הרשת האפלה - מדריך OpSec למשתמש

מאת שי ממן

הקדמה

במאמר הבא אנחנו נצלול אל עולם שלם של אנונימיות, פרטיות ואבטחה ברשת האינטרנט. בעולם שבו כולנו מנוטרים ופרטיות היא מילה גסה, ישנם אנשים ברחבי העולם שמצאו את הפתרון האידיאלי. כמו רובנו, נעדיף לשמור על הפרטיות שלנו תחת מעטה חסוי אך יש כאלו שגם חשובה להם האנונימיות עצמה.

אנשים ברחבי העולם נמצאים במצב שבו הם צריכים להסתיר את זהותם ואת פעילותם הרשתית מסיבות מגוונות שיכולות לנוע מאובססיביות לצורך בלהיות מחוץ לרדאר, למרגלים, אזרחי מדינות טוטליטריות חשוכות ואפילו ארגוני פשיעה. האנשים האלו משתמשים בטכנולוגיה של ניתוב הבצל (או בשמו המקורי: Onion Routing), שמאפשר יתרונות שרוב הגולשים אפילו לא יודעים שאפשר לקבל ובעזרתה להיעלם אל עולם הצללים.

פרטיות VS אנונימיות

בעולם שלנו, אנשים מסתובבים בתחושה שהם פרטיים, שאף אחד לא יודע מה הם עושים אם הם לא ישתפו את המידע הזה וגם ככה שכל עוד הם לא עושים משהו לא חוקי, אין להם מה להסתיר. זו תחושה מוטעית, כי בעולם הטכנולוגי שבו אנחנו חיים, אנחנו מנוטרים בכל שניה שעוברת. כל בקשה שלנו באינטרנט מנוטרת ונרשמת, אנחנו מצולמים ברחוב, מאגרי המידע של רשויות עמוסים במידע עלינו ובעצם אנחנו לא זוכים לפרטיות כמו שאנחנו חושבים.

- **פרטיות** - אף אחד לא צריך לדעת מה אני עושה, המעשים שלי שייכים רק לי. לדוגמא, אם אני אוהב לשיר במקלחת, זו בחירה שלי, וכל עוד אני לא משתף אנשים במידע הזה אז הוא ישאר פרטי.
- **אנונימיות** - המעשה שאבצע לא חייב להיות פרטי אך אף אחד לא יוכל להשתמש בפרטים המזהים שלי על מנת לקשור את הזהות שלי לאירוע. לדוגמא, שודד בנק שנכנס לסניף מלא באנשים ומצלמות ומבצע שוד אך הוא מכסה את הפנים שלו עם כובע גרב.

- **אבטחה** - מצב שבו המעשים שלי פרטיים ככל הניתן אבל אני גם מקפיד על כללים ומטשטש כל קשר של פרטי הזהות שלי אל המעשים שלי ובכך יוצר זהות הרבה יותר מאובטחת מפני פגיעה פוטנציאלית.

חלוקת הרשתות הקיימת

האינטרנט כפי שאנחנו מכירים אותו, מורכב מ-3 שכבות בסך הכל:

1. **הרשת הנקיה** - מדובר באינטרנטו שכולנו מכירים ומשתמשים בו. שלל מנועי חיפוש כמו גוגל, בינג ויאהו, שיודעים לאנדקס אתרים חדשים עם סיומות שונות, לדוגמא il, com או gov.

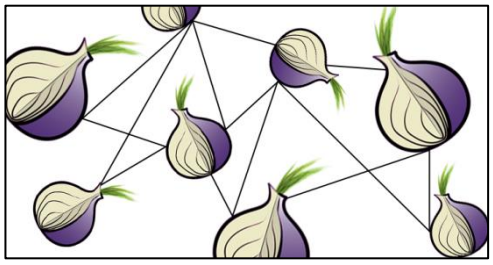
2. **הרשת העמוקה** - מדובר במעין שלב ביניים, שעדיין מתקיים ברשת הנקיה אך הוא לא נגיש לכל המבקש. הוא ידרוש אישור גישה ספציפי, בדרך כלל עם צורך בהזדהות עם שם משתמש וסיסמא, וכולל בתוכו אתרים פנימיים של חברות, מחקרים מוגנים בסיסמא ואפילו אתרים ממשלתיים פנימיים.

3. **הרשת האפלה** - פלטפורמה הפועלת על בסיס טכנולוגיית ניתוב שנקראת "ניתוב הבצל", המאפשרת אנונימיות מוגברת ומקשה על זיהוי המשתמש בפלטפורמה, מה שנותן לגיטימציה למשתמשים שרוצים לבצע פעולות בלתי חוקיות.

מה היא הרשת האפלה

מדובר ב-World Wide Web, פלטפורמה ברשת הדורשת גישה ייחודית ע"י תוכנה ספציפית, קונפיגורציה או אישור מיוחד. הרשת האפלה מאגדת בתוכה חלק קטן מה-Deep Web, ז"א החלק ברשת שלא ממופה ע"י מנועי חיפוש רגילים ומוכרים כמו גוגל.

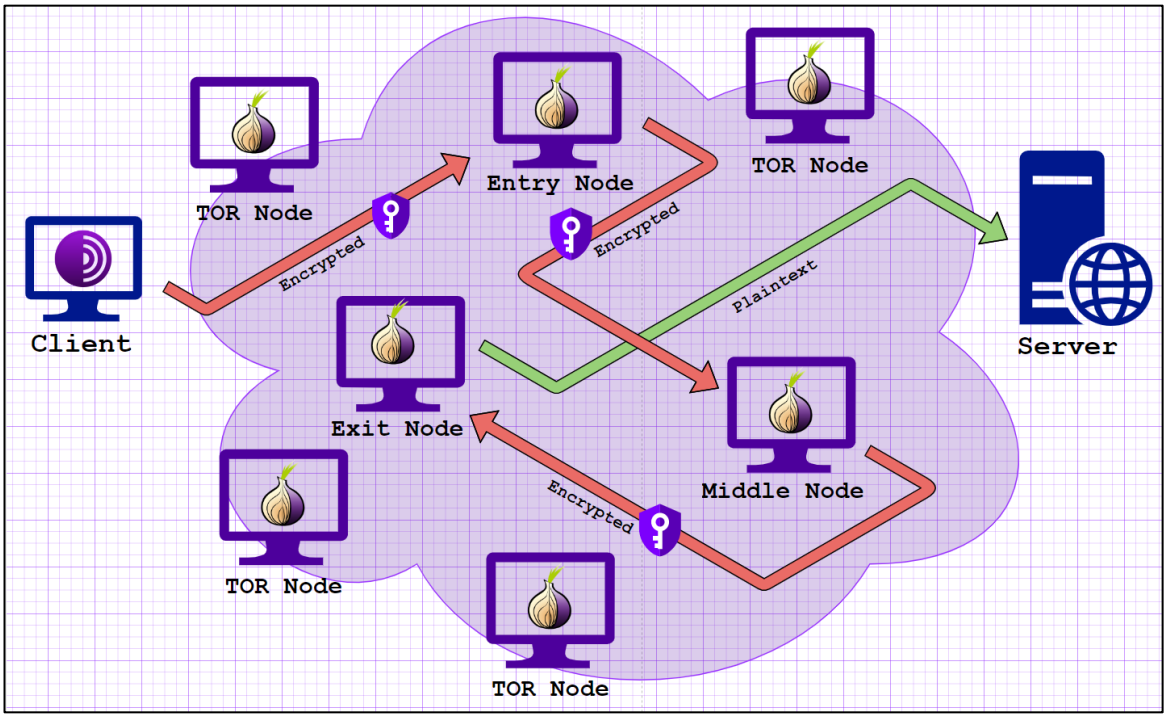
לחיפושים ברשת הזו יש צורך להשתמש בתוכנה ספציפית שנקראת שנקראת TOR, ראשי תיבות של The Onion Router והטכנולוגיה שעליה היא מתבססת נקראת Onion Routing. ה-Onion Routing, כשמו כן הוא מורכב משכבות שונות שמוסיפות בו הגנה. טכנולוגיית הניתוב הזו הומצאה בשנת 1995 במעבדות המחקר של חיל הים האמריקאי על מנת להגן על העברת מודיעין בחיל, ובשנת 1996 עברה להמשך פיתוח בסוכנות האמריקאית Darpa עד שבשנת 2006 פורסמה כפרויקט קוד חופשי של איגוד ללא מטרות רווח למען הפרטיות והאנונימיות באינטרנט. הניתוב הזה הוא טכניקה שמאפשרת תקשורת חסויה מאחר והודעות ברשת עוברות עטיפה (Encapsulation) ע"י כמה שכבות של הצפנה. המידע המוצפן הזה מועבר דרך צמתים שונים ורנדומליים ברשת (כל אחד יכול להקים שרת TOR בבית שלו, ובכל פניית רשת יש צומת שונה רנדומלית שנבחרת), הצומת הזו נקראת גם Onion Router.



[מקור: dogsbody.com]

הנתונים המוצפנים האלו עוברים דרך צמתי רשת וכל אחד מהם מבצע "קילוף" של שכבה אחת וחושף את היעד הבא של המידע וכאשר השכבה האחרונה מפוענחת, ההודעה מגיעה אל היעד האמיתי שלה.

בצורה הזו השולח נשאר מוצפן (מאחר וכל צומת "מכירה" רק את הצומת שקדמה לה ואת הצומת הבאה, מה שיוצר מצב שבו אנחנו בתור השולחים "חשופים" רק כאשר נצא בפעם הראשונה אל היעד הראשון וכאשר נגיע אל היעד הסופי שלנו. פתרון לבעיה הזו הוא גלישה בפרוטוקול מוצפן בלבד (HTTPS) ושילוב של שימוש בשרתי פרוקסי או VPN לצורך הגברת האנונימיות. המכניקה של ניתוב TOR נותנת יתרון אדיר, בכך שהיא מעבירה את הגולש דרך כמה שרתי Proxy, מה שמצמצם את שובל הראיות שיכול להוביל אל הגולש האמיתי.



דפדפן TOR וחבריו

דפדפן TOR פועל כולו על טכנולוגיית ניתוב הבצל ויודע לאנדקס סיומות onion המעידות על האתר כאחד שיודע לקבל תקשורת ב-TOR בלבד. כל חבילות הרשת עוברות דרך שלושה צמתים רנדומליים ברחבי העולם, וכל צומת מכירה רק את הקודמת לה ואת הבאה לה. הדפדפן ניתן להורדה באתר הרשמי של הפרויקט, שנקרא Project TOR ובו נוכל למצוא מגוון עצום של תוכן, משיתוף קבצים, לדיונים פוליטיים, שירותים פליליים ושנויים במחלוקת, הדלפות של מסמכים סודיים ואפילו פורומים עמוקים של מתנגדי משטר ברחבי העולם. דפדפן TOR הוא אמנם הכי מוכר אך ממש לא היחיד. פלטפורמה נוספת שקיימת נקראת ZeroNet והיא מספקת שירותי אחסון ברשת מבוזרת ("עמית לעמית"). כל בעל אתר בפלטפורמה משמש כ-Host בלעדי ולכן כמעט בלתי אפשרי לבצע מגבלות על תוכן בפלטפורמה.

פלטפורמת I2P קמה על מנת לספק מתחרה לדפדפן TOR, ולמרות שהיא מבצעת את אותה הפעולה שניתן להשיג בשימוש ב-TOR, היא פחות מוכרת בקרב חוקרים ורשויות החוק בכללי ולכן הניטור בה חלש יותר, מה שמגביר את תחושת הפרטיות של המשתמשים. גישה לפלטפורמה דורשת הורדה של תוכנת I2P שתפעל ברקע, ובזמן שימוש רגיל בדפדפן, כל חבילות המידע ינותבו דרך צמתי TOR בלבד.

עבודה נכונה בסביבת TOR

בסביבת מחקר יש צורך לשמור על אנונימיות גבוהה על מנת לשמר את סיפור הכיסוי שלנו כחוקרים, למזער את הסיכויים לנתב אלינו את חבילות המידע ולקשר אותנו לביצוע פעולות שונות שנבצע כחלק מהמחקר שלנו. במערכת ההפעלה של רוב המשתמשים, שלרוב תהיה מערכת ההפעלה Windows, נשמרים לוגים כדרך דיפולטיבית.

הלוגים האלו נשמרים ברקע, לרוב ללא ידיעת המשתמש, ומעידים על פעולות שונות המתבצעות במערכת ההפעלה. יתרה מזאת, ישנן תוכנות צד שלישי במחשב שיכולות להיות לא מעודכנות (דפדפן, אפליקציות שונות...), וגם אם כן, הן מדליפות מידע שנאסף כחלק מחווית המשתמש (אפשר לראות בדיוק איזה מידע בהסכם המשתמש שכולנו חותמים עליו לפני תחילת השימוש). בנוסף, ברוב המקרים שמורים במחשב מסמכים אישיים שלנו (תמונות אישיות, מסמכים עם פרטים אישיים) ובכללי פרטים שיכולים להסגיר את הזהות האמיתית שלנו במידה ותוכנה זדונית תגיע אל המחשב שלנו כחלק משיטוט באזורים בעייתיים ברשת האפלה ובכללי בסביבת מחקר שיכולה להיות עוינת. בשביל לפתור את הבעיה הזו, יש צורך להשתמש בתוכנת וירטואליזציה עם שתי אפשרויות של מערכות הפעלה:

מערכת ההפעלה Tails:

מדובר בהפצת לינוקס מסוג דביאן, מותקנת בדרך כלל על USB על מנת שנוכל להעלות אותה ע"י boot בכל פעם שנרצה ונצטרך. כל המידע שנשלח בתוך מערכת ההפעלה הזו עובר על TOR בלבד ללא כל צורך של הגדרה מצד המשתמש. המערכת משתמשת רק בזיכרון ה-RAM (זיכרון נדיף), מה שמאפשר את הפעולה של מחיקת כל זכר מהמידע שהשתמשנו בו וכל לוג שנשמר במערכת בכל פעם שמערכת ההפעלה תיכבה.

[מקור: tails.boum.org]

הפעולה הזו תגן על משתמש הקצה מכל חקירה פורנזית שיכולה להתבצע על מערכת ההפעלה. יש אפשרות להתקין את מערכת ההפעלה Tails באופן לוקאלי על המחשב אך הדבר פוגע ביתרון שהמערכת מספקת מאחר ולוגים ישמרו על תוכנת הוירטואליזציה ולא נוכל ליהנות מכל יתרונות השימוש במערכת.

מערכת ההפעלה Qubes:

הבעיה במערכות הפעלה אחרות היא שכל המידע נמצא במקום אחד, משמע אם בדרך כלשהי תוכנה זדונית מגיעה למחשב, הוא חשוף לחלוטין. במערכת ההפעלה Qubes, יש שימוש בוירטואליזציה שמאפשרת ליצור סביבות נפרדות בתוך מערכת ההפעלה, ולסביבות האלו קוראים דומיינים. בכל דומיין יש שימוש במערכת קבצים נפרדת וזיכרון נפרד לחלוטין, וכל דומיין ישמש לפעילות שונה (שמירת מסמכים, גלישה, עבודה, פנאי...).

[מקור: qubes-os.org]

בצורה הזו, גם אם דומיין אחד נחשף, הוא מבודד לחלוטין משאר הדומיינים וכמובן ממערכת ההפעלה הראשית של המחשב שלנו, וכל תוכנה זדונית שתמצא בדומיין תהיה מבודדת לחלוטין לדומיין בלבד.

עקרונות OpSec לעבודה ברשת האפלה

OpSec הוא ראשי תיבות של Operational Security, מונח שמגיע אלינו מצבא ארה"ב ומתאר מצב שבו כוח המשימה מנסה לחשוף כמה שפחות מידע רלוונטי על פעולותיו בשביל לצמצם את הסיכויים שיחשף ע"י היריב. בעזרת שמירה על כללי OpSec נכונים, נוכל לצמצם את הסיכויים להיחשף מאחורי רשת TOR.

בתור חוקרים שנמצאים בסביבת ה-Darknet, מן הסתם שנחשף לתכנים פליליים, ובמיוחד במקרים שבהם נדרש להשתמש בטכניקות Humint או Webint ו-Osint שונות (למשל שימוש ב-Web Crawlers, תגובות על פוסטים בפורומים פליליים, תקשורת עם אנשי מפתח בקבוצות פשע וכו).

יש חובה להשתמש בחשבון שנועד למטרות האלו בלבד, שהוקם עם זהות בדויה שסיפור הרקע שלה נבנה מבעוד מועד (שם מלא, פרטים מזהים, כינוי, גיל, מיקום גאוגרפי ופרטים מהימנים כתוספות לחשבון [פוסטים, היכרות עם אנשים בסביבה שבה אנחנו נמצאים, תמונות רלוונטיות]). החשבונות האלו צריכים להיות מוקמים בסביבה נפרדת מהמחשב האמיתי שלנו, לעולם לא עם מכשירים המקושרים אלינו (טלפון אישי מחוץ לתחום, סים חד פעמי שנרכש במזומן הוא תחליף לגיטימי) ותמיד לבדל כל חשבון בפני עצמו, משמע להתייחס אליו כאילו הוא החשבון האמיתי שלנו והיחיד שלנו. **יש חובה להשתמש ב-VPN בזמן הקמת החשבונות ובזמן כל שימוש בסביבה הזו.**

בחירת VPN עדיפה תהיה ספקית שלא שומרת לוגים (למרות שאני בספק שיש אחת כזו) אז אפשר לבחור בספקית שממוקמת במדינה שבה אין שיתוף פעולה עם רשויות החוק (למשל רוסיה) וצורת התשלום שלנו לספקית תהיה בקריפטו בלבד, עם חשבון מייל שהוקם במיוחד למטרה הזו ועם זהות שהוקמה במיוחד למטרה הזו (אין למסור פרטים מזהים אמיתיים לעולם). אם ישנה אפשרות להתחבר ב-VPN Over TOR ע"י הספקית זו תהיה האופציה המועדפת. עבודה נקיה תהיה ע"י מערכות וירטואליזציה הנפרדות מסביבת המחשב האמיתי שלנו (Tails או Qubes).

בניית חשבונות Sock Puppets

חשבון sock puppet היא זהות אינטרנטית בדויה שנועדה למטרות הונאה או הסוואה. בדרך כלל מדובר במהלך שיעשה ע"י Bad Actor מכל סוג שהוא אך לא רק, וגם לחוקרים בעצמם יש זהויות בדויות שישתמשו בהן על מנת להיות חלק מהקהילה ועל מנת להסוות את עצמם כאחד השותפים, וכמובן להגן על הזהות האישית והביטחון של אותו חוקר. לעולם לא נשתמש בפרטים אישיים אמיתיים שלנו או בכל חשבון קיים ואישי שלנו על מנת לבצע כל מהלך של חקירה.

כיום, אתרים רבים מחזיקים במנגנונים ושיטות לזיהוי של חשבונות כאלו וחוסמים אותם באופן מיידי ולכן ככל שהחשבון יהיה "עשיר" יותר, מלא בתכנים ופעילות כללית, האמינות שלו תגבר. מומלץ מאוד להשתמש בתוכנה לניהול סיסמאות ושמות משתמש בשביל להיות במעקב רציף אחרי כל החשבונות שניצור.

ליצור חשבון שכזה יכול לקחת לא מעט זמן ומשאבים, ולכן ישנם שירותים שעוזרים לג'נרט חשבונות כאלו עם מידע מזויף בתוכן, לדוגמא:

- fakeperson.com
- www.elfqrin.com/fakeid.php

כמובן שלכל זהות שניצור, נצטרך ליצור חשבונות קיימים ברשתות החברתיות, ולכן מומלץ מאוד להשתמש גם בתמונות רלוונטיות. יש אפשרות להשתמש בתמונות קיימות של אנשים אמיתיים אך שיטות של Photo Reverse Lookups יכולות לחשוף את הזהות המזויפת ו-"לשרוף" את החוקר. נוכל להשתמש באתרים הבאים על מנת לג'נרט תמונות:

- thispersondoesnotexist.com
- Gallery of AI Generated faces

יצירת חשבון מייל היא השלב הראשון והבסיסי לפני הקמת חשבון ברשת חברתית כזו או אחרת. חובה ליצור את חשבון המייל על אותה הזהות שנקים בשמה את חשבון הרשת החברתית (חשבון מייל בספק Clear Web):

- protonmail.com
- gmx.com
- yandex.mail

לעיתים יהיה צורך להשתמש ב-Burner Phones (טלפונים חד פעמיים) על מנת להירשם לאתרים ואפליקציות שדורשות מספרי טלפון. הסיבה שבגינה זה יכול לקרות היא שהאתר מנסה למנוע הקמת חשבונות מזויפים ע"י שליחה של קוד חד פעמי לטלפון שישמש כאמצעי הזדהות.

בשביל לקנות SIM זמני או אפילו טלפון חד פעמי, מומלץ לשלם במזומן בלבד מבלי למסור אף פרט מזהה. לאלו שירצו להרחיק לכת עוד יותר, כדאי להמתין עם הטלפון בין חודש לחודשיים עד לתחילת השימוש בו. יש גם אפשרות לשימוש בסימולטור טלפון (אפליקציה להורדה בתשלום). מומלץ לשלם בקריפטו בלבד ולא לחבר את האשראי האישי שלנו בשום אופן מאחר ופעולה שכזו קושרת אותנו באופן ישיר למספר, ומשם לחשבון שהוקם על אותו מספר ומסכנת את הזהות שיצרנו.

רוב החנויות שמוכרות טלפונים חד פעמיים או SIM Cards יחזיקו מצלמות במעגל סגור, אך המידע נשמר לתקופת זמן של עד כ-60 ימים בדרך כלל ולכן מומלץ להמתין את פרק הזמן הזה על מנת שלא תהיה כל דרך לקשר את הרכישה אלינו. חשוב להבין שבכל הפעלה של הטלפון, קישור המיקום הנוכחי שלנו באותו רגע יווצר עם המכשיר עצמו ולכן אין לחבר אותו לרשת הביתית, משרדית או כל רשת שלא נרצה להיות מזוהים איתה דרך אותו מכשיר. בשביל למנוע כל תדר מהמכשיר החוצה בזמנים שלא נרצה, נוכל להשתמש בכלוב פאראדיי (מתקן המונע מאותות חשמליים לחדור לתוכו ומבודד כל אות אפשרי). אם נכפה עלינו להשתמש בכרטיס אשראי לרכישות ספציפיות, אפשר להשתמש באתר privacy.com על מנת ליצור כרטיסי אשראי וירטואליים (כמובן לאחר שצורת התשלום שלנו תאומת).

תהליך יצירת חשבון Sock Puppet

1. שימוש ברשת WIFI ציבורית, ללא שימוש ב-VPN (רוב האתרים מזהים את זה כחשוד)
2. בחירת הרשת החברתית שנרצה לפתוח בה פרופיל (למשל Facebook)
3. שימוש במספר וירטואלי שרכשנו / מספר הטלפון האמיתי שלנו על מנת ליצור הזדהות
4. שמירת הפרטים בתוכנה לניהול סיסמאות ושמות משתמש
5. שמירה על עקרונות OpSec (סיסמא מורכבת, לעולם לא להשתמש בפרטים מזהים אמיתיים)
6. שינוי מספר הטלפון בהגדרות החשבון למספר של שירות VOIP
7. התנתקות מהחשבון בכל פעם שנסיים את הפעילות בו
8. הוספה של מידע רלוונטי לחשבון שיצרנו ויצירת אמינות

מה הוא שירות נסתר

השירותים הנסתרים הם שרתים המותאמים לקבל תקשורת רק דרך רשת TOR. בתור משתמשים, אנחנו רגילים לחפש בגוגל את מה שמעניין אותנו ודרך מנוע החיפוש של גוגל שמאנדקס את כל התוצאות האלו, להגיע אל מבוקשנו. העניין עם Tor Hidden Services הוא שגוגל לא מאנדקס אתרים עם סיומת onion ולכן לא נוכל למצוא את התוצאות האלו בחיפוש רגיל כמו שאנחנו מכירים. לשירות נסתר נוכל לגשת רק ע"י כתובת ה-onion שלו אז בשביל לגשת לשירותים שכאלו, נשתמש בEntry Points- שיאפשרו לנו לגשת לאתרים ע"י אתרים אחרים, משמע אנחנו פונים אל שירות נסתר והוא מתשאל את האתר הרלוונטי בשבילנו ומחזיר לנו את התשובה. השיטה הפשוטה ביותר היא לגשת דרך מנוע חיפוש או בעזרת שימוש באתרים שמאחסנים לינקים לאתרים אחרים.

מה אפשר למצוא ברשת האפלה

הרשת האפלה היא מנגנון משומן ומהווה זירת סחר המתבססת על היצע וביקוש. ככל שיהיו אנשים ברחבי העולם שידרשו שירותים מסוג מסוים, כך יקומו הספקים שימכרו את השירותים הללו תמורת כסף. נכון להיום, קטגוריית הסמים והכימיקלים מובילה בפער על שאר הקטגוריות, אך לא רק זו קיימת. במרחב הרשת האפלה נוכל למצוא ספקי שירות מגוונים שיוכלו להנפיק לנו תעודות זהות/דרכונים ורישיונות מזויפים מכל מקום בעולם, האקרים להשכרה שיוכלו לבצע עבורנו פעילות פליליות במרחב הסייבר (פריצה לחשבונות, תקיפת אתרים ותשתיות ואפילו רשתות בוטנטים להשכרה, מה שנקרא Botnet As A Service).

רוצחים שכירים הם גם משהו שקיים, לרוב מדובר בחיילים משוחררים שמשתמשים ביכולות שצברו במהלך שירותם בשביל להשתמש באלימות תמורת בצע כסף ולפי דרישת הלקוח (תאונה מבוימת, דקירות, פצצות, ירי צלפים ממוקד). זהויות גנובות וכרטיסי אשראי גנובים הם משהו שנוכל למצוא בשפע, בדרך כלל מדובר בהדלפות שהגיעו מחברות גדולות ע"י פריצה למסדי הנתונים שלהן ועכשיו תמורת כמה דולרים כל אחד יכול לרכוש את הפרטים האלו לשימוש אישי.

נוכל למצוא תחמושת מגוונת, נשקים וכדורים מכל הסוגים ואפילו רישומי תלת מימד להדפסות נשק תלת מימדי. פורומים ושווקים הם מנת חלקה של הרשת האפלה ועליה מבוססת רוב התקשורת עצמה.

בפורומים האלו נוכל למצוא את שלל גווני הרוע פורומים המוקדשים לשנאה והסתה (בעגה המקצועית נקרא Hate Speech, קבוצות ניאו נאצים והסתה כנגד אפרו אמריקאים ואפילו כנגד מוסלמים ושוטרים), פורומים הקשורים לטרור (האתר הרשמי של דעא"ש), מדריכים המוקדשים להכנת סמים במעבדה ביתית, הכנת פצצות בייצור עצמי (לרוב דשן), ביצוע עבירות סייבר (כתיבת תוכנות זדוניות והקמות של דפי תרמית), ואפילו תכנים מיניים קשים כמו פורנוגרפיית ילדים, ניצול בעלי חיים ואונס. רוב הפורומים

ידרשו התחברות מראש, לרובם תהיינה דרישה להזמנה מוקדמת ע"י חבר קיים (מגביר את אמינות המצטרף אם הוא מכיר כבר מישהו שנמצא בפנים והוא יהיה ערב לו) וכמובן תשלום בשביל כניסה.

אמנם השם של הרשת מעיד על עצמו אך לא רק אפלה אפשר למצוא בסביבה הזו. בזכות האנונימיות שמספקת הפלטפורמה, קהילות שלמות של אנשים שצריכים להישאר מתחת לרדאר יכולים להיות מי שהם באמת. למשל קהילת הלהט"ב באיראן פורחת בשימוש בפלטפורמת TOR, יש צ'אטים ממוקדים לנושא הזה והם מרגישים בטוחים לחלוטין להתנהל ברשת שלא חושפת או מסכנת אותם במדינה שלהם. קהילות האקרים שלמות בסין משתמשות ב-TOR, מאחר ואזרחי סין נמצאים תחת מעטה כבד של מידור מהעולם החיצוני (The Great Firewall) ובעזרת גישה לפלטפורמה רשתית לא מבוזרת, הם יכולים לראות מה קורה בשאר העולם גם כן ללא מסך העשן שהממשל כופה עליהם.

מנועי חיפוש ברשת האפלה

בתור גולשים מן השורה, אנחנו רגילים להיכנס לגוגל, שהוא מנוע חיפוש, ולרשום את מה שאנחנו רוצים למצוא. הסיבה שהדבר הזה מתאפשר, היא שמנוע החיפוש גוגל (ואחרים כמו בינג ויאהו!) יודעים לאנדקס אתרים חדשים עם סיומות לגיטימיות כמו סיומת com או co.il. גם בסביבת הדארקנט יש מנועי חיפוש מוגדרים שיודעים לאנדקס אתרים חדשים עם סיומות onion ואתרים שמאגדים לינקים רלוונטיים בתוכם לפי קטגוריות.

- **מנוע החיפוש Ahmia.fi** יודע להתמקד בשירותים נסתרים (יודע לאנדקס אתרים עם סיומות onion). אם למשל נחפש את המילה Drugs, סביר להניח שנמצא לינקים שונים שיובילו אותנו לתכנים הקשורים למכירת סמים שונים.מנוע החיפוש Ahmia.fi כן מצנזר תכנים ספציפיים הקשורים בניצול קטינים ובעלי חיים והוא לא יציג את הלינקים הקשורים בנושאים הללו.
- **מנוע החיפוש TORCH** הוא מנוע חיפוש נוסף שמאנדקס בתוכו המון מהשווקים הבלתי חוקיים ו-Hidden Services השיטה לחיפוש היא מאוד פשוטה, נכנסים למנוע החיפוש ופשוט מקלידים את מה שנרצה למצוא, למשל Credit Cards. המון תוצאות יופיעו.
- **האתר Fresh Onion** שמאנדקס אין ספור לינקים לפורומים שונים בנושאים שונים (רובם בלתי חוקיים)
- **האתר DarkNet Live** שמאנדקס בתוכו המון מידע על פורומים ושווקים, וכמו כן את הלינקים אליהם.
- **האתר Dargle** מאנדקס בתוכו המון דומיינים ע"י תהליך Crawling שמתבצע באופן תמידי ומעדכן את הלינקים הרלוונטיים.

חשוב להדגיש את האנונימיות לחוקר בזמן שהוא ניגש למקומות כאלו. ברוב הפעמים החוקר יזדקק להרשמה לאתרים האלו, משמע כהכנה מוקדמת יש חובה לפתוח חשבונות רלוונטיים (חשבון מייל ברשת TOR, זהות לקוח/מוכר, הסוואה דרך VPN או Proxy ועדיפות גדולה לביצוע של כל הגלישה והמחקר דרך מכונה וירטואלית בלבד).

צורות תשלום ברשת האפלה

ברשת האפלה אפשר למצוא המון שירותים, רובם לא חוקיים כמו פורומים שלמים למכירת סמים ונשק משלל סוגים, הזמנות חיסולים ופשעי אלימות, מדריכים להכנת פצצות, שירותי האקינג וגניבות פרטים פיננסיים ואפילו הזמנות של חלקים לפצצת אטום. מומלץ לא להשתמש באמצעי תשלום לגיטימיים כמו כרטיסי אשראי אישיים או חשבון בנק המקושר אל הרוכש מאחר ואלו מעידים ישירות על מבצע העסקה ומקושרים ישירות אל מיקום הרוכש, על העסקה שבוצעה ויכולים לשמש לזיהוי והוכחות שישמשו כנגד הרוכש ואפילו לגניבות פרטים וזהות.

לצורך תשלום בסביבות האלו, מומלץ במטבעות קריפטוגרפיים ובעיקר ביטקוין, אית'ריום ומונרו. כשרוכשים משהו בצורה לגיטימית, העסקה עוברת דרך חברת האשראי ודרך הבנק באופן ישיר (יש תיעוד של העסקה, ע"י מי היא נעשתה, איפה, מתי וגם על איזה מוצר). העובדה הזו מעידה על בעיה בפרטיות הרכישה. הפתרון הוא שימוש במטבעות קריפטוגרפיים שאינם תלויים בישות אחת בלבד אלא בשיטה של P2P (שיטה מבוזרת). בואו נניח שאליס רוצה לשלוח כסף לבוב. הפעולה שאליס תעשה היא יצירת ארנק קריפטו שיהיה מקושר עם שני מפתחות (פומבי ופרטי). אליס תיצור Transfer Request לבוב עם מספר המטבעות שהיא תרצה להעביר. להעברה הזו יש טביעת אצבע ייחודית התואמת לעסקה הזו בלבד. בעסקה עצמה, גם המפתח הפומבי יהיה משותף בשביל לוודא את חתימת העסקה והאימות שלה.

[מקור: coinmixer-es.net]

את העסקה הזו אליס שולח ל-Cryptocurrency Network שהיא רשת של מחשבים (לרוב עם הספק גבוה) ששומרים עותקים של כל העסקאות שהתרחשו. לרשת הזו קוראים Blockchain והיא אוספת רשומות פומביות שמאגדת את כל העסקאות שנעשו. העסקה תשלח לרשת הזו ושם תיבדק. אם היא תאושר, היא תתווסף לרשת ה-Blockchain כבלוק נוסף.

מאחר והרשת הזו פומבית לחלוטין וכל אחד יכול להוריד עותק שלה, אין שימוש בשמות או פרטים מזהים להעברה של כספים אלא בכתובת ארנק בלבד (מדובר בכתובת ארוכה וייחודית שלא מסגירה שום פרט). כל עוד Opsec נשמר (אבטחת זהות, חיבורים מאובטחים ושמירה על הכללים שהוזכרו בחלקים הקודמים), הארנק לא ייחשף. ככל שיש יותר עסקאות ברשת הבלוקצ'יין, כך יותר קשה לזהות עסקאות קודמות. עם זאת, אכן ישנן אפשרויות לקישור עסקאות הביטקוין בחזרה אל מבצע העסקה.

אמנם כל אחד ברשת יכול לראות את הטרנזקציות המתרחשות בכל רגע נתון (שזו מעידה על בעיה בפרטיות) אך הקושי הרב הוא בשיוך כל טרנזקציה לאדם ספציפי (שזו מעידה על יתרון של אנונימיות). אין כל אדם ששולט במערכת הזו, היא מבוזרת לחלוטין ובכל טרנזקציה אין צורך לחשוף את זהות המקבל, השולח, כתובות IP או כל מידע מזהה אחר.

אפשר ומומלץ להשתמש ב-Bitcoin Mixers שנועדו על מנת להסיר כל חתימה דיגיטלית הקשורה לטרנזקציה עצמה ובכך להקשות על החוקר לקבוע את מקור העסקה או יעדה הסופי.

יש שיוסיפו לעשות ויאבטחו את עצמם בשכבת הגנה נוספת והיא המרה של מטבעות הביטקוין למטבעות אחרים לפני שהם נסחרים בתמורה לשירות הרצוי ובכך לטשטש את היסטוריית העסקאות על פני שרשרת בלוק אחרת. את המפתח הפרטי רצוי לשמור מכל משמר, תחת אמצעים רבים של אבטחה ולעולם לא כקובץ טקסט (Plain Text) פשוט. אפשר לשמור את המפתח תחת הצפנה חזקה (AES-256) או בארנק אחסון קר.

אפילו אפשר להשתמש במחשב זול, או רסבפרי פאיי על מנת לאחסן בו את המפתח הסודי ולעולם לא לחבר את המכשיר הזה לרשת כלשהי. אפשר להשתמש ב-Trezor, מכשיר חומרה המשמש כארנק ביטקוין פיזי ומאפשר אחסון בטוח של המפתחות הפרטיים של הארנק. נצטרך להגדיר בו Seed, משפט המורכב מכמה מילים רנדומליות שבלעדיהן לא נוכל לשנות סיסמא או לשחזור חשבון בשום צורה, וכמו כן יש צורך להגדיר PIN לצורך שכבת אבטחה נוספת.

דרכים שבהן אפשר לקשר את ארנק הביטקוין שלנו אלינו, ומומלץ להימנע מהן

- פרסום השם שלנו וכתובת הארנק שלנו באינטרנט
- מסחר במטבעות בבורסה
- שימוש בביטקוין בלי חיבור VPN או TOR
- שימוש ב-Hosted Wallet (ספק צד שלישי שומר את המטבעות שלי בעבורי, דומה לתהליך שבו הבנק שומר על הכסף עבורינו)
- פתיחת ארנק / שימוש בארנק דרך הטלפון האישי שלנו

טעויות להימנע מהן בעסקאות קריפטו

- לא להשתמש ב-Cake Wallets. ארנק שבו כל המידע מאוחסן במכשיר האישי שלי. במידה ושוק מסוים נחשף (פשיטה משטרתית), יהיה קל מאוד לקשר טרנזקציה שאולי ביצענו אל הכתובת של הארנק ומשם אל המכשיר האישי.
- לעולם לא להשתמש בארנק המשויך לבורסה מסוימת שקונים בה מטבעות, תמיד להחליף את המטבעות לחשבון אחר שהקמנו מבעוד מועד
- מחיקת ארנקים לאחר סיום השימוש בהם
- שינוי ארנק לאחר כל שימוש / כמה שימושים

ישנם מטבעות אחרים שיותר מאובטחים וקשה יותר לנתח איתן מידע ועסקאות על מנת לגלות את מבצע העסקה. מטבעות כמו Monero או בשמו המקצועי XMR, שבזמן העברה במטבע, שש כתובות רנדומליות משרשרת הבלוקצ'יין מתערבבות עם הטרנזקציה הנוכחית מה שמקשה באופן אוטומטי על ניתוח העסקה והבנה שלה (אי אפשר להבין את החתימה של העסקה ולמי היא שייכת).

מונרו ספציפית מצפין את המידע של כל פעולה פיננסית (רק בעל המפתח המתאים יוכל לצפות במידע) ואז משייך כל פעולה פיננסית לקובץ ארנק חדש ולבסוף משתמש בטכניקה של Mixed Coins (האלגוריתם שלו מערבב את המידע של פעולות פיננסיות דומות).

רוב המשתמשים עושים שימוש בארנק אחד בלבד (משיקולי נוחות) אך בתיאוריה הדבר הזה מאפשר לזהות את המשתמש ע"י מציאת תבניות התנהגות במאגר המידע הפיננסי (רשת הבלוקצ'יין) שפתוחה לכולם.

סיכום

במאמר ראינו שפלטפורמת TOR מאפשרת אנונימיות מוגברת, יוצר פרטיות ובכך גורם לרמת אבטחה גבוהה יותר. בכל זאת, יש חובת שמירה על כללי ה-OpSec אם נרצה לשמר את כל היתרונות שאפשר לזכות בהם ולא להקל ראש ולסמוך רק על הטכנולוגיה. רשויות משתמשות והשתמשו בעבר בפיתוחים מיוחדים שנועדו על מנת לנסות ולשבור את ההצפנה של TOR, לנצל חולשות וליצור Exploits יעודיים למשתמשי הרשת על מנת לשבור את מנגנון הסודיות העוטף את משתמש הקצה.

נכון להיום, עוד לא הוכח שישנה הצלחה בנושא אך הדבר לא תקף למשתמשים שלא מעדכנים את הפלטפורמה שלהם. ברוב המקרים, כאשר הרשויות מבצעות פשיטה על שווקים ומידע של פושעים, ניתוח מעמיק שלו יכול לחשוף מידע נוסף רלוונטי שעלול לקשור עוד אנשים למעשים בלתי חוקיים ולהוסיף אותם לרשימת מעקב או לגרום למעצרם. במיוחד בשביל מקרים כאלו, כללי ה-OpSec קריטיים.

אם הזהות נבנתה בתהליך מעמיק ונכון, חשבונות המדיה מעולם לא קושרו עם חשבונות אמיתיים או מכשירים אישיים ופרטים מסגירים לא סופקו, יהיה מאוד קשה ועל גבול הבלתי אפשרי לרשות כלשהי ליצור קורלציה רשתית עם הממצאים שנאספו על מנת לזהות את המשתמש שמאחורי המסך. גם בעולם של חוסר בפרטיות ושל ניטור מתמשך אפשר למצוא את הכללים והטכנולוגיות שיאפשרו לשמור על רמה גבוהה יותר של אנונימיות. כל מה שצריך הוא להכיר את הדרכים ולבחור בדרך הנכונה להשתמש בהן וכל עוד נשמור על הכללים, נוכל לזכות לפרטיות ואנונימיות ובכך לחיות חיים מאובטחים הרבה יותר.

קישורים

- https://www.geeksforgeeks.org/onion-routing/
- https://www.fakeperson.com
- http://www.elfqrin.com/fakeid.php
- thispersondoesnotexist.com
- Gallery of AI-Generated faces