תשובה לרעיון המרכזי:

הרעיון המרכזי של המאמר הוא שלמרות מנגנוני ההצפנה המתקדמים המופעלים על ידי יישומי "מסרים מיידיים" (IM- Instant Messaging) מאובטחים פופולריים כמו Telegram, Signal ו-WhatsApp, יישומים אלה עדיין רגישים להתקפות סייבר של ניתוח תעבורת רשת.
מחברי המאמר מראים כי גורמים זרים יכולים לזהות במדויק את כתובות ה-IP של חברים ומנהלים של ערוצי IM ספציפיים על ידי **ניטור** תעבורת הרשת המוצפנת של משתמשי IM פגיעות זו מתעוררת עקב היעדר מנגנוני ערפול תנועה שנפרסו על ידי מפעילי IM, המאפשרים ליריבים לנצל דפוסי תעבורה ולהדליף מידע רגיש גם כאשר ההצפנה קיימת.

מאמר זה מדגיש את האיומים הפוטנציאליים בעולם האמיתי על משתמשים בשירותי IM "מאובטחים" כביכול, במיוחד באזורים שבהם ממשלות מדכאות מנסות לפצח ולהאזין לתושביהם. מחברי המאמר מציגים מודל סטטיסטי למאפייני תעבורת IM ,ומפתחים אלגוריתמים המבצע ניתוחי תנועה שיכולים לזהות משתתפים בתקשורת אפליקציות "מסרים מיידים". הם גם דנים באמצעי הגנה אפשריים ומציגים מערכת הגנה אשר נקראת IMProxy.

1. כיצד משיג התוקף מידע ממשי על תעבורת הערוץ?

עבור כל ערוץ ב IM שהוא מטרה (מסומן כ"C"), התוקף צריך לאסוף מידע על דפוסי התנועה של המידע בערוץ. ניתן להשיג זאת באמצעות שלוש שיטות:

ערוצים פתוחים: אם ערוץ היעד ציבורי ופתוח, התוקף יכול להצטרף לערוץ כחבר. על ידי הקלטת ההודעות שנשלחו בערוץ יחד עם הנתונים המרכזיים (Meta Data) שלהן (כגון זמן וגודל הודעה), התוקף יכול לקבל תובנות לגבי תעבורת הערוץ מכך שהוא מנתח זאת.

פרסום הודעות: אם התוקף חבר בערוץ ויכול לפרסם בו הודעות, הוא יכול לצפות ישירות בדפוסי התנועה. זה חל על קבוצות סגורות או מצבים שבהם התוקף מקבל הרשאות ניהול בערוץ. התוקף יכול גם להקליט הודעות קיימות וגם להציג הודעות משלו עם דפוסי תעבורה ברורים.

זיהוי IP: גם אם התוקף לא יכול להצטרף לערוץ, אם הוא מגלה את כתובת ה-IP של אחד מחברי הערוץ או המנהלים שלו, בצורה זו התוקף יכול להאזין לתנועת הרשת המוצפנת של המשתמש החשוף.
פרצה זו מאפשרת לתוקף לנתח את דפוסי התנועה ולאסוף מידע על פעילות התעבורה בערוץ.

2. כיצד התוקף מאזין או מצותת לתעבורה ברשת?

ההאזנה של התוקף תתבצע בעזרת ניטור תעבורת הרשת המוצפנת של משתמשי IM. ניתן לנטר זאת על ידי שליטה בנקודות רשת ספציפיות, כגון ספקי שירותי אינטרנט (ISP) או נקודות חילופי אינטרנט (IXPs), שם הן

מיירטות את התעבורה. חומת האש הגדולה של סין היא דוגמה למערכת המשמשת ליירוט כזה. לחלופין, התוקף יכול לפקח על תעבורת הרשת של אנשים ספציפיים, פוטנציאלית לאחר שהתוקף השיג צווים משפטיים המאפשרים להאזין למידע בסתר. המטרה היא לנתח את התקשורת המוצפנת שהוחלפה בין משתמשי IM כדי לזהות את המשתתפים בקבוצה או בערוץ היעד ולאתר אותם.

3. תאר בקצרה את המסקנות מטבלה 2 במאמר.

טבלה 2 מספקת פירוט מקיף של סוגי התכנים שהוחלפו ונשלחו באמצעות יישומי הIM, יחד עם נתונים סטטיסטיים רלוונטיים. הטבלה מציגה את התפלגות קטגוריות התוכן, נפח הנתונים הכולל המיוחס לכל קטגוריה, טווח גדלי הקבצים והגודל הממוצע של התוכן בכל קטגוריה.
ניתוח זה מציע תובנות לגבי דינמיקת התוכן ודפוסי צריכת הנתונים בתקשורת IM. הוא מגלה שלסוגים שונים של תוכן, כגון טקסט, תמונות, סרטונים, קבצים ואודיו, יש הפצות, נפחים וגדלים שונים, ומספקים תמונת מצב של מגוון התוכן המשותף בין משתמשי יישום הIM.

איור 8: איתור והוצאת מאורעות מהודעות ביישום ה- IM:

איור 8 במאמר ממחיש את תהליך הוצאת האירועים מהודעות ביישום ה IM. באופן ספציפי, הוא מתמקד בהודעות מיידיות שנשלחות או מתקבלות על ידי משתמש יעד. האיור מדגים כיצד נוצרים פרצי פאקטות מוצפנות בהודעות הנל, וכיצד התוקף יכול לאתר מאורעות ספציפיים מפרצי הפאקטות הללו שכן יהיה ניתן לראות זאת גם בפרוייקט שלנו.

המונח "מאורע" מתייחס לפעולה או התרחשות משמעותית, כגון שליחה או קבלה של הודעה, בהקשר של תקשורת מיידית. האיור ממחיש את הרעיון של פרצי פאקטות בצורה ויזואלית, שהן גושים של מידע ברשת כאשר כל הפאקטות מוצפנות ומתאימות למאורעות או הודעות ספציפיים.

תהליך חילוץ המידע כולל זיהוי וקיבוץ פאקטות השייכות לאותה ההודעה. על ידי ניתוח הדפוסים והמאפיינים של פרצי פאקטות אלה, התוקף יכול להסיק מידע על האירועים המתרחשים בתקשורת ה-IM. זה יכול לכלול את תזמון המאורעות(הודעות), המשתתפים המעורבים, ואולי אפילו את התוכן המועבר.

באופן כללי, איור 8 ממחיש את הרעיון של חילוץ הודעות ביישום הIM ומדגיש את תפקידם של פרצי פאקטות בחשיפת תובנות לגבי הפעילויות והאינטראקציות המתרחשות בתקשורת ה-IM.