שלומי דולב, ניב גלבוע, אסף כהן ועופר חרמוני

אוניברסיטת בן גוריון בנגב

תקציר

התקפות סייבר וסוגים רבים של הונאות דיגיטליות הן כמעט תמיד נטולות סיכון. תוקף המבצע התקפה על שירותים ממשלתיים, מוסדות פיננסיים או חברות מסחריות במרחב המקוון, יכול לשבת בנוחות ובבטיחות בביתו, ולבצע התקפה אחת אחרי השנייה. מוגן מפני זיהוי על ידי האנונימיות של האינטרנט, ומפני הליכים משפטיים על ידי המצאות בתחום שיפוט אחר או אפילו מדינה אחרת מהיעד, הסיכון הגדול ביותר עבור רוב התוקפים הוא שההתקפה שלהם תיכשל.

הגישה אופיינית להתמודדות עם התקפות היא זיהוי ומניעה. מפעילי הרשתות נוקטים באמצעים טכנולוגיים וחברתיים שונים על מנת להבטיח שהתעבורה ברשת שלהם אינה זדונית. כאשר התקפה מזוהה, חוסמים אותה. גישה זו מקבילה לדלתות נעולות, מערכת אזעקה ומצלמות אבטחה בעולם הפיזי. עם זאת, בעולם האמיתי ישנו מרכיב נוסף מעבר לזיהוי ומניעה והוא הרתעה ואכיפה. פושע פועל בסיכון ממשי להיתפס על ידי המשטרה, ואף להיענש על ידי מערכת המשפט.

בהצעת מחקר זו אנו מציעים פרדיגמה חדשה להרתעת תוקפים מרוחקים במרחב המקוון. הרעיון הבסיסי הוא הוספת מימד אחריות לאינטראקציה בין הלקוח לנותן השירות המקוון. הלקוח והשרת מגיעים להסכם המסדיר את התנהגות הלקוח, לדוגמא, דרישה לשימוש הוגן ללא התקפת סייבר או ניסיונות הונאה נגד השרת. לאחר מכן הלקוח שולח צ'ק דיגיטאלי חתום ומוצפן לשרת. כל עוד הלקוח פועל על פי הסכם, השרת לא יכול לפענח את הצ'ק ולקבל לידיו כל תשלום מהלקוח. אך אם הלקוח מפר את ההסכם, השרת מקבל את המידע הדרוש כדי לפענח את הצ'ק. השרת אינו יכול להתחזות ללקוח ולפענח את הצ'ק המוצפן על

ידי זיוף התקפה, מכיוון שהודעות הלקוח חתומות על ידו באמצעות המפתח הפרטי שלו שאינו ידוע לשרת.

השיטה דורשת שבשלב האתחול, ישתתף גם גורם שלישי המהימן על הצדדים, דוגמא לגורם כזה היא גורם מאשר (certificate authority - CA). ה- CA חייב לערוב לצ'ק הדיגיטאלי של הלקוח, אחרת השרת לא יכול להיות בטוח כי הצ'ק המוצפן אכן מכיל את סכום הכסף הדרוש, ואכן ממוען לשרת. בנוסף על ה-CA לחתום על המפתח הציבורי של הלקוח, כך שהשרת יכול לאמת את הודעות הלקוח.

במחקר זה אנו נראה את ההיתכנות של מודל זה ל"שטר ערבות דיגיטאלי", ונפתח גישות מעשיות ליישום המודל.

חלק מרכזי במחקר שלנו הוא זיהוי חריגות בהתנהגות הלקוח על מנת להתניע תהליך של פענוח הצ'ק הדיגיטאלי. גישה זו מאפשרת להרתיע מגוון רחב של מתקפות לא ידועות, אך גורמות לסטייה מהתנהגות הרגילה של לקוח ברשת. אנו מעוניינים במיוחד בפיתוח שיטות לגילוי חריגות אשר מבוטאות במעגלים לוגיים קטנים, על מנת לאפשר פענוח של הצ'ק הדיגיטאלי עם משאבים מעשיים. יתר על כן, אנו רוצים לפתח גישה היברידית לזיהוי התקפות המבוססת הן של איתור התקפות ידועות והן על זיהוי אנומליות, על מנת להפחית שני פרמטרים חשובים. הראשון הוא הפחתה של פענוח צ'קים במקרה של זיהוי חיובי כושל (false positive), לדוגמא תעבורה נורמאלית המתגלה כחריגה, והשני הוא זמן העיבוד של השרת בוידוא החתימה של הלקוח.

התנאי בו עומד הלקוח הופך את השיטה שלנו לאטרקטיבית עבור משתמשים לגיטימיים. הם לא צריכים לסמוך על השרת. ההתחייבות שלהם ניתנת לשרת, ואין להם כל חשש כל עוד הם לא מפרים את ההסכם שסוכם בין הלקוח לשרת, הפרה זו אינה המטרה של משתמש שומר חוק.