



וירוסים בסלולרי הפרטי שלי?

כמה יקר לכם המידע הפרטי או הארגוני שבמכשיר הטלפון החכם שלכם אם יגיע לגורם זר? עצם היותו קטן ונייד אך חכם לפחות כמו מחשב אישי, יוצר עבור הטלפון החכם בעיות אבטחה שפותחות בפני ההאקרים עולם חדש של הזדמנויות לנצל פרצות בקלות בלתי נסבלת - שבעבר נחשבו למשימה בלתי אפשרית

וקשוחה כמו שנעשה באפל, וזו הסיבה שכמות היישומים בחנות של גוגל המכילים רוגלה גדלו ב-58% בשנה האחרונה (לפי סקר של חברת TrustGo).

דבר נוסף: שאלתם את עצמכם פעם למה הסוללה מתרוקנת כל כך מהר בטלפון? בסקר שנערך באוגוסט האחרון על ידי חברת טרנד-מיקרו עלה, כי ישראל מחזיקה בתואר המדינה השנייה בעולם בקצב הורדת יישומי אנדרואיד שמרוקנים את הסוללה. זה נתון מעניין, שכדאי לשים לב אליו, שכן נמצא שהגורם להתרוקנות הסוללה נגזר ברובו מפעילות הפרסומות הקופצות באפליקציות החינמיות.

אבל מספיק לדבר על האדם הפרטי הממוצע, הוא לא מספיק טכני ואי אפשר לצפות ממנו לנהל סיכונים תפעוליים, לזהות חולשות, להתערכך במתקפות וכיוצא בזה.

לעומת זאת, ארגונים אשר משקיעים בשיפור אבטחת המידע בתשתיות המיחשוב באופן שוטף צריכים לתת את הדעת לנושא הזה ולפעול מהר כדי להדביק את הפער שנוצר בין הצורך העסקי לניידות והסיכון של חשיפת מידע עסקי, או חמור מכך - שירותים פנים-ארגוניים. הקדמה הטכנולוגית דורשת מענה אבטחתי הולם, ובהעדר שכזה הארגון חשוף ועלול לשלם מחיר כבד. יצרניות אבטחת המידע הגדולות, כמו גם עשרות סטארט-אפים (חלק ניכר תוצרת כחול לבן) עובדות במרץ על מיזמים לתת מענה לנושא.

הפתרון בארגונים מגוון בהתאם לצורך העסקי סוג המידע ואופי הארגון, לכן האפשרויות למענה אבטחתי מגוונות וצרה הידיעה מלפרט על הנושא כאן.

בכל זאת, אז איך נותנים מענה מהיר לבעיה מהסוג הזה:

- ברמה האישית - אני ממליץ לכל אחד להפעיל במידת האפשר אנטי וירוס מסוג שהוא במכשיר. אפשר להתקין אנטי וירוס במכשיר האנדרואיד, בוודאי, אך סביר להניח כי הוא יאט במידת מה את תפקוד המכשיר שממילא חנוק בהקצאת משאבי מעבד וזיכרון למייל-פייסבוק-יוטיוב-וכדומה.

כאן יש בשורה משמחת לציבור הרחב של בעלי הסמארטפונים מכל סוג שהוא - הפתרון הקיים בעולם הארגוני לסריקת וירוסים הגיע לעולם הסלולרי! פלאפון, בשיתוף פעולה עם החברה הישראלית צ'קפוינט, פיתחו יכולת לטפל בחסימת נוזקות עוד לפני שנחתו במכשיר הקטן והיקר שלנו.

אגב - מומלץ גם לארגונים ליישם פתרון זה, שהינו קל להפעלה על צי מכשירים בהינף יד.

- אפל משקיעה רבות באבטחת מידע של מערכת ההפעלה ומשחררת תיקוני אבטחה מדי רבעון כמעט, ואני ממליץ להתקין אותם מיד. לצערי, בעולם האנדרואיד זה עדיין לא קורה.

- אל תתקינו מה שלא נמצא בשימוש קבוע במכשיר שלכם.
- לא מומלץ לפרוץ את המכשיר (Root/Jailbreak) ולהתקין יישומים מחנות שאינה Appstore/Play, אלא אם אתם ממש טכניים ברמה שתאפשר לכם לזהות פעילות עוינת שאינה חלק מהתפקוד התקין של המכשיר.

שתהיה גלישה בטוחה !

* הכותב הוא מנהל אבטחת המידע של פלאפון תקשורת

טלפונים חכמים הפכו מזמן לנחלת הכלל. החל מכלי לשיפור התפוקה בארגונים ועד למשחקים מקוונים מרובי משתתפים. הכלי הזה פשוט ממכר ושואב חלק לא מבוטל מזמננו בשל יכולותיו היומרותיות לנהל את סדר היום מכף היד. סתם כדוגמה פשוטה, שימו לב כשאתם נכנסים למעלית כמה מהנוכחים אוחזים במכשיר ומתקתקים במרץ? או קוראים בשקיקה פיסת מידע שהגיעה? אין ספק כי מדובר במגמה שהולכת ומתחזקת עם השיפור ביכולות הטכנולוגיות שמביאות לנו יצרניות מערכות ההפעלה הגדולות מבית אפל והאנדרואיד לסוגיו.

מדי פעם עולות לכותרות ידיעות על סיכון כזה או אחר במכשירים החכמים. הרבה באזז קיים בארגונים סביב הנושא עם מגמות BYOD ופתרונות MDM/SecureContainer. מה כבר יכול לפגוע במכשיר כזה קטן? אתם שואלים. אז זהו, שעצם היותו קטן ונייד, אך חכם לפחות כמו מחשב אישי, יוצר בעיות אבטחה שפותחות בפני גורמים בעלי אינטרס עולם חדש של הזדמנויות לנצל פרצות בקלות בלתי נסבלת - שבעבר נחשבו למשימה בלתי אפשרית.

השורה התחתונה היא - כמה יקר לכם המידע הפרטי/ארגוני שבמכשיר אם יגיע לגורם זר? תמונות, אנשי קשר, תכתובת דואר אישי/ארגוני, ססמאות של חשבון הבנק ואפילו מיקומכם הפיזי בזמן אמת. הנה כמה עובדות שכדאי להיות מודע אליהן:

- האבולוציה של פיתוח אמצעי אבטחת המידע בעולם המחשבים לא חוזרת על עצמה בעולם הסמארטפונים. לכמה מכם יש אנטי וירוס (הטכניים בינינו יוסיפו .FW..) במחשב האישי אבל לא על הסמארטפון? למה לא, הרי לשניהם יש מערכת הפעלה חכמה וגישה ישירה לאינטרנט? אמנם חברת אפל הצהירה במאי האחרון שאין צורך באנטי וירוס - אז איך זה שאפשר לפרוץ ולעדכן את מערכת ההפעלה של מכשיר iPhone רק באמצעות גלישה לאתר JailbreakMe, תוך ניצול חולשות אבטחה של מערכת ההפעלה iOS?

- מערכת ההפעלה אנדרואיד חדשה יחסית ודרוש שיפור למנגנוני האבטחה שלה. בעצם, איך היא תהיה בטוחה אם קוד המקור שלה פתוח (גם להאקרים)?

האפליקציות החינמיות ב-GooglePlay לא עוברות בדיקה קפדנית

