19 בנובמבר 2023
ו' בכסלו תשפ"ד
סימוכין: ב-ס-1662

# פעילות כופרה במרחב הסייבר הישראלי

## תקציר

1. לאחרונה דווחו למערך הסייבר הלאומי אירועי תקיפות כופרה כנגד יעדים בישראל.
2. מטרת מסמך זה, הכרת שיטות הפעולה הנפוצות למימוש תקיפות כופרה, ודרכי התמודדות מולן.

## פרטים

1. האירועים מדווחים על רקע מלחמת "חרבות ברזל" ופעילות תוקפים מוטים פוליטית (hacktivists).
2. תקיפות כופרה מהוות חלק עיקרי מתקיפות שהמוטיבציה בבסיסן היא כלכלית. תקיפות מסוג זה עלולות לגרום לנזק רב לארגונים על ידי הצפנה ו/או הדלפת מידע שנגנב מהארגון, בדרישה לקבלת סכומי כסף גבוהים.
3. בשנים האחרונות, אנו מזהים מספר הולך וגדל של גורמים המבצעים תקיפות כופרה, כאשר שיטות הפעולה שלהם שונות ומבדילות ביניהם. עם זאת, מזוהה שימוש הולך וגובר בגישת כופרה כשירות (Ransomware as a Service), עובדה המאפשרת לגורמים פחות מנוסים לבצע תקיפות משמעותיות, תוך הסתמכות על פעילות מקדימה של גורמים מנוסים יותר.
4. בהמשך מסמך זה מתוארים טקטיקות, טכניקות ותהליכים (TTPs) מסוימים אשר עלולים להצביע על תקיפות כופרה בהתהוות. פעילויות אלו מהוות מכנה משותף בין גורמים רבים המבצעים תקיפות כופרה על פי מתווים מוכרים.
5. קיימות מספר שיטות מוכרות המשמשות תוקפים כוקטור תקיפה ראשוני להשגת אחיזה ברשת הארגון הנתקף. מפורטות להלן השיטות הנפוצות ביותר.

**6. ניצול ממשקי גישה מרחוק**

1. תוקפים רבים משתמשים בממשקי גישה מרחוק כוקטור תקיפה מועדף לרשת הנתקפת, לרוב על ידי מימוש פגיעות ספציפית ומוכרת בציוד הגישה מרחוק, או באמצעות שימוש בנתוני גישה לגיטימיים שהושגו בדרכים שונות: דלף, גניבה, קניה ברשת האפלה, או

ביצוע תקיפת Brute Force, Dictionary Attack או Password Spraying (שיטות לתקיפת נתוני הזדהות של משתמשים לגיטימיים).

7. **תקיפה ממצה (Brute Force Attack)** – תקיפה המנסה את כל צירופי הסיסמה האפשריים, באמצעות תוכנות ייעודיות, עד למציאת פרטי ההזדהות הנכונים. לרוב התקיפה תתבצע כנגד חשבונות הזדהות לציוד VPN או חשבונות לקישור מסוג RDP ודומיו, לשם השגת נגישות לציוד ה-VPN ודרכו לרשת הארגונית, או נגישות ישירה לעמדה עליה מותקנת תוכנה מסוג RDP או תוכנה אחרת לגישה מרחוק.
8. **דיוג או דיוג ממוקד**
   1. קמפייני דיוג – שליחת הודעות בצורה רחבה (דיוג) או ממוקדת במספר מצומצם של נתקפים פוטנציאליים (דיוג ממוקד), לצורך השגת פרטי גישה למערכות ארגוניות או פרטיות, בסיוע טכניקות של הנדסה חברתית ושיטוי בנתקף. ניסיון התקיפה יכול להתבצע באמצעות קישור או צרופה המצורף להודעה מטעם התוקף. ההודעה יכולה להיות הודעת דוא"ל, SMS, וואטסאפ, או כל רשת חברתית בשימוש הנתקף.
9. **ניצול פגיעויות מוכרות או חדשות (Zero Day)**
   1. אחד מוקטורי התקיפה הנפוצים ביותר הוא באמצעות ניצול פגיעויות מוכרות או חדשות במוצרים שונים. תקיפה מסוג זה יכולה להתבצע ישירות כנגד שירותים המוחצנים ונגישים מרשת האינטרנט, כגון ציוד VPN, שרתי EMAIL או WEB וכד', או להתבצע באמצעות צרופה המצורפת להודעה כלשהי, שפתיחתה תפעיל את הפגיעות בתוכנה הרלוונטית.

## דרכי התמודדות

1. **ניצול ממשקי גישה מרחוק**
   1. **הגבלת גישה** – הגדרת רשימה סגורה של משתמשים המורשים להשתמש בשירותי גישה מרחוק ישירות לעמדה ברשת הארגונית (RDP ותוכנות דומות). הגדרת כתובות ספציפיות המורשות לגישה מרחוק, או שימוש ב-VPN עם הצפנה והזדהות חזקה מתאימה.
   2. **הפעלת MFA (Multi-Factor Authentication)** – שימוש במספר סוגים של מגנוני זיהוי (2 לפחות) ולא במנגנון זיהוי הכולל שם משתמש וסיסמה בלבד.

3. **יצירת סיסמאות מורכבות –** שימוש בסיסמאות ארוכות ומורכבות (לפחות 12 תווים, מספר קבוצות שונות – אותיות קטנות וגדולות, מספרים ותווים מיוחדים), מגדיל את מרחב הסיסמאות הנדרש לתקיפה במתקפת Brute Force, ומקטין מאד הסיכויים להצלחתה.
4. **הגבלת מספר הכתובות המורשות לגישה בו-זמנית –** הגדרת מערכות האבטחה כך שכל משתמש מרוחק יכול להתחבר לרשת או לנקודת הקצה מכתובת אחת בלבד בכל רגע נתון.
5. **זיהוי דילוג בין כתובות רשת שאינו אפשרי מבחינה פיזית –** שימוש ביכולות Geolocation על מנת לזהות קישורים בלתי אפשריים, כגון משתמש המתקשר מכתובת מישראל ולאחר שעה מכתובת בארה"ב.

**2. דיוג או דיוג ממוקד**

1. **בדיקת מקור ההודעה** – כאשר מתקבלת הודעה הכוללת צרופה או קישור, והגעתה לא הייתה צפויה, גם אם השולח מוכר, יש לוודא מול השולח באמצעות ערוץ תקשורת שונה אם אכן שלח אותה. אם מתקבלת תשובה שלילית יש להעבירה לבדיקה בידי הגורמים המוסמכים לכך בארגון.
2. **מניעת ניצול על ידי הפעלת קישורים** – מעבר להעלאת מודעות המשתמשים לשימוש של תוקפים בהודעות שונות עם צרופות או קישורים, יש להנחותם לא להפעיל קישורים אלו אלא תמיד להעדיף גישה עצמאית אל האתר הרלוונטי באמצעות חיפוש עצמאי או שימוש במועדפים. מומלץ להיעזר במערכות סינון גלישה המונעות גישה לאתרים בעלי מוניטין מפוקפק.
3. **פתיחת והפעלת צרופות** – מומלץ לוודא כי מערכות האבטחה הארגוניות מונעות שימוש בקבצים בעלי סיומות כפולות, או כאלו בהם הסיומת אינה תואמת את תוכן הקובץ. מומלץ להגביל סוגי הקבצים הניתנים להכנסה לארגון למינימום הנדרש לצורך פעילותו השוטפת, ובפרט לא לאפשר כל סוג של קבצי הרצה כצרופות. מומלץ להפעיל ב-Office את מצב Protected View, ולחשוד בכל קובץ הכולל מסר המנסה לשכנע את המשתמש לבטלו או להפעיל מצב של Enable Content. בתוכנות להצגת PDF מומלץ לנטרל השימוש ב-JavaScript. כפי שצוין עבור קישורים, יש להימנע מפתיחת צרופות גם אם הגיעו ממקור מוכר, אך מועד הגעתן או התוכן אינו צפוי.

### 3. ניצול פגיעויות מוכרות או חדשות (Zero Day)

1. **עדכון גרסאות תוכנה** – יש לוודא באופן עיתי כי כל התוכנות בשימוש הארגון, ובפרט תוכנות ורכיבים המותקנים על גבי שרתים הנגישים מרשת האינטרנט, מעודכנים בכל עדכוני האבטחה הרלוונטיים שהופצו על ידי היצרן. עבור עדכוני אבטחה קריטיים יש לוודא קיום ותרגול נוהל המחייב בחינתם והתקנתם תוך פרק זמן סביר מפרסומם. יצרנים רבים מאפשרים רישום לרשימות תפוצה בדוא"ל המאפשרות קבלת מידע עדכני על עדכוני אבטחה במוצריהם.
2. הפגיעויות הבאות נמצאות בשימוש בחודשים האחרונים על ידי גורמים זדוניים ועלולות לשמש לתקיפות כופרה:

| מוצר | יצרן | CVE |
|---|---|---|
| IOX XE | Cisco | CVE-2023-20273<br>CVE-2023-20198 |
| ASA, FTD | Cisco | CVE-2023-20269 |
| Expressway Series, VCS | Cisco | CVE-2023-20209 |
| Catalyst SD-WAN Manager | Cisco | CVE-2023-20252 |
| NetScaler ADC<br>NetScaler Gateway | Citrix | CVE-2023-3519<br>CVE-2023-4966<br>CVE-2023-4967 |
| SharePoint | Microsoft | CVE-2023-29357 |
| Webmail | Roundcube | CVE-2023-5631<br>CVE-2020-35730<br>CVE-2020-12641<br>CVE-2021-44026 |
| Tomcat | Apache | CVE-2023-41080 |
| ActiveMQ | Apache | CVE-2023-46604 |
| SSL-VPN | Fortinet | CVE-2023-27997 |

| | | |
|---|---|---|
| vCenter | VMware | CVE-2023-34048 |
| WS_FTP | Progress | CVE-2023-40044<br>CVE-2023-42657 |
| Deep Discovery Inspector<br>Apex One<br>Worry-Free Business Security | Trend Micro | CVE-2023-3823<br>CVE-2023-3824<br>CVE-2023-41179 |
| FortiProxy<br>FortiOS<br>FortiWeb | Fortinet | CVE-2023-29183<br>CVE-2023-34984 |
| ESG | Barracuda | CVE-2023-2868 |
| Avalanche, Sentry | Ivanti | CVE-2023-32560<br>CVE-2023-38035 |

## 4. דיווח למערך הסייבר הלאומי

1. אם קיים חשש לפעילות זדונית ברשת הארגון, מומלץ לדווח למוקד 119 של מערך הסייבר הלאומי, הפעיל 24/7.
2. פרטו ככל האפשר את הממצאים שזוהו. ככל שמזהים פעילות זדונית בשלב מוקדם יותר ניתן להתמודד עימה טוב יותר, ועשויים למנוע ביצוע בפועל של תקיפות כופרה או תקיפות אחרות.
3. דיווח למוקד 119 מאפשר למערך לסייע הן לכם, והן לכלל המשתמשים במרחב הסייבר הישראלי, באמצעות זיהוי מגמות ושיטות תקיפה ופרסום המידע לגביהן בערוצים השונים.

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.