התקנים ניידים – סיוט לפרטיות ולאבטחה

המציאות

מכשירי הסמארטפון שברשותנו הנם התקנים מאוד אישיים ומרגשים שמספקים לנו נגישות בלתי פוסקת לאינסוף מידע, מקום לאחסון מידע אישי שלנו, אמצעי תקשורת מגוון ועוד הרבה מעבר.

חלק נכבד מחיינו הפרטיים והאישיים מאוחסן בהתקנים אלה ואצל רובנו גם לא מעט מידע ממקום העבודה נמצא במכשיר וזאת בנוסף לחיבור למערכת הדואר הארגונית ובארגונים רבים חיבורים למערכות ארגוניות נוספות.

אחת החוויות בשימוש במכשירים אלה היא היכולת שלנו להתאים אותם לעצמנו, לשנות רכיבי תוכנה, לשדרג, להוסיף ולהרחיב את חוויית השימוש, וכולנו מאושרים כשאנחנו מוצאים גאדג'ט אפליקטיבי חדש למכשיר שלנו, משהו שיספק לנו חווית שימוש נוספת, חדשה ומעצימה, בדרך כלל גם נרוץ מהר להתגאות מול החברים ולהראות את המציאה החדשה שלנו.

החדשות הרעות

יש חברה רעים שם בחוץ, הם יודעים בדיוק מה אנחנו מחפשים והם ינצלו זאת היטב.

איך?

כל המקרים הבאים אינם מבוססים על מחקרי שוק או על דוחות כלליים כאלה או אחרים, כולם מבוססים על מקרים אמתיים שאורבים לכולנו בפינה.

<u>אפליקציות מקלדת</u>

לא כולם מרגישים בנוח עם אפליקציית המקלדת שמגיעה עם המכשיר, לפעמים המקשים אינם בגודל הרצוי, התגובה שלהם לא נוחה, הצבע לא בדיוק..., להחליף שפה לא נוח, לא כל המקשים שאני רוצה נמצאים בדף הראשי וכד'.

מה עושים? מחפשים בחנות האפליקציות חלופה.

ומה אם אפליקציית המקלדת שהורדתי מרצוני, התקנתי בעצמי ונתתי לה במודע את ההרשאות הנדרשות גם מקליטה ושומרת בקובץ לוג כל הקשת מקלדת שלי? כולל שמות משמש וסיסמאות? אז בפועל, כן, הן עושות את זה...

ואנחנו גם נתנו להן במפורש את ההרשאה לשלוח את כל המידע בחזרה לשרתי הניהול שלהן כדי לעזור למפתחים לבאורה לשפר את השירות שלהם.

חושבים שזה לא קורה במציאות? חשבתם פעם כיצד שוב ושוב אלמונים משתלטים על חשבונות אינסטגרם של כל מני ידוענים ובכלל של ילדי דור המילניום? אין כאן שום מהלך האקינג מתוחכם, פשוט מאוד החברה האלה התקינו אפליקציות מקלדת מרגשות שבסופו של דבר שלחו ברקע לאותם אלמונים את פרטי ההתחברות שלהם ועוד הרבה מידע נוסף.

זה ממש לא נגמר בשם משתמש וסיסמה לאינסטגרם, כל הקלדה לאפליקציית חשבון הבנק, התחברות לדואר אלקטרוני, למערכות ארגוניות, כל כתובת URL, כל אתר שגלשתם אליו וכל פיסת מידע אחרת עברה מהמקלדת המותאמת ישירות לשרתי הניהול ומשם זה כבר לא בידיכם.

הישארו עם המקלדת שמגיעה עם המכשיר ותתרגלו אליה.

<u>אפליקציות מצלמה</u>

ומה אם אפליקציית המצלמה שהורדנו והתקנו כדי לצלם את עצמנו עושים פרצופים חמודים ומטופשים גם משדרות את כל התמונות "לספינת האם" (שרתי הניהול)?

המשתמשים בוחרים את התמונות הטובות ביותר, מוסיפים להן עיניים של גור חמוד, אף חמוד ואזני ארנב אבל אפליקציית המצלמה מגבה את כל הצילומים ברקע לשרתים, צילומים שחלקם מדויקים מאוד ובהחלט יכולים לשמש לפתיחת מערכות המתבססות על זיהוי פנים ואין להן חיישני עומק מבוססי אינפרא אדום? כבר ראינו מספר הדגמות כיצד מכשירי אנדרואיד הוטעו על ידי צילום פנים.

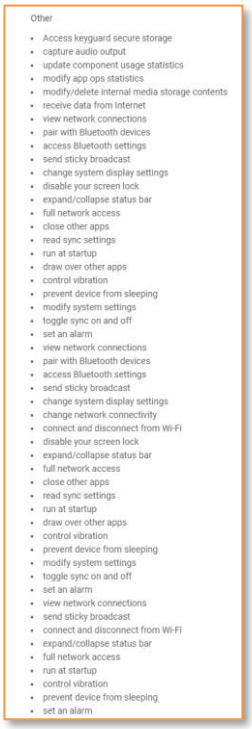
ובנוסף, האם נרצה שכל התמונות שלנו, פרטיות ואישיות ככל שיהיו ישכנו להן בשרתים כלשהם בעולם ביחד עם מידע נוסף עלינו? ממש תיק אישי ציבורי.

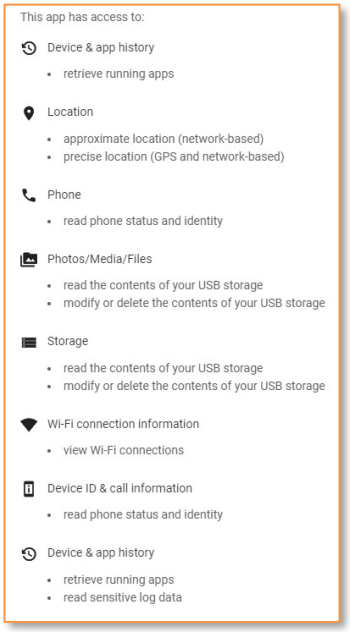
הישארו עם המצלמה שמגיעה עם המכשיר ותתרגלו אליה.

אפליקציות פנס

רציתם אפליקציית פנס מתוחכמת יותר מזו שמגיעה עם המכשיר, ומה אם היא רצה כל הזמן ברקע ועושה המון דברים שלא רציתם בכלל, אבל אישרתם לה לעשות הכול בהתקנה?

אפליקציות פנס ידועות כמקור לצרות וזה מתחיל כבר בשלב ההתקנה כשאנחנו מתבקשים לתת להן הרשאה לכל אלמנט אפשרי:





אפליקציות פנס כבר נתגלו כשהן מקפיצות פרסומות, פותחות דפי אינטרנט ברקע, מקלידות על אלמנטים שונים, מנסות להירשם לשירותים שונים, משדרות מידע אישי מהמכשיר שלכם לשרתי ניהול ואף מנסות לבצע רכישות בשם המשתמש.

הישארו עם הפנס שמגיע עם המכשיר ותתרגלו אליו.

משחקים

חשבתם שאולי המשחקים שהילדים שלכם מתקינים משתמשים בהקלקות החוזרות ונשנות במשחק כדי להקליק ברקע על פרסומות?

ומה אם המשחקים האלה מלקטים מידע נוסף כגון מהירות תגובה, נתוני מיקום, ג'יירוסקופ, ותאוצה כדי לחקות מדדי התנהגות וכך לרמות מערכות נגד הונאה שמנסות להפריד ולזהות בין פעולות ידי אדם לפעולות מכונה?

גם רכישות קטנות בתוך המשחק יכולות לספק מספיק מידע שבעזרתו ניתן בקלות לבצע על חשבונכם רכישות באתרי פורנו וכד'?

כמובן שגם משחקים שמכילים קוד זדוני יכולים לשלוף מידע פרטי או ארגוני ולשדר אותו לשרתי ניהול.

יש לבדוק היטב כל משחק לפני הורדה, לקרוא חוות דעות של משתמשים אחרים, לבדוק איזה הרשאות נדרשות ואם יש הרשאות חשודות, מי מפתח המשחק ובמקרה של כל דבר חשוד, פשוט לא להתקין.

אפליקציות מסרים

ומה אם אפליקציית המסרים שהורדתם מאזינה להודעות פאקטור ההזדהות הנוסף (הודעת SMS המכילה מספר חד פעמי שאותה אתם מקבלים כדי להזדהות מול הבנק שלכם או מול שירות רגיש אחר) ובעת האפליקציה יכולה להתחבר אל המערכת הבנקאית שלכם או כל מערכת רגישה אחרת? בסופו של דבר שעת שהתקנתם את אפליקציית המסרים אפשרתם לה הרשאת גישה לקריאה, מחיקה ומשלוח של הודעות SMS.

הרי בשום מקום לא נאמר שאתם תדעו בדיוק מתי האפליקציה ניגשת למידע הזה.

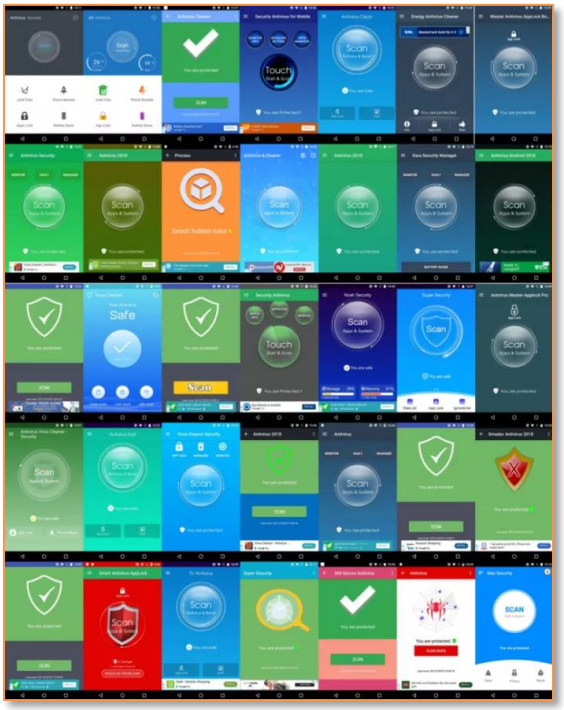
לאפליקציות אלה יש גם גישה למיקרופון של המכשיר, דבר שמאפשר להן להפעילו בכל רגע ולבצע הקלטות שלא בידיעתכם ויש להן גם גישה דומה למצלמה של המכשיר והן בעת יכולות להקליט כל דבר ולשלוח ביחד עם צילומים לשרתי הניהול.

רק נזכיר את היכולת הקימות של אפליקציות לחקות באופן מושלם את הקול של כל אחד מאתנו, כך שגם מערכות לזיהוי קולי אינן חסינות לאחר שהוקלטתם.

השתמשו בכל שניתן באפליקציות המובנות במכשיר.

אפליקציות "אנטי וירוס" ואפליקציות "לניקוי המכשיר"

ומה עם האפליקציות האלה שמקבלות הרשאת Admin של המכשיר שלכם ויכולות לעשות הכול הן בעצמן אפליקציות זדוניות? נשמע בדיוני? אז זהו, ממש לא, רק לאחרונה נתגלו 35 אפליקציות "אנטי וירוס" מזויפות לאנדרואיד שהן בעצמן תוכנות זדוניות והותקנו על ידי יותר מ 6 מיליון משתמשים בעולם:



לאפליקציות אלה הרשאת מנהל מערכת והן יכולות לעשות הכול, להיכנס למידע של אפליקציות אחרות, לשנות הגדרות, להוריד אפליקציות נוספות ואף להריץ אפליקציות נסתרות ברקע.

הטלפון שלכם מתחמם? הסוללה נגמרת מהר? חבילת הדאטה שלכם נגמרת כבר בתחילת החודש? כן, רוב הסיכויים שיש אפליקציה זדונית שפועלת ברקע, מנטרת את כל הפעילות והמידע במכשיר שלכם ומשדרת אותו לשרתי ניהול, גונבת לכם חשבונות משתמש, מבצעת בשמכם ובכספכם רכישות, מקפיצה פרסומות ועוד.

סיכום

אם התסריטים המתוארים כאן לא נשמעים לכם מציאותיים ואולי קצת דמיוניים נזכיר רק ש:

- שמעתם על הטלויזיות החכמות של סמסונג וויזיו שהאזינו לכל השיחות בחדר ושידרו לשרתי החברות?
- שמעתם על מחשבים ניידים של לנובו שהכילו רוגלה בלתי ניתנת להסרה?
- שמעתם על המחשבים הניידים של HP שהכילו Key Logger (מקליט הקשות מקלדת)?
- שמעתם על הטלפונים של בלו ו TLC ששידרו נתוני טלמטריה לשרתי החברות?
- עוד דוגמאות מסוג זה? קראו כאן:
  https://www.peerlyst.com/posts/kinda-obvious-but-know-who-is-spying-on-you-at-all-times-dr-augustine-fou-cybersecurity-ad-fraud-researcher

מה אפשר לעשות?

אנשים עם מכשירים פרטיים שאינם מוגנים במסגרת ארגונית כלשהי, צריכים קודם כל מודעות.
עצם ההכרה שהסיכון כאן, קיים, אמתי ומתרחש כל יום מחייב אתכם לנהוג במשנה זהירות.
לא לרוץ ולהתקין כל דבר מהר, לקרוא, לבדוק לפני ולהתייעץ.
לא למהר להקליק ולאשר שום דבר, כל קליק יכול לחכות עוד קצת.
לבדוק, האם הגיוני שאפליקציית פנס למשל צריכה הרשאה לכל אלמנט אפשרי במכשיר הטלפון?
גם אם לא רואים את זה, העולם הדיגיטלי מלא באיומים ועלינו לנהוג בהתאם, זהירות, חשדנות ובדיקה יסודית של כל דבר.

לעומת זאת בארגונים, מנהלי הארגון, מנהלי אבטחת המידע ואנשי מערכות המידע צריכים להבין את גודל הסיכון למידע הארגוני.
אותו מידע שהארגון עמל קשות להגן עליו והקיף את עצמו בחומות של פתרונות הגנה דיגיטליים מתקדמים ביותר, אותו מידע בדיוק נמצא בסיכון וחשיפה גבוהים מאוד בזכות מכשירי הטלפון החכמים שמחוברים למערכות הארגון וכדי להגן עליו יש ליישם את הפתרונות הנכונים באמצעות גוף מנוסה בתחום ייחודי זה.

מוביסק טכנולוגיות

מוביסק טכנולוגיות פועלת בישראל משנת 2011 ועוסקת בתכנון, יישום ותחזוקת פתרונות לניהול והגנה על התקנה קצה.
החברה אחראית למרבית היישומים בארגונים המובילים בישראל בתחומי הניהול וההגנה על התקנים ניידים.
מומחי החברה הנם בעלי ניסיון רב שנים והסמכות רבות לתכנון, יישום ותחזוקת המוצרים המובילים בתחומים אלה.
לפרטים נוספים: info@mobisec.co.il