הקדמה:

גופים גדולים (ממשלות) אשר פוגעות בחופש הביטוי ע"י הפעלת צנזורה קיצונית כגון חסימת אתרים, בעיקר אתרים שמשמים לקבלת/הפצת מידע שמכוון כנגדן. דוגמא טובה לתופעה זו היא הצנזורה שמפעילה ממשל סין כנגד תושביה ואף מפעילה פעולות ענישה קיצוניות כנגד אנשים פרטים שנתפסים משתמשים ו/או מפיצים מידע שהחליטה שראוי להיות מצונזר.

הגדרות (שלנו ושל המאמר):

ב- **client** הכוונה תהיה למשתמש סיני שרוצה לגשת למידע שהוא חסום ממנו.

**Spoofer** אצלנו יציין שרת שיושב **מחוץ** לגבולות סין שמטרתו לזייף כתובות IP כדי שיראו לגיטימיות

**Dummy** מציין שרת לגיטימי (מבחינת סין) שיושת מחוץ לגבולותיה – ננצל את כתובת הIP שלו בSpoofer

**מידע לא לגיטימי** יציין מידע שממשלת סין הייתה רוצה למנוע מהclient-ים לקבל

הרעיון העיקרי:

1.שימוש בproxy כדי להעביר מידע לא לגיטימי לclient .

2.שימוש ב-ipSpoofer ע"מ למנוע מהסינים לעלות על מקור המידע הלא לגיטימי ובכך להגן על הclient.

יכולות התוקף:

כיוון שמדובר כאן בממשלת סין, המודל הוא של תוקף מאוד חזק )בעל יכולות שהיינו מצפים ממשל כזה(. אנו לא רואים טעם בלחזור על המאמר ,אך נציין שכל יכולת **לגיטימית** לתוקף (למשל לא יכול לשבור AES) נמצאת במודל התוקף.

דברים שלא יעשה התוקף:

יכולות התוקף **כן** כוללות סגירת דוא"ל, VoIP או חסימת שימוש בתעבורה מוצפנת. **למרות זאת**, ההנחה היא שממשל סין **תבחר** **לא** לעשות לעשות ע"מ לא לפגוע בצורת נוראית בכללכלה של עצמה (בשפת המאמר: "תשלום של מחיר כבר").

מטרות המאמר:

1. התוקף לא יוכל לחסום את השיטה מבלי לספוג נזקים כבדים

2. התוקף לא יכול להבדיל בין משתמש לגיטימי בעינייו לבין משתמש שפועל לפי השיטה במאמר בלי נזק כבד

3. השיטה תהיה מסוגלת לעבוד עם אתרים פשוטים (לא אינטרקביטים לתורף יעילות)

4. השיטה צריכה להיות נגישה למשתמשים בעלי משאבים מוגבלים

דרך פעולה:

הברחת המידע הלא לגיטימי לתוך סין:

ע"מ להעביר למשתמש מידע לא לגיטימי, נשתמש בשרתי proxy שיוכלו לעביר את המידע.

הבעיה שממשלת סין יכולה בקלות להתחזות למשתמש , לזהות את כתובת הIP של הproxy , ולחסום גישה אליה. לכן, נרצה להביא למצב שהמשתשים לא יודעים מהי כתובת הIP האמיתי של הproxy.

הסתרת כתובת ה IP של הproxy

שליחת הבקשה לאתר החסום תהיה בעזרת מייל. משיכת מייל אינה תלוי בכתובת IP.בנוסף, ניתן להשתמש במספר גדול של מיילים מאותה כתובת IP. כיוון שבקשת האתר הינה קטנה, מגבלת רוחב הפס בערוץ (client->proxy) לא מהווה בעיה. אך לא ניתן להשתמש במייל בכיוון ההפוף כיוון שבו רוחב הפס כן בעל חשיבות.

השגת רוחב פס מתאים בערוץ (client->proxy)

המידע שישלח ה proxy ל client יעבור בשידור VoIP ,שהוא שידור בקצת מספיק מהיר לצרכים המדוברים.הבעיה בשידור זה הוא שהלקוח לומד את הIP של proxy. לכן לקוח שנשתל ע"י סין יוכל לחשוף את כתובת הproxy. נרצה למנוע מהמשתמש ללמוד כתובת זו ע"י זיופה.

זיוף כתובת הproxy

ע"מ לעשות זאת נשתמש בIpSpoofer. לא ניתן לזייף "סתם" כתובת )נקרא לה **(dummy** כיוון שהתוקף יכול לבדוק האם הכתובת הdummy באמת תומכת בסוג השיחה שאמורה להתנהג. לכן נאלץ לבחור את הdummy בחוכמה.

בחירת הdummy

כייון שהתקשורת שעומדת להתנהל אמורה להראות כמו תקשורת VoIP רגילה, נהיה חייבים לבחור כתובת dummy של מחשב שבאמת קיים ושתומך בתקשורת מסוג זה – אם לא התוקף יוכל לגלות זאת ולהבין שלא מדובר בשימוש שהשימוש עשוי להיות לא לגיטימי – מסכן את הclient.

\*יש כמובן עוד פרמטרים ע"מ לבחור dummy. לבחירה לא נכונה יכולות להיות השלכות שיביאו לגילוי הclient, נדבר עליהן בצורה יותר מפורטת כשנגיע להתקפות על הפרוטוקול המוצע והתגוננות מפניהן.

TCP VS UDP ??

VoIP over SIP??

לא בטוח שלצריך לדבר על זה

סכמת המאמר