GandCrab V5.2 变种追踪分析

2019-03-21

1. 前言

最近，安恒威胁情报追踪团队发现在 3 月 11 日传播的勒索软件 GandCrab V5.2 在 3 月 20 日又开始新变种传播，这次攻击者将邮箱投递的文件“03-11-19.rar”直接改成“INFORMATION!你必须在 3 月 21 日_下午 3 点向警察局报到!.zip”，变种 GandCrab 对恶意代码进行了混淆改进，需要引高度重视。

2. 攻击线索

将黑客攻击信息绘制成表格：

攻击时间	投递人	文件名称	文件 Hash	解压后文件名
2019-3-10	Min, Gap Ryong	03-11-19.rar	4e6374b0b3421c739ef90bbf4ffb92d5	你 须瞍 3 昱 11 祉 珥 3 铐添笮涎报羽.exe
2019-3-20	Min, Gap Ryong	INFORMATION!你必须在 3 月 21 日_下午 3 点向警察局报到!.zip”	40b7e2560b168a7882ab0b73377d870a	你必须在 3 月 20 日下午 3 点向警察局报到.doc.exe

平台检测到攻击者使用的邮箱，包括

beom-seyk@amaznsicherheitsdienst.com
beom-seyk@blackmonlabs.com
beom-seyk@idabostian.com
beom-seyk@illwaitforthemovie.com
byung-chal@amaznsicherheitsdienst.com
byung-chal@b4imports.com
jae-bong-police@drowsybear.com
jae-bong-police@idalbostian.com
jae-ho-policesupport@b4imports.com
jae-ho-policesupport@designerbasith.com
jae-ho-policesupport@drowsybear.com
jae-hyuk@amazosicherheitsdienst.com

jae-hyun@blackmonlabs.com
jae-hyun@illwaitforthemovie.com
jae-jin@amaznsicherheitsdienst.com
jae-jin@designerbasith.com
jae-jin@illwaitforthemovie.com
jae-jin@metricblog.com
jae-joon@idabostian.com

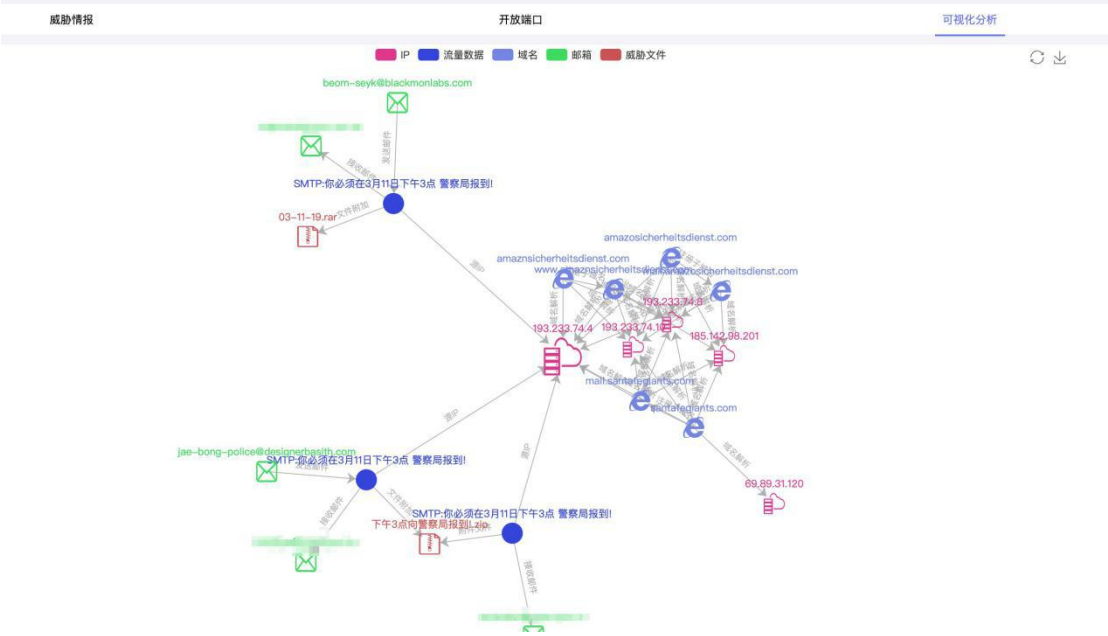
相关邮箱服务器的域名主要有：

- amaznsicherheitsdienst.com
- amazosicherheitsdienst.com
- b4imports.com
- blackmonlabs.com
- designerbasith.com
- drowsybear.com
- idabostian.com
- idalbostian.com
- illwaitforthemovie.com
- metricblog.com

域名其对应的 ip 分布：

- 193.233.74.2 ~ 193.233.74.10

目前，有些域名已经解析到其他地址，但 IP 归属都是俄罗斯。
通过安恒文件威胁分析平台能快速的将两个文件通过攻击信息快速关联起来

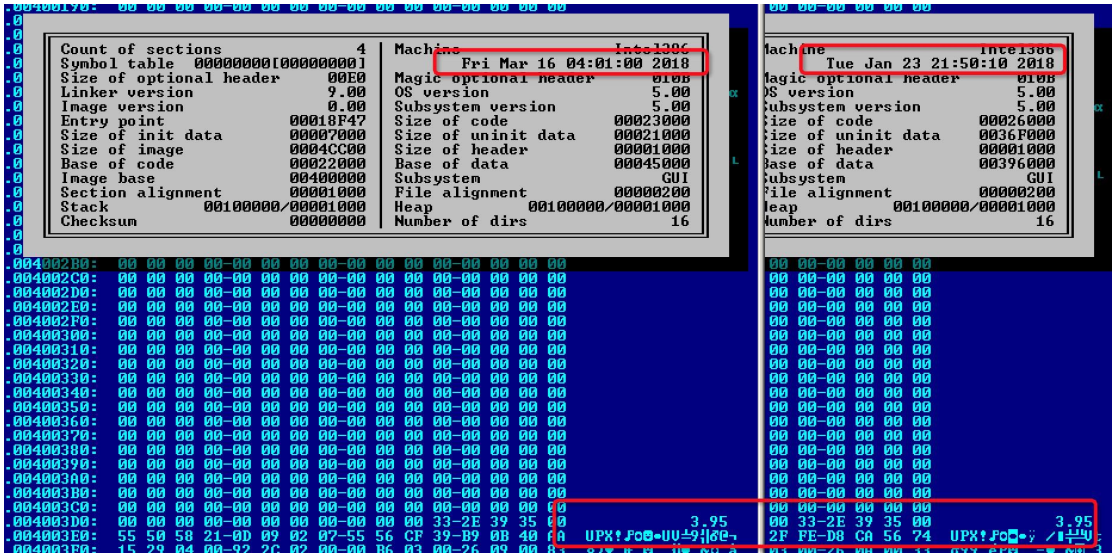


3. 样本分析

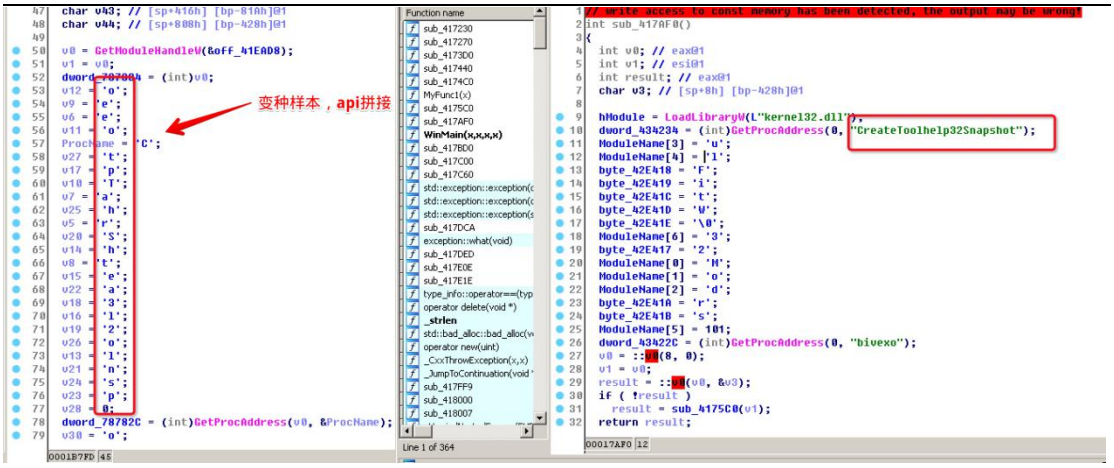
通过观察发现变种样本由原来的伪装 Word 图标成一个闹钟图案，

两个文件都是使用 Upx 进行加壳，编译时间都是 2018 年，且变种样本的编译时间比首次发现的样本时间要早，推出攻击者故意修改了编译时间。

- 2018-03-16 04:01:00 首次样本
- 2018-01-23 21:50:10 变种样本



对比原始样本，变种样本对字符串采用了拼接技术



使用填充垃圾指令绕过杀毒检测

```
0041B495  .  50            push    eax                              Class
0041B496  .  53            push    ebx                              hKey
0041B497  .  FF15 04C0410  call    dword ptr [<&ADVAPI32.RegQueryI   RegQueryInfoKeyA
0041B49D  .  53            push    ebx                              BackupName
0041B49E  .  53            push    ebx                              NewFileName
0041B49F  .  53            push    ebx                              Subkey
0041B4A0  .  53            push    ebx                              hKey
0041B4A1  .  FF15 0CC0410  call    dword ptr [<&ADVAPI32.RegReplac   RegReplaceKeyW
0041B4A7  .  53            push    ebx                              Count
0041B4A8  .  53            push    ebx                              pPoints
0041B4A9  .  53            push    ebx                              hDC
0041B4AA  .  FF15 2CC0410  call    dword ptr [<&GDI32.PolyBezier>]   PolyBezier
0041B4B0  .  53            push    ebx                              CombineMode
0041B4B1  .  53            push    ebx                              hSrcRegion2
0041B4B2  .  53            push    ebx                              hSrcRegion1
0041B4B3  .  53            push    ebx                              hDestRegion
0041B4B4  .  FF15 20C0410  call    dword ptr [<&GDI32.CombineRgn>]   CombineRgn
0041B4BA  .  53            push    ebx                              pStyle
0041B4BB  .  53            push    ebx                              StyleSize
0041B4BC  .  8D45 A0       lea     eax, dword ptr [ebp-60]
0041B4BF  .  50            push    eax                              pLogbrush
0041B4C0  .  53            push    ebx                              Width
0041B4C1  .  53            push    ebx                              PenStyle
0041B4C2  .  FF15 34C0410  call    dword ptr [<&GDI32.ExtCreatePen   ExtCreatePen
```

通过对内存进行加解密操作，从内存中解密出 PE 文件

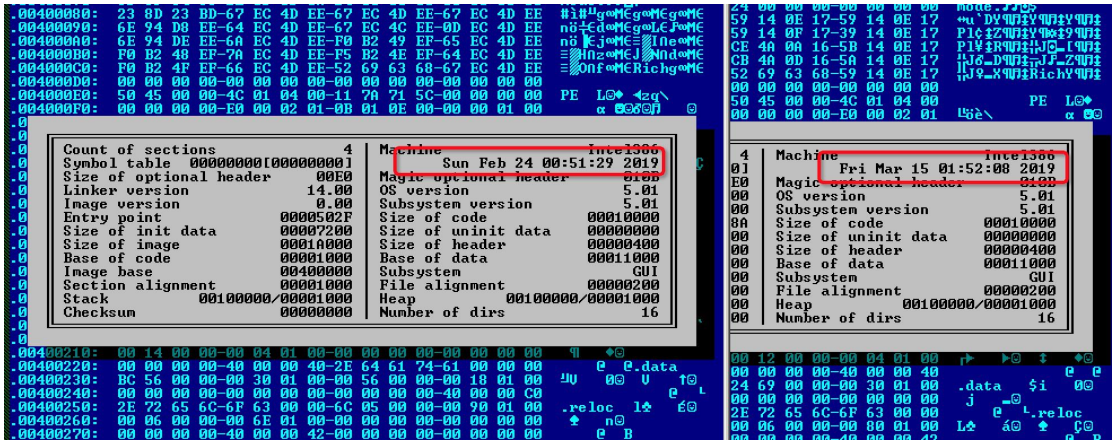
```
00159850   50              push    eax
00159851   E8 E3070000    call    0015A039
00159856   83C4 14         add     esp, 14
00159859   EB 43           jmp     short 0015989E
0015985B   83A5 48FFFFFF   and     dword ptr [ebp-B8], 0
00159862   EB 0D           jmp     short 00159871
00159864   8B85 48FFFFFF   mov     eax, dword ptr [ebp-B8]
0015986A   40              inc     eax
0015986B   8985 48FFFFFF   mov     dword ptr [ebp-B8], eax
00159871   8B85 58FFFFFF   mov     eax, dword ptr [ebp-A8]
00159877   8B8D 48FFFFFF   mov     ecx, dword ptr [ebp-B8]
0015987D   3B48 02         cmp     ecx, dword ptr [eax+2]
00159880   73 1C           jnb     short 0015989E
00159882   8B45 E0         mov     eax, dword ptr [ebp-20]
```

```
003D0000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ? ...¦...ÿÿ..
003D0010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ?.......@.......
003D0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003D0030  00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00  ............?...
003D0040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ■■?.???L?Th
003D0050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
003D0060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS
003D0070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
003D0080  1D 75 60 44 59 14 0E 17 59 14 0E 17 59 14 0E 17  ■u`DY■■■Y■■■Y■■■
003D0090  50 6C 9B 17 5A 14 0E 17 59 14 0F 17 39 14 0E 17  Pl?Z■■■Y■■■9■■■
003D00A0  50 6C 9D 17 52 14 0E 17 CE 4A 0A 16 5B 14 0E 17  Pl?R■■■蜆.■[■■■
003D00B0  CE 4A 0B 16 44 14 0E 17 CB 4A 0D 16 5A 14 0E 17  蜆■■D■■■蕯.■Z■■■
003D00C0  CE 4A 0C 16 58 14 0E 17 52 69 63 68 59 14 0E 17  蜆.■X■■■RichY■■■
003D00D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003D00E0  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00  ........PE..L丞.
003D00F0  C8 94 8A 5C 00 00 00 00 00 00 00 00 E0 00 02 01  葦獎.........?丞
003D0100  0B 01 0E 00 00 00 01 00 00 82 00 00 00 00 00 00  ■丞■...丞.?.....
```

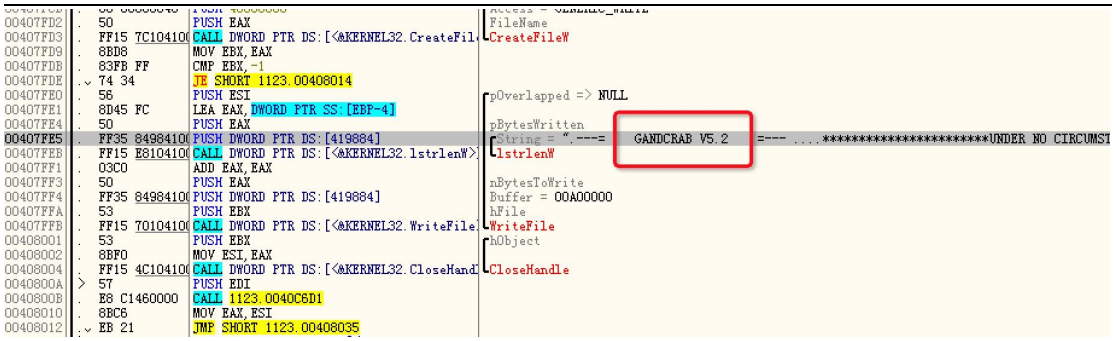
其 MD5:D1960357F97D64FB1339E44D90D09D47，对比第一次攻击样本文件在内存解密出来的文件 MD5：7AA1751726B3F25E695E40786187E451 的编译时间

- 2019-02-24 00:51:29　首次样本核心模块
- 2019-03-15 01:52:08　变种样本核心模块

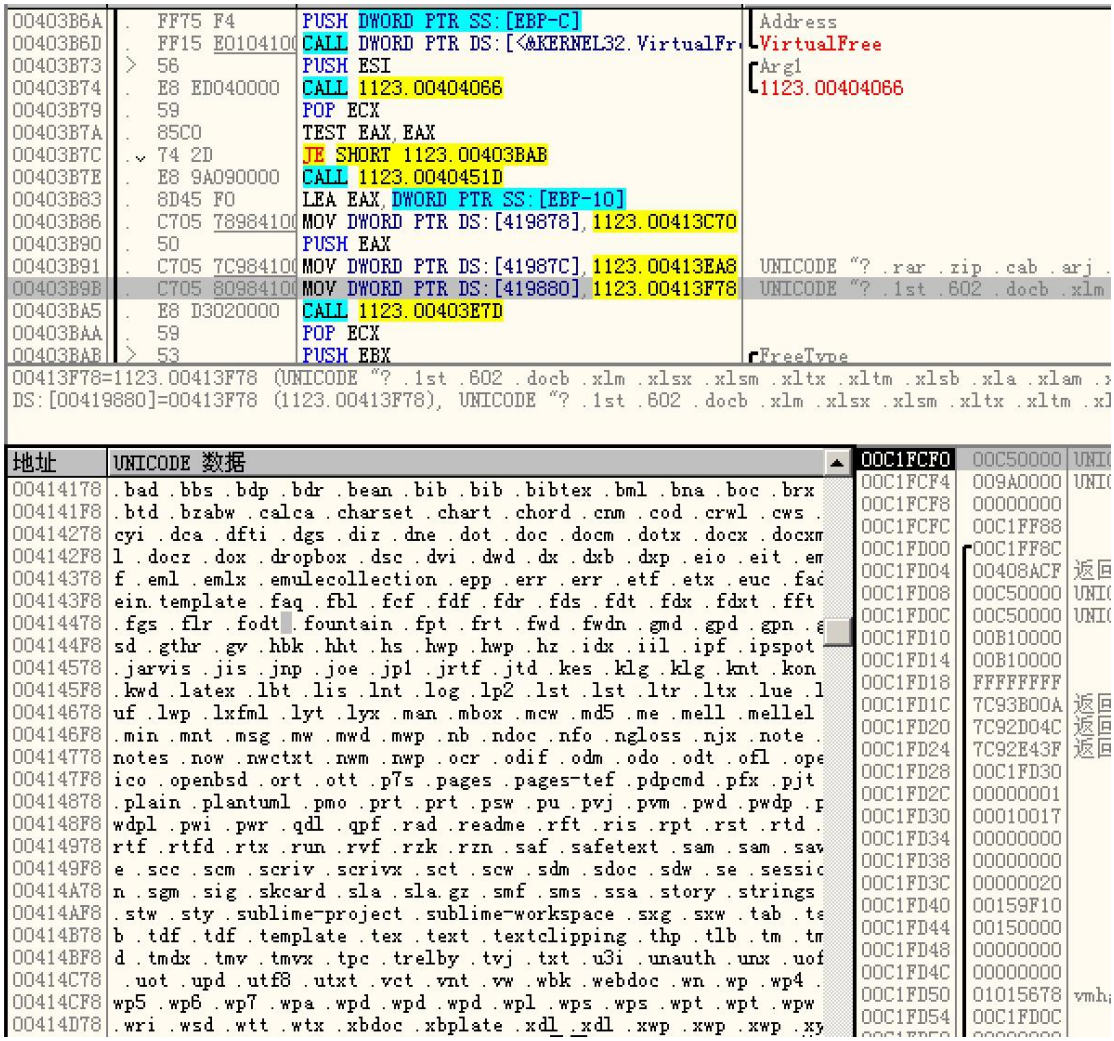
很明显这里的时间才是真实的攻击者开发时间，确定了外壳部分可能是人为修改或工具自动完成



在内存中明显发“GandCrab V5”字符串信息



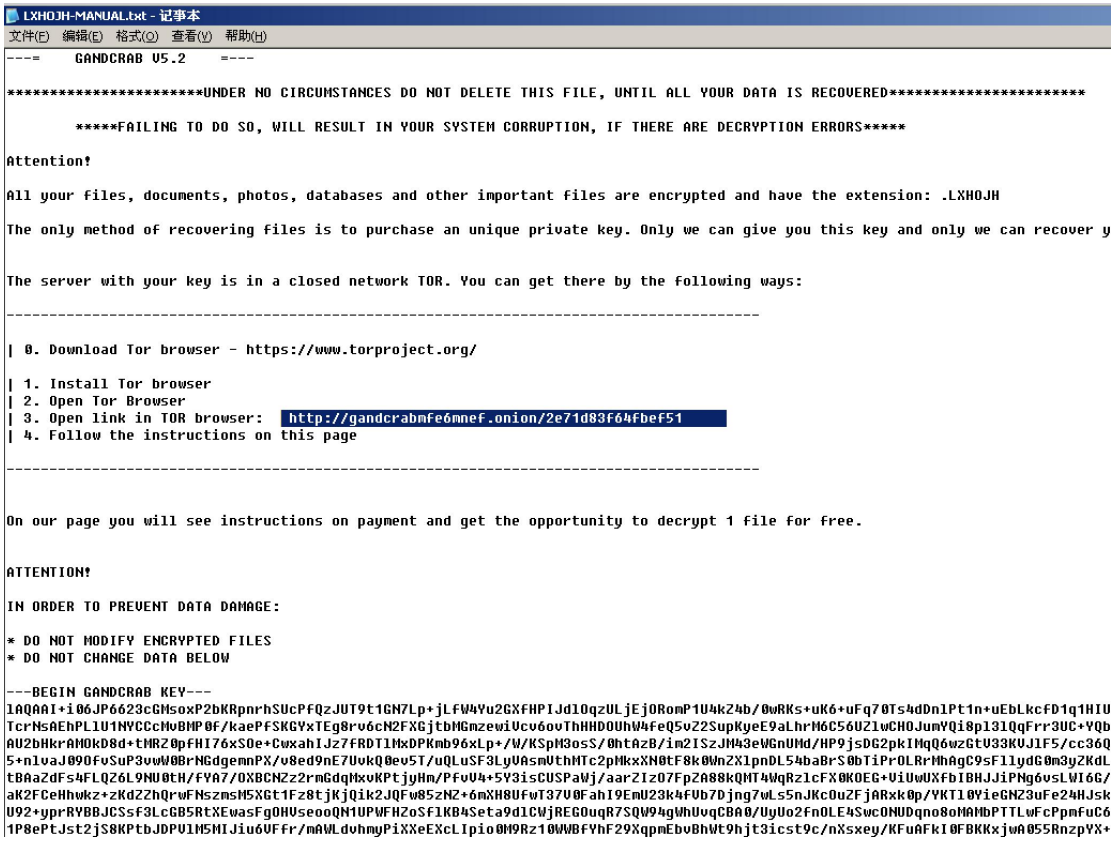
针对各种后缀文件进行加密，涉及对后缀名非常多。



该勒索软件加密的文本名称和后缀均为随机生成，勒索信息文本为固定格式{随机字符串}-MANUAL.txt

其中 Tor 节点如下

- hxxp://gandcrabmfe6mnef.onion/2e71d83f64fbef51



LXHOJH-MANUAL.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
---=    GANDCRAB V5.2    =---

**********************UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVERED**********************

        *****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS*****

Attention!

All your files, documents, photos, databases and other important files are encrypted and have the extension: .LXHOJH

The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover y


The server with your key is in a closed network TOR. You can get there by the following ways:

-------------------------------------------------------------------------------------------

| 0. Download Tor browser - https://www.torproject.org/

| 1. Install Tor browser
| 2. Open Tor Browser
| 3. Open link in TOR browser:  http://gandcrabmfe6mnef.onion/2e71d83f64fbef51
| 4. Follow the instructions on this page

-------------------------------------------------------------------------------------------


On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.


ATTENTION!

IN ORDER TO PREVENT DATA DAMAGE:

* DO NOT MODIFY ENCRYPTED FILES
* DO NOT CHANGE DATA BELOW

---BEGIN GANDCRAB KEY---
lAQAAI+i06JP6623cGMsoxP2bKRpnrhSUcPfQzJUT9t1GN7Lp+jLfW4Yu2GXfHPIJdlOqzULjEjORomP1U4kZ4b/0wRKs+uK6+uFq70Ts4dDnlPt1n+uEbLkcfD1q1HIU
TcrNsAEhPL1U1NYCCcMvBMP0f/kaePfSKGYxTEg8rv6cN2FXGjtbMGmzewiUcv6ovThHHDOUhW4feQ5vZ2SupKyeE9aLhrM6C56UZlwCHOJumYQi8p13lQqFrr3UC+YQb
AV2bHkrAMOkD8d+tMRZ0pfHI76xSOe+CwxahIJz7FRDTlMxDPKmb96xLp+/W/KSpM3osS/0htAzB/im2ISzJM43eWGnUMd/HP9jsDG2pkIMqQ6wzGtV33KVJlF5/cc36Q
5+nlvaJ09OfvSuP3vvW0BrNGdgemnPX/v8ed9nE7UvkQ0ev5T/uQLuSF3LyVAsmVthMTc2pMkxXN0tF8k0WnZX1pnDL54baBrS0bTiPrOLRrMhAgC9sF1lydG0m3yZKdL
tBAaZdFs4FLQ26L9NU0tH/fYA7/OXBCNZz2rmGdqMxvKPtjyHm/PfvV4+5Y3isCUSPaWj/aar2IzO7FpZA88kQMT4WqRzlcFX0KOEG+ViUwUXfbIBHJJiPNg6vsLWI6G/
aK2FCeHhwkz+zKdZ2hQrwFNszmsM5XGt1Fz8tjKjQik2JQFw85zNZ+6mXH8UfwT37V0FahI9EmU23k4fVb7Djng7wLs5nJKcOuZFjARxk0p/YKTl0YieGNZ3uFe24HJsk
U92+yprRYBBJCSsf3LcGB5RtXEwasFgOHVseooQN1UPWFHZoSflKB4Seta9dlCWjREGOuqR7SQW94gWhUvqCBA0/UyUo2fnOLE4SvcONUDqno8oMAMbPTTLwFcPpmfuC6
1P8ePtJst2jS8KPtbJDPV1M5MIJiu6VFfr/mAWLdvhmyPiXXeEXcLIpio0M9Rz10WWBfYhF29XqpmEbvBhWt9hjt3icst9c/nXsxey/KFuAFkI0FBKKxjwA055RnzpYX+
```

4. 建议

勒索病毒一旦感染主机会对珍贵数据进行加密并要求受害者支付赎金，在受害者支付赎金后仍有可能存在不可解密的风险，建议在关键信息基础设施所在单位部署网络安全态势感知系统，实时感知存在的网络安全威胁，加强网络防控能力；建议在关键信息基础设施服务器部署终端防护软件（EDR）、APT 预警平台等，都可有效防止勒索病毒感染与传播。