



חדשות

משפט הסייבר ההתקפי

אפל בין השורות: משרד הביטחון שותף של NSO

התביעה המהדהדת של ענקית הטכנולוגיה האמריקאית נגד מפתחת תוכנת הריגול הישראלית מתמקדת בטענה כי NSO לא פעלה רק בכוחות עצמה אלא נתמכה על ידי מדינת ישראל • מבלי להזכיר את שמה, התביעה מייחסת לישראל ולרשויות בה, שותפות בעזרה ישירה ועקיפה

עומר כביר

האקרים ידועים לשמצה. שכירי חרב חסרי מוסר מהמאה ה-21, שיצרו מנגנון מעקב סייבר מתוחכם שמזמין שימוש בוטה לרעה. במילים אלו מתארת אפל את NSO הישראליית בפתח התביעה שהגישה נגדה שלשום. ובעולם של מסמכים משפטיים, זה הדבר הקרוב ביותר ל"שירה".

כתב התביעה של אפל לא עושה ל-NSO שום הנחות, ובין השאר ממצב אותה כמאבק עקרוני בין שתי תפיסות עולם. "NSO היא האנטייזה לכל מה שאפל מייצגת מבחינת אבטחה ופרטיות", נכתב. "בשעה שאפל יוצרת מוצרים שמשדרים את ומגינים על משתמשיה, NSO תוקפת ומנסה לנצל את המוצרים האלו כדי לפגוע באפל והמשתמשים".

אבל מה שצריך להטריד את מדינת ישראל הוא המסגור שנתת אפל לתביעה שלה. לא כתביעה של חברה פרטית אחת נגד חברה פרטית אחרת, אלא תביעה נגד חברה במימון ותמיכת מדינה. המסגור הזה הופך את התביעה לכתב אישום לא רק נגד NSO אלא גם נגד מדינת ישראל. וכשהתובעת היא חברה של 2.8 טריליון דולר, לא מדובר במהלך שאפשר להתייחס אליו בניטול.

לדברי אפל, התביעה הוגשה במטרה לאלץ את NSO לשאת באחריות למעקב שמבוצע אחרי משתמשי אפל באמצעות תוכנות הריגול שלה. בנוסף, כרי מנוע פגיעה נוספת לרעה במשתמשיה, אפל מבקשת צו מניעה קבוע שיאסור על NSO לעשות שימוש במכשירים, תוכנה או שירותים של אפל. "הפעילויות הזרניות של NSO ניצלו לרעה את מוצרי אפל, פגעו במשתמשי אפל והזיקו לפעילות העסקית ולשם הטוב של אפל. המוצרים והשירותים הודוניים של NSO גם חייבו את אפל להשקיע אלפי שעות בחקירות המתקפות, זיהוי הנזק, אבחון היקף הפגיעה, ופיתוח תיקונים נחוצים כדי להבטיח שהשירותים והאפליקציות של אפל יישארו מאובטחים ליותר ממיליארד הפרטים והיחידות שמהווים חלק מקהילת אפל העולמית", נכתב.

קובץ PDF זדוני נשלח למכשיר

התביעה קשורה לפירצה ספציפית לאייפון, מק ואפל ווטש בשם FORCEDENTRY, שזוהתה על ידי חוקרי סיטיון לאב באוניברסיטת טורנטו בספטמבר ותוקנה מאז על ידי אפל. "FORCEDENTRY היתה פרצה בתוכנת iMessage של אפל, שמוקנת כברירת מחדל בכל מכשירי אפל", אמר ל"כלכליסט" ר"ד ביל מרוק מסיטיון לאב, שהוביל את זיהוי הפירצה. "התוקף שלח ב-iMessage קובץ PDF זדוני למטרה, והאפליקציה היתה מעבדת אותו אוטומטית. בזמן העיבוד, ה-iMessage PDF שיבש וחסף את השליטה ב-iMessage והוריד רושעה - תוכנה שמטרתה לגרום נזק, ופרצות נוספות כדי להתקיין את פגסוס על הטלפון. הפירצה בלתי-נראית למטרה, כי היא משבשת את iMessage לפני שמוצגת התרעה למשתמש".

■ **מזהה הפירצה: "התוקף שלח ב-iMessage קובץ PDF זדוני שחטף את השליטה ב-iMessage והוריד רושעה להתקנת פגסוס על הטלפון"**

חייסד NSO שלו חוליו. החברה בדרך למשה, השאכה את מ' היא תגרוור איתה לשם

לרברי אפל, בפרצה זו נעשה שימוש נגד מספר קטן של משתמשי אפל בכל העולם. החברה תודיע למשתמשים שנפגעו ותעשה כך גם בעתיד כשתאחר מתקפת רוגלה מצד שחקן נתמך מדינה. אפל וורשת מבית המשפט לחייב את NSO בתשלום פיצויי נזיקין ועונשין, וחילוט רווחים שהתקבלו מתקיפת מכשירים של אפל. משמעותי יותר - היא דורשת צו מניעה קבוע שיאסור על NSO לגשת או לעשות שימוש בשירותים, מכשירים, שירותים, חומרה, תוכנה, אפליקציות ומוצרים ושירותים אחרים של אפל.

לא מדובר באיסור סמלי אלא ברדישה מוחתית בעלת השפעות ישירות על פעילות החברה. בלי אפשרות חוקית לגשת למוצרים ושירותים של אפל, עובדי NSO לא יכולים לאתר בהם פרצות לתוכנת רוגלה שתשלט עליהם או לבדוק את פעילות הרוגלה. מכיוון שפירצה לאייפונים היא העסק המרכזי של

NSO, צו מניעה שכזה ישבית למעשה את פעילות החברה. אם היה ספק, אפל גם מבקשת צו מניעה שיאסור על NSO לפתח, להפיץ, להשתמש או לאפשר לאחרים להשתמש בכל רוגלה, נזקה או מכשירים זדוניים אחרים נגד מכשירים, מוצרים ושירותים של אפל, בלי הסכמה הן של החברה והן של המשתמש הרלבנטי. כלומר, אם NSO רוצה לרגל אחרי משתמש כלשהו, היא צריכה להודיע לו על כך ולבקש את הסכמתו.

נראה שהתביעה הכניסה את NSO להלם מוחלט, או העמיד קה את ההלם שבו החברה כבר היתה שרויה אחרי שכמה שעות קודם לכן הודיעה מוד"ס על הורדת דירוג החוב של החברה - צעד שמקרב אותה למצב של חדלות פירעון - שכן התגובה שלה היתה מהוססת ונעדרת השראה. "אלפי חיים מסביב לעולם ניצלו הודות לשימוש שעשו לקוחות NSO בטכנולוגיות שלה", נמסר. "פרופילים וטרוריסטים יכולים לפעול בחופשיות במקלטים טכנולוגיים, ואנחנו מספקים לממשלות את הכלי החוקי להלחם בזה". זה אותו קשקוש רגיל שכבר לא מרשים אף אחד. NSO תידרש ליותר מקוריות ויצירתיות על מנת להשיב לטענות אלו, תיאלץ לשלוף טיעונים מהותיים יותר מאשר הספינים השחוקים והממוחזרים שלה.

מדובר בקרב ביחסי כר חת לא הוגנים: השווי של אפל מתקרב ל-3 טריליון דולר, ל-NSO יש חוב



13.7.20

בית המשפט בישראל דוחה עתירה לבטל את רישיון היצוא של NSO

הצרות החתלגלות של NSO

הגילויים על שימוש לרעה בתוכנת הריגול שלה ואובדן ההכנסות והלגיטימציה

קואליציית חברות טכנולוגיה מובילות, בהן גוגל ומיקרוסופט, הגישה תצהיר תמיכה בבייסבוק בתביעה נגד NSO

22.12.20

חברת הדירוג מוד"ס לכלכליסט:

NSO תתקשה למכור רישיונות חדשים

רגולציה וליטיגציה יכולים לקחת שנים כדי להשפיע על פעילותן של חברות כמו NSO. וול סטריט מעניש מהר הרבה יותר. בימים אלו חוב בהיקף של 350 מיליון דולר שגייסה החברה ב-2019 הפך ממש רעיל כשסוחרים הציעו ככל הנראה 70 סנט על הדולר כדי להיפטר ממנו. הבעיה התחילה זמן קצר אחרי שממשלת ארה"ב הכניסה את החברה לרשימה השחורה והגדרה אותה כסכנה לביטחון הלאומי. בתגובה מלוויים ניסו למכור את החוב למשקיעים אחרים אך התקשו למצוא קונים, גם לא במחיר המזול. בתגובה מיהרה חברת הדירוג מוד"ס

להוריד את דירוג החוב בשתי רגות לרמה של Caa2 שנמוכה בשמונה דרגות מרמת השקעה. "לחברה יש נתח נמוך יחסית של הכנסות חוזרות", אמר ל"כלכליסט" דירק גוירי, אנליסט מוד"ס ומחבר הדו"ח. "בניגוד לחברות תוכנה רבות אחרות, היא תלויה מאוד במכירות של רישיונות חדשים שלרועי תנו יהפכו לקשות הרבה יותר בהתחשב בפעולות שננקטו נגדה". לדברי גוירי אם החברה לא תמצא נתיב לטיפול בחוב, היא עלולה לעלות על נתיב של חדלות פירעון.

בעיות המוניטין של החברה צפויות לא רק להאט מכירת מוצרים חדשים ולפגוע בתורים המזומנים שלה, אלא אף להקשות עליה לגייס הון ולסכל בוודאות גדולה את תוכנית ההנפקה לפי שווי מתוכנן של 2 מיליארד דולר. כעת הכרוך בידים של הבנקים המלי וויס קרדיט סוויס וג'פריס ססירבו להי תייחס לנשוא. השניים העניקו לחברה אשראי של 500 מיליון דולר ב-2019. אז זה נעשה על בסיס דירוג של B2 שנחשב לגבוה ביותר לחברת סייבר. באותו זמן הדירוג לא גילם את הסכנה במתן אשראי לחברה שסומנה על ידי ארגוני החברה האזרחית כמפרה זכויות אדם.

ויקי אוסלנדר

אפקט NSO

ישראל צמצמה ל-37 את המדינות ליצוא סייבר

שיש בה כיום 500 חברות סייבר. לא ברור עדיין מדוע צומצמה הרשימה אבל ייתכן מאוד שאחת הסיבות לכך היא העובדה שמשרד הביטחון ידע מראש על כוונת הרשויות בארץ הישראליות - NSO וקנדירו - לרשימת החברות שפעילותן נוגדת את האינטרס לביטחון הלאומי האמריקאי. רשימה זו מקבלת עוצמה גדולה יותר אל מול תביעתה של אפל נגד חברת NSO. לפי הודעת משרד המסחר האמריקאי, "כלים אלו אפשרו לממשלות זרות לבצע פעולות דיכוי חוצות גבולות - הנוהג של ממשלים סמוכתיים לתקוף מתנגדים, עיתונאים ואקטיביסטים מחוץ לגבולותיהן כדי להשתיק התנגדות. נוהג כזה מאיים על הסדר הבינלאומי".

- בלעדי לכלכליסט -

בתחילת נובמבר פרסמה ישראל את רשימת המדינות שמותר לייצא אליהן סייבר. הרשימה כוללת 37 מדינות - מרביתן במערב אירופה, אוסטרליה, ארה"ב וקנדה (הרשימה המלאה בסוף הידיעה). ל"כלכליסט" נודע שרשימה זו קטנה משמעותית לעומת הרשימה שהיתה עד הערוך וכללה 102 מדינות.

ברשימה שהתפרסמה בנובמבר לא נכללות מדינות דוגמת מרוקו, מקסיקו, ערב הסעודית או איחוד האמירויות אשר על פי הפרסומים רכשו מערכות סייבר התקפי של חברת NSO. החברה הישראלית אמנם לא אישרה את מרבית הפרסומים אבל ציינה שלכל המדינות אליהן מכרה היא קיבלה את אישור המדינה. אם טענתה של החברה הישראלית אכן נכונה, אז משתמע שישראל השתמשה בצורה מדינית מאוד באישורים המיוחדים שהיא רשאת לתת והיתה מיודעת בכל מקרה לאן מוכרת החברה הישראלית.

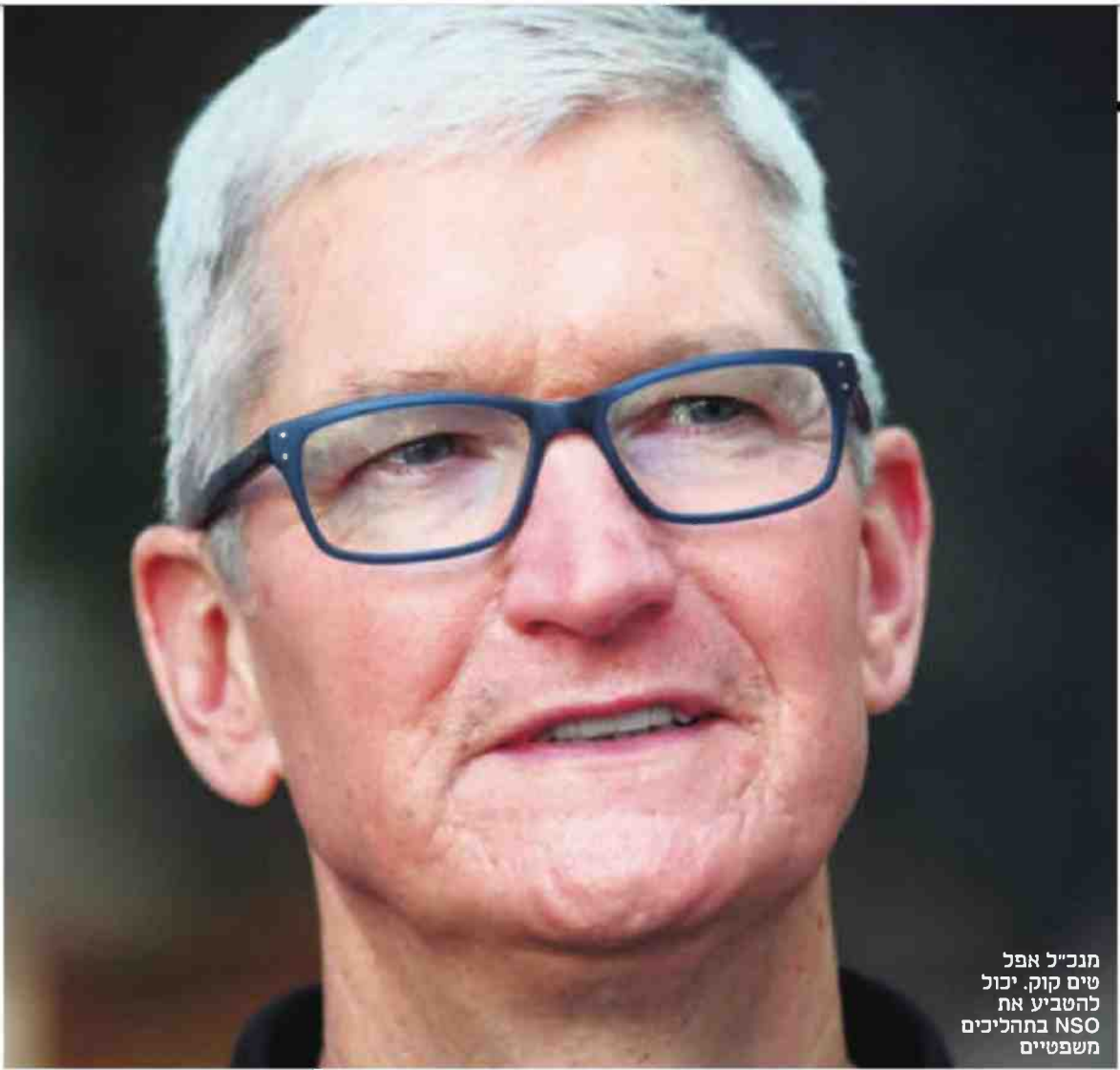


שר הביטחון בני גנץ. הפיקוח על יצוא סייבר התקפי

בתגובה נמסר ממשרד הביטחון כי "מדינת ישראל בוחנת כל העת את מדיניות הפיקוח על היצוא הביטחוני שלה ובכלל זה את מדיניות הפיקוח על יצוא של מוצרי סייבר. מדינת ישראל מאשרת יצוא מוצרי סייבר רק עבור גורמי ממשל, לשימוש חוקי ולמטרות מניעת חקירת פשיעה ולוחמה בטרור בלבד. כל זאת, בכפוף להתייעלות מטעם המדינה הרלוונטית".

כשת. ככל שמתברר כי נעשה שימוש בניגוד לתנאי הרישיון או בניגוד להצהרות מטעם המדינה הרוכשת ננקטים הליכים מתאימים. מדינת ישראל אינה מפרטת אודות מדיניות הפיקוח על היצוא הביטחוני.

ברשימת המדינות החדשה שאליהן ניתן לייצא סייבר, נכללות: אוסטרליה, איטליה, אירלנד, אסטוניה, בולגריה, בלגיה, בריטניה, גרמניה, דנמרק, הולנד, יוון, לוקסמבורג, לטביה, ליטא, ליכטנשטיין, מלטה, נורבגיה, סלובניה, סלובקיה, ספרד, פורטוגל, פינלנד, צ'כיה, צרפת, קרואטיה, קפריסין, רומניה, שוודיה, שווייץ, אוסטרליה, הודו, יפן, ניו זילנד, דרום קוריאה, ארצות הברית וקנדה.



מנכ"ל אפל טים קוק. יכול להטביע את NSO בתהליכים משפטיים

■ אפל מבנה ש-NSO הגיעה למעמדה בעזרת המנגנון של מדינת ישראל שכולל עזרה ישירה לקשרים בכניסה למדינות ורגולציה שמספקת מטרית הגנה

לתת. המדינה לא מוכרת לאורך ההודעה לעיתונות, שלא מציינת אפילו ש-NSO היא חברה ישראלית, אבל לא צריך להיות שרלווק הולמס כדי להבין שהתביעה היא לא אפל נגד NSO, היא למעשה אפל נגד מדינת ישראל. אפל מבנה היטב שער כמה שיש מקום לביקורת ופעילות נגד NSO, החברה לא היתה מגיעה למעמדה בלי המנגנון של מדינת ישראל מאחוריה. זה כלל עזרה ישירה ברמות קשרים שסייעו להיכנס למדינות שונות ומנגנון רגולטורי לא אפקטיבי במכוון, שנועד לספק ל-NSO מטריות הגנה משקיפות ומתביעות ולאפשר לה לפעול בחסות הטענה שהיא נמצאת תחת פיקוח ולכן משתמע שכל פעילויותה תקינות. זה התבטא ברמות שיתופי פעולה, במסגרתם NSO שימשה כמעין זרוע לא רשמית של מדינת ישראל במדינות שאיתן אין יחסים רשמיים. ברמה העמוקה יותר, הקשר הזה כולל סיוע לא ישיר ברמות הכשרת כוח האדם של NSO. החברה לא ציחה להכשיר את העובדים שלהם מאפס, מדינת ישראל עושה את זה בשבילה, דרך יחידת 8200 שממנה מגייסת NSO חלק ניכר מעובדיה. אחת הסיבות שיש בישראל כל כך הרבה חברות סייבר התקפיות ברמות NSO היא איכותי של כוח אדם מנוסה שיוצא מדי שנה לשוק העבודה.

NSO היא לא סתם חברה ישראלית. היא חברה שיכולה לפעול כפי שהיא פועלת רק בישראל. המדינה היא שותפה של NSO, יודעת היטב מה היא עושה ומי הם לקוחותיה, מעודדת ותומכת בה לכל אורך הדרך. אפל מבנה את זה היטב, ואם ההודעה שלה היא אינדיקציה למשהו עלולה להפוך את זה לנרטיב מרכזי בתביעה נגד החברה. יש כאן קופת רצים עמוסה, ואפל מחזיקה במפתח.

של 500 מיליון דולר. אפל יכולה להטביע אותה במסמכים משפטיים, תצהירים, בקשות לגילוי ראיות ופרקליטים באופן שיהפוך את התביעה למעמסה שתחבל בפעילות של NSO, ולא להרגיש אפילו דרגו קל בשוררה התחזונה שלה. טים קוק לא יאבד שעות שינה בגלל התביעה הזו. שלו חוליו זה כבר סיפור אחר.

ארגון מסחרי שפועל בשליחות מדינה

צדפו לזה את הצרות האחרות של NSO - התביעה של מטא (לשעבר פייסבוק) בעקבות הפריצה לווטסאפ שקיבלה אור ירוק מבית משפט פדרלי לערעורים; הכניסה לרשימה השחורה של מחלקת הסחר של ארה"ב; הגילויים המתמשכים על שימוש לרעה בתוכנת הריגול שלה; אובדן חושים על רקע החשיפות האחרונות; אובדן הלגיטימציה והאמינות הבינלאומיות - והמצב של החברה נראה כבי רע. היא כנראה תשרוד את 2021. אך לגבי 2022 - כל האפשרויות פתוחות, במיוחד אם הצרות ימשיכו בקצב הנוכחי. NSO בדרך למטה. השאלה הבאה היא את מי החברה עוד תגי רור איתה לשם. כי כמו שאפל מבהירה היטב, החברה לא פועלת בוואקום, לא קמה ופרחה לגמרי בכוחות עצמה. אף שכתב התביעה עוסק ב-NSO, ההודעה לעיתונות שפרסמה אפל ממסגרת את החברה לא כיישות פרטית ועצמאית, אלא כיישות שפועלת במימון/תמיכה/חסות של מדינה (sponsored state). אפל מבהירה שמבחינתה היא לא מתמודדת מול חברה פרטית, אלא מול ארגון שפועל בשליחות מדינה, ושנהנה מתמיכה ומשאבים שרק מדינה מסוגלת

מאיר אורבך

23.11.21

מודי'ס חותכת את דירוג החוב של NSO ואפל תובעת את החברה



איציק בנבנישתי עוזב את NSO פחות משבועיים לאחר שמונה לתפקיד המנכ"ל

11.11.21

8.11.21

התביעה של מטא (לשעבר פייסבוק) בעקבות הפריצה לווטסאפ קיבלה משפט פדרלי

3.11.21

NSO הוכנסה לרשימה השחורה של מחלקת הסחר של ארה"ב

24.8.21

לפי דו"ח חדש של סיטיזן לאב, מגוסט שימשה לריגול אחרי פעילי זכויות אדם ומתנגדי משטר בחריינים

19.7.21

מתפרסם "פרויקט פגוסוס" - תחקיר בינלאומי ענק שחושף את היקף השימוש בתוכנת פגוסוס

5.2021

מודי'ס הורידה לראשונה את דירוג האשראי של NSO ל-B3 בשל "התכווצות ביצועים והחלשות הנזילות"



צילומים: אוראל כהן, קובי קואנוקס, רויטרס, אי.אף.פי