איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

23/01/2022
כ״א שבט תשפ״ב

חומרי רקע מטעם איגוד האינטרנט הישראלי לדיון המיוחד בנושא "טענות אודות שימוש משטרת ישראל בתוכנת פגסוס"

איגוד האינטרנט הישראלי (ע״ר) [1], מתכבד להעביר לוועדת בטחון הפנים חומרי רקע תמציתיים לקראת הדיון המיוחד שיתקיים ביום 24.1.2022 בנושא ״טענות אודות שימוש משטרת ישראל בתוכנת פגסוס״. מסמך זה אינו מבקש לכסות את כלל הרבדים של הדיון אודות הפעלת טכנולוגיות מעקב מתקדמות על ידי רשויות החקירה בישראל, אלא להניח תשתית ראשונית לדיון הציבורי אשר ראוי לקיים בהקדם.

א. <u>מבוא</u>

בשנים האחרונות, משטרת ישראל מפעילה כלים פורנזיים מתקדמים לאיסוף ועיבוד של מידע דיגיטלי מאמצעי מחשוב בכלל ומטלפונים ניידים בפרט. למרות השימוש ההולך וגובר של רשויות החקירה בישראל בטכנולוגיות רבות-עוצמה לפריצה וחיפוש בטלפונים ניידים, אין כמעט שקיפות ציבורית בנוגע לתדירות, לאופי המקרים ולטכנולוגיות השונות שבהן רשויות אכיפת החוק משתמשות. אימוץ טכנולוגיות אלו באופן חד צדדי וללא דיון ציבורי בנוגע לסיכונים הכרוכים בהפעלתן והבנת עוצמת הפגיעה שלהן בזכויות הפרט של אזרחי ישראל – הוא מדאיג ביותר.

בהקשר זה, נהוג להבחין בין כלים פורנזיים המחייבים תפיסה פיזית של המכשיר הנחקר (למשל, כלי Cellbrite בהם משטרת ישראל וגופי אכיפה נוספים משתמשים מזה שנים) לכלים פורנזיים המאפשרים גישה לנתוני המכשיר מרחוק (למשל, כלי פגסוס מתוצרת NSO). עם זאת, כלים אלו חולקים מאפיינים ויכולות חסרות תקדים: (א) פריצה או עקיפה של מרבית תכונות האבטחה המובנות בטלפון ויכולת להעתיק את עושר הנתונים השמורים בו, כמו גם נתונים מחשבונות ענן אליהם מקושר המכשיר ו-(ב) יכולות ארגון וניתוח מידע מתקדמות המאפשר לרשויות אכיפת החוק לבחון ולנתח שפע המידע מהטלפון החכם בקלות וביעילות.

הכלים הפורנזיים שמפעילה כיום משטרת ישראל לפריצה וחיפוש בטלפונים ניידים מספקים גישה למאות ג׳יגהבייט של נתונים בכל טלפון, העשויים להיות חושפניים באופן בלתי צפוי – ביחס למושא החקירה אך גם ביחס לצדדים שלישיים רבים. כלים אלו יכולים לאסוף יומני שיחות, רשימות אנשי קשר, מסרונים ותמונות, אך גם הרבה יותר מידע ממה שנכלל תחת הקטגוריות האלה: נתונים מחשבונות מקוונים, אפליקציות של צד שלישי, נתונים ״שנמחקו״ ועוד.

על רקע זה, סקירה ראשונית זו מטעם איגוד האינטרנט הישראלי (ע״ר) מבקשת להפנות זרקור על האופנים בהן טכנולוגיות מידע חדשות – בתחום מחשוב הענן ובתחום טכנולוגיות פורנזיות – מחייבת לעדכן את האסדרה המשפטית של חיפושים בחומר מחשב ככלל, ופריצה וחיפוש בטלפונים חכמים ושירותי ענן בפרט.

[1] איגוד האינטרנט הישראלי הוא עמותה בלתי תלויה וללא כוונת רווח, המנהלת שתי תשתיות אינטרנט חיוניות בישראל - מרשם שמות המתחם המדינתי (.il) והפצת המידע על אודותיו ל-DNS, ומחלף האינטרנט הפנים-מדינתי (IIX). האיגוד הוכרז בשנת 2018 כמפעיל ״מערכת ממוחשבת חיונית״ על פי חוק הסדרת הבטחון בגופים ציבוריים, התשנ״ח-1998. במקביל לפעולתו התשתיתית, פועל האיגוד לקידום ושמירה על עקרונות דמוקרטיים בפעולתו של האינטרנט בישראל. בכלל זה, מפרסם איגוד האינטרנט מחקרי מדיניות המיועדים ליידע ולטייב את זירת האינטרנט הישראלית והגלובלית, על בסיס עבודת מחקר מקיפה ומומחיותיו בצמתים מגוונות של משפט וטכנולוגיה. מחקרי מדיניות אלו כוללים ידע מקצועי והמלצות מעשיות עבור גורמי ממשל והקהל הרחב. למידע נוסף, ראו https://www.isoc.org.il.

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

ב. יכולותיהן הטכנולוגיות של כלים פורנזיים לחיקור טלפונים ניידים

כלים פורנזיים לפריצה או גישה מרחוק לטלפונים חכמים נועדו להעתיק את כלל הנתונים שניתן למצוא בדרך כלל בטלפון סלולרי ולחלץ ממנו מידע רב ככל האפשר. הנתונים כוללים מידע כמו אנשי קשר, תמונות, סרטונים, סיסמאות שמורות, תיעוד GPS, רשומות שימוש בטלפון ואפילו נתונים "שנמחקו" – לרוב תוך עקיפת תכונות האבטחה המובנות בטלפון או ניצול חולשות בתכנון החומרה או התוכנה שלו.

טכנולוגיות פורנזיות אלו מאפשרות לרשויות אכיפת החוק לסרוק ולנתח בקלות את הנתונים שהועתקו, ומספקים אמצעים לעיבוד מהיר של גיגהבייטים של נתונים – משימה שבנסיבות אחרות תדרוש עבודה רבה. יכולות אלה מאפשרות למפות מיקום של אדם על סמך נתוני GPS, לחפש מילות מפתח מסוימות ולמיין צילומים באמצעות כלי קיטלוג תמונות.

אמצעי אבטחה להצפנת המידע המאוחסן בטלפון אמנם זוכים לתשומת לב ציבורית רבה, אולם כלי הזיהוי הפלילי לטלפונים מסוגלים לעקוף את רובם ולהעתיק את הנתונים. העובדה שטלפונים רבים פגיעים - בין אם מדובר בפרצות אבטחה ובין אם האשם בליקוי מובנה - פירושה שהכלים הזמינים לרשויות מתמודדים בהצלחה עם אתגרי גישה למידע. כלים אלה יכולים בדרך כלל להתגבר גם על מנגנוני אבטחה סלולריים מתקדמים ולחלץ נתונים משמעותיים מהטלפונים.

כלים פורנזיים לפריצה וחיקור של טלפונים ומכשירים חכמים אחרים מספקים גישה להיקף עצום של מידע אישי ורגיש. השימוש העיקרי של הכלים הוא איסוף יומני שיחות, רשימות אנשי קשר, מסרונים ותמונות. אבל בטלפונים מאוחסן הרבה יותר מידע ממה שנכלל תחת הקטגוריות האלה. למשל:

- נתונים מאפליקציות: כל אפליקציה סלולרית שומרת נתוני משתמשים, החל מהיסטוריית הגלישה וכלה בנתונים רפואיים, תשלומים בסלולרי, שיחות באפליקציות היכרויות ועוד. הטכנולוגיות הפורנזיות שמפעילות רשויות החקירה בישראל יכולות להעתיק נתונים מהאפליקציות הפופולריות ביותר, תוך עדכונים שוטפים לתמיכה במגוון אפליקציות. למשל: גוגל מפות, גוגל תמונות ו-Gmail; אפליקציות היכרויות כמו טינדר, גרינדר ו-OkCupid; אפליקציית Nike + Run; אפליקציות מדיה חברתית, כמו פייסבוק, אינסטגרם, טוויטר וסנאפצ'ט; דפדפנים כמו כרום ופיירפוקס; ואפילו אפליקציות מסרים מיידיים מוצפנות, כמו סינגל וטלגרם. מכיוון שאפליקציות צד שלישי שמתקינים המשתמשים נוטות לאחסן נתונים בשיטות מוכרות, הכלים הפורנזיים יכולים להעתיק ולנתח את המידע בקלות רבה.
- נתונים ש"נמחקו": כלי זיהוי פלילי למכשירים ניידים יכולים לעיתים לגשת לנתונים "שנמחקו" מהטלפון. בדומה לאופן שבו קבצים שנמחקים במחשב מועברים בדרך כלל ל"סל המיחזור", כך גם קובץ שנמחק מהטלפון ניתן לעיתים לשחזור. יתרה מכך, מחיקת הקובץ מהטלפון עצמו לא תמיד מוחקת אותו מגיבוי הענן של המשתמש, או ממגוון המקומות האחרים שבהם הוא נשמר אולי בשלב מסוים. לפעמים ניתן לשחזר קבצים "שנמחקו לצמיתות" בעזרת הכלים המתאימים, כי הם לא נמחקים, אלא מסומנים כ"שטח פנוי" עד שהם מוחלפים בנתונים אחרים.
- נתונים נוספים בטלפון (meta data): טלפונים מתעדים כמויות עצומות של נתונים הנוגעות לאופן שבו אנשים מתקשרים עם המכשיר - מידע שמוגדר כ"מכרה זהב דיגיטלי". כלי זיהוי פלילי למכשירים ניידים יכולים לשחזר רשומות שמראות מתי אפליקציות הותקנו, היו בשימוש ונמחקו, כמו גם באיזו תדירות השתמש בהן. נתונים אחרים מגלים מתי המכשיר ננעל או נפתח, מתי

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

המשתמש קרא הודעה, האם ומתי בוצעה התחברות להתקן בלוטות', מילים שנוספו למילון המשתמש, תוכן של התראות או חיפושים בשירות Spotlight המובנה במכשירי אייפון, שמציג תוצאות מהמכשיר ומהאינטרנט. טלפונים עשויים אפילו לאחסן צילומי מסך של אפליקציות פתוחות המוצגות למשתמשים כאשר הם עוברים בין יישומים פתוחים.

ג. עוצמת הפגיעה הקשה של חדירה לטלפון נייד בעידן מחשוב ענן

המונח "מחשוב ענן" (Cloud Computing") מתאר מודל לשירותי תקשוב (ICT) מבוססי רשת מחשבים, המאפשר גישה לפי-דרישה למאגר משותף של משאבי מחשוב המצויים בשרתים מרוחקים, כגון אחסון מרוחק של קבצים ונתונים ללא צורך בשמירת המידע על מכשירי הקצה. היישום המוכר והנפוץ של מחשוב ענן הוא אחסון קבצים ומידע באופן מרוחק, להבדיל מהמודל המסורתי של מחשבים ומכשירים חכמים, בו הקבצים והמידע אותם יוצר או "מוריד" המשתמש מאוחסנים על גבי מכשירי הקצה שברשותו (מחשבים וטלפונים חכמים של המשתמש הרגיל, ושרתים מקומיים בארגונים).

כך, מחשוב ענן משנה באופן יסודי את פרדיגמת טכנולוגיות המחשוב והמידע, מסביבת חישוב אישית/ארגונית לסביבת חישוב מבוזרת, כאשר רשת האינטרנט מספקת לרוב את עמוד השדרה הנדרש כדי לספק את שירותי הענן.

לעניינו, המשמעות העיקרית של מהפכת מחשוב הענן ביחס לחיפושים במחשבים ומכשירים חכמים היא שהיקף המידע אותו ניתן להפיק מפריצה לטלפונים חכמים לא מוגבל עוד לשטח האחסון של המכשיר ובמקרים רבים המידע נמצא בשרתים מרוחקים, לרוב מחוץ למדינת ישראל. אפליקציות רבות מבוססות על יצירת חשבון משתמש, ומסנכרנות את הנתונים בענן כדי לאפשר למשתמשים גישה מרחוק. כך, נתונים שנוצרו במכשיר אחר עשויים להיות שמורים או זמינים לצפייה בטלפון, ונתונים מהטלפון עשויים להיות מגובים בענן. **הכלים הפורנזיים שקיימים כיום בידי רשויות האכיפה בישראל לוקחים בחשבון את כל האפשרויות, וספקים רבים מציעים פיצ'רים או מוצרים ספציפיים לחילוץ גיבויים משירותי ענן ופרטי חשבון אחרים.**

למשל, היסטוריית המיקומים של גוגל היא אחד ממקורות המידע העיקריים. כל משתמש שמפעיל את אפשרות שמירת המיקום בחשבון המשתמש בגוגל מאחסן רשומות מקוונות של מיקומו. משתמשים רבים לא מבינים שהנתונים המדויקים על אודות תנועותיהם במרחב נשמרות לזמן בלתי מוגבל. למעשה, גוגל שומרת את המידע גם כאשר המשתמש לא מבצע פעולה שמשתמשת במיקום המכשיר. אם יש לרשויות אכיפת החוק גישה פיזית או מרוחקת לטלפון, הן יכולות להשתמש בכלים הפורנזיים שברשותן כדי להיכנס לחשבון המשתמש בגוגל, להעתיק את היסטוריית המיקומים ולהציגה על ציר זמן או מפה.

ד. אי-עדכון החקיקה בנושא חיפושים והאזנות סתר לעידן האינטרנט והענן לא מאפשר להבטיח את מידתיות הפגיעה שלהם בחירויות הפרט

פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט-1969 ("פקודת סדר הדין הפלילי") מסדירה היבטים שונים של חקירת עבירות פליליות, לרבות מעצרים, חיפוש, תפיסה וחילוט. בשנת 1995, במקביל לחקיקת חוק המחשבים, עודכנה פקודת סדר הדין הפלילי על מנת להסדיר את האופן שבו רשויות החקירה רשאיות לבצע חדירה לחומר מחשב, בדומה לאופן בו מוסדרת יכולתן לבצע חיפוש במקומות פיזיים.

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

עם זאת, הוראות פקודת סדר הדין הפלילי בעניין זה מנוסחות באופן לקוני, ולא עודכנו להתמודד עם האתגרים הקשים והייחודיים של חיפוש בחומר מחשב בעידן הרשת והמידע: סעיף 23א(א) קובע כי "חדירה לחומר מחשב וכן הפקת פלט תוך חדירה כאמור, יראו אותן כחיפוש וייעשו על-ידי בעל תפקיד המיומן לביצוע פעולות כאמור". סעיף 23א(ב) מגדיר באופן לקוני למדי את התנאים לביצוע חדירה לחומר מחשב מצד רשויות החקירה, אשר תעשה על פי צו שיפוטי המפרט את מטרות החיפוש ותנאיו "שייקבעו באופן שלא יפגעו בפרטיותו של אדם מעבר לנדרש".

באופן דומה, גם חוק האזנות סתר, תשל"ט-1979 – שעליו לכאורה מתבססת הפעלת כלים רבי-עצמה לחדירה מרחוק לטלפונים חכמים כגון נוזקת פגסוס ודומותיה מהווה מסגרת חקיקתית מיושנת, שהתעצבה במאה-הקודמת, בעידן בו לא ניתן היה לדמיין את העושר והאינטימיות של המידע שניתן להפיק באמצעות התחקות אחר מכשיר הטלפון הנייד של אזרחים.

למרות שבבתי המשפט התגבשה זה מכבר ההכרה בהיקפי הפגיעה העצומים של סמכויות רשויות המדינה לתפוס ולחדור לחומרי מחשב וטלפונים ניידים בפרט, החקיקה הרלוונטית נותרה הרחק מאחור ואינה מספקת מענה מספק לאתגרים החוקתיים הייחודיים שמתעוררים כתוצאה מהיקף המידע האישי והרגיש שרשויות החקירה יכולות להפיק מחדירה וחיפוש במכשירים דיגיטליים אישיים.

על רקע זה, כנקודת מוצא לדיון הציבורי שיש לקיים בימים אלו, חשוב להבין שהיעדרה של מסגרת חקיקתית עדכנית לחיפושים או "האזנה" לטלפונים חכמים בשיאו של עידן הרשת והמידע, למרות העליה בהיקף השימוש בהם על ידי רשויות החקירה בישראל, מאפשרת להפעיל כלים חודרניים ורבי עצמה ללא מגבלות או מנגנוני פיקוח הנדרשים כדי למנוע פגיעה לא-מידתית שלהם בזכות הפרט.

***

עם חתימה נציין כי איגוד האינטרנט הישראלי משלים בימים אלו מסמך סקירה ומדיניות מקיף על טכנולוגיות הפריצה והחיפוש המתקדמות שמפעילות רשויות החקירה בישראל והצורך בעדכון המסגרת המשפטית להפעלתן – אשר חלקו הראשון צפוי להתפרסם בשבועות הקרובים.

נשמח לעמוד לרשותכם בכל הבהרה או בקשה למידע נוסף. ניתן לפנות אלינו באמצעות הדוא"ל: policy@isoc.org.il.

בברכה ובכבוד רב,

ד"ר אסף וינר
ראש תחום רגולציה ומדיניות
איגוד האינטרנט הישראלי (ע"ר)

עו"ד יורם הכהן
מנכ"ל
איגוד האינטרנט הישראלי (ע"ר)