משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

בלמ"ס

TLP: **לבן**

27 דצמבר 2017
ט' טבת תשע"ח
סימוכין: ב-ס-403

תקיפות לכריית מטבעות וירטואליים – זיהוי והתגוננות

תקציר

מטבעות וירטואליים הפכו בשנים האחרונות לדרך תשלום מוכרת בעולם בכלל וברשת האינטרנט בפרט. העלייה התלולה שחלה בחודשים האחרונים במחיריהם של מטבעות וירטואליים רבים, ובפרט מטבע הביטקוין, הביאה למגמה מתגברת של תקיפת מחשבים ושרתים על מנת להשתמש במשאבי המחשוב שלהם (בעיקר מעבד ומעבד גרפי) לצורך כריית מטבעות וירטואליים לטובת התוקפים. התרעות בנושא הופצו בסימוכין ב-ס-404, ב-ס-318, ב-ס-311 וכן ב-ס-143.

מסמך זה יתאר את התופעה וכן יפרט דרכים לזיהוי ולהתמודדות עמה.

פרטים

רקע – כריית מטבעות והאטרקטיביות לתוקפים

כריית מטבעות וירטואליים היא הדרך שבה משתמשי מטבע וירטואלי "משלמים" לגורמים העוסקים בווידוא הטרנזקציות השונות של המטבע. תמורת השקעתם בהפעלת האלגוריתם המאפשר לוודא את הטרנזקציות של המטבע הווירטואלי, אלגוריתם הדורש משאבי מחשוב רבים, המפעילים מקבלים בעצמם הקצאה של מטבע וירטואלי, בשיטה המבוססת לרוב על הוכחת ביצוע עבודה מסוימת (Proof Of Work). פעולה זו נקראת "כריית מטבע".

המטבעות הווירטואליים הראשונים, ובפרט ביטקוין, מצריכים בדרך כלל שימוש בחומרה ייעודית ויקרה לצורך כרייה יעילה. עם זאת, בשנים האחרונות פותחו מטבעות וירטואליים אשר ניתנים לכרייה יעילה גם על גבי מחשבים אישיים או אף פלטפורמות חלשות יותר כגון ציוד IoT וטלפונים סלולריים. בנוסף, ככל שרשת המחשבים הנגישה לתוקפים גדולה יותר, כמות הציוד המשתתף באלגוריתם מפצה חלקית על האיטיות היחסית של המעבדים לעומת חומרה ייעודית.

לאור העלייה המסחררת בשעריהם של המטבעות הווירטואליים, נוצר אפיק רווח ישיר לתוקפים, באמצעות ניצול מחשבים מותקפים לכריית מטבע עבורם. פעולה זו לכאורה נטולת קורבן, משום

שהתוקף אינו מעלים קבצים מהגורם המותקף כפי שעושה כופרה, או גונב את סודותיו כפי שעושה רוגלה.

למעשה, הפעולה אינה נטולת קורבן כלל ועיקר. כריית מטבעות וירטואליים הינה מטלה הדורשת משאבים רבים, בעיקר של המעבד ו/או המעבד הגרפי, ובכך מונעת לחלוטין או מאיטה מאוד את פעולת המשתמש הלגיטימי בעמדה. בנוסף, השימוש האינטנסיבי במעבד מעלה את צריכת החשמל של העמדה, שעליה ישלם המשתמש המותקף, ועלול במקרים קיצוניים אף לגרום לנזק פיזי למחשב עקב נזקי חום למעבדים.

יעדי התקיפה

זוהו תקיפות למטרת כריית מטבעות נגד מחשבים אישיים (הן באמצעות פוגען ייעודי והן באמצעות הרצת סקריפט בדפדפן בזמן הגלישה באתר התוקף), שרתים, ציוד IoT, נתבים, טלפונים סלולריים, מערכות מחשוב בענן וכד'.

אופן התקיפה

וקטור התקיפה יכול להיות פוגען קלאסי המתקין עצמו על הציוד המותקף, או סקריפט הפועל רק כאשר הדפדפן פתוח על האתר התוקף. קיימים אתרים שכורים מטבע באמצעות ציוד המשתמשים כתחליף להצגת פרסומות, ונצפו אתרים אליהם הוזרק קוד לכרייה על ידי תוקף ללא ידיעתם, לאחר תקיפת השרתים בשיטות שונות.

במקרה של קוד כרייה המופעל כסקריפט בלבד, ללא התקנה, סגירת הדפדפן או מעבר לאתר אחר תפסיק את התקיפה.

התקפה באמצעות סקריפט קיבלה חיזוק משמעותי בעקבות הופעת האתר Coinhive, אשר הציע סקריפט מוכן לביצוע כרייה של מטבע מסוג Monero. הפעלת הסקריפט פשוטה מאוד ודורשת הוספת שורות קוד ספורות בלבד לדף באתר.

<u>דרכי התמודדות</u>

זיהוי

המזהה האופייני ביותר לתקיפה מסוג זה היא עלייה תלולה בצריכת משאבי המעבד של העמדה, לעיתים אף עד כדי 100% שימוש במעבד. עם זאת, תוקפים עלולים להגביל את צריכת המשאבים על מנת לעכב גילוי, ולכן כל **חריגה מתמשכת** מצריכת המשאבים האופיינית לעמדה או השרת (ה-

BASELINE), או ריבוי קפיצות בצריכת המעבד לאורך זמן (למשל, רק בעת ביקור באתר מסוים), עלולות להעיד על תקיפה מסוג זה.

מניעה

קיימות מספר דרכים למניעת השימוש בכורי מטבע וירטואליים:

א. הפעלת שיקול דעת בפתיחת צרופות ו/או לחיצה על לינקים בהודעות דוא"ל, במיוחד בהודעות שמקורן לא מוכר או שהגיעו במועד לא צפוי.

ב. תוכנות אנטי-וירוס עשויות לזהות ו/או למנוע הפעלה של כורי מטבע וירטואלי.

ג. תוספים לדפדפן המונעים הרצת סקריפטים, ימנעו הרצת סקריפטים בכלל, וסקריפטים לכריית מטבע וירטואלי בפרט. התוסף המוכר ביותר בתחום זה הוא NoScript עבור הדפדפן Firefox, אך קיימים תוספים דומים גם לכרום.

ד. תוספים לדפדפן המונעים הרצת סקריפטים ספציפיים המיועדים לכרייה, כגון הסקריפט של Coinhive. המוכר מכולם הוא תוסף בשם NoCoin המיועד לדפדפנים כרום ו- Firefox. תוסף נוסף מסוג זה הוא minerBlock.

ה. תוספים לדפדפנים המיועדים לחסימת פרסומות (Ad Blockers) החלו לאחרונה לחסום גם הם סקריפטים לכריית מטבעות.

במידה שבבדיקתכם התגלה ממצא כלשהו נבקש לקבל היזון חוזר. לכל מידע נוסף ניתן לפנות אלינו.

הערה: שיתוף מידע עם ה- CERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כל שהוא, במידה שהתגלה צורך כזה.

בברכה,

CERT-IL

טל: 9344*

team@cert.gov.il