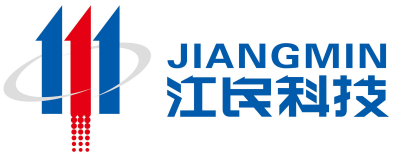
Petya（勒索病毒）样本分析报告



北京江民新科技术有限公司

二〇一七年六月二十八日

目　录

一、 病毒介绍

二、 病毒危害

三、 文件系统变化

四、 系统注册表变化

五、 网络症状

六、 病毒主要行为

七、 预防应对措施

病毒名称： Trojan.RansomPetya.a

病毒类型： 木马|后门

壳信息： **无壳，此病毒没有加壳行为**

传播方式：垃圾邮件、主机系统漏洞利用传播

影响系统： Windows XP, Windows Server 2003/x,Windows vista,Windows 7,Windows 8,Windows 10 等没有安装 CVE-2017-0199、MS17-010 补丁的 Windows 系统

病毒介绍:

据外媒消息，近日乌克兰、俄罗斯、印度、西班牙、法国、英国以及欧洲多国正在遭遇 Petya 勒索病毒袭击，政府、银行、电力系统、通讯系统、企业以及机场都不同程度的受到了影响。

与 WannaCry 不同之处在于：该病毒加密多种格式文件、加密 NTFS 分区、覆盖 MBR、阻止机器正常启动，影响更加严重。攻击者通过发送恶意的求职邮件进行鱼叉攻击。

Petya 和其他流行勒索软件不一样，它是通过攻击底层的磁盘架构达到无法访问整个系统的目的。恶意软件的作者不仅创建了自身的引导程序，而且还创建了一个微型的内核，长度为 32 节区。Petya 释放的文件向磁盘头部写入恶意代码，被感染系统的主引导记录被引导加载程序重写，并且加载一个微型恶意内核。接着，这个内核开始进行加密。Petya 声称加密了所有的磁盘，但事实不是这样。相反它只加密了主文件表，因此文件系统不可读。

该变种疑似采用了邮件、下载器和蠕虫的组合传播方式。病毒采用 CVE-2017-0199 漏洞的 RTF 格式附件进行邮件投放，之后释放 Downloader 来获取病毒母体，形成初始扩散节点，之后通过 MS17-010（永恒之蓝）漏洞和系统弱口令进行传播。同时初步分析其可能具有感染域控制器后提取域内机器口令的能力。因此其对内网具有一定的穿透能力，对内网安全总体上比此前受到广泛关注的 WannaCry 有更大的威胁，而多种传播手段组合的模式必将成为勒索软件传播的常态模式。

病毒危害:

1. 对系统磁盘扇区和重要文件进行加密，以此来勒索用户付费解密。
2. 复写 MBR 实现内核感染，阻止感染主机正常启动。
3. 通过 MS17-010 漏洞和系统弱口令在内网中传播。

文件系统变化:

1、在远程计算机创建病毒源文件副本，

例如： \\192.168.1**.2**\admin$\sample.dll

2、新增病毒文件：

c:\windows\dllhost.dat

%TMP%**.tmp

被感染主机会遍历磁盘目录，加密以下类型的文件，修改后缀不修改。

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

注册表变化:

无

网络症状:

利用 TCP 445 端口（Server Message Block/SMB）进行病毒传播，并利用漏洞攻击其它未感染主机，恶性传播。

```
:33:17    c:\windows\system32\rundll32...  访问网络          TCP [本机 : 1039] -> [192.168.174.254 : 445 (microsoft-ds)]
```

作者邮箱：wowsmith123456@posteo.net。

比特币钱包：1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

病毒主要行为:

1、勒索软件的传播途径是通过邮件进行传播，邮件伪装成求职简历。木马通过链接的方式加入邮件中，链接指向 dropbox 上的一个压缩文件，包含两个文件：

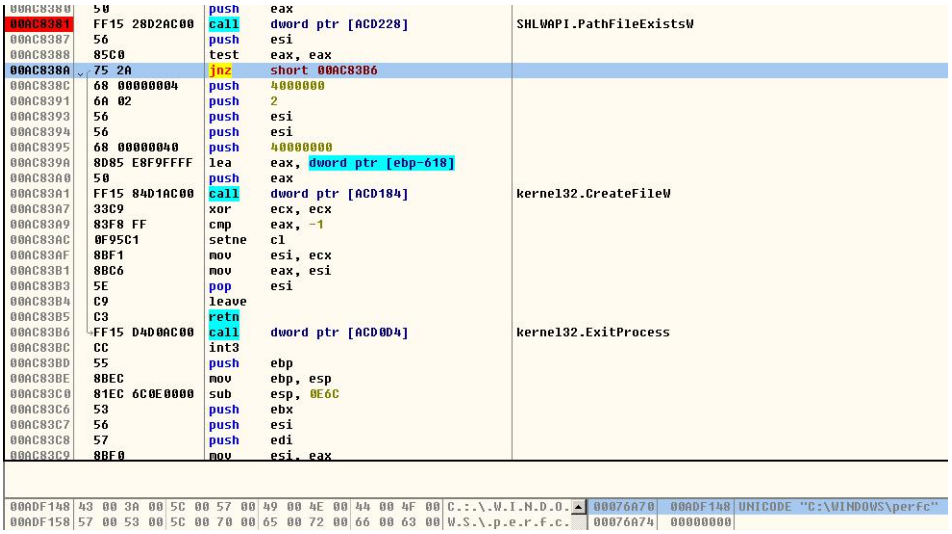
一张申请人的照片（该照片是未经许可使用的库存图片）

一个伪装成简历的自解压的可执行文件或者是 PDF 文件（该文件释放一个恶意的 32 位 PE 文件）。

2、勒索模块：

a) 启动参数："C:\Windows\System32\rundll32.exe \"C:\Windows\sample.dll\" #1

b) 如果发现文件"C:\WINDOWS\perfc",则退出程序，否则创建该文件向下执行加密操作。

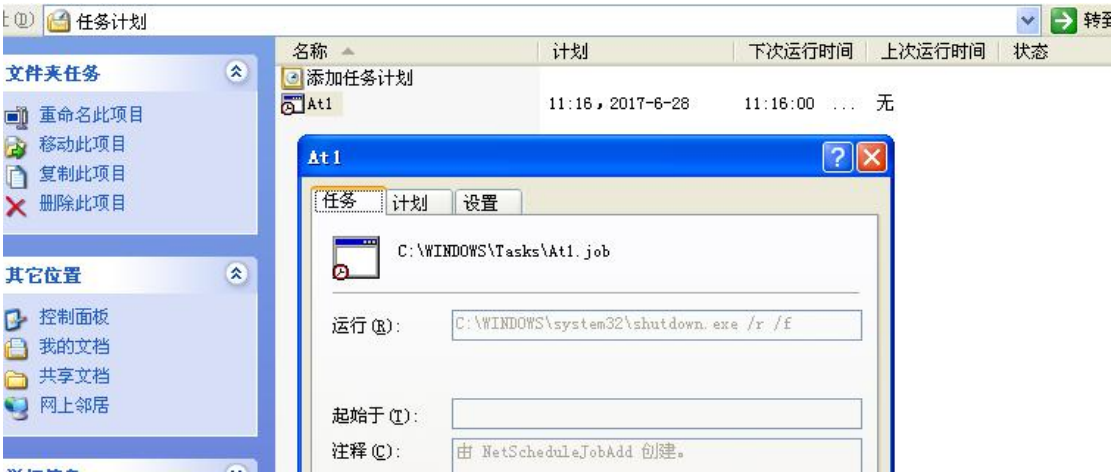


c) 木马获取权限操作。

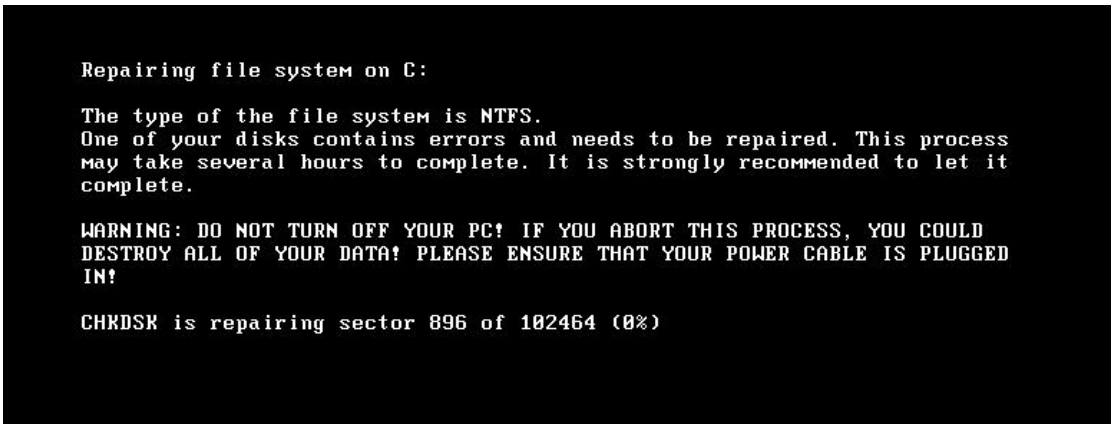
```
dwErrCode = 0;
TokenHandle = 0;
v2 = GetCurrentProcess();
if ( OpenProcessToken(v2, 0x28u, &TokenHandle) )
{
  if ( LookupPrivilegeValueW(0, lpName, (PLUID)NewState.Privileges) )
  {
    NewState.PrivilegeCount = 1;
    NewState.Privileges[0].Attributes = 2;
    v1 = AdjustTokenPrivileges(TokenHandle, 0, &NewState, 0, 0, 0);
    dwErrCode = GetLastError();
    if ( dwErrCode )
      v1 = 0;
  }
}
SetLastError(dwErrCode);
return v1;
```

i. 该文件被加载后遍历用户磁盘文件（除 C:\Windows 目录下），并对指定后缀名的文件进行加密，加密后不修改原文件名和扩展名。

ii. 文件修改 MBR，同时，添加计划任务，在等待一段时间后，关闭计算机。



iii. 当用户开启计算机时，会伪造显示磁盘检测的界面，然后显示勒索界面和信息并无法进入系统。



4、使用了微软的加密库进行加密。所使用的加密算法为 RSA+AES。

```
if ( CryptAcquireContextW(
       (HCRYPTPROV *)(pszDir + 8),
       0,
       L"Microsoft Enhanced RSA and AES Cryptographic Provider",
       0x18u,
       0xF0000000u) )
  goto LABEL_7;
v1 = GetLastError();
if ( v1 == -2146893799 )
{
  v6 = -268435456;
  v5 = 24;
  v4 = 0;
}
else
{
  if ( v1 != -2146893802 )
  {
LABEL_10:
    v2 = pszDir;
    goto LABEL_11;
  }
  v6 = 8;
  v5 = 24;
  v4 = L"Microsoft Enhanced RSA and AES Cryptographic Provider";
}
if ( !CryptAcquireContextW((HCRYPTPROV *)(pszDir + 8), 0, v4, v5, v6) )
  goto LABEL_10;
LABEL_7:
v2 = pszDir;
if ( sub_10001B4E() )
{
  sub_10001973((LPCWSTR)pszDir, 15, pszDir);
  sub_10001D32((LPCWSTR)pszDir);
  CryptDestroyKey(*(_DWORD *)(pszDir + 20));
}
CryptReleaseContext(*(_DWORD *)(pszDir + 8), 0);
LABEL_11:
```

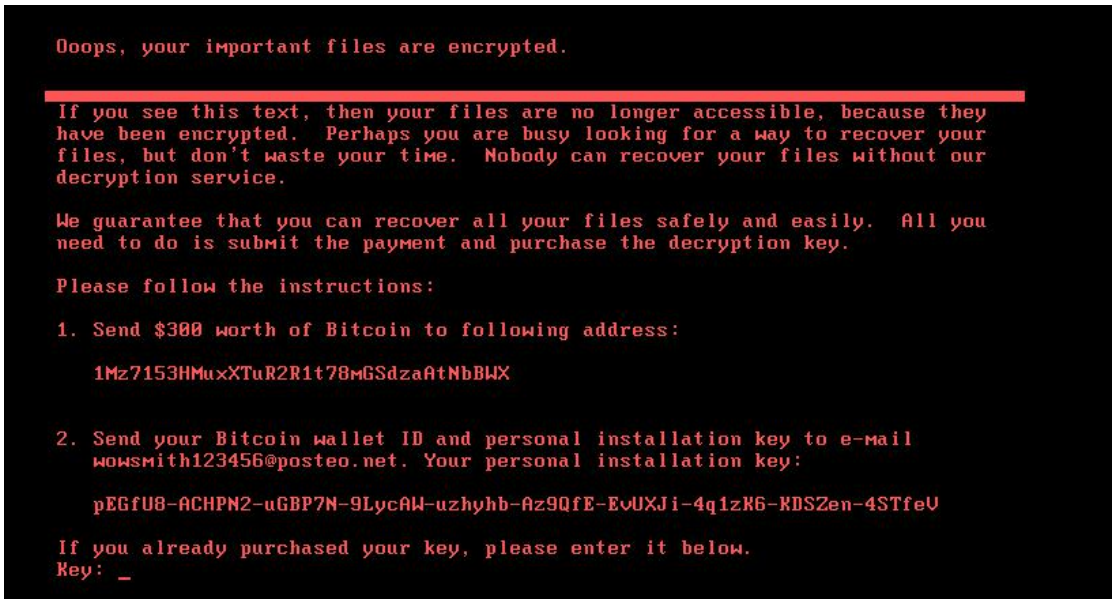
5、除 C:\Windows 目录下外，所有盘符下的所有文件夹均会被加密。

6、释放出名为 dllhost.dat 的文件，用于在远程机器上执行命令。控制端和被控制端的数据传输都是通过 445、135 或 139 端口进行。

7、使用了 Windows 自带的 wevtutil 工具进行日志清除工作。

```
wsprintfW(
  &v15, HANDLE
  L"wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D %c:",
  Filename);
v16 = 0;
sub_100083BD((int)&v15, 3);
```

弹出被加密勒索的提示界面



预防应对措施：

1、Petya 勒索软件变种首次传播通过邮件传播，所以应警惕钓鱼邮件。建议收到带不明附件的邮件，请勿打开；收到带不明链接的邮件，请勿点击链接。

2、及时更新操作系统补丁（ms17-010）等重要补丁。

3、更新 Microsoft Office/WordPad 远程执行代码漏洞（CVE-2017-0199）补丁。

4、禁用 WMI 服务：控制面板-管理工具-服务-Windows Management Instrumentation-属性-选择已禁用-确定。

5、如操作系统存在空口令或弱口令的情况，请及时将口令更改为高强度的口令。

6、要让你的计算机其免疫，只需要在 C:\Windows 文件夹下建立名为 perfc 的文件，并将其设为“只读”即可。