מבט על, גיליון 444, 8 ביולי 2013

שימוש בקוד מוטציה לייצור נשק קיברנטי רב פעמי

דניאל כהן ואביב רוטברט

השימוש ההולך וגובר בכלים ללוחמת סייבר, יוצר מצב בלתי נמנע שבו גרסאות של נשק קיברנטי מתוחכם ובעל יכולת לביצוע נזק אסטרטגי ימצאו את דרכן לידיהן של מדינות תומכות טרור, ארגוני טרור וארגוני פשע. כתוצאה מכך, הנשק הקיברנטי לא יישאר לעד נחלתם של מעטים.

כדוגמה, אפשר לבחון את המתקפה על אתרי הגרעין האיראניים באמצעות וירוס סטקסנט (stuxnet). ההתקפה פעלה במשך שנים באופן חשאי, אך ברגע שהתגלתה, היא הביאה למחקר ולניתוח מעמיקים ביותר של קוד הווירוס. תוצאות הניתוח יכולות לשמש באופן מידי לפיתוח של וירוסים חדשים בעלי עקרונות פעולה דומים לאלה של סטקסנט. מרגע שהסוד נחשף – הנשק התפשט.

בעולם הביולוגיה, מוטציה גנטית היא מושג המתאר מצב של טעות בשכפול ה – DNA. המוטציות הן הגורם להבדלים בין בני האדם. בזכות המוטציות יכולים היצורים לעבור התאמה לסביבה והן המניעות את האבולוציה. כאשר וירוס עובר מוטציה, מדובר למעשה בווירוס שעובר שינוי גנטי מסוים – שינוי המשפיע על חלק מהתכונות שלו ועשוי להפוך אותו לעמיד יותר בפני מערכת החיסון של האדם, לקטלני יותר ובעל יכולת התפשטות טובה יותר. מדי שנה מתמודדת מערכת הבריאות עם מוטציות חדשות של וירוסים מוכרים.

קיימת סברה לגבי מרחב הלחימה הקיברנטי, לפיה וירוס או קוד זדוני – לאחר שנעשה בו שימוש לצורך תקיפה והתגלה על ידי חברות אבטחה – הופך להיות חסר תועלת, מכיוון שתוכנות האנטי וירוס מכירות אותו, מפתחות חיסון נגדו והוא לא יכול להזיק עוד. במילים אחרות – וירוס מחשבים הוא נשק חד פעמי. אך לא כך הם פני הדברים. בדומה לווירוסים מעולם הביולוגיה, גם קוד זדוני יכול לעבור תהליך שינוי, שיהפוך אותו לחסין מפני תוכנות האנטי-וירוס. קוד זה יכונה להלן כ-"קוד מוטציה". ייחודו של קוד מוטציה, הוא שלמרות היותו בעל מאפיינים פונקציונליים דומים (עד כדי זהות מוחלטת) לקוד האב שממנו הוא נוצר, ההבדל בין קוד האב ל"קוד מוטציה" הוא סינטַקטי (מִבני) בלבד ולא סמנטי, במטרה לחמוק מהרדאר של תוכנות לזיהוי פוגענים.

כיצד נוצר "קוד מוטציה"? בדומה למוטציה גנטית, גם קוד מוטציה לא נדרש להיות שונה מאוד מהקוד המקורי. קוד מחשב, ובכלל זה קוד של וירוס, מורכב בדרך כלל מכמה רכיבי תוכנה המתקשרים ביניהם לצורך ביצוע משימות. לעיתים, מספיק שינוי קל באופן שבו מתקשרים הרכיבים זה עם זה, או שינוי באחד הרכיבים, כדי לייצר מוטציית קוד שלא ניתנת לזיהוי על ידי מערכת החיסון של המחשב – תוכנות ההגנה והאנטי-וירוס. לעיתים, יידרשו שינויים כבדים יותר: תהליכים אשר יגרמו לקוד זדוני להיראות שונה מאוד מהקוד המקורי שהיווה את הבסיס ליצירתו. אבל שינויים אלו הם רק למראית עין: אחרי שהווירוס עובר את חומות ההגנה והפיקוח של המחשב, הוא חוזר לצורתו המקורית ומתחיל לפעול באופן דומה לווירוס המקורי. שתי שיטות מוכרות לשינוי קוד מחשב ידועות בעולם התוכנה כעֵרפול (obfuscation) ואריזה (packing). אלו ישנו את הקוד (יגרמו לו להיראות כתמונה, טקסט, או רצף תווים חסר משמעות) אך לא יפגעו בפונקציונאליות שלו.

הסביבה האסטרטגית-קיברנטית כוללת שימוש בנשק קיברנטי לפעולות חדירה למערכות האויב לצורך ריגול, לוחמה פסיכולוגית, הרתעה, נזק למערכות תקשוב או ליעדים פיזיים. מרחב הלחימה הקיברנטי מגוון מאוד ושחקנים רבים יכולים לפעול בו על פי האינטרסים והיכולות השונות, המצויות ברשותם. ארסנל הנשקים כולל יכולות מתקדמות, אשר לרוב יימצאו אך ורק בידי מספר מצומצם של מדינות, ובהן היכולות לחדור למערכות האויב בלי להתגלות, לאסוף מידע, לשבש פעילות מבלי לעורר חשד ואף לחבל במערכות פיזיות המקושרות למרחב הסייבר.

בארסנל ניתן למצוא גם נשקים פשוטים יותר, זולים יותר לייצור, אשר נמצאים בשימוש של שחקנים אחרים: ארגוני פשע, ארגוני טרור וחברות עסקיות. נשקים אלו ישמשו לרוב למטרות פגיעה זמנית ברשתות (התקפות מניעת שירות), חדירה למערכות מחשב שאינן מאובטחות ברמה גבוהה, גניבת מידע ושיבוש של מערכות אלה. יכולות מהסוג הזה מוצעות למכירה ברשת האינטרנט לכל דורש – דבר שמגביר את תפוצת הנשק הקיברנטי והופך אותו נגיש גם עבור גורמים שאין להם יכולות טכנולוגיות אך יש בידם כסף לשלם עבור רכישתן.

היכולת ליצור קודי מוטציה מצמצמת את הפער הטכנולוגי בין שחקנים במרחב הסייבר. על מנת ליצור כלי נשק קיברנטי מתוחכם נדרשים משאבי המדינה, אולם בכדי לשכפל אותו או לייצר מוטציות, מספיקה קבוצה אזרחית של האקרים מוכשרים. אלה יכולים לעשות בו שימוש לצרכיהם או למכור ולהפעיל אותו עבור אחרים תמורת תשלום.

כיום רשת האינטרנט ורשתות תקשורת אחרות המבוססות על פרוטוקולים דומים – אינן מוגנות מספיק ותוקף בעל מוטיבציה יכול לפגוע בהן. ההסתמכות של תשתיות המדינה על מגזריה השונים ברשת והתלות בה קורצות מאוד הן לארגוני טרור, המבקשים לחדור לתודעה הציבורית ולשנות מצב פוליטי קיים, והן לארגוני פשע המעוניינים בהשגת רווח כלכלי. אלה וגם אלה יכולים להשיג את מטרותיהם באמצעות תקיפה קיברנטית, שלעיתים תהיה זולה ופשוטה יותר מאשר פעולות טרור ופשע קינטיות – אך תשיג אפקט דומה.

מאפייני שדה הקרב הקיברנטי מציבים בפני התוקף דילמות הנובעות מהיותו של הנשק הקיברנטי רב-פעמי. כתוצאה מכך, עצם השימוש בו חושף את מאפייניו בפני הקורבן, שיכול מצדו לעשות בו שימוש חוזר, כולל נגד התוקף עצמו ("אפקט הבומרנג"). כלי נשק בעלי יכולת הרס אסטרטגי (כגון סטקסנט) עלולים ליפול (ויתכן שכבר נפלו) בידי מדינות תומכות טרור וארגוני טרור ופשע, ולשמש בסיס לתקיפות סייבר.

נגישות של נשק קיברנטי לארגוני טרור ופשע מהווה איום לביטחון הלאומי של מדינות בכלל ומדינת ישראל - בפרט. עם התגברות השימוש בנשק הסייבר על ידי מדינות, אנו נהיה עדים לתפוצה של נשק זה גם בקרב מדינות נוספות ושחקנים לא מדינתיים (ארגוני טרור, פשע, חברות עסקיות). לכן, בניתוח האיומים במרחב הסייבר יש להתייחס לכלי נשק קיברנטיים כנשקים רב-פעמיים שניתן לנצלם לתקיפות נוספות.