

אלו הן רק גרסאות החינם. אנחנו לא ניכנס כאן לויכוח העתיק האם גרסאות חינם של תוכנות אבטחה מספיקות למשתמשים או לא, אבל



בכל מקרה, כל החברות בתחום מציעות גם גרסאות תמורת שלום שאמורות להיות מקיפות, חזקות ויותר, שגם זוכות לעדכונים תכופים יותר.

נעילה מרחוק

ולסיום נתייחס אל עוד נקודה שהוצגה בחלק הראשון של המדריך. סיפרנו לכם על האפשרות שגוגל מספקת לאיתור, נעילה ומחיקת מכשיר האנדרואיד שלכם מרחוק. ובכן, לא רק גוגל מציעה את האפשרות הזו, אלא גם אפליקציה בשם Android Lost. בעקרון מדובר בתהליך דומה למה שמציעה גוגל לעשות במקרה של אובדן מכשיר, והאפליקציה הקטנה שמונתקת במכשיר מאפשרת גישה מהאתר של האפליקציה, אבל כמות הדברים שניתן לעשות באמצעות Android Lost עולה לאין שיעור על מה שגוגל מציעה בשירות הפשוט שלה. ניתן לשלוח הודעות, לגרום למצלמה הקדמית לצלם את המשתמש שמחזיק בטלפון, ולהציק למי שגנב או לבקש עזרה מ-'שומרני טוב' במגוון רחב אפשרויות, וזאת מעבר להפעלת אזעקה או נעילה/מחיקה מרחוק שמציעה גם גוגל. מומלץ בחום אם אתם רוצים להשתמש באפשרות הזו. בשורה התחתונה, חשוב עם זאת לזכור: בסופו של דבר רק אתם אחראים למה שקורה למכשיר שלכם, ורק אתם יכולים להחליט עד כמה חשובה לכם האבטחה שלו.

בהרשאות הגישה שיש לכל אפליקציה, רק שבמקרה דגן מקבלים את המידע באופן צבועוני ואפילו ברור, כולל הסברים מהי הפגיעה האפשרית בפרטיות. בסופו של דבר, הבחירה האם להשתמש באפליקציה זו או אחרת נותרת בידי בעל המכשיר, אבל בזכות Clueful אפשר לקבל החלטה מודעת יותר.

עוד דרך להבין שייתכן ויש בעיה עם אפליקציה אחת או יותר במכשיר שלכם היא להשתמש ב-Network Monitor. אפליקציה זו אולי אינה אפליקציית אבטחה לשמה, אבל היא מעניקה למשתמשים כלי מאוד חשוב: אפשרות לעקוב אחר שימושי הרשת של האפליקציות השונות והמגוונות שמותקנות במכשירם. למה זה חשוב? כי בדרך כלל אפליקציה מרושעת מתחילה להעביר כמעט מייד נתונים מהמכשיר אל איזשהו שרת במיקום מרוחק, ובנוסף, במקרה של שימוש בסוס טרויאני, תיתכן הזרמה של הנתונים לתוך המכשיר כדי לאפשר שימוש בו כזומבי לצורך תקיפות על מטרות אחרות. התנועה החוצה ופנימה באות לידי ביטוי בתצורה גרפית של כמות המידע הנכנס ויוצא של כל אפליקציה, וגם באופן כללי. אם זה מוצמד לאפליקציה שלא ממש אמורה לתקשר הרבה עם הרשת, זה אומר שכדאי להתחיל לחשוד.

הגנה כוללת יותר ולא נקודתית

כן, בדיוק כמו במחשב האישי, כדי להגן באופן רחב ככל האפשר על מכשיר האנדרואיד שלכם, התקינו בו אפליקציית אנטי וירוס. אל תאמרו לעצמכם לי זה לא יקרה, ותתעלמו מכל אלו שמספרים לכם שמכשיר אנדרואיד זה לא PC עם חלונות: כל חברות האבטחה הגדולות חוזרות שוב ושוב על כך שבגלל הגידול הענק במספר המכשירים הניידים שנמצאים כיום בשוק, ומכיוון שאנדרואיד שולטת בשוק הזה ביד רמה, זו הפכה מערכת ההפעלה המותקפת יותר מכולן. אנחנו באנשים ומחשבים כבר הצגנו בפניכם את CM Security. מדובר באפליקציה חנימית שהיא יותר מאנטי וירוס. כשהיא סורקת את המכשיר היא בודקת את כל האפליקציות המותקנות במכשיר אחת אחרי השנייה כדי לזהות אם מדובר באפליקציה תקינה או נוזקה מכלשהו. אבל לא רק: היא גם בודקת הגדרות חשובות במכשיר. כי אם תזכרו בכתבה הראשונה התייחסנו לנושא של אפשרות התקנות של אפליקציות מגורם אחר שאינו Google Play. אם CM Security מזהה שההגדרה הזו מאופשרת, היא מייד מוציאה הודעה מתאימה שממליצה לסגור את הפינה הזו. מעבר לכך סורקת האפליקציה את האפליקציות האחרות שמבקשים להתקין במכשיר בזמן שהן מורדות אליו, ולא רק אפליקציות חדשות, אלא גם עדכונים לכאלו שכבר מותקנות במכשיר האנדרואיד שלכם. היא יכולה גם, אם תרצו, לסרוק את כרטיס הזיכרון שלכם, וזה חשוב מאוד אם אתם כאלו שמחליפים אותו מדי, או מוציאים אותו מדי פעם כדי לשלבו במכשיר אחר או במשחב האישי בבית.

הגלישה באינטרנט

נושא אחר אליו היא מתייחסת היא הגלישה באינטרנט. אם תאפשרו לה היא תבדוק את האתרים אליהם אתם גולשים כדי לוודא שלא מדובר באתרים בעייתיים בעיקר בכל מה שקשור לאתרי Phishing שהם אתרים שמתחזים לאתרים 'חוקיים' כדי לשאוב מאלו שמגיעים אליהם מידע חשוב, החל מפרטים אישיים ועד פרטי כרטיסי אשראי. כפי שאתם מבינים, CM Security היא יותר מרק אנטי וירוס. למעשה מדובר באפליקציית אבטחה למכשיר אנדרואיד, ומכיוון שמדובר בנושא חשוב לנו, גם נציין שהיא כמוזן לא היחידה בשוק הזה. בחנות של גוגל אפשר למצוא את כל השמות הגדולים שבתחום, ורוב החברות מציעות מספר כלי אבטחה. כך למשל תוכלו למצוא לא מעט יישומים של סימנטק תחת המותג NortonMobile; אנטי וירוס מקיף של ביטדיפנדר; את הגרסה של AVG שמוכרת היטב למשתמשי ה-PC כמו גם זו של אווירה; ואפילו גרסה חנימית של קספרסקי ועוד.