**{title}**

**{date}**

{%imageTag}

**© הודעה בדבר זכויות יוצרים:** אין להעתיק, לשכתב, לצלם או לשלוח מסמך זה או חלקים ממנו מבלי לקבל אישור בכתב מבנק ירושלים, המידע המופיע במסמך זה הנו רכושו הבלעדי של בנק ירושלים 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 בנק ירושלים.

**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

[רקע אודות פתרון Eye Of The Enemy: 3](#_Toc130919029)

[תקציר מנהלים - טבלה מסכמת לתוצאות בדיקת ההיתכנות: 5](#_Toc130919030)

[תרחיש מספר 1 – הרצת קוד זדוני באמצעות Control.exe 8](#_Toc130919031)

[תרחיש מספר 2 –הרצת קוד זדוני באמצעות פרוקסי על ידי שימוש ב-tar.exe 10](#_Toc130919032)

[תרחיש מספר 3 – שיבוש חקירה על ידי יצירת לוגים מזויפים באמצעות EventCreate.exe 12](#_Toc130919033)

[תרחיש מספר 4 – קימפול קוד זדוני באמצעות aspnet\_compiler.exe 14](#_Toc130919034)

[תרחיש מספר 5 – התחמקות מאמצעי הגנה על ידי קידוד ל-base64 תוך שימוש ב-tar.exe 16](#_Toc130919035)

[תרחיש מספר 6 – הרצת קוד זדוני באמצעות הזרקת dll זדוני ל-recover.exe 18](#_Toc130919036)

[תרחיש מספר 7 – שיבוש חקירה על ידי מחיקת Jumps Lists 20](#_Toc130919037)

רקע אודות פתרון Eye Of The Enemy:

דו״ח זה מציג את פירוט בדיקת ההיתכנות, אשר בוצעה בבנק ירושלים בתאריך 27.03.2023 ואת כלל הממצאים שאותרו במהלך הבדיקות אותן ביצע צוות המחקר של חברת White-Hat .

בבדיקה זו בוצע שימוש ב – "Silver Bullets" של החברה במטרה להוכיח יכולות הפתרון:  
 **Eye Of The Enemy**.

במסגרת השירות, מורצים אצל הלקוח בכל חודש מספר Silver Bullets העוקפים את כל מערכות ההגנה ומדמים תוקף אמיתי ברשת הארגונית. מדובר בקטעי קוד (Payloads) אשר מפותחים על ידינו בכדי לדמות מתקפות אמיתיות ועדכניות על הרשת הארגונית של הלקוח.

ההתקפות מדמות שלבים שונים של התקפת APT על הרשת הארגונית:

* איסוף מידע וחדירה לרשת
* עקיפה של כלי הגנה קיימים והתפשטות ברשת
* הסלמת הרשאות והגעה למשאבי רשת קריטיים
* הזלגה של מידע רגיש מהרשת הארגונית
* יצירת תקשורת C&C לשרת מרוחק ועוד

הייחודיות ב- Silver Bullets היא שהם מיוצרים, מפותחים, ונבדקים מקצה לקצה ע"י צוות המחקר בחברה, תוך התאמה בזמן אמת למערכות ההגנה הספציפיות בארגון ה"נתקף".

ברובן 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 אינם חתומים במנועים מוכרים, וניתנים לזיהוי אך ורק על ידי תהליכי זיהוי**

**מבוסס התנהגות חריגה (אנומליות) וחוקים ייעודים**.

במסגרת הפתרון, WHITE-HAT תספק 5 התקפות **בכל חודש**, המבוססות על חולשות עדכניות, שיטות תקיפה אמיתיות ומחקרי מודיעין המבוצעים בחברה.   
**היתרון המהותי בפתרון, מתייחס לעובדה כי על סמך הממצאים העולים מהצלחת הרצת הפיילודים ולאור פתרונות ההגנה המוטמעים במשרד, תבוצע חסימה של הפערים אשר עלו מההתקפות באמצעות טיוב המערכות הקיימות, ללא רכישה או הטמעה של חדשות.**

בנוסף לכך, White-Hat תספק תמיכה מודיעינית על ידי מוקד SOC פעיל, התרעה על כל חשיפה רלוונטית לארגון שלכם וכן תאפשר העברת בקשות ייעודיות לפיתוח התקפות שתהיו מעוניינים לנסות על הרשת הארגונית שלכם.

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.

לדוגמא, 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).

לאחר מכן, בשיתוף עם הלקוח, אנו מבצעים "איחוד" להתקפות שונות ומייצרים תרחישי התקפה מקצה לקצה, בהתאם ליכולת המעקף למערכות השונות בארגון.

השירות מסייע לארגון לבחון, לשפר ולאתגר את מערכות ההגנה שלו מול האיומים המורכבים והעדכניים ביותר, ללא צורך בפריסה או התקנה של מערכות שונות ותוך קשר אישי ישיר לצוות המחקר שמבצע גם שינויים מותאמים לארגון ע"מ לייצר את ההתקפות היעילות והמתקדמות ביותר בזמן קצר מרגע הפרסום והשימוש In The Wild.

לאחר הרצת ההתקפות יסופקו ללקוח חוקי הגנה מתאימים ו/או המלצות לשינויים קונפיגורציה על מנת לאפשר לשפר ולתקן את הפערים שהתגלו במערך ההגנה מהר ככל שניתן. מרבית החוקים הינן חוקי EDR התנהגותיים המותאמים למערכות ההגנה הקיימות בארגון.

תהליך העבודה במבט על :

תקציר מנהלים - טבלה מסכמת לתוצאות בדיקת ההיתכנות:

בחלק הבא של הדו״ח, נציג בפניכם באופן מפורט את התרחישים שהורצו ונפרט המלצות הנדרשות לביצוע ע"מ לחסום התקפות כאלו במערכות ההגנה הקיימות שלכם.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | תרחיש | פורמט הקובץ | פירוט התרחיש | עבר / לא עבר |
| 1. | הרצת קוד זדוני באמצעות Control.exe | .ps1 | בתרחיש הנ"ל, תוקף יכול להריץ קוד זדוני על תחנת עבודה על ידי יצירת אפליקציית Control Panel זדונית והרצתה תוך שימוש ב-Control.exe. | **√** |
| 2. | הרצת קוד זדוני באמצעות פרוקסי על ידי שימוש ב-tar.exe | .ps1 | בתרחיש הנ"ל, תוקף יכול להריץ קוד באמצעות פרוקסי על ידי שימוש בכלי יצירת ארכיבים tar.exe. | **√** |
| 3. | שיבוש חקירה על ידי יצירת לוגים מזויפים באמצעות EventCreate.exe | .ps1 | בתרחיש הנ"ל, תוקף יכול לשבש חקירה של תקיפה על ידי שינוי יצירה מלאכותית של אירועים מזויפים שיפנו את החוקרים לכיוונים לא מועילים. | **√** |
| 4. | קימפול קוד זדוני באמצעות aspnet\_compiler.exe | .ps1 | בתרחיש הנ"ל, תוקף יכול לקמפל ולהריץ להריץ קוד על ידי יצירת אפליקציית web באמצעות aspnet\_compiler.exe. | **√** |
| 5. | התחמקות מאמצעי הגנה על ידי קידוד ל-base64 תוך שימוש ב-tar.exe | .ps1 | בתרחיש הנ"ל, תוקף יכול להתחמק מאמצעי הגנה ולקודד קבצים רגישים ל-base64 תוך שימוש בתוכנת יצירת ארכיבים tar.exe. | **√** |
| 6. | הרצת קוד זדוני באמצעות הזרקת dll זדוני ל-recover.exe | .ps1 | בתרחיש הנ"ל, תוקף יכול להריץ קוד זדוני על התחנה על ידי הזרקת dll זדוני לכלי השירות recover.exe | **√** |
| 7. | שיבוש חקירה על ידי מחיקת Jumps Lists. | .ps1 | בתרחיש הנ"ל, תוקף יכול לשבש חקירה של תקיפה על ידי מחיקה של Jump Lists המכילות מידע אודות גישה לאובייקטים. | **√** |
| 8. | הרצת קוד זדוני על באמצעות diskshadow.exe | .ps1 | בתרחיש הנ"ל, תוקף יכול להריץ קוד זדוני על ידי הרצת כלי השירות diskshadow.exe. | **X** |
| 9. | ביטול חתימת דרייברים באמצעות bcdedit.exe | .ps1 | בתרחיש הנ"ל, תוקף יכול להסיר את הדרישה לווידוא חתימה של דרייברים על ידי שימוש ב-bcdedit.exe. | **X** |

מיפוי התקפות לפי שלבים בתהליך התקיפה:

**סיכום הרצה**

הרצת קוד זדוני:

* **הרצת קוד זדוני באמצעות Control.exe.**
* **הרצת קוד זדוני באמצעות פרוקסי על ידי שימוש ב-tar.exe**
* **קימפול קוד זדוני באמצעות aspnet\_compiler.exe**
* **הרצת קוד זדוני באמצעות הזרקת dll זדוני ל-recover.exe**

שיבוש חקירה:

* **שיבוש חקירה על ידי יצירת לוגים מזויפים באמצעות CreateEvents.exe**
* **שיבוש חקירה על ידי מחיקת Jumps Lists.**

התחמקות מאמצעי הגנה:

* **התחמקות מאמצעי הגנה על ידי קידוד ל-base64 תוך שימוש ב-tar.exe**

כלל המתקפות הורצו באמצעות סקריפטים ייעודים בשפת PowerShell אשר הוחדרו אל עמדת הבדיקות בערוץ המייל הארגוני באמצעות שליחה בפורמט טקסט גלוי (.txt), תוך קידוד תוכן הקובץ לפורמט Bytes ויצירה מחדש של קובץ ה-PowerShell בעמדה.

פירוט התרחישים והממצאים:

{#scenarios}

תרחיש מספר {scenarioNumber} – {scenarioTitle}

**רמת קושי במימוש התרחיש:** **{scenarioDifficulty}**

**רמת סיכון לארגון:** **{scenarioImpact}**

{#photos}

:הוסף הסבר כאן

{%imageTag}

{/photos}

הגנות:

**EDR:**

{#edrRecommendations}

* **{.}**

{/edrRecommendations}

**Sysmon:**

{#sysmonRecommendations}

* **{.}**

{/sysmonRecommendations}

{/scenarios}