14 דצמבר 2020
כ"ח כסלו תשפ"א
סימוכין: ב-ס-1234D
[עדכון]
16 דצמבר 2020
א' טבת תשפ"א
[עדכון]
27 דצמבר 2020
י"ב טבת תשפ"א
[עדכון]
29 דצמבר 2020
י"ד טבת תשפ"א

[עדכון4] קמפיין תקיפה רחב כנגד גופים במשק הישראלי

תקציר

1. בשבועות האחרונים מטפל מערך הסייבר הלאומי בקמפיין תקיפה המופעל ע"י קבוצת תקיפה משמעותית כנגד מספר רב של גופים במשק.
2. המערך מוצא לנכון לשתף את הגופים במשק בממצאי החקירה אשר נאספו עד כה מהחברות הנתקפות והועשרו על בסיס מקורות שונים.
3. [עדכון4] ההתרעה הנ"ל כוללת קובץ מזהים מעודכן הכולל מזהים חדשים אותם יש לנטר ו\או לחסום במערכות הארגוניות בצורה הרמטית ככל שניתן, ולדווח למערך על כל התאמתות של אחד או יותר מהם. ההתרעה כוללת גם חוק YARA נוסף.

פרטים

1. בשבועות האחרונים מטפל מערך הסייבר הלאומי בקמפיין תקיפה משמעותי הפועל כנגד מספר רב של גופים ממגזרים שונים ואשר עלול לייצר סיכון ניכר למשק.

2. חלק משמעותי מן הנתקפים שזוהו עד כה הינם לקוחותיה של חברה אשר דרכה הצליח התוקף לייצר נגישות רשתית למערכותיהם במתווה שרשרת אספקה.
3. התוקף העומד מאחורי הקמפיין משתמש במגוון כלים, אשר חלקם עשויים לשמש גם לתכליות לגיטימיות, אולם מקבץ המזהים המצורף להתרעה הינו אינדיקטיבי דיו לטובת איתור פעילותו.
4. חשוב לציין כי בחלק מהגופים הנתקפים אותרו ממצאים המקושרים לכופרה Pay2Key אשר פורסמה ע"י מספר חברות אבטחה לפני מספר שבועות ועל כן חשוב להשקיע את מירב המאמצים במימוש ההמלצות המובאות להלן.
5. בין האמצעים המשמשים את התוקף זוהתה בחלק מן הגופים יצירה של משתמש בעל הרשאות מנהלן ברשת (Administrator) וכן יצירה של משימה מתוזמנת (Scheduled Task) בשם VerifiedPublisherCertStoreVerify, הממוקמת בנתיב Microsoft\Windows\AppID\ ברשימת המשימות המתוזמנות.
6. [עדכון] זוהתה יצירה של משימה מתוזמנת נוספת על ידי התוקף, הממוקמת בנתיב Microsoft\Windows\WDI\ResolutionServer ברשימת המשימות המתוזמנות.
7. [עדכון] בנוסף, התוקף משתמש בטכניקה נוספת המתבססת על מנגנון Sticky Keys על מנת לשמר אחיזה בעמדה הנתקפת, וזאת באמצעות החלפת קובץ המשמש לסיוע לנגישות c:\windows\system32\sethc.exe בקובץ cmd.exe.
לאחר שינוי קונפיגורציה זה, ברגע שהתוקף יקיש 5 פעמים על Shift במסך הנעילה, הוא יקבל גישת CMD לעמדה הנתקפת בהרשאת System ללא צורך בהזדהות.
פרטים על תקיפה זו בקישור https://attack.mitre.org/techniques/T1546/008.
8. מערך הסייבר ממשיך לטפל בגל התקיפות המתואר לעיל ולהפיץ למשק מזהים ואמצעי התגוננות עדכניים ככל שיתווספו כאלו.

דרכי התמודדות

1. להתרעה זו מצורף קובץ מזהים - מומלץ מאד לנטרם בכל המערכות הארגוניות הרלוונטיות (FW, AV, שרתי פרוקסי, EDR, SIEM, CDR, מערכות הלבנה, מערכות סינון דוא"ל), וכמו כן לבצע חיפוש של מזהים אלו במערכות הרלוונטיות 3 חודשים לאחור.

2. עבור מזהי הקבצים (Hashes) - מומלץ לבצע סריקה אקטיבית בתחנות עבודה ובשרתים, ישירות או באמצעות הגדרת חוקים במערכות AV או EDR.
3. [עדכון] מצורפות להתרעה גם חתימות YARA אותן מומלץ מאוד להטמיע במערכות האבטחה הארגוניות המאפשרות זאת וכן בעמדות הקצה והשרתים בארגון.
4. מומלץ לאתר משתמשי מערכת לא מזוהים ו/או שנוצרו בתקופה האחרונה, בפרט בעלי הרשאות מנהלן, ולוודא כי יצירתם בוצעה באופן לגיטימי על ידי גורמים מורשים בארגון.
5. [עדכון] מומלץ לבדוק אם במערכותיכם קיימת משימה מתוזמנת בשם VerifiedPublisherCertStoreVerify, בנתיב \Microsoft\Windows\AppID\.

אם זוהתה משימה מתוזמנת זו, מומלץ למחקה מרשימת המשימות המתוזמנות. **תשומת לב – משימה זו שונה ממשימה בשם VerifiedPublisherCertStoreCheck שהיא משימה של מערכת ההפעלה, אותה אין למחוק.**

6. [עדכון] מומלץ לבדוק אם במערכותיכם קיימת משימה מתוזמנת בשם ResolutionServer, בנתיב \Microsoft\Windows\WDI\.

אם זוהתה משימה מתוזמנת זו, מומלץ למחקה מרשימת המשימות המתוזמנות. **תשומת לב – משימה זו שונה ממשימה בשם ResolutionHost שהיא משימה של מערכת ההפעלה, אותה אין למחוק.**

7. [עדכון] אם קיים חשד שעמדה הותקפה, מומלץ לבדוק את ה-Properties של הקובץ c:\windows\system32\sethc.exe, ולוודא כי בשדה File description מופיע התיאור Accessibility shortcut keys.
8. באם אחד או יותר מהמזהים המצורפים מזוהים במערכותיכם, נבקש לפנות מיידית למערך הסייבר הלאומי.
9. מערך הסייבר הלאומי יצר שאלון המיועד לספקים, ונועד לאפשר לארגונים הערכה של הסיכונים והבנה של רמת ההגנה של הספק ובמקביל, לאפשר לספקים להבין את הדרישות והבקרות הנדרשות על מנת לעמוד ברמת הגנה נאותה. את השאלון ניתן למצוא בקישור https://www.gov.il/he/departments/news/querysupply.

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.