安全威胁每周警讯

2020/03/23～2020/03/29

本周威胁指数

亚信安全 网络安全监控中心

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	PE_RAMNIT.DEN	File infector	★	↑	该文件感染程序执行删除的文件。结果，被删除文件的恶意例程会显示在受影响的系统上。
2	Trojan.ALS.BURSTED.AA	Trojan	★	↓	用于 AutoCAD 使用的脚本语言，用于在 AutoCAD 启动时加载的脚本。
3	WORM_WCRY.F	Worm	★★★	↓	挖矿病毒，通过其他恶意软件感染。
4	ALS_DUXFAS.K	Trojan	★	→	该木马可能会与恶意软件包捆绑在一起作为恶意软件组件。
5	Ransom_WCRY.THAOBFJ	Worm	★★★	↓	勒索病毒，通过其他恶意软件感染。
6	LNK_DORKBOT.SM1	Trojan	★	↑	木马病毒，它可能是使用者手动安装的
7	HTML_RAMNIT.SM	Trojan	★★★	↑	此特洛伊木马执行已删除的文件。在受影响的系统上显示已删除文件的恶意例程
8	TROJ_EQUATED.J	Trojan	★★	↑	此特洛伊木马可能与恶意软件包捆绑 在一起作为恶意软件组件。它作为被 其他恶意软件丢弃的文件或用户在访 问恶意站点时在不知不觉中下载的文 件到达系统。它可以由用户手动安装。
9	Worm.Win32.OTORUN.NKLSFG	Worm	★★	↑	蠕虫病毒，通过其他恶意软件感染。
10	Coinminer_TOOLXMR.E-WIN32	Coinminer	★★	→	挖矿病毒，可能是和其他病毒一并下载，需要运行在一些特殊的参数环境中

AsiaInfo | 亚信安全

病毒通告

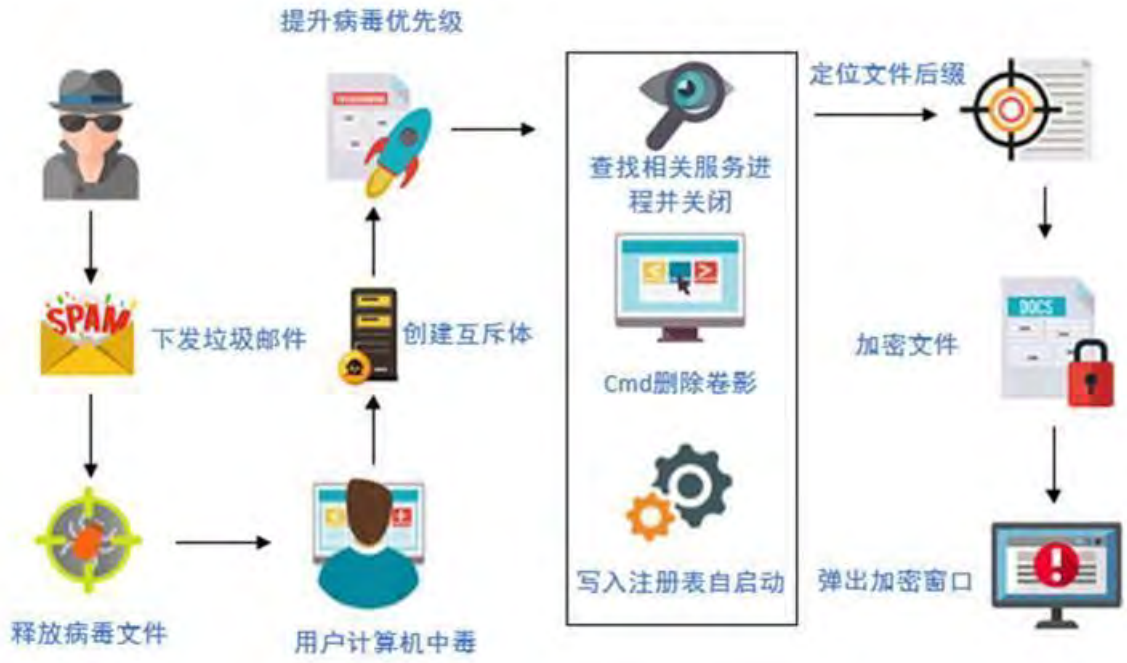
2020 年 3 月 27 日

海盗王勒索病毒通告

事件描述

近日，亚信安全截获新型海盗王勒索病毒，该病毒的勒索界面中有海盗图标，因此得名。经过分析，我们发现该病毒为 CRYSIS 勒索家族的最新变种文件，其通过垃圾邮件附件传播，加密磁盘中的文件，加密后的文件扩展名为 id-XXXXXX.wang_team888@aol.com.ROGER，亚信安全将其命名为 Ransom.Win32.CRYSIS.SM。

加密流程



详细分析

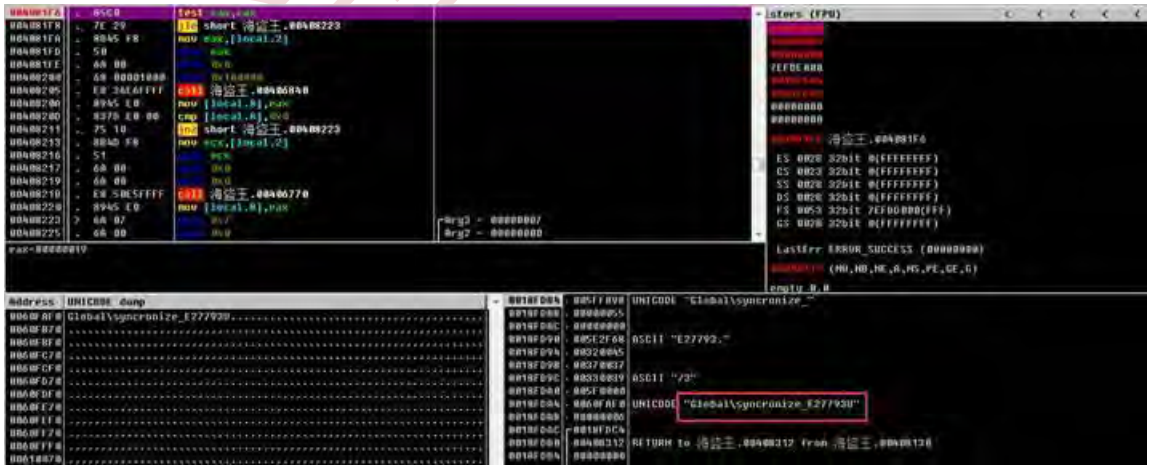
病毒首先会向寄存器写入特定扩展名，后面将会对这些扩展名文件进行加密：

.doc	.docx	.pdf	.xls	.xlsx	.ppt	.zip
.rar	.bz2	.7z	.dbf	.1cd	.jpg	

临界区初始化，提升程序能够竞争到的时间片：

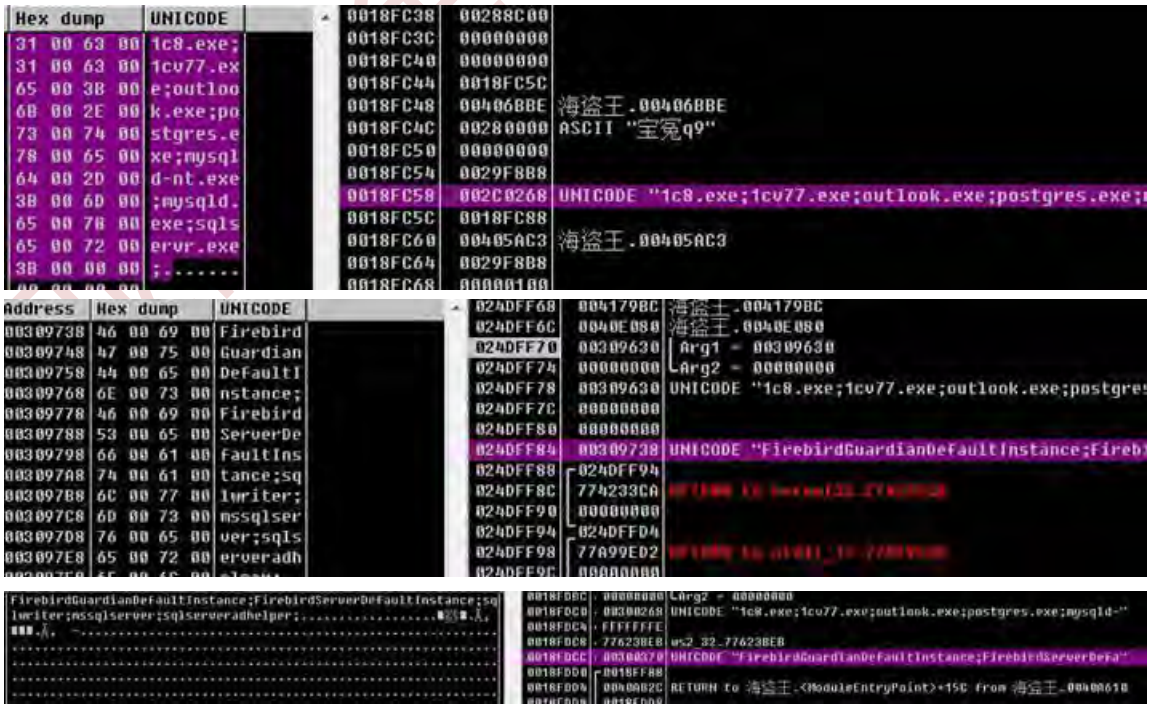
```
if ( v1 )
{
  // 初始化临界区，让程序获得更多系统的时间片
  InitializeCriticalSectionAndSpinCount((LPCRITICAL_SECTION)(v1 + 8), 0xFA0u);
  *(_DWORD *)v1 = 0;
  *(_DWORD *)(v1 + 4) = 0;
}
return v1;
```

创建名为 Global\syncronize_E27793A 和 Global\syncronize_E27793U 的互斥体，防止程序多次运行：

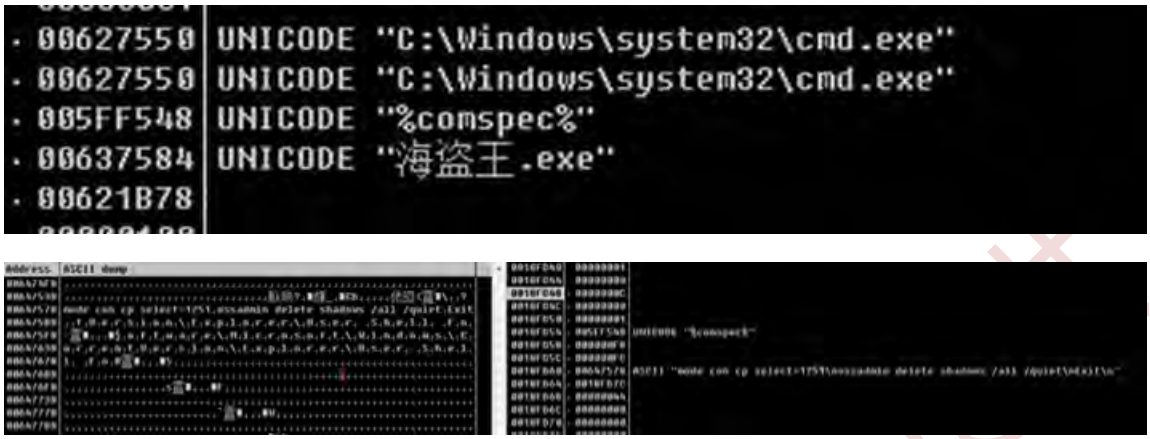


然后开始枚举系统中是否含有以下进程，若有以下进程，则将其终止，并停止所有数据库相关的进程服务，为后面加密数据库做准备：

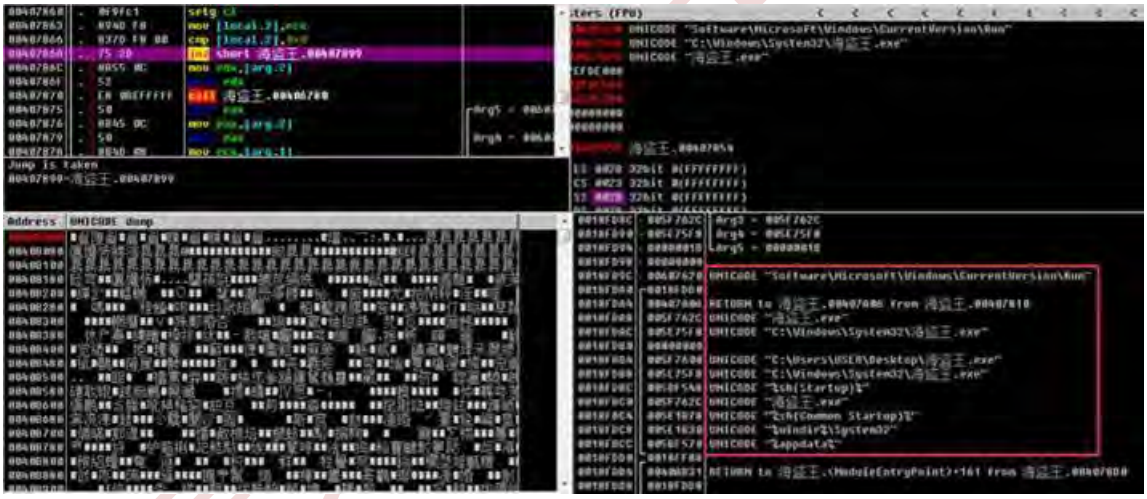
- 1c8.exe
- 1cv7.exe
- outlook.exe
- postgres.exe
- mysqld.exe
- sqlservrexe
- Sqlwriter
- Mssqlserver
- Sqlserveradhelper
- mysqld-nt.exe
- FirebirdGuardianDefaultInstance
- FirebirdServerDefaultInstance



随后该病毒通过%comspec%获取 cmd.exe 的路径，并执行删除系统卷影，防止系统恢复：

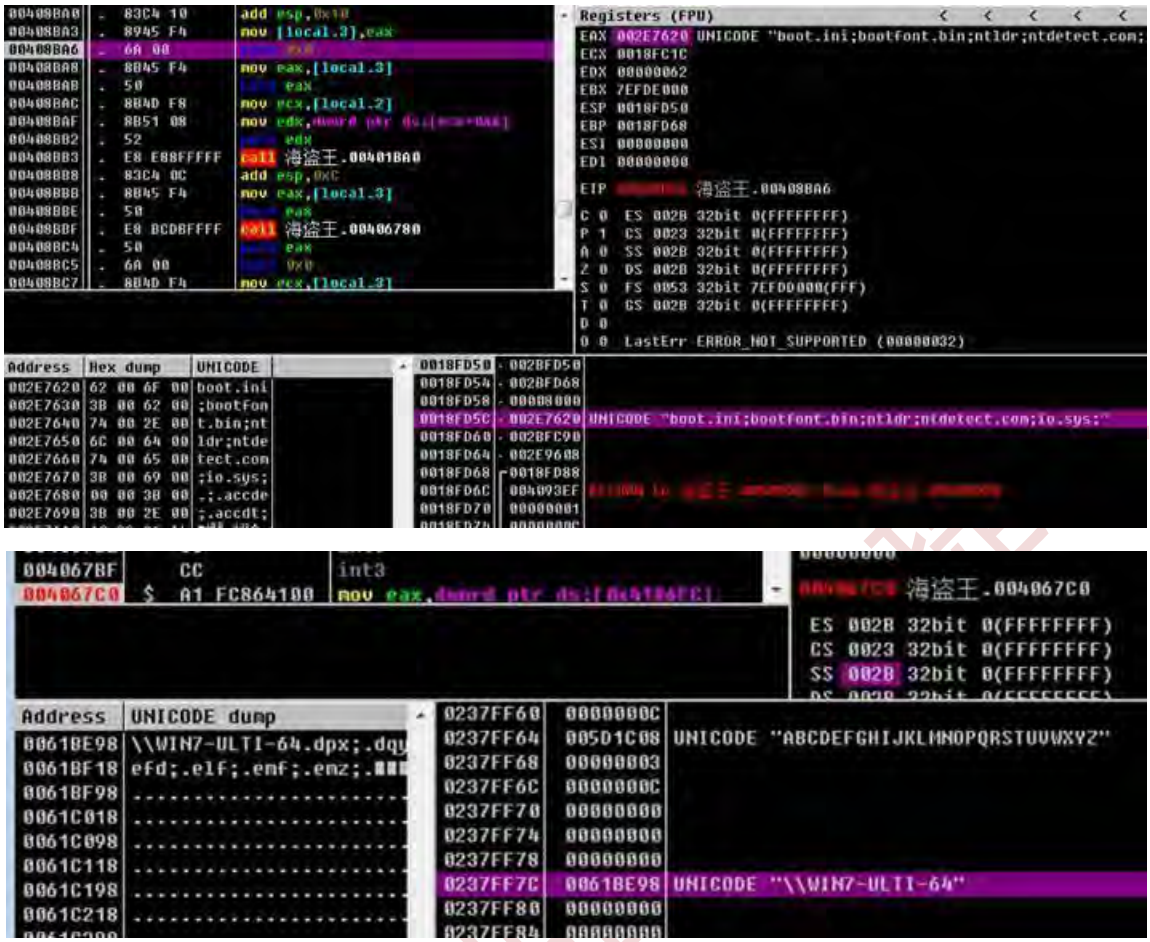


该病毒通过修改注册表中的键值，达到开机自启动目的：

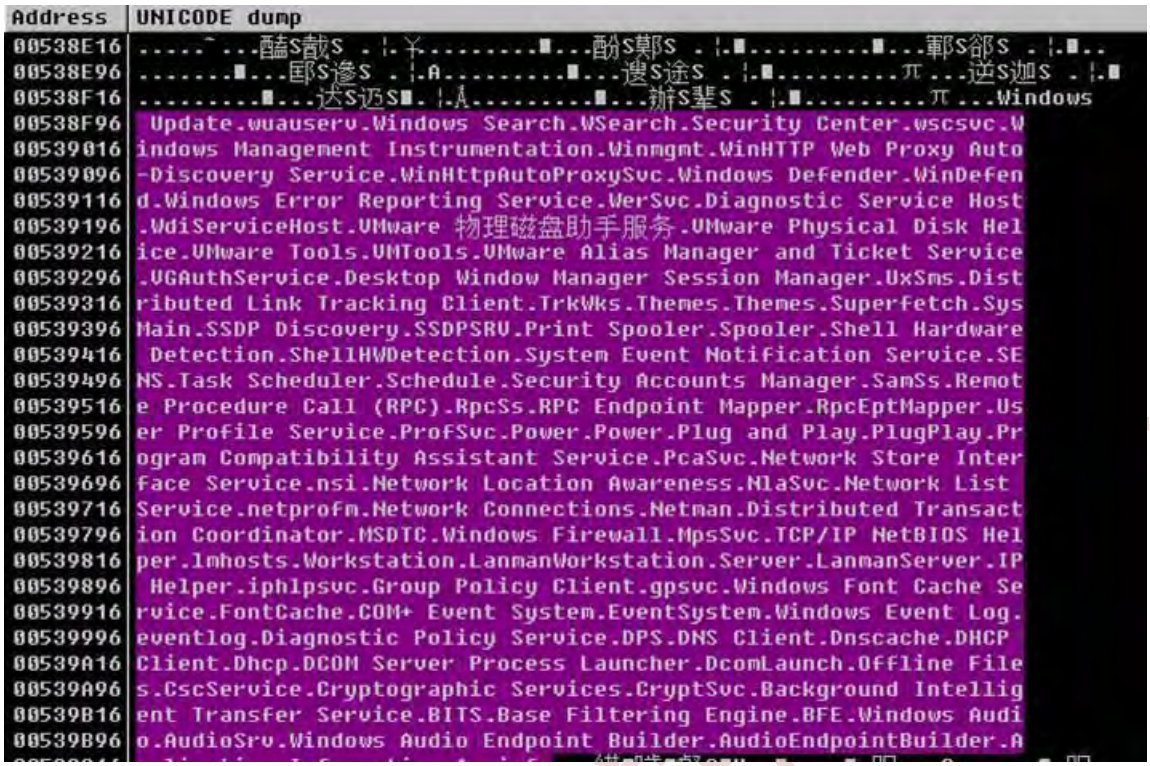


为了读取系统信息并保证系统正常运行，病毒把如下文件列入白名单，不加密：

- boot.ini
- bootfont.bin
- ntldr
- ntdetect.com
- io.sys



病毒关闭下列服务:



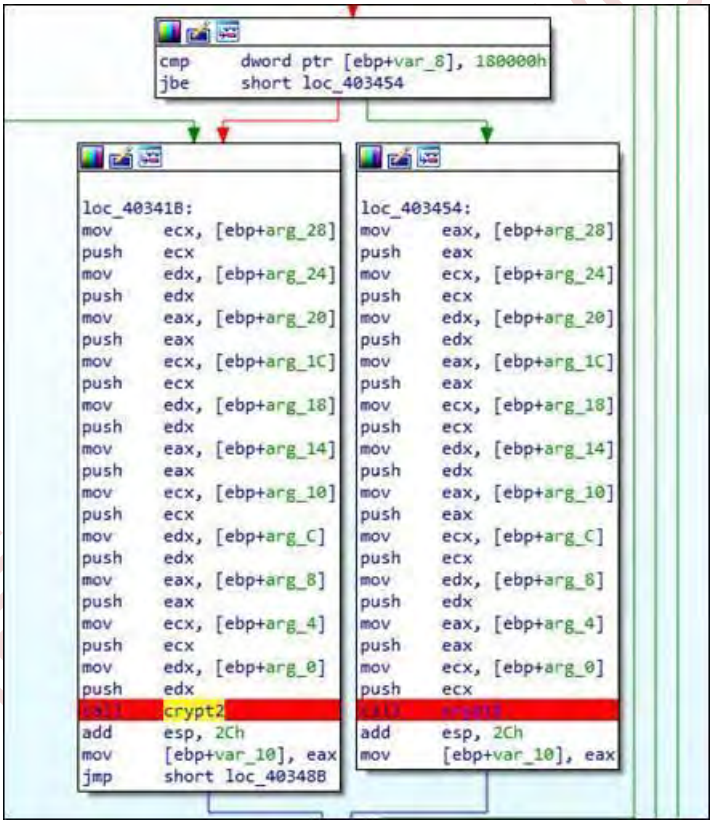
调用系统函数，遍历磁盘 A~Z:

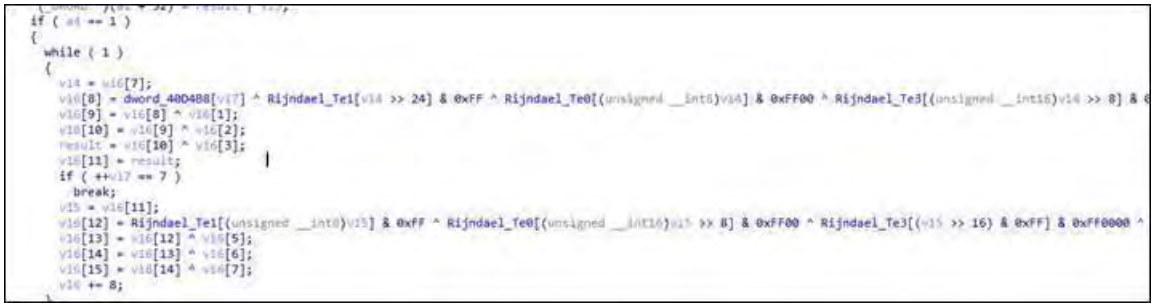
```
v10 = (char *)get_user_file((int)&unk_40E508, (int)&unk_40E080, 128, 2u);// 获取用户文件夹
v2 = sub_406780();
v9 = sub_406850(8 * v2);
v8 = 0;
v15 = dirve() & 0xFFFFFFFC;                    // 调用遍历磁盘函数
for ( i = 0; i < 32; ++i )
{
  if ( v15 & (1 << i) )
  {
    v11 = *(_WORD *)&v10[2 * i];
    v12 = 58;
    v13 = 0;
    v3 = traverse((int)&v11, a1, 1, a2);       // 遍历磁盘数据
    *(_DWORD *)(v9 + 4 * v8) = v3;
    if ( v3 )
      ++v8;
    v4 = traverse((int)&v11, a1, 0, a2);
    *(_DWORD *)(v9 + 4 * v8) = v4;
    if ( v4 )
      ++v8;
  }
}
```

```
0018FD9C  004097D6  CALL to GetLogicalDrives From 海盗王.004097D1
0018FDA0  00000000
0018FDA4  0018FDC8
0018FDA8  00000000
0018FDAC  002A2E08
0018FDB0  002A18C0  UNICODE "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
0018FDB4  00000003
```

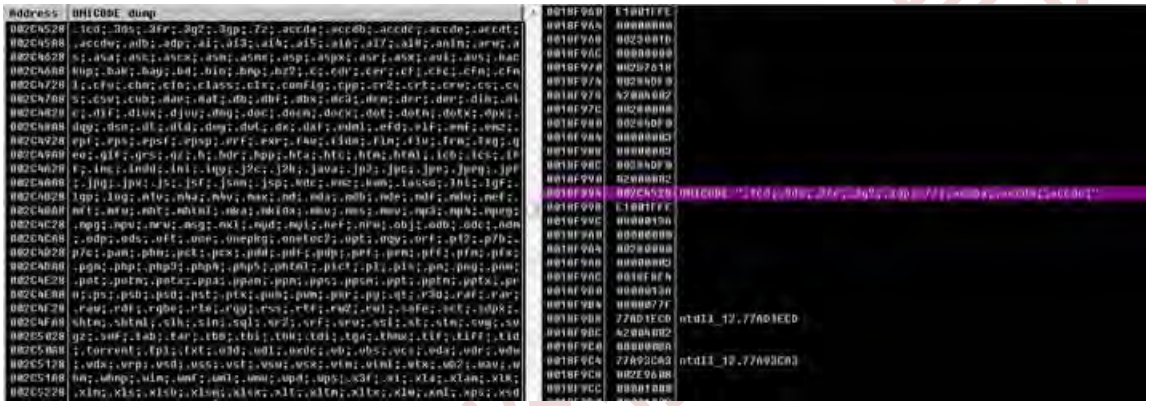
加密分析：

病毒首先判断文件大小，以文件大小来进行加密，调用的是基于 AES 的高级分组加密算法 Rijndael：

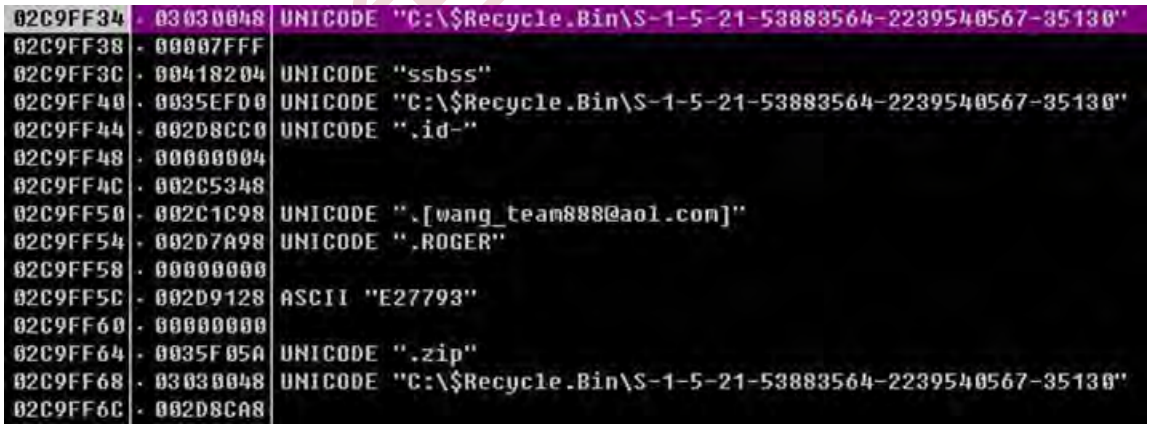




病毒会枚举加密后缀：

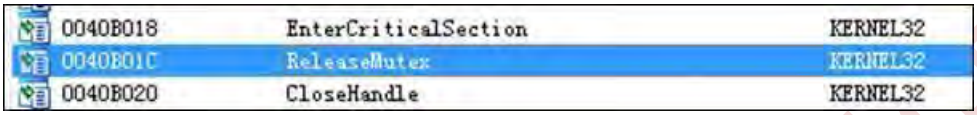


加密后文件后缀为 id-XXXXXX.wang_team888@aol.com.ROGER：



加密国家和地区黑名单：

病毒最后调用 releaseMutex，释放互斥变量：



该病毒勒索界面：

解决方案

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

亚信安全解决方案

✓ 亚信安全病毒码版本 15.765.60，云病毒码版本 15.765.71，全球码版本 15.767.00 已经可以检测，请用户及时升级病毒码版本。

IOC

文件名	SHA-1	亚信安全检测名
海盗王.exe	F92F7E91F9160626953711380140D2C04865E62D	Ransom.Win32.CRYSIS.SM