# הנדסה לאחור

# מטלה 2

# WannaCry

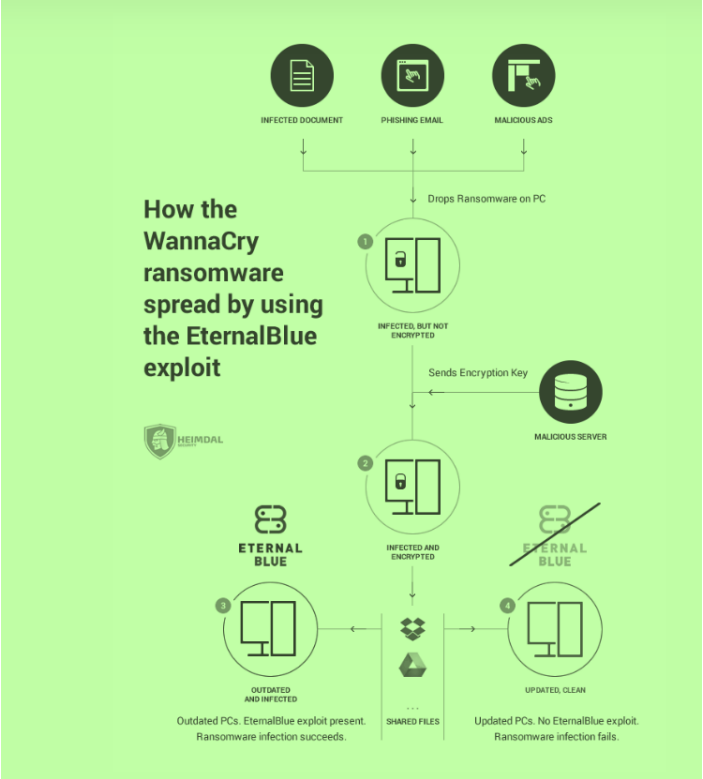
תוכנה הכופר WannaCry היא שמה של תוכנת כופר שהופיעה לראשונה בפעולה במהלך מתקפת ענק על מספר מדינות בתאריך 12.5.17.
על-פי דיווחים שונים מספקי אבטחה, כמאות אלפי מערכות במעל ל-150 מדינות נפגעו פגיעה קריטית. הפגיעה השפיעה ישירות על ישויות רבות שבהן מערכות ביראות, ממשלות, המדיות, ואפילו יצרני גז.
הקושי בהתגוננות מפני תוכנת הכופר WannaCry הוא בגלל יכולתה להתפשט למערכות אחרות בעזרת "רכיב תולעת" (באנגלית: worm component). יכולת זו הופכת את ההתקפה ליותר קטלנית ולכן דורשת טכניקת הגנה שיכולה להגיב בזמן אמת. בנוסף, לתוכנת כופר זו יש רכיב הצפנה שמבוסס על מפתח קריפטוגרפיה ציבורי.
במהלך תהליך התקיפה, תוכנת הכופר WannaCry משתמשת בפרצות הנקראות EternalBlue ו-DoublePulsar שלכאורה הודלפו בשלהי אפריל 2017 על-ידי קבוצה הנקראת The Shadow Brokers.
הפרצה EternalBlue מנצלת את החולשה שיש ל-SMB (server message block) שיושמה על-ידי מייקרוסופט בתאריך 14.3.17 ושתוארה כאבטחת MS17-010. חולשה זו מאפשרת לפורצים להפעיל קוד מרחוק על המערכות שהורעלו על-ידם בכך שהם שולחים הודעה מותאמת אישית לשרת ה-SMB v1 המתחברת לפורטי ה-TCP מספר 139 ו-445 של מערכות WINDOWS שעליהן לא יושמה באבטחה שצוינה לעיל.
במיוחד, חולשה זו משפיעה על כל המערכות WINDOWS שעליהן לא יושמה האבטחה שלעיל החל מ-WINDOWS XP ועד ל-WINODWS 8.1 (ללא WINDOWS 10).
הפרצה DoublePulsar היא "דלת אחורית קבועה" (סוג של פרצה שנועדה במקור עבור מפתחי המערכת המקוריים כדי שתהיה להם גישה מאזור סודי במערכת) שכנראה מיודעת למטרת גישה וביצוע לפועל של קוד על מערכות סודיות קדומות, ולכן דבר זה מרשה לתוקפים להתקין עוד תוכנות זדוניות על המערכת.
במהלך תהליך ההפצה, רכיב התולעת של WannaCry משתמש ב-EternalBlue כדי להתחיל את תהליך "ההרעלה" באמצעות חולשת ה-SMB שהוזכרה לעיל, על-ידי כך שבאופן אקטיבי בודק פורטי TCP מתאימים ובמידה והצליח, מנסה לפרוץ באמצעות הדלת האחורית ששמה DoublePulsar שהוזכרה מקודם על המערכות שהורעלו.
תוכנת הכופר WannaCry נכתבה בשפת ה-C++.

| WannaCry components | |
|---|---|
| | Worm component |
| MD5 | db349b97c37d22f5ea1d1841e3c89eb4 |
| SHA1 | e889544aff85ffaf8b0d0da705105dee7c97fe26 |
| SHA256 | 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c |
| File type | PE32 executable (GUI) Intel 80386, for MS Windows |
| | Encryption component |
| MD5 | 84c82835a5d21bbcf75a61706d8ab549 |
| SHA1 | 5ff465afaabcbf0150d1a3ab2c2e74f3a4426467 |
| SHA256 | ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa |
| File type | PE32 executable (GUI) Intel 80386, for MS Windows |

רכיב התולעת

# התפשטות הנוזקה

רכיב התולעת של תוכנת הכופר WannaCry אחראי על עיקר ההתפשטות והפרצה, הוא זה שמפיק את היכולת של פרצת ה-EternalBlue והדלת האחורית הנקראת DoublePulsar על-מנת לנצל את חולשת ה- MS17-010 SMBשהוזכרה במסמך זה.
לאחר ביצוע ההתקשרות ההתחלתית ובדיקת החיבור עם דומיין ה-KillSwitch (זהו דומיין להשבתת מערכת), יכולת רכיב התולעת מתבצעת על-ידי התחלת שירות שנקרא mssecsvs2.0 service אשר מותקן לאחר שתוכנת הכופר WannaCry מופעלת.
השירות מנסה לפזר את ה-payload של ה-WannaCry באמצעות חולשת ה-SMB על כל מערכת פגיעה הן ברשת הפנימית והן ברשת החיצונית. כדי לבצע תהליך זה, תוכנת הכופר WannaCry יוצרת ושולחת 2 איומי תוכנה נפרדים שבו-זמנית שתיהן מבצעות שכפול של ה-payload של רכיב התולעת בכל הרשתות שזוהו.
ברשת הפנימית, לפני תחילת תהליך ההתפשטות, רכיב התולעת משיג את כתובות ה-IP של ממשקי הרשת הפנימית על ידי הפעלת פונקציה שנקראת GetAdaptersInfo ומוצאת את כל ה-subnet-ים הקיימים ברשת. לאחר מכן, רכיב התולעת מנסה להתחבר לכל כתובות ה-IP הקיימות בכל רשת אפשרית שנמצאת בפורט 445 שהוא הפורט שנקבע כברירת-מחדל עבור ה-SMB לשירותי ה-IP. במידה ורכיב התועלת הצליח, הוא מנסה לפרוץ את השירות הנ"ל בעזרת חולשת ה-MS17-010.




תיאור תהליך התקיפה

# מי הם

# Shadow Brokers?

קבוצת ה-Shadow Brokers היא קבוצת האקרים שנודעה לראשונה בשנת 2016 כאשר היא התחילה לשחרר פרצת קוד שלכאורה נלקחו מ-NSA.
נראה כי פרצת הקוד נוצרה בשנת 2013 לאחר חשיפת מידע חסוי מ-NSA על ידי אדם ששמו הו אדוארד סנאודן.
קבוצת ה-Shadow Brokers שחררה את EternalBlue לציבור כחלק מההדלפה החמישית של קוד מסווג בשלהי אפריל 2017. הקבוצה הנ"ל טענה שהיא לכאורה גנבה בנוסף ל-EternalBlue גם פרצות אחרות וכלי תקיפת סייבר אחרים מ-NSA הקשורים לקבוצת Equation (קבוצת האקרים מסוכנת מאוד).
פעולה זו, שמה את ה-NSA לבושה בעיני הציבור ופגעה קשות ביכולות איסוף המידע שלה ובאותו זמן נתנה גישה לכלי תקיפת סייבר לכל מי שחפץ בכך.
הקבוצה חשפה חולשות קריטיות מאוד ב:

- ראוטרי CISCO
- Microsoft windows
- שרתי המייל של לינוקס

הפגיעה בישויות הנ"ל זעזע את החברות שישויות אלו בבעלותן ואת לקוחותיהן.

# האשמה היא מדינת קוריאה הצפונית

חוקרי אבטחה בחברת Symantec ובחברות אחרות קישרו לראשונה את תולעת ה-WannaCry לקבוצה הנקראת Lazarus. זוהי קבוצת האקרים זדונית הקשורה ישירות לממשלת קוריאה הצפונית. בשלהי דצמבר 2017, הבית הלבן שבארצות הברית הצהיר רשמית את הקשר של תקיפות WannaCry לקוריאה הצפונית. ניתן לראות בבירור שניתוח הקוד אכן תרם לזיהוי יוצרי הנוזקה, אך לא ברור איזו גרסה זו הייתה של הנוזקה שדלפה.
קבוצת ה-Lazarus היא קבוצת האקרים הידועה לשמצה וגם תת-הקבוצות שלה הנקראות Bluenoroff ו-Andariel , שייכות שלושתן ל-RGB, משרד המודיעין המרכזי של קוריאה הצפונית. ביחד, שלושת החברות פגעה בישויות וחברות אמריקאיות עם עשרות מתקפות סייבר זדוניות הכוללות באופן נרחב מתקפות של תוכנות כופר זדוניות, גניבות מידע ואפילו גניבה של 571 מיליון דולר במטבעות וירטואליים (כדוגמת הביטקוין) בעזרת רק 5 מתקפות.
קבוצת האקרים Lazarus הופיעה בתחילת 2010 וידועה בעיקר עבור זאת שהיא עמדה מאחורי המתקפה נגד Sony Pictures Entertainment שהתרחשה ב-2014 ועבור קשריה למתקפה הגלובלית של WannaCry שהתרחשה ב-2017.
קבוצת Bluenoroff הייתה זאת שאחראית לגניבת 80 מיליון דולר מחשבון הבנק של מדינת בנגלדש בניו-יורק על-ידי גניבת פרטי אשראי. קבוצה זאת השתמשה המון בניסיונות פישינג ופרצות של דלתות אחוריות במטרה לתקוף מקורות פיננסיים. לפי הדיווחים, בשנת 2018 ניסתה חברה זו לגנוב יותר ממיליארד דולרים ממכונים פיננסיים.
תת-הקבוצה השנייה שקראת Andariel שהופיעה לראשונה בשנת 2015 ושמה לה למטרה לתקוף את קוריאה הדרומית על-ידי אספת מידע ויצירת כאוס. הקבוצה הנ"ל ניסתה לגנוב מידע של כרטיסי אשראי על-ידי פרצות לכספומטים ולמשוך משם כסף או לגנוב מלקוחות פרטים כדי למכור אותם לשוק השחור. הקבוצה פיתחה בנוסף תוכנת תקיפה זדונית כדי לתקוף אתרי הימורים ומשחקי פוקר על-מנת לגנוב משם כסף. עד כמה שידוע כיום, אין הערכה להיקף ההשקעה בפיתוח התוכנה.

# איך המתקפה נעצרה?

חוקר אבטחה מבריטניה בשם מרקוס הוטצ'ין גילה שהוא יכול להפעיל את הטריגר שנועד לכבות את תוכנה הכופר בכך שהוא צריך להירשם לרשת הדומיין ולפרסם שם דף אינטרנט. במקור, מרקוס הוטצ'ין רצה לעקוב אחר הפצת תוכנת הכופר דרך הדומיין שאליו התוכנה מתחברת, אך הוא גילה במהרה שהרישום לדומיין הפסיק את הפצת תוכנת הכופר.

# קישורים שדרכם הגענו לנוזקה


- https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
- https://searchsecurity.techtarget.com/definition/wannacry-ransomware
- https://research.checkpoint.com/eternalblue-everything-know/
- https://heimdalsecurity.com/blog/security-alert-wannacry-computers-vulnerable/
- https://www.europol.europa.eu/wannacry-ransomware
- https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/
- https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack