ברוכים הבאים לחדר המזוהם

סיור מאחורי הקלעים של המרכז לחקר הנוזקות של ענקית אבטחת המידע סימנטק ◆ כך נראה "קו החזית נגד הרעים" ◆ כתב אנשים ומחשבים סייר במוקד האיומים וחזר עם כמה תובנות

יוסי הטוני

נורמנים, אשר שמם נגזר מכינוי ל"אנשי הצפון", היו פולשים סקנדינבים, במיוחד ויקינגים-דנים, אשר במהלך המאה ה-12 פלשו לאי האירי ולבירתו והצליחו להשתלט עליו. היום, כשרוב המלחמות הפיזיות כבר לא נערכות כל כך מערבה ביבשת הישנה, צריכים בדבלין להתמודד עם פולשים שונים לגמרי, אבל לא פחות מסוכנים.

מרכז שירות הלקוחות של סימנטק לבריטניה ולאירלנד שוכן בפאתי הבירה האירית, ובאחד האגפים בבניין של ענקית האבטחה, מנסים אנשי החברה להתמודד מול "הרעים" החדשים - וירוסים, תולעים ושאר נוזקות. שליח אנשים ומחשבים סייר במרכז של ענקית אבטחת המידע, Symantec Security Response Centre, וחזר עם כמה תובנות מעניינות.

"למרות שמרכז התגובה נמצא באותו בניין, האגף הזה, שבו אנו מנתחים נוזקות - נפרד ממנו לחלוטין", אמרה **אורלה קוקס**, ממנהלות מרכז התגובה. לדבריה, הבידוד מתבצע במערכות תקשורת ומיחשוב נפרדות, כמו גם העדר יכולת ליצור תקשורת אינטרנט אלחוטית. "לא סתם האגף מכונה אצלנו 'החדר המזוהם', בהשאלה מעולם בתי החולים. פה אנו יכולים לטפל בנוזקות, לחקור אותן לעומק, בלא חשש שמשהו מהפעולות שנעשה יפגע בשאר מחשבי החברה ובלקוחותיה", אמרה.


אורלה קוקס

לדבריה, "מרכז התגובה שלנו הוא קו החזית מול הרעים. פה אנו אחראים לזיהוי, גילוי, ניתוח ויצירת תגובת-נגד לכל הסוגים האפשריים של המתקפות". קוקס עובדת בענקית האבטחה 16 שנים, והייתה אחראית לניתוח של כמה מהנוזקות המפורסמות, ביניהן סטוקסנט וקונפיקר. מרכז התגובה באירלנד הוא אחד משלושה בעולם של החברה, ופועל לצד שני מרכזים דומים, בארה"ב וביפן. המרכז מונה 70 חוקרים, ואף שהדבר לא צוין, יש להניח כי חלקם הם האקרים לשעבר ש"חצו את הקווים", ועברו לעבוד עם הטובים. לדברי קוקס, "במרכז עושים שני דברים. האחד, מפיקים תובנות ובינה מודיעינית על כלל האיומים, והשני - נותנים מענה להם, משמע מספקים יכולת תגובה".

היא ציינה כי בניגוד לעבר, "כיום הלקוחות רוצים לדעת לא רק את מהות האיומים ואת הדרך להתגונן מפניהם - אלא גם את זהות התוקפים. מדובר בסוג שונה של מחקר, וגם אותו אנו מספקים. הדבר קשה לעיתים כי התוקפים ברובם לא נוטים להזדהות, ומשתמשים בטכניקות שונות של הסוואה, כגון שימוש בשרתים ממדינות שונות, או שימוש במחשבי זומבי (מחשבים שהשתלטו עליהם מרחוק, בלא ידיעת בעליהם)".

על בסיס התובנות המופקות מהחקר של הנוזקות מנפיקה ענקית אבטחת המידע את דו"ח האיומים השנתי - ISTR (Internet Security Threat Report) שלה, זה 19 שנים.

מענה תוך פחות משעה

על פי קוקס, "ברגע שאנו מבחינים בהתפתחות של טכניקה חדשה של איומים, אנו מנתחים אותה לעומק וממהרים לעדכן את ההגנות שלנו. אם המדובר באיום רציני, העדכון ייעשה בתוך פחות משעה. במקביל, יש לנו יעד לא פחות חשוב והוא לצמצם את כמות התראות השווא. המטרה היא לקבוע בתוך דקות מועטות אם קובץ כלשהו מכיל חומר זדוני או לא, ואם המענה הוא חיובי - לנתח אותו במשך שעות או ימים. אנו עסוקים רבות בהתלבטויות מה 'מעניין' ומה לא. על סטוקסנט, למשל, עבדנו ששה חודשים".

בנוסף לחקר הנוזקות לכשעצמן, אמרה קוקס, "עלינו להבין את ההקשר שלהן. עלינו להבין האם חל שינוי במפת האיומים, מהן המגמות הכלליות, מעבר לגילוי נוזקה חדשה ספציפית זו או אחרת. אנו מנסים למצוא קשרים והקשרים בין תוקפים ובין תוקפים - ובין תוקפים ובין נוזקות. מיפוי שכזה מייצר יכולות הגנה טובות יותר".

פעמים רבות, אמרה קוקס, "המוצרים שלנו, המותקנים אצל הלקוחות, משמשים כמעין 'מרגלים' המדווחים לנו על איומים חדשים או על תוקפים שלא ידענו עליהם". היא ציינה כי מקורות נוספים למידע על הנוזקות הם "מלכודות דבש" אותם החוקרים יוצרים באופן פעיל ותדיר, ניתוח תעבורת מיילים, וכן מודיעין קוד פתוח, OSINT - מידע מודיעיני שנאסף ממקורות זמינים לציבור. יצויין כי המינוח אינו קשור לקוד פתוח של תוכנה. עוד מקורות, לדברי קוקס, הם רשויות אכיפת חוק בעולם וגופי אבטחת מידע למיניהם, אשר עימם ענקית האבטחה עובדת בשיתוף פעולה.

במרכז לחקר הנוזקות, אמרה קוקס, "בנינו שלוש מערכות - RATS, SPANC ו-Pokemon. המערכות הללו מאפשרות לנו להבין טוב יותר ובאופן מפורט ומעמיק יותר את הנוזקות והסביבה שלהן. המערכות 'מקליטות' את הנוזקות ומספקות לנו תמונת מצב על ההקשר שלהן. המערכות המנתחות עונות על שלוש שאלות: מיהו התוקף, משמע זיהויו, למה הוא תקף ומתי. כך אנו מקבלים את היכולת לקשר בין המתקפות ובין התוקפים. זיהוי התוקפים הוא החלק המאתגר ביותר". לשאלת אנשים ומחשבים השיבה קוקס כי "רוב המתקפות נועדו לצורך גניבת קניין רוחני, ובעקיפין - ליצירת כסף. המניע השני למתקפה הוא ריגול תעשייתי". על פי קוקס, "אנו משתפים פעולה עם המשטרה בשני תנאים - שיש אישור של הלקוח שהותקף לעשות זאת, ושאנו יודעים בוודאות את זהות התוקפים. מדובר במצב נדיר. לרוב אנו יודעים רק 'בערך' מיהו או מיהם התוקפים - ופועלים ליצירת יכולת מניעה והתגוננות".

צמיחה בכמות המתקפות

על פי **פול ווד**, מחבר הדו"ח השנתי, כמות המתקפות נגד אתרים צמחה משמעותית בשנה החולפת - כמות המתקפות היומית הממוצעת על אתרים עמדה על 568,700 - נתון המשקף גידול של 23% לעומת 464,100 מתקפות ב-2012. מדי יום, ציין ווד, הם גילו 1.6 מיליון וריאציות חדשות על נוזקות קיימות. ווד אמר כי הם מחלקים את התוקפים