

אלו המורידים מחנות האפליקציות של החברה".
 "כמו כן, כאשר אפליקציה של אפל רצה על מכשיר נייד, היא מוגבלת ביכולתה להשפיע על אפליקציות שכנות ועל מערכת ההפעלה", הוסיף. "ועדיין, לדברי עמית, יש לאפליקציות יכולת לקנפג את המערכת באמצעות קובץ XML - דבר שמהווה נקודת תורפה. התוקף יכול להשפיע ולפתוח אפליקציות אחרות. אם רוצים לגנוב זהות, ישנה אפשרות לעשות זאת דרך פייסבוק או אתרים אחרים. כשהתקנו על מכשיר מערכת המדווחת אלינו על גישות לאפליקציות והסתבר לנו למשל שכל אפליקציות הבנקאות הגדולות פגיעות".

יובל נתיב, מנהל תחום תקיפה בחברת See Security, תיאר מערכת התנהגותית של קוד עוין. הוא הדגים כלי קוד פתוח הפועלים על מערכת חלונות XP, שמסוגלים בין השאר לשהות ברקע של המערכת תוך כדי בדיקה על כל התהליכים הפתוחים ומה המערכת עושה.

"פושעי הסייבר היו דומיננטיים מאוד בשנה החולפת"

"פושעי הסייבר ידאגו לתעסוקה לחברות אבטחת הסייבר בשנת 2014, כך אמר **בועז דולב**, מנכ"ל Clear Sky. דולב הציג את המסקנות שאליהן הגיעו בשתי החברות בשנת 2013: "פושעי הסייבר היו דומיננטיים מאוד בשנה החולפת. זיהינו גידול ניכר בפעילויות של מגוון קבוצות פשיעה - כשהבולטת שבהם היא קבוצה שמקורה ברוסיה אך מבצעת תקיפות בכל העולם. הנזק הכספי של תקיפות אלה מאיים על חברות ברמה האסטרטגית.

"קבוצת פושעי הסייבר מדגימה הלכה למעשה את האיומים הניצבים לפנינו, בין השאר על ידי שימוש מוגבר בתוכנות קבוצות המצפינות קבצים ודורשות תשלום תמורת מסירת מפתח. מדובר במגיפה שהדביקה מאות אלפי מחשבים בעולם. יש לציין שבעקבות השימוש ההולך והגובר בכסף



בועז דולב

וירטואלי, הביטקוין הפך לאמצעי חשוב בקרב פושעי הסייבר".
 דולב לא התעלם גם מהגורמים האנושיים המוכרים יותר: "האיום השני בחשיבותו היה הגורם הפנימי - מדובר באנשים מתוך המערכת שגונבים מידע, כאשר הדוגמה המוכרת לכולם היא, כמובן, אדוארד סנאודן. מקרים כדוגמת סנאודן בחברות פרטיות גרמו נזק אסטרטגי רב.

"חוקן מהגורמים הפנימיים, ישנם גם את ההאקטיביסטים - מפגיני הסייבר. בשנה החולפת בוצעו מספר רב של קמפיינים של גורמים מהסוג הזה, לרבות כאלה המגיעים ממדינות ערב. מדובר בקמפיינים שגרמו נזק לנכסים מקוונים, אבל כאן בישראל לא הרגישו אותו כל כך, בעיקר בזכות העובדה שיש כיום פתרונות

בועז דולב: "קבוצת פושעי הסייבר מדגימה הלכה למעשה את האיומים הניצבים לפנינו, בין השאר על ידי שימוש מוגבר בתוכנות המצפינות קבצים ודורשות תשלום תמורת מסירת מפתח. מדובר במגיפה שהדביקה מאות אלפי מחשבים בעולם"

על Wi-Fi בעזרת מגברים רבי עוצמה, במקרים שבהם אין גישה למחשב הקצה, ויש גם אנטנה ניידת שמשלתת על שידורי הסלולר, במחיר שאינו שווה לכל נפש - 40 אלף דולר", אמר.

שני אף דיבר על הלבנה והשחרה של קבצים, כאשר השחרה היא איתור המידע והלבנה היא הורדת הסכנה.

"במאבק להגנה על קבצים", אמר שני, "אנטי וירוס יכול לתת במקרה הטוב פתרון של 15% להתקפות ויתר אזורי המידע בארגון לא מטופלים. בדיקת דואר אלקטרוני היא שילוב של הלבנה והשחרה. זהו השלב הקריטי שבו פורץ יכול לחדור פנימה". המסקנה, לדבריו, היא: "תשכחו מהגנה על קבצים יחידים, כי יש בלי סוף, התפיסה צריכה להיות הגנה על פלטפורמה".

שי חן, סמנכ"ל טכנולוגיות בחברת הקטיקס מקבוצת ארנסט אנד יאנג, דיבר על שיטות לאיתור מתקפות שעברו מנגנוני הגנה בארגונים, במטרה להגדיל את היקף הגילויים של איומים שטרם הגיעו להבשלה. "אנחנו יודעים על מתקפות שבוצעו ונערכים להן, אבל אנחנו לא יודעים מספיק על איומים שלא הגיעו לכלל התקפה", אמר.

"הטלפון שלכם הוא כלי ריגול מושלם"

"בימים עברו, כשסוכן או סתם חוקר פרטי רצה לרגל אחרי מישהו בנעליים או בטלפון החוגה מכשירי ציטוט, או שהיה חמוש בעט מצלמה", אמר **ארז מטולה**,



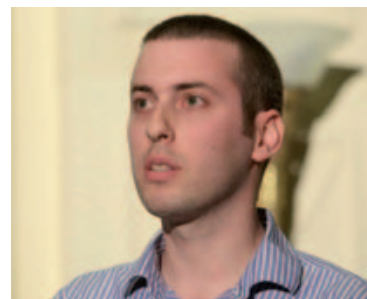
ארז מטולה

מייסד Appsec Labs. מטולה הוסיף: "הימים האלה נגמרו כי היום כל אחד הולך בכיס עם טלפון שיש לו את כל מה ששמי שרוצה לרגל אחרינו יכול לנצל - מיקרופון בו ניתן להקליט כל שיחה, מסך מגע לו ניתן לעשות קי-לוגינג כדי לדעת מה מוקלד, NFC באמצעותו ניתן לצוטט לטלפון אחר בסביבה או לייצטט תשלומים, וכמובן למצוא את

מיקום מחזיק המכשיר באמצעות המצלמה או ה-GPS".
 הוא הסביר על שיטות ישנות יותר שמתעדכנות: "בעולם הישן, אפליקציות ווב היו מוקד לבעיות של מניעת שירות, הזרקת SQL ועוד, דברים שנשארו גם היום, כי האפליקציות האלו משמשות תשתית לאפליקציות הסלולריות, אך כעת יש לנו וקטורי תקיפה חדשים - למשל איך המידע נשמר".

לדבריו, "בעולם המובייל יש גם מתקפות שרצות על המכשיר עצמו, למשל התקפות צד - אפליקציה תמימה ששולחת הודעות בתוך המכשיר וגורמת נזק. יש אפליקציות שמציבות 'סנייפר', רחרחן, שבודק אפליקציות אחרות על אותו מכשיר".

"כל אפליקציות הבנקאות הגדולות פגיעות"



יאיר עמית

יאיר עמית, שותף מייסד ו-CTO בחברת Skycure דיבר על הגנת מכשירי טלפון מבוססי מערכת ההפעלה iOS של אפל: "בעוד שבאנדרואיד יש אפליקציות עוינות רבות ובהן כאלה הפוגעות בפרטיות, ב-iOS הגן הסגור של אפל מגן על המשתמשים, לפחות על