**{title}**

**{date}**

{%imageTag}

**© הודעה בדבר זכויות יוצרים:** אין להעתיק, לשכתב, לצלם או לשלוח מסמך זה או חלקים ממנו מבלי לקבל אישור בכתב מחברת מגדל, המידע המופיע במסמך זה הנו רכושו הבלעדי של חברת מגדל וחברת White-Hat, כל הקורא מסמך זה, כולו או מקצתו, ואינו מורשה לצפות במידע המופיע בו, חשוף לתביעה משפטית. המוצא מסמך זה מתבקש להעבירו לידי חברת מגדל.

**הצהרת אחריות**: מסמך זה וההמלצות הכלולות בו, נכתבו ונערכו בהתאם למידע שסופק ונחקר על ידי חברת White-Hat החברה אינה טוענת כי השימוש במסמך או בכל חלק ממנו יבטיח תוצאה מוצלחת. המתודולוגיה המוצעת במסמך מהווה מסגרת לביצוע "הפרויקט" אצל הלקוח ואינה מהווה תחליף לעמידה בכל הדרישות וההנחיות אשר הלקוח נדרש לעמוד בהן.

תוכן עניינים

[AeDebug– חוק מס' 1 (Rule 56) 6](#_Toc120449465)

[תיאור המתקפה – (ID: T1547, Persistence): 6](#_Toc120449466)

[פירוט החוק: 6](#_Toc120449467)

[pktmon – חוק מס' 2 (Rule 57) 7](#_Toc120449468)

[תיאור המתקפה – (ID: T1547, Collection): 7](#_Toc120449469)

[פירוט החוק: 8](#_Toc120449470)

[DisableAdminUac – חוק מס' 3 (Rule 58) 8](#_Toc120449471)

[תיאור המתקפה – (Defense Evasion): 8](#_Toc120449472)

[פירוט החוק - GPO: 9](#_Toc120449473)

[DisableShutDown – חוק מס' 4 (Rule 59) 9](#_Toc120449474)

[תיאור המתקפה – ( Impact): 9](#_Toc120449475)

[פירוט החוק - GPO: 10](#_Toc120449476)

[Disk Cleanup – חוק מס' 5 (Rule 60) 10](#_Toc120449477)

[תיאור המתקפה – (ID: T1547, Persistence): 11](#_Toc120449478)

[פירוט החוק: 12](#_Toc120449479)

[Event Viewer Uac Bypass – חוק מס' 6 (Rule 61) 12](#_Toc120449480)

[תיאור המתקפה – (ID: T1547, Persistence): 12](#_Toc120449481)

[פירוט החוק: 13](#_Toc120449482)

[Global Flags – חוק מס' 7 (Rule 62) 14](#_Toc120449483)

[תיאור המתקפה – (Persistence): 14](#_Toc120449484)

[פירוט החוק: 15](#_Toc120449485)

[Html Helper – חוק מס' 8 (Rule 63) 15](#_Toc120449486)

[תיאור המתקפה – (Persistence): 15](#_Toc120449487)

[פירוט החוק: 16](#_Toc120449488)

[MappingShares – חוק מס' 9 (Rule 64) 17](#_Toc120449489)

[תיאור המתקפה – (Persistence): 17](#_Toc120449490)

[פירוט החוק - GPO: 18](#_Toc120449491)

[MsiInstaller – חוק מס' 10 (Rule 65) 18](#_Toc120449492)

[תיאור המתקפה – ( Privilege Escalation): 18](#_Toc120449493)

[פירוט החוק: 19](#_Toc120449494)

[Netplwiz – חוק מס' 11 (Rule 66) 19](#_Toc120449495)

[תיאור המתקפה – (ID: T1547, Persistence): 19](#_Toc120449496)

[פירוט החוק: 21](#_Toc120449497)

[PortMonitor – חוק מס' 12 (Rule 67) 21](#_Toc120449498)

[תיאור המתקפה – (ID: T1547, Persistence): 21](#_Toc120449499)

[פירוט החוק - GPO: 22](#_Toc120449500)

[Rstrui – חוק מס' 13 (Rule 68) 23](#_Toc120449501)

[תיאור המתקפה – (ID: T1547, Persistence): 23](#_Toc120449502)

[פירוט החוק: 24](#_Toc120449503)

[WER Debugger – חוק מס' 14 (Rule 69) 24](#_Toc120449504)

[תיאור המתקפה – (ID: T1547, Persistence): 24](#_Toc120449505)

[פירוט החוק: 25](#_Toc120449506)

[RecycleBin Persistence – חוק מס' 15 (Rule 70) 25](#_Toc120449507)

[תיאור המתקפה – (ID: T1547, Persistence): 25](#_Toc120449508)

[פירוט החוק: 26](#_Toc120449509)

[WMP Share Proxy Execution – חוק מס' 16 (Rule 71) 27](#_Toc120449510)

[תיאור המתקפה – (ID: T1547, Persistence): 27](#_Toc120449511)

[פירוט החוק: 28](#_Toc120449512)

[Windows Shortcut – חוק מס' 17 (Rule 72) 28](#_Toc120449513)

[תיאור המתקפה – (ID: T1547, Persistence): 29](#_Toc120449514)

[פירוט החוק - GPO: 29](#_Toc120449515)

[Device Enroller Execution – חוק מס' 18 (Rule 73) 29](#_Toc120449516)

[תיאור המתקפה – (ID: T1547, Persistence): 30](#_Toc120449517)

[פירוט החוק: 31](#_Toc120449518)

[Installed components – חוק מס' 19 (Rule 74) 31](#_Toc120449519)

[תיאור המתקפה – (ID: T1547, Persistence): 31](#_Toc120449520)

[פירוט החוק: 32](#_Toc120449521)

[Mofcomp – חוק מס' 20 (Rule 75) 33](#_Toc120449522)

[תיאור המתקפה – (ID: T1547, Persistence): 33](#_Toc120449523)

[פירוט החוק: 34](#_Toc120449524)

רקע

דו״ח זה מציג את פירוט הרצת המתקפות ואת כלל חוקי ההגנה אשר הוטמעו במהלך הבדיקות אותן ביצעה חברת White-Hat בחברת ״מגדל״ בחודש נובמבר 2022 כחלק משירות EOTE.

במסגרת השירות מורצים בחברתכם התקפות / Silver Bullets העוקפים את כל מערכות ההגנה ומדמים תוקף אמיתי ברשת הארגונית. מדובר בקטעי קוד (Payloads) אשר מפותחים על ידינו בכדי לדמות מתקפות אמתיות ועדכניות על הרשת הארגונית של הלקוח ולאחר מכן מוטמעים במערכות ההגנה חוקים התנהגותיים לסגירת הפערים וזיהוי התקפות אלו.

ההתקפות מדמות שלבים שונים של התקפת APT על הרשת הארגונית :

* איסוף מידע וחדירה לרשת
* עקיפה של כלי הגנה קיימים והתפשטות ברשת
* העלאת הרשאות והגעה למשאבי רשת קריטיים
* הזלגה של מידע רגיש מהרשת הארגונית

הייחודיות ב- Silver Bullets היא שהם מיוצרים על ידי White-Hat ומותאמים למערכות ההגנה בחברתכם, ברובם מבוססות ההתקפות על מגמות וטרנדים בעולם אבטחת המידע ולא רק על בסיס חולשות הניתנות לסגירה על ידי טלאי אבטחה או תיקון התלוי בשדרוג מוצרים קיימים אלא בהטמעה של חתימות התנהגותיות מתקדמות במערכות האבטחה הקיימות.

חשוב לציין כי קטעי הקוד שלנו **אינם** חתומים במנועים מוכרים, וניתנים לזיהוי אך ורק על ידי תהליכי זיהוי מבוסס התנהגות חריגה (אנומליות) וחוקים ייעודים.

**בוצעה הרצה מלאה של הפיילודים מול מוצר ה EDR + חסימה של הפערים אשר עלו מההתקפות באמצעות טיוב המערכות הקיימות ללא רכישה או הטמעה של מערכות חדשות.**

חשוב להדגיש, כי ההתקפות מדמות שלבים שונים של מתקפת סייבר ובמקרים רבים אנו "מדלגים" על חלק ממערכות ההגנה ועל שלב ההנדסה החברתית במתקפה, זאת בכדי לזקק חוק רלוונטי ואיכותי ולא להתעכב על שלבים אשר פחות רלוונטיים לתוצאה הסופית.

למשל, אנו נשלח סקריפט PowerShell ללא מעטפת, זאת בידיעה שסקריפט כזה היה נחסם בערוץ המייל- פרט זה אינו רלוונטי משום שמטרת בדיקה זו היא לבדוק תרחיש של משתמש בעל הרשאות ולא תרחיש של הכנסת קובץ מסוג זה במייל (לדוג' מקרה בו מנסה תוקף לבצע תנועה רוחבית ברשת).

תהליך העבודה במבט על :

חוקי ההגנה שהוטמעו – פירוט ראשוני

{#DefenceRules}

{defenceRuleTitle}– חוק מס' {defenceRuleNumber}

## תיאור המתקפה – (ID, [Persistence](https://attack.mitre.org/tactics/TA0003)):

מהלך המתקפה:

הרצת דמה של המתקפה בעמדה המחוברת לרשת הארגון:

## פירוט החוק:

יצירת החוק ב-Palo Alto Cortex:

{/DefenceRules}