



## Buran 勒索病毒样本分析

### 目录

|    |                |   |
|----|----------------|---|
| 一、 | 样本概况 .....     | 2 |
| 二、 | 具体行为分析 .....   | 2 |
| 三、 | 清理病毒残留思路 ..... | 9 |

# 一、样本概况

SHA256: 5c1141aa7d0b9fba71822607f3b1b086e2cc4529e63221a9a6ede74fa366512f

该样本启动自身后，释放新的 PE 文件，通过 CreateProcessInternalW 创建系统假进程和通过 ShellExecuteExW 启动了一个隐藏界面的进程，并且在注册表设置该程序为自启动。通过 cmd 进程，根据参数的不同来执行不同的流程；在病毒运行前，进行了国家和地区的检查对比，特定的国家不运行该病毒程序。程序运行后删除系统的备份文件，同时删除自身。

# 二、具体行为分析

## 删除文件

|              |           |            |      |             |   |            |           |
|--------------|-----------|------------|------|-------------|---|------------|-----------|
| 15:52:50:546 | buran.exe | 4116:50... | 4116 | FILE_remove | C:\Users\15PB\AppData\Local\Temp\68299f59-buran           | 0x00000000 | [操作成功完成。] |
| 15:52:52:839 | cmd.exe   | 3466:56... | 4116 | FILE_remove | C:\Users\15PB\Desktop\buran\buran.exe                     | 0x00000000 | [操作成功完成。] |
| 15:53:12:979 | lsass.exe | 5696:26... | 4116 | FILE_remove | C:\Users\15PB\AppData\Local\Temp\68299f59-buran           | 0x00000000 | [操作成功完成。] |
| 15:56:43:385 | cmd.exe   | 956:4564   | 4116 | FILE_remove | C:\Users\15PB\AppData\Roaming\Microsoft\Windows\lsass.exe | 0x00000000 | [操作成功完成。] |

## 循环遍历系统中的文件并加密

| 时间           | 进程名         | 进程ID       | 任务组ID | 动作         | 路径  | 参数                                   | 结果                   |
|--------------|-------------|------------|-------|------------|---|--------------------------------------|----------------------|
| 15:52:47:832 | buran.exe   | 4116:50... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\B2F...  | offset:0x00000000 datalen:0x0000018C | 0x00000000 [操作成功完成。] |
| 15:52:48:144 | buran.exe   | 4116:20... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\07CE... | offset:0x00000000 datalen:0x00000070 | 0x00000000 [操作成功完成。] |
| 15:52:48:144 | buran.exe   | 4116:20... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Low\Microsoft\CryptnetUrlCache\Content\07CEF... | offset:0x00000000 datalen:0x000002D8 | 0x00000000 [操作成功完成。] |
| 15:52:48:144 | buran.exe   | 4116:50... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\07CE... | offset:0x00000000 datalen:0x0000018E | 0x00000000 [操作成功完成。] |
| 15:52:48:331 | buran.exe   | 4116:52... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\204...  | offset:0x00000000 datalen:0x00000070 | 0x00000000 [操作成功完成。] |
| 15:52:48:331 | buran.exe   | 4116:52... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Low\Microsoft\CryptnetUrlCache\Content\204C...  | offset:0x00000000 datalen:0x000001D7 | 0x00000000 [操作成功完成。] |
| 15:52:48:331 | buran.exe   | 4116:50... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\204...  | offset:0x00000000 datalen:0x00000196 | 0x00000000 [操作成功完成。] |
| 15:52:48:346 | buran.exe   | 4116:50... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Temp\Cab393C.tmp                                | offset:0x00000000 datalen:0x00000638 | 0x00000000 [操作成功完成。] |
| 15:52:48:346 | buran.exe   | 4116:50... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Temp\Tar393D.tmp                                | offset:0x00000000 datalen:0x00000800 | 0x00000000 [操作成功完成。] |
| 15:52:49:267 | buran.exe   | 4116:20... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\07CE... | offset:0x00000000 datalen:0x00000100 | 0x00000000 [操作成功完成。] |
| 15:52:49:267 | buran.exe   | 4116:52... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Low\Microsoft\CryptnetUrlCache\Content\204C...  | offset:0x00000000 datalen:0x00000100 | 0x00000000 [操作成功完成。] |
| 15:52:49:267 | buran.exe   | 4116:50... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\204...  | offset:0x00000000 datalen:0x00000100 | 0x00000000 [操作成功完成。] |
| 15:52:49:275 | buran.exe   | 4116:50... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Temp\68299f59-buran                             | offset:0x00000000 datalen:0x00000001 | 0x00000000 [操作成功完成。] |
| 15:52:50:577 | cmd.exe     | 5856:52... | 4116  | FILE_write | C:\Users\15PB\AppData\Roaming\Microsoft\Windows\lsass.exe                   | offset:0x00000000 datalen:0x00010000 | 0x00000000 [操作成功完成。] |
| 15:53:12:308 | lsass.exe   | 5696:26... | 4116  | FILE_write | C:\Users\15PB\AppData\Local\Temp\B2F1B8C43-buran                            | offset:0x00000000 datalen:0x00000001 | 0x00000000 [操作成功完成。] |
| 15:53:38:001 | wbadmin.exe | 4336:45... | 4116  | FILE_write | C:\Windows\Logs\WindowsBackup\Wbadmin.0.etl                                 | offset:0x00000000 datalen:0x00002800 | 0x00000000 [操作成功完成。] |
| 15:53:38:266 | wbadmin.exe | 5020:24... | 4116  | FILE_write | C:\Windows\Logs\WindowsBackup\Wbadmin.0.etl                                 | offset:0x00000000 datalen:0x00002800 | 0x00000000 [操作成功完成。] |
| 15:53:38:391 | wbadmin.exe | 4100:884   | 4116  | FILE_write | C:\Windows\Logs\WindowsBackup\Wbadmin.0.etl                                 | offset:0x00000000 datalen:0x00002800 | 0x00000000 [操作成功完成。] |
| 15:53:38:500 | wbadmin.exe | 5412:38... | 4116  | FILE_write | C:\Windows\Logs\WindowsBackup\Wbadmin.0.etl                                 | offset:0x00000000 datalen:0x00002800 | 0x00000000 [操作成功完成。] |
| 15:53:52:352 | lsass.exe   | 2436:61... | 4116  | FILE_write | D:\010 Editor\010Editor.idb   | offset:0x00000000 datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:365 | lsass.exe   | 6072:47... | 4116  | FILE_write | C:\Program Files\010 Editor\010Editor.news                                  | offset:0x00000005 datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:375 | lsass.exe   | 6072:47... | 4116  | FILE_write | C:\Program Files\010 Editor\010Editor.qhc                                   | offset:0x00000000 datalen:0x0000008C | 0x00000000 [操作成功完成。] |
| 15:53:52:377 | lsass.exe   | 6072:47... | 4116  | FILE_write | C:\Program Files\010 Editor\010Editor.qhc                                   | offset:0x0048C000 datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:427 | lsass.exe   | 6072:47... | 4116  | FILE_write | C:\Program Files\010 Editor\010Editor.qhc                                   | offset:0x00004400 datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:456 | lsass.exe   | 6072:47... | 4116  | FILE_write | C:\Program Files\010 Editor\010Editor.url                                   | offset:0x0000003E datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:465 | lsass.exe   | 6072:47... | 4116  | FILE_write | C:\Program Files\010 Editor\BuyNow.url                                      | offset:0x0000003A datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:477 | lsass.exe   | 6072:47... | 4116  | FILE_write | C:\Program Files\010 Editor\Changes.txt                                     | offset:0x0000012B datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:491 | lsass.exe   | 6072:47... | 4116  | FILE_write | C:\Program Files\010 Editor\file_id.diz                                     | offset:0x00000042 datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:509 | lsass.exe   | 6072:47... | 4116  | FILE_write | C:\Program Files\010 Editor\qhcrcm  | offset:0x00000018 datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:509 | lsass.exe   | 2436:61... | 4116  | FILE_write | D:\010 Editor\010 Editor\010Editor.news                                     | offset:0x00000000 datalen:0x0000008C | 0x00000000 [操作成功完成。] |
| 15:53:52:509 | lsass.exe   | 2436:61... | 4116  | FILE_write | D:\010 Editor\010 Editor\010Editor.qhc                                      | offset:0x00000060 datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:524 | lsass.exe   | 2436:61... | 4116  | FILE_write | D:\010 Editor\010 Editor.qhc  | offset:0x00476400 datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:540 | lsass.exe   | 2436:61... | 4116  | FILE_write | D:\010 Editor\010 Editor.qhc  | offset:0x00008000 datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:555 | lsass.exe   | 2436:61... | 4116  | FILE_write | D:\010 Editor\010 Editor.url  | offset:0x0000003E datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:571 | lsass.exe   | 2436:61... | 4116  | FILE_write | D:\010 Editor\BuyNow.url  | offset:0x0000003A datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:571 | lsass.exe   | 2436:61... | 4116  | FILE_write | D:\010 Editor\Changes.txt   | offset:0x0000012B datalen:0x00000003 | 0x00000000 [操作成功完成。] |
| 15:53:52:587 | lsass.exe   | 6072:47... | 4116  | FILE_write | C:\Program Files\010 Editor\Readme.txt                                      | offset:0x00000859 datalen:0x00000003 | 0x00000000 [操作成功完成。] |

这里有大量的文件遍历和写入操作，猜测应该是加密文件

## 设置注册表项

| 时间           | 进程名       | 进程ID       | 任务组ID | 动作         | 路径  | 参数   | 结果 |
|--------------|-----------|------------|-------|------------|---|--|----|
| 15:52:45:554 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\buran_RASAP32\Enable...   |  |    |
| 15:52:45:554 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\buran_RASAP32\Enable...   |  |    |
| 15:52:45:554 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\buran_RASAP32\FileTr...   |  |    |
| 15:52:45:554 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\buran_RASAP32\Cons...     |  |    |
| 15:52:45:554 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\buran_RASAP32\MaxFil...   |  |    |
| 15:52:45:554 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\buran_RASAP32\FileDir...  |  |    |
| 15:52:45:554 | buran.exe | 4116:60... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\buran_RASMANCS\Ena...     |  |    |
| 15:52:45:554 | buran.exe | 4116:60... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\buran_RASMANCS\Ena...     |  |    |
| 15:52:45:554 | buran.exe | 4116:60... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\buran_RASMANCS\File...    |  |    |
| 15:52:45:554 | buran.exe | 4116:60... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\buran_RASMANCS\Con...     |  |    |
| 15:52:45:554 | buran.exe | 4116:60... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\buran_RASMANCS\Ma...      |  |    |
| 15:52:45:554 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne...  |  |    |
| 15:52:45:554 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne...  |  |    |
| 15:52:45:570 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne...  |  |    |
| 15:52:45:570 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne...  |  |    |
| 15:52:47:816 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\2CAAF688...  |  |    |
| 15:52:47:816 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\2CAAF688...  |  |    |
| 15:52:47:816 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\2CAAF688...  |  |    |
| 15:52:47:816 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\2CAAF688...  |  |    |
| 15:52:47:816 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\2CAAF688...  |  |    |
| 15:52:47:816 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\2CAAF688...  |  |    |
| 15:52:47:816 | buran.exe | 4116:50... | 4116  | REG_setval | HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\2CAAF688...  |  |    |
| 15:52:50:593 | reg.exe   | 4448:756   | 4116  | REG_setval | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Loca... | type:0x00000001 data:134 data:"22... 0x00000000 [操作成功完成。]  |    |
| 15:52:50:733 | lsass.exe | 5696:26... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\lsass_RASAP32\Enable...   | type:0x00000004 data:4 data:"00 00... 0x00000000 [操作成功完成。] |    |
| 15:52:50:733 | lsass.exe | 5696:26... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\lsass_RASAP32\Enable...   | type:0x00000004 data:4 data:"00 00... 0x00000000 [操作成功完成。] |    |
| 15:52:50:733 | lsass.exe | 5696:26... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\lsass_RASAP32\FileTra...  | type:0x00000004 data:4 data:"00 00... 0x00000000 [操作成功完成。] |    |
| 15:52:50:733 | lsass.exe | 5696:26... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\lsass_RASAP32\Consol...   | type:0x00000004 data:4 data:"00 00... 0x00000000 [操作成功完成。] |    |
| 15:52:50:733 | lsass.exe | 5696:26... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\lsass_RASAP32\MaxFil...   | type:0x00000004 data:4 data:"00 00... 0x00000000 [操作成功完成。] |    |
| 15:52:50:733 | lsass.exe | 5696:26... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\lsass_RASAP32\FileDir...  | type:0x00000002 data:4 data:"25 7... 0x00000000 [操作成功完成。]  |    |
| 15:52:50:749 | lsass.exe | 5696:59... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\lsass_RASMANCS\Enabl...   | type:0x00000004 data:4 data:"00 00... 0x00000000 [操作成功完成。] |    |
| 15:52:50:749 | lsass.exe | 5696:59... | 4116  | REG_setval | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\lsass_RASMANCS\Enabl...   | type:0x00000004 data:4 data:"00 00... 0x00000000 [操作成功完成。] |    |

释放 PE 文件，修改注册表自启动项，删除病毒程序本体，启动自释放的文件。

| 时间           | 进程名       | 进程ID       | 任务组ID | 动作                   | 路径   | 参数                |
|--------------|-----------|------------|-------|----------------------|--|-------------------|
| 15:52:50:577 | cmd.exe   | 5856:52... | 4116  | BA_extract_pe        | C:\Users\15PB\AppData\Roaming\Microsoft\Windows\lsass.exe          |                   |
| 15:52:50:593 | reg.exe   | 4448:756   | 4116  | BA_register_autoran  | "C:\Users\15PB\AppData\Roaming\Microsoft\Windows\lsass.exe" -start | type:'Common/Run' |
| 15:52:50:680 | lsass.exe | 4116:50... | 4116  | BA_exe_extractedfile | C:\Users\15PB\AppData\Roaming\Microsoft\Windows\lsass.exe          |                   |
| 15:52:52:816 | cmd.exe   | 3464:56... | 4116  | BA_self_delete       | C:\Users\15PB\Desktop\buran.exe                                    |                   |
| 15:52:52:816 | lsass.exe | 5696:26... | 4116  | BA_exe_extractedfile | C:\Users\15PB\AppData\Roaming\Microsoft\Windows\lsass.exe          |                   |
| 15:52:52:816 | lsass.exe | 5696:26... | 4116  | BA_exe_extractedfile | C:\Users\15PB\AppData\Roaming\Microsoft\Windows\lsass.exe          |                   |
| 15:52:52:816 | lsass.exe | 5696:26... | 4116  | BA_exe_extractedfile | C:\Users\15PB\AppData\Roaming\Microsoft\Windows\lsass.exe          |                   |

## 勒索信中的内容

|   |               |
|---|---------------|
| !!! ALL YOUR FILES ARE ENCRYPTED !!!  | !!! 勒索信内容 !!! |
| 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)   | 勒索信内容         |
| ==== GERMAN ====  | 勒索信内容         |
| Alle Ihre Dateien, Dokumente, Fotos, Datenbanken und andere wichtige Dateien werden verschlüsselt.  | 勒索信内容         |
| Sie können es nicht selbst entschlüsseln! Die einzige Methode Zum Wiederherstellen von Dateien muss ein eindeutiger privater Schlüssel erworben werden. | 勒索信内容         |
| Nur wir können Ihnen diesen Schlüssel geben und nur wir können Ihre Dateien wiederherstellen.   | 勒索信内容         |
| Um sicher zu gehen, dass wir den Entschlüsseler haben und er funktioniert, können Sie einen senden  | 勒索信内容         |
| Senden Sie eine E-Mail an Wiederherstellung@cock.li oder Wiederherstellungsdatei@airmail.cc und entschlüsseln Sie eine Datei kostenlos.                 | 勒索信内容         |
| Aber diese Datei sollte nicht wertvoll sein!  | 勒索信内容         |
| Möchten Sie Ihre Dateien wirklich wiederherstellen?   | 勒索信内容         |
| Schreiben Sie eine E-Mail an Wiederherstellung@cock.li  | 勒索信内容         |
| Wiederherstellungsdatei@airmail.cc (reservieren)  | 勒索信内容         |
| Ihre persönliche ID: <- ID ->   | 勒索信内容         |
| Beachtung!  | 勒索信内容         |
| * Benennen Sie verschlüsselte Dateien nicht um.   | 勒索信内容         |
| * Versuchen Sie nicht, Ihre Daten mit Software von Drittanbietern zu entschlüsseln.   | 勒索信内容         |
| Dies kann zu dauerhaftem Datenverlust führen.   | 勒索信内容         |
| * Entschlüsselung Ihrer Dateien mit Hilfe von Dritten möglich   | 勒索信内容         |
| verursachen Sie erhöhten Preis (sie addieren ihre Gebühr zu unserem) oder Sie können Opfer eines Betrugs werden.  | 勒索信内容         |
| ==== ENGLISH ====   | 勒索信内容         |

打开 url: <http://geoiptool.com>, 对比国家和地区, 特定国家和地区不会发起攻击

|                     |  |   |                                  |  |   |                          |                           |
|---------------------|--|---|----------------------------------|--|---|--------------------------|---------------------------|
| 00B6835 50 PUSH EAX | 00B6836 E8 2DE0FEFF CALL <JMP.&wininet.InternetOpenUrlA> | 00B683B 8945 F8 MOV DWORD PTR SS:[EBP+0x8], EAX | 00B683E 33D2 XOR EDX, EDX        | 00B6840 55 PUSH EBP                            | 00B6841 68 F86BF000 PUSH buran.00BF6BF0 | EAX=00000000             | 堆栈 SS:[0014FE3C]=00000000 |
| 地址                  | HEX 数据   | ASCII   | 0014FE44 0014FE44 buran.00BF683B | 0014FE44 0014FE44 ASCII "http://geoiptool.com" | 0014FE44 0014FE44 指向下一个 SEH 记录的指针       | 0014FE44 0014FE44 SE处理程序 | 0014FE44 0014FE44         |



| 地址       | HEX 数据      | 反汇编                              | 注释                   | 寄存器 (FPU)                                    |
|----------|-------------|----------------------------------|----------------------|--|
| 00BF855D | E8 9611FFFF | CALL buran.00BE04F8              |                      | EAX 00629900 ASCII "lsass.exe"               |
| 00BF8562 | 8B55 00     | MOV EDI, DWORD PTR SS:[EBP-0x40] | Belorussia           | ECX 0060C058                                 |
| 00BF8565 | A1 30FABF00 | MOV EAX, DWORD PTR DS:[0xBFFA30] |                      | EDX 0060C000                                 |
| 00BF856A | E8 7DC5DFFF | CALL buran.00BD4AE0              |                      | EBX 7FFD0000                                 |
| 00BF856F | 74 38       | JE SHORT buran.00BF85A9          |                      | ESP 0014FE88                                 |
| 00BF8571 | 8D55 BC     | LEA EDI, DWORD PTR SS:[EBP-0x44] |                      | EBP 0014FF24                                 |
| 00BF8574 | D8 0389BF00 | MOV EAX, buran.00BF89F0          |                      | ESI 00000000                                 |
| 00BF8579 | E8 7A11FFFF | CALL buran.00BE96F8              |                      | EDI 00000000                                 |
| 00BF857E | 8B55 BC     | MOV EDI, DWORD PTR SS:[EBP-0x44] | Kazakhstan           | EIP 00BF8615 buran.00BF8615                  |
| 00BF8581 | A1 30FABF00 | MOV EAX, DWORD PTR DS:[0xBFFA30] |                      | 0 0 ES 0023 32位 0 (FFFFFFFF)                 |
| 00BF8586 | E8 61C5DFFF | CALL buran.00BD4AE0              |                      | P 1 GS 001B 32位 0 (FFFFFFFF)                 |
| 00BF858B | 74 10       | JE SHORT buran.00BF85A9          |                      | A 0 SS 0023 32位 0 (FFFFFFFF)                 |
| 00BF8590 | B8 F489BF00 | MOV EAX, buran.00BF89F4          |                      | Z 1 DS 0023 32位 0 (FFFFFFFF)                 |
| 00BF8595 | E8 5E11FFFF | CALL buran.00BE96F8              |                      | S 0 FS 003B 32位 7FFDF000 (FFF)               |
| 00BF859A | 8B55 BC     | MOV EDI, DWORD PTR SS:[EBP-0x48] | Russian Federation   | T 0 GS 0000 NULL                             |
| 00BF859D | A1 30FABF00 | MOV EAX, DWORD PTR DS:[0xBFFA30] |                      | D 0  |
| 00BF85A2 | E8 45C5DFFF | CALL buran.00BD4AE0              |                      | 0 0 LastErr ERROR_SUCCESS (00000000)         |
| 00BF85A7 | 75 0A       | JNZ SHORT buran.00BF85B3         | 判断程序运行的国家是否为上述的国家之一  | EFL 00000246 (NO, NB, E, BE, NS, PE, GE, LE) |
| 00BF85A9 | 68 9A020000 | PUSH 0x29A                       |                      | ST0 empty 0.0                                |
| 00BF85AE | E8 EDE2DFFF | CALL JMP, &kernel32.ExitProcess> | 如果是上述国家之一, 那么程序就直接退出 | ST1 empty 0.0                                |
| 00BF85B3 | E8 70B0FFFF | CALL buran.00BF3634              |                      | ST2 empty 0.0                                |
| 00BF85B8 | 8400        | TEST AL, AL                      |                      | ST3 empty 0.0                                |

| 地址       | HEX 数据      | 反汇编                              | 注释 | 寄存器 (FPU)                    |
|----------|-------------|----------------------------------|----|------------------------------|
| 00BF8612 | 8B 45 AC 50 | MOV EDI, DWORD PTR SS:[EBP-0x40] |    | EAX 00000000                 |
| 00BF8622 | FF 8B 45 AC | MOV EDI, DWORD PTR SS:[EBP-0x40] |    | ECX 00000000                 |
| 00BF8632 | E8 45 DF FF | CALL buran.00BF86F0              |    | EDX 00000000                 |
| 00BF8642 | FF A3 04 FA | MOV EAX, DWORD PTR DS:[0xBFFA04] |    | EBX 00000000                 |
| 00BF8652 | B2 01 A1 00 | MOV EDI, DWORD PTR SS:[EBP-0x40] |    | ESP 0014FE88                 |
| 00BF8662 | 00 A1 2C FA | MOV EAX, DWORD PTR DS:[0xBFFA2C] |    | ESI 00000000                 |
| 00BF8672 | E8 09 D4 FF | CALL buran.00BF86F0              |    | EDI 00000000                 |
| 00BF8682 | FF A3 28 FA | MOV EAX, DWORD PTR DS:[0xBFFA28] |    | EIP 00BF86B7 buran.00BF86B7  |
| 00BF8692 | A1 28 FA BF | MOV EAX, DWORD PTR DS:[0xBFFA28] |    | 0 0 ES 0023 32位 0 (FFFFFFFF) |
| 00BF86A2 | 00 E8 A8 B3 | MOV EAX, DWORD PTR DS:[0xBFFA00] |    | P 0 OS 001B 32位 0 (FFFFFFFF) |

添加自启动项服务, 调用 cmd 进程, 创建 lsass.exe 并添加自启动项 Local Security Authority Subsystem Service, 如下图:

|          |          |  |
|----------|----------|--|
| 0014FE14 | 00629A20 | ASCII "\ -start"                                     |
| 0014FE18 | 0023710C | UNICODE "\ -start"                                   |
| 0014FE1C | 005FDAB8 | ASCII "" /t REG_SZ /F /D ""                          |
| 0014FE20 | 0029FF8C | UNICODE "" /t REG_SZ /F /D ""                        |
| 0014FE24 | 0026EE7C | UNICODE "Local Security Authority Subsystem Service" |

| 地址                      | HEX 数据      | 反汇编                              | 注释     | 寄存器 (FPU)  |
|-------------------------|-------------|----------------------------------|--------|--|
| 00BF6D73                | E8 24E3DFFF | CALL buran.00BD509C              |        | EAX 0025C390 UNICODE "C:\Users\15BP\AppData\Roaming\LM |
| 00BF6D78                | 8D45 90     | LEA EAX, DWORD PTR SS:[EBP-0x70] |        | ECX 00000003   |
| 00BF6D7B                | E8 64C6FFFF | CALL buran.00BF33E4              |        | EDX 002370E4 UNICODE "-start"                          |
| 00BF6D80                | 8B45 90     | MOV EAX, DWORD PTR SS:[EBP-0x70] |        | EBX 7FFD0000   |
| 00BF6D83                | 33C9        | XOR ECX, ECX                     |        | ESP 0014FE44   |
| 00BF6D85                | 8B55 00     | MOV EDI, DWORD PTR SS:[EBP-0x10] | 添加自启动项 | EBP 0014FE88   |
| 00BF6D88                | E8 BF1CFFFF | CALL buran.00BE8A60              |        | ESI 00000000   |
| 00BF6D90                | 8B45 EC     | MOV EAX, DWORD PTR SS:[EBP-0x14] |        | EDI 00000000   |
| 00BF6D93                | E8 9B1EFFFF | CALL buran.00BE8C30              |        | EIP 00BF6D87 buran.00BF6D87                            |
| 00BF6D95                | 8400        | TEST AL, AL                      |        | 0 0 ES 0023 32位 0 (FFFFFFFF)                           |
| 00BF6D97                | 74 27       | JE SHORT buran.00BF6D00          |        | P 0 OS 001B 32位 0 (FFFFFFFF)                           |
| 00BF6D99                | 8D55 B8     | LEA EDI, DWORD PTR SS:[EBP-0x78] |        | A 1 SS 0023 32位 0 (FFFFFFFF)                           |
| 00BF6DA0                | B8 0270BF00 | MOV EAX, buran.00BF70AC          |        | Z 0 DS 0023 32位 0 (FFFFFFFF)                           |
| 00BF6DA1                | E8 5229FFFF | CALL buran.00BE96F8              |        | S 0 FS 003B 32位 7FFDF000 (FFF)                         |
| 00BF6DA6                | 8B55 B8     | MOV EDI, DWORD PTR SS:[EBP-0x78] |        | T 0 GS 0000 NULL                                       |
| 00BF6DA9                | 8D45 80     | LEA EAX, DWORD PTR SS:[EBP-0x74] |        | D 0  |
| 00BF6DAD                | E8 EF1FDFFF | CALL buran.00BD4FA0              |        | 0 0 LastErr ERROR_SUCCESS (00000000)                   |
| 00BF6DB1                | 8B55 B0     | MOV EDI, DWORD PTR SS:[EBP-0x74] |        | EFL 00000212 (NO, NB, NE, A, NS, PO, GE, G)            |
| 00BF6DB4                | 8B45 EC     | MOV EAX, DWORD PTR SS:[EBP-0x14] |        | ST0 empty 0.0  |
| 00BF6DB7                | E8 BF0FFFFF | CALL buran.00BF6AA4              |        | ST1 empty 0.0  |
| 00BF6DBD                | C645 EB 01  | MOV BYTE PTR SS:[EBP-0x15], 0x1  |        | ST2 empty 0.0  |
| 00BF6DC0                | 3300        | XOR EAX, EAX                     |        | ST3 empty 0.0  |
| 00BF6DC2                | 5A          | POP EDI                          |        | ST4 empty -8.1809127579924311200e+18                   |
| 00BE8A40-buran.00BE8A40 |             |                                  |        | ST5 empty -1.119945650323486220e+18                    |

| 地址       | HEX 数据      | 反汇编                              | 注释 | 寄存器 (FPU)                    |
|----------|-------------|----------------------------------|----|------------------------------|
| 00BF8A94 | DC 8F 16 08 | MOV EDI, DWORD PTR SS:[EBP-0x40] |    | EAX 7FFD0000                 |
| 00BF8A97 | 37 EE 39 2A | MOV EAX, DWORD PTR DS:[0xBFFA39] |    | ESP 0014FE44                 |
| 00BF8AB4 | 07 17 06 06 | MOV EAX, DWORD PTR DS:[0xBFFA07] |    | EBP 0014FE88                 |
| 00BF8AC4 | 01 EC F9 24 | MOV EAX, DWORD PTR DS:[0xBFFA01] |    | ESI 00000000                 |
| 00BF8AD4 | EF 2E 64 39 | MOV EAX, DWORD PTR DS:[0xBFFA0E] |    | EDI 00000000                 |
| 00BF8AE4 | 3F 00 4E 00 | MOV EAX, DWORD PTR DS:[0xBFFA3F] |    | EIP 00BF8A97 buran.00BF8A97  |
| 00BF8AF4 | 71 A9 19 4E | MOV EAX, DWORD PTR DS:[0xBFFA71] |    | 0 0 ES 0023 32位 0 (FFFFFFFF) |
| 00BF8B04 | 80 4F 49 04 | MOV EAX, DWORD PTR DS:[0xBFFA80] |    | P 0 OS 001B 32位 0 (FFFFFFFF) |
| 00BF8B14 | 08 66 2D 10 | MOV EAX, DWORD PTR DS:[0xBFFA08] |    | A 1 SS 0023 32位 0 (FFFFFFFF) |
| 00BF8B24 | 5B 14 B4 00 | MOV EAX, DWORD PTR DS:[0xBFFA5B] |    | Z 0 DS 0023 32位 0 (FFFFFFFF) |

退出当前进程并删除执行目录下的病毒文件:

| 地址       | HEX 数据      | 反汇编                              | 注释 | 寄存器 (FPU)  |
|----------|-------------|----------------------------------|----|--|
| 00BF657C | 55          | PUSH EBP                         |    | EAX 00000000   |
| 00BF657D | 8BEC        | MOV EBP, ESP                     |    | ECX 00000000   |
| 00BF657F | B9 06000000 | MOV ECX, 0x6                     |    | EDX 00604E60 ASCII "c for /l %x in (1,1,999) do (ping -n 3 127.1 & del " |
| 00BF6584 | 6A 00       | PUSH 0x0                         |    | EBX 7FFD0000   |
| 00BF6586 | 6A 00       | PUSH 0x0                         |    | ESP 0014FE44   |
| 00BF6588 | 49          | DEC ECX                          |    | EBP 0014FE88   |
| 00BF6589 | 75 F9       | JNZ SHORT buran.00BF6584         |    | ESI 00000000   |
| 00BF658B | 3300        | XOR EAX, EAX                     |    | EDI 00000000   |
| 00BF658D | 55          | PUSH EBP                         |    | EIP 00BF65A9 buran.00BF65A9  |
| 00BF658E | 68 0066BF00 | PUSH buran.00BF6600              |    | 0 0 ES 0023 32位 0 (FFFFFFFF)   |
| 00BF6593 | 64 FF30     | PUSH DWORD PTR FS:[EAX]          |    | P 1 GS 001B 32位 0 (FFFFFFFF)   |
| 00BF6596 | 64 8920     | MOV DWORD PTR FS:[EAX], ESP      |    | A 0 SS 0023 32位 0 (FFFFFFFF)   |
| 00BF6599 | 8D55 F4     | LEA EDI, DWORD PTR SS:[EBP-0x6]  |    | Z 1 DS 0023 32位 0 (FFFFFFFF)   |
| 00BF659C | B8 D466BF00 | MOV EAX, buran.00BF66D4          |    | S 0 FS 003B 32位 7FFDF000 (FFF)   |
| 00BF65A1 | E8 5231FFFF | CALL buran.00BE96F8              |    | T 0 GS 0000 NULL   |
| 00BF65A6 | 8B55 F4     | MOV EDI, DWORD PTR SS:[EBP-0x6]  |    | D 0  |
| 00BF65A9 | 8D45 F8     | LEA EAX, DWORD PTR SS:[EBP-0x8]  |    | 0 0 LastErr ERROR_SUCCESS (00000000)                                     |
| 00BF65AB | E8 EFE9DFFF | CALL buran.00BD4FA0              |    | EFL 00000246 (NO, NB, E, BE, NS, PE, GE, LE)                             |
| 00BF65B1 | FF75 F8     | PUSH DWORD PTR SS:[EBP-0x8]      |    | ST0 empty 0.0  |
| 00BF65B4 | 8D55 F0     | LEA EDI, DWORD PTR SS:[EBP-0x10] |    | ST1 empty 0.0  |
| 00BF65B7 | 3300        | XOR EAX, EAX                     |    | ST2 empty 0.0  |
| 00BF65B9 | E8 2A28FFFF | CALL buran.00BE8DE8              |    | ST3 empty 0.0  |
| 00BF65BC | FF75 F0     | PUSH DWORD PTR SS:[EBP-0x10]     |    | ST4 empty 0.0  |

```

00BF6630 8B55 D0 MOV EDX, DWORD PTR SS:[EBP-0x30]
00BF663F 8D45 D4 LEA EAX, DWORD PTR SS:[EBP-0x20]
00BF6642 E8 59E9DFF CALL buran.00BD4FA0
00BF6647 8B45 D4 MOV EAX, DWORD PTR SS:[EBP-0x20]
00BF664A E8 61E9DFF CALL buran.00BD4FB0
00BF664F 50 PUSH EAX
00BF6650 6A 00 PUSH 0x0
00BF6652 E8 004FEFF CALL <JMP.&shell32.ShellExecuteW>
00BF6657 6A 00 PUSH 0x0
00BF6659 E8 4202FEFF CALL <JMP.&kernel32.ExitProcess>
00BF665E 33C0 XOR EAX, EAX
00BD6B54 <JMP.&shell32.ShellExecuteW>

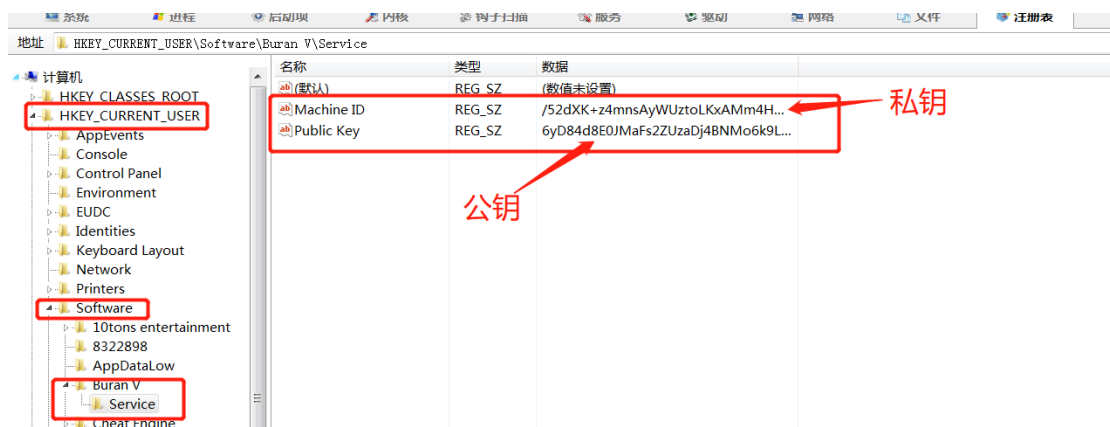
A 0 SS 0023 32位 0 (FFFFFFFF)
Z 0 DS 0023 32位 0 (FFFFFFFF)
S 0 FS 003B 32位 7FFDF000 (FFF)
T 0 GS 0000 NULL
D 0
0 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO, NB, NE, A, NS, PO, GE, G)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 4.3954422017120149680e+18
ST5 empty -8.4791934852591962390e+18
ST6 empty 6.0622383608932193440e+18

hWnd = NULL
Operation = "open"
FileName = "C:\Windows\system32\cmd.exe"
Parameters = "/o for /i %x in (1,1,999) do ( ping -n 3 127.1 & del "C:\Users\15PB\Desktop\buran\buran.exe" & if not exist "C:\Users\15PB\Desktop\buran\buran"
DefDir = NULL
IsShown = 0x0
指向下一个 SEH 记录的指针
SE处理程序
ASCII "open"
UNICODE "open"

```

生成对用户文件加密的公钥和私钥：

病毒程序为当前用户生成一对 RSA 私钥和私钥，其中私钥通过攻击者 RSA 公钥处理并 base64 编码后放入注册表。如下图：



```

lea edx, [ebp+var_9C]
mov eax, [ebp+var_4]
call sub_419660 ; RC4加密
mov eax, [ebp+var_9C]
lea edx, [ebp+var_98]
call sub_416FC0 ; base64加密
mov edx, [ebp+var_98]
lea eax, [ebp+var_4]
call sub_404780 ; RC4解密
lea edx, [ebp+var_A0]
mov eax, [ebx+24h]
call sub_419660 ; base64加密
mov eax, [ebp+var_A0]
lea edx, [ebp+var_8]
call sub_416FC0 ; RC4解密
lea edx, [ebp+var_A4]
mov eax, offset dword_422248
call sub_4196F8
mov edx, [ebp+var_A4]
mov ecx, [ebp+var_4]
mov eax, 80000001h
call sub_416970 ; 公钥
lea edx, [ebp+var_A8]
mov eax, offset dword_422294
call sub_4196F8

```

删除备份的文件和日志，首先进行提权操作，如下图：

```

sub_404B44(a2);
u8 = &savedregs;
u7 = &loc_418868;
u6 = __readfsdword(0);
__writefsdword(0, (unsigned int)&u6);
u2 = 0;
u3 = GetCurrentProcess(); // 获得当前进程
if ( OpenProcessToken(u3, 0x20u, &TokenHandle) )// 进行提权相关的操作
{
    NewState.PrivilegeCount = 1;
    u4 = (const CHAR *)sub_404B54();
    LookupPrivilegeValueA(0, u4, (PLUID)NewState.Privileges);// 查看进程的权限
    if ( u12 )
        NewState.Privileges[0].Attributes = 2;
    else
        NewState.Privileges[0].Attributes = 2147483648;
    AdjustTokenPrivileges(TokenHandle, 0, &NewState, 0x10u, 0, &ReturnLength);// 提权
    if ( !GetLastError() )
        LOBYTE(u2) = 1;
    CloseHandle(TokenHandle); |
}
__writefsdword(0, u6);
sub_4046E8(&loc_41886F);
return u2;
}

```

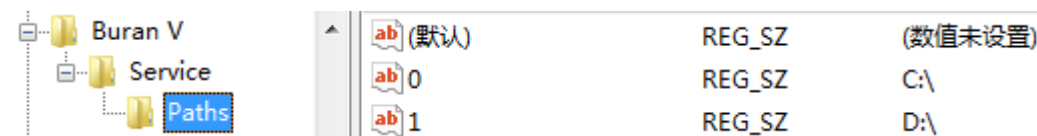
在高权限的情况下，调用 cmd 执行命令，实现备份数据的删除，禁用系统开机自动修复，清空注册表记录，清空系统日志，禁用事件记录。如下图：

```

.text:00425AF2 loc_425AF2: ; CODE XREF: sub_425A80+FF↓j
.text:00425AF2 lea     eax, [ebp+var_C]
.text:00425AF5 mov     edx, [ebp+var_4]
.text:00425AF8 movzx   edx, byte ptr [edx+ebx-1]
.text:00425AFD call    sub_4048D0
.text:00425B02 mov     eax, [ebp+var_C]
.text:00425B05 push    eax
.text:00425B06 lea     edx, [ebp+var_10]
.text:00425B09 mov     eax, offset dword_425F14
.text:00425B0E call    sub_4196F8 ; 解密字符串
.text:00425B13 mov     edx, [ebp+var_10]
.text:00425B16 pop     eax
.text:00425B17 call    sub_404AEC ; 0:相等 ; 1:不相等
.text:00425B17 jnz     short loc_425B62
.text:00425B1C lea     edx, [ebp+var_18]
.text:00425B21 mov     eax, offset nullsub_3
.text:00425B26 call    sub_4196F8
.text:00425B2B lea     eax, [ebp+var_18]
.text:00425B2E mov     edx, [ebp+var_8]
.text:00425B31 call    sub_404990
.text:00425B36 mov     edx, [ebp+var_18]
.text:00425B39 lea     eax, [ebp+var_14]
.text:00425B3C call    sub_404FA0
.text:00425B41 mov     eax, [ebp+var_14]
.text:00425B44 push    eax
.text:00425B45 lea     eax, [ebp+var_1C]
.text:00425B48 call    sub_4233E4
.text:00425B4D mov     eax, [ebp+var_1C]
.text:00425B50 xor     ecx, ecx
.text:00425B52 pop     edx

```

Buran 通过 WNetResourceW 等相关系统 API 枚举可访问的网络资源，记录本地磁盘中并将所有资源写入注册表项 HKCU\\Software\\Buran V\\Service\\Paths，键值为资源根目录名。如下图：



```

.text:00428759 loc_428759:                                ; CODE XREF: .text:004287AA↓j
.text:00428759     lea     edx, [ebp-74h]
.text:0042875C     mov     eax, offset byte_428B30 ; 参数
.text:00428761     call    sub_4196F8             ; R04 字符串解密
.text:00428766     lea     eax, [ebp-74h]
.text:00428769     push    eax
.text:0042876A     lea     edx, [ebp-78h]
.text:0042876D     mov     eax, esi
.text:0042876F     call    sub_407F6C
.text:00428774     mov     edx, [ebp-78h]
.text:00428777     pop     eax
.text:00428778     call    sub_404990
.text:0042877D     mov     edx, [ebp-74h]
.text:00428780     lea     eax, [ebp-70h]
.text:00428783     call    sub_404FA0
.text:00428788     mov     eax, [ebp-70h]
.text:0042878B     push    eax
.text:0042878C     lea     edx, [ebp-7Ch]
.text:0042878F     xor     eax, eax
.text:00428791     call    sub_418DE8
.text:00428796     mov     eax, [ebp-7Ch]
.text:00428799     mov     cx, 1
.text:0042879D     pop     edx
.text:0042879E     call    sub_418B4C
.text:004287A3     mov     [edi], eax
.text:004287A5     inc     esi
.text:004287A6     add     edi, 4
.text:004287A9     dec     ebx
.text:004287AA     jnz     short loc_428759
.text:004287AC     loc_4287AC:                                ; CODE XREF: .text:0042874F↑j
.text:004287AC     mov     ebx, esi

```

通过 cmd 参数 -start 运行进程等待新创建的加密子进程执行完毕后，在桌面创建勒索信息提示文件，使用记事本 notepad.exe 打开文件以提示用户，最后自我删除退出。

```

.text:004287E3     call    sub_4222D8
.text:004287E8     lea     edx, [ebp-84h]
.text:004287EE     xor     eax, eax
.text:004287F0     call    sub_418920             ; 获得桌面路径
.text:004287F5     mov     edx, [ebp-84h]
.text:004287FB     mov     cl, 1
.text:004287FD     mov     eax, ds:dword_42FA2C
.text:00428802     call    sub_42542C             ; 打开记事本
.text:00428807     mov     al, 1
.text:00428809     call    sub_42657C             ; 退出进程
.text:0042880E ; -----
.text:0042880E     xor     eax, eax
.text:00428810     pop     edx
.text:00428811     pop     ecx
.text:00428812     pop     ecx
.text:00428813     mov     fs:[eax], edx
.text:00428816     push    offset loc_4288A7
.text:0042881B     loc_42881B:                                ; CODE XREF: .text:004288A2↓j
.text:0042881B     lea     eax, [ebp-84h]

```

文件的加密：

病毒程序对本地资源和局域网资源文件加密；在对本地资源进行加密时，搜索判断文件资源所在的目录，对于用户浏览器需要用到的资源不加密，而在网络资源加密则是通过文件名的后缀来进程加密的。

```

.text:004284C2      call     sub_4196F8
.text:004284C7      mov     edx, [ebp-34h]
.text:004284CA      lea     eax, [ebp-30h]
.text:004284CD      call    sub_404FA0
.text:004284D2      mov     edx, [ebp-30h]
.text:004284D5      pop     eax
.text:004284D6      call    sub_4050E4
.text:004284DB      jnz     short loc_4284F5 ; 本地文件
.text:004284DD      push    1
.text:004284DF      mov     ecx, ds:dword_4304A0
.text:004284E5      mov     dl, 1
.text:004284E7      mov     eax, ds:off_425968
.text:004284EC      call    sub_4259D8
.text:004284F1      mov     ebx, eax
.text:004284F3      jmp     short loc_42850B ; 网络文件
.text:004284F5      ; -----
.text:004284F5      loc_4284F5:                                ; CODE XREF: .text:004284DB↑j
.text:004284F5      push    0
.text:004284F7      mov     ecx, ds:dword_4304A0
.text:004284FD      mov     dl, 1
.text:004284FF      mov     eax, ds:off_425968
.text:00428504      call    sub_4259D8
.text:00428509      mov     ebx, eax
.text:0042850B      loc_42850B:                                ; CODE XREF: .text:004284F3↑j
.text:0042850B      mov     eax, ebx
.text:0042850D      call    sub_414554
.text:00428512      push    0FFFFFFFh
.text:00428514      mov     eax, [ebx+4]
.text:00428517      push    eax
.text:00428518      call    WaitForSingleObject
.text:0042851D      loc_42851D:                                ; CODE XREF: .text:004284AF↑j
.text:0042851D      push    0

```

|          |               |                                   |            |
|----------|---------------|-----------------------------------|------------|
| 00422E11 | 8BD0          | MOV EDX, EAX                      |            |
| 00422EE3 | 8B8D 24FDFFFF | MOV ECX, DWORD PTR SS:[EBP-0x2DC] |            |
| 00422EE9 | 8B45 F0       | MOV EAX, DWORD PTR SS:[EBP-0x10]  |            |
| 00422EEC | E8 AB47FFFF   | CALL <buran.WriteFile>            | 加密后的内容写入文件 |
| 00422EF1 | 8D45 E0       | LEA EAX, DWORD PTR SS:[EBP-0x20]  |            |
| 00422EF4 | 50            | PUSH EAX                          |            |
| 00422EF5 | 8D85 E8FCFFFF | LEA EAX, DWORD PTR SS:[EBP-0x318] |            |
| 00422EFB | 8B4D F8       | MOV ECX, DWORD PTR SS:[EBP-0x8]   |            |
| 00422EFE | 8B55 FC       | MOV EDX, DWORD PTR SS:[EBP-0x4]   |            |
| 00422F01 | E8 D61AFEFF   | CALL buran.004049DC               |            |
| 00422F06 | 8B85 E8FCFFFF | MOV EAX, DWORD PTR SS:[EBP-0x318] |            |
| 00422F0C | 8B55 F4       | MOV EDX, DWORD PTR SS:[EBP-0xC]   |            |
| 00422F0F | 8D4A 0C       | LEA ECX, DWORD PTR DS:[EDX+0xC]   |            |
| 00422F12 | 8B55 F4       | MOV EDX, DWORD PTR SS:[EBP-0xC]   |            |
| 00422F15 | 83C2 14       | ADD EDX, 0x14                     |            |
| 00422F18 | E8 4FE3FFFF   | CALL buran.0042126C               | RSA加密      |
| 00422F1D | 8D95 E4FCFFFF | LEA EAX, DWORD PTR SS:[EBP-0x31C] |            |
| 00422F23 | 8B45 E0       | MOV EAX, DWORD PTR SS:[EBP-0x20]  |            |
| 00422F26 | E8 3567FEFF   | CALL <buran.EncodeFile>           |            |

|          |               |                                  |                |
|----------|---------------|----------------------------------|----------------|
| 00421288 | 8945 FC       | MOV DWORD PTR SS:[EBP-0x4], EAX  |                |
| 0042128B | 8B45 FC       | MOV EAX, DWORD PTR SS:[EBP-0x4]  |                |
| 0042128E | E8 B138FEFF   | CALL buran.00404B44              |                |
| 00421293 | 8D45 E8       | LEA EAX, DWORD PTR SS:[EBP-0x18] |                |
| 00421296 | 8B15 0CED4100 | MOV EDX, DWORD PTR DS:[0x41EDCC] | buran.0041EDD0 |
| 0042129C | E8 C73FEFF    | CALL buran.00405268              |                |
| 004212A1 | 8D45 E0       | LEA EAX, DWORD PTR SS:[EBP-0x20] |                |
| 004212A4 | 8B15 0CED4100 | MOV EDX, DWORD PTR DS:[0x41EDCC] | buran.0041EDD0 |
| 004212AA | E8 B93FEFF    | CALL buran.00405268              |                |
| 004212AF | 8D45 D8       | LEA EAX, DWORD PTR SS:[EBP-0x28] |                |
| 004212B2 | 8B15 0CED4100 | MOV EDX, DWORD PTR DS:[0x41EDCC] | buran.0041EDD0 |
| 004212B8 | E8 AB3FEFF    | CALL buran.00405268              |                |
| 004212BD | 8D45 D0       | LEA EAX, DWORD PTR SS:[EBP-0x30] |                |
| 004212C0 | 8B15 0CED4100 | MOV EDX, DWORD PTR DS:[0x41EDCC] | buran.0041EDD0 |
| 004212C6 | E8 9D3FEFF    | CALL buran.00405268              |                |
| 004212CB | 33C0          | XOR EAX, EAX                     |                |
| 004212CD | 55            | PUSH EBP                         |                |

|          |               |                                     |    |
|----------|---------------|-------------------------------------|----|
| 00405250 | 8500          | TEST EAX, EAX                       |    |
| 0040525E | 0F84 88FBFFFF | JG buran.00404DEC                   |    |
| 00405264 | 8902          | MOV DWORD PTR DS:[EDX], EAX         |    |
| 00405266 | 03            | RET                                 |    |
| 00405267 | 90            | NOP                                 |    |
| 00405268 | 3109          | XOR ECX, ECX                        | 加密 |
| 0040526A | 53            | PUSH EDX                            |    |
| 0040526B | 8A4A 01       | MOV CL, BYTE PTR DS:[EDX+0x1]       |    |
| 0040526E | 56            | PUSH ESI                            |    |
| 0040526F | 57            | PUSH EDI                            |    |
| 00405270 | 89C3          | MOV EBX, EAX                        |    |
| 00405272 | 8D7411 0A     | LEA ESI, DWORD PTR DS:[ECX+EDX+0xA] |    |
| 00405276 | 8B7C11 06     | MOV EDI, DWORD PTR DS:[ECX+EDX+0x6] |    |
| 0040527A | 8B14          | MOV EDI, DWORD PTR DS:[ESI]         |    |



### 三、清理病毒残留思路

1. 杀死进程 C:\Windows\System32\cmd.exe

2. 删除自启动注册表项

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\Local Security Authority Subsystem Service

3. 删除文件

"%HOMEPATH%\AppData\Roaming\Microsoft\Windows\lsass.exe" -start

"C:\Windows\system32\cmd.exe" /C bcdedit /set {default} bootstatuspolicy ignoreallfailures

bcdedit /set {default} bootstatuspolicy ignoreallfailures

%HOMEPATH%\AppData\Local\Temp\C46E9A24.buran

%HOMEPATH%\AppData\Local\Temp\58AE9100.buran

bcdedit /set {default} recoveryenabled no

4. 恢复注册表值

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\D1EB23A46D17D68FD92564C2F1F1601764D8E349\Blob