14 בספטמבר 2021
ח' בתשרי תשפ"ב
סימוכין: ב-ס-1377

# פעילות קבוצת תקיפה במרחב הסייבר הישראלי

## תקציר

1. מטרת מסמך זה להתריע על פעילותה של קבוצת תקיפה למול גופים וארגונים במרחב האינטרנט הישראלי.
2. המסמך כולל פירוט של כלים ושיטות פעולה מוכרות של הקבוצה, וכן המלצות למניעה וזיהוי של פעולות אלו.
3. להתרעה זו מצורף קובץ מזהים אותם מומלץ לנטר במערכות הארגוניות הרלוונטיות.

## פרטים

1. בחודשים האחרונים פועלת קבוצת תקיפה משמעותית כנגד עשרות יעדים במרחב הישראלי.
2. תכלית הפעילות העיקרית של הקבוצה הינה תקיפה לצורך איסוף מידע ( CNE – Computer Network Exploitation) מארגונים במנעד רחב של מגזרים, בהם מגזרי האנרגיה, תחבורה, שילוח, לוגיסטיקה, IT וממשל.
3. מסמך זה סוקר את שיטות הפעולה, הטכניקות והטקטיקות ( TTPs - Tactics, techniques and procedures) בהן משתמשת הקבוצה, לצד המלצות לדרכי התמודדות, ומטרתו לאפשר לארגונים במשק לאתר תקיפות עבר ולהתמגן מפני תקיפות עתידיות בשיטות דומות.
4. המידע במסמך מתבסס על עיבוד והיתוך ממצאים שעלו מחקירות רבות שביצע מערך הסייבר הלאומי בארגונים אשר נתקפו ע"י הקבוצה, וכן ממידע שנאסף ממקורות שונים של המערך וקהיליית ההגנה בישראל.

**<u>מיפוי TTPs</u>**

1. תשתיות מבצעיות
    1. עיקר פעילותה של הקבוצה מתבצע משרתים ייעודיים – רובם שייכים לספקיות אמריקאיות וממוקמים בין היתר בארה"ב, בריטניה, ישראל ומדינות נוספות.
    2. חלק מהפעילויות מתבצעות באמצעות שרתים משתנים הפועלים תחת שירותי VPN מסחריים.
2. חדירה אל היעד
    1. קבוצת התקיפה משתמשת בשיטות שונות לטובת השגת נגישות ראשונית לגופים הנתקפים –
        1. סריקות וניצול חולשות בשרתים ארגוניים החשופים לפגיעויות – Exchange, VPN ועוד.
        2. התפרצות לחשבונות Office 365.
        3. התפרצות לשרתים באמצעות SQLi (SQL Injection).
        4. חדירה מבוססת שרשרת אספקה בין-ארגונית – ניצול חיבוריות רשתית ו/או אפליקטיבית בין גופים לטובת דילוג בין רשתות (לדוגמה, על בסיס תוכנות שליטה מרחוק דוגמת RDP או חיבורי VPN תוך שימוש בנתוני אימות לגיטימיים אשר נלקחו מהארגון המשיק)
3. שימור אחיזה ביעד
    1. RunTimeBroker –
        1. כלי Backdoor ייעודי של הקבוצה מבוסס .NET. .
        2. לשם התממה והערמת קושי בזיהוי, שם הקובץ זהה לקובץ לגיטימי של מערכת ההפעלה הנמצא בנתיב C:\winodws\system32.
        3. זוהה שימוש חוזר בשמות מותממים כגון svchost ו-msupdate ובן התקנה של הכלי בתיקיה c:\windows\microsoft.net\framework64\v4.0.30319. (תיקיה המשמשת להתקנת .NET)

4. הכלי בדרך כלל משתמש בשירות DropBox (Api.dropbox.com ו-content.dropboxapi.com) לצורך קבלת פיקודים, שינוע קבצים והזלגת תוצרים מהנתקף.
5. זוהה שימוש בכלי Winrar לטובת דחיסת קבצים טרם הזלגתם לשרתי התוקף.
6. הכלי מתקין Service בשם "Network host detection" לשם שימור אחיזה בעמדה המותקפת (persistence).

2. Webshells – הקבוצה משתמשת בכלי Webshell ייעודיים ופומביים לטובת שימור אחיזה בשרתי Web בארגונים הנתקפים.

4. כלים המשמשים את הקבוצה לביצוע תנועה רוחבית ברשת – לעיתים מותקנים בתיקיה הלגיטימית c:\windows\tapi.

1. PAexec –כלי פומבי המאפשר להריץ תוכנות על שרתים מרוחקים בעלי מערכת הפעלה Windows.
2. Mimikatz - כלי המשמש לאיסוף נתוני גישה של משתמשים מהעמדות המותקפות, על מנת לאפשר תנועה רוחבית והעלאת הרשאות.
3. Procdump - כלי המבצע Dump לתהליכים, בפרט לתהליך lsass.exe לטובת איסוף נתוני גישה של משתמשים מהזיכרון של תהליך זה, על מנת לאפשר לתוקף תנועה רוחבית והעלאת הרשאות.
1. נציין כי לעיתים התוקף משנה את ערך ה-UserLogonCredential (תחת הערך של Wdigest ב-registry) מ-0 ל-1 ורק לאחר זמן מה מבצע את פעולות ה-dump.

## דרכי התמודדות

1. המלצות ממוקדות לזיהוי פעילות של קבוצת התקיפה המתוארת לעיל:
1. התרעה זו כוללת קובץ מזהים עדכני אותם מומלץ לנטר בכל מערכות האבטחה הארגוניות הרלוונטיות (EDR, SIEM, CDR, AV, מערכות הלבנה, מערכות סינון דוא"ל) באופן הדוק ככל האפשר.

2. מומלץ לבדוק האם מזהים אלו נצפו במערכות הרלוונטיות בחצי השנה האחרונה, וכן מומלץ מאד לבצע סריקה אקטיבית לאיתור מזהי קבצים באופן ישיר או באמצעות הזנתם למערכות AV/EDR.
3. נבקש לעדכן את מערך הסייבר הלאומי במקרה של זיהוי אחד או יותר ממזהים אלו או משיטות הפעולה שפורטו לעיל במערכותיכם.
4. מומלץ לבדוק האם קיים שירות (service) בשם Network host detection service והאם הוא מריץ קובץ שמקורו בנתיב שצוין מעלה (סעיף 3.1.3 תחת "מיפוי TTPs" לעיל).
    1. אם קיים service זה – מומלץ לעצור פעולתו ולהסירו וכן למחוק את הקובץ שהוא מריץ (בסבירות גבוהה זהו הכלי runtimebroker).
5. מומלץ לבדוק האם ערך ה-UserLogonCredential ב-registry השתנה מ-0 ל-1.
    1. אם התשובה חיובית - מומלץ להחזיר את הערך המקורי תוך החלפת והקשחת הסיסמאות של כל המשתמשים באותו השרת.
6. מומלץ לבדוק האם קיימים קבצים וכלים אשר צוינו בסעיף "פרטים" לעיל, בתיקיית c:\windows\tapi (כגון paexec, procdump, rar וכן קבצי פלט של procdump או לחילופין כלי ה-runtimebroker בשם אחר).
7. אם קיים חשד להימצאות הכלי, מומלץ באופן זמני לבצע חסימה ב-firewall/proxy לתעבורה ל-dropbox עד להסרתו.
8. אם הארגון אינו עושה שימוש בשירותי dropbox, ניתן לאתר תחנות חשודות כנתקפות על בסיס תעבורת תקשורת לשירות זה.
9. אם הארגון אינו עושה שימוש בכלי paexec, ניתן לאתר שימוש בו על-ידי בדיקת קיום של קובץ בנתיב %systemroot%\PAExec-<random_number>-<source_hostname>.

2. המלצות כלליות
    1. מומלץ להקפיד על התקנה של עדכונים עבור מערכות ההפעלה, התוכנות והקושחות בשימוש הארגון, תוך זמן קצר ככל האפשר מרגע הפצתן ע"י היצרן.

2. מומלץ לבצע סקר עיתי של מערכות ההגנה הארגוניות, על מנת לוודא שפעולתן תואמת את המדיניות הארגונית הרלוונטית.
3. מומלץ להקפיד על סגמנטציה רשתית ובידול של שרתי ותשתיות הניהול, והגבלת הגישה אליהם לעמדות ייעודיות בלבד.
4. מומלץ להתקין Firewall מקומי על שרתי הניהול ולהגביל את הגישה אליהם לעמדות ייעודיות ופרוטוקולים נחוצים בלבד.
5. מומלץ לצמצם למינימום את מספר המנהלנים ברשת הארגונית, ולהקשיח את השימוש בחשבונות אלו באמצעות הגדרת שימוש בהזדהות חזקה דו-שלבית (MFA), מניעת או הגבלת שימוש מחוץ לרשת הארגונית, ורישום לוג מלא של פעילות המנהלן, לרבות פעולות להתקנת תוכנה.
6. מומלץ לצמצם למינימום את מספר הספקים הנדרשים לגישה לרשת הארגונית ולהקשיח את התנאים לביצוע הגישה: שימוש בהזדהות חזקה דו-שלבית (MFA), שימוש בציוד ארגוני, עבודה על פי דרישה (On Demand) ופיקוח או הקלטה של הפעילות.
7. מומלץ להגדיר החלפת סיסמאות תכופה (מנהלנים ומשתמשים, לרבות אפליקטיביים) ושימוש בהזדהות חזקה דו-שלבית (MFA) באופן הרחב ביותר האפשרי.

3. פעולות מניעה של חדירה "אל היעד"
   1. VPN
      1. מומלץ מאד לבחון ולעדכן בהקדם האפשרי את גרסת המוצר בשימוש ארגונכם לגרסה העדכנית ביותר הנתמכת בציוד. שימוש בציוד VPN שאינו עדכני עלול לאפשר לתוקף וקטור לתקיפה ישירה של הרשת הארגונית.
      2. לאחר העדכון, מומלץ מאד לאתחל את סיסמאות הגישה של כלל המשתמשים בציוד.
      3. מומלץ להשתמש בהזדהות חזקה (Multi Factor Authentication) עבור גישה באמצעות VPN לרשת הארגונית.

4. מומלץ לבחון האפשרות למניעת חיבור אל הארגון מכתובות המזוהות עם שירותי VPN ציבוריים.

2. Exchange

1. מומלץ לוודא כי השרת מעודכן לגרסאות העדכניות ביותר. משתמשי OWA, מומלץ למנוע גישה ישירה לשירות מרשת האינטרנט ולאפשר גישה באמצעות שירות כגון VPN עם הצפנה והזדהות חזקה מתאימה.

3. Office365

1. ראו פרסומי מערך הסייבר הלאומי בנושא תקיפות במתווה זה:

1. https://www.gov.il/he/departments/publications/reports/cloud_1269
2. https://www.gov.il/he/departments/publications/reports/auto_mach_abuse
3. https://www.gov.il/he/departments/publications/reports/saml

4. מניעה וזיהוי של שימוש ב-Webshells:

1. ראו מסמך ה-NSA בנדון בקישור:

1. https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF
2. https://github.com/nsacyber/Mitigating-Web-Shells

5. מניעת/עיכוב סריקה מקדימה של הארגון:

1. מומלץ לאפשר גישה מרשת האינטרנט בפורטים ההכרחיים לפעילות העסקית של הארגון בלבד, ולכתובות הנדרשות לגישה זו בלבד. מומלץ להגדיר מניעת גישה בשאר הפורטים, ולהעדיף שימוש בחוקי Drop על פני חוקי Reject.

4. הגנה רשתית

1. טיוב חוקת Firewall - מומלץ לטייב את החוקה ולהימנע מהצירופים הבאים:
    1. Any in 3/2 Fields
    2. Any in Destination
    3. Risky Ports
    4. Any in Service
    5. Bidirectional Rules
    6. Disabled Rules
    7. מומלץ ליישם סגמנטציה ובקרת תעבורה לכל הפחות בין רשת שרתים, תמיכה וניהול, ומשתמשים. מומלץ לבחון אפשרות למנוע תעבורה בין תחנות קצה ולאפשר תעבורה מתחנות קצה לשרתים ושירותים ארגוניים בלבד. **מומלץ לבחון שינוי זה בסביבת ניסוי טרם הטמעה בסביבת ייצור.**
5. פעולות מניעה "על היעד"
    1. תחנה / שרת / אמצעי ברשת הארגונית:
        1. מומלץ לנטר התחברות ראשונה של משתמש חדש בתחנה.
        2. מומלץ לוודא הפעלת מוצר AV/Anti-Malware עדכני בתחנות ובשרתים.
        3. מומלץ להקשיח את מערכות ההפעלה של תחנות העבודה, השרתים וציוד התקשורת לפי הנחיות יצרן. מומלץ לוודא שלא הופעלו שירותים (Services) שאינם נחוצים.
        4. מומלץ לנטרל הרצת PowerShell/CMD בתחנות של משתמשי קצה, שאינם משתמשים בו באופן יומיומי ואינם זקוקים לו לביצוע עבודתם.
        5. מומלץ ליישם פתרונות מתקדמים בתחנות קצה של משתמשים המהווים סיכון גבוה למימוש תקיפה, כגון קיבוע תצורה, הרצת קוד חתום בלבד, עבודה בתצורת Read Only בלבד וכיו"ב.
        6. מומלץ להטמיע פתרון כגון LAPS – Local Administration Password Solution, לצמצום הסיכון של שימוש בהרשאות Local Admin. מומלץ להסיר הרשאות Local Admin שאינן נחוצות עסקית מתחנות קצה ושרתים. מידע נוסף לגבי Local Admin Password Solution (LAPS):

1. https://adsecurity.org/?p=3164
7. מומלץ לנטר התקנת/הפעלת Service בשם המוזכר בסעיף 3.1.5, בכל עמדות העבודה והשרתים הארגוניים.
8. כלים לשיטות למניעת תקיפה מסוג SQL Injection ניתן למצוא בפרסום של OWASP:
    1. https://owasp.org/www-community/attacks/SQL_Injection
9. מומלץ לנטר פעילות מרשת הארגון לאתרים של Dropbox על מנת לזהות פעילות חריגה בהיקפה או בזמן ביצועה. אם ארגונכם אינו עושה שימוש באתר זה, מומלץ לבחון חסימת הגישה אליו.
10. מומלץ לנטר הפעלה ממוכנת של תוכנת Winrar בעמדות הארגוניות, בפרט אם תוכנה זו אינה חלק מערכת ההתקנה הסטנדרטית בעמדות אלו. אם ארגונכם יכול ליישם פתרון מסוג Application Whitelisting, לפחות בעמדות מנהלנים, מומלץ לבחון זאת.

6. פעולות לגיבוי ושחזור
1. מומלץ לוודא ביצוע יומיומי של גיבוי מידע בעל חשיבות ארגונית ועסקית. ביצוע הגיבוי נועד לאפשר שחזור מהיר של מידע בשעת הצורך (אם המידע ימחק/יוצפן או ישובש).
2. מומלץ לוודא שמירה של הגיבוי על מדיה נפרדת, במיקום נפרד ומאובטח. כלל, מומלץ לבצע גיבוי במספר ערוצים במקביל (שירותי ענן, שרתי גיבוי, קלטות וכד').
3. אם אחסון הגיבוי מבוסס ענן מבוצע באמצעות שירותים מקוונים המאחסנים את הקבצים ע"ב האינטרנט, חשוב לוודא כי השרות מספק הצפנת נתונים ואימות רב שלבי (MFA).
4. מומלץ לבצע גיבויי תצורה לרכיבי תשתית ותקשורת (דוגמת נתבים, Firewall, מערכות אבטחה ועוד).
5. מומלץ לוודא קיום וריענון של תכנית אירגונית להתאוששות מאירוע סייבר.

6. מומלץ לוודא עדכניות נוהל התאוששות ושחזור לגרסה תקינה בעת הצורך. מומלץ לבצע בדיקות עיתיות ולוודא שהשחזור תקין.
7. מומלץ לבחון התקנת Sysmon לניטור פעילות חשודה, איסוף המידע לשרת לוגים מרכזי, וקביעת דרכי תגובה במקרה של זיהוי פעילות חשודה.
8. מומלץ להגדיר נעילת מסך בעמדות קצה ושרתים לאחר פרק זמן של חוסר פעילות:

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-machine-inactivity-limit

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.