכוללות קוד זדוני.
   3. גרסאות מתקדמות יותר של הנוזקה כוללות יכולות תנועה רוחבית, בין היתר באמצעות גניבת מפתחות SSH פרטיים.
   4. לצורך שימור אחיזה (persistence), הנוזקה יוצרת שירותים במערכות המותקפות עם שמות כדוגמת "Postgres Monitor Service" או "System Telemetry Service".

5. לפוגען יכולת הרצה של קוד זדוני נוסף, בהתאם לפקודות מרחוק המתקבלות באמצעות מנגנון C2 עם שרתי התוקף.
6. בשבוע האחרון דווח כי התוקפים עושים שימוש גם ב-publish tokens ל־PyPI, המנוצלים להדבקה של חבילת הפייתון הפופולרית LiteLLM . הנוזקה שהושתלה בספריה היא מסוג stealer, ומטרתה גניבת מידע רגיש, לרבות:
   1. סודות של סביבות ענן
   2. מפתחות SSH
   3. סיסמאות למסדי נתונים
   4. קבצים ומפתחות הקשורים לארנקי קריפטו
7. ביממה האחרונה נודע כי התוקף השיג נגישות לחבילת התוכנה Axios, אחת החבילות הפופולריות במאגר NPM, ופרסם 2 גרסאות הכוללות קוד זדוני שהושתל בהן.

[דרכי התמודדות]

1. מומלץ מאד לעקוב אחר פרסומים של חברות אבטחה אודות חבילות קוד פתוח נוספות שנדבקו בתולעת או הודבקו ב-stealer.
2. לארגון החושד שנעשה שימוש בגרסת תוכנה נגועה במערכותיו, מומלץ לפעול לפי נהלי הארגון. בפרט, אם זוהתה הדבקה באמצעות חבילת תוכנה נגועה, יש לבצע רוטציה של כלל ה-secrets בסביבות הפיתוח הארגוניות, ומומלץ לפנות לייעוץ של חברת IR המתמחה בטיפול באירועים מסוג זה.
3. פורסם ברשת מאגר מזהים רלוונטי לאירוע זה. כתובתו בקישור מס' 2. מומלץ לבדוק לאחור לפחות 30 יום, האם מזהים ממאגר זה מופיעים במערכותיכם.
4. רשימת החבילות הנגועות שהושתלו על ידי התוקף נמצאת גם היא במאגר זה (אין התחייבות שהרשימה מקיפה ויש לעקוב אחר הפרסומים בנדון). מומלץ מאד לבדוק נוכחות או שימוש (dependency) בחבילות בגרסאותיהן הזדוניות בסביבות הפיתוח הארגוניות.
5. מומלץ לבדוק נוכחות של repositories שמתחילים בשם tpcp-docs בסביבות ה-github הארגוניות.

[מקורות]

1. https://www.gov.il/BlobFolder/reports/alert_1934/he/ALERT-CERT-IL-W-1934.pdf
2. https://ramimac.me/teampcp/
3. https://opensourcemalware.com/
4. https://docs.litellm.ai/blog/security-update-march-2026
5. https://checkmarx.com/blog/checkmarx-security-update/
6. https://www.aquasec.com/blog/trivy-supply-chain-attack-what-you-need-to-know/
7. https://www.wiz.io/blog/axios-npm-compromised-in-supply-chain-attack