לשחק עם מרכיבים ביולוגיים כמו שמשחקים עם אבני לגו ולהרכיב אותם לחומרים בעלי תכונות שונות ומשונות, לפי רצוננו. למשל, וירוסים או חיידקים לא מוכרים", אמר. "תארו לעצמכם שיש וירוסים שאוכלים סיליקון ומכלים את מוצרי האלקטרוניקה - וירוסים אמיתיים, לא של מחשבים".

ד"ר שרן צפה, כי "מושגים נוספים שנתוודע אליהם בעתיד הם ביו-האקינג וביו-טרור. ניתן לחדור לתוך הגנום שלנו ואז באמת לא נדע מהי פרטיות".

"פנינו למומחים לכל התחומים הללו ברחבי אירופה ושקללנו את הסבירות להתפתחות תחום טכנולוגי מסוים לעומת הנזק שהוא גורם", הוסיף. "האיום בתחום הננו-טכנולוגיה ילך ויעלה עד 2030, ולאחר מכן יתחיל לרדת. יש לנו עוד זמן לפתח אמצעי התגוננות או למנוע את היכולת של טרוריסטים לעשות שימוש בטכנולוגיות כאלה". תחום נוסף שציין הוא הביולוגיה הסינתטית, שהאיום בה יימשך עד 2035.

"בנוסף, קיימים איומים שהסבירות שיתממשו נמוכה, אולם הם הכי מאיימים והשפעתם, אם יתממשו, תהיה גבוהה", אמר ד"ר שרן. "אנחנו מכנים את התופעה הזאת 'קלפים פרועים'. מדובר במטה חומרים, קטליזה במים, צ'יפים מושתלים במוח, טרוריסטים מונהגים, רובוטים, העשרה אנושית, להקות רובוטים ורובוטים עם תבונה מלאכותית".

לסיכום, המליץ ד"ר שרן "לשים לב לטכנולוגיות מתפתחות שיגבירו או יחליפו את עולם הסייבר. אם נחשוב כמה שנים מראש, ייתכן שיהיו לנו מספיק אמצעים למנוע את השימוש האפל בהן".

גיא מזרחי

מוטי שגיא

ד"ר גיל דוד

האיום האיראני - גרסת הרשת

"איראנים שנכנסים בשמות ישראליים בדויים ומציעים חברות בפייסבוק העלו ברשתם רבים בתעשיות הביטחוניות של ישראל", כך אמר **גיא מזרחי**, יועץ לוחמת סייבר מחברת סייבריה.

הוא סיפר, כי באחרונה ביקש ממנו מתחזה חברות בפייסבוק, במסווה של בחורה בשם שירי באר, שטענה שהיא עובדת באלביט. מכיוון שמזרחי עצמו עבד בעבר באלביט ולא הכיר אותה, הוא ביצע בדיקה קלה בפייסבוק והעלה ש"שירי באר" היא בעצם איראנית. בינתיים היא התקדמה כביכול לתעשייה האווירית ויש לה 112 חברים ישראלים בפייסבוק.

מזרחי תיאר את תהליך ביצועה של מתקפת סייבר על גופי היעד (APT - Advanced Persisted Threat). לדבריו, התהליך מתחיל באיסוף מידע במטרה להשיג סיסמאות כניסה לתיבות דואר של אנשים שקשורים לארגון המותקף, למשל באמצעות חבירה אליהם ברשתות חברתיות כגון פייסבוק ולינקדאין. לאחר מכן מבוצעים חדירה לתיבת הדואר של הקורבן ומשלוח של מסמך תמים לכאורה שבעצם מכיל סוס טרויאני. החברים של המתחזה פותחים ומפעילים את התוכנה הזדונית, ללא ידיעה.

"יש לעבור לפתרונות הגנה לא מסורתיים"

מוטי שגיא, יועץ בכיר לאבטחת מידע בפורטינט, אמר שיש זן חדש של איומים מצידם של "האקטיביסטים", כמו אלה שפגעו באתרים של ממשלות סין, אסטוניה וגיאורגיה. הוא ציין שהאקרים מסוג זה יזמו את מתקפות הסייבר על אתרי הבורסה בתל אביב ואל על, שלא לדבר על ההאקר הסעודי, שחשף מספרי כרטיסי אשראי של ישראלים.

"אנחנו עדים למעבר מ'סתם' פריצות למתקפות APT ממושכות על מטרה מוגדרת מראש", אמר. "חייבים לעבור לפתרונות הגנה לא מסורתיים מפני מתקפות כאלה, מפתרונות מבוססי חתימות לפתרונות פרו-אקטיביים, כאלה שיודעים להתמודד עם איומי זמן אפס. הפתרונות צריכים לתמוך גם בתוך הפיזי וגם בתוך האלחוטי".

לאחר מכן הציג שגיא את מערכת התוכנה Application Control, שבוחנת את התנהגות המשתמש ואם יש סטייה - היא מתריעה. כמו כן מציעה פורטינט גלאי הסורק את רשת הרדיו ומחפש פגיעויות במתגים האלחוטיים.

הגנה ממוקדת באמצעות זיהוי אנומליות

ד"ר **גיל דוד**, מנכ"ל חברת הייעוץ Brainstorm, אמר ש-"מתקפות APT הפכו קשות בשנים האחרונות". הוא מנה ביניהן "מתקפות ממוקדות על כורים גרעיניים, השתלטות על תחנות כוח והחשכה של ערים שלמות, הדלפת מידע מסווג מארגונים ביטחוניים, גניבת כרטיסי אשראי במסות, השתלטויות על אתרי מסחר המרכזים טריליוני דולרים ותולעים המתפשטות למיליוני מחשבים בתוך דקות".

"כל ההתקפות הללו קרו, קורות ויקרו יותר בעתיד", אמר. "הן מאיימות על הביטחון הלאומי של מדינות. מתקפות APT הן מתקפות מאוד מתוחכמות שנבנות במאמצים רבים. הן עובדות לאט ונמוך מתחת לרדאר. מדובר בהתקפות שעוברות אמצעי הגנה ובלתי ניתנות לזיהוי, והן נבנו במיוחד לארגון ספציפי". כמו כן, הוא ציין ש-"לתוקף יש הרבה מוטיבציה, הרבה סבלנות, משאבים גדולים וכוח אדם טכנולוגי מיומן".

"נגד אותן מתקפות יום הדין הגיע הזמן להכניס למערכה את ה-Dooms Day Analysis And Mining, שבעזרתו אפשר להשביח את מערך ההגנה", הוסיף ד"ר דוד. לדבריו, "הדרך שבה פועלות מערכות אלה היא באמצעות זיהוי אנומליות. אנומליה היא תבנית שחורגת ממידע נורמלי שראינו בעבר, מידע שאנחנו מצפים לראות אותו במקום שבו אנחנו נמצאים. אותן אנומליות מתורגמות לאינפורמציה קריטית, שיכולה להעיד על שינוי משמעותי מההתנהגות הנורמלית".

הוא ציין, כי "על ידי זיהוי אנומליות אפשר להגיע להגנה ממוקדת, שנבנית אוטומטית וספציפית עבור הארגון והמשאב עליו רוצים להגן".

Techeads 2012 Q1
יריד התעסוקה של ההיי-טק בישראל
יום ג', 06.03.2012,
Airport City ,Avenue
בין השעות: 09:00-16:00
www.pc.co.il/yarid