**תרגול סגור: סייבר- SHAMOON**

**1. ש**אמון הוא פוגען. מדובר בווירוס שנועד להרוס את הכונן הקשיח המחשב על ידי מחיקת ה- MBR (רשומת האתחול הראשית אשר מכילה את רצף הפקודות הנדרשות לאתחול מערכת). Shamoon לא רק מרגל אחר מערכות נגועות, הוא גם הופך אותן לבלתי ניתנות להפעלה על ידי השמדת מערכות חיוניות.

**2.** אלו הם שלושה מרכיבים אשר בהם הפוגען Shamoon משתמש כדי לתקוף מחשב. לכל מרכיב שכזה יש תפקיד שונה:

1. dropper- תפקיד המרכיב הוא ליצור שירות מתמיד על המחשב שנתקף. הוא יכול להופיע בשתי גרסאות (32 או 64 ביט). הוא מופיע בגרסה המסוימת בהתאם למה שמגלה במחשב שתוקף. ה- dropper מעתיק את עצמו לרשתות נוספות אליהן המחשב מחובר על מנת להפיץ את הקוד הזדוני. הוא חודר למערכת המחשב הנתקף, לעתים קרובות תוך שימוש בהנדסה חברתית או ניצול חולשות במערכות. ברגע שנכנס למערכת, הוא מאתחל את שאר הרכיבים של הפוגען.

2. wiper- זהו מרכיב שמפעיל מרכיב נוסף בשם Eldos driver (= זהו סוג של התקן שיוצר אינטראקציה עם קבצים, דיסקים וכו' ומאפשר שינוי ישיר של נתונים בכונן הקשיח של המחשב). ה-wiper מחליף באופן שיטתי קבצים עם נתונים אקראיים, דבר שהופך אותם לבלתי ניתנים לשליפה. בנוסף, הוא מאתחל את ה-MBR, מה שהופך את המערכת כולה לבלתי פעילה ומאתגרת לשחזור. כמו כן, ההתקן מאפשר למשתמש גישה לכונן הקשיח של המחשב הנתקף ללא שימוש ב- windows APIs (= מאפשר לתוכניות שהמשתמש כתב לקיים אינטראקציה עם windows).

3. reporter- מרכיב נוסף בו משתמש הפוגען. הוא אחראי ליצור תקשורת עם שרת הבקרה והשליטה (שאותו התוקפים מפעילים בעצמם). הוא מעביר נתונים על המערכת הנגועה, עוקב אחר התקדמות התקיפה ואף עשוי לקבל הנחיות נוספות.

**3.** המתקפה ב2012 הייתה בערב הסעודית, על גופים השייכים לתעשיית האנרגיה. המתקפה פגעה בחברת הנפט הלאומית של ערב הסעודית, הנקראת Aramco ובחברת אנרגיה נוספת בשם Rasgas. הסיבה לתחילת המתקפה הייתה תקיפה לשם גמול על פשעים שהסעודים ביצעו במדינות השכנות באזור, כמו סוריה ולבנון.

**4.** קבוצה בשם "the cutting sword of justice" (בעברית- "חרב החיתוך של הצדק") לקחה אחריות על המתקפה. על פי החשד, האחראים על המתקפה קשורים לאיראן. החשד הוא שאיראן ביצעה את המתקפה כסוג של נקמה על מחויבותה של Aramco הסעודית לייצר יותר נפט על מנת לשמור על האספקה ​​במהלך אמברגו (=חרם כלכלי, הגבלה) ארה"ב-האיחוד האירופי נגד איראן.

**5.** הפוגען יכול לרוץ על מחשבים בעלי מערכת הפעלה windows. החל מ- windows XP ועד windows 10. העובדה שShamoon רץ על מחשבים עם מערכת הפעלה של windows בלבד, פוטנציאל ההתקפה שלו נרחב. זאת משום שמערכת ההפעלה windows נפוצה מאוד הן בסביבות ארגוניות והן בסביבות אישיות.

**6.** Ransomware זוהי תוכנה זדונית המצפינה קבצים במחשב ומונעת גישה אליהם, וכדי להסירה דורשים התוקפים תשלום כופר. הדבר מתקשר למתקפה של הפוגען Shamoon בכך שבניגוד לransomware (תוכנת כופר), מטרתו של הפוגען Shamoon אינה להשיג כופר מסוים (פיצוי כספי) אלא רק לרגל, להרוס ולשבש את המערכת של המחשב הנתקף.

**7.** לפי הממצאים של X-Force IRIS, נקודת הכניסה הראשונית שבה השתמשו התוקפים הייתה מסמך המכיל מאקרו זדוני (מאקרו= תוכנה שמאפשרת למשתמש להגדיר סדרת פקודות הניתנת למחשב כפקודה אחת) שכאשר הופעל, אפשר תקשורת C2 (= זוהי צורה של מתקפת סייבר בה התוקף עושה שימוש בשרת כדי לתת הוראות למחשבים שנפגעו על ידי תוכנה זדונית דרך רשת ולקבל נתונים שנגנבו מרשת היעד לשרת התוקף) באמצעות PowerShell (= סביבת עבודה של מיקרוסופט).

פרט למסמך התגלו גם מסמכים זדוניים ועמוסי PowerShell נוספים, כאלה המכילים בתוכם קורות חיים ומסמכי משאבי אנוש, שחלקם קשורים לארגונים בסעודיה.

**8.** שלבי התקיפה:

1. התוקפים שולחים מייל לעובדי הארגון אותו מעוניינים לתקוף (Phishing). המייל מכיל בתוכו מסמך של Microsoft Office כקובץ מצורף.

2. פתיחת הקובץ המצורף מהמייל מפעילה את PowerShell ומאפשרת גישה בשורת הפקודה למחשב שנפרץ.

3. בשלב זה התוקפים מסוגלים לתקשר עם המחשב שנפרץ ולבצע בו פקודות מרחוק.

4. התוקפים משתמשים בגישה שהשיגו כדי לפרוס כלים נוספים ותוכנות זדוניות לנקודות קצה אחרות או להשיג הרשאות נוספות ברשת.

5. התוקפים לומדים את הרשת על ידי חיבור למערכות נוספות ואיתור שרתים חשובים.

6. התוקפים פורסים את התוכנה הזדונית של Shamoon.

7. מתחילה התפרצות מתואמת של Shamoon:

א. ראשית מרכיב הdropper מופעל וברגע שהוא בפנים הוא מפעיל את שאר המרכיבים.

ב. מרכיב ה- wiper ומרכיב ה- reporter מופעלים.

8. הכוננים הקשיחים של המחשבים בארגון המטרה נמחקים לצמיתות.

**9.**

1. החברות הנפגעות היו יכולות להעלות את המודעות בקרב העובדים לסכנות שבפתיחת מיילים וקבצים לא מוכרים ואף לבצע השתלמויות או אפילו הרצאות העוסקות בPhishing ובמתקפות סייבר באופן כללי. הרי במידה והעובדים לא היו פותחים את הקבצים שנשלחו אליהם במייל, התקיפה לא הייתה מצליחה להתבצע. כל חברה/ ארגון המחזיק בפוזיציה משמעותית ונחשקת (כמו אנרגיה למשל) חשוף למתקפות סייבר ואני חושבת שהחברות הנפגעות היו צריכות להיות מודעות לסכנה ולהכין גם את העובדים שלהן.

2. צעד נוסף בו היו יכולות לנקוט החברות הנפגעות הוא עדכוני אבטחה שוטפים למערכת שלהם וגיבוי מידע מתמיד.

**10.** במסגרת תפקיד הreporter נוצרת תקשורת עם השרת של התוקפים. יכול להיות שבאמצעות מרכיב הreporter אפשר למצוא את כתובת הIP של השרת של התוקפים וכך לדעת מה מקור התקיפה (מיקום גאוגרפי) ולהפסיק אותה מהר ככל הניתן.