

# קוד מוטציה בשדה הקרב הקיברנטי

דניאל כהן ואביב רוטברט

לוחמת סייבר או השיגו אותן כבר, לרבות היכולת לבצע מתקפות סייבר. **ארגוני פשע** - מונעים בעיקר מאינטרסים פוליטיים ועסקיים; ארגוני פשע מאורגן משתמשים בהאקרים, ובעיקר במפעילי רשתות שביות למטרות רווח: גניבת זהות, הונאה, דואר זבל, פורנוגרפיה, הסוואת פעילות פלילית, הלבנות הון וכיוצא באלה.

**חברות עסקיות** - פועלות בעיקר בתחום ההגנתי, כיוון שהיקף ההתקפות במרחב הקיברנטי בהקשרים עסקיים הולך וגדל במידה ניכרת, אולם חלק מהן עלולות לפנות (או שכבר פנו) לאפיק של התקפה על חברות מתחרות לצורך ריגול עסקי.

**ארגוני טרור** - יתרונות הגלומים בשימוש בסייבר מנוצלים על ידי גורמים חבליים על מנת להעביר מסרים מוצפנים, לגייס תומכים, לרכוש מטרות, לאסוף מודיעין, להסוות פעילות וכדומה.

**גורמים "אנרכיסטיים"** - מתנגדים למערכת הממסדית הקיימת מעוניינים לחבל בה מבפנים או מבחוץ ויבקשו לתקוף את מערכת המחשוב, שהיא כיום הבסיס לניהולה, בכוונה לשבש ואף להרוס את



אביב רוטברט

הסדר החברתי ואת מרקם החיים במדינה. שימוש בנשק קיברנטי לתקיפת יעדים אסטרטגיים במרחב הפיזי והסייבר מצריך יכולת השמורה, לפי שעה, למספר מצומצם של מדינות בעלות יכולות ומשאבים טכנולוגיים ברמה גבוהה. לעומת זאת, ישנה "מדרגת כניסה נמוכה" וכלי נשק קיברנטיים בעלי יכולת פגיעה עם נזקים טקטיים. יכולת ייצור המוני של כלי נשק קיברנטיים כאלה היא מהירה ובעלות נמוכה יחסית, חלקם אף זמינים בשוק החופשי. מדינות מנצלות את מרחב הסייבר כדי להשיג יתרון ולקדם את האינטרסים שלהן באמצעות איסוף מידע, השגת כושר פגיעה ביכולותיהן של מי שנתפס כאויב, ועוד. גם שחקנים לא-מדינתיים כגון ארגוני טרור ופשיעה ממנפים את מרחב הסייבר למטרותיהם, ומפיקים תועלת במרחב המתיר גם לשחקנים קטנים להשפיע באופן שאינו יחסי לגודלם. לכל השחקנים במרחב הסייבר יש אינטרס לייצר קודי מוטציה ולהשתמש בהם למטרותיהם, מכיוון שזו הדרך המהירה והזולה להגיע ליכולות תקיפה קיברנטיות.

כל מתקפת סייבר חדשה שמתגלה מקרבת את הפיכתו של נשק הסייבר לנחלת הכלל. עם התגברות השימוש בכלים ללוחמת סייבר, לא מן הנמנע שנשק קיברנטי מתוחכם ובעל יכולת לביצוע נזק אסטרטגי יתפוך לחזון נפרץ, וגרסאות שלו ימצאו את דרכן לידהן של מדינות תומכות טרור וארגוני טרור. כדוגמה, אפשר להתבונן על המתקפה על אתרי הגרעין האיראניים באמצעות ירוס סטקסנט (stuxnet). ההתקפה פעלה במשך שנים באופן חשאי, אך ברגע שהתגלתה היא הביאה למחקר ולניתוח מעמיקים ביותר של קוד הירוס, ולניסיון להבין את כל ההיבטים שאפשרו את הצלחתו. תוצאות הניתוח יכולות לשמש באופן מיידי לפיתוח של ירוסים חדשים בעלי עקרונות פעולה דומים לאלה של סטקסנט. הסוד נחשף, הנשק התפשט. מבחינה תיאורטית, הימצאות וניתוח קוד זדוני בידי חברות ומומחי

בכל שנה, לקראת בואו של החורף, אנחנו מתלבטים אם כדאי לחסן את גופנו מפני נגיפי השפעת החדשים שצפויים לתקוף אותנו עם בוא עונת הגשמים. המערכת החיסונית שלנו לעיתים לא מסוגלת לעמוד בפני עצמה מול הנגיפים החדשים מכיוון שהיא לא מכירה אותם ולא יודעת

כיצד להתמודד איתם. הנגיפים החדשים הללו הם בד"כ מוטציות של נגיפים אחרים, מולם מערכת החיסון יודעת להתמודד. מוטציה היא למעשה ירוס שעובר שינוי גנטי מסוים - שינוי שמספיע על חלק מהתכונות שלו ועשוי להפוך אותו לעמיד יותר בפני מערכת החיסון, קטלני יותר, בעל יכולת התפשטות טובה יותר. כל עונה אנחנו מתמודדים עם מוטציות חדשות של ירוסים מוכרים.



דניאל כהן

בהשאלה מעולם הביולוגיה, אנו משתמשים לפעמים במושג "ירוס מחשבים". הכוונה כאן

היא לקוד מחשב זדוני שמסוגל לחדור למערכת מחשוב ולבצע בה פעולות של ריגול או גרימת נזק. כתגובה לכך, קיימות תוכנות אנטי-ירוס שמטרתן להכיר ירוסים שעשויים לתקוף מערכת מחשוב ולבלום אותם כאשר הם מנסים לחדור אל תוך המערכת. קיימת סברה לגבי מרחב הלחימה הקיברנטי, לפיה ירוס או קוד זדוני אחר שנעשה בו שימוש לתקיפה, והתגלה על ידי חברות אבטחה, הופך להיות חסר תועלת בעתיד - מכיוון שתוכנות האנטי ירוס מכירות אותו, פותח חיסון נגדו והוא לא יכול להזיק יותר. במילים אחרות - ירוס מחשבים הוא נשק חד פעמי.

אנו נטען כי לא כך הם פני הדברים. עם התגברות התקיפות במרחב הסייבר, יגברו תפוצת הכלים ויכולות הסייבר בעולם. אחת הסיבות העיקריות לכך היא שניתן לעשות שימוש בנשק סייבר, כדוגמת קוד זדוני ששימש לתקיפה אחת, גם בתקיפות אחרות, וזאת לאחר הסבתו. אם נמשיך את ההשאלה מעולם הביולוגיה, נוכל לכתוב קוד זה כ- "קוד מוטציה". קוד זה הוא בעל מאפיינים פונקציונליים דומים (עד כדי זהות מוחלטת) לקוד האב שממנו הוא נוצר. ההבדל בין קוד האב לקוד המוטציה הוא סינטקטי (מבני) בלבד ולא סמנטי, במטרה לחמוק מהרדאר של תוכנות לזיהוי פוגענים.

מכך ניתן להסיק כי נפילת קוד זדוני לידי יריב בעל מוטיבציה ויכולת נותנת לצד המותקף נשק שב"חיוש" מתאים, תוך ביצוע פעולות מורכבות כגון הנדסה לאחור (Reverse Engineering), יכול להיות מנוצל לשימוש רב-פעמי. כמו כן, שימוש יעיל יכול להיעשות על ידי תוקף שמכיר את הנשק ויכול לשנות אותו על פי צרכיו לביצוע מתקפות נוספות. על מנת לעמוד על היקף התופעה של שימוש בקודי מוטציה, יש להבין כיצד נראה ומתנהל מרחב הלחימה הקיברנטי, ובפרט - מי הם השחקנים העיקריים בו ומה האינטרסים והיכולות שלהם.

חמש קבוצות עיקריות משתמשות כיום, או שיש להן פוטנציאל לשימוש בעתיד, בכלי תקיפה קיברנטיים.

**מדינות** - מפתחות יכולות התקיפות והגנתיות כחלק מיכולות הפעלת הכוח שלהן. הערכות סבירות הן שכארבעים מדינות מצטיידות ביכולות