# הצד האפל של האינטרנט

## בקצהו של עולם האינטרנט נמצא עולם אפל של מלחמות, פשע וריגול – רק צריך לדעת היכן לחפש

**מאת ד"ר גיל דוד**

אילוסטרציה: Shutterstock

את האימרות הנפוצות בעולם האינטרנט היא שאם משהו לא מופיע בתוצאות החיפוש של גוגל הוא לא באמת קיים, אולם המציאות שונה לחלוטין. מנועי החיפוש כמו גוגל ודומיו מצליחים לגרד רק את קצה קצהו של עולם האינטרנט, כאשר בפועל ישנו ב"בטן" האינטרנט עושר עצום של תכנים מעניינים ומרתקים, וגם עולם חבוי ואפל של תככים, מלחמות, פשע וריגול.

מקובל לחלק את עולם האינטרנט למספר שכבות. השכבה העליונה, המוכרת לכולנו, מכונה בשם ה–Surface Web. השכבות התחתונות מכונות בשם Deep Web והן מרכיבות את הצד האפל של האינטרנט.

שכבת ה–Surface Web המכונה גם בשם Clearnet, מכילה את כל הדפים אליהם ניתן להגיע באמצעות מנועי החיפוש הנפוצים כמו Google, Yahoo ו–Bing. מנועים אלה סורקים את רשת האינטרנט, וכך הם מציירים מעין מפה או אינדקס של כל האתרים והדפים אליהם הם הגיעו. שיטה זו מאפשרת להם לכסות את כל עולם האינטרנט הנגיש למנועי החיפוש ואוסף כל הדפים האלה מהווה את השכבה הראשונה באינטרנט.

לפי מספר הערכות, שכבת ה–Surface Web מכילה כמה עשרות עד מאות טרה של מידע שנמצא בעשרות מיליארדי דפי אינטרנט אליהם ניתן להגיע באמצעות מנועי החיפוש. שכבה זו מכילה רק אחוז קטן מהמידע הקיים בעולם האינטרנט – על מנת להגיע אל שאר המידע יש לצלול מתחת ל–Surface Web ולהיכנס אל הצד האפל של האינטרנט.

שכבת ה–Deep Web המכונה גם בשמות Invisible Web ו–Hidden Web, מכילה את כל החלקים באינטרנט שאינם נגישים למנועי החיפוש של השכבה הראשונה. לפי הערכות שונות, שכבה זו מכילה כמה עשרות אלפיטרה של מידע, הנמצא במאות מיליארדי דפי אינטרנט. כלומר, הצד האפל של האינטרנט גדול באלפי אחוזים מה–Surface Web – כאשר קצב גדילתו גדול בהרבה.

מקובל לחלק את שכבת ה–Deep Web – לשתי שכבות משנה:

Deep Web Layer 1 מהווה את החלק המרכזי והגדול ביותר, ומורכבת מסוגים שונים של אתרים, דפים ומידע. סוג אחד של דפים בשכבה זו הוא Unlisted pages. כלומר, דפים שאינם רשומים באינדקסים של מנועי החיפוש.

אחת הסיבות לכך שמידע לא נרשם יכולה להיות בקשה מפורשת של בעל העמוד. לדוגמא, סרטים מסויימים ביוטיוב שהגולש שהעלה אותם לאתר וביקש שהם לא יופיעו במנועי החיפוש, כך שרק מי שיש לו לינק ישיר אליהם יוכל לגשת אליהם. במקרה זה, יוטיוב תייצר לינק עבור



הסירטון, ובעליו יכול לשלוח למכריו מייל המכיל את הלינק, אולם רק מי שניגש דרך הלינק יוכל להגיע אליו.

הסוג השני של הדפים בשכבת העומק הראשונה הם כאלה שלמנועי החיפוש אין הרשאה להגיע אליהם. דפים אלה מכילים תוכן שרק משתמשים מסויימים יכולים לראותו, לאחר שהרשאותיהם אומתו אל מול האתר. למשל, חשבונות הג'ימייל או חשבונות הבנק של המשתמשים מוגנים בסיסמא, ורק בעל הסיסמא יכול להגיע אל התוכן שלהם.

הפוטנציאל הטמון בחיפוש ב–Deep Web Layer 1 הוא אדיר. אוקיאנוס המידע מכיל תוכן עצום שרוב הגולשים אינם חשופים אליו, ולכן מי שישכיל "לחפור" במידע הטמון שם יוכל להשיג יתרון משמעותי, למשל במגזר העיסקי, המודיעיני וכדומה.

## הרשת האנונימית

בתחתית הצד האפל של האינטרנט נמצאת השכבה התחתונה ביותר של עולם האינטרנט, שהינה Deep Web Layer 2 של ה–Deep Web. שכבה זו, המכונה גם בשם, או הרשת האנונימית, הינה חלק קטן ביותר מה–Deep Web אך היא מהווה מקור רב ערך עבור ארגוני מודיעין, פשע וטרור.

בניגוד לשכבות העליונות של האינטרנט, בהן ניתן ברוב המקרים לקשר את האתרים והתכנים שבהם לבעליהם, ואת הגולשים הווירטואליים למשתמשים האמיתיים שמאחוריהם, בשכבה זו האנונימיות הינה ערך עליון. בעלי האתרים והגולשים בהם הם אנונימיים לחלוטין, ואפילו התשלומים הווירטואליים המתבצעים בשכבה זו הינם באמצעות מטבעות וירטואלים אנונימיים. כפי שניתן להעריך, במקום בו יש אנונימיות כמעט מוחלטת, ניתן למצוא מגוון משתמשים. החל מגורמי ממשלה, ביטחון וביון, דרך האקרים, מרגלים, מהפכנים וחוקרים ועד לסוחרי סמים, חוטפים, מתנקשים ואנשי מאפיה.

חשוב להבהיר, שהכניסה ל–Anonymous web מיועדת רק לאנשים שבקיאים ברזי האינטרנט, מבינים לעומק את הסכנות הטמונות בו, שולטים לחלוטין בתחומים של אנונימיות, התקפות ואבטחה ברשת, ומוכנים לקחת את הסיכונים הרבים שנמצאים כמעט בכל פינה של הרשת האנונימית.

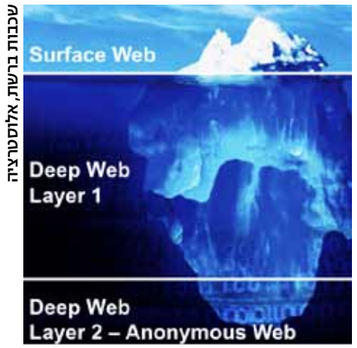
הנחת המוצא של הגולש הנכנס לרשת האנונימית צריכה להיות שבכל שלב הוא עלול להיות מותקף ללא ידיעתו על ידי מיטב ההאקרים והתוקפים המשתמשים בנשק סייבר מתוחכם ומתקדם. על כן, את הכניסה לרשת האנונימית יש לבצע מתוך מחשב ייעודי או מחשב וירטואלי, המנותק לחלוטין מכל רשת מחשבים, ומשמש אך ורק לצורך זה ולא לשום פעילות אחרת של הגולש. כמו כן, מומלץ לנתק את כל האמצעים החיצוניים המחוברים למחשב כגון GPS, BT, מיקרופון ומצלמת רשת.

לאחר שנכנסים לרשת האנונימית, מתגלה בפני הגולש עולם שלם, שבמבט ראשון נראה דומה לעולם האינטרנט המוכר, אך בפועל חוקי המשחק בו שונים לחלוטין. בחלק זה של העולם אין צנזורה, אין כללים, אין אכיפה של החוק,

> "ארגוני מודיעין שישכילו לחקור ולנטר את הרשת האנונימית, יוכלו למצוא שם 'אוצרות', החל ממסמכים מסווגים ביותר שהודלפו מאירגונים ביטחוניים וממשלתיים בעולם, דרך התארגנויות של תאי טרור ועד לסחר בנשק סייבר מתוחכם ומתקדם"

ולמעשה הכל מותר בו, אפילו אם הוא בלתי חוקי בעליל בזכות האנונימיות וחופש הביטוי המוחלט בשכבה זו, היא מהווה באופן טבעי קרקע פוריה להפצה של מידע מודיעיני או ממשלתי רגיש שהודלף באופן חשאי, אם על ידי האקרים, עובדים ממורמרים או חושפי שחיתויות. למשל, אחת הסברות היא שמאות המסמכים האמריקאיים הסודיים הנוגעים למתקן המעצר בגואנטנמו שפורסמו על ידי ויקיליקס הגייעו מה–Deep Web, ולמעשה האתר העלה אותם מתחתית האינטרנט אל ה–Surface Web. בעוד שתכנים הנמצאים ב–WikiLeaks אפשר לחסום או להוריד מהרשת, את הרשת האנונימית חסינים מפני צנזורה מכל סוג שהוא.

חשוב לציין שחלק מהמידע בשכבה זו מושתל באופן מכוון על ידי גורמים ממשלתיים, ומהווה פיתיון עבור פושעים למיניהם. המטרה היא שאותם פושעים ייתפסו ברשת עת הם ניגשים למידע הלא חוקי, יחשפו את זהותם וייעצרו על ידי גורמי האכיפה.




שכבות ברשת, אלוסטרציה

## ניטור ותקיפה

הרשת האנונימית מהווה קרקע פורייה למגוון פעילויות ביטחוניות בתחום הסייבר, הן מהצד ההגנתי והן מהצד ההתקפי. רשת זו מציבה אתגרים משמעותיים בפני הגופים הבטחוניים המעוניינים להשתמש בה לצרכיהם.

למשל, ישנה חשיבות רבה לניטור שוטף של אתרי ה–Deep Web האנונימיים, על מנת לאתר מבעוד מועד פעילויות לא חוקיות של טרוריסטים, פושעים והאקרים, אולם אותם כלי ניטור קונבנציונליים בהם משתמשים ב–Surface web אינם תקפים בתחתית העמוקה של האינטרנט.

ארגוני מודיעין שישכילו לחקור ולנטר את הרשת האנונימית, יוכלו למצוא שם "אוצרות", החל ממסמכים מסווגים ביותר שהודלפו מאירגונים ביטחוניים וממשלתיים בעולם, דרך התארגנויות של תאי טרור ועד לסחר בנשק סייבר מתוחכם ומתקדם. ברוב המקרים, מידע זה קיים אך ורק בשכבה הזאת של ה–Deep Web ולא בשכבות העליונות של האינטרנט.

לא מן הנמנע שבעתיד תעבור חלק מזירת הלחימה של הסייבר אל הרשת האנונימית, כאשר התקיפות תתבצענה מתוך הרשת האנונימית אל ה–Surface web וכן אתרי שליטה ובקרה של Botnets יסתתרו במעמקי הרשת האנונימית. במקרים אלה, זיהוי מקור התקיפה וחסימתו יהוו אתגר מורכב עבור מערכי ההגנה.

ד"ר גיל דוד הוא הבעלים והמנכ"ל של חברת Brainstorm Private Consulting לייעוץ בעולם הסייבר והמודיעין. הוא משמש כפרופסור אורח באוניברסיטה באירופה ומשתף פעולה עם גופים ביטחוניים, מסחריים ואקדמיים בארץ ובעולם. www.gostorm.net