

Date : 12/30/2018 10:24:37 AM
From : "Nir Seri"
To : "Liat Ben Ari" , "Jonathan Tadmor" , "Etty Ben Dor"
Cc : "Elad Pinchas" , "Noga Blickstein Shchory" , "Yaron Golomb"
Subject : תקלה במערכת הסלברייט
Attachment : [oledata.mso;195684_image002.jpg](#);

שלום לכולם

ברצוני לעדכן אותכם, כי הובא בפניי, שככל הנראה ישנה תקלה במערכת הסלברייט באופן בו תוצאות החיפוש שנעשים במערכת ייתכן ואינן מהימנות.

בתיק אמה/עוז אותו אני מלווה, החוקרים במשך תקופה ארוכה פועלים למיצוי חומרי המחשב. לפני מספר שבועות החוקרים עצרו את פעולת המיצוי, לאחר שהתגלו תקלות שונות במערכת:

א. בחיפוש שבוצע לא אותרה תעבורת מיילים לתקופות ממושכות, למרות שניתן היה לצפות כי בתקופות אלה תימצא תעבורת מיילים כזו.

ב. שם השולח/מקבל המייל בתוצאת החיפוש הופיע כ-unknown.

ג. חוסר התאמה בין מספר האירועים שתוצאת החיפוש מניבה לבין מספר האירועים שמצורפים לדו"ח חיפוש.

לאחר שעודכנו כי התקלות נפתרו, חזרו החוקרים להמשיך בביצוע מיצוי חומרי המחשב. במערכת סלברייט המשודרגת תקלות א' וג' נותרו על כנן. תקלה ב' נפתרה כמעט באופן מלא.

החוקרים עבדו במקביל על מערכת ה-NUIX שגרסה שלה נמצאת ברשות המסים לבחינת התקשרות עתידית, ובחיפוש באמצעות מערכת ה-NUIX נמצאה תעבורת מיילים (גם אם דלילה) בתקופה בה במערכת הסלברייט לא הניבה תוצאות.

בנוסף חיפוש שם שולח שבמערכת הסלברייט לא הניב תוצאות, הניב תוצאות במערכת ה-NUIX.

ניר

From: SharonBe2@taxes.gov.il [mailto:SharonBe2@taxes.gov.il]

Sent: Thursday, December 27, 2018 1:52 PM

To: Nir Seri

Cc: DrorCo@taxes.gov.il

Subject: סיכום פעילות במעבדה מאתמול - OZ./משימת מיצוי הראיות מהמחשבים בתיק רגב/ר.ש.ת. (26/12/18))

This message has been analyzed and no issues were discovered.

ניר שלום,

אני רואה לנכון לשתף אותך, מעבר לכך שדיברנו על כך בע"פ, גם בכתב בדברים שהעלינו דרור ואנוכי במהלך הניסיון הנוסף להתקדם במשימת מיצוי הראיות מהמחשבים שביצענו במעבדה של אילן אבנרי אתמול.

כדי שיהיה לך כתוב מול העיניים ותזכור שאנחנו ממתנינים להחלטה אופרטיבית שלך בעניין:

ניר שים לב במיוחד למה שהדגשתי בצהוב

<p>לאחר הפסקה יחסית ארוכה של כחודשיים (מאז אוקטובר) בעבודת מיצוי הראיות מהמחשבים, שהופסקה בעקבות תקלות שונות ובאגים במע' סלברייט, התקבל אישור מאילן שנוכל להגיע ולהמשיך לעבוד. מערכת סלברייט שודרגה לשרת חדש ("16") וגרסה חדשה שלה לאחר שעברה אינדוקס, אמורה להפיק דו"חות מלאים יותר, ללא</p>	<p>ביקור נוסף של שרון ברגר ודרור כהן במעבדת מיצוי ראיות המחשבים של אילן אבנרי בראש"צ לצורך המשך עבודה, הזנת חיפושים והפקת דו"חות. יש לקרוא את כל תוכנה של העמודה השמאלית שתועדה כאן עבור יום זה אשר בסיומו נקבע עם אילן אבנרי כי יודיע לנו (דרור ושרון) בימים הקרובים, מתי ניתן יהיה להגיע להמשך חיפושים (ובעיקר לפי איזו מערכת נעבוד – האם Cellebrite או Nuix).</p>	<p>26.12.18</p>
---	--	-----------------

שרון אמר לאילן שבשבוע הקרוב אנחנו פנויים ונוכל להגיע אליו באינטנסיביות מידי יום.

אירועי "UNKNOWN" וללא "חורים בזמן" וכן עם ספירה מדוייקת של אירועים וכן להיות מסוגלת להפיק דו"חות שיש בהם הרבה יותר אירועים מהגרסה הקודמת (בקודמת, דו"ח עם כמה מאות כבר היה מפיל את המערכת, ובנוכחית אמורים להיות מסוגלים להפיק דו"חות עם אלפי אירועים.

הביקור של דרור ושרון במעבדת המחשבים ב- 26/12 העלה את הממצאים הבאים: במערכת הסלברייט בגרסתה החדשה ישנם הרבה יותר אירועים מאשר במערכת בגרסתה הישנה. בערך פי 10. (למשל אם תנאי חיפוש שהוזן במערכת הישנה הניב כ- 2,000 תוצאות, הרי שבמערכת החדשה אותו חיפוש יניב כ- 20,000 תוצאות. **דבר נוסף:** עדיין יש תופעה תמוהה שבשנים 2006 עד 2008 אין שום תעבורת אימיילים כלשהיא מ/אל רשת/wreat ושום איכור לתיבות דוא"ל

בעלות הסיומת gecko.gb.com ואף **מדאיג יותר מכך** הוא שגם בשנת 2010 ישנה מעין "דממה" בתכתובות (לאחר ש-2009 דווקא עמוסה בתכתובות). **בנוסף לאלו**, עדיין ישנה תופעת אי התאמה בין מספר האירועים שתנאי חיפוש מוליד, ובין מספר המשבצות שיש לסמן ב-√ כדי להפיק דו"ח וכן ישנה מגבלת אירועים לדו"ח: אמנם המגבלה היא כ-20,000 לדו"ח אבל הצרופות מוגבלות ל-1,000 (כלומר מספיק שיש דו"ח עם 1,500 אירועים שלכל אחד מהם יש Attachment הדו"ח יקרוס ולא יופק, למרות שמספר האירועים נמוך בהרבה מ-20,000. כ"כ, צרופות קבצי *.dat לא נפתחים.

בעת הביקור הזה אילן אבנרי הציג בפני שרון ודרור אנשי תוכנה של מערכת נוספת, מקבילה לסלברייט – מערכת בשם **NUiX** של חברת ביזטק (נציג החברה: בן, טל' 050-7899467). בן הציג את המערכת שלהם ואת אופן הרצת החיפוש באמצעותה. לצורך השוואה מול מע' סלברייט, הורצו חיפושים בחתך לפי חלון תאריכים 1.3.2006 עד 31.12.2007 כדי לראות האם גם במערכת זו אין אירועים (כמו בסלברייט) ועלו 3,165 תוצאות ואולם כאשר ביצענו חיפוש על gecko מתוך ה-3,165 התוצאות הללו – התוצאה היתה 0. (team6 מתוך ה-3,165 נתן 806 תוצאות) וכאשר הרצנו את שם הדירקטור Stevenson (מתוך כוונה למצוא את David Stevenson יצאו 9 תוצאות של

david.stevenson@fortisintertrust.com

<p>וזו גם התוצאה (9) שיצאה כשהרצנו את fortisintertrust. במערכת הזו Nuix כאשר הרצנו חיפוש על gecko יצא שהמייל הראשון אי פעם שהועבר מכתובת זו (או אל כתובת זו) היה מתאריך 16/12/2008. בחיפוש מוגבל תאריך 1.1.2010-31.12.2010 הועלו במערכת Nuix 92,992 אירועים (נזכיר כי בסלברייט לא הועלו אלא מספר אירועים בודדים במרווח זמן זה !!!) וכאשר חתכנו את ה- 92,992 אירועים הללו לפי gecko הועלו 1,751 אירועים (וחיתוך נוסף של ה- 1,751 לפי @wreat העלה 1,476.</p>		
<p>שרון גם הציע בשיחה זו לניר סרי להסתפק בחומרים שכבר הדפסנו מתוך Cellebrite והינם תוצאה של חיפושים שביצענו עד כה, כדי להטיח אותם בנחקרים ולקדם את אפיק חקירה זה לאור התמשכותו הארוכה מעבר לזמן סביר, ולאור התקלת הרבות שלא נפתרות וכן כניסתה לבחינה של מערכת חדשה. ניר אמר לגבי הצעה זו שהוא יצטרך לחשוב על זה ולתת את תשובתו בעניין ובכל מקרה אמר שנצטרך להפיק דו"חות באשר להפקת הפלטים ששרון כיוון אליהם בהצעתו ושרון אמר שאין בעיה להפיק דו"חות שיפרטו איך הופקו פלטים אלו.</p>	<p>שרון ברגר ודרור כהן התקשרו לניר סרי מהמשרד ועדכנו אותו בדבר הממצאים של יום האתמול, לרבות המערכת החדשה והתקלות שמאפיינות את המערכת הישנה Cellebrite</p>	<p>27.12.18</p>



שרון ברגר, חקירות מס הכנסה
טל. 03-7633894 | קרית הממשלה ת"א