פרויקט בכופרה 236499

RANSOMWATCH

SPRING 2019

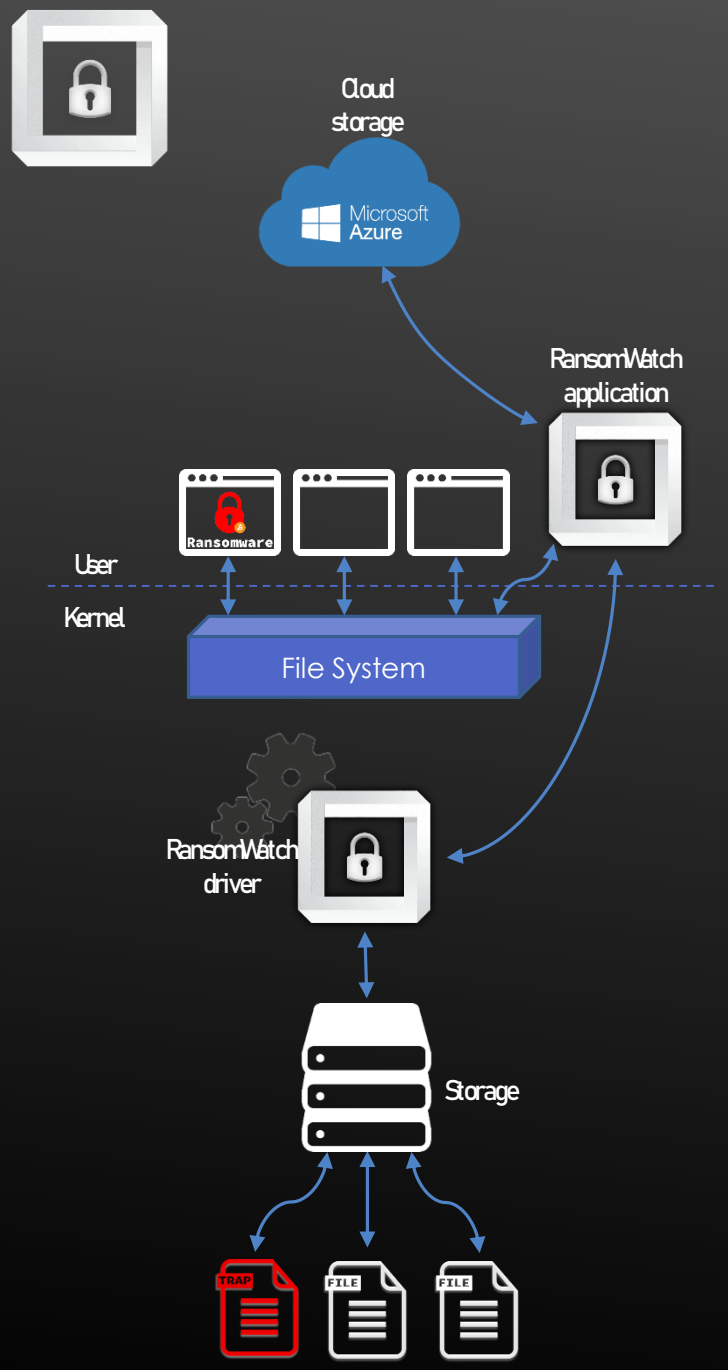
מגישים: רפאל וורף ואביעד גפני

מנחה: אסף רוזנבאום

RANSOMWATCH

- פתרון לתוכנות כופרה בנקודת קצה.
- מזהה ומנטרל כופרות בזמן אמת על ידי ניטור פעילות במערכת.
- מגבה קבצים מוגנים לגיבוי ענן.
- לאחר זיהוי של כופרה, משחזר קבצים בהם הכופרה פגעה.

אופן עבודת הפתרון



- מחולק לשניים: דרייבר ואפליקציה
- הדרייבר אחראי על איסוף פעילות של אפליקציות מול המערכת, עצירת תהליכים זדוניים ומעקב אחר יצירת תהליכים.
- האפליקציה אחראית על הגדרת האזורים המוגנים, ניתוח פעילות, גיבוי אזורים מוגנים ושחזור במקרה של זיהוי.

אופן עבודת הפתרון

- בתחילת העבודה משתמש מגדיר אזורים עליהם הוא רוצה להגן, אזורים אלו מגובים וניתן לבצע להם שחזור.
- באזורים מוגנים אנו יוצרים קבצי מלכודת בהתאם לקבצים הנמצאים בתיקיות.
- מעקב אחר פעילות נעשה ברמת אפליקציות.

אופן עבודת הפתרון

1. לכל אפליקציה שמבצעת פעולה מול מערכת הקבצים (כגון קריאה, כתיבה, פתיחה, מחיקה ועוד) באזור מוגן:
    1. אסוף מידע אודות הפעולה.
    2. העברת הפעולה לניטור ולבניית תמונת מצב של אפליקציה.
    3. ניתוח תמונת המצב החדשה.
    4. קבלת החלטה האם האפליקציה זדונית:
        1. עבור אפליקציה זדונית מתבצע ניסיון עצירה וניסיון שחזור של קבצים שנפגעו.
2. המתנה לפעולות נוספות וחזרה לשלב 1.

זיהוי

- דינאמי, נעשה לפי מדדים הלוקחים בחשבון התנהגות של אפליקציות.
- שילוב של מספר מדדים גורר זיהוי של אפליקציה כזדונית.
- נעשה שימוש במלכודות לשיפור יכולת הזיהוי, לפעולות על המלכודות משקל רב יותר.
- מתאים לכופרות מסוגים שונים.

זיהוי

מדד	תיאור	רציונל
מחיקת קבצים	מספר הקבצים שנמחקו ביחס למספר הקבצים המוגנים והקבצים אליהם האפליקציה ניגשה.	כופרות רבות מוחקות את הקבצים המקוריים לאחר הצפנה
יצירת קבצים	מספר הקבצים שנוצרו ביחס למספר הקבצים אליהם האפליקציה ניגשה .	כופרות רבות כותבות קובץ מוצפן חדש עבור כל קובץ אותן הן מצפינות.
שינוי שמות קבצים	מספר הקבצים ששם שונם ביחס למספר הקבצים אליהם ניגשה האפליקציה.	כופרות רבות משנות שמות קבצים.
קריאת תוכן תיקיות	מספר התיקיות שנקראו ביחס למספר התיקיות הכולל.	כופרות חייבות לסרוק את התיקיות בהן הקבצים אותם היא הולכת להצפין.
אנטרופיה גבוהה	ממוצע האנטרופיה לפי שיטת שנון של פעולות הכתיבה ביחס לממוצע האנטרופיה של פעולות הקריאה.	הצפנות מאופיינות באנטרופיה גבוהה. צמצמום זיהויים כוזבים בעזרת השוואה לקריאה.
שימוש בסיומות	מספר הקטגוריות בהם אפליקציה השתמשה ביחס למספר הקטגוריות. מספר הסיומות אותם כתבה האפליקציה ביחס למספר הסיומות שנפתחו.	כופרות ניגשות למספר קטגוריות רב ביחס לתוכנות לגיטימיות.
שינוי סיומות	מספר שינויי הסיומת של קבצים ביחס למספר הקבצים אליהם ניגשה האפליקציה.	כופרות רבות משנות סיומת של קבצים לאחר הצפנת קבצים.
שימוש במלכודות	דגל המציין האם מספר התיקיות המכילות מלכודות שנפתחו עבר את הסף.	אפליקציות לגיטימיות לא ייפתחו קבצי מלכודת רבים. כופרה אינה מסוגלת להבדיל קבצים אלו מקובץ רגיל.
קריאת קבצים	מספר הקבצים שנקראו ביחס למספר הקבצים המוגנים.	כופרות קוראות קבצים רבים.
גישה לקבצים	מספר הקבצים שנכתב אליהם ביחס למספר הקבצים שאליהם האפליקציה ניגשה.	כופרות כותבות לאותו מספר קבצים בערך כמו מספר הקבצים אותם היא קוראת.
הזזת קבצים	מספר הקבצים שהוצאו מאזור מוגן ביחס למספר הקבצים שהוכנסו.	כופרות מסוימות מזיזות קבצים על מנת להקשות על זיהוי תהליכי הצפנה.

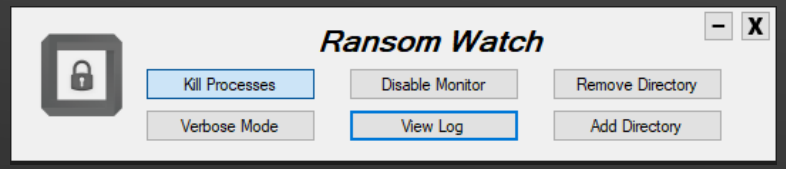
דרייבר

- ממומש כ-Windows Minifilter driver
- נרשם לפעולות פתיחה, סגירה, קריאה, כתיבה ושינוי מידע קובץ במערכת הקבצים.
- בהתאם לתיקיות שנבחרו להגנה, מעביר אינפורמציה על פעילויות מנוטרות לאפליקציה.
- מנטר אחר יצירה וסגירת תהליכים במערכת.
- משייך אפליקציה תחת מזהה ייחודי GID.
- אפליקציה בעלת GID שזוהתה כזדונית נעצרת בעזרת הדרייבר.

מערכת GID

- מאפשר שיוך של אפליקציה מרובת תהליכים לצורך זיהוי משותף.
- מאפשר לעצור מנגנוני גיבוי של כופרות.
- בעת יצירת תהליך שאינו תהליך מערכת מוקצה לתהליך מזהה GID.
- לכל תהליך שנוצר מתהליך בעל GID משויך GID כמו לתהליך האב.

אפליקציה



- כתובה ב-C++/Cli ומשלבת GUI.
- מאפשרת הגדרה של אזורים מוגנים ומבצעת להם גיבוי.
- מבקשת מהדרייבר עדכון על פעולות אחרונות מול מערכת הקבצים.
- לכל אפליקציה נשמר מידע בהתאם ל- GID.
- לאחר איסוף נתונים מנתחת אפליקציות בהתאם למדדים.
- במקרה של זיהוי אפליקציה זדונית, מבקשת מהדרייבר לעצור את האפליקציה ומשחזרת קבצים שנפגעו.

גיבוי ושחזור

- מבוסס ענן – אחסון Azure.
- מאפשר שחזור של מידע שנפגע כתוצאה מכופרה.
- ללא התערבות משתמש.
- מבצע גיבוי באינטרוולים של אזורים מוגנים, ומגבה קבצים ששונו.

(לא מומש גיבוי אינטרוולי)

בדיקות שנעשו

- הפתרון נוסה בהצלחה מול כופרות שונות:

  Katyusha, Cerber, Jigsaw, Wannacry, Locky ועוד.

- לאחר הדבקה התבצע בהצלחה שחזור לקבצים שנפגעו.

- נבדקה דחיסת קבצים, כולל בדיקת הצפנה. ביצענו דחיסה של קבצים באזורים מוגנים בעזרת תוכנות כגון Zip, 7z.

- עבודה רגילה מול מערכת הקבצים אינה מזוהה כזדונית.

תוצאות

WannaCry

מחלקת את פעולות הקריאה, איסוף הקבצים וכתיבה בין שני תהליכים.
הכופרה מייצרת קובץ נוסף לכל קובץ שאותו היא מצפינה, כותבת לשם את התוכן המוצפן ולאחר מכן משנה את הקובץ המקורי.
זוהתה על ידי כך שהיא יצרה קבצים רבים, קראה וכתבה לסיומות שונות, שינתה סיומות לקבצים.

Jigsaw

מבצעת קריאה של קבצים, יוצרת קובץ נוסף ליד הקבצים עם שם דומה וסיומת fun, כותבת את הקובץ שנקרא מוצפן לקובץ חדש ולאחר מכן מוחקת את הקובץ המקורי.
זוהתה על ידי כך שהיא יצרה, כתבה ומחקה קבצים רבים, נגעה בקבצים בעלי סיומות שונות וכתבה באנטרופיה גבוהה ביחס לקריאה.

בעיות ושיפורים אפשריים

- שימוש במודל סטטי לזיהוי, זיהוי תבניות בקוד ושמירת חתימות של זיהויים.
- הכנסת אומדן זמנים לניתוח אפליקציות.
- שימוש בדרייבר רשת לזיהוי התנהגות חשודה של כופרה.
- ניקוי קבצי הרצה של כופרות, ניקוי תיקיית Registry, Task scheduler, Start-up.
- טעינה אוטומטית של הדרייבר והתוכנה באתחול.
- שמירת מידע אודות תיקיות מוגנות ומלכודות לאחר סגירת האפליקציה.
- שיפור של מערכת הגיבוי.
- הגנה של הפתרון על קבצים בהם הוא משתמש (הגנה עצמית).

בעיות ושיפורים אפשריים

קיימת שיטת תקיפה המתוארת במאמר הבא, שלא ניתן לה מענה בפתרון שלנו ולא נמצאו כופרות המשתמשות בשיטה זו.

בשיטת תקיפה זו אפליקציה פותחת HANDLE (רפרנס לקובץ) ל-Volume בו קיים מידע שהיא רוצה להצפין. שיטת זו מאפשרת לקרוא ולכתוב קבצים שלא דרך ה-Minifilter דרייבר או hooks אחרים.

R. Van Gorp. Low-level writing to NTFS file systems. 2018

הדגמות

RANSOMWATCH

- קוד הפרויקט, דו"ח הסיום, הדגמות ומצגת זו נמצאים ב-GitHub:

https://github.com/RafWu/RansomWatch