

למצוא דרך לנצל את החולשה. תהליך זה עשוי להימשך בין ימים לשבועות, כתלות במורכבות הטלאי ובנחישות של ההאקר. לעומת זאת, ניתוח מעמיק של כלי מתוחכם כמו פליים ידרוש זמן רב יותר, וכוח אדם מקצועי ומיומן יותר. בדרך כלל, ניתוח כזה נעשה על ידי מדינות או חברות אבטחה ולא על ידי אנשים פרטיים. לדוגמה, נשק הסייבר מיני-פליים (MiniFlame) שנתח באופן מעמיק על ידי חברת קספרסקי. ניתוח זה, שארך מספר חודשים ודרש משאבי כוח-אדם רבים, בוצע על מנת לפתח הגנה מפני הכלי ולהפיץ אותו בקרב לקוחות החברה. אבל תוצרי הניתוח יכולים לשמש בסיס לקוד מוטציה, העושה שימוש בטכניקות דומות ולעיתים אף בחלק מהקוד של הנשק המקורי. אם תוצרים אלה ידלפו מחברת קספרסקי לגורמים המפתחים נשק סייבר, לא יהיה זה מפתיע לגלות כלים חדשים החולקים קוד משותף עם המיני-פליים אך מופעלים על ידי תוקפים אחרים, נגד מטרות אחרות (ייתכן שאף נגד היוצר הראשוני של הנשק - אפקט הבומרנג).

כיום, ארסנל כלי הנשק הקיברנטיים בעלי יכולת פגיעה טקטית מצמצם את פער ההצטיידות בין מדינות לבין שחקנים לא-מדינתיים. לעומת זאת, מתרחב הפער בין מדינות בעלות ארסנל יכולות תקיפה נגד יעדים אסטרטגיים, לבין מדינות ושחקנים שאין ביכולתם להגיע לסף הכניסה הגבוה. לא מן הנמנע שמדינות ושחקנים נוספים יחזרו להשגת יכולת של נשק קיברנטי בעל כושר פגיעה פיזית, ומגמת העלייה הדרמטית באיומים במרחב הסייבר מחייבת כיווני פעולה להתמודדות עם איומים אלה. לכן קיים צורך חשוב להעלות לדיון את תפיסת כלי הנשק הקיברנטיים כנשק רב-פעמי שניתן לנצלו לתקיפות נוספות.

אבטחה עשויה לחשוף את הירוס כלפי חוץ לגורמים שונים, החל ממדינות ועד ארגוני טרור. הנשק הקיברנטי לא יישאר לעד נחלתם של מעטים. קיימת סברה שלפיה הנשק הקיברנטי הינו חד-פעמי, והדבר יהווה גורם מרסן בשימוש בו וגורם מאט בפיתוח של כלי לוחמת סייבר חדשים, בשל הצורך לחדש כל העת והימנעות משימוש בכלי נשק שהתגלה כבר ונחתם על ידי תוכנות ההגנה. סברה זו לא הוכיחה את עצמה, ומהתבוננות בשטח ניתן להבחין שדווקא ההפך הוא הנכון - הווה אומר, קיים שימוש חוזר נרחב בכלי לוחמת סייבר שעוברים שינויים על מנת לאפשר להם לחמוק מהרדאר של תוכנות ההגנה.

נשק קיברנטי שהתגלה ונחתם אמנם נחסם לשימוש בצורתו המקורית, אך מכאן ועד לחסימה הרמטית והפיכת כל הקוד שפותח ללא-רלוונטי - המרחק עדיין רב. ראשית, כל כלי תקיפה מורכב ממספר מודולים (רכיבי תוכנה). בין היתר, ניתן למנות את המודול האחראי להסוואת הכלי במערכת המותקפת, מודולים שונים לאיסוף מידע, מודול לאחסון המידע ומודול לשליחת המידע אל שרתי הפיקוד והבקרה של הכלי. אם סוס טרויאני התגלה ונחתם, ניתן לעשות שימוש חוזר בחלק מן המודולים שלו, כאשר אלה משולבים בתוך קוד של סוס טרויאני אחר. שילוב כזה ייצור קוד מוטציה שעשוי לחמוק מתחת לרדאר של מערכות אבטחה-יורוס. דרך אחרת לשימוש חוזר בקוד זדוני היא על ידי הסוואתו בשיטות המוכרות מעולם התוכנה כערפול (obfuscation) ואריזה (packing). אלה יכולות לעיתים לשנות את הקוד הזדוני באופן שהוא לא יתגלה על ידי תוכנת הגנה. לבסוף, גם אם לא יתאפשר שימוש בקוד שהתגלה, ניתן לפתח כלי חדש המבוסס על רעיונות ואופני פעולה דומים ומנצל את אותן החולשות כמו הקוד המקורי.

היכולת ליצור נשק סייבר חדש המבוסס על נשק קיים או על חולשה שפורסמה איננה תמיד מיידית ופשוטה. ההאקרים שמנצלים את עדכוני האבטחה של מייקרוסופט כדי לגלות את קיומן של חולשות במערכת ההפעלה "חלונות" צריכים להשקיע זמן בניתוח הטלאי, ובהשוואת הקבצים שהוא מתקן לקבצים המקוריים לפני התיקון (כדי לזהות היכן בדיוק התבצע התיקון, כיוון ששם נמצאת החולשה). לבסוף הם גם צריכים



## תחרות האוסקר הישראלי באינטרנט



### לוח זמנים

**15.6.13** מועד אחרון להגשת מועמדות

**20.7.13** סיום שלב שיפוט ראשון

**30.7.13** שלב שיפוט שני - מפגש פרונטאלי של הארגונים שעלו לגמר התחרות

**6.10.2013** סיום השיפוט ומקס הכרתת הזוכים במלון שרתון תל אביב

# מי האתרים שיזכו ב-Webi2013?

הירשמו עוד היום לתחרות: [www.webi2013.events.co.il](http://www.webi2013.events.co.il)  
לפרטים נוספים: חגית קדם 03-7330746 [hagitk@pc.co.il](mailto:hagitk@pc.co.il)