PowerShell Script משמש למימוש פוגען מסוג Wiper

07/04/2026
כ' ניסן תשפ"ו

[תקציר]

1. לאחרונה דווח למערך הסייבר הלאומי על תקיפה העושה שימוש בסקריפטים הכתובים ב-PowerShell למימוש מחיקה של עמדות קצה ושרתים (Wiper).
2. מטרת מסמך זה, היכרות עם האיום שמהווה שימוש בלתי מוגבל או בלתי מנוטר ב-PowerShell לרשת הארגונית, והיכרות עם שיטות הגנה שונות.

[פעולות מידיות לביצוע]

- להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם בכל מערכות האבטחה הארגוניות הרלוונטיות.
- מומלץ לכל ארגון לשקול אלו שיטות להגבלת גישה וניטור של פעילות PowerShell מתאימות עבורו, ולבחון אותן בסביבת ניסוי טרם הטמעה בסביבת ייצור.

[פרטים]

1. PowerShell הינו כלי ייחודי, וחיוני בסל הכלים של מנהלי מערכת, מנהלנים, ומשתמשים מתקדמים.
2. עם זאת, מדובר בכלי בעל יכולות גבוהות מאד להתממשק למגוון מערכות ארגוניות, העלול לשמש כאמצעי לתקיפה מסוג Living of the Land, שבה התוקפים מנצלים כלי מערכת/ניהול לגיטימיים למימוש התקיפה.

[דרכי התמודדות]

1. להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם בכל מערכות האבטחה הארגוניות הרלוונטיות.
2. מערך הסייבר הלאומי פרסם כבר בשנת 2017 מסמך העוסק בהגבלת וניטור פעילות PowerShell בארגונים. ראו קישור מס' 1.
3. להלן מספר דרכים להגבלת השימוש ב-PowerShell. (ניתן למצוא מידע נוסף בקישור מס' 2 ובמקורות המצוינים בו):
    1. מדיניות ביצוע (PowerShell Execution Policies)
        1. הגדרות מסוג "AllSigned" או "RemoteSigned" נועדו למנוע הרצת סקריפטים בטעות, אך ניתן לעוקפן בקלות באמצעות שימוש בהגדרה "-ExecutionPolicy Bypass".
    2. חסימת נתיבים באמצעות SRP (Software Restriction Policies)
        1. ניתן לחסום את הקבצים "powershell.exe" ו-"powershell_ise.exe" לפי נתיב או Hash. יש להקפיד על מתן הרשאות גישה לקבוצות המשתמשים שנדרשות לשימוש ב-PowerShell לצורך ביצוע תפקידן.
    3. AppLocker/WDAC ו- Constrained Language Mode
        1. באמצעות אכיפה של AppLocker או WDAC, PowerShell עובר למצב Constrained Language Mode (CLM) עבור סקריפטים שאינם מזוהים

כמהימנים. הגדרה זו עשויה לסייע מאד בחסימת כלי תקיפה המסתמכים על אובייקטים של .NET או גישת COM.

4. ניהול הרשאות מוגדרות (Just Enough Administration - JEA)
   1. JEA מאפשר להגדיר למשתמשים נקודות קצה (Endpoints) מוגבלות. ניתן להפעיל רק פקודות ופרמטרים ספציפיים שאושרו מראש, ללא צורך להגדיר הרשאות ניהול מלאות על עמדת הקצה.
5. ניטור ותיעוד (Script Block Logging and Auditing)
   1. הפעלת Script Block Logging (Event ID 4104) תרשום ללוג אילו פקודות הורצו, גם אם הן מוצפנות. זוהי הגדרה חיונית לזיהוי ותחקור אירועים (Forensics).

4. מצ"ב טבלה מסכמת של השיטות שהוצגו, האפקטיביות שלהן והקושי ביישומן. על כל ארגון לשקול אלו שיטות מתאימות עבורו, ולבחון אותן בסביבת ניסוי טרם הטמעה בסביבת ייצור:

בקרה מוצעת	מטרת הבקרה	קושי יישום	אפקטיביות
Execution Policies	מניעת הרצת סקריפטים שגויה על ידי משתמשים	נמוך מאוד	נמוכה
חסימת נתיבי SRP	חסימה בסיסית עבור משתמשים שאינם טכניים	בינוני	בינונית
AppLocker / CLM	הקשחת תחנות עבודה נגד נוזקות מודרניות הפועלות בשיטת (Fileless) Living of the Land	גבוה	גבוהה
Role Based JEA	מתן גישת ניהול ממוקדת ללא הרשאות Shell מלאות	גבוה מאוד	גבוהה מאוד
Logging & Auditing	מימוש תחקור וזיהוי איומים בזמן אמת	בינוני	בינונית

5. תודה ל-Code Blue על הסיוע בהכנת התרעה זו.

[מקורות]

1. https://www.gov.il/he/pages/power_shell
2. https://media.defense.gov/2022/Jun/22/2003021689/-1/-1/1/CSI_KEEPING_POWERSHELL_SECURITY_MEASURES_TO_USE_AND_EMBRACE_20220622.PDF