דוח אירוע - 1

מגיש: עוז מעתוק 305181158

שם התרחיש: Active attack – by SQL Injection

תהליך התקפה: תהליך ההתקפה מתחיל בהטמעת קוד פעולה ביעד, לכן ההתקפה נקראת "הזרקה". הכדי להיות אפקטיבי, קוד הפעולה ראשית יוצר/משתלט על משתמש מגדיר לו הרשאות ניהול ודרכו מריץ Script אשר מבצע מספר פעולות על היעד. במקרה שלנו היעד הזה שרת ה – SQL של הרשת, ובתוכו רץ Automaic Script אשר יצר/השטלת על משתמש בשם sqlusr ודרכו מריץ Script אוטומטי אשר מממש שיטת ההתקפה מסוג Crawling. Crawling Hack היא התקפה אשר גורפת מידע מתוך היעד עליו היא עובדת.

תהליך הזיהוי: תחילה העמדנות תצפית בכל כלי שיכולנו, כאשר הכלים האפקטיבים היו ה – ArcSight, וה – Zenoss. הסיבה לכך שדווקא כלים אלו היו רלוונטים לתרחיש היא מפני שה ArcSight מאפשר לנו לזהות תרחישים שאינם עומדים בחוקיות המוטמעת במערכת. במקרה שלנו התקיפה זהותה בעקבות הפרת חוק אשר נכתב בספריית החוקים של Elbit. בהמשך ישיר לנתונים ב ArcSight הבחנו בפעולות קריטיות בארגון כמו נפילת תהליך ה DNS על שרת ה DC, והפסקת תהליך ה kdc גם כן על שרת ה DC. זאת יכולנו לגלות בעזרת שירות ה Zenoss אשר עוקב אחר השירותים והתהליכים של הארגון, מאתר ומתריע על שינויים לא שיגרתים במערכת. בעקבות אירועים אלו פנינו ל Tracker של Checkpoint אשר מאפשר לנו לעקוב אחר תנועות ברשת שלנו בצורה נוחה לאחר הגדרת המעקב הרצוי לביצוע פילטור לפי דרישה, ע"י סינכרון זמני האירועים מצאנו ב Tracker את פרטי התוקף! כתובת ה – IP ממנה הגיעה התקיפה, וכתובת ה – IP אליהה התקיפה מכוונת. חשוב לציין כי ע"פ הנתונים אשר הוצגו לנו ב Tracker היה ניתן להבחין כי יעד התקיפה היה מסד הנתונים של המערכת.

<u>תהליך ההגנה ראשוני:</u> כתגובה הגנתית אוטומטית לנפילת התהליכים ברשת ה DC, ביצענו חיבור מרחוק למערכת ההפעלה של השרת אשר מריץ Windows Server ע"י תוכנת ה Vmware vSphare אשר מספקת ממש התחברות מרחוק למערכות הפעלה שונות ברשת. דרך השירותי המנהל של ה Windows server ניתנה לנו גישה לניהול התהליכים אשר רצים על מערכת הפעלה של השרת, וכך החזרנו את התהליכים אשר הופסקו לפעולה. לאחר מכן סרקנו את רשימות ה logs אשר מסופקות ע"י כלי המנהל של מערכת ההפעלה Windows server על שרת ה DC. בביצוע הסריקה חיפשנו פעולות שאינן סדירות של השרת, המיוחד בכניסה ויציאה של משתמשים ע"י סימכרון מול ציר הזמן הרלוונטי לנו מתוך רשימת המקרים בתהליך הזיהוי. כתוצאה מסריקה זו שמנו לב לפעולות חריגות ע"י המשתמש sqlusr כמו כניסות ויציאות בתדירות גבוהה, נגיעה בקבצים על השרת, והגדרת הרשאות ניהול במערכת. כמובן שפעולות אלו היו אינן לגיטימיות עבור משתמש בסגנון המוצג, לכן, עדיין בעזרת כלי הניהול של Windows server פתחנו את רשימת כלל המשתמשים הרשומים על השרת, ובדקנו מהן ההרשאות של המשתמש שמעניין אותנו, sqlusr. אכן בהתאם למה שנראה בלוגים, ההרשאות היו הרשאות מנהל אשר אינן מתאימות למשתמש הנ"ל, לכן כתגובה לכך הסרנו לו את ההרשאות.

<u>תהליך הגנה מונעת:</u> בכדי לתת מענה להתקפה החוזר, היה נדרש מאיתנו לאתר את כתובת ה IP אשר ממנה מבוצעת ההתקפה, זאת היה ניתן להבחין ע"י תוכנות ה ArcSight וה Checkpoint smartView Tracker אשר פירסמה לנו נתונים אודות התקיפה. כך, ע"י שימוש בכתובת ה IP של התוקף יכלנו להוסיף חוק חסימה לכתובת זו על שתי ריכיבי חומות האש אשר קיימות לנו ברשת (את האמת, מספיק לבצע זאת רק על חומת האש החיצונית מפני שכתובת התקיפה אינה הגיעה מתוך הרשת). בנוסף לכך לנטרל את המשתמשים על השרתים אשר בעזרתם התקיפה מונעת, לאתר ותמחוק את הקוד אשר הוזרק למערכת.
כתגובה עתידית למקרים דומים ניתן לאמץ תוכנות הגנה כמו Crawler By HPE אשר מנטרת ניסיונות להתקפות Crawling על אתר אינטרנט ושרתים נוספים.

<u>הסבר מפורט על אופן ההתקפה (התמקדות בחולשות):</u> החולשה שבעקבותיה התרחשה ההתקפה נמצאת בפירצת האבטחה של שרת ה SQL. השימוש הפירצה זו להתקפות סייבר נקרא SQL Injection והוא מתבצע ע"י גישה למסד הנתונים של האתר/הרשת והכנסת קוד מסויים לשאילתת SQL. הקוד בעצם מבצע פריצה ל Database ופותח את האפשרות לבצע שינויים על ה Database ללא ההרשאות הנדרשות. כך יכול התקף לחדור לDatabase של השרת, ולבצע פעולות חריגות על מסד הנתונים. משם, המשך ההתקפה התבסס על יצירת משתמש בעל הרשאות מנהל ע"י השליטת במסדי הנתונים, הרצת פקודות קוד (Automatic Script) להפסקת תהליכים מתאימים (לתוקף היה צורך בהפסקת תהליכים ספציפיים בכדי לבצע את התקיפה המתוכננת)על שרת ה DC, והצמדת מצביעים לנק' שונות ברשת ובשרתים.

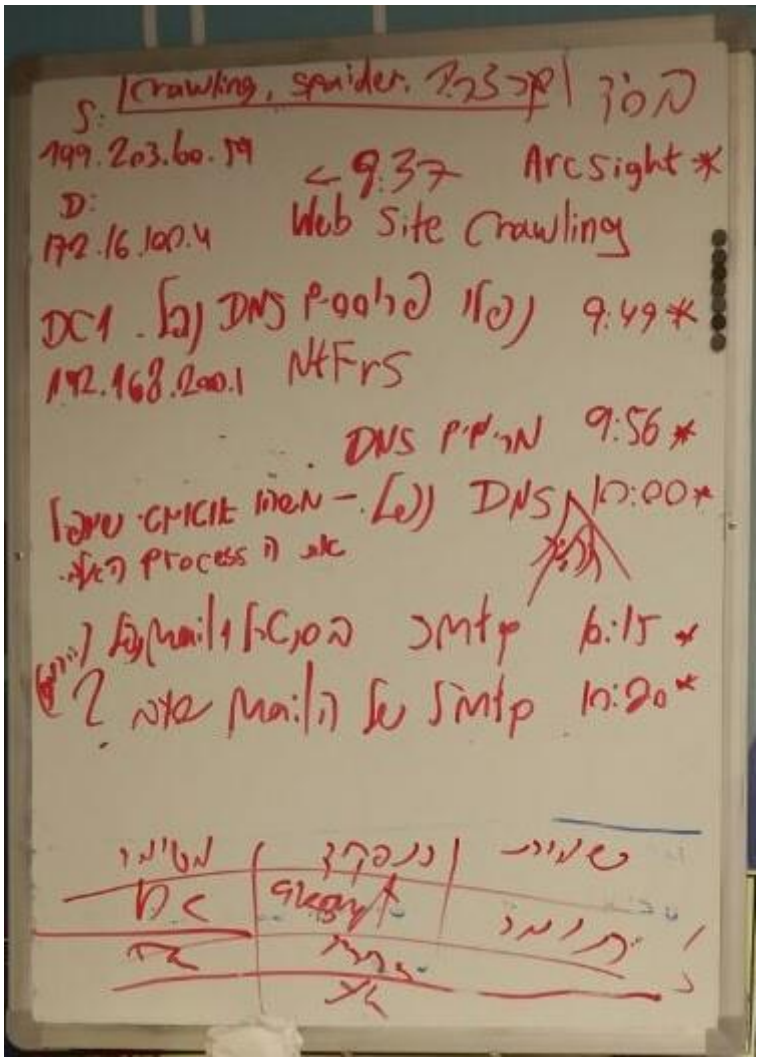
- <u>יש לציין כי פעולות פעולות החייאת התהליכים, ושלילת הרישיונות למשתמש המזיק אינן הועילו מפני שתהליך קרה בצורה חוזרת למרות הניסיון הבסיסי שלנו לטפל בכך. התהליך הופסקו שוב ושוב, ולמשתמש הוגדרו הרשאות בצורה אוטומטית בכל פעם.</u>

כלים חדשים שפיתחתם/השתמשתם: בכלים העיקריים בהם השתמשנו הם ה – ArcSight וה – Zenoss לתהליך זיהוי ההתקפה (כמו שמפורט), ולאחר מכן בתוכנת ה vSphare ומערכת ההפעלה של Windows Server אשר איפשרה לנו לתת מענה מתוך המערכת להתקפה המתוארת.

אופן עבודת הצוות: עבודת הצוות התבצע ע"י חלוקת משימות בין חברי הקבוצה כאשר קיים חבר יחיד אשר מנהל את חלוקת המשימות דואג לסנכרון בין חברי הצוות ומערכן את כולם ואת הלוח באירועים המתרחשים בכל התהליך. יש לציין כי זו משימה ראשונה של הצוות ביחד כצוות, ופעולה ראשונה על הכלים אשר ניתנו לנו להתמודדות עם התרחיש, בעקבות סיבות אלו, הצוות עבד בצורה איטית מפני שהיה בשלבי היכרות ראשונה עם הכלים ואח עם השני.

חוסרים/קשיים/בעיות: החוסר הגדול ביותר שהקשה עלינו היה עצם העובדה כי תוכנת ה Dashboard של Checkpoint לא הייתה זמינה עבורנו. בנוסף, העובדה כי ההתקפה בוצעה באופן אוטומטי, ולא נדרשה פריצה ישירה לשרתים בכל פעם דרשה מאיתנו ביצוע מעקב ארוך על הרשת. בנוסף לכך פיזור ההתקפה גם על שרת ה SQL וגם על שרת ה DC והרצת קוד סקריפט אשר מבצע את הפעולה הנדרשת הטילו קשיים על תהליכי הזיהוי והתגובה של הצוות להתקפה.

תמונה: צילום לוח האירועים בכתה + פירוט המקרים בצמוד לזמנים הרלוונטים



אירועים מרכזיים:

9:37 הבחנה ב Crawling בעזרת תוכנת ה ArcSight

במקביל, איבחון המקרה ב Tracker והפקת כתובת התוקף והמטרה

Source IP: 199.203.100.59

Dest IP: 172.16.100.14

- <u>יש לשם לב כי כתובת מקור התקיפה היא חיצונית ואינה מתוך הרשת שלנו.</u>

9:49 נפילות של תהליכים DNS, kds, NTfrs בשרת ה DC1 ברשת שלנו.

9:56 החייאת התהליכים והפעלתם מחדש בשרת

10:00 נפילה חוזרת של התהליכים הנ"ל

להרחבה / קישורים נוספים:

SQL Injection

Crawling Hack \ Web crawler

Crawler –

התקפה תוכנתית אשר מבקרת אצל ייעדים מסויים, בד"כ אתרי אינטרנט, ומצמידה מצביעים (Indexs) למיקומים וערכים אשר מעניינים אותה. התוכנה בסופו של דבר יוצרת סוג של מנוע חיפוש עבור כלל המידע שהיא אספה ונותנת לבעלים שלה גישה ישירה ונוחה למידע אשר ברוב המקרים דורש הרשאות פנימיות. חשוב לציים כי הרעיון העומד מאחורי ה Crawler הוא שידרוג הפעולה אשר תוכנות כמו Spider ו – Bot מבצעים, להפקת מידע בצורה יותר רחבה.

Spider –

העכביש היא שיטת התקפה אשר ממומשת ע"י קוד תוכנה (סקריפט בדר"כ). התוכנה שואבת מידע מהמחשב המותקף אשר הוטמעה בו והופכת אותו לנגיש עבור מפעיל ההתקפה.

Bot (Internet Bot)

Procces –

תהליך הוא יישות תוכנתית אשר רצה על מערכת ההפעלה של המחשב / השרת ובעלת מדימה מסויימת המשרתת את מערכת ההפעלה או תוכנות גדולות ואחרות אשר רצות עליה. קיימים סוגי תהליכים שונים במהותם, הרשאותם ובתפקידם, חלק יכולים להיות מבוזרים וחלקם לא. כולם ממומשים ע"י קוד אשר מופעל בצורה מתאימה למערכת ההפעלה אשר הוא רץ עליה.

Microsoft advisior for crawling attacks + suggested solutions

ArcSight SEIM by HPE

Zenoss

Vmware vSphare

Checkpoint smartView Tracker

תוכנת בקרת רשת מבית checkpoint המספקת ממשק נוח ויעיל לאיתור אירועים ברשת. התוכנה מספקת כלים מאוד משמעותיים בסינון פעולות אשר מעניין את העוקב. התוכנה בנוסף מציגה לוגים רלוונטים לפעולות ברשת ומנתחת את תעבורת הרשת.