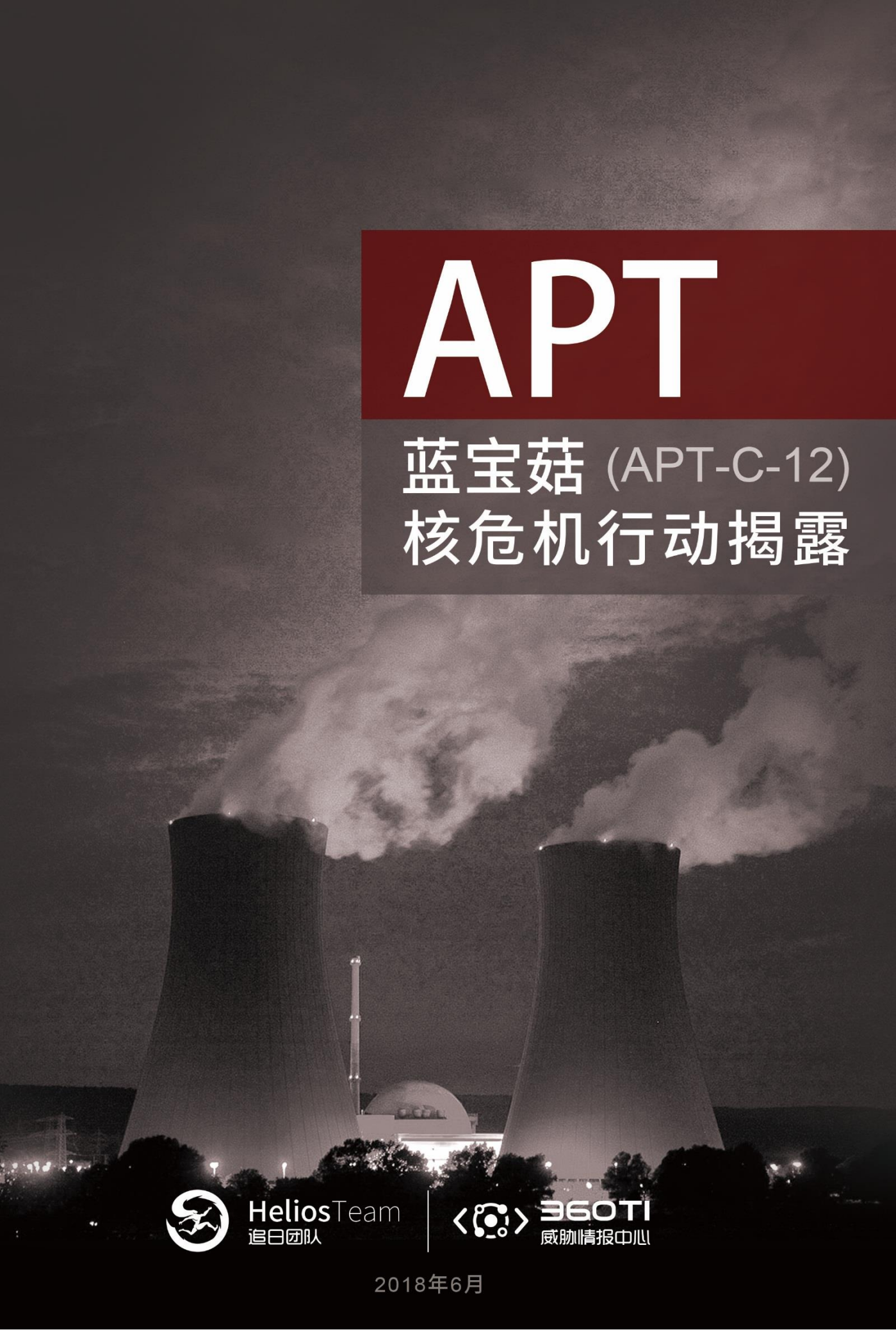


APT

蓝宝菇 (APT-C-12) 核危机行动揭露

HeliosTeam 追日团队

360TI 威胁情报中心

2018年6月

摘要

- 从 2011 年开始持续至今，高级攻击组织蓝宝菇（APT-C-12）对我国政府、军工、科研、金融等重点单位和部门进行了持续的网络间谍活动。该组织主要关注核工业和科研等相关信息。被攻击目标主要集中在中国大陆境内。
- 360 追日团队捕获的首个蓝宝菇组织专用木马出现在 2011 年 3 月左右。目前已总共捕获该组织恶意代码 670 余个，其中包括 60 余个专门用于横向移动的恶意插件。目前已经发现该组织相关的 C&C 域名、IP 数量多达 40 余个。
- 由于该组织相关恶意代码中出现特有的字符串（Poison Ivy 密码是：NuclearCrisis），结合该组织的攻击目标特点，360 威胁情报中心将该组织的一系列攻击行动命名为核危机行动（Operation NuclearCrisis），考虑到核武器爆炸时会产生蘑菇云，并结合该组织的一些其他特点及 360 威胁情报中心对 APT 组织的命名规则，我们将该组织名为蓝宝菇。
- 截止 2018 年 5 月，360 追日团队已经监测到核危机行动攻击针对的境内目标近 30 个。其中，教育科研机构占比最高，达 59.1%，其次是政府机构，占比为 18.2%，国防机构排第三，占 9.1%。其他还有事业单位、金融机构制造业等占比为 4.5%。

关键词：蓝宝菇、核危机、APT

目　　录

第一章　综述

从 2011 年开始持续至今，高级攻击组织蓝宝菇（APT-C-12）对我国政府、军工、科研、金融等重点单位和部门进行了持续的网络间谍活动。该组织主要关注核工业和科研等相关信息。被攻击目标主要集中在中国大陆境内。

360 追日团队捕获的首个蓝宝菇组织专用木马出现在 2011 年 3 月左右。目前已总共捕获该组织恶意代码 670 余个，这些恶意代码可分为 4 类 RAT，细分版本为 7 种。其中，还包括 60 余个专门用于横向移动的恶意插件，从功能区分来看也至少有 5 种。目前已经发现该组织相关的 C&C 域名、IP 数量多达 40 余个。

由于该组织相关恶意代码中出现特有的字符串（Poison Ivy 密码是：NuclearCrisis），结合该组织的攻击目标特点，360 威胁情报中心将该组织的一系列攻击行动命名为核危机行动（Operation NuclearCrisis），考虑到核武器爆炸时会产生蘑菇云，并结合该组织的一些其他特点及 360 威胁情报中心对 APT 组织的命名规则，我们将该组织名为蓝宝菇。

在核危机行动针对中国的网络间谍活动中，下述相关时间点值得关注：

1） 2011 年 3 月，首次发现与该组织相关的木马，针对政府相关机构进行攻击。

2） 2011 年 11 月，对某核工业研究机构进行攻击。

3） 2012 年 1 月，对某大型科研机构进行攻击。

4） 2012 年 3 月，对某军事机构进行攻击。

5） 2012 年 6 月，对国内多所顶尖大学进行攻击。

6） 2013 年 6 月，对某中央直属机构进行攻击，同时开始使用新类型的 RAT。

7） 2014 年 8 月，发现该组织使用 5 种以上的横向移动恶意代码针对重点目标机构进行大量横向移动攻击。

8） 2014 年 12 月，发现新的 RAT，我们将其命名为 Bfnet，该后门具备窃取指定扩展名文档等重要功能。

9） 2015 年 9 月，针对多个国家的华侨办事机构进行攻击。

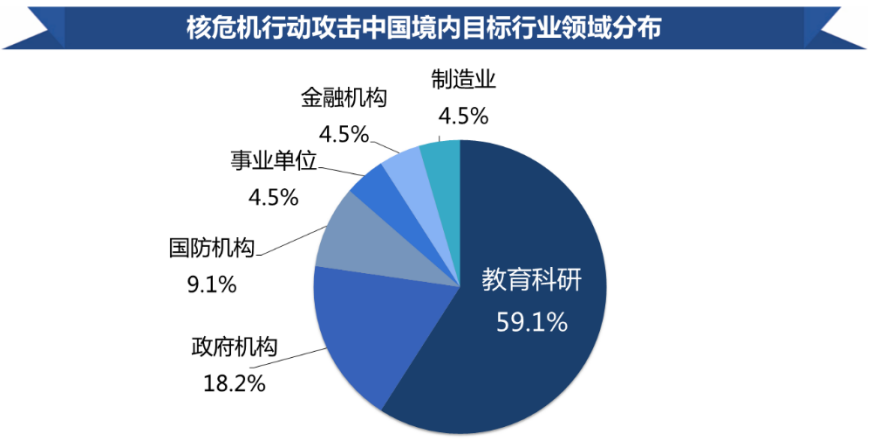
10）2018 年 4 月，针对国内某重要敏感金融机构发动鱼叉邮件攻击。

注：以上所述的“首次发现”时间，仅是我们目前已经了解掌握的情况，不代表我们已经掌握了该组织的全部攻击事件和行为。

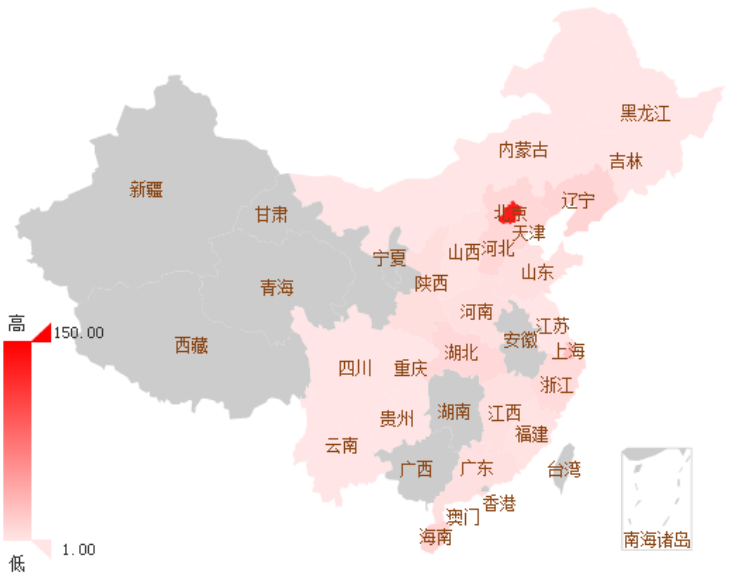
第二章　攻击目的和受害分析

一、　行业分布

截止 2018 年 5 月，360 追日团队已经监测到核危机行动攻击的境内目标近 30 个。其中，教育科研机构占比最高，达 59.1%，其次是政府机构，占比为 18.2%，国防机构排第三，占 9.1%。其他还有事业单位、金融机构制造业等占比为 4.5%。



二、　地域分布



中国北京地区是核危机行动攻击的重点区域，其次是上海、海南等地区。

第三章　持续的网络间谍活动

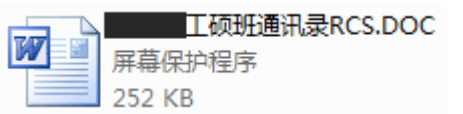
一、　初始攻击

在核危机行动的多次攻击中，我们发现其初始攻击主要采用鱼叉邮件携带二进制可执行文件这种攻击方法。攻击者仿冒官方邮件向受害者发送鱼叉邮件，诱导受害者点击邮件所携带的恶意附件。

（一） RLO[1]伪装文档扩展名

在攻击的初期，攻击者使用的邮件附件多为一个 WinRAR 压缩包，其中包含伪装成 Word 文档的 SCR 文件。

下图为核危机行动鱼叉邮件压缩包中的一个伪装成 Word 文件的专用木马的图标和文件名截图。该文件伪装成一份通信录文件，同时，为了更好的伪装诱饵文档，攻击者使用了 RLO 控制符。RLO 控制符是 Unicode 控制符的一种，用来显示中东文字，中东文字的书写顺序是从右到左的。攻击者通过在文件名中插入 RLO 控制符，使得字符的显示顺序变成从右至左，从而来隐藏文件的真实扩展名。



MD5	文件名	病毒名
a2c***7dcf**	****工硕班通讯录 RCS.DOC（真实扩展名.SCR）	Dropper.Win32.FakeDoc

表 1 核危机行动伪装成通讯录的专用木马 1

当受害者点击打开这个伪装成 Word 文档的专用木马后，木马会在释放攻击代码的同时，释放一个真正的 Word 文档。下图为该诱饵 Word 文档打开后的信息内容，其中信息确实是一份详细的通讯录。可见，该组织在文件伪装方面确实下足了功夫。

[1] RLO，http://en.wikipedia.org/wiki/Unicode_character_property

下面是我们截获的另外一个使用了 RLO 伪装，同时伪装成通讯录的专用木马样本信息及该样本打开后的截图。

MD5	文件名	病毒名
e26******** **********65f0**	第六组通讯录更新 SRCS.DOC （真实扩展名.SCR）	Dropper.Win32 .FakeDoc

表 2 核危机行动伪装成通讯录的专用木马 2

下面是我们截获的第三个使用了 RLO 伪装的专用木马样本信息及该样本打开后的截图。该文件的文件名格式伪装方法与前述两个样本相同，但具体内容则伪装成了一份智库文件。

MD5	文件名	病毒名
e26******** ********65f0**	《****智库》SRCS.DOC（真实扩展名.SCR）	Dropper.Win32.FakeDoc

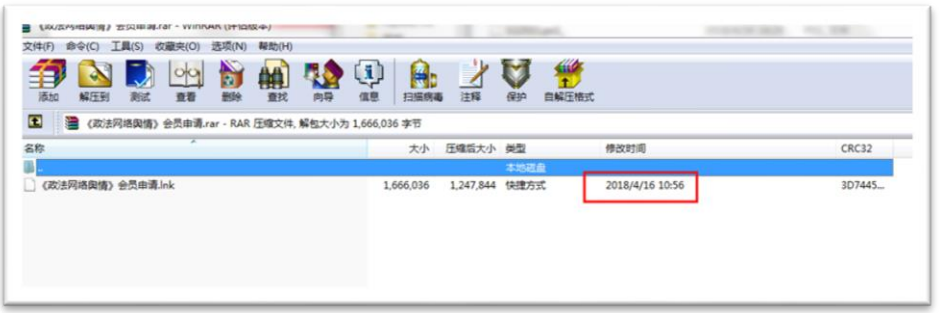
表 3 核危机行动伪装成某智库文件的专用木马

（二） LNK 文件

2018 年 4 月，我们捕获到了一次核危机行动的最新攻击活动。某些重要的政府和企业机构的邮箱用户收到一份发自 boaostaff[@]163.com 的鱼叉邮件，鱼叉邮件仿冒博鳌亚洲论坛主办方向受害者发送了一封邀请函：

邮件附件是一个 163 邮箱的云附件，为 RAR 压缩包文件。点开云附件，会跳转到对应的云端下载地址将附件下载到本地，这一过程与早期的攻击活动大致相同。

不同的是，此次新攻击下载得到的附件包含的是一个恶意 LNK 文件：



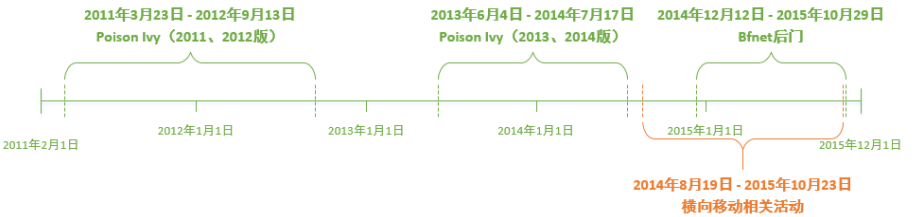
一旦受害者被诱导打开该 LNK 文件，LNK 文件便会通过执行文件中附带的 PowerShell 恶意脚本来收集上传用户电脑中的敏感文件，并安装持久化后门程序长期监控用户计算机。

二、 持续渗透

核危机行动从 2011 年 3 月开始一直持续至今，我们总共捕获到 4 种 RAT，细分版本达到 7 种，另外发现大量横向移动的恶意代码，从功能区分至少有

5 种。

从时间段上看，在 2011-2012 年，核危机行动所使用的主要攻击木马是 Poison Ivy；而到了 2013-2014 年，Poison Ivy 虽然仍在继续使用，但被升级到了几个全新的版本；2014 年三季度--2015 年，核危机行动开始大量进行横向移动攻击，并从 2014 年底开始，使用 Bfnet 后门。



下面就对核危机行动在上述几个阶段攻击活动的主要特点进行简要的分析说明。

（一） 2011-2012 年

通过深入分析，我们发现该攻击组织每次在发起新的攻击时，往往都会采用不同以往的诱饵文件名。如在 2012 年 1 月中旬至下旬期间，主要采用“2012 龙年运程”和“龙年贺卡”这两个文件名。就该组织这一特性，我们对其在 2011-2012 年的攻击行动中所使用的诱饵文件名进行了相关统计分析：

1） 2011 年主要诱饵文档文件名

通信录类：通讯录、***工硕班通讯录、第**组通讯录更新、***第 13 期驻外人员培训班人员通讯录。

其他：**战略、《****智库》约稿 S、《国家**》S、Taitravel、*****万言书-***2012。

2） 2012 年主要诱饵文档文件名

太子传奇系列：如，太子传奇 B、太子传奇 C、太子传奇 E 等（以英文字母编号的“太子传奇”系列文件供发现近 20 种）。

其他：****全家福_pan、龙年贺卡 MA、宝贝 S、88 届十二队通讯录、2012 龙年运程、******基金重大项目研究选题推荐表。

特别值得一提的是：攻击者除了对诱饵文件的文件名进行了精心的伪装之外，对诱饵文件的内容也进行了精心的设计。以最为频繁使用的“通信录”诱饵文件为例：被打开的 Word 文档的内容确实为相关机构人员或相关培训参与者的详细通信录信息，而且有持续的更新，如前面截图案例所示。这就使得被攻击者很难识破其中的攻击行为。同时，考虑到被攻击目标本身所处机构的敏感性，我们有理由认为，攻击者在发起攻击的过程中，已经对攻击

的目标机构或个人有了比较充分的了解。

从木马的类型来看，在 2011-2012 年的攻击中，核危机行动主要采用了 Poison Ivy 这款专用木马，其在本质上一款远程控制木马程序，对应的 Poison Ivy 木马生成器版本主要为 2.3.2。Poison Ivy 木马生成器从 1.0.0 版本开始总共 10 个版本，最新版本为 2.3.2。Poison Ivy 木马生成器可以生成 exe 和 ShellCode 两种版本的木马。在核危机行动中，我们目前已经截获的 Poison Ivy 专用木马均为 ShellCode 形态。

（二） 2013-2014 年

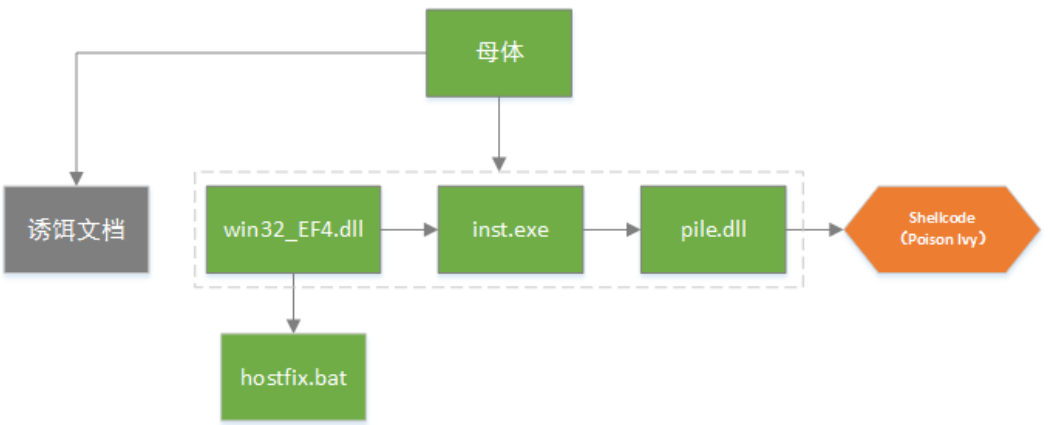
2013-2014 年，核危机行动中所使用的 Poison Ivy 与 2011-2012 的版本相比有较大的改动和升级，但仍可通过大数据及多维分析，发现其同源性。

Poison Ivy 的 2013 版本与 2014 版本的一个主要区别是“inst.exe”和“pile.dll”释放的路径不同。

2014 版本的路径为：%APPDATA%/Microsoft/Internet Explorer/

2013 版本的路径为：%TEMP%/

下图给出了核危机行动 2013-2014 版的 Poison Ivy 专用木马的执行流程。



（三） Bfnet 后门

Bfnet 是一种此前未知的 RAT，目前我们捕获到 Bfnet 有两个版本：Bfnet2014 和 Bfnet2015。

Bfnet 后门的母体大多为利用文档图标的 PE 程序，执行后会释放相关后门程序（早期版本只是一个 DLL 文件，最新版本会有多个文件）和后门配置文件（内容主要是上线地址、端口和 ID）。另外木马在执行的同时会将内置的诱饵文档打开来迷惑被攻击对象。

Bfnet 释放的后门程序会修改开始菜单的程序里面的所有快捷方式：在

实现快捷方式的正常功能的同时，指向 rundll32，加载运行 dll 后门程序。

特别的，Bfnet 后门会针对 WPS 程序进行专门攻击。Bfnet 执行后会删除 TEMP 目录和 LOCALAPPDATA 目录下 WPS 程序，具体是删除 WPS 更新程序：wpsupdate.exe、updateself.exe，删除 WPS 通知程序：desktoptip.exe、wpsnotify.exe。下图是 Bfnet 删除 WPS 相关程序代码截图

```
sub_10001303(L"del /s /F /q \"%TEMP%\\..\\Application Data\\Kingsoft\\WPS Office\\wpsupdate.exe\"");
sub_10001303(L"del /s /F /q \"%TEMP%\\..\\Application Data\\Kingsoft\\WPS Office\\wpsnotify.exe\"");
sub_10001303(L"del /s /F /q \"%TEMP%\\..\\Application Data\\Kingsoft\\WPS Office\\desktoptip.exe\"");
sub_10001303(L"del /s /F /q \"%TEMP%\\..\\Application Data\\Kingsoft\\WPS Office\\updateself.exe\"");
sub_10001303(L"del /s /F /q \"%LOCALAPPDATA%\\Kingsoft\\WPS Office\\wpsupdate.exe\"");
sub_10001303(L"del /s /F /q \"%LOCALAPPDATA%\\Kingsoft\\WPS Office\\wpsnotify.exe\"");
sub_10001303(L"del /s /F /q \"%LOCALAPPDATA%\\Kingsoft\\WPS Office\\desktoptip.exe\"");
```

Bfnet 后门的 2015 版和 2014 版之间也有一定的差异。2015 版除了部分指令和功能有变化外，还增加了加密功能，会对部分关键字符串进行加密。

（四） 对抗技术

核危机行动中所使用的专用木马，采用了一定程度的对抗技术。主要表现在两个方面：一方面是杀软对抗技术，一个是反虚拟机技术。

1） 杀软对抗技术

Poison Ivy 母体会判断系统中是否有瑞星进程，如果有则会将 Poison Ivy 的 ShellCode 中注入默认浏览器的操作（在 ShellCode 的尾部）代码删除。

另外，母体还会判断是否有 360、卡巴斯基、金山的进程，但通常只是做判断而不做后续操作。一个比较特殊的操作是：在核危机行动 2013-2014 版的 Poison Ivy 中，木马一旦发现系统中有 360、卡巴斯基等杀软存在，就会用 ICMP 协议发送一条固定数据到一个指定的服务器。这条固定数据如下：

“!"#$%&'()*+,-./0123456789:;<=>?”

2） 反虚拟机技术

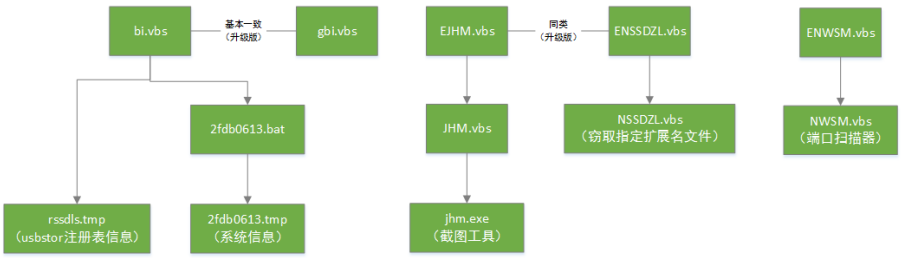
我们在核危机行动的多个代码中，都发现了一个特殊的导出函数 szFile。导出函数 szFile 是一个 104 字节大小的字符串数组，运行的时候会动态填写字符串“VirtualAlloc”，并动态修改 PE 中导出表的大小为“0X80000000”，这样调用 GetProcAddress(handle,""szFile") 的时候会返回 VirtualAlloc 的地址，这样可以对抗轻量级的虚拟机。

（五） 插件分析

我们截获了很多核危机行动的功能插件，疑似是 Bfnet 的其他功能插件，或者通过 Bfnet 下放的其他恶意程序。相关插件工具都是攻击者对被感染机器进行筛选后进一步定向投放的，不同目标存在的插件工具不同。

相关插件工具主要是进一步探测用户环境和窃取指定用户文件，整体偏

向横向移动的作用。下图给出了部分插件及其作用分析。



1） NSSDZL.vbs

该文件是由 ENSSDZL.vbs 文件释放出来，NSSDZL.vbs 的主要功能是将指定文件（通过指定文件扩展名）拷贝到指定目录（usb_tmp）。相关文件扩展名包括：PDF，DOC，DOCX，XLS，XLSX，PPT，PPTX，WPS，ET，DPS，7Z，ZIP，RAR

2） NWSM.vbs

NWSM.vbs 是由 ENWSM.vbs 释放。NWSM.vbs 功能最为复杂，包含内网渗透，并且通过流试方式写入脚本。

3） C0A80101.vbs 等其他 9 个同类脚本

这些脚本会查看局域网其他 IP（手动指定）的 NetBIOS 信息，包括计算机名、MAC 地址；查看远程计算机服务及状态；将批处理文件通过流试方式写入到：“当前文件名”.tmp:smzl.dat。

4） rar.bat 等其他 7 个同类脚本

使用 rar.exe 打包加密指定目录的制定扩展名文件，包括：doc、docx、pdf、pptx、ppt、xls、xlsx 等，密码为 1q2w3e4r5t，按照 2M 的大小分割，打包到“%temp%\360scanA248DDEGB**GC.log（其中，**是 2 个数字）”中，并且设置"%temp%"目录下的.log 和.rar 为隐藏属性。

5） Jhm.exe

这是一个攻击者自己开发的截图工具，截图到"%temp%"目录或当前目录下，命名为 2ce605ed.tmp 或 2ce605ed.bmp（不同版本路径不同，但文件名相同，有的需要 JHM.vbs 配合移动文件到%temp%目录）。

PDB 路径：C:\Users\Lab08612\Documents\Visual Studio 2012\Projects\ c++ print screen\Release\cprintscreen.pdb

6） otb.exe

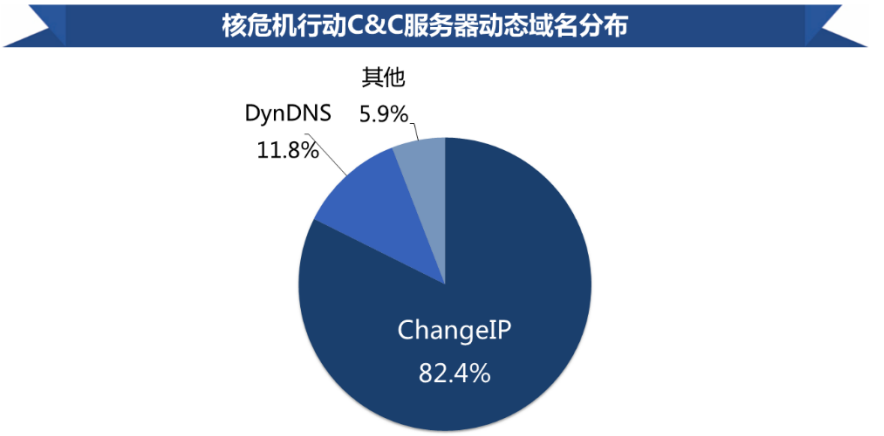
这个插件的功能主要是盗取 Outlook 密码。一种方式是输出 Outlook 密

码到控制台（无需参数），一种方式是输出 Outlook 密码到指定文件（需要参数：-f + 文件路径）

三、 C&C 分析

核危机行动在不同的时期选择的 C&C（控制服务器）有较大变化。在 2011-2012 年期间主要以动态域名为主，动态域名服务商的选择是以境外 ChangeIP 为主；从 2013 年开始逐渐转为直接访问指定 IP，Bfnet 两个版本的后门均访问指定 IP，而不再通过域名解析 IP。

截止 2018 年 5 月，360 追日团队共截获核危机行动相关 C&C 服务器动态域名 20 余个，固定 IP 地址 20 余个。在动态域名中，ChangeIP 域名占 82.4%，DynDNS 域名占 11.8%，其他占 5.9%。



核危机行动所采用的域名，很多还具有明显的含义，如 360、土豆、新浪等知名网站域名都被用来做了动态域名的注册子域名。如：

视频类 Youtube、tudou

购物类 Tmall

手机类 android23、iphone5

互联网综合类 360sc2、sohu、sogou、sina、baidu2

以下是核危机行动中所使用的部分指定 IP：

韩国：210.***.***.90、210.***.***.90

美国：162.***.***.33、173.***.***.200

加拿大：63.***.***.25

巴西：200.***.***.22

瑞典：95.***.***.37

还有一点值得注意的是，在目前已经截获的核危机行动的 RAT 中，部分 RAT 会内会内置两个 IP，其中一个 IP 是专门用来迷惑分析人员的。

附录1 360 追日团队（Helios Team）

360 追日团队（Helios Team）是 360 公司高级威胁研究团队，从事 APT 攻击发现与追踪、互联网安全事件应急响应、黑客产业链挖掘和研究等工作。团队成立于 2014 年 12 月，通过整合 360 公司海量安全大数据，实现了威胁情报快速关联溯源，独家首次发现并追踪了三十余个 APT 组织及黑客团伙，大大拓宽了国内关于黑客产业的研究视野，填补了国内 APT 研究的空白，并为大量企业和政府机构提供安全威胁评估及解决方案输出。

联系方式

邮箱：360zhuiri@360.cn

微信公众号：360 追日团队

扫描右侧二维码关微信公众号

附录2 360 安全监测与响应中心

360 安全监测与响应中心，是 360 为服务广大政企机构而建立的网络安全服务平台，旨在第一时间为政企机构提供突发网络安全事件的预警、通告，处置建议、技术分析和 360 安全产品解决方案。突发网络安全事件包括但不限于：安全漏洞、木马病毒、信息泄露、黑客活动、攻击组织等。

360 安全监测与响应中心兼具安全监测与响应能力：中心结合 360 安全大数据监测能力与海量威胁情报分析能力，能够全天候、全方位的监测和捕获各类突发网络安全事件；同时，基于 10 余年来为全国数万家大型政企机构提供安全服务和应急响应处置经验，中心能够在第一时间为政企机构应对突发网络安全事件提供有效的处置措施建议和应急响应方案。

在 2017 年 5 月发生的永恒之蓝勒索蠕虫（WannaCry）攻击事件中，360 安全监测与响应中心在 72 小时内，连续发布 9 份安全预警通告，7 份安全修复指南和 6 个专业技术工具，帮助和指导全国十万余家政企机构应对危机。

A-TEAM 是 360 安全监测与响应中心下属的一支专业技术研究团队，主要专注于 Web 渗透与 APT 攻防技术研究，并持续展开前瞻性攻防工具预研，以提前探知更多的未知威胁、新兴威胁。A-TEAM 的技术研究从底层原理、协议实现入手，能够深度还原攻与防的技术本质。

附录3 360 威胁情报中心

360 威胁情报中心由全球最大的互联网安全公司奇虎 360 特别成立，是中国首个面向企业和机构的互联网威胁情报整合专业机构。该中心以业界领先的安全大数据资源为基础，基于 360 长期积累的核心安全技术，依托亚太地区顶级的安全人才团队，通过强大的大数据能力，实现全网威胁情报的即时、全面、深入的整合与分析，为企业和机构提供安全管理与防护的网络威胁预警与情报。

360 威胁情报中心对外服务平台网址为 https://ti.360.net/。服务平台以海量多维度网络空间安全数据为基础，为安全分析人员及各类企业用户提供基础数据的查询，攻击线索拓展，事件背景研判，攻击组织解析，研究报告下载等多种维度的威胁情报数据与威胁情报服务。

微信公众号：360 威胁情报中心

关注二维码：