



感谢您订阅由亚信安全客户服务中心撰写的《信息系统安全周报》。
我们竭诚为您提供最新的安全资讯、病毒流行趋势、系统漏洞提示及网络安全防护技巧。

病毒情报中心	系统漏洞信息
一周病毒情况报告 亚信安全热门病毒综述- Backdoor.MSIL.REMCOS.AOJ	KB4530689
病毒通告	亚信安全产品
警惕 SODINOKIBI 勒索病毒再变种 勒索巨额赎金	病毒码发布情况

一周病毒情况报告

本周用户报告感染数量较多的病毒列表

- TROJ_EQUATED 家族

亚信安全热门病毒综述

亚信安全热门病毒综述-Backdoor.MSIL.REMCOS.AOJ

该后门病毒通过携带有.ISO 附件的垃圾邮件传播，其链接如下 URL 接收远程用户发送的命令：

- rennelautos.{BLOCKED}w.com:2404
- rennelautos.{BLOCKED}o.org:2404
- kellyben.{BLOCKED}o.org:2404
- jkharding2014.{BLOCKED}s.net:2404
- sunwap878.{BLOCKED}s.net:2404
- sunwap878.{BLOCKED}u.net:2404
- jessen.{BLOCKED}o.org:2404
- jessen.{BLOCKED}s.rocks:2404

- 对该病毒的防护可以从下述链接中获取最新版本的病毒码：15.559.60

<http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/>

- 病毒详细信息请查询：

<https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/backdoor.msil.remcos.aoj>

系统漏洞信息

Windows 安全更新 (4530689)

Windows 10 Version 1607 for 32-bit Systems

Windows 10 Version 1607 for x64-based Systems

描述: <https://portal.msrc.microsoft.com/zh-cn/security-guidance>

亚信安全产品

病毒码发布情况

亚信安全在最近一周发布中国区病毒码情况如下:

2019 年 12 月 09 日发布病毒码 15.545.60
2019 年 12 月 10 日发布病毒码 15.547.60
2019 年 12 月 11 日发布病毒码 15.549.60
2019 年 12 月 12 日发布病毒码 15.551.60
2019 年 12 月 13 日发布病毒码 15.553.60

截至目前, 病毒码的最高版本为 15.559.60 发布于 2019 年 12 月 16 日。

病毒码下载地址为:

<http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/>

您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新:

<http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/TSUT/>

趋势科技在最近一周发布全球病毒码情况如下:

2019 年 12 月 09 日发布病毒码 15.547.00
2019 年 12 月 10 日发布病毒码 15.549.00
2019 年 12 月 11 日发布病毒码 15.551.00
2019 年 12 月 12 日发布病毒码 15.553.00
2019 年 12 月 13 日发布病毒码 15.555.00

截至目前, 病毒码的最高版本为 15.561.00, 发布于 2019 年 12 月 16 日。

病毒码下载地址为:

<http://support.asiainfo-sec.com/Anti-Virus/Main-Pattern/>

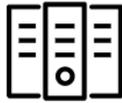
您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新:

<http://support.asiainfo-sec.com/Anti-Virus/TSUT/>

系统安全技巧

近日, 亚信安全截获 SODINOKIBI 勒索病毒最新变种文件, 与以往不同的是, 本次截获的勒索病毒的 payload 是一个 DLL 文件 (以往样本是 EXE 可执行文件), 通过进程注入方式加载, 从而逃避检测。其首先通过 .net 外壳程序启动一个正常的 vbc.exe 进程, 然后将勒索模块注入到该进程中, 最后加载执行数据加密。另外一个值得注意的是, 本次勒索病毒的勒索赎金最高达 4 万美金。亚信安全将该勒索病毒命名为 Ransom.MSIL.SODINOKIBI.A。

Your network has been infected!



Your documents, photos, databases and other important files **encrypted**



To decrypt your files you need to buy our special software - **931gf1hhl-Decryptor**



You can do it right now. Follow the **instructions below**. But remember that you do not have much time

931gf1hhl-Decryptor price

the price is for all PCs of your infected network

You have **1 day, 14:47:06**

* If you do not pay on time, [the price will be doubled](#)

* Time ends on Dec 2, 07:41:32

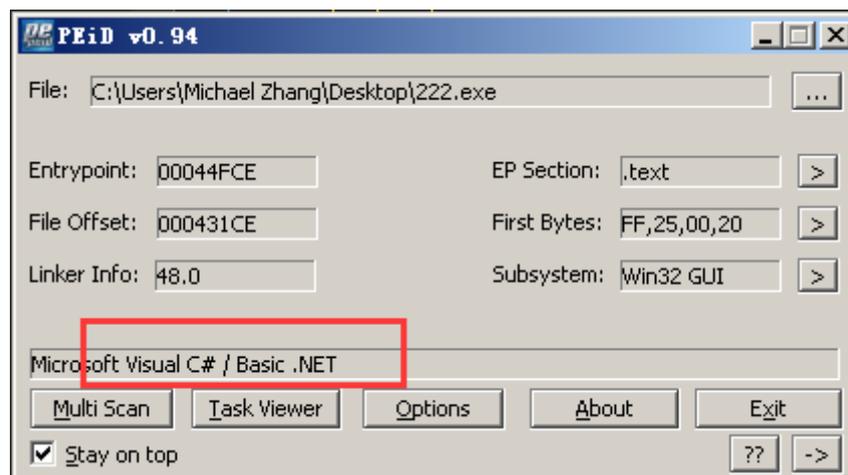
Current price **2.60766732 BTC**
≈ 20,000 USD

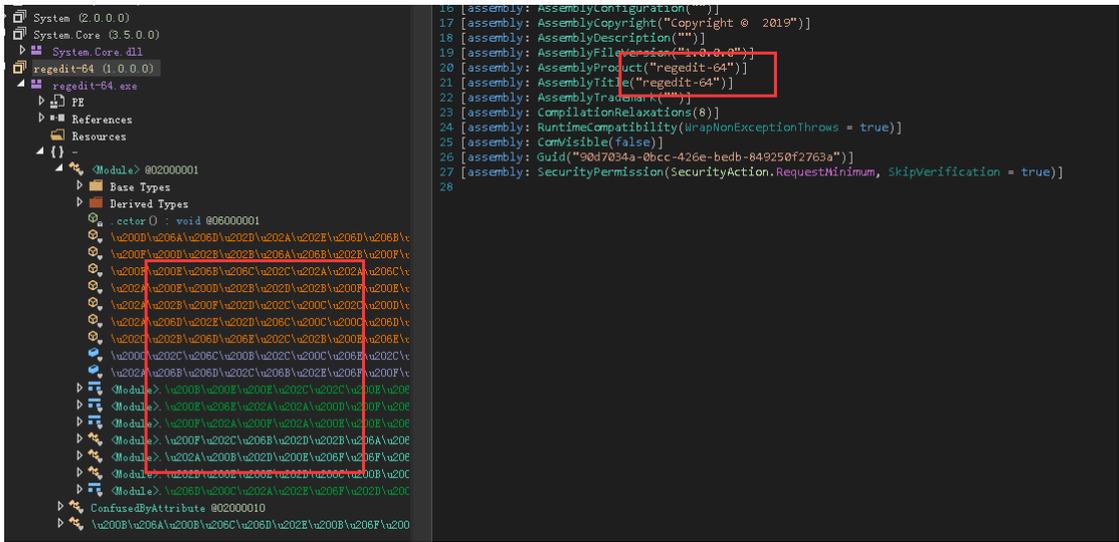
After time ends **5.21533464 BTC**
≈ 40,000 USD

病毒详细分析

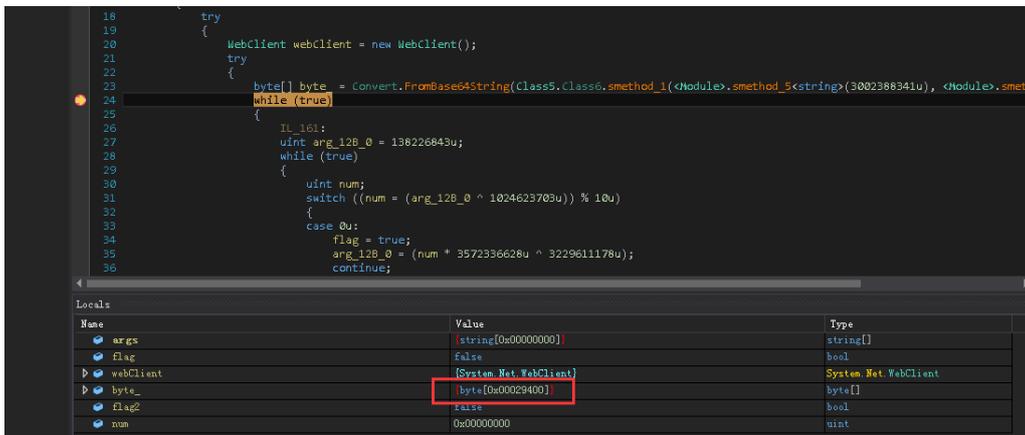
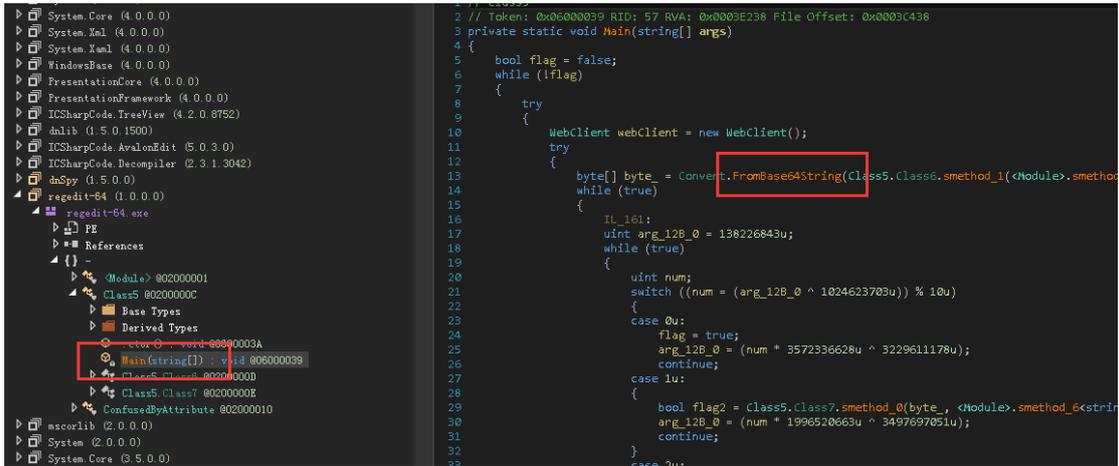
外壳程序分析

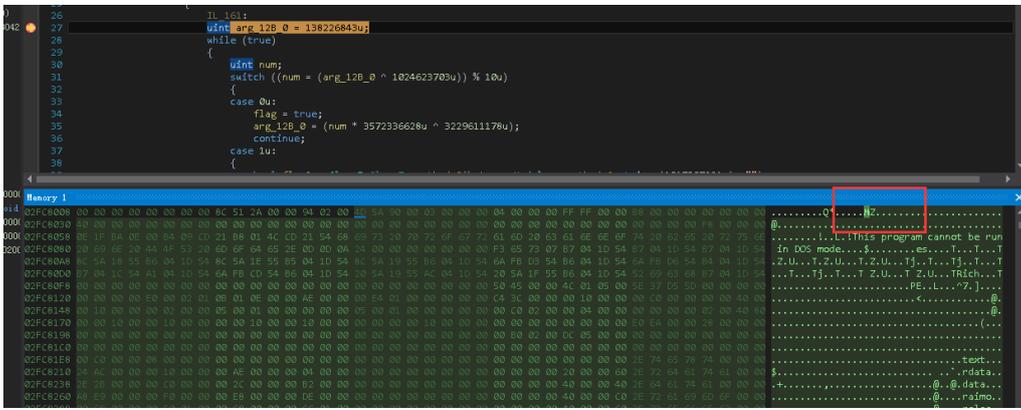
该样本是由.Net 编写，并且进行了混淆处理。样本信息如下图所示：



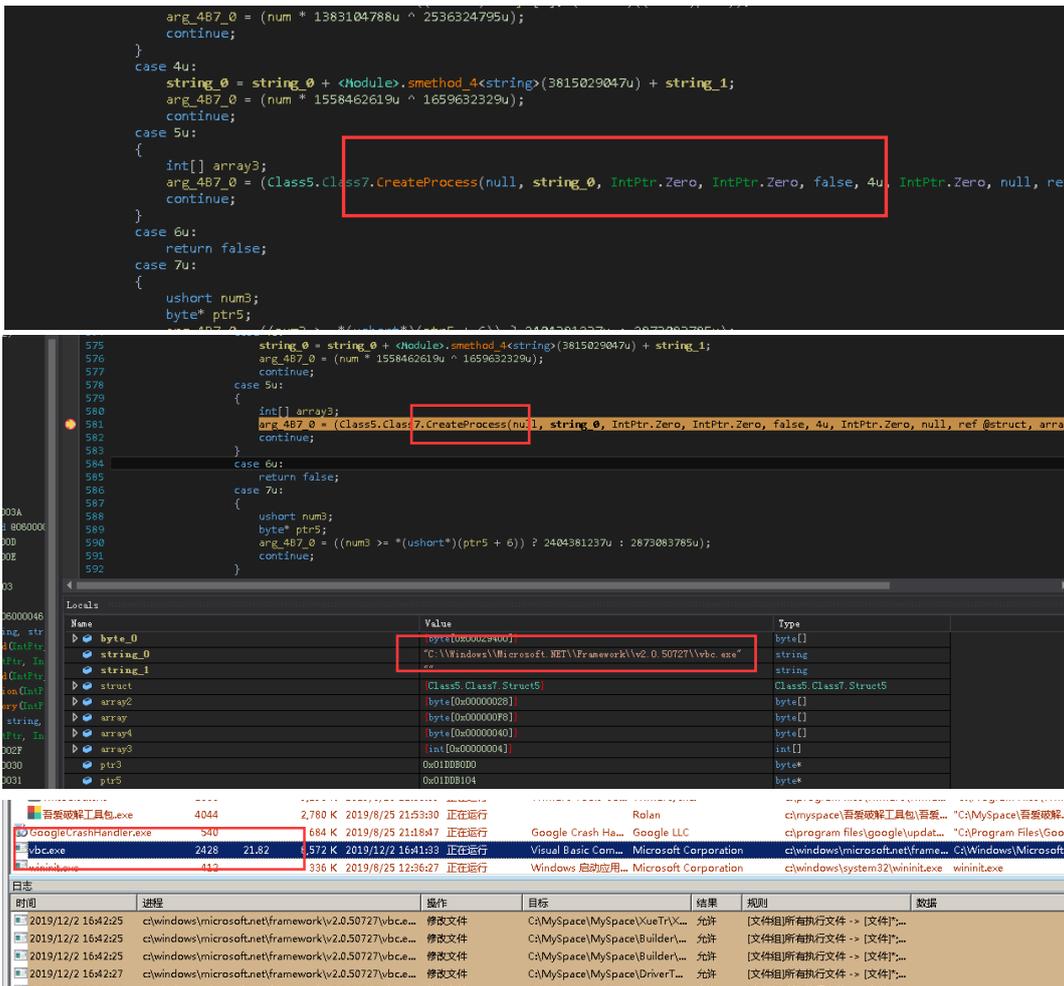


去除相关混淆后，我们可以清楚地看到具体程序流程，其首先使用 base64 解密数据到数组中，通过动态调试可知，解密后的数据就是核心勒索 payload DLL（我们 dump 出为 payload.dll），用于后续的进程注入：





然后启动 Windows 的正常进程 vbc.exe:



通过进程内存修改和恢复线程的方式进行注入操作:

```

{
    byte* ptr3;
    int[] array3;
    IntPtr IntPtr;
    byte* ptr2;
    Class5.Class7.NtWriteVirtualMemory((IntPtr)array3[0], (IntPtr)((long)((int)IntPtr) + (long)((ulong)*(uint*)(ptr3
ptr2 = null;
    arg_4B7_0 = (num * 1332703686u ^ 2364008670u);
    continue;
}
case 10u:
{
    byte* ptr5;
    IntPtr IntPtr = new IntPtr(*(int*)(ptr5 + 52));
    int[] array3;
    Class5.Class7.NtUnmapViewOfSection((IntPtr)array3[0], IntPtr);
    arg_4B7_0 = 2696633156u;
    continue;
}
case 11u:
{
    int[] array3;
    byte* ptr4;
    IntPtr IntPtr;
    Class5.Class7.NtWriteVirtualMemory((IntPtr)array3[0], (IntPtr)((long)((ulong)*(uint*)(ptr4 + 172))), IntPtr, 4u,
    byte* ptr5;
    *(int*)(ptr4 + 176) = (int)IntPtr + (int)*(uint*)(ptr5 + 40);
    arg_4B7_0 = (num * 1469301692u ^ 2319547507u);
    continue;
}

    arg_4B7_0 = (num * 1060589996u ^ 3687621749u);
    continue;
case 15u:
    Class5.Class7.smethod_0(byte_0, string_0, string_1);
    arg_4B7_0 = (num * 3284657263u ^ 1425938922u);
    continue;
case 16u:
{
    int[] array3;
    Class5.Class7.NtResumeThread((IntPtr)array3[1], IntPtr.Zero);
    arg_4B7_0 = (num * 2980304615u ^ 1404029858u);
    continue;
}
case 17u:
{

```

进程注入操作用到的库函数列表:

```

4 // Token: 0x0200000E RID: 14
5 public static class Class7
6 {
7     // Token: 0x0600003F RID: 63
8     [DllImport("kernel32.dll", SetLastError = true)]
9     private static extern bool CreateProcess(string string_0, string string_1, IntPtr IntPtr_0, IntPtr IntPtr_1, bool bool_0, uint uint_2,
10     IntPtr IntPtr_2, IntPtr IntPtr_3, IntPtr IntPtr_4, IntPtr IntPtr_5);
11     // Token: 0x06000043 RID: 67
12     [DllImport("ntdll.dll", SetLastError = true)]
13     private static extern int NtGetContextThread(IntPtr IntPtr_0, IntPtr IntPtr_1);
14
15     // Token: 0x06000045 RID: 69
16     [DllImport("ntdll.dll", SetLastError = true)]
17     private static extern uint NtResumeThread(IntPtr IntPtr_0, IntPtr IntPtr_1);
18
19     // Token: 0x06000044 RID: 68
20     [DllImport("ntdll.dll", SetLastError = true)]
21     private static extern int NtSetContextThread(IntPtr IntPtr_0, IntPtr IntPtr_1);
22
23     // Token: 0x06000041 RID: 65
24     [DllImport("ntdll.dll", SetLastError = true)]
25     private static extern uint NtUnmapViewOfSection(IntPtr IntPtr_0, IntPtr IntPtr_1);
26
27     // Token: 0x06000042 RID: 66
28     [DllImport("ntdll.dll", SetLastError = true)]
29     private static extern int NtWriteVirtualMemory(IntPtr IntPtr_0, IntPtr IntPtr_1, IntPtr IntPtr_2, uint uint_4, IntPtr IntPtr_3);
30
31     // Token: 0x0600003E RID: 62 RVA: 0x0003E9F8 File Offset: 0x0003CBF8
32     public unsafe static bool smethod_0(byte[] byte_0, string string_0, string string_1 = "")
33     {
34         Class5.Class7.Struct5 @struct = default(Class5.Class7.Struct5);

```

payload.dll 文件分析

此文件是勒索病毒主体文件，与以往 SODINOKIB 勒索样本基本类似，需要在内存中解密出核心加密主程序，然后跳转至入口执行：

```

.text:00403CC1
.text:00403CC4
.text:00403CC4 ; ===== SUBROUTINE =====
.text:00403CC4
.text:00403CC4
.text:00403CC4
.text:00403CC4
.text:00403CC4
.text:00403CC4 start      public start
.text:00403CC4          proc near
.text:00403CC4          push      0
.text:00403CC6          call     sub_403C7B ; SodInokibi勒索病毒典型入口
.text:00403CC8          push      0
.text:00403CCD          call     sub_40457B
.text:00403CD2          pop       ecx
.text:00403CD3          retn
.text:00403CD3 start      endp
.text:00403CD3
.text:00403CD4
.text:00403CD4 ; ===== SUBROUTINE =====
.text:00403CD4
.text:00403CD4 : Attributes: bp-based frame

```

加密后的文件后缀名为.gt0w210:

名称	日期/时间	类型	大小
jdk-11.0.4_windows-x64_bin	2019/12/2 16:39	文件夹	
MySpace	2019/12/2 16:39	文件夹	
01lyDBG最终完美版	2019/12/2 16:40	文件夹	
吾爱破解工具包2.0	2019/12/2 16:39	文件夹	
Beyond_Compare4.0.7.rar	2019/12/2 16:39	GT0W210 文件	9,299 KB
ChromeSetup.exe	2019/8/25 21:16	应用程序	1,125 KB
fakenet1.4.3.zip.gt0w210	2019/12/2 16:39	GT0W210 文件	5,853 KB
ghidra_9.0.4_PUBLIC_20190516.zip.gt0w210	2019/12/2 16:39	GT0W210 文件	291,508 KB
ghidra-master.zip.gt0w210	2019/12/2 16:39	GT0W210 文件	68,735 KB
gt0w210-readme.txt	2019/12/2 16:39	文本文档	7 KB
jdk-11.0.4_windows-x64_bin.zip.gt0w210	2019/12/2 16:39	GT0W210 文件	175,358 KB
PDFStreamDumper_Setup.exe	2019/8/25 22:38	应用程序	3,709 KB
pdfstreamdumper-master.zip.gt0w210	2019/12/2 16:39	GT0W210 文件	5,372 KB

勒索提示信息文件:

```

gt0w210-readme.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
----- Welcome. Again. -----

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your computer has extensic
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, y

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not
To check the ability of returning files, You should go to our website. There you can decrypt one file for free
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
a) Download and install TOR browser from this site: https://torproject.org/
b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkxbr6wketf56nf6aq2nmyoyd.onion/437B7AD0D0BC7A73

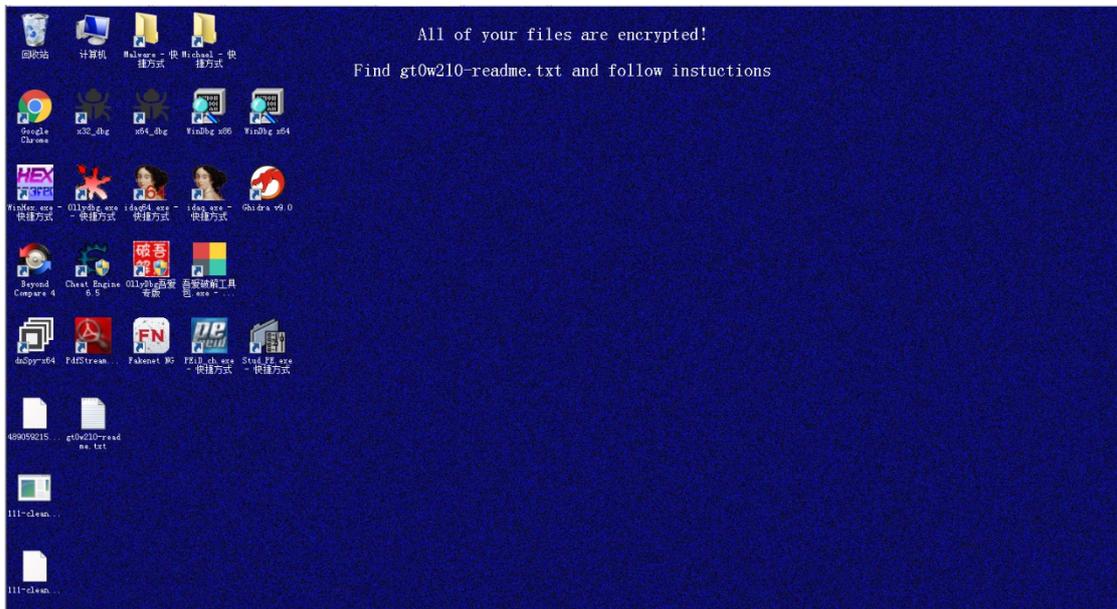
2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
b) Open our secondary website: http://decryptor.top/437B7AD0D0BC7A73

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:

```

修改桌面背景图片:



解决方案

- ✓ 不要点击来源不明的邮件以及附件；
- ✓ 不要点击来源不明的邮件中包含的链接；
- ✓ 采用高强度的密码，避免使用弱口令密码，并定期更换密码；
- ✓ 打全系统及应用程序补丁；
- ✓ 尽量关闭不必要的文件共享；
- ✓ 请注意备份重要文档。备份的最佳做法是采取 3-2-1 规则，即至少做三个副本，用两种不同格式保存，并将副本放在异地存储。

亚信安全解决方案

- ✓ 亚信安全病毒码版本 15.533.60，云病毒码版本 15.533.71，全球码版本 15.533.00 已经可以检测，请用户及时升级病毒码版本。

详情可登陆亚信安全官网 www.asiainfo-sec.com 或拨打免费咨询热线 800-820-8876