מטלות

שם: ליאור זרו

ת.ז: 205467806

הנדסאי תוכנה שנה ב' סמסטר ב'

Ransomware- נקרא בעברית וירוס כופר, *הנו סוג של נוזקה המגבילה גישה למערכת המחשב הנגוע, ומעלה דרישה לתשלום כופר למפעיל הנוזקה וכדי להסיר את ההגבלה. חלק מהכופרות מצפינות קבצים בכונן הקשיח ואחרות נועלות את המערכת כולה ותוך הצגת הודעת דרישת תשלום Ransomware .מופצת כסוס טרויאני המתחפש לקובץ מוכר*. כך בפועל, כל המידע החיוני - הכלכלי, התפעולי, העסקי והמסחרי - וכן שרותים שהעסק שלכם מספק כסחר מקוון, ניהול מלאים והזמנות וכו' יכולים להפוך ללא זמינים עבורכם ועד כדי השבתה מלאה של הפעילות העסקית שלכם שתגרור נזק מיידי אך בעיקר נזק ארוך טווח למותג, לאמינות, לנאמנות קהל הלקוחות, קשרי העבודה עם ספקים ושותפים עסקיים ועד כדי השבתה וסגירת העסק.

Ransomware אינה תופעה חדשה ולמעשה *כופרה קיימת כבר מספר שנים, אבל לאחרונה ניכרת עליה בשימוש בה על-ידי פושעי סייבר*.

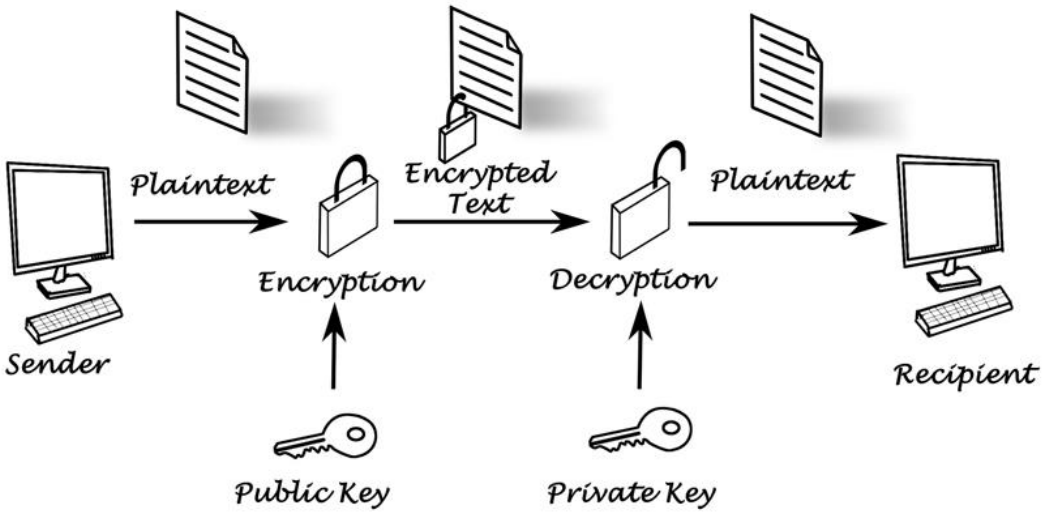
המונח Ransomware הוא כינוי לסוגים שונים של תוכנות זדוניות המשמשות את פושעי האינטרנט לסחיטה של כסף מחברות ומשתמשים פרטיים בצורה של כופר. ההאקר משתלט לכם על המחשב, חוסם את הגישה אל התמונות או העבודות שלכם וכדי לשחרר את החסימה הוא דורש תשלום המשתנה ממדינה למדינה הנטייה של מרבית המותקפים ועל פי *מחקרים שנעשו לאחרונה רבים מהגולשים שנופלים קורבן למתקפות כאלו בוחרים לשלם את הכופר הנדרש כדי לקבל את הקבצים שלהם בחזרה*, אך חשוב לציין כי בכך אין שום ערובה כי נקבל בחזרה את המידע העסקי הכה חיוני לנו. כי *אפילו אם בחרנו לשלם את הכופר עלינו לזכור שמדובר פה במילה של עברין ולמעשה לגולש אין ערובה לכך שהקבצים שלו יוחזרו או שלא יעשה בהם שימוש אחר או שהאקר לא ישנה פתאום את גובה הכופר*.

תהליך ההתקפה של וירוס כופר איך מתבצע ומטרה- תוכנת כופר מוסווית לרוב כסוס טרויאני ,ויכולה לחדור למערכת על ידי קובץ שהורד למחשב או ניצול פרצות בשירותי רשת שונים. לאחר מכן התוכנה מריצה את הפקודות הזדוניות. במסגרת הפעלת התוכנה ייתכן שתופיע הודעת אזהרה מזויפת מטעם רשויות החוק, לדוגמה, טענות שקריות על כך שהמערכת שימשה למטרות לא חוקיות, ושהיא מכילה תוכן לא חוקי כגון פורנוגרפיה ותוכן פיראטי ,או שהמערכת היא גרסה לא חוקית של.Microsoft Windows

חלק מתוכנות הכופר מתוכננות לנעול או להגביל את המערכת עד שיבוצע התשלום. ההגבלה מבוצעת בשיטות שונות. ישנן תוכנות כופר שמשנות את ה Master boot record- או את הגדרות ה- Windows shell . הדרך המתוחכמת ביותר היא הצפנת קבצים: מרבית תוכנות הכופר משתמשות בהצפנה חזקה כך שרק לכותב הנוזקה יש מפתח ההצפנה המתאים.

לרוב, המטרה היא קבלת תשלום על מנת להסיר את תוכנות הכופר על ידי אספקת תוכנה אשר יכולה לפענח את הקבצים או על ידי שליחת הקוד המתאים לפתיחת ההצפנה - דבר שייתכן ואכן יקרה, וייתכן שלא. מרכיב מרכזי בדרישת התשלום היא שהתשלום יבוצע באמצעות מערכת תשלומים שלא ניתנת למעקב. קיים מגוון רחב של שיטות תשלום, כולל: העברה בנקאית, העברה באמצעות מסרון ,ושימוש במטבע הדיגיטלי ביטקויין.

דוגמא איך עובדת ההצפנה:



דרכי התמודדות עם וירוס כופר- במקרה שזוהתה התקפת כופרה, מומלץ לפעול על פי ההמלצות הבאות:

1. ניתוק המחשב הנגוע מכל הרשתות שאליהן הוא מחובר, כולל רשתות קוויות ואלחוטיות כגון Fi-Wi או Bluetooth ניתוק כל הרכיבים החיצוניים המיועדים לאחסון קבצים או התקני זיכרון נייד. המטרה היא למנוע ככל האפשר התפשטות של הכופרה באמצעות רשתות אלו לעמדות נוספות.

2. הימנעות מביצוע פעולות כלשהן על המחשב הנגוע- בשלב זה אין למחוק קבצים, להפעיל כלי ניקוי דיסק או סריקות אנטי-וירוס.

3. הבנת היקף הפגיעה - ביצוע סריקה לבירור כמות הקבצים שהוצפנו וסוגיהם. מומלץ לבדוק ב- Registry או בקבצים מסוימים שם הכופרה שומרת בדרך כלל את רשימת הקבצים שהוצפנו על ידה . לבדוק האם לעמדה שהותקפה יש גישה ל:

תיקיות משותפות Folders Shared

כוננים קשיחים חיצוניים

אמצעי אחסון רשתיים

התקני זיכרון נייד (Key On Disk)

והאם קבצים על אמצעים אלו הוצפנו.

4. לבדוק באיזה סוג של כופרה מדובר- במידה וקיימים פרסומים ברשת לגבי סוג הכופרה, ניתן ללמוד מהם את היקף התקיפה הצפויה ומאפייני ההתפשטות השונים כגון: סוגי קבצים מוצפנים, האם מבוצעת תנועה רוחבית והצפנת קבצים ברשת או באזורי אחסון משותפים, האם מבוצעת גישה לשירותי ענן.

דוגמא להתקפת וירוס כופר שנעשתה לאחרונה היא על חברת שירביט חברה גדולה לביטוח במדינת ישראל קישור לכתבה:

https://13news.co.il/item/news/tech-digital-science/cyber-attack-on-israeli-/company-1171086

sql injection- קודם כל שאנחנו מדברים על sql נסביר מה זה, אז sql היא שפה של מסד נתונים שתפקידה לעבד נתונים מאגרי מידע שבהם משתמשים אתרים אפליקציות תוכנות וכד', זאת אומרת כשאנחנו נכנסים לאתר או אפליקציה או משהו אחר אז כל המאמרים הטקסטים המידע שלהם וכו' מוזנים אל תוך מסד נתונים. במסד נתונים זה יש את כל המידע והנתונים שיש באותו יישום בו אנו משתמשים .בעולם האינטרנט של היום אין כמעט אתר שלא משתמש ב database כדי לאחסן ולארגן את המידע שהוא מכיל .
Databaseאלו מהווים את המטרה הכי גדולה של ההאקרים של ימנו זה המזון שלהם והם מנצלים את זה לבצע את זממם משום שהם יכולים להכיל מידע רגיש וחשוב ביותר כמו פרטים אישיים של המשתמשים באותו יישום ואפילו מספרי כרטיס אשראי וחשבונות בנק .
injection Sql היא אחת ההתקפות הנפוצות והוותיקות בעולם ההאקרים היא שיטה לניצול פרצת אבטחה בקוד התוכנית היא בנויה בעצם על הזרקת שאילתת sql של ההאקר.
התקפות injection SQL מאפשרות לתוקפים לזייף זהות ,להתעסק בנתונים קיימים, לגרום לבעיות דחייה כמו ביטול עסקאות או שינויים בלתי צפויים במערכת, לאפשר חשיפה מוחלטת של כל הנתונים במערכת, להרוס את הנתונים או להפוך אותם לבלתי זמינים ולהפוך למנהלי מערכת של שרת ה .database האקר המשתמש בשיטה זו מנצל את שכבת הנתונים של אותו יישום בו אנו משתמשים וההתקפה מתחילה לעבוד כאשר המשתמש מזין נתונים לאותו פלט של היישום שלשם לכאורה היה אמור להכניס נתונים תמימים אשר שולח אותה למשתמש שגולש באותו יישום שהתקיפה מתבצעת עליו וההאקר יכול לשאוב מידע מה databaseבמקרה הטוב ההאקר יכול להזין או לשנות נתונים שהוא לא אמור לשנות, כמו לשדרג את הפרופיל שלו, לפגוע בפרופילים אחרים וכו׳, או במקרה היותר גרוע להוציא מידע רגיש, כמו סיסמאות של משתמשים אחרים ,כתובות דואר אלקטרוני או אפילו מספרים של כרטיסי אשראי. על ידי הזרקת נתונים, ההאקר יוצר לעצמו למעשה גישה חופשית ומלאה למסד הנתונים שלנו, בדרך כלל זה מאפשר להאקר להציג נתונים שהם בדרך כלל לא מסוגלים לאחזר, זה עשוי לכלול נתונים השייכים למשתמשים אחרים, או כל נתונים אחרים שהיישום עצמו מסוגל לגשת אליהם ובמקרים מסוימים מוציאים פקודות למערכת ההפעלה . במקרים רבים, האקר יכול לשנות או למחוק נתונים אלה, ולגרום לשינויים מתמשכים בתוכן או בהתנהגות היישום. במצבים מסוימים, ההאקר יכול להחריף את התקפת injection sql ולסכן את השרת הבסיסי או תשתית אחורית אחרת או לבצע התקפת מניעת שירות. למרות שה injection sql היא אחת ההתקפות הישנות היא עדיין גורמת נזק רב.

דוגמא להתקפת sql injection- בדוגמה הבאה, הנתונה ב־ ASP, ביקש המתכנת לקלוט מהמשתמש את סיסמת הגישה שלו לאתר אינטרנט מאובטח, לבדוק את תקינותה כנגד מסד הנתונים ולאשר את הגישה אם הסיסמה אכן קיימת. הקוד (הפגיע לפריצה) הבונה את שאילתת ה SQL-נראה כך:

```
SQL = "SELECT * FROM users WHERE password='" & Request("password") & "'"
```

כאשר האובייקט Request משמש לקבלת נתונים מטפסים. כעת, השימוש התקין שראה המתכנת לנגד עינו הוא הכנסת סיסמה, למשל 1234, שתייצר את שאילתת ה SQL-הבאה:

```
SQL = "SELECT * FROM users WHERE password='1234'"
```

בהנחה שאין בטבלת users רשומה שבה העמודה password מכילה את הערך '1234', לא נוכל לקבל גישה.

אך על ידי הזרקת SQL יכול משתמש זדוני להכניס את הקלט הבא: ' OR 'a'='a שייצר את שאילתת ה SQL-הבאה:

SQL = "SELECT * FROM users WHERE password='' OR 'a'='a'"

על ידי הכנסת "נתון" שהוא למעשה בחלקו נתון ובחלקו קוד מבני של השאילתה, שינה המשתמש את השאילתה לכזו שמחזירה את כל הרשומות בטבלה, משום שהערך 'a' תמיד שווה לעצמו. קוד התוכנית שפועל אחרי הרצת השאילתה יניח שמאחר ותוצאת השאילתה אינה ריקה, יש לאפשר גישה מלאה למשתמש, אף שבפועל אין לו סיסמה תקפה. לפורץ כעת יש גישה כאילו הכניס סיסמה.

דרכי התמודדות למניעת התקפת :sql injection

- סינון נתונים מקיף - באתרי אינטרנט אקטיביים צריך לבדוק את תקינות הקלט לפני שעושים בו שימוש. כדאי לסנן את כל קלט נתוני המשתמש בהתאם להקשר. לדוגמה, בשדה לכתובות דואר אלקטרוני יש לסנן ולאפשר מעבר רק לתווים החוקיים בדואר אלקטרוני, בשדה למספרי טלפון יש לסנן ולאפשר רק למספרים לעבור, וכן הלאה.
- הגבלת הרשאות מסד נתונים להקשר. יצירת חשבונות משתמש עם רמה מינימלית של הרשאות לסביבת השימוש שלהם. לדוגמה, הקוד מאחורי דף כניסה צריך לבצע שאילתת מסד נתונים באמצעות חשבון מוגבל רק לטבלת האישורים הרלוונטיים. בדרך זו, הצלחה בתקיפה באמצעות ערוץ זה לא תאפשר בהכרח פגיעה במסד הנתונים כולו.
- הימנעות מבניית שאילתות SQL עם קלט משתמש – שימוש במנגנונים מובנים לבנית שאילתה סגורה. שימוש בשאילתת SQL לקבלת קלט משתמש עם פרוצדורות מאוחסנות, ללא שימוש בשאילתות פתוחות הנבנות דינמית מקלט המשתמש.
- מניעת היכולת ליבוא קבצים חיצוניים.
- שימוש בחומת אש ליישומי אינטרנט WAF (Web Application Firewall).

כל אחת מהגנות אלו מפחיתה באופן משמעותי את הסיכוי להתקפת הזרקת SQL מוצלחת. יישום כל ההגנות הללו יספק הגנה ברמה טובה מאוד.

trojan data leakage- תקריות של אובדן ודליפת נתונים הופכות לאירוע

אבטחתי כאשר המידע שדלף מכיל נתונים רגישים כגון: פרטים על לקוחות החברה ,מידע פיננסי ,כרטיסי אשראי ועוד. לעיתים, הנתונים שדלפו עשויים להיות בעלי ערך רב ולהירכש על ידי מתחרים וגורמים בלתי מורשים. דליפת נתונים ומידע היא דאגה ביטחונית חשובה במערכות הנוכחיות. מספר טכניקות למניעת דליפת נתונים (DLP) הוצעו בספרות כדי למנוע דליפת נתונים חיצונית כמו גם פנימית. מרבית הפתרונות הללו מנסים להתחקות אחר זרימת נתונים ולבצע בדיקות הרשאות בכדי להבטיח את אבטחת הנתונים ברמת התוכנה והמערכת. פגיעות של דליפות ברמת אדריכלות כמו Spectre ו- Meltdown ניתנות למיתון באמצעות תיקוני תוכנה יקרים לביצועים או באמצעות שינוי הארכיטקטורה עצמה. עם זאת,

פתרונות אלה מניחים כי פלטפורמת החומרה הבסיסית מאובטחת ונטולת התעסקות. HarTBleed, סוג של התקפות מערכת הכוללות חומרה שנפרצה עם טרויאן המוטמע במעבד. אנו מראים כי ניתן להשתמש בהתקפות שנוצרו במיוחד לשימוש בסוס הטרויאני להשגת מידע רגיש ממרחב הכתובות של התהליך. אנו מציעים להשתמש בהדק טרויאני מבוסס קבלים המנצל את הכתובת הווירטואלית של מטמון L1 כדי להפעיל מטען טרויאני המאפס כניסה למאגר התצוגה (TLB) לתרגום יעד כדי למפות בזדון לנתונים רגישים בזיכרון. הדמיית מעגלים מקיפה מציינת כי ההדק הטרויאני המוצע אינו מופעל במהלך בדיקה או פעולה רגילה אפילו במגוון רחב של תנאי תהליך / טמפרטורה. לכן הוא נותר בלתי מזוהה. ניצול מוצלח מבוסס HarTBleed מודגם באמצעות קוד התקפה על ידי הצגת אפקטים טרויאניים בסימולטור GEM5.

קיימות כמה סוגי הדלפות להלן כמה:

זיהוי ומניעת דלף העובר ברשת- הטכנולוגיה מותקנת בנקודות היציאה ברשת ומנתחת את התעבורה כדי לאתר נתונים רגישים שנשלחו תוך הפרה של מדיניות אבטחת המידע.

זיהוי ומניעת דלף מעמדות קצה- הטכנולוגיה מותקנת בתחנות עבודה או בשרתים פנימיים ומנטרת את המידע שעובר בהם. מערכת למניעת דלף מידע מגנה מפני העתקה של קבצים אל מדיה חיצונית, העברה של הנתונים באמצעות הדואר האלקטרוני ותוכנות מסרים מיידיים ועוד. למערכת יכולת בדיקה של מידע שהוצפן על ידי המשתמש. אם הקובץ המוצפן מכיל מידע רגיש, המערכת תחסום אותו ותדווח על כך. יש לשים לב שהודעת דואר אלקטרוני המכילה מידע רגיש שמעולם לא נשלחה, לא תנוטר על ידי המערכת למניעת דלף מידע. לא ניתן להתקין את מערכת למניעת דלף מידע על טלפונים סלולריים ומחשבי כף יד.

מניעת דלף בעת שימוש בנתונים- פעולה זו מתרחשת כאשר המשתמש משתמש בקבצים, מערכות למניעת דלף מידע, מגנות על הנתונים בזמן השימוש ויכולות לנטר ולדווח על פעולות לא מורשות (צילום מסך ,העתקה או שינוי של מידע ,הדפסה ומשלוח בפקס ועוד).

מניעת דלף בעת העברה- פעולה זו מתרחשת כאשר הנתונים עוברים דרך רשת פנימית או חיצונית אל נקודת הקצה. מערכות למניעת דלף מידע מגנות ועוקבות אחר הנתונים הרגישים שמועברים ברשת.

DDOS DNS amplification- התקפות מניעה (DDoS) מאיים

לפגוע בפעילות התקינה של רשת האינטרנט. מדובר בהתקפות שעושות מניפולציה על פרוטוקולי תקשורת נפוצים בכדי לייצר נפחי תעבורה של מאות ג'יגות במטרה למנוע גישה לאתרים ושירותים מקוונים. משבש את תעבורת רשת האינטרנט העולמית באמצעות הצפה של תעבורת נתונים בנפחים שטרם נראו. מדובר במתקפה המכונה "מתקפת הגברה " (Amplification Attack)על פרוטוקול זמן בשם NTP הנחשב לאחד הנפוצים ברשת האינטרנט. בשונה מהתקפת DDoS רגילה, בווקטור החדש מנצלים התוקפים פרוטוקולים ידועים לצורך הגברה של נפח ההתקפה.

ישנן התקפות המשתמשות באותו עיקרון לניצול פרוטוקולי DNS, SNMP או .CHARGEN שרת DNS אחראי על ההמרה בין כתובת IP של אתר לשם (דומיין) שלו. כלומר, כאשר רושמים בדפדפן כתובת של אתר, שרת ה DNS-עושה המרה לכתובת ה IP-שלו. בתהליך הזה נשלחת תגובה משרת ה DNS-ללקוח שרוצה לגלוש לאתר מסוים. ההגברה של תגובת השרת בהתקפות מסוג זה יכולה להגיע למדדים של עד פי 50. גם במקרה זה התגובה היא בפרוטוקול.UDP

לעומת ה DNS-או ה ,CHARGEN-התקפת SNMP היא המסוכנת ביותר מבחינת יכולת ההגברה שלה שיכולה להגיע לפי 650 או יותר מהתעבורה המקורית SNMP .הוא פרוטוקול שאחראי לניהול התקני רשת בכל רשת מחשבים, ולכן מדובר בפרוטוקול נפוץ מאד. כדי לקיים התקפה כזו, התוקף סורק את הרשת למציאת התקנים מארחים (Hosts) העושים שימוש בפרוטוקול, ואז באמצעות זיוף כתובת ה IP-של מקור הבקשה, הוא גורם לאותם מארחים לשלוח את התשובה לכתובת הקורבן.

הפתרון להתקפות אלו היא אכיפת תקינה ושיתוף פעולה בינלאומי, ליישם תקינה ארגון IETF משמש ככוח משימה להנדסה באינטרנט הוציא כבר בשנת 2000 תקינה תחת השם BCP38 שמטרתה למנוע זיופים של כתובות .IP הבעיה היא שכמו כל תקינה, אם לא מיישמים אותה, היא לא שווה הרבה.

פעולה נוספת שאפשר לעשות היא לשתף מידע בצורה גלובלית סביב התמודדות עם התקפות אלו. גם במקרה זה, כמו בסוגים אחרים של מתקפות סייבר, לגיאוגרפיה אין משמעות. שרתים שנמצאים במדינה אחת יכולים לייצר מתקפה בכמה מדינות אחרות. מכאן, שיש צורך ביישום תקינה ואכיפה שלה. בנוסף, יש צורך בשיתוף פעולה גם ברובד המשפטי והטכני. ברובד הטכני מדינה צריכה שתהיה לה את האפשרות 'להוריד' שרתים שמייצרים התקפות כאלו במדינה אחרת בשיחת טלפון. בצורה כזו, ההתקפה יכולה גדע בעודה באיבה לפני שהיא מגיעה לממדים של 400 Gbpsאו יותר. ברובד המשפטי, צריך כלים שיאפשרו סגירת מעגל הפללה מהיר בינלאומי מהרגע שמזהים את יוצר ההתקפה (אם מזהים) ועד הפללת החשודים.

דוגמא להתקפה בפברואר GitHub, 2018 שירות אחסון וניהול קוד הגדול בעולם, היה יעד למתקפת ה DDoS-הגדולה ביותר שנצפתה עד כה: מתקפה בנפח תעבורה של לא פחות מ-1.35 Tbps. כן, 1.35 טרה ביטים. המתקפה התבצעה באמצעות טכניקה הנקראת Attack Amplification, מתקפת הגברה, כלומר התוקפים השתמשו בזיוף כתובות IP ובשירות צד שלישי תמים ותגובותיו לבקשות המזויפות, וכך הצליחו לייצר תנועה עצומה שמטרתה פגיעה מכוונת.

Syn flood- הוא צורה נפוצה של התקפת מניעת שירות (DDoS) שיכולה למקד לכל מערכת המחוברת לאינטרנט ומספקת שירותי פרוטוקול בקרת שידור (TCP) (למשל שרת אינטרנט, שרת דוא"ל, העברת קבצים). Syn Flood הוא סוג של התקפת מצב של מיצוי TCP המנסה לצרוך את טבלאות מצב החיבור הקיימות ברכיבי תשתית רבים, כמו איזוני עומסים, חומות אש, מערכות מניעת פריצה (IPS) ושרתי היישומים עצמם. סוג זה של התקפת DDoS יכול להוריד אפילו מכשירים בעלי קיבולת גבוהה המסוגלים לשמור על מיליוני חיבורים. Syn Flood מתרחש כאשר שכבת TCP רוויה, ומונעת את השלמת three-way handshake TCP בין לקוח לשרת בכל יציאה. בניגוד לסוגים אחרים של התקפות DDoS, התקפות SYD של Syn Flood אינן מתכוונות לנצל את כל זיכרון ה host, אלא למצות את מאגר החיבורים הפתוחים המחוברים ל port, מכתובות IP אינדיבידואליות ולעיתים קרובות מזויפות. Syn Flood נקראים לעתים קרובות התקפות "half-open " מכיוון שמתקפת DDoS מסוג זה מתכוונת לשלוח פרץ קצר של הודעות SYN ל port, ולהשאיר חיבורים לא בטוחים פתוחים וזמינים, ולעתים קרובות מביאים לקריסת שרתים מוחלטת.

דרכי התמודדות עם התקפה זו חומות אש והתקני IPS, למרות שהם קריטיים לביטחון הרשת, אינם מספקים כדי להגן מפני התקפות DDoS מורכבות. מתודולוגיות ההתקפה DDoS המתוחכמות יותר של ימינו דורשות גישה רבת פנים המאפשרת למשתמשים

להסתכל על תשתית אינטרנט וזמינות רשת. חלק מהיכולות שיש לקחת בחשבון להגנה חזקה יותר על DDoS והפחתה מהירה יותר של התקפות TCP SYN flood DDoS כוללות:

תמיכה בפריסה מוטמעת והן בפריסה out-of-band כדי להבטיח שאין נקודת כשל אחת ברשת.

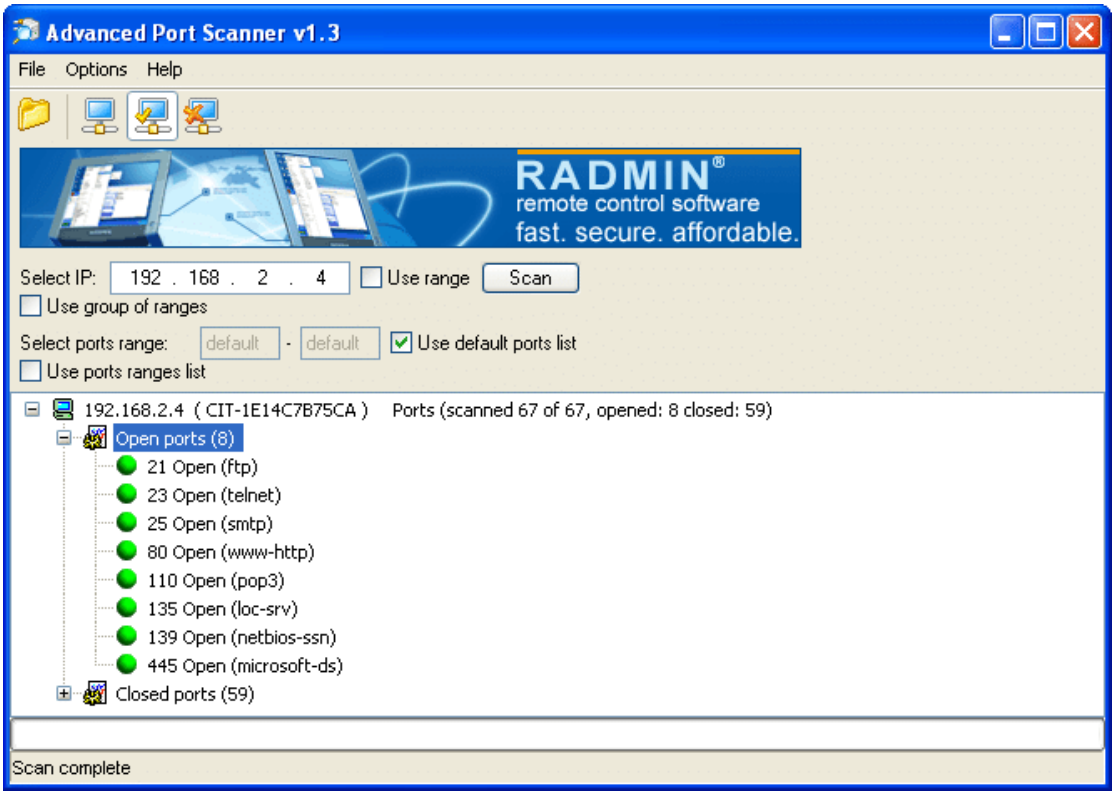
נראות רשת רחבה עם יכולת לראות ולנתח תעבורה מחלקים שונים ברשת

מקורות מגוונים של מודיעין איומים, כולל איתור חריגות סטטיסטיות, התראות סף הניתנות להתאמה אישית וטביעות אצבע של איומים ידועים או מתעוררים במטרה להבטיח זיהוי מהיר ומדויק

מדרגיות לניהול התקפות בכל הגדלים, החל מקצה נמוך (למשל, Gbps1) ועד high-end (למשל, Gbps40).

דוגמה לתקפת TCP SYN flood התוקף ב- host "A" יכול להשתמש בכל כלי סורק port כדי לזהות את רשימת TCP ports הפתוחות אצל ה host הקורבן. לאחר מכן, התוקף יכול לבחור מספר TCP port פתוח אחד ולהשתמש בו כמספר port היעד בחבילות ההתקפה של TCP SYN. לדוגמא, האיור הבא הוא צילום מסך המציג את התוצאה של סריקת port TCP של host היעד "B", באמצעות הכלי Advanced Scanner Scanner (Radmin Port Scanner, 2013):

ישנם 8 יציאות TCP פתוחות במארח "B".



-web defacement

נקרא בעברית השחתת אתר אינטרנט היא תקיפה של אתר אינטרנט שמטרתה, על פי רוב, היא החלפת דף הבית של האתר. השחתת האתר יכולה להיעשות רק בהינתן ההרשאות המתאימות לשינוי תוכן האתר, הרשאות המושגות במרבית המקרים על ידי ניצול פרצת אבטחה באתר עצמו או בשרת המריץ אותו.

כדי להשחית אתר, התוקף משנה את תוכנם של דפים קיימים או מוסיף חדשים. ההשחתה עשויה להיות מאוד ברורה או נסתרת. השחתה תתרחש לעתים קרובות, ובדרך כלל אחרי התקפה על שרת האינטרנט או מערכת ניהול התוכן (CMS) כדוגמת ג'ומלה, וורדפרס ודרופל. למשל: על ידי ניצול לרעה של חולשה במערכת או על ידי פרטי משתמש וסיסמא . השחתה יכולה להתמקד בארגון ספציפי, אבל ברוב רובם של המקרים ההשחתה אינה ממוקדת. השחתה לא ממוקדת המתבצעת אוטומטית בעזרת כלי פריצה יכולה לשנות מספר רב של אתרים בעת ובעונה אחת .השחתתם של מאות אלפי אתרים ברחבי העולם בכל יום היא עניין שבשגרה .השחתה יכולה גם להתבצע גם בדיסקרטיות. תוקף יכול להוסיף או לשנות מאמר אחד באתר חדשות, כך שייקח זמן רב בטרם מישהו יבחין בשינוי, עד אז סביר מאוד שהמסר יועבר. כמו כן, השחתה יכולה להפוך את האתר לנקודת הפצה לתוכנה זדונית.

על פי חוקרי אבטחת מידע מונים מספר סיבות הגורמות להאקר להשחית אתרים:

כאמצעי לקידום מעמדו של ההאקר המבצע בקרב קהילת ההאקרים.

כאמצעי להעברת מסרים אידאולוגים באמצעות האתר המושחת.

כתחביב של האקרים צעירים להשחית אתרים, בדומה לריסוס כתובות גרפיטי בשנות ה-80.

מבצעי ההתקפה הם האקרים, תוקפים לא מנוסים המכונים "סקריפט קידיס" ותוקפי סייבר יבצעו השחתה לרוב רק כי הם יכולים. הם מפעילים תוכנות לסריקה האינטרנט בחיפוש אחר אתרים פגיעים ויחליפו את דף הבית עם דף משלהם במה שמכונה "השחתה המונית". צורה זו של השחתה היא סוג של גרפיטי דיגיטלי שבו האקר משאיר מאחור את החתימה (Tag) שלו, אקטיביסטים כדוגמת קבוצות אנונימוס או האקרים כמו הצבא הסורי האלקטרוני מבצעים השחתת אתרים במדינה מסוימת או בארגונים ממגזר מסוים כדי להפיץ את המסר האידיאולוגי שלהם או כדי לפגוע במתנגדיהם.

במרדף אחר רווח כספי פושעי סייבר ישחיתו אתרים ויפיצו תוכנות זדוניות על מנת לגנוב פרטים התחברות אישים או לחבר אותם לבוטנט (botnet). גם כאן, התוקפים ינסו לבצע זאת בדיסקרטיות בכדי שהאתר יישאר פרוץ זמן רב ככל האפשר מבלי להתגלות. תופעה נוספת המתרחבת כרוכה בהצבת פרסומות נגועות בתוכנות זדוניות באתרים תמימים. לבסוף, יש מקרים שבם עובדים לשעבר ממורמרים ישחיתו בזדון את האתר של המעסיק אצלו הועסקו. הם מסוגלים לעשות את זה כי יש להם עדיין את שמות המשתמשים והסיסמאות שהם צריכים כדי לשנות את אתר האינטרנט בקלות.

דרכי התמודדות/מניעה של התקפה זו, למרות שאף פעם לא ניתן לשלול לחלוטין את הסיכוי להשחתת האתר, ישנם אמצעי מניעה שונים שניתן לנקוט כבעליו של האתר (או באמצעות הספק) כדי להפחית את הסיכון לפגיעה באופן משמעותי.

לוודא כי השרת מוקשח ואין בו שירותים (Services) מיותרים.

להקפיד להתקין את התיקונים האחרונים ועדכוני אבטחה המופצים למערכת.

לבדוק באופן קבוע שהמערכת מעודכנת לגרסה האחרונה

לבדוק קיומם של תוכנות זדוניות

לא להשתמש בחשבונות וסיסמאות סטנדרטיים למערכות ההפעלה או ה- CMS

למחוק מיד את חשבונות המשתמש של עובדים שעזבו את הארגון או שאינם זקוקים לגישה למערכת ניהול התוכן או שרת האינטרנט

להתקין חומת אש ולסנן את תעבורת הרשת לדפוסים חשודים

להגביל את מספר כתובות ה IP שיכולות לקבל גישה לשרת ומערכת ניהול התוכן

חיבור ל CMS יעשה רק באמצעות חיבור TLS מאובטח.

היכן שאפשרי, לאבטח את הגישה לשרת האינטרנט ומערכת ניהול התוכן עם מערכת אימות כפול)-2 factor authentication(.

לסרוק באופן קבוע את רמת האבטחה של האתר, באמצעות סורקים אוטומטיים. לתאם זאת מראש עם מנהל האתר או בעלים, כך שזה לא יראה כניסיון תקיפה.

הצגת מדיניות גילוי נאות, כך שנקודות תורפה שימצאו באתר האינטרנט ידווחו בסודיות, זה יאפשר גילויים ותיקונם של חולשות טרם שינוצלו על ידי גורמים זדוניים.

במידה והאתר מתארח אצל ספק חיצוני, חשוב להגדיר עמו מדיניות ברורה בדבר אבטחת האתר.

דוגמא להתקפות השחתת אתרים היא מתקפת סייבר על האינטרנט בישראל כ-150 אלף אתרים המבוססים על פלטפורמת UPress עברו הבוקר השחתה .(Defacement) מי שנכנס לאתרים האלו רואה את ההודעה: "הספירה הפוך (הכוונה הספירה לאחור, א"ז) להרס ישראל נתחל מלפני הרבה זמן". בין היתר מוצגת תמונה של מסגד אל אקצה. בין האתרים עליהם השתלטו האיראנים נמצא האתר של הגוף המתאם של קרן ההלוואות בערבות מדינה.

בנוסף, ובוודאי אם האתר או תדמיתו של הארגון חשובה במיוחד או שקיים סיכון גבוה מהממוצע להשחתה, ניתן לשקול :ביצוע בדיקות חדירות תקופתיות לאיכות האבטחה של אתר האינטרנט ולתקן כל חולשה שזוהתה כדוגמת פגיעות. XSS בנוסף יש ליישם מערכת זיהויי חדירה(IDS(כדי לאתר פעילות חשודה מוקדם ככל האפשר.

תשובות מטלה מתקפות סייבר

1. ddos ברוחב פס גבוה- פתרונות אבטחת מידע סטנדרטיים כדוגמת חומת אש (FireWall) או התקני IPS (Intrusion prevention System) המותקנים בארגון מתקשים להגן היום על הארגון מאחר ונפחי התעבורה המגיעים בעת התקפת מניעת שירות הינם בעלי רוחב פס גדול הרבה יותר מרוחב הפס הקיים בארגון

Ddos מוגבר התקפה זו היא הניסיון לגרום לשרת, אתר אינטרנט או שירותים אחרים להפוך ללא זמינים על ידי ניצול מרבי של אחד מהמשאבים של השירות לדוגמא : מעבד, זיכרון, רוחב פס. הסיבה שקוראים להתקפות האלו התקפת מניעת שירות מבוזרת מכיוון שתנועת הגולשים המזויפת מגיעה מכמות עצומה של מחשבים שונים. התקפות DDoS משתמשות

ב Botnet - שהוא אוסף של הרבה מחשבים או מכשירים בעלי אפשרות גלישה באינטרנט הנשלטים מרחוק בעזרת תוכנות זדוניות בכדי לבצע מתקפה. המטרות להתקפות מניעת שירות הן לצורך שעשוע, דרך פשיעה, עבור בטרור וכלה בלוחמת סייבר.

ddos ברוחב פס נמוך תקיפות כנגד שכבת האפליקציה הינן בעלות רוחב-פס נמוך, קשות לזיהוי ומכוונות הן כנגד לקוחות והן כנגד שירותי התמיכה הנלווים של מפעילי הרשת, דוגמת DNS, HTTP, WEB Services :ועוד.

2. בדיקת Fuzzing היא טכניקת שעושה בדיקת תוכנה אוטומטית כאשר יש בה אספקת נתונים לא חוקיים, בלתי צפויים או אקראיים. לאחר מכן יש מעקב אחר התוכנית בשביל לאתר חריגים כגון קריסות, קביעות קוד מובנות כושלות או דליפות זיכרון אפשריות. בדרך כלל משתמשים Fuzzing לבדיקת תוכניות שלוקחות תשומות מובנות .

3. התקפת SQL injection מורכבת מהכנסה או "הזרקה" של שאילתת SQL דרך נתוני הקלט מהלקוח ליישום. התקפת הזרקת SQL מוצלחת יכולה לקרוא נתונים רגישים מהמאגר כגון סיסמאות, פרטי כרטיס אשראי או מידע אישי על המשתמש, לשנות את נתוני בסיס הנתונים ולבצע פעולות ניהול במסד הנתונים ובמקרים מסוימים מוציאים פקודות למערכת ההפעלה.

4. זוהי אחת ההתקפות הנפוצות כיום שתוקפת משתמשי אתרי אינטרנט על ידי הסתננות לתוך יישום האינטרנט. ההתקפה פוגעת בפרטיות הגולש כאשר פרטיו נגנבים או מטופלים על ידי גורמים עבריינים. בהתקפת XSSיש שלושה צדדים: התוקף, הקורבן והאתר האינטרנט. במהלך ההתקפה סקריפטים זדוניים מוזרקים לתוך האתרי האינטרנט והתוקף מצליח לעלות קוד זדוני הפועל בצד הדפדפן וקוד זה מורד ומופץ בדפדפנים של קורבנות.התקפה כזאת מתאפשרת במקום בו יישום האינטרנט משתמש בקלט משתמש ללא אימות ואינו מזהה שהועלה לאתר קוד ולא נתונים כקלט הקורבן לא מודע שנשלח אליו סקריפט זדוני שיכול לגשת לכל העוגיות הנשמרות בדפדפן ויכול להגיע לכל מידע רגיש שנשמר על הדפדפן מול האתר המותקף.

5. phishing בדואר- נעשה בדרך כלל בדואר זבל אלקטרוני, כלומר באמצעות פנייה למספר רב מאוד של נמענים, כך שמבחינתו של השולח, אחוז קטן מאוד של נופלים בפח כדי להשיג את המטרה. הפנייה בהודעות אלה בדרך כלל אינה אישית (למשל: "לקוח יקר"), אך לעיתים מתבסס השולח על רשימת שמות שנפלה לידיו, כגון רשימת כל העובדים או הלקוחות בארגון מסוים, ופונה באופן אישי לכל נמען, צעד המגביר את אמינותה של הודעת PHISHING . בנוסף, לעיתים מציין השולח כתובות ושמות של חברות, ארגונים ואנשים אמיתיים (שמות וכתובות של משרדי עורכי דין, מספרי חשבון בנק אמיתיים) לצורך הגברת אמינות ההודעה.

6. phishing מאקרו- שימוש בקובץ וורד המצורף להודעת אימייל, אשר בכדי לקרוא את תוכנו מתבקשים הנמענים לאפשר הפעלת מאקרו. מרגע ההפעלה מתחיל באופן מידי תהליך של התקנת קוד עויין מסוג סוס טרויאני על המחשב. הודעת האי-מייל נראית כהודעה פנים ארגונית תמימה, אשר מכילה צרופה (Attachment)בקובץ וורד אשר שמו Financial Statement.doc. לאחר שמורידים את הקובץ ופותחים אותו לצפייה התוכן נראה מטושטש ובלתי קריא, ובראש הדף מופיעה הודעה אשר מציינת כי הטקסט טושטש במכוון לצורך אבטחה, ובמידה ומעוניינים לקרוא את המסמך ולהסיר את הטשטוש יש לאפשר הפעלת מאקרו במסמך ע"י לחיצה על הכפתור המתאים בוורד, אשר נמצא מתחת לסרגל הכלים.

7. phishing העתקת אתרים- לחיצה על הקישור עשויה להוביל משתמש לדף מזויף הנראה כמו דף של אתר לגיטימי. כאשר המשתמש מכניס את פרטיו הדף מפנה אותו באופן אוטומטי לאתר האמיתי ומכניס עבורו את הפרטים כך שהמשתמש אינו יודע שמסר את פרטיו לאתר מזויף.

9. התקפת התאום המרושע- התקפת תאומים מרושעת היא התקפת גרזן שבה האקר מקים רשת Wi-Fi מזויפת שנראית כמו נקודת גישה לגיטימית לגנוב פרטים רגישים של הקורבנות. לרוב, הקורבנות של התקפות כאלה הם אנשים רגילים כמוך וכמוני. ההתקפה יכולה להתבצע כהתקפת אדם באמצע (MITM). נקודת הגישה המזויפת של Wi-Fi משמשת לציתות למשתמשים ולגנוב את אישורי הכניסה שלהם או מידע רגיש אחר.

10. התקפת הרעלת ARP- שיטה לפריצה של רשתות Ethernet שנותנת אפשרות לפורץ לנטר את הנתונים שעוברים ברשת המקומית או לעצור את התעבורה. העיקרון של ההתקפה הוא לשלוח הודעות ARP מזויפות ברשת המקומית שמכילות כתובות MAC שקריות ובכך מטעה משאבי רשת וגורם לתעבורת המידע לעבור בתצורה שונה מהמקור. לדוגמה ברשת ניתן לקבוע Gateway למחשב קצה ותחת פעולה זו לאלץ את המחשב להאמין כי הכתובת המדומה החדשה תואמת את ה-Gateway המקורי ובכך התעבורה היוצאת תישלח אל המחשב בעל הכתובת המזויפת, כך הוא יכול לבצע פעולות ניטור לרשת ובכך לחשוף מידע רב העובר בתצורה בלתי מוצפנת ברשת. העמדה המזויפת יכולה לאחר מכן להעביר את השדרים אל התחנה האמיתית ובכך להטמיע את עצמה בצורה שקופה למשתמש או לחלופין לגרום לכלל התעבורה להינתב למיקום רשת אחד ובכך להעמיס על משאביו ולגרום לקריסתו (התקפת מניעת שירות - Denial of Service).

11. התקפת הרעלת DNS- תקיפת הרעלת DNS או הרעלת מטמון DNS היא תיאור לתקיפה שבאמצעותה המחשב המותקף מופנה על ידי שרת DNS אל כתובת איי-פי (IP) פיקטיבית. לרוב תקיפה זו היא תקדים לתקיפת פישינג. תקיפת הרעלת DNS מתבצעת בשני שלבים וישנן שתי שיטות עיקריות לביצוע השלב הראשון של תקיפת הרעלתDNS :

התוקף מקים שרת DNS פיקטיבי ופונה אליהם דרך פורט תקשורת לוגי UDP 53/מחכה לפניות ממחשבים.

התוקף חודר אל שרת DNS ומשחית רשומות NS קיימות כדי שמחשבך יופנה אל אתר פיקטיבי.

12. היא נוזקה שמגבילה גישה למערכות המחשב הנגוע בדרך מסוימת, ומשמשת לסחיטה מהמשתמש תשלום כסף (דמי כופר) כדי שתוסר מגבלת הגישה. חלק מתוכנות הכופר מבצעות הצפנה לקבצים על הכונן הקשיח, וכך הופכות את תהליך הסרת ההצפנה לקשה מבלי לשלם כופר עבור מפתח ההצפנה,. לרוב, חודרת תוכנת הכופר למחשב כסוס טרויאני, המוסווה כקובץ תמים.

דוגמא להתקפת וירוס כופר שנעשתה לאחרונה היא על חברת שירביט חברה גדולה לביטוח במדינת ישראל קישור לכתבה:

https://13news.co.il/item/news/tech-digital-science/cyber-attack-on-israeli-company-1171086/