



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- Ransom.Win32.NEMTY.C	KB4525236
系统安全技巧	亚信安全产品
CRYSIS 勒索病毒变种预警	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_FAKEAV 家族

亚信安全热门病毒综述

亚信安全热门病毒综述-Ransom.Win32.NEMTY.C

该病毒利用社会工程学，通过伪造的海关信息邮件进行传播。其附件是一个伪造的 Word 文档文件，诱骗用户点击，一旦用户运行该文件后，磁盘中的重要文件将被加密，加密后的文件扩展名为.nemty。

- 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：15.499.60

<http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/>

- 病毒详细信息请查询：

<https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom.win32.nemty.c>

系统漏洞信息

Windows 安全更新 (4525236)

Windows 10 Version 1709 for 32-bit Systems

Windows 10 Version 1709 for 64-based Systems

Windows Server 2016

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

病毒码发布情况

亚信安全在最近一周发布中国区病毒码情况如下：

2019 年 11 月 11 日发布病毒码 15.485.60
2019 年 11 月 12 日发布病毒码 15.487.60
2019 年 11 月 13 日发布病毒码 15.489.60
2019 年 11 月 14 日发布病毒码 15.491.60
2019 年 11 月 15 日发布病毒码 15.493.60

截至目前，病毒码的最高版本为 15.499.60 发布于 2019 年 11 月 18 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：

2019 年 11 月 11 日发布病毒码 15.487.00
2019 年 11 月 12 日发布病毒码 15.489.00
2019 年 11 月 13 日发布病毒码 15.491.00
2019 年 11 月 14 日发布病毒码 15.493.00
2019 年 11 月 15 日发布病毒码 15.495.00

截至目前，病毒码的最高版本为 15.497.00，发布于 2019 年 11 月 18 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，亚信安全截获最新 CRYISIS 勒索病毒变种文件，CRYISIS 勒索病毒源于 2016 年，其主要通过 RDP 暴力破解和垃圾邮件进行传播。CRYISIS 勒索病毒在 2017 年万能密钥被公布之后，消失了一段时间，2018 年该病毒卷土重来，变种繁多，至今一直处于活跃阶段。本次截获的样本文件会加密系统中的重要文件，加密后的扩展名为[bitlocker@foxmail.com].wiki，亚信安全将其命名为 Ransom.Win32.CRYISIS.TIBGES。

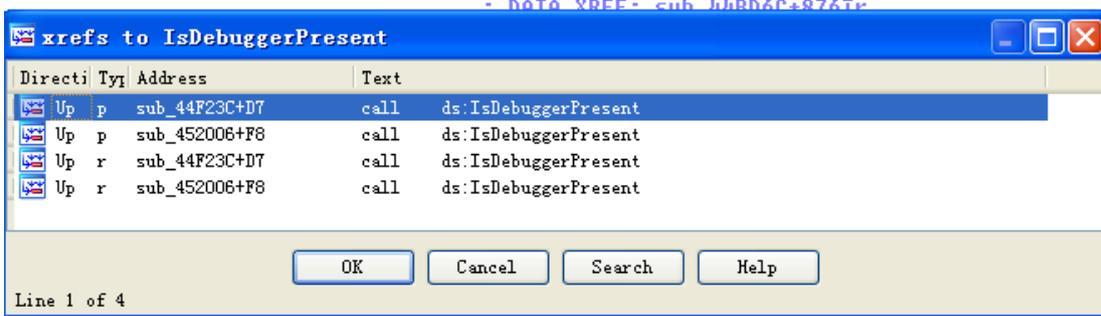
详细分析

经过逆向分析，我们发现该样本多处存在反调试：

```

.text:0044F2E6      mov     [ebp+var_2C], 10000h
.text:0044F2E9      push   50h
.text:0044F2EB      mov     [ebp+var_270], eax
.text:0044F2F1      lea    eax, [ebp+var_58]
.text:0044F2F4      push   0
.text:0044F2F6      push   eax
.text:0044F2F7      call   sub_44FAD0
.text:0044F2FC      mov     eax, [ebp+var_4]
.text:0044F2FF      add     esp, 0Ch
.text:0044F302      mov     [ebp+var_58], 40000015h
.text:0044F309      mov     [ebp+var_54], 1
.text:0044F310      mov     [ebp+var_4C], eax
.text:0044F313      call   ds:IsDebuggerPresent
.text:0044F319      push   0 ; lpTopLevelExceptionFilter
.text:0044F31B      lea    ebx, [eax-1]
.text:0044F31E      neg    ebx
.text:0044F320      lea    eax, [ebp+var_58]
.text:0044F323      mov     [ebp+ExceptionInfo.ExceptionRecord], eax
.text:0044F326      lea    eax, [ebp+var_324]
.text:0044F32C      sbb    bl, bl
.text:0044F32E      mov     [ebp+ExceptionInfo.ContextRecord], eax

```



该样本生成随机命名的文件并且添加自启动项:

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\%APPDATA%\Info.hta
Value: mshta.exe "%APPDATA%\Info.hta"
Type: REG_SZ
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\%windir%\System32\Info.hta
Value: mshta.exe "%windir%\System32\Info.hta"
Type: REG_SZ
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\JTyRXjSv.exe
Value: %windir%\System32\JTyRXjSv.exe
Type: REG_SZ
%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Startup\JTyRXjSv.exe
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\JTyRXjSv.exe
%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Startup\JTyRXjSv.exe
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\JTyRXjSv.exe
%windir%\System32\JTyRXjSv.exe

其会将自身复制到系统目录中:

%windir%\System32\JTyRXjSv.exe
File is copied from %WorkingDir%\JTyRXjSv.exe to %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Startup\JTyRXjSv.exe
File is copied from %WorkingDir%\JTyRXjSv.exe to %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\JTyRXjSv.exe
File is copied from %WorkingDir%\JTyRXjSv.exe to %windir%\System32\JTyRXjSv.exe

该样本的遍历逻辑及加密函数:

```

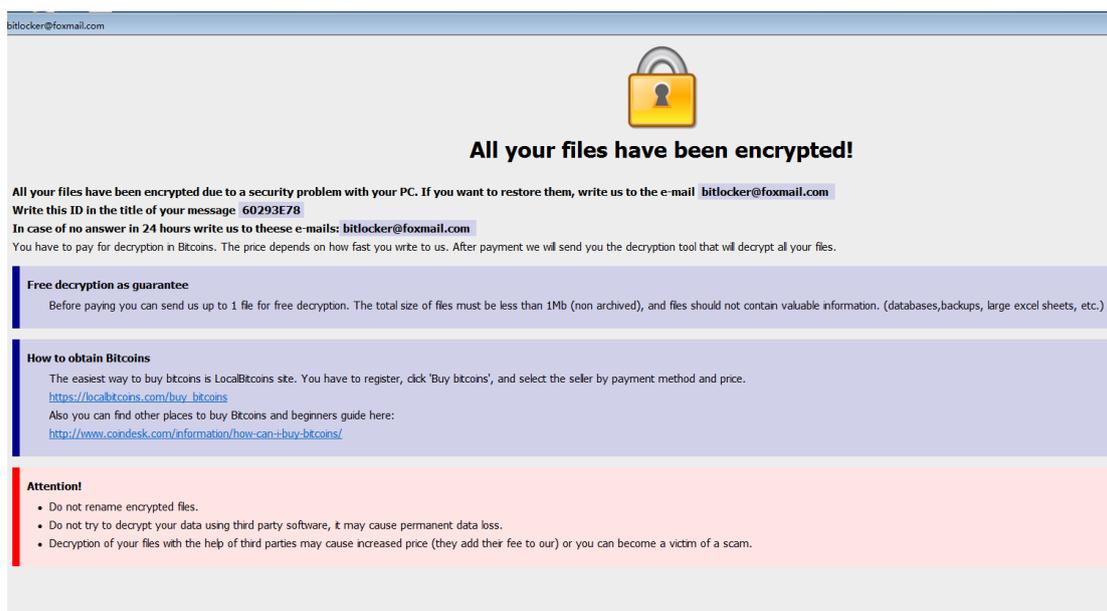
{
    u27 = (*(_DWORD *) (u35 + 4) - *( _DWORD *) u35) >> 2;
    while ( 1 )
    {
        u29 = 0;
        u30 = 0;
        lpLen = 0;
        u32 = 0;
        u33 = 0;
        u34 = 0;
        v14 = sub_45F336();
        v15 = sub_45ED4B(&WideCharStr, (int)&u29, (int)&u36, v14);
        v16 = v15 == 0 ? (unsigned int)lpLen : 0;
        if ( *( _BYTE *) v16 != 46 || (v17 = *( _BYTE *) (v16 + 1)) != 0 && (v17 != 46 || *( _BYTE *) (v16 + 2)) )
        {
            v18 = sub_45F02A(v16, lpMultiByteStr, u28, u35);
            u26 = v18;
            if ( v18 )
                break;
        }
        if ( u34 )
            sub_458158(lpLen);
        if ( !FindNextFileW(v13, (LPWIN32_FIND_DATAW)((char *)&u36 + 1)) )
        {
            v19 = (*( _DWORD *) (u35 + 4) - *( _DWORD *) u35) >> 2;
            if ( u27 != v19 )
                sub_4d0560(*( _DWORD *) u35 + 4 * u27, v19 - u27, 4u, (int (__cdecl *) (unsigned int, unsigned int)) sub_45EC81);
            goto LABEL_31;
        }
    }
    if ( u34 )
    {
        sub_458158(lpLen);
        v18 = u26;
    }
    u8 = v18;
LABEL_31:
    FindClose(v13);
}
if ( u25 )
    sub_458158(u22);
return u8;
}

```

样本运行后，系统内文件被加密，加密后的文件扩展名为[bitlocker@foxmail.com].wiki。



勒索提示信息:



bitlocker@foxmail.com



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail bitlocker@foxmail.com
Write this ID in the title of your message: **60293E78**
In case of no answer in 24 hours write us to these e-mails: bitlocker@foxmail.com
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
<http://www.comdesk.com/information/how-can-i-buy-bitcoins/>

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

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用 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 15.465.60, 云病毒码版本 15.465.71, 全球码版本 15.429.00 已经可以检测, 请用户及时升级病毒码版本。

详情可登陆亚信安全官网 www.asiainfo-sec.com 或拨打免费咨询热线 800-820-8876