

## "שכחנו שצריך להגן על היישום"

"יש להעמיד את היישום במרכז מאמצי אבטחת המידע. ענף אבטחת המידע איבד את המיקוד שאמור לכוון אותו, אנחנו כבר לא ממוקדים במה שאנחנו צריכים להגן עליו. שכחנו שצריך להגן על היישום", כך אמר **צורי תמם**, מהנדס פריסייל בכיר ב-F5 Networks ישראל.



צורי תמם

לדברי תמם, כשבודקים את התקפות הסייבר שהופנו נגד מדינות שונות רואים שרק בחלק קטן מהן ההאקרים תקפו מטרות ישראליות. כך או כך, הדבר המשותף לכל ההתקפות העיקריות הוא שהן כוונות ליישומים.

הוא הציע להתייחס בעת טיפול בהתקפות להיבטים שונים, כגון היקף, משתמשים וכוונות נזק. "הסיבות להתקפות יכולות להיות שונות - כסף, תהילה, סיבות פוליטיות, שעמום, רוע לשמו או אפילו כדי לאפשר לתוקף להתאמן", אמר תמם. "בכל מקרה, התוקפים ממקדים את עיקר המאמצים ביישום, כדי לפגוע בעסק של הארגון המותקף. יש לזכור שהיישומים הם הדרך שבה העסק מחצין את עצמו ולא משנה היכן הוא נמצא. צריך לאתר דרך להגן על היישום בלי לסמוך על אף מנגנון אחר". "האקרים לעתים מייצרים מסך עשן, כדי להסתיר התקפה אמיתית", הוסיף תמם. "הם יכולים לנסות לפגוע במוניטין של ארגון. מספיק שכותבים שאתר של עסק מסוים הושבת למשך כמה דקות - דבר שברור שניתן לעשות - והנזק כבר נגרם. ללקוח שקורא את זה לא משנה איפה יושב האתר שהותקף. קיימים ערוצי תקיפה נפוצים שונים, אבל הפגיעויות נחשפות בסופו של דבר ביישום".

תמם דיבר בהמשך על F5 וציון שהכנסותיה עומדות על כ-1.4 מיליארד דולרים. הסיניף הישראלי של החברה מונה 120 עובדים, רבים מהם אנשי אבטחת מידע, ולו כ-400 לקוחות.

"העובדה שאנחנו מספקים בקר העברת יישומים (Application - ADC Delivery Controller) מאפשרת לנו להימצא במיקום מאוד מרכזי ברשת של הארגון. מיקום כזה מאפשר לנו לנהל אבטחת מידע בצורה הולמת. פתרון ה-TMOS של F5 מספק את היישום באשר הוא למשתמש ושם דגש על זמינות ועל אבטחת מידע. לשם כך צריך להבין את הפגיעויות הרלבנטיות".

פתרון נוסף אותו ציון תמם הוא BIG-IP. "מדובר בקופסה אחת שמספקת את היישומים ולקוחותינו שמים אותה לפני הפיירוול. אנחנו מסתמכים על עקרון ה-Reverse proxy, לפיו המשתמשים לעולם לא נוגעים ישירות ביישום. מי ש'מדבר' עם היישום הוא הרכיב שמסתיר אותו. כל זאת בפלטפורמה אחודה שיש לה גם יכולות חכמות של ניהול זהות, הפחתת סיכונים והצפנה. אנחנו עושים סקירה של האבטחה שמה שנמצא במרכז שלה הוא היישומים. הפלטפורמות של F5 מסוגלות לתת מענה למתקפות Zero Day - מתקפות שלא הוכרו קודם לכן".

## "חשפנו את מאורטיניה, ההאקר שפרץ לאתרים ישראלים"

בישראל נשמו אמנם ררווחה לאחר שאנשי אנונימוס לא הצליחו לבצע את תוכניתם להשבית את האינטרנט הישראלי במבצע #Oplrael, אולם "המתקפה הזאת הצליחה יותר מאשר מספרים לנו", אמר **גיא מזרחי**, מנכ"ל סייביריה ובעלים בסייבר-האט. לדבריו, אנשי החברה הצליחו לגלות את ההאקר שעמד בראש המתקפה.

במהלך ההרצאה, שהתקיימה תחת הכותרת "יומנו של האקר", הסביר מזרחי, כי בניגוד למה שנאמר בתקשורת, #Oplrael לא הייתה כישלון חרוץ. "יש במתקפה הזאת הרבה דברים שלא התגלו", אמר. הוא ציין, כי "הצלחנו לזהות מיהו מאורטיניה, אותו האקר שעמד בראש המתקפה. בניגוד לשמו, הוא מתכנת צעיר בן 23 בשם יעקוב שמגיע דווקא מטוניסיה וחבר בקבוצת Tunisian Hackers Group. הצלחנו לזהות גם את יתר חברי הקבוצה. אלה הצליחו לגייס לצורך המתקפה את אחת הקבוצות המשמעותיות באנונימוס - Anonghost, שגם אליהם חדרנו".

"למרות מה שאומרים, אפשר להגיע לאנשי אנונימוס", אמר מזרחי. עם זאת, הוא הזהיר ש"הם כבר תקפו את מי שחשף אותם בעבר. יש להם האקרים טובים ביותר, רובם צעירים שעובדים בחברות היי-טק, ואסור לזלזל בהם".

"אני מחזיק כלים ויכולות המגיעים לחלקים באינטרנט מהם אני מייצר ידיעות רלוונטיות על חברות המחזיקות בנכסי מידע של הארגון, ידיעות על חולשות אבטחה חדשות ודרכי התמודדות, מודיעין ממוקד, איכותי ורלוונטי", ציין מזרחי. "הרעיון הבסיסי הוא לזהות היערכויות נגד הארגון, לזהות מוקדם את קטורי התקיפה ולאפשר לארגון לבצע היערכות ממוקדת נגד המתקפה שעתידה לקרות. הלקוחות מקבלים דו"ח חודשי או שבועי רמת המתקפות על הארגון ושירות התראות ממוקד שמתריע מתי אנשי אנונימוס עתידים לתקוף אותם".



גיא מזרחי

"כמעט כל הארגונים מותקפים. זו עובדה בסיסית", ציין מזרחי. "כל ארגון שיש לו לפחות כתובת IP אחת מותקף על ידי סינים או גורמים אחרים. נורטל לא קיימת בגלל ריגול סיני. כל חברה שעובדת מול חברה סינית צריכה להיות מוכנה למגננה מפני מתקפות קיברנטיות".

הוא ציין סוגים שונים של פשיעת סייבר: "פעילות עבריינית מזדמנת, פשעים של הזדמנות; פעילות רשת עבריינית סדורה - מפעל לפשיעת סייבר; ופעילות עבריינית נתמכת ברשת, קרי: פשיעה "רגילה" שנעזרת במימד הסייבר. סוגי הפשיעה המוכרים ביותר הם מתקפות למניעת מניעת שירות (DDOS) והונאות כרטיסי אשראי. ישנם אתרים שמוכרים זהויות ומאפשרים מתקפות ממוקדות. כאשר לקוח שלנו מקבל מכתב איום, יש באפשרותנו לדעת האם זה איום אמיתי או משהו שלא צריך להתייחס אליו".

## "אפילו שעון נוכחות יכול לשמש לפריצה לרשת"

"חברת החשמל לוקחת ברצינות את היותה חברת תשתית חיונית: היא עושה את כל הדרוש כדי שגורמים עוינים לא יחדרו לרשת המחשבים שלה, ולא משאירה שום פירצה, אפילו לא שעוני נוכחות או מכונות קפה" - כך אמר **משה מורגנשטרן**, אחראי אבטחה בחברת חשמל באזור הצפון. מורגנשטרן תיאר את מערכת בקרת הגישה, האוכפת את מדיניות השימוש ברשת חברת החשמל. "קיבלנו משימה ב-2006 - ליישם בקרת גישה לרשת המוצר, SWAT, שנאכף עלינו על ידי גוף אבטחת המידע בחברת החשמל. המימוש בוצע על ידי XOR. הקמנו שתי מערכות: במרחב דרום - מאילת עד נתניה, ובמרחב צפון - מנתניה עד קריית שמונה וצפון רמת הגולן. המערכות נתנו מענה לבקרת גישה ברמת אישורי גישה, תוך חינוך המשתמשים. כך, לאחר שמתמש ידע שאם הוא מפקיר