**דו״ח סיכום הרצה**

**{documentName}**

{date}

{%imageTag}

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

**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](#_Toc131935882)

[תקציר מנהלים - טבלה מסכמת לתוצאות בדיקת ההיתכנות 5](#_Toc131935883)

[פירוט התרחישים והממצאים 7](#_Toc131935884)

[תרחיש מספר 1 – Outlook C2 7](#_Toc131935885)

[תרחיש מספר 2 – nltest Discovery 9](#_Toc131935886)

[תרחיש מספר 3 – Disable Driver Signature Enforcement 10](#_Toc131935887)

[תרחיש מספר 4 – Safe Mode with Networking 11](#_Toc131935888)

[תרחיש מספר 5 – Screen Capture Recording 12](#_Toc131935889)

[תרחיש מספר 6 – AD CS Misconfiguration 13](#_Toc131935890)

רקע אודות פתרון Eye Of The Enemy

דו״ח זה מציג את פירוט בדיקת ההיתכנות, אשר בוצעה בבנק דיסקונט בתאריך 02.04.2023 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 (Malware / Payload) 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 ותזוזה רוחבית 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 המערכות 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 ה Malware / Payloads 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 מתקפות 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 ולתוצר הסופי.

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | תרחיש | פורמט הקובץ | פירוט הממצא | עבר / לא עבר |
| 1 | Outlook C2 | .ps1 | בתרחיש הנ"ל, תוקף מנצל את תשתית ההתקנה של תוכנת ה Outlook אשר מותקנת על עמדת הקורבן לשליטה מלאה על מחשב הקורבן וזאת על ידי שליחת פקודות בפורמט מייל לקורבן, ביצוע Exfiltration לתוצאות הפקודה / הפעולה ומחיקת המייל למטרות Anti-Forensics. | **√** |
| 2 | nltest Discovery | .ps1 | בתרחיש הנ"ל, תוקף מנצל את פקודת nltest.exe המובנת במערכת ההפעלה Windows לאיסוף מודיעין פנימי של הרשת ולגילוי מידע כגון הדומיין ושרתי ה DC. | **√** |
| 3 | Disable Driver Signature Enforcement | .ps1 | בתרחיש הנ"ל, תוקף מבטל את מנגנון אמינות וחתימות Drivers במערכת ההפעלה Windows ובכך תוקפים מסוגלים להטמיע Windows Drivers זדוניים מבלי שהמנגנון מוודא את אמינותם ובכך להשיג אחיזה ברמת Rootkit. | **√** |
| 4 | Safe Mode with Networking | .ps1 | בתרחיש זה, התוקף מכניס את המחשב למצב של Safe Mode בכדי לבטל מערכות הגנה כגון AV/EDR ובכך להריץ קוד זדוני על העמדה ללא ניטור ומניעה. | **√** |
| 5 | Screen Capture Recording | .exe | בתרחיש זה, התוקף אוסף מידע על ידי הקלטת מסך מחשב הקורבן וייצוא הקובץ לפורמט MP4. | **√** |
| 6 | AD CS Misconfiguration | .ps1 | בתרחיש הנ"ל, ניתן להשיג שליטה מלאה ב-Domain הארגוני תוך ניצול Misconfiguration באופן שבו מוגדרות תעודות בארגון. | X |

תקציר מנהלים - טבלה מסכמת לתוצאות בדיקת ההיתכנות

מיפוי התקפות לפי שלבים בתהליך התקיפה

פירוט התרחישים והממצאים

{#scenarios}

תרחיש מספר{scenarioNumber} - {scenarioTitle}

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

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

:**המתקפה**

{tactic}

**פירוט התרחיש:**

{description}

**הסבר על תהליך התקיפה:**

**{#attackFlow}**

**{%imageTag}**

**{/attackFlow}**

**הוכחת יכולת באתר הלקוח:**

**{#photos}**

**{%imageTag}**

**{/photos}**

**חוקי הגנה:**

{#recommendations}

* {.}

{/recommendations}

{/scenarios}