22 ספטמבר 2020
ד' תשרי תשפ"א
סימוכין:ב-ס-1161

# קמפיין תקיפה כנגד יעדים בישראל באמצעות שרשרת אספקה

## תקציר

במהלך הימים האחרונים חשף מערך הסייבר הלאומי ניסיונות לתקיפת סייבר כנגד ארגונים בישראל ללא גרימת נזק. ניסיונות התקיפה בוצעו באמצעות שרשרת האספקה של אותם הארגונים או התכתבויות עבר מול לקוחות.
קמפיין התקיפה בעל מאפיינים הדומים לקמפיינים שבוצעו בעבר, ומטרתו היא השגת נגישות למספר רב של ארגונים בישראל.
מסמך זה יתאר את הקמפיין, ודרכי התמודדות מומלצות.

## פרטים

<u>שלב התקיפה הראשון - פריצה לחברות בשרשרת האספקה</u>

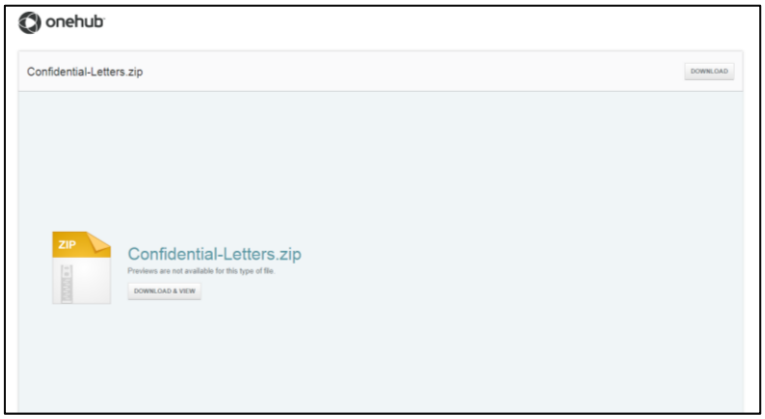
1. בשלב התקיפה הראשון הושגה גישה לשרתי הדוא"ל של מספר ארגונים.
2. וקטורי התקיפה הראשוניים היו שרתי **VPN** או **OWA** שלא עודכנו בזמן עם עדכוני אבטחה קריטיים (CVE-2020-0688, CVE-2018-13379), ושרתי **OWA** שהותקפו באמצעות נתוני משתמש שהושגו מראש בדרך שעדיין לא זוהתה.
3. וקטורים אלו שימשו להשגת אחיזה ראשונית ברשת, גם בארגונים בהם לא בוצע השלב השני של התקיפה.
4. לשימור האחיזה בשרתים, נעשה שימוש ב-**Webshells**.

5. שירותי ה-VPN שימשו את התוקפים להשגת נגישות לשרתי הדוא"ל הארגוניים.
6. <u>שלב התקיפה השני - הפצה והתפשטות באמצעות הדוא"ל</u>
   1. ההודעות שנשלחו כללו שימוש בכתובות שולח אשר אמורות להיות מוכרות לנמענים, וכן שימוש בגרסאות זדוניות של תכתובות עבר בין הנמענים לארגון השולח.

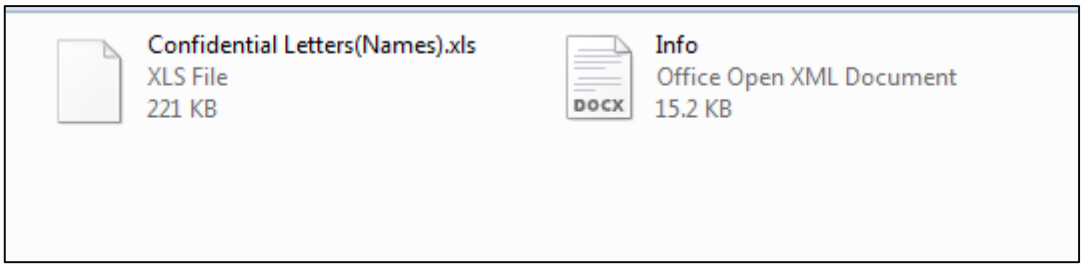
### דוג' למתווה הודעות

7. מתווה ההודעות הראשון כלל קישורים שהוטמעו בהודעה, באופן שגרם להם להיראות כאילו מדובר בצרופה בשם Confidential-Letters.zip.

8. לחיצה על הקישור העבירה את המשתמש לדף באתר בשם ws.onehub[.]com, הכולל קישור להורדת קובץ בשם דומה.




9. קובץ זה הכיל 2 קבצים: Confidential Letters(Names).xls ו-Info.docx.




10. קובץ ה-DOCX מיועד לשלוח מידע לאתר בשם canarytokens[.]com, על מנת לעדכן שהקובץ נפתח על ידי הנמען.
11. קובץ ה-XLS כולל מאקרו מעורפלים (Obfuscated) אשר יוצרים 3 קבצים ו-2 משימות מתוזמנות, אשר מטרתן יצירה ושימור אחיזה בעמדת הקצה.

### מתווה הודעות שני

12. הודעות זדוניות אחרות שנשלחו במהלך הקמפיין מכילות קישורים ל-2 URL אחרים באתר ws.onehub[.]com:
    1. הקישור הראשון מוביל לקובץ RAR המכיל קובץ בשם File.Pdf.exe.
    2. הקישור השני מוביל לקובץ RAR המכיל קובץ בשם report.pdf.exe וקובץ DOCX בעברית.
    3. קובץ ה-DOCX מיועד לשלוח מידע לאתר בשם canarytokens[.]com, על מנת לעדכן שהקובץ נפתח על ידי הנמען.
    4. הקבצים בעלי סיומות pdf.exe, לאחר פתיחתם, מציגים מסמך דמה, וברקע פונים לשרת C2 של התוקף בכתובת hXXps://185.183.98[.]242/default.php.

## דרכי התמודדות

1. להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם במערכות הארגוניות הרלוונטיות.
2. מומלץ לוודא מול גופים בשרשרת האספקה של הארגון כי שרתי VPN ו-OWA עודכנו בזמן עם עדכוני אבטחה קריטיים (CVE-2020-0688, CVE-2018-13379), וקיימת מדיניות להתקנה עיתית של עדכוני אבטחה.

3. מומלץ לתכנן וליישם פרוטוקול התקנת עדכוני אבטחה קפדני, בפרט לשרתים החשופים לאינטרנט או משמשים לגישה מאובטחת לארגון.
4. מומלץ לבחון אמצעים לזיהוי התקנה של תוכנות לא מורשות בעמדות עבודה ושרתים, ובפרט כאלו הנגישות לאינטרנט.
5. מומלץ לוודא כי מנועי AV המותקנים על שרתי Web, ובפרט שרתי OWA, סורקים גם קבצי ASPX, העלולים לשמש תוקפים להתקנת Webshells. מומלץ לבחון המלצה זו בסביבת ניסוי טרם הטמעה בסביבת ייצור.
6. מומלץ לפתוח קבצי Office שמקורם באינטרנט רק כאשר מאקרו מנוטרלים ותחת "Protected View". כל הנחיה בקובץ המבקשת לנטרל אמצעי אבטחה אלו צריכה להיחשב כמחשידה, ולגרום להעברת הקובץ לטיפול גורמי אבטחת מידע ארגוניים.
7. מומלץ כי קבצים המורשים להיכנס לרשת הארגונית בכל צורה שהיא, ובפרט קבצים המצורפים להודעות דוא"ל או מורדים מרשת האינטרנט, יוגבלו לאוסף המינימלי של סוגי קבצים הנדרשים לקיום הפעילות העסקית בארגון. קבצים מסוגים מורשים מומלץ לבחון במנועי AV ו-CDR (Content Disarm and Reconstruction), טרם הכנסתם לרשת הארגונית. קבצים מסוגים אחרים, מומלץ למנוע כניסתם או לשומרם בהסגר עד לבדיקה בידי גורמי אבטחת מידע ארגוניים. באופן דומה, גם קבצים היוצאים מהארגון מומלץ לבדוק באמצעות AV ו-CDR.
8. מומלץ להזכיר לעובדי הארגון שלא לפתוח צרופות או להפעיל קישורים המגיעים מגורמים לא מוכרים, או אף מגורמים מוכרים - אם ההודעה הגיעה באופן שאינו צפוי או נראית חריגה בכל אופן שהוא (כדוגמת קישורים המופיעים כצרופה).
9. מומלץ כי גישה לשרתי OWA תתאפשר באמצעות שימוש ב-VPN עם הזדהות חזקה (2 Factor Authentication).
10. מומלץ לבחון ולהטמיע שימוש בהזדהות חזקה בכל המערכות הארגוניות התומכות בכך.
11. מומלץ לבחון דרכים לזיהוי יצירת משימות מתוזמנות חדשות בעמדות, לדוגמה באמצעות שימוש ב-Sysmon ומשלוח הלוגים לאיסוף מרכזי וניטור.

12. מומלץ לבחון אמצעים להגבלת הרצת תוכנות וסקריפטים (Application Whitelisting) על עמדות עבודה ושרתים בארגון. יש לבחון אמצעי זה בסביבת ניסוי טרם הטמעה בסביבת ייצור.

לכל מידע נוסף ניתן לפנות אלינו. במידה שעלו ממצאים בבדיקתכם, נבקש לקבל היזון חוזר.

## מקורות

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.

בברכה,
CERT-IL