

לרשת המותקפת ומנסה להתקשר עם השרת שלו. ברגע שהפוגען מצליח לדבר עם השולח שלו, מתחיל השלב הרציני של התקיפה, שכולל תנועה בתוך הארגון ואחר כך גם הזלגת המידע החוצה מתוך הארגון אל הארגון התוקף." גם תמיר מציע להשתמש ב-ADS - Advance Detection System לצורך ניתוח המידע באמצעות ביג דטה ואיתור ערוצי השליטה והבקרה של הנוזקות: "ברגע שמנתקים את הקשר בין הנוזקה לשולחיה, כבר מצמצמים את הנזק.

"שיטה זו מאפשרת גילוי משפחות שלמות ולא מוכרות של פוגענים. המערכת חוקרת למעלה מ-300 מאפיינים של תקשורת, עורכת עליהם סטטיסטיקות ויודעת מה שונה ומה לא נראה למערכת מתאים על פי מודלי לימוד המכונה".

רון קינג: " בשנים האחרונות משתמשים ב-DMZ כדי לשתף מידע עם לקוחות, ספקים, ומשתמשים מרוחקים. כתוצאה מכך יש צורך בהכפלת המידע - בתוך הארגון ובאזור ה-DMZ שהפך גם עדין להאקרים"

תמיר סיכם: "מודיעין היא הזרוע החסרה והזרוע הבולטת שיכולה לתת לארגונים ולחברות את ההגנה הטובה ביותר מפני התקפות סייבר וכדי להבין מההיסטוריה מהן מתקפות באמצעות ניתוח של מיליוני מתקפות שקרו בעבר".

אזור ה-DMZ הפך גן עדן להאקרים

רון קינג, סגן נשיא לניהול שיווק בחברת Safe-T תיאר את שינוי הגישה בתפקיד ה-DMZ: "לפני רשתות ה-DMZ כל מי שרצה

מידע מהארגון היה עובר דרך הפירוול ונכנס לשרת וכשהוא בפנים הוא היה גם האקרים ניצלו את המצב הזה. יכלו לשרוק את הפירוול, לגלות פורטים פתוחים, להיכנס, לגנוב מידע או לשבש את הרשת.

"המטרה הראשונית הייתה להוציא את המידע מתוך הרשת הפנימית את המידע שרוצים לשתף לרשת ה-DMZ. כל עוד זה היה מידע סטטי, לא הייתה בעיה אבל בשנים האחרונות משתמשים ב-DMZ כדי לשתף

מידע עם לקוחות, ספקים, ומשתמשים מרוחקים. כתוצאה מכך יש צורך בהכפלת המידע - בתוך הארגון ובאזור ה-DMZ שהפך גם עדין להאקרים. ישנה גישה חדשה שבה המידע חוזר לתוך הארגון, אך התקשורת איתו עוברת דרך ערוץ מאובטח וייעודי לפי המשתמש".



רון קינג

גיא תמיר: "לתוקפים יש את כל הזמן שבעולם. הם צריכים רק הזדמנות אחת קל מאוד היום לאסוף מידע על הרגלי המשתמשים, מידע שיאפשר לפרוץ את הסיסמאות או את מערכות ההגנה שהם מרכיבים. אם זה לא הולך"

מחשבים פרוצים וכל זאת בתוך פחות משעה. "רוב המכשירים שנמצאו בסריקה היו נתבים ביתיים, שהוא תחום מאוד פריץ, אך גם מכשירים כגון מערכות לפתיחה מרחוק של דלתות בבתי כלא לא היו מוגנים בסיסמאות יצירתיות".



שחר טל

להשתמש ב-Big Data לטובת אבטחת הסייבר

"יש צורך להשתמש בשיטות של ביג דטה כדי לנתח מתקפות קודמות וללכוד מתקפה בעת התרחשותה. "כך מציע **דורי פישר**, CTO בחברת WE-ANKOR המסכם גם עשור לחמ"ל הסייבר הלאומי וניסיון בהטמעת SIEM SOC.

הוא המשיך והסביר, ש"הנחת העבודה היא שכל ארגון הוא מטרה, ואין סוף לאפשרויות, עובדה שאפילו פתרונות כגון AIRGAP לא עובדים.



דורי פישר

דוגמא טובה לכך היא מה ששמענו מאדוארד סנאוודן, שה-NSA השתיל רכיבי חומרה בתוך לוחות מבוססי USB המשרדים מידע החוצה בגלי רדיו."

"הדרך לתקוף את בעיית הגילוי היא להבין מה הסיכון - למשל אובדן מידע. אחר כך אפשר להחליט אילו מערכות להפעיל ובנוסף צריכים

לדעת מה לעשות כשאין תרחיש, ואז צריך להבין את המערכות שלנו ואת התהליכים שלנו, ולזכור שכל הידע חייב להישאר במוצר ולא אצלנו".

"מספיקה היום הצלחה אחת כדי שכל עבודת ההגנה תרד לטימיון"

גיא תמיר, דירקטור ניהול מוצר ורינט באמן דיבר על האסימטריה במתקפות הסייבר: "הפורצים הולכים על מקומות פגיעים, וכך מספיקה הצלחה אחת כדי שכל עבודת ההגנה תרד לטימיון.

"לתוקפים יש את כל הזמן שבעולם. הם צריכים רק הזדמנות אחת. קל

מאוד היום לאסוף מידע על הרגלי המשתמשים, מידע שיאפשר לפרוץ את הסיסמאות או את מערכות ההגנה שהם מרכיבים. אם זה לא הולך, אז תמיד אפשר לתת כמה מאות דולרים למישהו כדי לדחוף דיסק און קי למחשב אליו רוצים לחדור. "בשלב הראשון: הארגון התוקף אוסף כל מידע



גיא תמיר

שהוא יכול על הארגון המותקף - מערכות הפעלה, אנטי וירוס, חברת אבטחת המידע המספקת שירותים לחברה ועוד. הם גם עובדים דרך רשתות חברתיות. בשלב השני בונים את כלי התקיפה תוך שימוש בכל המידע שהגיע מהשלב הראשון. בשלב השלישי והקריטי, הפוגען מוכנס