

קיברנטי", אמר ווד, "הפוטנציאל לרווחים שארגוני פשע מאורגן ישלמו להאקרים עבור מתקפות ענק מוצלחות הוא ענקי. לכן ברור כי מתקפות הענק הן כאן, והן כאן כדי להישאר". לדבריו, "חברות מכל הגדלים צריכות לבחון מחדש, לחשוב מחדש ואולי גם לבנות מחדש את ארכיטקטורת אבטחת המידע שלהן, בהתחשב בהיקף האימונים החדשים".

לפי ווד, "מה שמנהלי אבטחת המידע הארגוניים נדרשים לעשות, הוא לדעת את הנתונים של הארגון, משמע ההגנה צריכה להתמקד במידע - ולא במגוון המכשירים של העובדים, או בדטה סנטר. יש לדעת את כל מה שנדרש אודות הנתונים הארגוניים הרגישים, עסקית או אישית, ובהם נדרש להתמקד בהגנה". היבט נוסף, לדברי ווד, הוא "הצורך בחינוך של העובדים. על דרגי ההנהלה בכלל ועל מנהלי אבטחת המידע בארגונים בפרט לפעול להעמקת



חדר המצב המנטר את האימונים בעולם בזמן אמת

ההדרכה בנושאי אבטחת מידע, תוך שימת דגש על מגוון האימונים. כל ארגון צריך שתהיה לו מדיניות אבטחת מידע, עם נהלים להגנה על נתונים רגישים, אשר מצויים במכשירים האישיים והעסקיים של העובדים".

ווד ציין כמה מגמות חדשות שהופיעו בשנת 2013, הצפויות להימשך השנה. האחת, ביצוע מתקפות על כספומטים, בשל העובדה כי 95% מהכספומטים בעולם מבוססים מערכת הפעלה חלונות XP, שתוקפה עומד לפוג בתוך שבועות. השנייה, גידול של ביצוע "חטיפות לצורך כופר" של אתרים. בשנה החולפת, אמר ווד, חל גידול של 500% בהיקף חטיפות אתרים, נתון שבחודשים מסויימים עמד על 100-200 חטיפות ובחודש

נובמבר האחרון עמד על יותר מ-900 מקרים שכאלה. נעילת האתרים, ציין ווד, מבוצעת תוך השתלטות מרוחק על האתר ודרישה לתשלום כופר בן מאות או אלפי דולרים תמורת "שחרור". המתוחכמים שבחוטפים, ציין, לא "סתם" מורידים את האתר מהאוויר, אלא משאירים אותו עובד - אך נטול גישה אליו בשל ביצוע הצפנה של קבצים בו.

מגמה נוספת שצמחה ב-2013 ונמשכת השנה, אמר ווד, נוגעת לשימוש בהדבקה של נזקות באמצעות הרשתות החברתיות והמכשירים הניידים, "הטלפון החכם הפך לשלוחה של ה-PC, וקל יותר להדביק באמצעותו בנוזקות". כך, ציין ווד, 38% מבעלי הטלפונים החכמים חוו בשנה החולפת פעילות

של עבריינות קיברנטית על המכשירים שלהם. הוא סיכם באומרו כי "ביצוע מתקפות משולבות, בעולם הנייד וברשתות החברתיות, הוא המגמה השלטת השנה".

סיור העיתונאים הסתיים בהדגמות חיות של פריצות למחשבים ניידים, לטלפונים חכמים וכניסה לאתרים של האקרים בשוק השחור של המידע. עוד נכנסו החוקרים לאתרים - אף הם של האקרים - בהם מפורטים נתונים סטטיסטיים על היקף השימוש בכל כלי וכלי פריצה, מידת יעילותו, היקף הפגיעה שלהם, כמות המסמכים שנגנבו, אופי ופירוט המסמכים הגנובים, שוויים ועוד.

\* הכותב היה שליח אנשים ומחשבים לאירלנד

"גניבת מידע תהיה קלה מחר יותר מאשר היא קלה היום", סיכמה ג'ון, "כי המידע, שכבר כיום הוא נגיש ולא מאובטח - יהיה עוד יותר נגיש ועוד יותר לא מאובטח מחר - ובעיקר יהיה הרבה יותר מידע. השוק השחור העתידי במידע זה הוא רק עניין של זמן - עם מציאת הערך הכלכלי שלו. כשימצא הערך הכלכלי - המידע ייגנב, בוודאות".

### "לפושעים נולדה תכונה חדשה - סבלנות"

"מה שהפתיע אותנו הוא שנולדה אצל הפושעים הקיברנטיים למיניהם תכונה חדשה - סבלנות. הם הפנימו כי התועלת הכספית שתנבע להם

ממתקפת ענק, Mega breach, או פוטנציאל הנזק ממתקפה כזו, הם כמו ביצוע של 50 מתקפות 'קטנות', ולכן היה כזה גידול בהיקף מתקפות הענק", כך אמר פול ווד, סימנטק, לאנשים ומחשבים.

ווד התראיין לאנשים ומחשבים במסגרת פרסום דו"ח האימונים השנתי של ענקית אבטחת המידע, עליו הוא אמון בחברה. השנה היא השנה ה-19 להפקת הדו"ח.

לדבריו, "מדובר בשינוי התנהגותי משמעותי מבחינת עברייני הסייבר. הם נערכים לביצוע כל מתקפת ענק במשך חודשים. הם מבינים כי מתקפות אלה עדיפות מבחינת הערך הכספי של המידע שייגנב", הוא הסביר.

על פי ווד, "גם השנה המשיכה המגמה שמאפיינת את המתקפות בשנים האחרונות,

של גידול ברמת התחכום שלהן, כמו גם בהיקפן". מגמה נוספת, לא מפתיעה, לדברי ווד, "היא שההגנה והאבטחה הפכו לקשים יותר למימוש, לעומת הקלות הבלתי נסבלת של ביצוע הפריצות והמתקפות. הדבר משפיע באופן משמעותי על המוניטין של הארגונים שהותקפו, מהם נגנבו סוגים שונים של פרטים אישיים - מספרי כרטיסי אשראי, חשבונות בנק ורשומות רפואיות".

### הצלחת העברין הקיברנטי

"אין דבר המוביל יותר להצלחה כמו הצלחה - בייחוד אם אתה עברין

### פול ווד: "מדובר בשינוי התנהגותי

### משמעותי מבחינת עברייני

### הסייבר. הם נערכים לביצוע כל

### מתקפת ענק במשך חודשים. הם

### מבינים כי מתקפות אלה עדיפות

### מבחינת הערך הכספי של המידע

### שייגנב"