

עלייתו ונפילתו של האתר Silk Road

מאת יורם שפר

COUNT ONE (Narcotics Trafficking Conspiracy)

1. From in or about January 2011, up to and including in or about September 2013, in the Southern District of New York and elsewhere, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and others known and unknown, intentionally and knowingly did combine, conspire, confederate, and agree together and with each other to violate the narcotics laws of the United States.

2. It was a part and an object of the conspiracy that ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and others known and unknown, would and did distribute and possess with the intent to distribute controlled substances, in violation of Title 21, United States Code, Section 841(a)(1).

[צילום מסך מתוך כתב האישום נגד רוס אולברייכט - Dread Pirate Roberts]

מבוא

בראשית 2011 הוקם אתר דרך המשי (SilkRoad) ברשת האפלה. הוא הופל ומפעילו לכאורה, רוס אולברייכט נעצר בספטמבר 2013.

האתר חולל מהפכה בחווית המשתמש של הדארקנט והצליח להפוך את הסחר הבלתי חוקי למסודר ונוח. האתר תיווך בעסקאות סמים, נשק וחיסולים בהזמנה. הדומיננטי ביותר והקשה לעצירה היה שוק הסמים. זאת משום שקל יחסית להעביר אותם בדואר ממדינה למדינה. זאת בעוד שסחר בנשק מסובך יותר בגלל הגילוי של המתכת בדואר. ורוצחים שכירים? ... - טוב, כאן חייבים לסמוך על ביצוע החיסול ע"י אדם שלא נותן לכם שום ערובה לסמוך עליו (דוגמה להונאה כזאת בהמשך הרשומה).

רשויות החוק היו חסרות אונים. האתר הפך למפורסם כמעט בן לילה ואלפי אנשים ברחבי העולם נהנו משירותיו.

ואולם חוסר האונים היה רק לכאורה. הרשת האפלה פועלת לשני הכיוונים: הפעילים מסתתרים מהחוק והחוק מסתתר מהפעילים ובולש אחריהם באותם כלים בדיוק: התחזות ואנונימיות.

מניתוח צבר העסקאות, החוקרים טוענים שמאז החל האתר לפעול בינואר 2011 ועד מעצרו של אולברייכט בספטמבר 2013, בוצעו דרך האתר עסקאות שכללו סך מצטבר של קילו הרואין, 5 קילו קוקאין ו-500 גרם

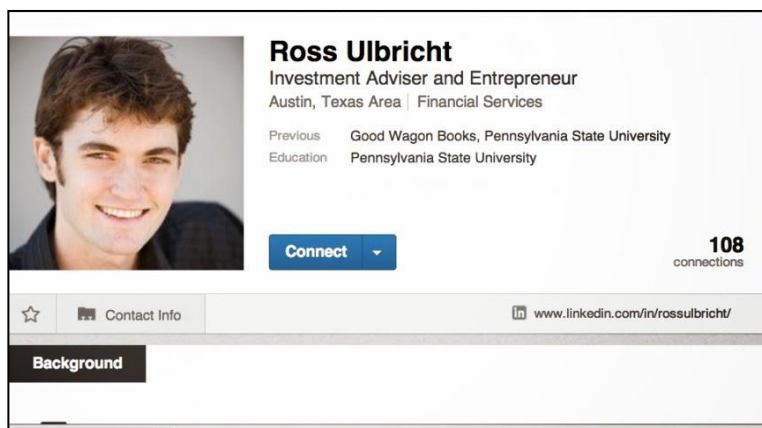
מתאמפיטמינים. האתר גם תיווך בעסקאות מכירה של תוכנות פריצה, [Keyloggers](#) (תוכנות שמקליטות את כל מה שמוקלד במחשב) ומספרי כרטיסי אשראי פעילים, סייע בהלבנת כספים ותיווך מכירה והזמנה של מסמכי מדינה מזויפים. קרוב למליון משתמשים היו לאתר ערב מעצרו של אולברייט, מה שהביא גם לסגירת האתר. על פי מעקב ה-FBI, נערכו בו מליון ורבע פעולות בביטקוין במשך חצי השנה שקדמה למעצר. בקיצור, סצנה רוחשת.

בנוסף, טוען כתב האישום, רוברטס הזמין במרץ 2013 רצח של אדם שאיים לחשוף שמות של אלפי משתמשים בדרך המשי.

<u>Date/Time</u>	<u>Total Bitcoins</u>	<u>Approx. USD</u>
9/14/2013 6:00 UTC	18205.50649	\$2,548,770.91
9/14/2013 12:00 UTC	17420.92877	\$2,438,930.03
9/14/2013 18:00 UTC	17088.67959	\$2,358,237.79
9/15/2013 0:00 UTC	13950.06159	\$1,911,158.44
9/15/2013 6:00 UTC	16143.52567	\$2,195,519.49
9/15/2013 12:00 UTC	15955.46307	\$2,217,809.37
9/15/2013 18:00 UTC	16069.43546	\$2,233,651.53

[מחזור ימי ממוצע ערב סגירת דרך המשי]

ועכשיו לסיפור



Ross Ulbricht
Investment Adviser and Entrepreneur
Austin, Texas Area | Financial Services

Previous Good Wagon Books, Pennsylvania State University
Education Pennsylvania State University

Connect

108 connections

www.linkedin.com/in/rossulbricht/

Background

עד כאן ההאשמות. אבל מה הולך לכתב האישום מסמר השיער הזה ומיהו בכלל רוס אולברייט? צעיר בן 28, בעל תואר שני בפיסיקה ומאמין בתיאוריות אנרכיסטיות.

אולברייט [התגורר בשכירות משנה](#) בסן פרנסיסקו תחת השם המזויף ג'ושוע טרי. הצעיר השקט לא עורר

תשומת לב אצל שותפיו, מאחר שהיה קבור רוב היום מול המחשב הנייד שלו ועסק לדבריו בסחר בשערי חליפין של מטבעות. כמה הופתעו לגלות יום אחד בעיתון שהשכן שלהם נעצר והואשם כמוח שמאחורי רשת הסחר בסמים האינטרנטית הגדולה בעולם. אוניברסיטת דאלאס אגב מיהרה להתנער ממנו וימים ספורים לאחר המעצר [מתקה](#) סימנים ללימודיו אצלה, צעד שהודתה בו אחר כך.



באוגוסט 2013, שבועים לפני שנעצר, [התראיין](#) אולברייט באופן אנונימי לאנדי גרינברג מהעיתון [פורבס](#) וטען שלא מדובר רק בסחר בסמים והרצון להתעשרות (והאמת היא שלמרות שצבר כסף רב, המשיך לחיות בצניעות רבה. ואולי סתם היה קמצן חולני, שכן בראיון התפאר שיום אחד ייכנס לרשימת ה-500 של פורבס), אלא בלחימה לחופש ממרות המדינה וברצון לאפשר לאנשים לבחור באופן חפשי כל מה שהם רוצים לצרוך. "ניצחנו את הקרב על הסמים בזכות [הביטקוין](#)", כתב רוברטס בראיון, שנערך בתקשורת מאובטחת. את כינויו-Dread Pirate Roberts, שאב מסיפור הפנטזיה The Princess Bride וטיפח בחדווה את ההערצה מצד משתמשי האתר שראו בו מושיע, גיבור צ'ה גווארה שלנו, מייצר מקומות עבודה וכו'.

אולברייט היה סטודנט מבריק למדי. בתואר הראשון זכה במלגות שכיסו את כל לימודיו ואת התואר השני בפנסילבניה (Penn state) העביר כעוזר מחקר וכתב את התזה שלו בהנדסת חומרים. בתקופת לימודיו היה גם פעיל פוליטי והשתתף בוויכוחים ציבוריים (debates) על תאוריות כלכליות. הוא נודע [כליבריאני](#) וגם בדרך המשי הרצה את משנת החופש שלו בדבר מיזעור כוחה של המדינה למען מתן אפשרות לפריחת יצירתיות אנושית.

לאחר תום לימודיו עבר לסן פרנסיסקו ונטש את הפיסיקה. הוא אף הודיע על השינוי בדרכו בדף הלינקדאין שלו (שתמונת מסך ממנו מופיעה למעלה).

בחודשיים הראשונים בסן פרנסיסקו התגורר בדירה של חבר בשכונת Hayes Valley, ככל הנראה רנה פינל (Pinnell). פינל אגב לא ידע דבר על פעילותו של אולברייט וסבר שהוא מתקיים מסחר בביטקוין, כשלעצמה פעילות חוקית.

הוא החל לפעול מקפה אינטרנט ולנהל את פעילותו משם. לאחר אותם חודשיים, עבר לשכונת West Portal, שם גם ניסה לשלוח לעצמו מסמכי זיהוי מזויפים. מסמכים רשמיים מזויפים אגב הם גם מוצר שנמכר בדרך המשי ואולברייט היה כנראה לקוח של אחד מסוחרי האתר שלו עצמו.

בעקבות כך הגיעו אליו אנשי המכס וההגירה, מולם נאלץ להזדהות בשמו האמיתי, אולם עדיין לא קישרו בינו ובין דרך המשי. לכיתדו אירעה לבסוף בספריה הציבורית של Glen Park, שבחיבור האינטרנט שלה השתמש. מקום כל כך סמלי ללכוד בו חנון.

הפעילות

סוכני ה-FBI ישבו לו כל הזמן על הזנב ורק חיכו לאיסוף מספיק הוכחות. בין השאר, כפי שמצוטט בכתב האישום, דגמו פעילות כלכלית בחשבוננו ביום רגיל אחד בקיץ 2013 ומצאו שבאותו יום בלבד הרוויח



אולברייכט יותר מ-19,000\$ בעמלות. כלומר, אולברייכט היה מליונר. אמנם בביטקוין ואם היה פודה זאת בדולרים, מן הסתם היה נשאל שאלות על מקור הכסף, אבל בכל זאת מליונר.

חלק מכתב האישום מתייחס לניסיון חיסול לכאורה של אחד ממשתמשי האתר.

מעשה שהיה כך היה: משתמש באתר בעל הכינוי FriendlyChemist יצר קשר עם אולברייכט במרץ 2013 וטען שיש לו רשימה של משתמשים וסוחרים באתר והוא יפרסם אותה אלא אם יקבל כופר של חצי מליון דולר.

אולברייכט דרש הוכחות ו-FriendlyChemist שלח דגימה של כמה מאות שמות. אולברייכט הבין שזה רציני. הוא גם הבין שאם ישלם את הסכום, תבוא דרישה נוספת בעתיד ולכן החליט לאתר את הסחטן ולרצוח אותו. הוא יצר קשר עם מי שטען שהוא רוצח שכיר, משתמש בעל הכינוי redandwhite וניהל איתו משא ומתן על חיסולו של FriendlyChemist.

המשא ומתן התקדם. לאולברייכט נודע ש-FriendlyChemist הוא קנדי מהעיר White Rock בקולומביה הבריטית, נשוי עם שלושה ילדים. הרוצח השכיר redandwhite קבע שני מחירים: חיסול נקי ב-300,000 דולר (כלומר, כזה שייראה כמו תאונה) או חיסול לא נקי ב-150,000 דולר. אולברייכט שוב שלף את עקרונותיו הנעלים: לא אכפת לי שהחיסול לא יהיה נקי כתב לרוצח. FriendlyChemist הפר את עקרון האנונימיות, שעומד ביסודה של דרך המשי. אכן, הכינוי שנתנו לו חסידיו כצ'ה גווארה לא היה רחוק מהמציאות ואני מתכוון לקטלניות שהאחרון היה מוכן להפעיל בשם אידאולוגיה (לכאורה, הכל לכאורה).

אחרי מיקוח, הם סגרו על 150,000 דולר והכסף הועבר בביטקוין. באותו ערב, redandwhite שלח הודעה: האיש לא יסחט אותך יותר ואף שלח תמונה של הקורבן אחרי הרצח. אולברייכט הודה לו בחום. חקירת ה-FBI לא העלתה עם זאת שום מקרה רצח ידוע ב-White Rock, מה דמפחית את האישום לניסיון לרצח, שכן אולברייכט מבחינתו הלך עד הסוף.

אני מודה שמה שלא מובן לי הוא איך פסקו ההודעות על הסחיטה, שכן אם redandwhite רימה את אולברייכט ולא רצח אף אחד, הרי שלכאורה הסחטנות היתה אמורה להמשיך. קיימת כמובן אפשרות שהרוצח השכיר redandwhite הוא עצמו הסחטן, אולם אפשרות זו אינה נראית סבירה, מאחר שאולברייכט פנה אליו במקרה לאחר קבלת הודעת הסחיטה, כאחד מתוך רוצחים שכירים רבים באתר, או כאלו שמציגים עצמם ככאלה.

ימים ראשונים

זמן קצר לאחר ההודעה בלינקדאין על שינוי מטרתן שמטרתן להביא חופש לעולם על ידי שחרור מאלימות הנכפית על ידי המדינה (קיצור של תרגום חפשי), הופיעה בינואר 2011 פורום של אתר פטריות ההזיה [Shroomery](#) הודעה נלהבת של משתמש בשם altoid שטען שהוא "נתקל במקרה" באתר שניתן להגיע אליו דרך TOR. "זהו אתר שמאפשר לכם לקנות ולמכור פטריות באופן אנונימי. חשבתי לקנות שם, אבל רציתי לשאול קודם מה דעתכם ואם מישהו כבר עשה בו שימוש" שואל בהיתממות חבר הפורום. "אפשר להגיע לשם על ידי כניסה לאתר silkroad420.wordpress.com משם תועברו לאתר" הוא מסביר.

מעקב אחרי ההיסטוריה של אותה כתובת בוורדפרס מגלה שהכתובת נרשמה ארבעה ימים לפני אותו פוסט על ידי משתמש בשם altoid, שביצע את הרישום באמצעות שימוש אנונימי ברשת ב-TOR. כלומר, לכאורה זהו אותו משתמש שכתב את ההודעה בפורום. במילים אחרות, מישהו שרצה לקדם את דרך המשי על ידי כתיבת הודעה מתעניינת, שיטה מוכרת ובדוקה לקידום אוביקטיבי לכאורה באמצעות פורומים.

מספר ימים אחר כך, באתר Bitcoin Talk, הופיעה הודעה של altoid בשרשור שעסק בקניה ומכירת סמים באמצעות TOR. גם שם הודיע altoid על הדרך להגיע לדרך המשי באמצעות אותה כתובת בוורדפרס. באותו עמוד היו הנחיות לשימוש ב-TOR, עבור מי שלא מכיר את הדארקנט.

אבל איך מקשרים את altoid לאולברייכט?

שמונה חודשים אחרי אותם שני פוסטים בודדים, altoid מפרסם מודעה בה הוא מודיע כי הוא מחפש מומחה מערכות מידע כדי לפתח מיזם מבוסס ביטקוין. את העונים למודעה הוא מפנה ללא פחות מאשר הג'י מייל הפרטי שלו שעונה לכתובת, תחזיקו חזק - rossulbriect@gmail.com. בינגו, הקישור נעשה.

אני לא משפטן, אבל מנחש שכל אלו אינם מספיקים כדי להרשיע את אולברייכט. אחרי הכל, הוא יכול לטעון כי גם אם הוא altoid, הוא בסך הכל התעניין בדרך המשי ולא קידם אותו כאתר שלו וכן, עצם העובדה שפרסם מודעה עם הג'ימייל הפרטי שלו רק מעצימה את העובדה שהוא פעל ללא דופי, שכן שמר על פרופיל גלוי. וכן - מותר לאדם לפתח מיזם סחר בביטקוין, כשלעצמו המטבע חוקי.

אבל ב-FBI לא טמבלים. הם המשיכו לחפש קישורים נסיבתיים. נבירה בחשבון גוגל+ של אולברייכט (שם גם הופיעה תמונה שלו. ייתכן שהחשבון גם אומת טלפונית, מה שנהוג בגוגל, הוכחה לכך שהוא שלו) הצביעה על קישור ל-mises.org. זהו מוסד אקדמי באוסטריה, הקרוי על שם לודוויג פון מיזס, שבין השאר מקדם את התיאוריה הליברטריאנית הכלכלית, שרוס מאמין בה בדבר מינימום התערבות מדינה וחופש

עלייתו ונפילתו של האתר Silk Road

www.DigitalWhisper.co.il



מקסימלי ליחידים. אולברייט היה משתמש רשום באתר. החתימה של המשתמש בשם דרך המשי באתר דרך המשי כללה תמיד את הקישור למכון Mises. בפוסטים רבים התייחס המשתמש דרך המשי (מי) שהפך אחר כך ל-Dread Pirate Roberts) לאידאולוגיה של מיזס וכלכלן נוסף בשם רוטבארד, כבסיס לפעולה של דרך המשי.

שוב, אני לא משפטן, אבל נראה לי שזה כבר מתחיל להיראות אלגנטי יותר ויותר, הדרך בה ה-FBI קושרת את רוס לזהות של מפעיל ומייסד דרך המשי. כי אם אחד זהה לשלוש (אולברייט הפיזי לאולברייט של ג'ימייל ו-altoid, אוהד של התאוריות של מיזס) ושתיים זהה לשלוש (כלומר המשתמש דרך המשי ל-altoid ולאואד מיזס), אז כנראה אחד זהה לשתיים (אולברייט הוא altoid הוא משתמש המכונה דרך המשי, שהפך באופן ידוע ל-Dread Pirate Roberts).

מתחמם

ה-FBI הצליח לגלות, באמצעות נתונים שקיבל מגוגל (העובדה שהאחרון לא שומר על הפרטיות שלנו כבר ידועה לכל) שהכניסות לניהול אתר דרך המשי נעשו מאינטרנט אלחוטי בבית קפה בסן פרנסיסקו, הסמוך למקום מגוריו הידוע של אולברייט.

רישום נוסף, שהגיע מחברת קומקאסט (עוד חברה שלא שומרת על הפרטיות שלכם), ספקית תשתית אינטרנט, מגלה שכניסה לניהול האתר התרחשה מכתובת IP של לקוח קומקאסט, שידוע כחבר של אולברייט. כתב האישום אינו מפרט מיהו אותו חבר, אך אנדי גרינברג מפורבס מנחש שמדובר בפינל עליו ספרנו קודם, אצלו אולברייט התגורר בחודשים הראשונים אחרי הגעתו לסן פרנסיסקו.

הטבעת מתהדקת

מפעיל דרך המשי, או אולברייט, אם אתם מאמינים בכך, שמר על זהירות רבה בדרך לניהול האתר. בדיעבד, הזהירות הזו היתה בעוכריו ופעלה כחרב פיפיות נגדו:

הכניסה למימשק הניהול של האתר היתה מוגבלת לכתובת IP אחת מסוימת, כלומר רק ממנה נתן לנהל את האתר.

זה טוב, אבל אם עולים על אותה כתובת, זה גם מפליל, כי זה אומר שאתה מנהל את האתר... חקירה העלתה כי הכתובת הולכת לרשת וירטואלית - VPN. עכשיו, רשת וירטואלית זה דבר נפלא ויודע להסתיר אותך נהדר, אלא אם החברה שספקה לך את הרשת הוירטואלית לא מסגירה אותך...

היא כן.

אותה חברה, ששמה לא מוזכר בכתב האישום, סיפקה ל-FBI את כתובת ה-IP האמיתית שעומדת מאחורי הרשת הוירטואלית. אותה כתובת מוליכה לקפה אינטרנט ברחוב לגונה בסן פרנסיסקו, אותו קפה אינטרנט שאולברייט פעל ממנו.



[המסמכים המזויפים של אולברייט. מתוך סופט-פדיה]

ביולי 2013, בבדיקת מכס שגריתית, נתפסו מסמכים מזויפים שנשלחו בדואר לאולברייט. סוכני מכס והגירה נשלחו לביתו והראו לו את המסמכים המזויפים, כדי לחקור את הקשר שלו אליהם. הוא הציג לפניהם את מסמכיו האמיתיים והתוודה בפניהם שהוא משתמש בשם אחר אל מול שותפיו לדירה. בסדר, כולה קרא לעצמו ג'וש.

מה שמענין יותר ומחזק את הקשר בין אולברייט ל-DPR, מפעיל דרך המשי הוא, שמעט זמן קודם לכן אותו משתמש גילה ענין בהשגת מסמכים מזויפים ורכש אותם מאחד הסוחרים שלו באתר. הוא גם הסביר, שעליו להגדיל את כמות השרתים שברשותו ולעשות זאת שלא באמצעות שמו האמיתי. כאשר סוכני ההגירה פגשו את אולברייט עם המסמכים המזויפים, הפטפטן חסר הניסיון אף הודה בפניהם שניתן לרכוש סמים באמצעות רשת TOR. סתם, לא מרשיע כשלעצמו, אבל די אידיטי לומר זאת.

בערך באותה תקופה אולברייט התענין, עם המייל האמיתי שלו, [בפורום תכנתים מוכר](http://www.DigitalWhisper.co.il), בדרך להתחבר ל-TOR באמצעות קוד פתוח. הוא התלונן שאינו מצליח וביקש עזרה. נכון, גם זה לא מרשיע כשלעצמו. לכן קראתי לראש הפרק הזה "הטבעת מתהדקת".

עלייתו ונפילתו של האתר Silk Road

www.DigitalWhisper.co.il

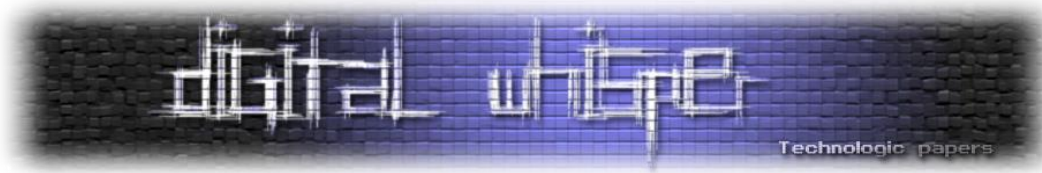
ואז קרה עוד אירוע נסיבתי, שהראה שה-FBI יושבים לו באמת על הוריד ומתעדים ומשוים כל פעולה שלו:

ראשית, הגישה ל-TOR מדרך המשי נעשית באותה שיטה בה היא תוארה בפוסט בו DPR ביקש עזרה. שנית, חודשים מספר לאחר הגשת אותה שאילתה בפורום התכנתים, DPR החליף את פרטיו והכניס את המייל הבלתי קיים frosty.com בתור המייל שלו. זה עוד מילא, אנשים רבים עושים זאת. אבל השימוש ב-frosty@frosty נעשה בתוך דרך המשי עצמה כדי להתחבר באמצעות חיבור מאובטח מוצפן (SSH). חיבור כזה נושא תמיד מבנה קבוע, הכולל בתוכו את שם המחשב המתחבר ב-SSH ואחרי סימן ה-@, שם השרת אליו הוא מתחבר. אולברייטס היה יכול לטעון שהכל נכון, אבל הוא אינו המשתמש מהפורום. דא עקא, הוא חיבר את עצמו לפורום ול-Frosty, בכך שהשתמש במייל האמיתי שלו חודשים לפני כן עבור אותו חשבון.

כן, יכול להיות שכל זה הוא מקריות מדהימה וצירוף נסיבתי שיכול לשלוח אדם חף מפשע לכלא. ייתכן גם שמישהו, ערום ומתוחכם, גנב את זהותו של אולברייטס ופועל בשמו מקפה אינטרנט ליד מקום מגוריו של הפיסיקאי המחונן. יכול להיות. נכון לזמן כתיבת שורות אלה, אולברייטס [עוד לא הורשע](#).



[שלא תחשבו לרגע שזה הסוף של דארקנט. מתוך ויקיפדיה]



פרולוג ותהיות

אולברייכט לא נתפס על חם. שימו לב כי כל כתב האישום הוא נסיבתי ובנוי כמו תשבץ, אבל בשום מקום לא נתפס עם מחשב פתוח, בעודו מפעיל את האתר, לפחות על פי כתב האישום.

אולברייכט כאמור (מרץ 2014) כופר בכל ההאשמות ומענין אם הוא יורשע על בסיס כל אלה.

סביר להניח שכתב האישום לא מגלה לנו את הכל. אחרי הכל, הוא פתוח לציבור (משם שאבתי את המידע לרשומה הזו) ומן הסתם נותח על ידי אנשים נוספים. השמועה בפורומים טוענת שה-FBI ניצל פירצה ב-TOR. הפריצה תוקנה אחרי לכידתו, אבל מי יתקע לידנו שאין עוד כאלה?

על פי כתב האישום, הכל החל בזה שמשתמש בשם altoid המליץ על דרך המשי. הקשירה של המשתמש הזה למייל הפרטי של אולברייכט נעשתה די בקלות ומשם הכל זרם.

אבל איך החלה ההתמקדות באותה הודעה קצרה של אולברייכט ב-Shroomery? הרי זה האם-אמא של המחט בערימת השחת: בכל יום [מתפרסמות](#) מאות אם לא אלפי סקירות והמלצות על אתרי דוארקנט אמניים יותר או פחות ב-reddit. ההתמקדות בהודעה הבודדת של אולברייכט נראית הגיונית למתבונן מן הצד, אבל לחלוטין לא סבירה כאשר חושבים על כמות המידע הדומה שרצה ברשת בכל רגע נתון. זה מגביר את החשד שכתב האישום מסתיר מקורות מידע נוספים להגעה לאולברייכט.

מהם אותם מקורות מידע?

- סוכנים שהצליחו להתקרב לאולברייכט דרך התחזות לסוחרים ומנהלי משנה באתר?
- מעקב פיזי אחרי שרתים?
- פרצות ו-backdoors במערכות המבטיחות אנונימיות לכאורה?
- כל התשובות נכונות?

כנראה שאף פעם לא נדע...

על המחבר

יורם שפר, יוצר סרטי תעודה מאז 1997 לערוצים בישראל ובעולם, יוצר סרט על הדארקנט ומחפש אנשים שיספרו על חווית הדארקנט שלהם. סודיות, במקרה הצורך, מובטחת. פרטים נוספים באתר הסרט:

<http://www.darknetmovie.net/>