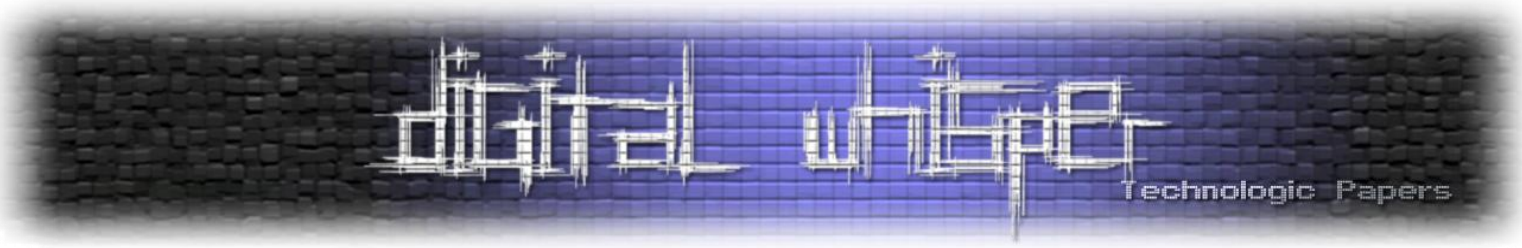


Google's GeoLocation API - איפה נמצאות כל המכונות המקוונות בעולם?

מאת: דור זוסמן

הקדמה

פייסבוק שואל "על מה אתה חושב עכשיו?", טוויטר מתעניין "מה קורה עכשיו?", אך אלו כבר חדשות ישנות. היום כולם רוצים לדעת "איפה אתה עכשיו?" פייסבוק הרימו את Places, טוויטר חברו אל Where.com, ורשתות כמו Foursquare, Gowalla , Brightkite ואחרות ממשיכות להופיע...

"איפה אתה?", זאת שאלה שקשה למחשב לענות עליה - אי אפשר לסמוך על המשתמש שיענה עליה, ולא לכל מחשב יש את הציוד המתאים בשביל לענות עליה. למי יש את הציוד המתאים? לסמארטפונים, כל אחד ואחד מהם, מכיל בתוכו רכיב קטן שמסוגל להגיד בדיוק של כמה עשרות מטרים איפה אתה בעולם בכל רגע נתון.

זו הדלת לתוך העולם הזה, אבל כמובן שלא נשאיר את המחשבים מאחור, ולכן קם אדם בשם Stan Wiechers והחליט למצוא לבעיה זו פתרון. בשיתוף עם גוגל, (שבמקרה החזיקה בבעלותה מאגר די נרחב של כתובות MAC של ראוטרים ונ.צ. שלהם...), החליט לכתוב API ב-Javascript, שיותר מאוחר יתחבר ל-HTML5 ויאפשר לכל מתכנת, למצוא את הנ.צ. של גולש, ב-3 שורות קוד פשוטות, נשמע מפחיד? גם לנו.

איך זה עובד ומה נעשה עם המידע?

במחשב האישי:

על מנת למצוא את הנ.צ. של הלקוח, GeoLocation מבקש מהדפדפן כמה דברים:

- כתובת ה-MAC, עוצמת הקליטה וה-SSID של ה-AP .
- כתובת ה-MAC, של המתאם האלחוטי (אם יש).
- הרשתות האלחוטיות שנמצאות בטווח קליטה, הכתובות הפיזיות שלהם, SSID ועוצמת הקליטה של כל אחת מהם.

כל המידע נאסף ע"י הדפדפן ונשלח לכתובת www.google.com/loc/json בצורה הבאה:

```
{
   "version":"2.0.0",
   "request_address":true,
   "access_token":"2:TOKEN",
   "wifi_towers":
   [
      {"MAC_address":"r4-72-20-11-gf-
34","ssid":"MyOwnWifi","signal_strength":-20},
      {"MAC_address":"00-33-64-d1-34-
0d","ssid":"OtherWiFi","signal_strength":-64},
      {"MAC_address":"00-13-62-e1-36-
cd","ssid":"OtherWiFi2","signal_strength":-84}
   ]
}
```

המידע שחוזר מכיל את הנ.צ. המשוער של הלקוח, חשוב להגדיש שהשרתים של גוגל משתמשים גם בכתובת ה-IP של הלקוח ובכך משפרים את דיוק התוצאה, וכן המסד מבצע התאמות וכיול מחדש של המידע שכבר מאוכסן, ביחס למידע החדש ובכך משפר את דיוקו מפעם לפעם.

בסמארטפון:

אותם הפרטים יאספו כמו במחשב במידה ואין חומרת GPS במכשיר, במידה וקיימת חומרה כזו, מכשיר ה-GPS יאסוף את הנ.צ. מהלווייינים.

נבצר ממני להראות לכם פאקט של סמארטפון ואיני יודע אם המידע מועבר ישירות לאתר או עובר דרך גוגל. אני מניח שהמידע נשמר ע"י גוגל (במיוחד אחרי שקראתי את המחקר של סאמי בנושא סמארטפונים וGPS), ואני בטוח שהמידע הזה גם משמש לייעול ושיפור המאגר.

הסכנות הפוטנציאליות שדבר

כל חוקר אבטחה שקרא עד פה מדמיין כבר את ניצולים לרעה אפשריים. כמה שאני חושב עליהם:

1. הונאות פישינג העושות שימוש במידע זה על מנת לקנות את אמונו של הקורבן.
2. Malware המנצל לרעה מנגנון זה ומוסיף אתר זדוני ל-White-List של הדפדפן, או שולח בעצמו את חבילת המידע ומשתמש במידע לצורך פרסום או חשיפת זהותו האמתית של הקורבן.
3. אתר המשלב מסד של מרשם אוכלוסין (אגרון לדוגמא...), מסד של רחובות והנ.צ. שלהם ומסוגל להעריך את זהותו של הגולש בעזרת נתוני המיקום.
4. Adware מותאם לקורבן מבחינת מיקום ושפה.
5. וכמו כמעט בכל נושא- הדמיון הוא הגבול. כל מה שצריך זה להיות יצירתיים.

תומך בכל פלטפורמה, וזמין לכל מתכנת - איך GeoLocation עובד בפועל?

כמו שניתן לראות בתמונה למטה, טכנולוגית ה-GeoLocation נתמכת בכל גירסה חדשנית של דפדפן גדול ובכל גירסה יחסית חדשה של מערכת הפעלה לסמארטפונים, וברוב אילו שאינו תומך, ניתן להתקין פאטצ'ים פשוטים.

GEOLOCATION API SUPPORT						
IE	FIREFOX	SAFARI	CHROME	OPERA	IPHONE	ANDROID
9.0+	3.5+	5.0+	5.0+	10.6+	3.0+	2.0+

הפשטות שבה אפשר לעשות בטכנולוגיה הזאת שימוש מפחידה. בעזרת 3 שורות קוד בלבד, ניתן לזמן בקשה זו ולעשות כאוות נפשנו במידע:

```
function get_location() {
  navigator.geolocation.getCurrentPosition(show_map);
}
```

כעת יש לנו ביד שני קבועים (const):

- position.coords.latitude - קו הרוחב המשוער
- ו-position.coords.longitude - קו האורך המשוער

כאשר מניחים את שניהם על מפת עולם בגודל סטנדרטי, הנקודה בה הם חוצים זה את זה היא הנקודה שבה הלקוח ממוקם פיזית כביכול.

Google maps יודע לעשות זאת לבד, רק נכניס את הקורדינטות לחיפוש עם פסיק המפריד ביניהם ונראה שתופיע לנו נקודה על המסך, שם הלקוח שלנו נמצא.

ישם עוד מספר משתנים שנוכל לקבל בתוך position שיכולים לעזור לנו, כגון coords.accuracy, שמסמל את רדיוס מרווח הטעות שלנו במטרים, timestamp - שמסמל מתי נדגם מיקומינו וכו'.

כל זה נמצא בתוך מחלקה בשם gears_init.js. מחלקה זו היא המחלקה שמזמנת את Google Gears במידה והוא מותקן (מובנה בתוך כרום) ואם לא, מזמנת את המחלקה geo.js שהיא מחלקת ה-GeoLocation העומדת בפני עצמה.

אם נעיין בקוד נוכל למצוא דברים מעניינים, כמו הקריאה למחלקה בתוך Google Gears במידה והוא מותקן:

```
provider=google.gears.factory.create('beta.geolocation');
```

או הקריאה לרכיב ה GPS במכשירי Palm:

```
r=new Mojo.Service.Request('palm://com.palm.location', {
      method:"getCurrentPosition",
      parameters:parameters,
      onSuccess: function(p){success({timestamp:p.timestamp, coords:
{latitude:p.latitude,
```

ועוד מספר רב של דברים מעניינים, אני ממליץ לעבוד ברפרוף על geo.js על מנת להבין את התפקוד של GeoLocation בצורה טובה יותר.

אחרי שהצגנו את הטכנולוגיה, נעבור לחלק המעניין של מאמר זה ☺

חבילת המידע המכילה את כתובות ה-MAC, SSID של הרשתות וכתובת המתאם שלנו נשלח על ידי הדפדפן, בלי מעורבות של האתר שביקש את המידע. **הפרדת הגורמים הזו חשובה בכדי למנוע מגורמים לא רצויים לגשת למידע רגיש זה**. הנקודה המעניינת היא שמכיוון שהדפדפן בשליטתנו, אנו נוכל לשלוט במה שישלח מהדפדפן וכמובן- במה שיתקבל.

נוכל לעמוד בין הדפדפן לגוגל, להחליף את המידע על הרשתות הסובבות אותנו במידע שאנו נבחר, ובכך נוכל לאתר כתובת MAC של **מכשיר שלא בבעלותינו!**

נערוך את הבקשה שנשלחת לגוגל, בצורה הבאה:

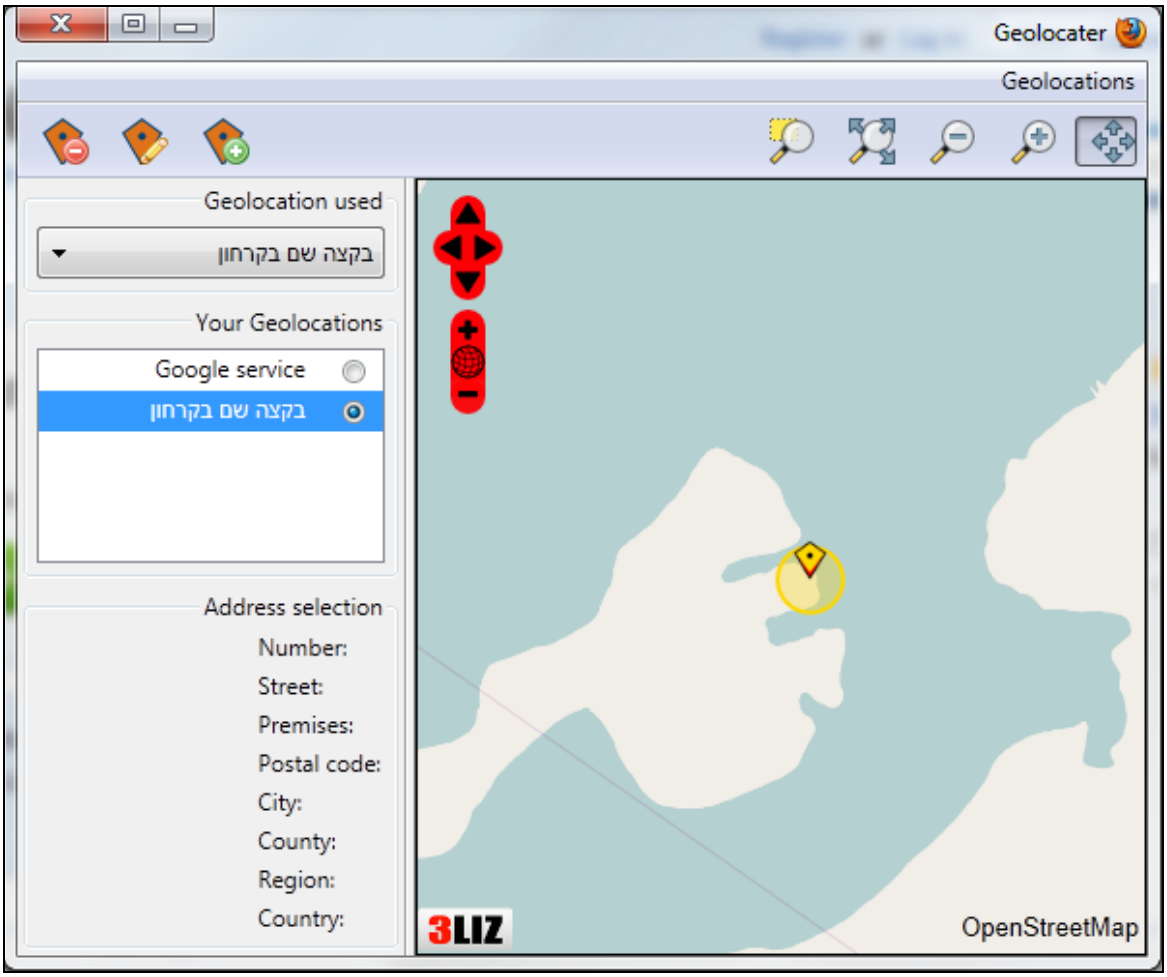
```
{
   "version":"2.0.0",
   "request_address":true,
   "access_token":"2:TOKEN",
   "wifi_towers":
   [
      {"MAC_address":"(MAC address of device)"}
  ]
}
```

וזהו זה...

חוקר האבטחה Sami Kamkar, החליט לעשות את זה עוד יותר פשוט: הוא בנה אתר נוח עם ממשק Ajax, השולח שולח את הבקשה בשמנו, ומדפיס את התוצאה בתוך מפה של Google maps. כל מה שנותר הוא להדביק את כתובת ה-MAC וללחוץ על הכפתור...

זה רק כיוון אחד של ניצול, מה עם הכיוון השני? הרי אם אנחנו שולטים במה ישלח לגוגל, אנו יכולים גם לשלוט במה גוגל יחזיר לנו לא? כמובן שאפשר לעשות זאת עם כל sniffer בעזרת עריכת חבילת המידע הספציפית ואין טעם להסביר איך עושים זאת, אבל נסביר כיצד ניתן לעשות זאת עם שימוש ב-Addon לפיירפוקס בשם GeoLocater ו"לעבוד" על פייסבוק Places.

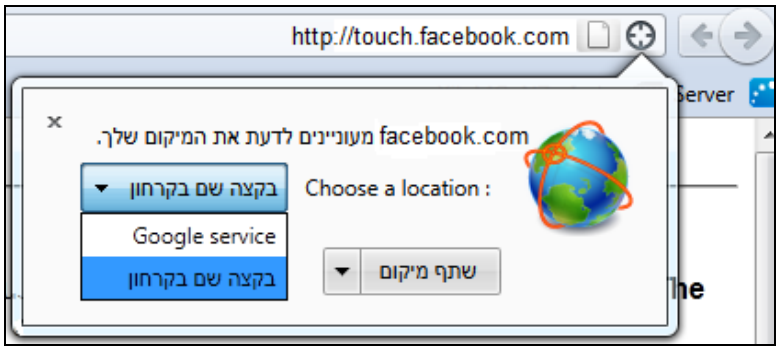
את GeoLocater ניתן להוריד באתר התוספות הרשמי של מוזילה, והקונפיגירציה שלו די ברורה. נוסיף נקודת ציון מזוייפת וניתן לה שם:



כעת, נשתמש בתוספת נוספת בשם User Agent Switcher שיעזור לנו להכנס לגירסה לניידים של פייסבוק (זאת מכיוון שאין גישה ל-Places דרך הממשק הרגיל של הדפדפן).

נפעיל מחדש את הדפדפן ונשתמש ב-UA של Chrome. נגלוש ל-facebook.com ונראה שהועברנו ל-m.facebook.com, אבל זה כמובן לא מספיק לנו, אנו צריכים גירסה יותר חדישה של הממשק, נגלוש ל-touch.facebook.com. נבחר ב-More ושם ננווט ל-Places כאשר נתבקש לבחור בספק שירות שיתן לנו את הקורדינטות, נבחר בשם נקודת הציון שהוספנו ונלחץ "שתף מיקום".

והתוצאה לפניכם:



אם נמשיך כרגיל, נראה שבסוף התהליך נוצר לנו מקום חדש, שטוען שאנחנו באנטרקטיקה, מה שנשאר לעשות זה רק להעלות תמונות שלנו עם פינגווינים ודובי קוטב, ולפרסם בפייסבוק ☺

זוהי רק דוגמא בסיסית לשימוש בטכנולוגיה הזו לרעה. ובמקרה הנ"ל מדובר במקרה לא מזיק. אך ניתן לחשוב על סיטואציות שבהם התבססות על טכנולוגיה זאת לאיכון המשתמש יכולים להיות פחות תמימים, כגון מנגנוני הגנה המאפשרים גישה רק ממקומות מסוימים בעולם.

סיכום

מי יודע באילו רוגלות ורשעות יש ניצול של מאגר זה. לטעמי אסור לאף חברה להחזיק כזה מאגר, ובטח שלא בצורה כל כך לא מאובטחת, הרי גוגל כבר הוכיחו שדאגתם האחרונה היא מי ניגש אל המאגר...

אני מניח שהשאלה שלי היא בעצם - מי הסמיך את גוגל להיות אוצרת המיקומים של כל רכיב אלקטרוני הניגש לאינטרנט בעולם, ולמה לאף אחד לא אכפת מזה?

על המחבר

אני דור, חוקר אבטחה די צעיר מהמרכז, עוד לא בגיל צבא אפילו, לאחרונה החלטתי לעשות משהו מועיל ולהציע עזרה ל-DigitalWishper, מתוך רצון לשפר את הקהילה הישראלית וכמובן לתמוך במגזין הנהדר הזה, אחרי כמה מיילים עם cp77fk4r מצאנו נושא והתחלתי את המחקר, זה המאמר הראשון שאני כותב בצורה מקצועית אי פעם ומפרסם אותו, ולכן אשמח למשוב מכל סוג שהוא, אם למישהו יש הערות / הארות ניתן תמיד לפנות אלי הדוא"ל: risomrisom@gmail.com ואחזור אליכם בהקדם האפשרי.