

של טרואינים המצפינים את המידע על מכשירים ניידים ומונעים גישה לתמונות, אנשי קשר והודעות - עד שישולמו דמי חסות להסרת החסימה. סמארטפונים מבוססי אנדרואיד יהיו ללא ספק הראשונים שיוחקפו.

תקיפות בעננים

"האקרים מכוונים את פעילותם נגד עובדים בשירותי ענן", קובעים חוקרי קספרסקי, "מאחר והם מזהים בהם את החוליה החלשה בשרשרת האבטחה. התקפה מוצלחת יכולה להעביר לידי עברייני הסייבר את המפתחות להיקפים עצומים של נתונים. בנוסף לגניבת מידע, התוקפים עלולים גם למחוק או לשנות מידע. במקרים מסוימים, יצירת מידע שגוי יכולה להיות בעלת ערך גבוה אף יותר עבור מזמיני המתקפות, מדובר במגמה מתמשכת".

בתחזית של סימנטק נכתב, בין השאר, כי "אנשים סוף סוף יחלו לנקוט צעדים פעילים כדי לשמור על המידע פרטי שלהם". עוד מציינים חוקרי ענקית האבטחה, כי "הרמאים, אספני הנתונים והפושעים הקיברנטיים לא יתעלמו מאף רשת חברתית, לא משנה כמה 'נישיתית' או חבויה היא". לגבי מגמת "האינטרנט של דברים", מציינים החוקרים, כי מגמה זו תהפוך ל"אינטרנט של פגיעויות".

עלייה במתקפות נגד SMBs

כל חברות האבטחה סמוכות ובעטות כי 2014 תאופיין בעלייה חדה במתקפות כנגד חברות קטנות ובינוניות (SMBs). פושעי סייבר יתקפו יותר ויותר חשבונות בנק בשווי 70-15 אלף דולרים. בסייבר ארק מאמינים, ש"זהו מקום טוב לאותם פושעים, כיוון שלעסקים קטנים יש בדרך כלל אמצעי הגנה דלים ואין להם המשאבים הדרושים כדי להגיב באופן פרואקטיבי למתקפות כאלה. זאת, בעוד שהמתקפות הראוותניות נגד תאגידים גדולים ימשיכו להיות מונעות מטעם גופי ביון של מדינות או מריגול תעשייתי".

לסיום, קובעים בסייבר ארק, צפוי גידול במתקפות מטעם מדינות: "חשיפת תוכניות הריגול של ה-NSA, ה-GCHQ (סוכנות הביון הבריטית) וסוכנויות ביון אחרות - יצרה תקדים באשר לדרך שבה ממשלות משתמשות באינטרנט ובטכנולוגיה להגנה לאומית. נראה יותר ויותר מדינות שהולכות בדרך הזאת ואף מעבר לכך - הן בפיקוח על פעילות אינטרנט בשטחן, והן בתקיפות סייבר ופעילות אינטרנט מעבר לשטחן.

השחקניות המרכזיות בזירה (ארצות המערב, איראן, סין ורוסיה) ימשיכו לחדד את פעילות הסייבר שלהם, ובנוסף יצטרפו שחקניות חדשות ליזרה ואף קבוצות טרור במימון ממשלות. כפי שראינו במקרה של סטוקסנט, התקפות מתוחכמות של שחקנים גדולים יילמדו על ידי אחרים, שיתאימו אותן לצורכיהם, ושיתו את התקפות יועתקו. ב-2014 נראה עוד התקפות מסוג זה, ממגוון רחב של סיבות - כלכליות, פוליטיות, וטרור".

היא חדירה לקבוצות סגורות בלינקדאין, שחבריה מניחים שההאקר הוא חבר בקבוצה וניתן לחשוף בפניו פרטים סודיים, עסקית או ביטחונית".

שוק ההאקינג מתמסחר ועובר לעבודה במודל Cyber-Crime-as-a-Service: הגידול בכמות כלי העבודה להאקרים, לצד ריבוי דלתות אחוריות באינטרנט, תורמים לצמיחת שוק שחר המתפתח במהירות, שמאפשר לכל אחד לשכור את שירותיו של האקר. "ההתמסחרות של שוק פושעי הסייבר תביא לגידול במספר המתקפות", קובעים חוקרי סייבר ארק. הם מציינים בנוסף, כי יחול ב-2014 גידול במגמת רכישות גישה לסיסמאות אדמיניסטרטיביות ולהרשאות.

"האיום העיקרי - מערכות הפעלה לא מעודכנות"

על פי טרנד מיקרו, מערכות הפעלה שאינן מעודכנות ושאין מטולאות (Unpatched) יהוו השנה איום עיקרי. החברה אף ציינה, שהמתקפות הממוקדות העיקריות צפויות להיות מתקפות יום אפס.

התחזית של מעבדות FortiGuard של פורטינט צופה לשנה הנוכחית "איומים על מערכות אנדרואיד, מערכות בקרה תעשייתיות (ICS/SCADA), התקנים לבישים, טאבלטים ומערכות שליטה ביתיות".

עוד חוזים בחברה, כי "פושעי הסייבר ייאבקו זה בזה ב-Deep Web: ה-FBI ימשיך לנגוס ברשת Tor האפלה ובשירותי שיתוף קבצים מפוקפקים כמו Megaupload. הפיקוח המוגבר יביא לגרסאות חדשות ומשופרות, שיהיו קשות עוד יותר לחדירה". על פי התחזית, יהיו בנוסף רמת פיקוח מוגברת ונשיאה באחריות מול ספקי אבטחת הרשת. "לקוחות ידרשו הוכחה, וכאשר הם יהיו חשופים לסיכון שלא לצורך הם ידרשו נשיאה באחריות. הדבר יביא לשקיפות גדולה יותר סביב ניהול שרשרת אספקה, ניהול גרסאות מערכת הפעלה ופרקטיקות (SDL (Secure Development Lifecycle). החברה אף צופה עליית בפגיעות של מערכות ההפעלה החל מ-8 באפריל, אז תפסיק מיקרוסופט את התמיכה בחלונות XP. מערכת ההפעלה הלא חדישה נמצאת עדיין בשימוש ביותר מ-30% ממחשבי PC-ה בעולם.

השפעה של אדוארד סנואודן תימשך

על פי מומחי קספרסקי, "אירועי אדוארד סנואודן וחשיפותיו לגבי היקפי האזנות של ה-NSA ישפיעו גם על 2014. המשתמשים, יותר מאי פעם, נחוישים לשמור על פרטיותם. המשמעות היא הגנה על המידע המאוחסן במחשביהם ומאמץ להבטיח כי הפעילות המקוונת תישאר חסויה. מאמצים אלו יובילו לפופולאריות גדולה יותר של שירותי VPN ושל כלים לשמירת אנונימיות, כמו גם ביקוש גובר לכלי הצפנה מקומיים". ענקית האבטחה הרוסית גורסת, כי "עברייני הרשת ימשיכו לפתח כלים לגניבת כסף בצורה ישירה או עקיפה. כדי לשדוד את המשתמשים בצורה ישירה, ישפרו עברייני הרשת את כלי הגישה לחשבונות הבנק של בעלי מכשירים ניידים (פייסינג נייד, סוסים טרואיניים למגזר הבנקאות - "ה"), וכן צפויים פעילות נרחבת של רכישה וקנייה של בוטנטים ניידים, שימשו להפיץ קבצים מצורפים זדוניים בשם גופים חיצוניים". כדי לתמוך בגניבה עקיפה, נכתב, "נראה גרסאות מתוחכמות יותר