אאוץ! | יוני 2019

עלון מודעות אבטחת מידע למשתמשי מחשב

הרשת האפלה

סקירה כללית

ייתכן ששמעתם את המונח "הרשת האפלה" ממשתמשים אחרים או בתקשורת ותהיתם "מהי הרשת האפלה?" או "האם עלי לעשות משהו בקשר לזה?". היום נסביר מה היא הרשת האפלה ומה הן המשמעויות עבורך.

מה זה?

הרשת האפלה מורכבת ממערכות באינטרנט המיועדות לתקשורת או לשיתוף מידע באופן מאובטח ואנונימי. אין "רשת אפלה" אחת; זה לא משהו כמו פייסבוק שמופעל על ידי ארגון אחד, אלא הרשת האפלה היא אוסף של מערכות ורשתות שונות המ־נוהלים על ידי אנשים שונים המשמשים למגוון מטרות. מערכות אלו עדיין מחוברות והן חלק מהאינטרנט, אך בדרך כלל לא תמצא אותן באמצעות מנועי החיפוש הרגילים שלך. לעתים קרובות אתה צריך תוכנה מיוחדת במחשב שלך כדי למצוא או לגשת אליהם. דוגמה אחת היא פרויקט Tor. כדי לגשת לרשת האפלה , נדרש להוריד ולהתקין את דפדפן Tor. כאשר אתה מתחבר לשרתי אינטרנט באמצעות דפדפן Tor, התקשורת שלך מוצפנת ועוברת דרך מחשבים אחרים המשתמשים גם הם ב-Tor. כאשר התקשורת "קופצת" דרך המחשבים האלה, כתובת ה-IP של המקור משנה משמעות וכאשר אתה מגיע לאתר האינטרנט, הפעילות המקוונת שלך היא אנונימית. דוגמאות נוספות של הרשת האפלה כוללות Zeronet, Freenet ו-I2P.

מי משתמש בה?

רוב השימוש ברשת האפלה נעשה ע"י פושעי סייבר. הם מפעילים את אתרי האינטרנט והפורומים ברשת האפלה כדי לאפשר פעילות פלילית שלהם כגון רכישת סמים או מכירת כמויות רבות של נתונים גנובים - כולם בעילום שם ובבטחה. לדוגמה, כאשר פושעי סייבר פורצים לבנק או לחנות קניות מקוונת, הם גונבים מידע רב ככל האפשר, ולאחר מכן מוכרים את המידע הזה לפו־שעים מקוונים אחרים באתרים ברשת האפלה.

יש גם שימושים לגיטימיים של הרשת האפלה. לדוגמה, אנשים במדינות שבהן הצנזורה משתוללת יכולים להשתמש ברשת האפלה כדי לשתף מידע ולראות מה קורה בעולם, תוך שמירה על פרטיותם והישארות אנונימיות. עיתונאים, חושפי עוולות ואנשים המודעים לפרטיות יכולים להשתמש ברשת האפלה כדי להגדיל את האנונימיות שלהם ולעקוף את הצנזורה. בנוסף,

אנשים כמו אלה יכולים להשתמש בטכנולוגיות כמו דפדפן Tor לא רק כדי לגשת לרשת האפלה, אלא באופן אנונימי לגלוש באינטרנט רגיל.

מה עלי לעשות?

אלא אם כן יש לך סיבה ספציפית לגשת לרשת האפלה, אנו מזהירים אותך מפני זאת. חלק מאתרי הרשת האפלה משמשים למטרות בלתי חוקיות, רבים מהאתרים ישתמשו במחשב שלך ב"רשת עמיתים" כדי להשיג את המטרות שלהם, ובמקרים מסוימים המחשב שלך עלול אפילו להיבדק או להיתקף. יש חברות המציעות שירותי ניטור כדי ליידע אותך אם השם שלך או מידע אחר נגנב על ידי עברייני המרחב הקיברנטי נמצא על הרשת האפלה. הערך בפועל של שירותים אלה מוטל בספק. הדרך הטובה ביותר להגן על עצמך היא להניח חלק מהמידע שלך כבר נמצא ברשת האפלה בשימוש על ידי עבריינים הקיברנטי. לכן . . .

- **חשוד בכל שיחות טלפון או הודעות דוא"ל בכך שמעמידים פנים להיות ארגונים רשמיים ולוחצים אותך לנקוט פעולה, כגון תשלום קנס. פושעים עשויים אפילו להשתמש במידע שהם מצאו אודותיך כדי ליצור התקפה מותאמת אישית.**
- **פקח על כרטיס האשראי שלך ודוחות הבנק. אולי אפילו הגדר התראות יומיות על כל העסקאות שקורות. בדרך זו תוכל לזהות אם הונאה פיננסית מתרחשת. אם אתה מזהה הונאה, לדווח על כך מיד לחברת האשראי או הבנק שלך.**
- **הקפא גישה לניקוד האשראי שלך. זה לא משפיע איך שימוש בכרטיס האשראי שלך, אך זה אחד הצעדים היעילים ביותר שאתה יכול לנקוט כדי להגן על עצמך מפני גניבת זהות.**

עורך אורח

מיכה הופמן (@WebBreacher) הוא החוקר הראשי ב- Spotlight Infosec LLC, מדריך מכון SANS מוסמך ומחבר הקורסים של SANS OSINT. התשוקה של מיכה לסייבר ולמודיעין בשימוש בקוד פתוח נראית בפרויקטים, בלומדות וסגנון ההוראה שלו.

מקורות

התקפות מותאמות אישית:	https://www.sans.org/u/RfW
הנדסה חברתית:	https://www.sans.org/u/Rg1
גניבת זהות:	https://www.identitytheft.gov
זיכוי אשראי:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
דפדפן Tor:	https://www.torproject.org
קורס SANS OSINT:	https://sans.org/sec48