APT

洋葱狗 (APT-C-θ3)

交通能源的觊觎者

潜伏3年的定向攻击威胁

SkyEye 天眼实验室 | 追日团队

目录

第1章 概述

主要发现

2016 年 2 月 25 日，Lazarus 黑客组织以及相关攻击行动由卡巴斯基实验室[1]、AlienVault 实验室[2]和 Novetta[3]等安全企业协作分析并揭露。2013 年针对韩国金融机构和媒体公司的 DarkSeoul 攻击行动[4]和 2014 年针对索尼影视娱乐公司（Sony Pictures Entertainment，SPE）攻击[5]的幕后组织都是 Lazarus 组织。该组织主要攻击以韩国为主的亚洲国家，进一步针对的行业有政府、娱乐&媒体、军队、航空航天、金融、基础建设机构。

在 2015 年我们监控到一个针对朝鲜语系国家的组织，涉及政府、交通、能源等行业攻击的 APT 组织。通过我们深入分析暂未发现该组织与 Lazarus 组织之间有联系。进一步我们将该组织 2013 年开始持续到 2015 年发动的攻击，命名为“洋葱狗”行动（Operation OnionDog），命名主要是依据 2015 年出现的木马主要依托 onion city[6]作为 C&C 服务，以及恶意代码文件名有 dog.jpg 字样。相关恶意代码最早出现在 2011 年 5 月左右。至今至少发起过三次集中攻击。分别是 2013 年、2014 年 7 月-8 月和 2015 年 7 月-9 月，在之后我们捕获到了 96 个恶意代码，C&C 域名、IP 数量为 14 个。

“洋葱狗”恶意程序利用了朝鲜语系国家流行办公软件 Hangul 的漏洞传播，并通过 USB 蠕虫摆渡攻击隔离网目标。此外，“洋葱狗”还使用了暗网网桥（Onion City）通信，借此无需洋葱浏览器就可直接访问暗网中的域名，使其真实身份隐蔽在完全匿名的 Tor 网络里。另外通过我们深入分析，我们推测该组织可能存在使用其他已知 APT 组织特有的技术和资源，目的是嫁祸其他组织或干扰安全研究人员进行分析追溯。

---

[1] Operation Blockbuster revealed，https://securelist.com/blog/incidents/73914/operation-blockbuster-revealed/

[2] Operation BlockBuster unveils the actors behind the Sony attacks，https://www.alienvault.com/open-threat-exchange/blog/operation-blockbuster-unveils-the-actors-behind-the-sony-attacks

[3] Operation Blockbuster，https://www.operationblockbuster.com/resources/index.html

[4] 2013 South Korea cyberattack，https://en.wikipedia.org/wiki/2013_South_Korea_cyberattack

[5] https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

[6] http://onion.link

第2章 持续的网络间谍活动

1. 初始攻击

从目前捕获的数据来看恶意程序主要通过 HWP 漏洞文档和伪装为 HWP 文档文件进行传播。这种形态的伪装，通常是利用鱼叉式钓鱼邮件攻击进行传播。

其中 Hangul 是一款韩国本土主流的办公软件[7]，文件格式是 HWP（Hangul Word Processor）。攻击者除了采用伪装 HWP 文档文件，而且还使用 HWP 漏洞文档，也就是说明被攻击目标用户熟悉或经常使用 HWP 这款办公软件。

诱饵文档

样本 MD5	诱饵文档相关内容
588eef80e6f2515a2e96c9d8f4d67d5a	政府信息安全
700e94d4e52c4c15ebed24ec07f91f33	港口 VTS
b9164dd8260e387a061208b89df7bb6b	培训
3c983b300c533c6909a28cef7d7469ba	IT,简历
3df1c88a4a7dae7fdf9282d2c4375433	铁路事故调查报告
4ad5d70d79ea5b186d48a10dfdf8085d	公务员福利
5fbe59513167be2197c9f8fbf0afa7dd	公务员休假制度
cbcf18e559b87afdd059cae1f03b18d1	韩国电力公司薪资
3e9ac32a9418723c93e8de269ad63077	暑假期间检查计划
90b36bd4d12f34d556f363d6e5f9564f	韩国国土交通部商业计划书

表 1 部分诱饵文档列表

[7] http://www.hancom.com/group.eng_main.main.do

철도사고조사보고서(2015.6.11., 보고서번호: ARAIB/R 15-3)

운영기관: 한국철도공사

운행노선: 동해남부선(부산진역 ↔ 포항역)

발생장소: 울산광역시 덕하구역내(부산진역기점 65.312km 지점)

사고열차: 제3251호 화물열차[DL7346호 + 유조화차 20량]

사고유형: 열차탈선

사고일시: 2014년 7월 25일(금) 01시 35분경

그림 1 사고 현장 위치

图 1“韩国铁路事故调查报告书”诱饵文档

전국 주요 항만, VTS 설치 현황

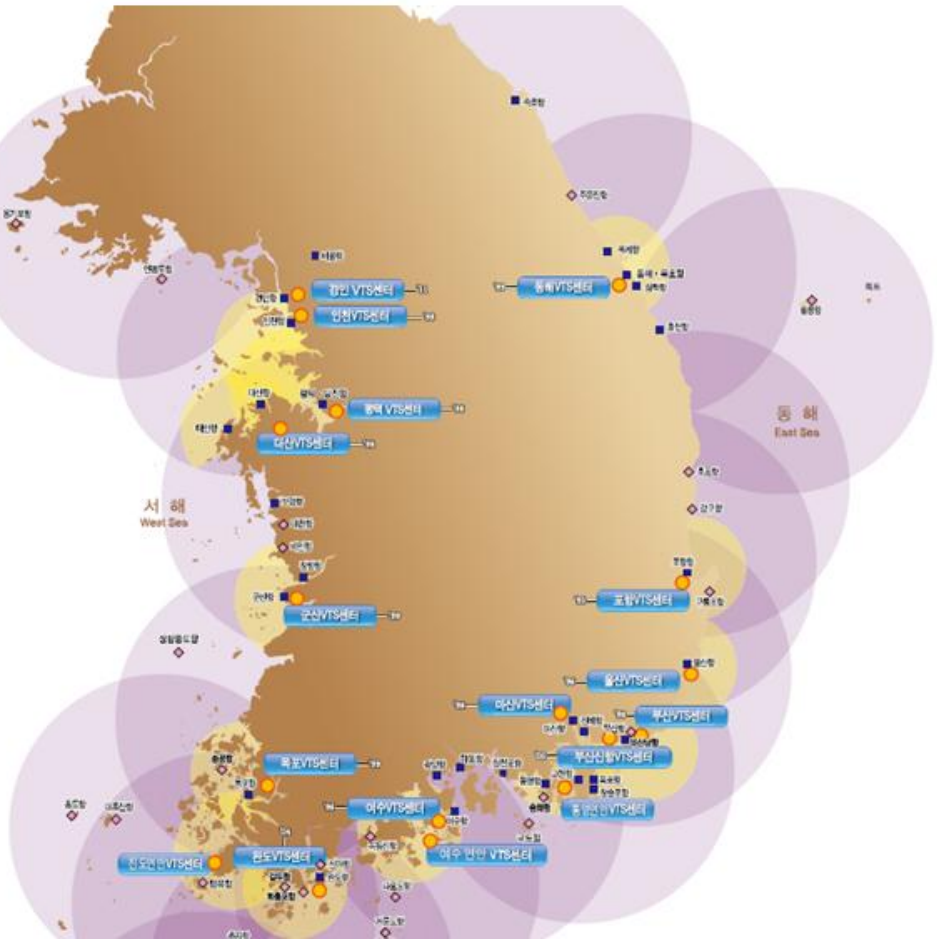


图 2“全国重要港湾，VTS 安装现状”诱饵文档

정보보호 침해사고 대응지침

제정 통계청예규 제78호 2012.5.18.

제1장 총칙

제1조(목적) 본 지침은 정보보호 침해사고에 의해 중요자료 유출 및 정보자산의 손실, 절도, 파괴 등으로 정상적인 업무수행에 지장을 초래하는 사고 발생 시 신속하게 대응하고, 그 과정을 기록 관리함으로써 정보보호 침해사고에 효과적으로 대응하는 것을 목적으로 한다.

제2조(용어정의) 본 지침에서 사용되는 용어의 정의는 다음 각 호와

图 3《防止信息泄露应对方案》诱饵文档

2015년도 을지훈련 대비 보안점검 계획

1. 목 적

을지훈련 기간 동안 각 기관의 보안점검을 통하여 전 직원 보안의식 고취 및 침해사고 대응절차 숙지

2. 을지훈련 前 사전점검 계획

□ **개인별 점검사항**

① 개인별 작업중인 모든 보안성자료(*문서, 노트북, 보조기억매체 등*)가 방치되지 않도록 잠금장치가 설치된 캐비넷·보관함 등에 보관

② 불필요한 자료 세절 처리

③ 개인 PC의 백신 설치, 상시 실행 및 최신 엔진으로 업데이트

④ 개인 PC의 운영체제(OS), 응용프로그램의 최신 업데이트 적용

⑤ 업무와 무관한 웹사이트 방문 금지

⑥ 출처 불분명 파일, 불법 프로그램 실행 금지

□ **분야별 점검사항**

① 네트워크 보안관리 담당자는 방화벽 규칙 점검

② 네트워크 보안관리 담당자는 IDS/IPS의 최신 규칙 적용

③ 서버 담당자는 주요 서버 내 DB 및 중요 자료의 1일 1회 백업

④ 메일 담당자는 메일 서버의 스팸 필터 규칙 점검

3. 점검 방법 및 내용

图 4《2015 年对比“乙支训练”安全检查计划》诱饵文档

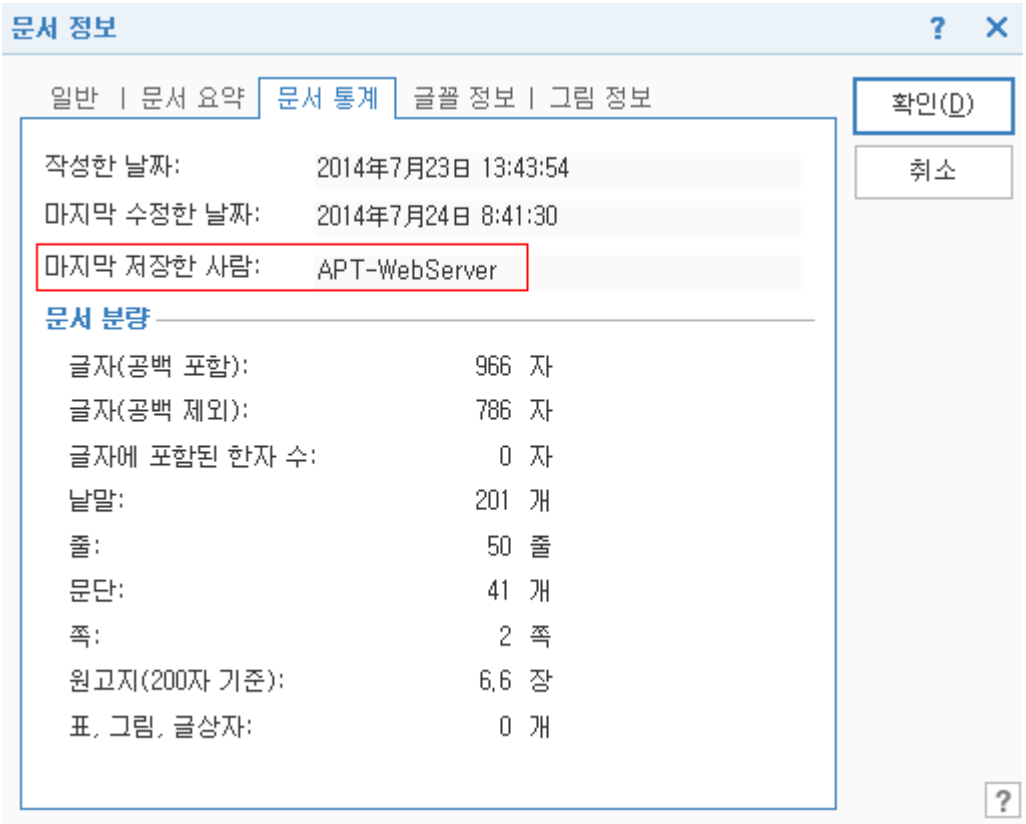


图 5 典型 HWP 诱饵文档属性截图

文档属性	具体内容
样本 MD5	cbcf18e559b87afdd059cae1f03b18d1
诱饵文档 MD5	9a4fafb0aa9f79dee2a117d237eaa931
内容	韩国电力公司薪资
文档大小	25,088
作者	test1234
创建时间	2014 年 7 月 23 日 13:43:54
最后编辑时间	2014 年 7 月 24 日 8:41:30
最后编辑	APT-WebServer

表 2 典型 HWP 诱饵文档属性表

2. 攻击流程

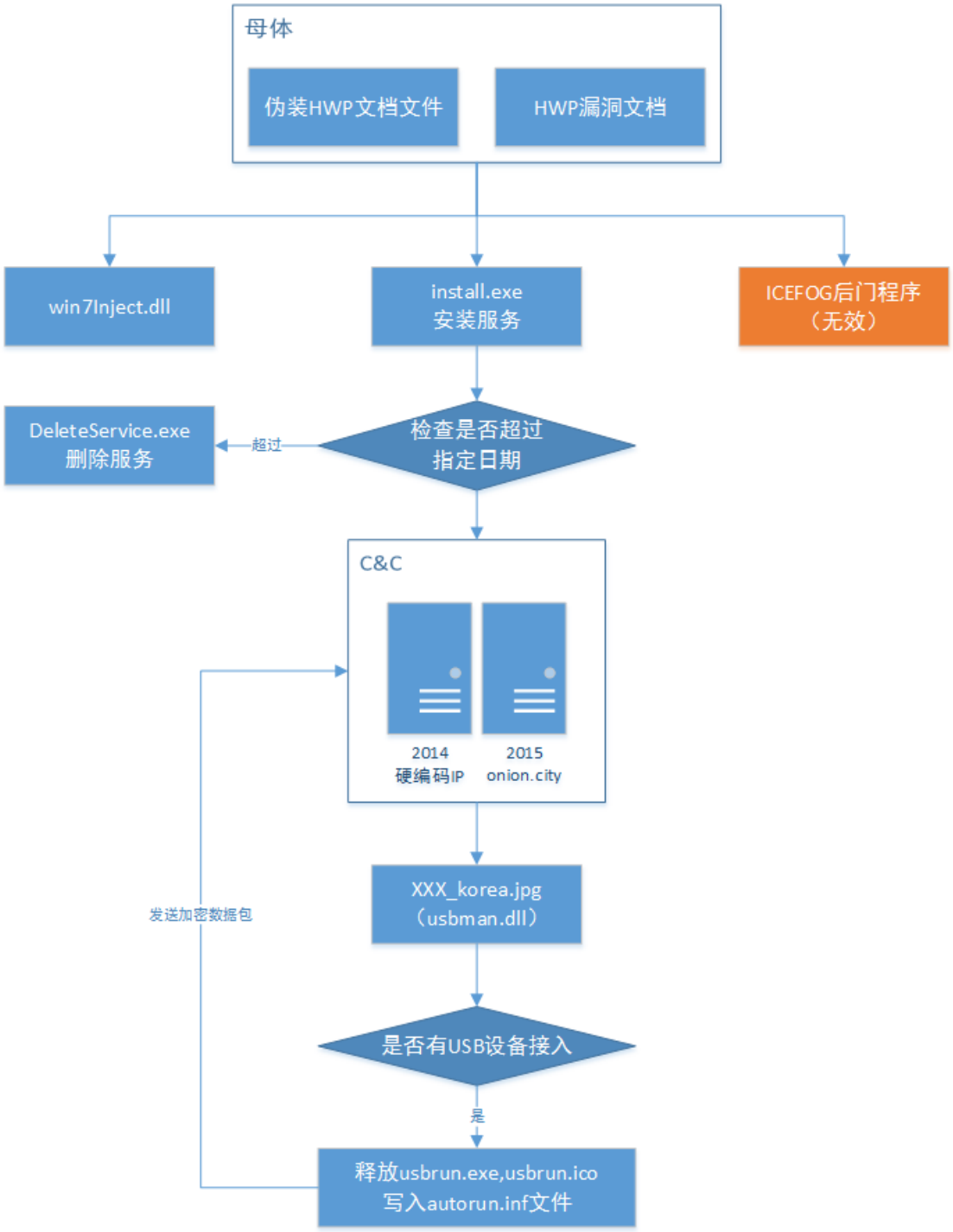


图 6 攻击流程图

伪装 HWP 文档木马或者 HWP 漏洞文档执行安装服务成功后，会判断当前日期是否为指定日期（具体日期如下表所示）。如果超过指定日期则会删除服务，结束执行。如果在指定日期范围内，则会请求 C&C 进行通信，2014 年版本的恶意程序会请求一个硬编码 IP，通过 HTTP 下载其他木马程序，2015 年版本中 C&C 域名统一更换为“onion.city”。在“C&C 分析”章节会进行详细介绍。

下载的木马程序其中一种是 USB 蠕虫，当发现有 USB 设备接入后会进行感染，进一步将当前时间、计算机名称、MAC 地址、USB 感染成功 或 USB 感染失败等信息回传到 C&C 服务器。

另外 HWP 漏洞文档触发成功后除了以上功能，还会释放一个后门程序。

2015 年 9 月 8 日
2015 年 8 月 8 日
2015 年 7 月 13 日
2014 年 8 月 9 日
2014 年 7 月 31 日
2013 年 10 月 25 日

表 3 截至具体日期

Dropper

Dropper 除了主要区分伪装 HWP 文档木马和 HWP 漏洞文档以外，进一步以伪装 HWP 文档木马为主分为三类硬编码 IP、Onion.city 和测试木马三个版本。分类依据主要是从 C&C 地址的差异性出发，这三类从代码架构对比差异性很小。其中时间戳和截至时间是 2014 年的恶意程序会请求一个硬编码 IP，而时间是 2015 年的 C&C 域名统一更换为 onion.city，另外 2014 年和 2015 年还有部分样本无 C&C 地址，下载的图片名称为“hello”，或者 C&C 地址只是“127.0.0.1”，我们认为这类是属于测试木马。

当 dropper 执行成功且在截至日期范围内，则会请求 C&C 地址，下载其他木马，并保存到%temp%目录下，并以类似“XXX_YYY.jpg”这种形态作为文件名，进一步我们结合诱饵文档，分析得出这些名称都是有特定涵义，一般都是指向了具体某个行业，具体如下图所示：

时间	相关资源名称	所属行业
2014	leepink_kosep	韩国东南电力
	jhryum12_komipo	韩国中部电力
	wypark_kwater	韩国水资源公社
	lhyuny_kospo	韩国南部电力
2015	vts_korea	韩国 VTS
	zerotaek_korea	韩国港口
	andong4_seoulmetro2	首尔地铁
	dydgh80_kdhc	韩国供暖
	myforce_humetro2	釜山地铁
	2060262_smrt3	首尔快速公交

表 4 相关资源名称的涵义

“洋葱狗”的攻击目标精准锁定在朝鲜语系国家的基础行业。2015 年，该组织主要攻击了港口、VTS（船舶交通服务）、地铁、公交等交通机构；而在此前 2014 年的一轮攻击中，“洋葱狗”则侵袭了多家电力公司和水资源公社等能源企业。

USB 蠕虫

下载的木马程序其中一种是 USB 蠕虫，当发现有 USB 设备接入后会进行感染，进一步将下述信息回传到 C&C 服务器。

具体执行流程可以参看下图，USBman.dll 运行时会发送计算机名称、mac 地址、ip 地址、当前日期时间、감염 Agent 실행 성공（感染 Agent 运行成功）到 hXXp://strj3ya55r367jqd.onion.city/main.php，端口为 80（来自 Dropper 的配置字段）封包经过异或加密后发出(TCP 包)。然后注册一个不可见的窗口(类名和窗口名都为 USB Manager)，窗口初始化时，注册 GUID_DEVINTERFACE_USB_DEVICE（USB 设备）和 GUID_DEVINTERFACE_DISK（磁盘设备）的通知消息。

当 WM_DEVICECHANGE（设备到达和移除）消息到达时判断设备是否为磁盘，是的话释放 usbman.dll 中的资源 101 到 usb 磁盘\usbrun.exe，107 资源到 usb 磁盘\usbrun.ico，新建 usb 磁盘\autorun.inf，达到感染 USB 磁盘的目的。

联网成功时,发送当前时间、计算机名称、IP 地址、mac 地址、盘符、设备名称、USB 감염 성공（USB 感染成功）或 USB 감염 실패（USB 感染失败）等到指定的服务器（hXXp://strj3ya55r367jqd.onion.city/main.php，端口为 80），如果有 USB 连接日志，文件名称为盘符\设备 ID，则以行为单位发送到服务器。

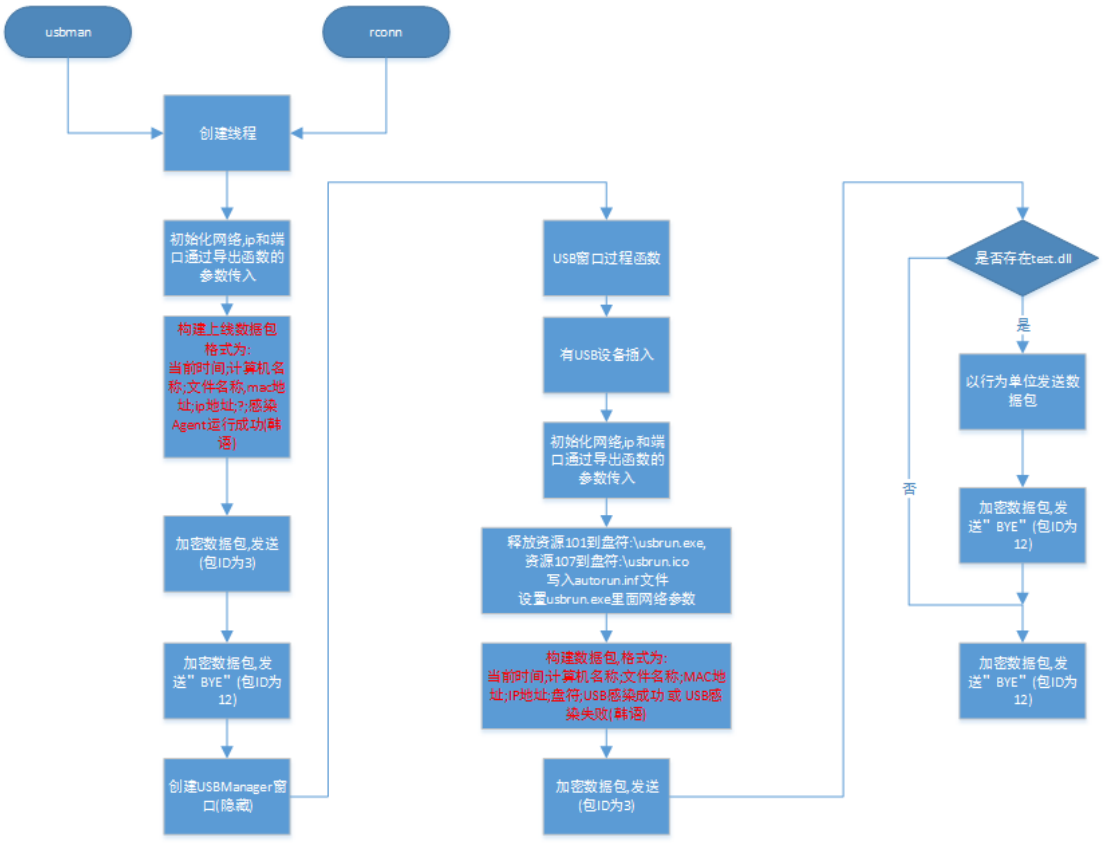


图 7 USB 蠕虫具体执行流程（USBman.dll）

当 usbrun.exe 被激活运行时,，如果联网成功则发送当前时间、计算机名称、mac 地址、ip 地址、设备名称、盘符、PC 감염 성공（PC 感染成功）到服务器，如果没有联网，则保持 usb 连接日志到盘符\设备 ID 文件，等联网成功时再发送。然后释放 106 资源为 test.dll，写入配置，载入 DLL 继续执行 usb 感染.test.dll 的功能和 Dropper 相同。

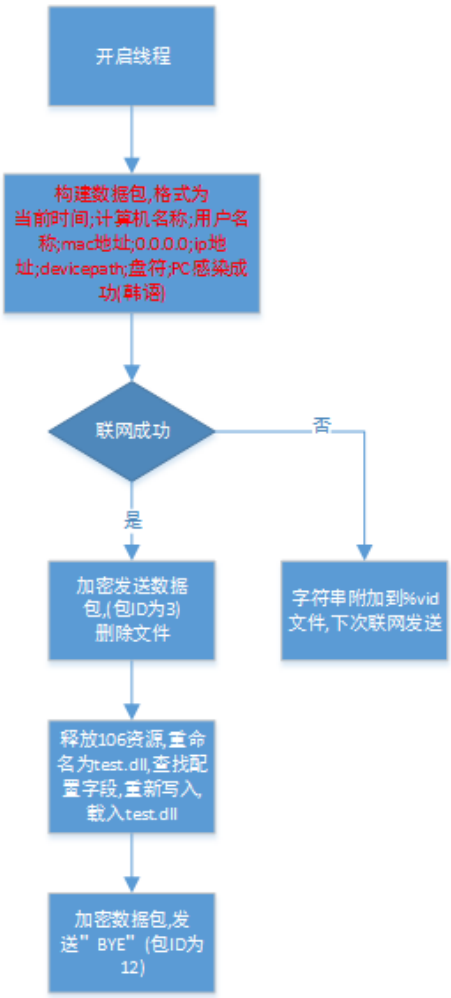


图 8 usbrun.exe 执行流程

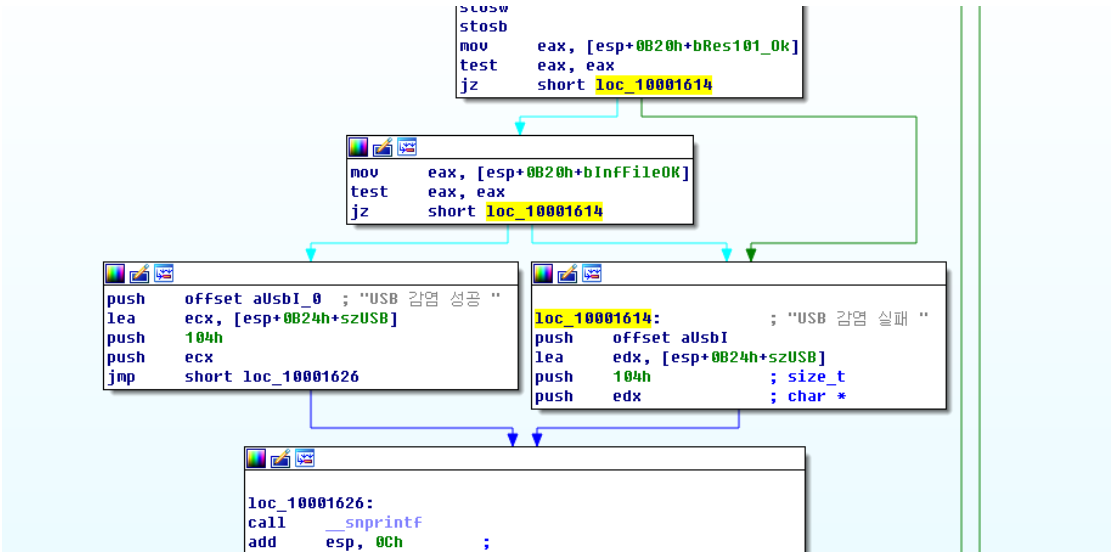


图 9 USB 感染成功/感染失败

ICEFOG 后门

关于该后门与“洋葱狗”行动的关系具体请参看“第 5 章 ICEFOG‘重生’：误导？嫁祸？”。关于该后门相关功能，请参看卡巴斯基 ICEFOG 技术报告[8]。

3. 长期监控、集中攻击

图 10 攻击时间轴

“洋葱狗”行动中的恶意木马程序，除了 ICEFOG 后门以外，如果要执行全部功能，则首先需要判断主机日期是否在指定日期范围内。从下表我们可以看出编译时间和截至日期之间的存活天数平均约 15 天左右。通过上面时间轴可以看出，攻击者从 2013 年开始每年都会进行类似攻击，且持续时间很短，另外我们发现截至时间 2014 年有 8 月 9 日，2015 年是 8 月 8 日，具体日期非常接近。

截至日期	编译时间	存活天数
2015 年 9 月 8 日	2015 年 8 月 27 日	12
2015 年 8 月 8 日	2015 年 8 月 5 日	3
2015 年 8 月 8 日	2015 年 8 月 3 日	5
2015 年 8 月 8 日	2015 年 7 月 23 日	16
2015 年 8 月 8 日	2015 年 7 月 10 日	29
2015 年 7 月 13 日	2015 年 7 月 10 日	3
2014 年 8 月 9 日	2014 年 7 月 18 日	22
2014 年 8 月 9 日	2014 年 7 月 15 日	25
2014 年 7 月 31 日	2014 年 7 月 13 日	18
2013 年 10 月 25 日	2013 年 10 月 10 日	15

[8] The Icefog APT: A Tale of Cloak and Three Daggers,https://securelist.com/blog/research/57331/the-icefog-apt-a-tale-of-cloak-and-three-daggers/

```
BOOL CheckDate()
{
  int dwYear; // ebx@1
  char *v1; // edi@1
  const char *v2; // esi@2
  char *v3; // edi@2
  const char *v4; // edi@3
  struct _SYSTEMTIME CurSystemTime; // [sp+10h] [bp-80h]@1
  int dwDay; // [sp+20h] [bp-70h]@1
  int dwMonth; // [sp+24h] [bp-6Ch]@1
  char szBuf[260]; // [sp+28h] [bp-68h]@1

  GetSystemTime(&CurSystemTime);
  dwYear = 0;
  szBuf[0] = 0;
  memset(&szBuf[1], 0, 0x103u);
  dwMonth = 0;
  dwDay = 0;
  v1 = strstr(a2015y8m8d, "Y");
  if ( v1 )
  {
    v2 = v1 + 1;
    dwYear = atoi(a2015y8m8d);
    v3 = strstr(v1 + 1, "M");
    if ( v3 )
    {
      v4 = v3 + 1;
      dwMonth = atoi(v2);
      if ( strstr(v4, "D") )
        dwDay = atoi(v4);
    }
  }
  _snprintf(szBuf, 0x104u, "Setting : %d year %d month %d day", dwYear, dwMonth, dwDay);
  memset(szBuf, 0, 0x104u);
  _snprintf(
    szBuf,
    0x104u,
    "Current : %d year %d month %d day",
    CurSystemTime.wYear,
    CurSystemTime.wMonth,
    CurSystemTime.wDay);
  return CurSystemTime.wYear >= dwYear
      && (CurSystemTime.wYear != dwYear || CurSystemTime.wMonth >= dwMonth)
      && (CurSystemTime.wYear != dwYear || CurSystemTime.wMonth != dwMonth || CurSystemTime.wDay >= dwDay);
}
```

图 11 检查截至日期相关代码

第3章 漏洞研究

1. 简介

通过深入分析，我们确定本次使用的 HWP 漏洞并不是首次出现，是已知漏洞，在 2011 年 nprotect 公司已经发布了相关预警和漏洞分析[9]。

Hangul Word Processor(Hwp)在读取 hwp2.0 版本的文档时，处理字体名称使用 strcpy 函数没有限制长度，导致缓冲区溢出，覆盖了 SEH 记录,，触发内存访问异常后使用 pop pop ret 指令串运行位于 Next SEH Record 的 shellcode，攻击者因此可以执行恶意代码。

该漏洞涉及 HWP 2010 以及早期多个版本，具体如下列表所示：

受影响的版本
HWP 2002 5.7.9.3047 及更早版本
HWP 2004 6.0.5.764 及更早版本
HWP 2005 6.7.10.1053 及更早版本
HWP 2007 7.5.12.604 及更早版本
HWP 2010 8.0.3.726 及更早版本
不受影响的版本
HWP 2002 5.7.9.3049 及更新版本
HWP 2004 6.0.5.765 及更新版本
HWP 2005 6.7.10.1055 及更新版本
HWP 2007 7.5.12.614 及更新版本
HWP 2010 8.0.3.748 及更新版本

表 5 受影响 HWP 相关版本

下表是“洋葱狗”攻击行动中使用的 HWP 漏洞文档：

MD5	CVE 编号
26b416d686ce57820e13e572e9e33cce[10]	无
de00286f6128fb92002e0c0760855566[11]	无

表 6 HWP 漏洞文档列表

2. HWP 漏洞原理分析

HWP 支持 hwp、doc、wps、ppt 等格式。其中 hwp 包括 hwp2.0、hwp3.0、hwp5.0 三个版本、hwp2.0 是比较老的格式。hwp 程序打开 hwp2.0 的文档时会自动转换为 hwp3.0 格式。

[9] [Warning] Detected malicious file using HWP file’s vulnerability ，
http://en-erteam.nprotect.com/2011/07/caution-detected-malicious-file-using.html

[10] https://cryptam.com/docsearch.php?md5=26b416d686ce57820e13e572e9e33cce

[11] https://cryptam.com/docsearch.php?md5=de00286f6128fb92002e0c0760855566

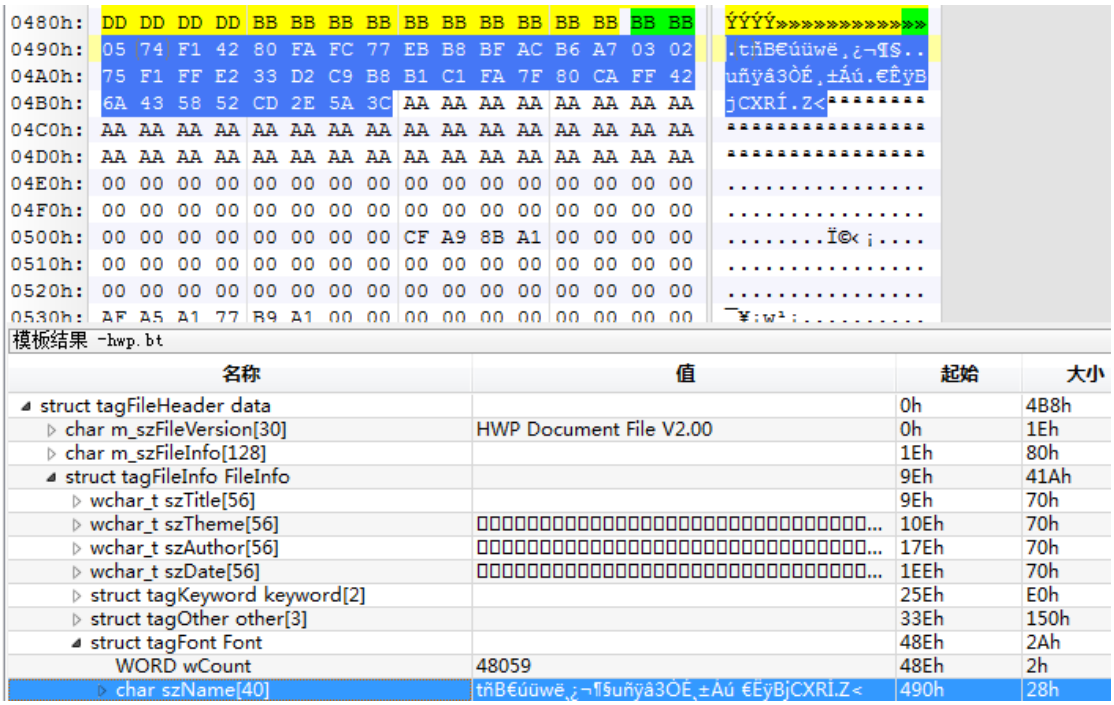


图 12 HWP 漏洞文档文档格式

Hwp2.0 偏移 0x48E 的位置开始是字体结构,前两个字节是字体名称数量，每个字体名称长度为 0x28。程序处理 hwp2.0 文档时，调用 CHwp20ToHwp30FilterLibrary 类的 ConvertFilterFileToWorkFile 函数转换为 hwp3.0 格式，处理字体结构调用 Set20FontList 子函数。

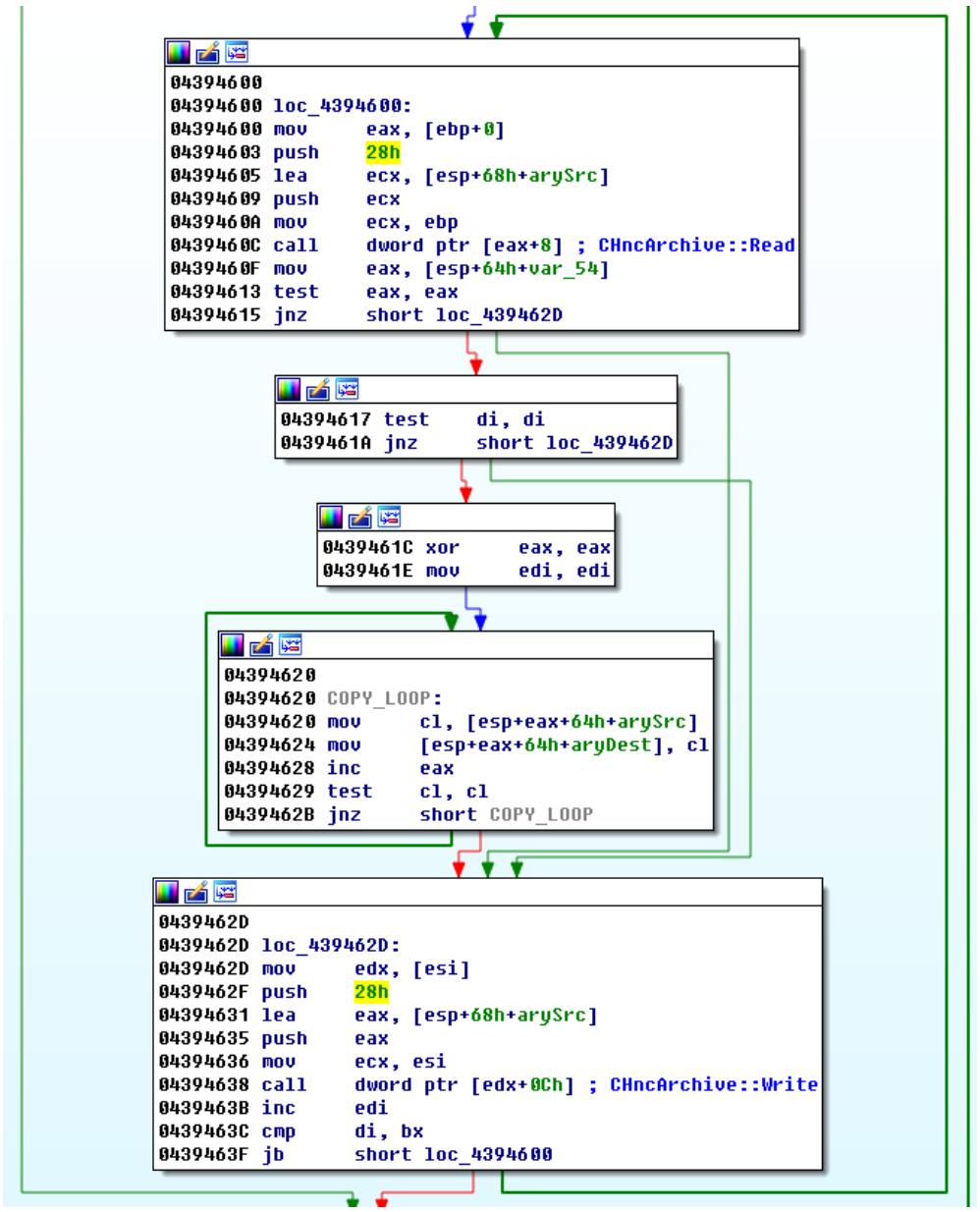


图 13 Set20FontList 函数

Set20FontList 函数中读取 hwp2.0 文档的 0x28 个字节，到数组 arySrc[0x28]中，循环拷贝到 aryDest[0x28]中，退出循环的条件为当前拷贝字节是否为 0。

而在内存中，arySrc 数组后面紧接着就是 aryDest，当拷贝到 arySrc 最后一个字符 0x3C 时由于不是 0，继续取下一个字符，取到了 aryDest 的第一个字符。如此反复直至触发 C0000005 访问异常。

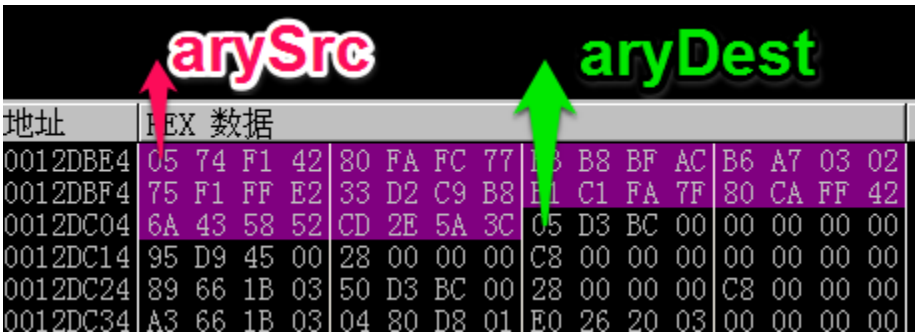


图 14 arySrc aryDest 内存结构

覆盖的地址里面包括 CHwp20ToHwp30FilterLibrary::ConvertFilterFileToWorkFile 函数设置的 SEH 记录。

图 15 SEH 记录被覆盖后

接下来当拷贝到 00130000 时，触发 C0000005 异常，来到 windows 异常处理流程，调用 SEH Handler(7FFAC1B1)，此时第二个参数指向 12E4B8。

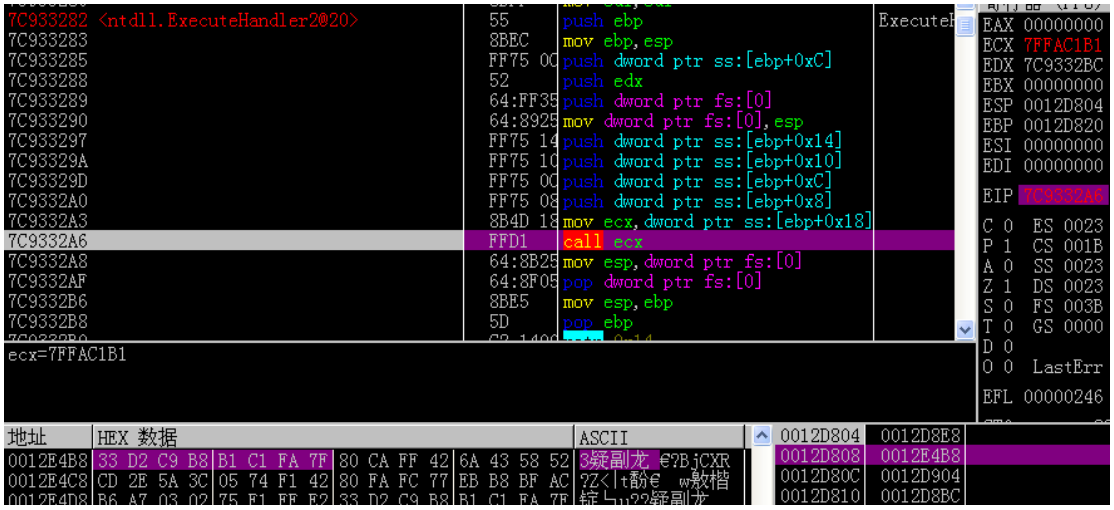


图 16 调用 SEH 处理函数

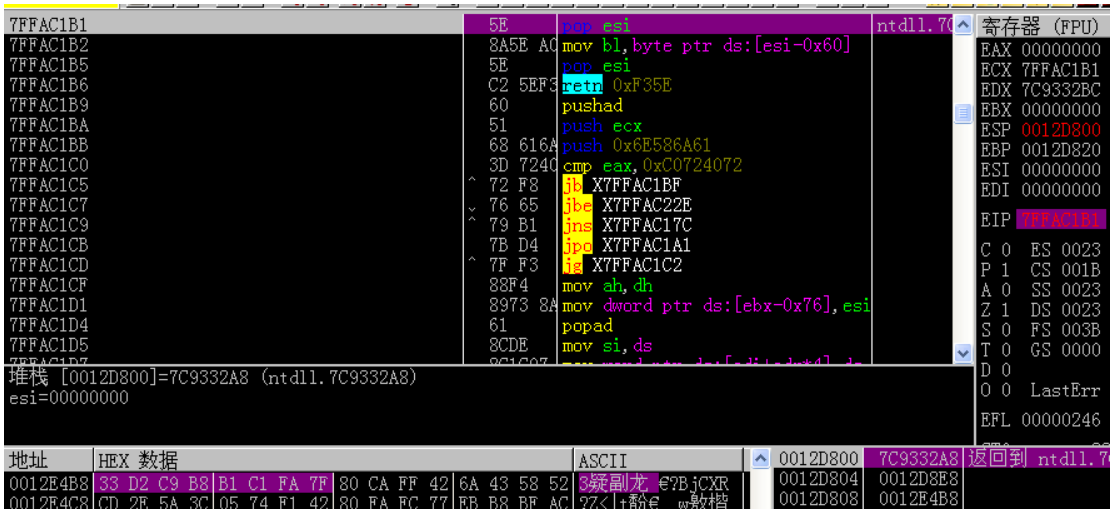


图 17 pop pop ret 指令串

来到 ntdll.7FFAC1B1,，是一个 pop pop ret 指令串。经过两个 pop 指令后，此时 esp 指向 12E4B8，shellcode 代码起始位置，Retn 执行后就来到了 shellcode。

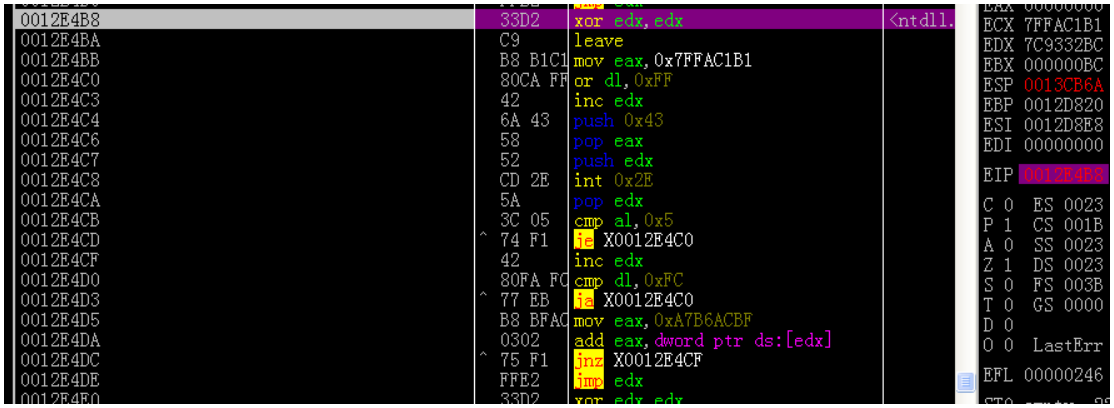


图 18 开始执行 shellcode

最后在临时目录中创建真正的 hwp 文档，启动 hwp 2007 目录下的 hwp.exe，载入临时目录的 tmp.hwp，释放并启动 msserver.exe（洋葱狗），ICEFOG 样本并没有释放。

第4章 C&C 分析

“洋葱狗”行动中相关样本进行通信主要分为两种，这也是我们区分“洋葱狗”版本的主要依据，主要是 2014 年基于硬编码 IP 进行通信和 2015 年基于暗网网桥（Onion.City）进行通信。下图是“洋葱狗”相关样本和 C&C 直接的对应关系。

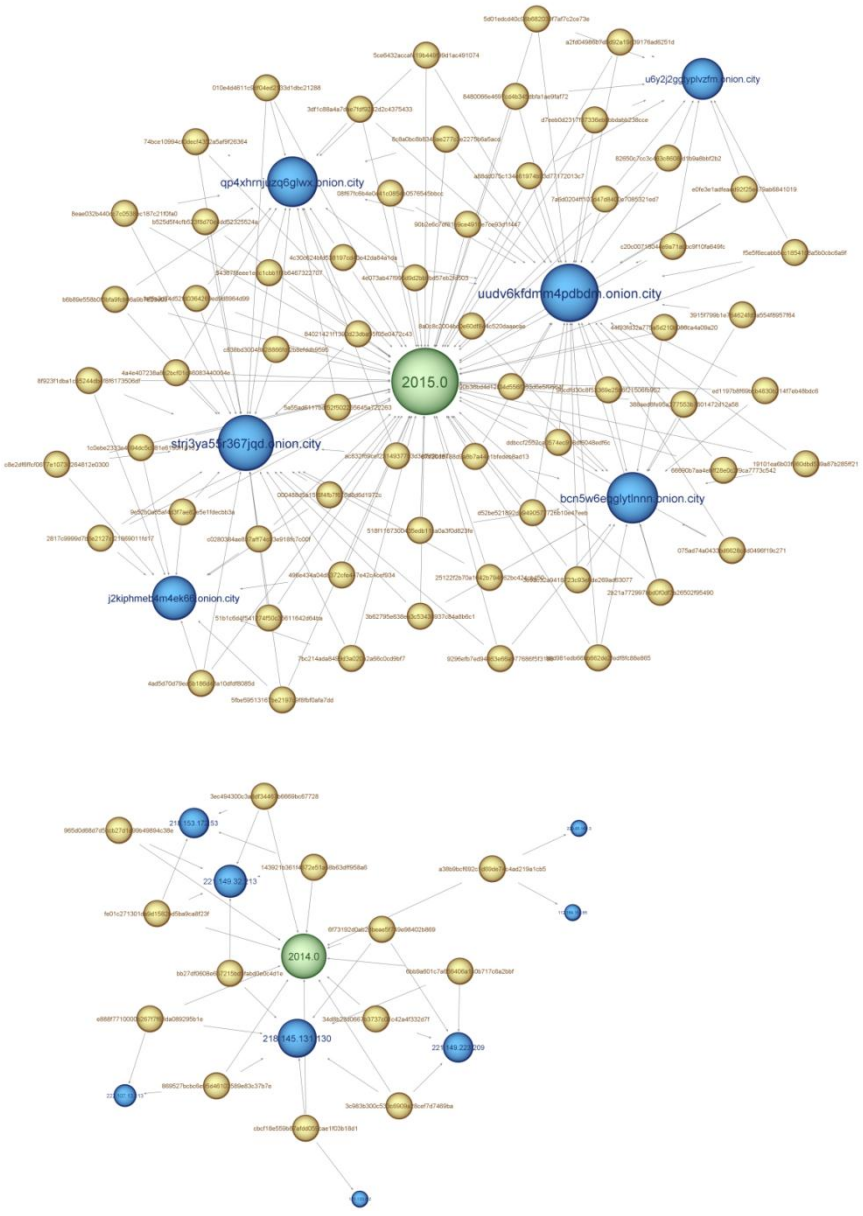


图 19 样本文件与 C&C 之间的关系

1. 暗网网桥（Onion.City）

涉及 onion.city 的具体 URL
hXXp://uudv6kfdmm4pdbdm.onion.city/main.php

hXXp://strj3ya55r367jqd.onion.city/main.php
hXXp://u6y2j2ggtyplvzfm.onion.city/index2.php
hXXp://qp4xhrnjuzq6glwx.onion.city/index2.php
hXXp://j2kiphmeb4m4ek66.onion.city/index2.php
hXXp://bcn5w6eqglytlnnn.onion.city/index2.php

表 7 相关 onion.city 链接

2015 年，“洋葱狗”的网络通信全面升级为暗网网桥（Onion.City），这也是目前 APT 黑客攻击中比较高端和隐蔽的网络通信方式。其中“index2.php”相关 URL 的作用是下载其他恶意代码，“main.php”相关 URL 是进行窃取数据的回传。

暗网网桥，是指暗网搜索引擎利用 Tor2web 代理技术，可以深度访问匿名的 Tor 网络，而无需再专门使用洋葱浏览器。“洋葱狗”正是利用暗网网桥将控制木马的服务器藏匿在 Tor 网络里。

2. 硬编码 IP

出现在 2013 年和 2014 年的恶意木马内的通信 C&C 均是直接连接 IP 地址，这些 IP 地址都是硬编码在恶意代码中。而且这些 IP 地址的地理位置均位于韩国，当然这并不意味着攻击者位于韩国，这些 IP 更可能只是傀儡机和跳板。

C&C IP	地理位置
218.153.172.53	韩国
218.145.131.130	韩国
222.107.13.113	韩国
221.149.32.213	韩国
221.149.223.209	韩国
220.85.160.3	韩国
112.169.154.65	韩国
121.133.8.2	韩国

表 8 相关硬编码 IP 和地理位置

第5章 ICEFOG“重生”：误导？嫁祸？

1. 关联分析中的惯性思维

在分析追溯“洋葱狗”攻击行动中，我们主要基于 360 威胁情报中心相关数据，目的是发现不同资源直接的关联性。期间主要发现了伪装 HWP 文档文件的 PE 恶意木马和 HWP 漏洞文档文件， HWP 漏洞文档除了包含诱饵文档和“洋葱狗”样本以外，比伪装 HWP 文档类型还多一个后门程序，如下图所示。

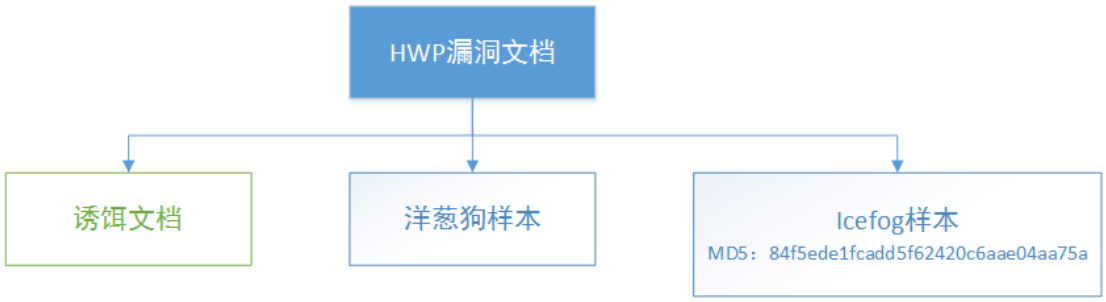


图 20 HWP 漏洞文档释放 3 类衍生物

针对该后门我们引擎扫描鉴定结果是 ICEFOG 家族，通过人工分析进一步确定该样本的确属于 ICEFOG，其中具备明显一些 ICEFOG 样本特征，如：加密内容存放位置“%TMP%\mstmpdata.dat”，数据与“&*^*@~^%9?i0h”进行异或，该后门 C&C 是 www.sejonng.org 等信息。

由于 ICEFOG 已经在 2013 年被卡巴斯基曝光，而 HWP 漏洞文档出现时间是 2014 年 7 月期间，所以我们通过分析该 ICEFOG 后门时间戳和在第三方机构（virustotal）最早出现时间（如下表所示），证明该 ICEFOG 后门的编译时间戳是可信的，且相关样本在卡巴斯基发布报告之前就已经存在，由此也基本证明该样本属于 ICEFOG。

ICEFOG 样本 MD5	84f5ede1fcadd5f62420c6aae04aa75a
ICEFOG 样本编译时间	2013-05-01 23:39:10
ICEFOG 样本 Virustotal 最早出现时间	2013 年 5 月 6 日
卡巴斯基发布 ICEFOG 报告时间[12]	2013 年 9 月 25 日
ICEFOG 样本 C&C	www.sejonng.org
C&C 曝光时间（ICEFOG 报告发布）	2013 年 9 月 25 日

表 9 HWP 漏洞文档包含的 ICEFOG 样本相关信息

	HWP 漏洞文档 1	HWP 漏洞文档 2
MD5	26b416d686ce57820e13e572e9e33cce	de00286f6128fb92002e0c0760855566
Malware tracker	2014 年 7 月 25 日	2014 年 8 月 18 日
virustotal	2014 年 7 月 25 日	2014 年 8 月 18 日
释放的“洋葱狗”MD5	bb27df0608e657215bd5fabd0e0c4d1e	869527bcbc6e95d46103589e83c37b7e

[12] The Icefog APT: A Tale of Cloak and Three Daggers,https://securelist.com/blog/research/57331/the-icefog-apt-a-tale-of-cloak-and-three-daggers/

“洋葱狗”编译时间	2014-07-18 10:36:46	2014-07-18 10:36:46
内嵌的 ICEFOG MD5	84f5ede1fcadd5f62420c6aae04aa75a	84f5ede1fcadd5f62420c6aae04aa75a
ICEFOG 编译时间	2013-05-01 23:39:10	2013-05-01 23:39:10
诱饵文档 MD5	9a4fafb0aa9f79dee2a117d237eaa931	843c6952e47564586a9094320f8d8c22
诱饵文档创建时间	2014 年 7 月 23 日	2014 年 7 月 23 日

表 10 HWP 漏洞文档相关资源信息列表

既然证明了该 ICEFOG 样本的真实性，那 ICEFOG 样本和“洋葱狗”样本由同一个 HWP 漏洞文档释放，从常规的关联分析思路，则认为 ICEFOG 与“洋葱狗”有联系，或许“洋葱狗”幕后是 ICEFOG 组织？

2. 剥茧抽丝：还原真相

起初我们也是猜测“洋葱狗”幕后或许是 ICEFOG 组织，但进一步发现“洋葱狗”HWP 漏洞文档是活跃在 2014 年 7 月左右，其他“洋葱狗”样本也主要活跃在 2013 年 10 月、2014 年 7、8 月和 2015 年 7、8、9 月相关时间范围内，另外卡巴斯基是在 9 月末就已经曝光了 ICEFOG 行动。所以这些都让我们不能完全确定之前的猜测，另外一般在安全机构曝光一个 APT 组织，该组织相关活动会暂时暂停，一般相关 C&C 和样本后门程序将不再继续使用，但也不排除攻击者为了尽可能多的达到目的而不惜暴露自身。

介于以上一些时间节点以及我们分析其他 APT 组织的经验来看，我们认为在一次新的攻击行动中攻击者使用了以往陈旧的后门工具，且相关后门程序以及 C&C 均都已经被曝光和查杀，这种情况攻击者的意图我们推测大概如下：

a、 攻击组织能力不足，迫于无奈只能使用陈旧技术和资源；

b、 攻击组织对相关目标环境非常了解，有信心基于陈旧技术和资源，也可以达到攻击目的；

c、 攻击组织使用其他组织特有的技术和资源，目的是嫁祸其他组织，干扰安全研究人员进行追溯。

首先我们对 HWP 漏洞文档在虚拟环境进行了相关测试，发现实际情况中 HWP 漏洞文档触发成功后首先会释放并打开诱饵文档，进一步释放并执行洋葱狗样本，而从始至终都没有释放 ICEFOG 样本。也就是当目标用户受到该 HWP 漏洞文档的攻击，只会安装并执行洋葱狗样本，而不会释放执行 ICEFOG 样本。这一现象让我们立即产生了怀疑，为何攻击者会将一个后续攻击中不使用的后门程序放到 HWP 漏洞文档中？

进一步我们带着以上这些疑点，将 HWP 漏洞文档相关资源进行深入的梳理，如下时间轴。除了以上我们分析到的 ICEFOG 本身时间戳和卡巴斯基曝光时间，以及 HWP 漏洞文档、“洋葱狗”相关样本相关活跃时间以外。下图中还有两个重要的时间节点，是关于 C&C 域名“www.sejonng.org”的域名状态。

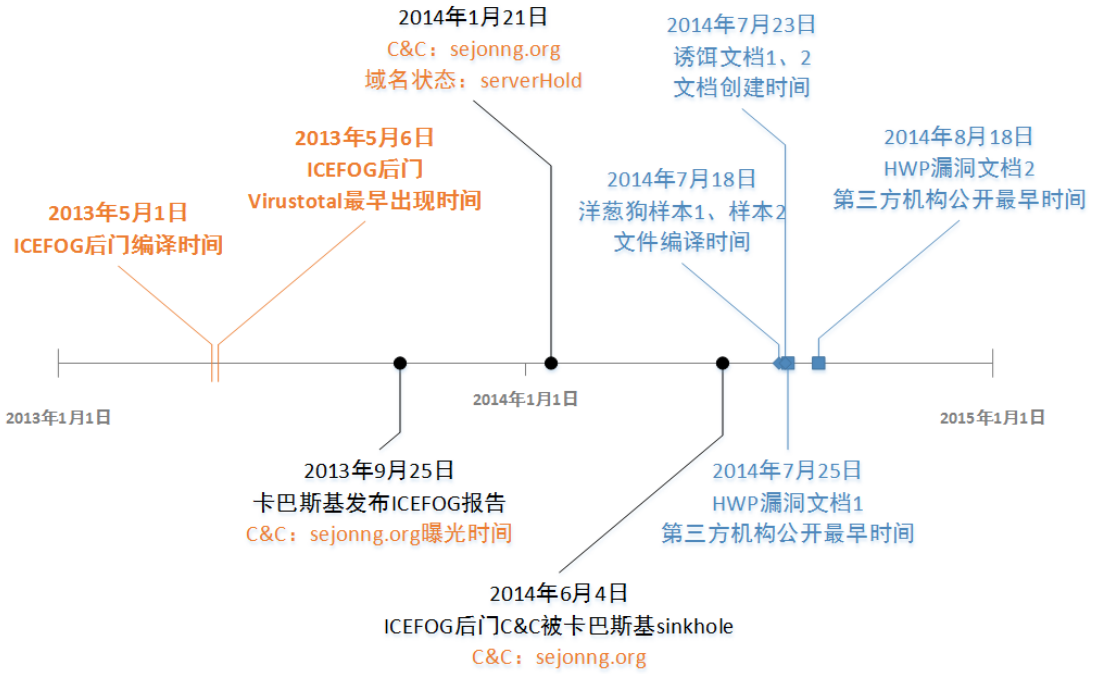


图 21 HWP 漏洞文档相关资源时间轴

在卡巴基斯 2013 年 9 月 25 日报告的 ICEFOG 报告中“www.sejonng.org”域名并没有标记为“SINKHOLED by Kaspersky Lab”，我们基于 domaintools[13]的 WHOIS 历史数据，发现“www.sejonng.org”域名在 2014 年 1 月 21 日的域名状态是“serverHold”（域名暂停解析[14]），进一步我们通过 domaintools 提供的网站页面截屏历史记录发现最晚在 2014 年 6 月 4 日“www.sejonng.org”域名[15]已经被卡巴斯基 sinkhole[16]了。

另外关于“www.sejonng.org”域名最新的 WHOIS 记录[17]是已经被 virustracker.info 接管进行 sinkhole 了。

[13] https://whois.domaintools.com/
[14] https://www.icann.org/en/system/files/files/epp-status-codes-30jun11-en.pdf
[15] https://research.domaintools.com/research/screenshot-history/sejonng.org/#0
[16] https://en.wikipedia.org/wiki/DNS_sinkhole
[17] https://whois.domaintools.com/sejonng.org

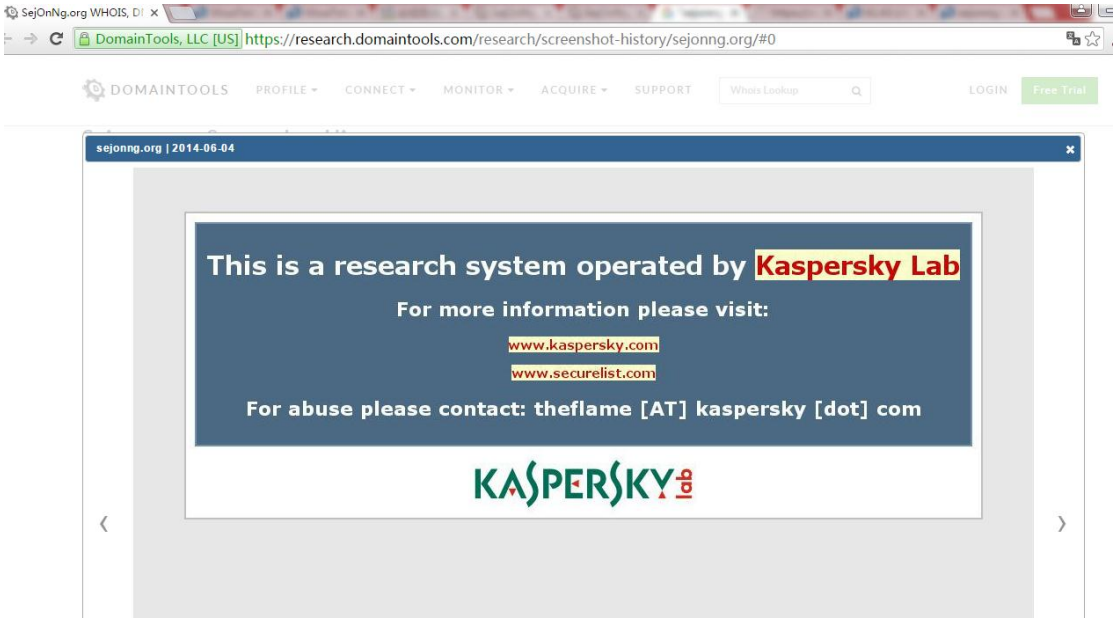
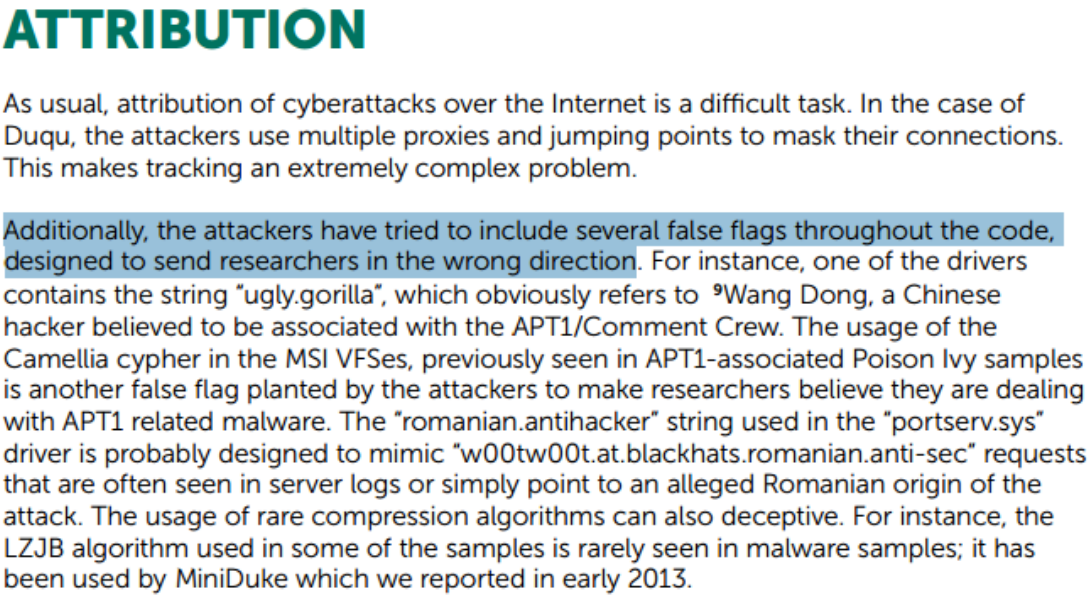


图 22“www.sejonng.org”相关历史页面截图（domaintools 数据）

我们推断攻击者在 2014 年 7 月将相关 HWP 漏洞文档投入使用的时候，其中 ICEFOG 后门程序的 C&C 域名的管理权限已经不再被攻击者所持有了。通过以上一些依据推测，我们更倾向于我们之前的第三点推测“攻击组织使用其他组织特有的技术和资源，目的是嫁祸其他组织，干扰安全研究人员进行追溯。”

其实在以往的 APT 攻击中，APT 组织构造一些虚假信息（假情报）来误导安全研究人员的情况也出现过，比如：卡巴斯基安全研究人员在分析 duqu2.0 的时候，发现了攻击者在代码中添加了一些虚假标识和使用罕见的压缩算法，目的是误导研究人员以为是与 APT1 或 MiniDuke 有关的恶意代码。



ATTRIBUTION

As usual, attribution of cyberattacks over the Internet is a difficult task. In the case of Duqu, the attackers use multiple proxies and jumping points to mask their connections. This makes tracking an extremely complex problem.

Additionally, the attackers have tried to include several false flags throughout the code, designed to send researchers in the wrong direction. For instance, one of the drivers contains the string "ugly.gorilla", which obviously refers to [9]Wang Dong, a Chinese hacker believed to be associated with the APT1/Comment Crew. The usage of the Camellia cypher in the MSI VFSes, previously seen in APT1-associated Poison Ivy samples is another false flag planted by the attackers to make researchers believe they are dealing with APT1 related malware. The "romanian.antihacker" string used in the "portserv.sys" driver is probably designed to mimic "w00tw00t.at.blackhats.romanian.anti-sec" requests that are often seen in server logs or simply point to an alleged Romanian origin of the attack. The usage of rare compression algorithms can also deceptive. For instance, the LZJB algorithm used in some of the samples is rarely seen in malware samples; it has been used by MiniDuke which we reported in early 2013.

图 23 引自卡巴斯基 duqu2.0 技术报告[18]

[18] THE DUQU 2.0 Technical Details，https://cdn.securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

第6章 特殊线索信息

1. PDB 路径

	相关样本	PDB 路径
PDB1[19]	10861ed5e2b01ba053d2659eebdce1a2	W:\2014 work\27 **APT-USB**\140701 APT\svcInstaller\Release\DeleteService.pdb
PDB2	a38b9bcf692c1d69de74c4ad219a1cb5	W:\2014 work\27 **APT-USB**\130701 APT\svcInstaller\Release\DeleteService.pdb
PDB3[20]	598f2b1b73144d6057bea7ef2f730269	W:\2013 work\130610 **APT**\svcInstaller\Release\DeleteService.pdb

表 11 典型 PDB 路径和样本对应列表

从上表我们看来 PDB（符号文件）路径中存在大量“APT”字样，另外相关 PDB 路径也 viruslab.tistory.com 网站曝光了。

2. 诱饵文档属性

文档属性	具体内容
样本 MD5	cbcf18e559b87afdd059cae1f03b18d1
诱饵文档 MD5	9a4fafb0aa9f79dee2a117d237eaa931
内容	韩国电力公司薪资
文档大小	25,088
作者	test1234
创建时间	2014 年 7 月 23 日 13:43:54
最后编辑时间	2014 年 7 月 24 日 8:41:30
最后编辑	**APT-WebServer**

表 12 典型 HWP 诱饵文档属性表

3. 韩文

通过分析我们发现恶意代码中出现了大量韩文信息，相关韩文信息是作为最终发送给 C&C 服务器数据包中的内容出现。

[19] http://viruslab.tistory.com/3534
[20] http://viruslab.tistory.com/3567

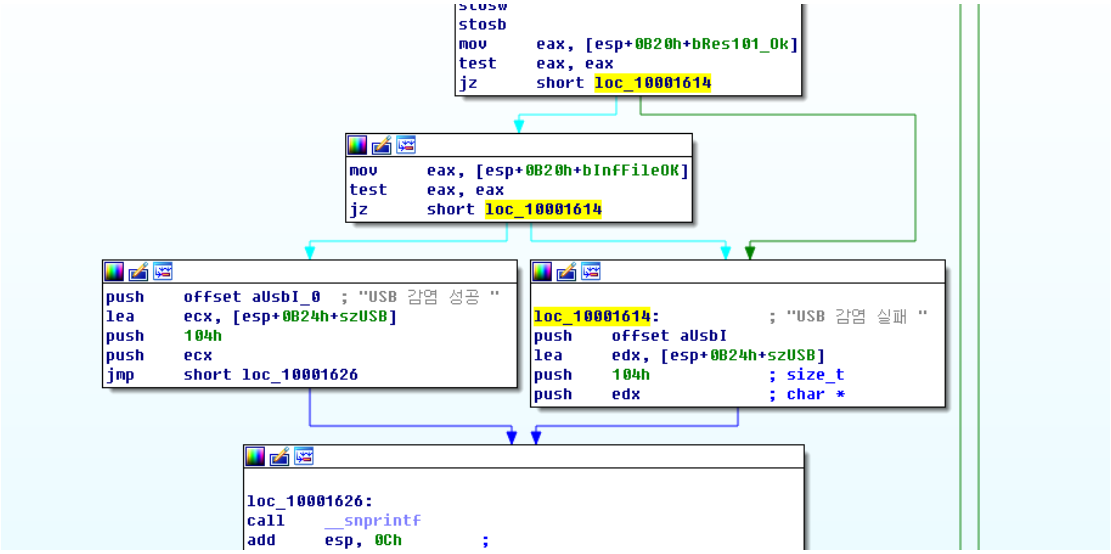
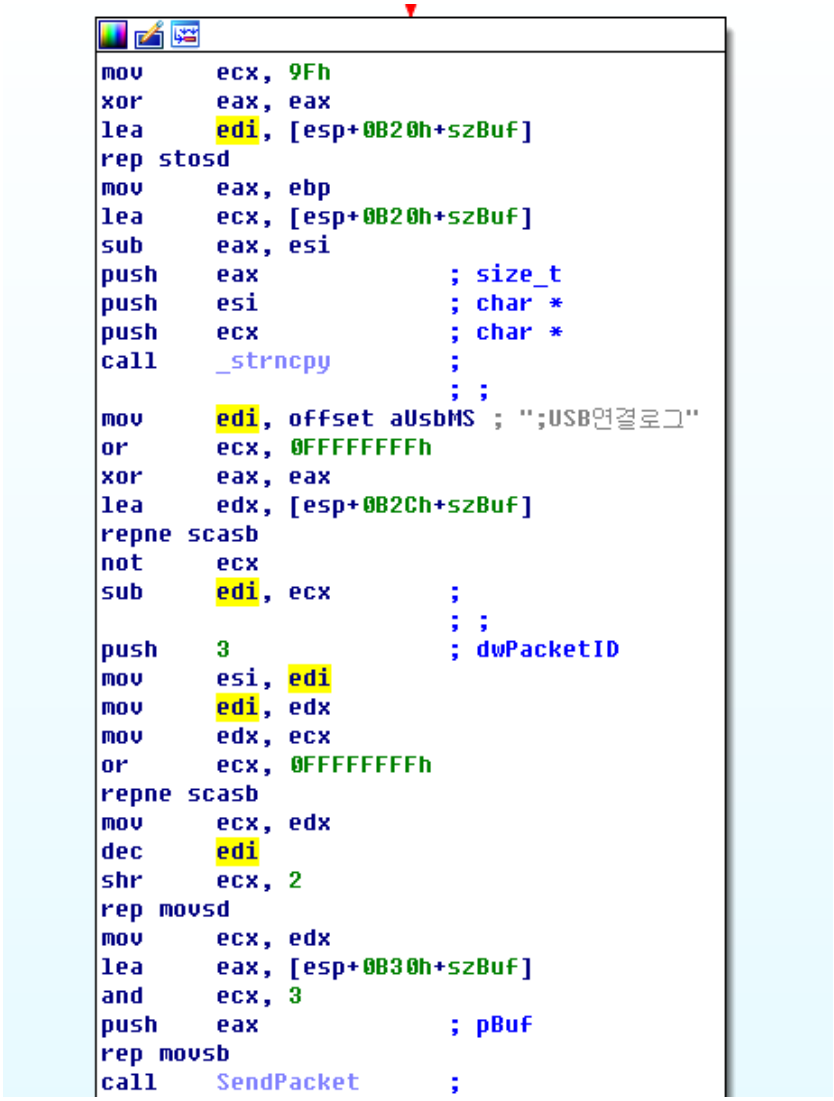


图 24 USB 感染成功/感染失败

```
loc_10002B60:
mov     ecx, 40h
xor     eax, eax
lea     edi, [esp+4CCh+szAgent+1]
mov     [esp+4CCh+szAgent], bl
rep stosd
stosw
push    offset aIAgentR ; "감염Agent실행 성
lea     ecx, [esp+4D0h+szAgent]
push    104h            ; size_t
push    ecx             ; char *
stosb
call    __snprintf
add     esp, 0Ch        ;
                        ; ;
call    GetMachineInfo  ;
                        ; ;
lea     edx, [esp+4CCh+SystemTime]
push    edx             ; lpSystemTime
call    ds:GetLocalTime ;
```

图 25 感染 Agent 运行成功



```
mov     ecx, 9Fh
xor     eax, eax
lea     edi, [esp+0B20h+szBuf]
rep stosd
mov     eax, ebp
lea     ecx, [esp+0B20h+szBuf]
sub     eax, esi
push    eax             ; size_t
push    esi             ; char *
push    ecx             ; char *
call    _strncpy        ;
                        ; ;
mov     edi, offset aUsbMS ; ";USB연결로그"
or      ecx, 0FFFFFFFFh
xor     eax, eax
lea     edx, [esp+0B2Ch+szBuf]
repne scasb
not     ecx
sub     edi, ecx        ;
                        ; ;
push    3               ; dwPacketID
mov     esi, edi
mov     edi, edx
mov     edx, ecx
or      ecx, 0FFFFFFFFh
repne scasb
mov     ecx, edx
dec     edi
shr     ecx, 2
rep movsd
mov     ecx, edx
lea     eax, [esp+0B30h+szBuf]
and     ecx, 3
push    eax             ; pBuf
rep movsb
call    SendPacket      ;
```

图 26 USB 连接日志

```
add     esp, 24h
lea     eax, [esp+0B10h+szDevicePath]
lea     ecx, [esp+0B10h+szDateTime]
push    offset aPcI     ; "PC 감염 성공"
push    edx
push    eax
push    offset szIP
push    offset a0_0_0_0 ; "0.0.0.0"
push    offset szMac
push    offset szUserName
push    offset szComputerName
push    ecx
push    offset aSSSSSSSCS ; "%s;%s;%s;%s;%s;%s;%s;%c;%s"
lea     edx, [esp+0B38h+szSendBuf]
push    635             ; size_t
push    edx             ; char *
call    __snprintf      ;
                        ; .
```

图 27 PC 感染成功

第7章 总结

近年来，针对基础行业设施和大型企业的黑客 APT 攻击活动频繁曝出，其中有的会攻击工控系统，如 Stuxnet（震网）、Black Energy（黑暗力量）等，直接产生巨大的破坏力；还有的则是以情报窃取为主要目的，如此前由卡巴斯基、AlienVault 实验室和 Novetta 等协作披露的 Lazarus 黑客组织，以及本次最新曝光的 OnionDog（洋葱狗），这类秘密活动的网络犯罪所造成的损失同样严重。

在“洋葱狗”的恶意代码活动中，有着近乎“强迫症”的规范：首先，恶意代码从被创建的 PDB（程序数据库文件）路径上，就有着严格的命名规则，例如 USB 蠕虫的路径是 APT-USB，钓鱼邮件恶意文档的路径是 APT-WebServer；当“洋葱狗”的木马成功释放后，它会请求 C&C（木马服务器），下载其它恶意程序并保存到%temp%目录，再统一以“XXX_YYY.jpg”形态作为文件名。这些名称都有着特定涵义，一般是指向攻击目标。种种迹象表明，“洋葱狗”对出击时间、攻击对象、漏洞挖掘和利用、恶意代码等整套流程都有着严密的组织和部署，同时它还非常重视隐藏自己的行迹。

2014 年，“洋葱狗”使用了韩国境内的多个硬编码 IP 作为木马服务器地址，当然这并不意味着攻击者位于韩国，这些 IP 更可能只是傀儡机和跳板。到了 2015 年，“洋葱狗”的网络通信全面升级为暗网网桥，这也是目前 APT 黑客攻击中比较高端和隐蔽的网络通信方式。

“洋葱狗”HWP 漏洞文档中包含 ICEFOG 样本这一资源之间存在联系的情况，让我们推测出该组织有可能存在使用其他已知 APT 组织特有的技术和资源，目的是嫁祸其他组织或干扰安全研究人员进行分析追溯。另外更多是对我们在对抗 APT 工作中的警示，无论是对研究方法还是对情报数据的不加甄别，而单一维度简单追溯关联，最终有可能被误导走入攻击者的陷阱。我们只能更加严谨，从不同维度去分析研究，最终做到客观陈述，避免主观臆断。

另外在推测 ICEFOG“重生”的工作中，我们除了基于自主的威胁情报数据，也使用了大量如 virustotal、domaintools，以及卡巴斯基等第三方厂商机构的相关分析结果或资源，不同来源的数据进过交叉验证，这样极大的保证了数据的可靠性。在以前安全厂商与恶意代码、APT 进行对抗，存在资源严重不对称的情况，我们希望从 2016 年开始通过各个厂商、机构等反 APT 领域之间的防守协作得到改善。