**样本分析与评估报告**

### **一、**概述

样本（MD5：fbbdc39af1139aebba4da004475e8839）是Bad Rabbit 勒索病毒团伙的恶意软件样本，属于勒索软件攻击类型，是一个典型的“虚假更新诱导 + 勒索加密 + 内网扩散”复合型攻击样本，伪装为Adobe Flash Player虚假更新程序（如 flash\_player.exe或通过网页挂马诱导下载），诱导用户执行后部署勒索模块与横向移动脚本，加密本地文件并尝试内网传播，维持持久化控制与数据勒索。

Bad Rabbit勒索软件于 2017 年 10 月首次出现，主要影响俄罗斯和乌克兰的组织。该勒索软件通过一种名为“路过式下载”的方法传播，即当用户访问受感染的网站时，恶意软件会自动下载。该恶意软件伪装成 Adobe Flash 更新，诱骗用户在系统上安装。​

通过对样本的攻击行为以及造成影响进行分析，得出结论该样本属于“当前典型”勒索软件样本，理由如下：使用常见的攻击载体（虚假Flash更新程序），收集系统信息并加密高价值文件（如文档、数据库等），通过修改计划任务和注册表实现持久化驻留。利用SMB协议横向传播至内网其他主机，是典型的"感染-加密-扩散"勒索模型。符合"当前典型"勒索软件样本特征。

### 二、基本信息

样本文件名为630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da.exe，大小为431 KB，基本信息主要包括Hash、文件结构信息、平台、编译器信息等，如下表所示。

表 样本基本信息

|  |  |
| --- | --- |
| **名称** | **值** |
| 样本名称 | 630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da.exe |
| MD5 | fbbdc39af1139aebba4da004475e8839 |
| SHA-1 | de5c8d858e6e41da715dca1c019df0bfb92d32c0 |
| SHA-256 | 630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da |
| SHA512 | 74eca8c01de215b33d5ceea1fda3f3bef96b513f58a750dba04b0de36f7ef4f7846a6431d52879ca0d8641bfd504d4721a9a96fa2e18c6888fd67fa77686af87 |
| **文件大小** | 431 KB |
| **文件类型** | EXE |
| **文件位数** | 32位 |
| **系统类型** | MS Windows |
| **文件格式** | Portable executable for 80386 (PE) |
| **编译时间戳** | 2017年10月22日10:33:58 |
| **语言** | C++ |
| **工具** | Microsoft Visual Studio(2010) |
| **编译器** | Microsoft Visual C/C++(18.00.40629)[C] |
| **归属组织** | Bad Rabbit |

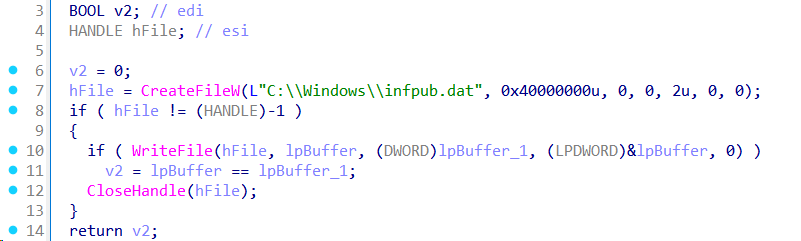
### 三、样本分析

#### 3.1 重要行为特征

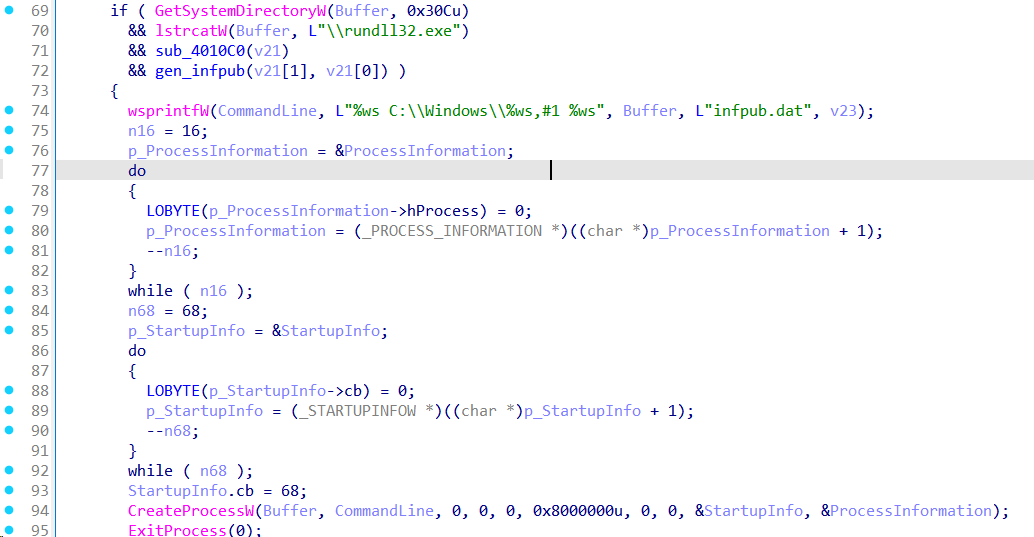
该样本是BadRabbit组织的勒索木马，主要功能是加密磁盘文件、加密MBR、通过SMB服务传播等。

首先样本会伪装成正常的flash player安装程序，以欺骗用户进行软件安装。





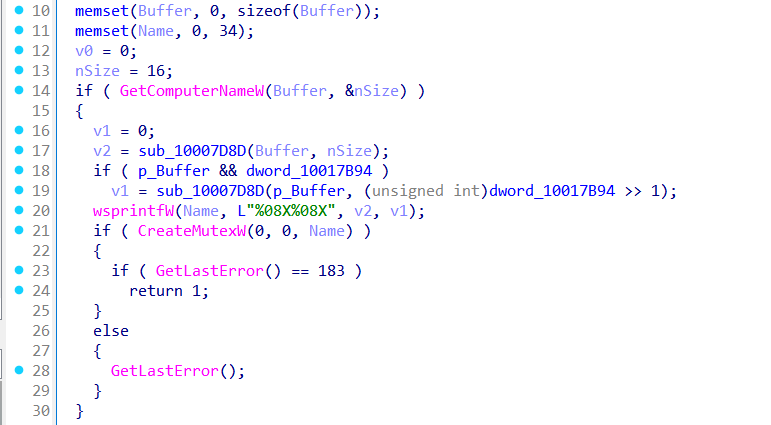
将恶意代码隐藏在infpub.dat文件中并使用rundll32.exe调用导出函数实现代码隐藏。



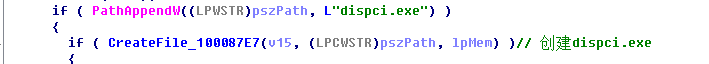
对自身进程进行提权操作，其中包括关机特权、调试特权及创建任意用户的安全令牌特权，以进行后续特权操作。

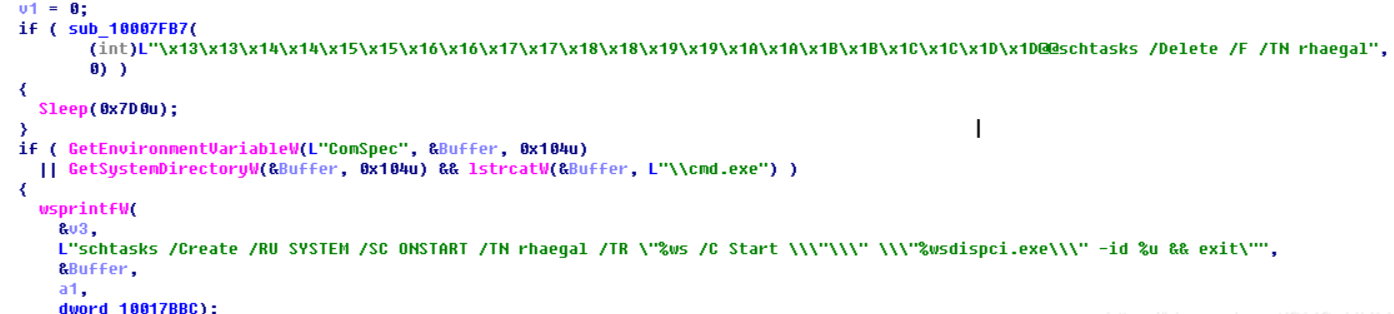


通过获取主机名称生成特定字符串，用于创建以此为名的互斥体常量实现唯一实例。



创建dispci.exe并调用schtasks.exe创建计划任务实现dispci.exe程序的持久化。

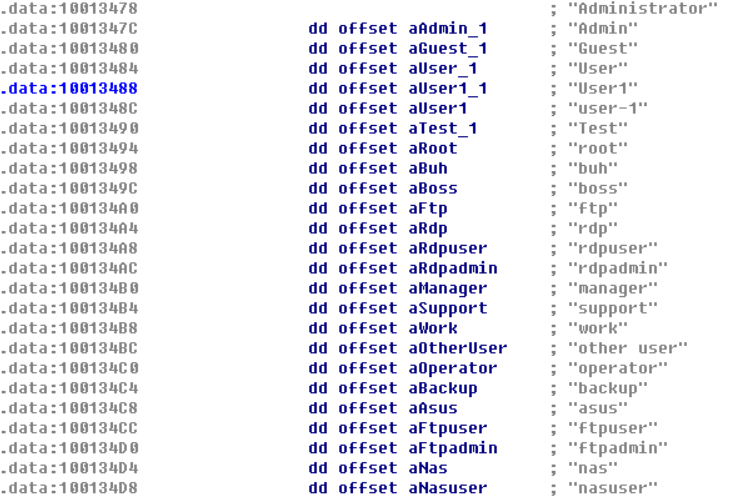




释放文件到共享局域网下并使用弱口令爆破的方式进行恶意代码的传播。



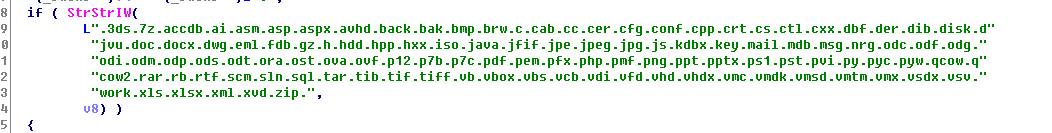
程序所使用的弱口令如下。



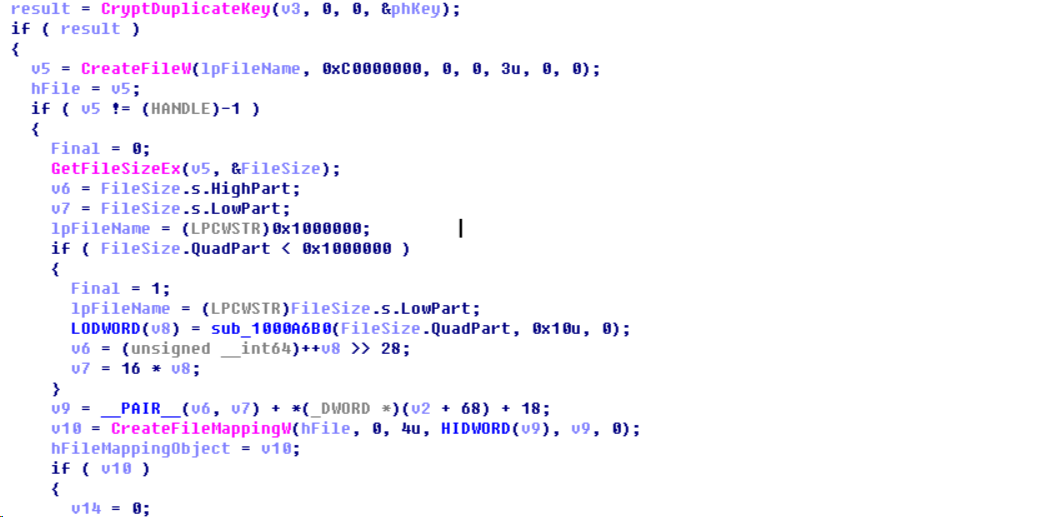
遍历文件，并加密特定后缀的文件。

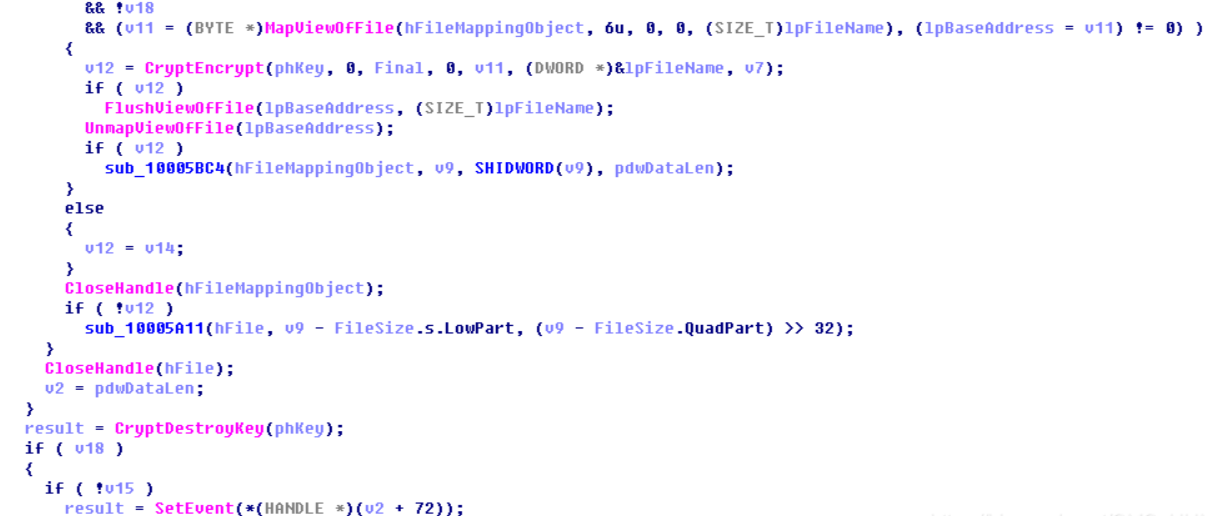


指定文件后缀名。

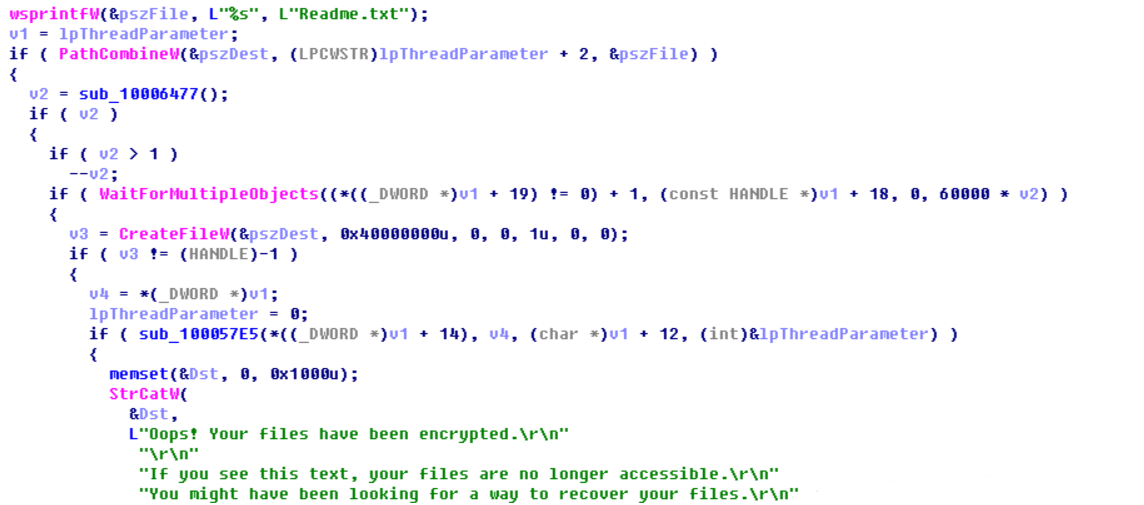


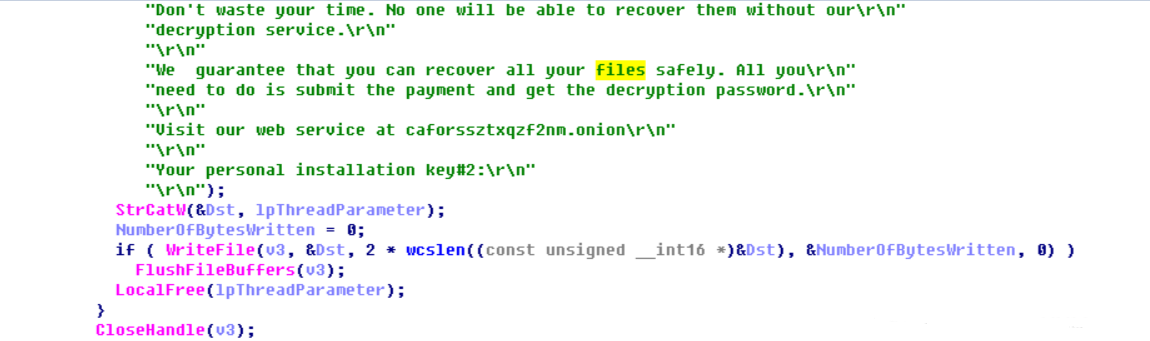
创建文件内存映射并加密文件，会在每个加密文件的末尾添加文件标记字符 “encrypted”。



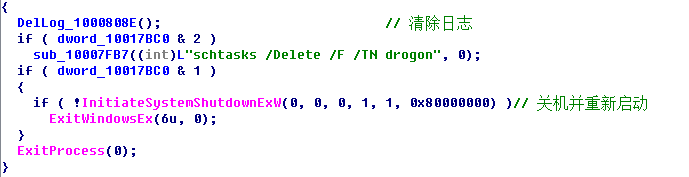


执行完加密操作后创建Readme.txt勒索文件，并写入勒索信息。





加密完成后，清除日志痕迹然后关机并重新启动。



#### 3.2 重要IOC特征

原始样本Hash：fbbdc39af1139aebba4da004475e8839

文件：

C:\Windows\infpub.dat

C:\Windows\System32\Tasks\drogon

C:\Windows\System32\Tasks\rhaegal

C:\Windows\cscc.dat

C:\Windows\dispci.exe

注册表项：

HKLM\SYSTEM\CurrentControlSet\services\cscc

HKLM\SYSTEM\CurrentControlSet\services\cscc\Type1

HKLM\SYSTEM\CurrentControlSet\services\cscc\Start0

HKLM\SYSTEM\CurrentControlSet\services\cscc\ErrorControl3

HKLM\SYSTEM\CurrentControlSet\services\cscc\ImagePathcscc.dat

HKLM\SYSTEM\CurrentControlSet\services\cscc\DisplayName\Windows Client Side Caching DDriver

HKLM\SYSTEM\CurrentControlSet\services\cscc\GroupFilter

HKLM\SYSTEM\CurrentControlSet\services\cscc\DependOnServiceFltMgr

HKLM\SYSTEM\CurrentControlSet\services\cscc\WOW641

被加密的目标文件的扩展名：

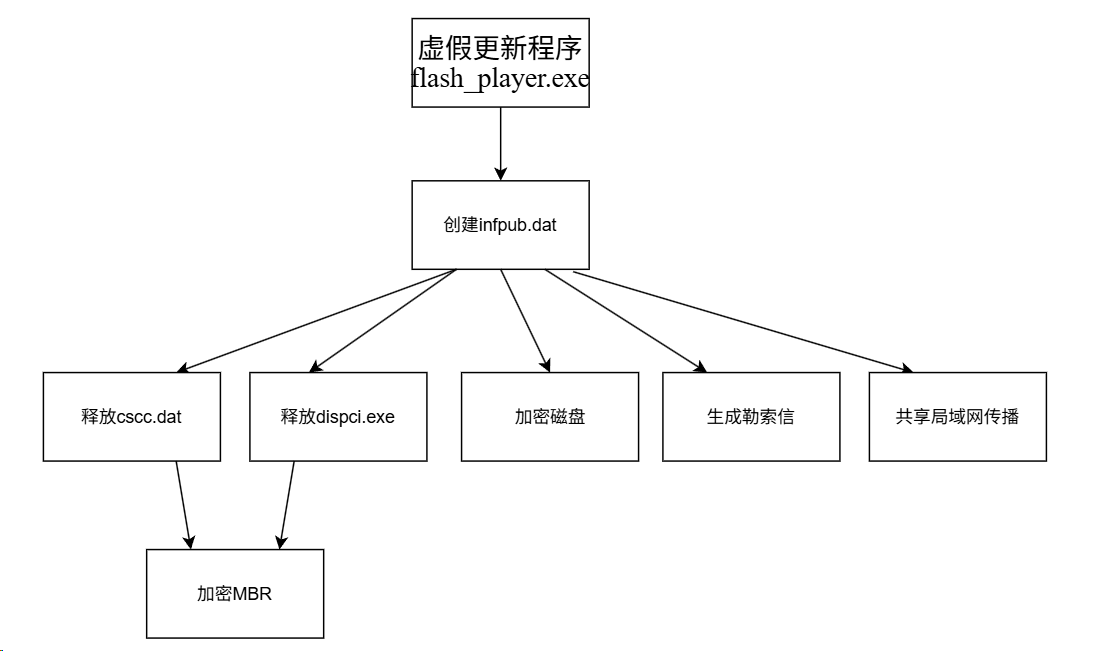
 .3ds .7z .accdb .ai .asm .asp .aspx .avhd .back .bak .bmp .brw .c .cab .cc .cer .cfg .conf .cpp .crt .cs .ctl .cxx .dbf .der .dib .disk .djvu .doc .docx .dwg .eml .fdb .gz .h .hdd .hpp .hxx .iso .java .jfif .jpe .jpeg .jpg .js .kdbx .key .mail .mdb .msg .nrg .odc .odf .odg .odi .odm .odp .ods .odt .ora .ost .ova .ovf .p12 .p7b .p7c .pdf .pem .pfx .php .pmf .png .ppt .pptx .ps1 .pst .pvi .py .pyc .pyw .qcow .qcow2 .rar .rb .rtf .scm .sln .sql .tar .tib .tif .tiff .vb .vbox .vbs .vcb .vdi .vfd .vhd .vhdx .vmc .vmdk .vmsd .vmtm .vmx .vsdx .vsv .work .xls .xlsx .xml .xvd .zip

勒索信：



#### 3.3 攻击链

通过对BadRabbit恶意样本进行深入分析，攻击链分析如下图所示。



#### 3.4 ATT&CK映射

通过对恶意软件样本进行分析得到 MITRE ATT&CK 标准技术框架TTP映射，如下表所示。

表 MITRE ATT&CK标准技术框架TTP映射表

|  |  |
| --- | --- |
| **ATT&CK Tactic** | **ATT&CK Technique** |
| DEFENSE EVASION | Obfuscated Files or Information [T1027] |
| DISCOVERY | File and Directory Discovery [T1083] |
| EXECUTION | Command and Scripting Interpreter [T1059] |

#### 3.5 敏感数据

通过勒索信得到洋葱域名信息为：caforssztxqzf2nm.onion。

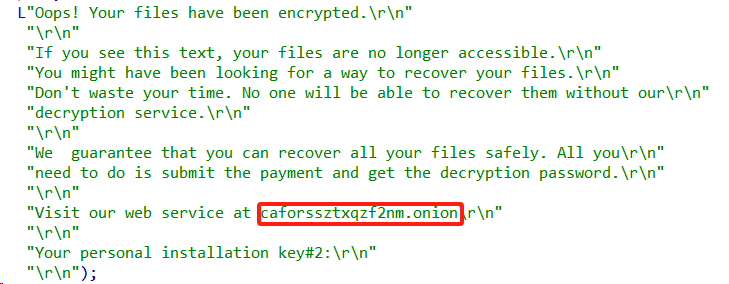


图 洋葱域名

内嵌的RSA-2048密钥：

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5clDuVFr5sQxZ+feQlVvZcEK0k4uCSF5SkOkF9A3tR6O/xAt89/PVhowvu2TfBTRsnBs83hcFH8hjG2V5F5DxXFoSxpTqVsR4lOm5KB2S8ap4TinG/GN/SVNBFwllpRhV/vRWNmKgKIdROvkHxyALuJyUuCZlIoaJ5tB0YkATEHEyRsLcntZYsdwH1P+NmXiNg2MH5lZ9bEOk7YTMfwVKNqtHaX0LJOyAkx4NR0DPOFLDQONW9OOhZSkRx3V7PC3Q29HHhyiKVCPJsOW1l1mNtwL7KX+7kfNe0CefByEWfSBt1tbkvjdeP2xBnPjb3GE1GA/oGcGjrXc6wV8WKsfYQIDAQAB

#### 3.6主要构件

该样本的主要构件包括：

1. 伪装成官方Adobe Flash Player更新程序的可执行文件flash\_player.exe，通过已被黑网站展示虚假的Flash更新通知，诱导用户主动点击下载并执行。

2. 释放并加载DiskCryptor驱动的修改版本（cscc.dat，即dcrypt.sys驱动的重命名文件）。

3. 创建名为"Windows Client Side Caching DDriver"的Windows服务，用于持久化加载加密驱动。

4. 使用基于DiskCryptor开源项目修改的磁盘加密驱动，修改主引导记录(MBR)以展示勒索信息，实现系统启动级别的锁定。

5. 通过计划任务"Rhaegal"在用户登录时自动执行命令："C:\Windows\dispci.exe" -id [id] && exit启动加密流程。对文件内容进行AES加密，在文件末尾添加"encrypted"标记（不修改原文件扩展名）。

6. 利用窃取的本地凭证或常见弱口令尝试访问内网共享资源，通过SMB协议（445端口）传播至网络中的其他计算机，将自身组件复制到网络共享位置并远程执行。

### 四、附录

