12 בינואר 2021
כ"ח בטבת תשפ"א
סימוכין: ב-ס-1255

פוגען ייעודי לגניבת ארנקי מטבעות קריפטוגרפיים

תקציר

1. חברת Intezer פרסמה לאחרונה מידע לגבי פוגען ייעודי לגניבת ארנקי מטבעות קריפטוגרפיים.
2. על פי הפרסום, הפוגען היה פעיל במשך כשנה ופגע בכ-6,500 משתמשים בעולם.

פרטים

1. הפוגען מכונה ElectroRAT, כתוב בשפת Go, ומיועד להרצה על מערכות ההפעלה Windows, macOS ו-Linux.
2. הפוגען הותקן בתוך 3 יישומים שנכתבו ע"י התוקפים. 2 מהיישומים (Jamm ו-eTrade) יועדו להתחזות כתוכנות לניהול מסחר במטבעות קריפטוגרפיים, ויישום נוסף (DaoPoker) הינו משחק פוקר מבוסס מטבע קריפטוגרפי.
3. לאחר התקנת היישומים והפעלתם, הם מציגים מסכים המותאמים לסוג היישום, אך ברקע מפעילים את הפוגען. הרצת הפוגען מתבצעת באמצעות תהליך בשם mdworker. הפוגען מנסה לגנוב נתוני גישה לאתרי מסחר ומפתחות פרטיים.
4. הפוגען מתקשר עם עמודים ספציפיים באתר pastebin לקבלת הכתובת של שרת ה-C2. עמודים נוספים שהועלו על ידי אותו משתמש, מלמדים על שימוש התוקפים גם בפוגענים מוכרים בשם KPOT ו-Amadey, לגניבת ארנקי מטבעות קריפטוגרפיים.
5. לפוגען יכולות מגוונות כגון הקלטת הקשות מקלדת, ביצוע צילומי מסך, העלאת קבצים לשרת C2, והורדת קבצים והרצתם על עמדת המשתמש.

6. על מנת ליצור את הרושם כי מדובר ביישומים תמימים, התוקפים יצרו אתרי Web ליישומים, קידמו אותם בפורומים ייעודיים כגון bitcointalk ו-SteemCoinPan , ואף פתחו חשבונות בטוויטר ובטלגרם על מנת לפרסמם, כולל תשלום לגורם משפיע (Influencer) בעל 25 אלף עוקבים על מנת לקדמם.

דרכי התמודדות

1. להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם במערכות הרלוונטיות.
2. אם התקנתם את אחד היישומים המוזכר בהתרעה, מומלץ להסירו מיד. מומלץ לוודא כי העמדה נקיה באמצעות כלי אבטחת מידע שברשותכם (AV, EDR וכד'). מומלץ להעביר את כל המטבעות הקריפטוגרפיים שברשותכם לארנקים חדשים ולהחליף סיסמאות גישה.

מקורות

https://www.intezer.com/blog/research/operation-ElectroRAT-attacker-creates-fake-companies-to-drain-your-crypto-wallets/

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו.
המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.