部分利用社工技巧的群发邮件样本关联分析

安天实验室

首次发布时间：2015 年 04 月 28 日 16 时 37 分

本版本更新时间：2015 年 05 月 27 日 16 时 37 分

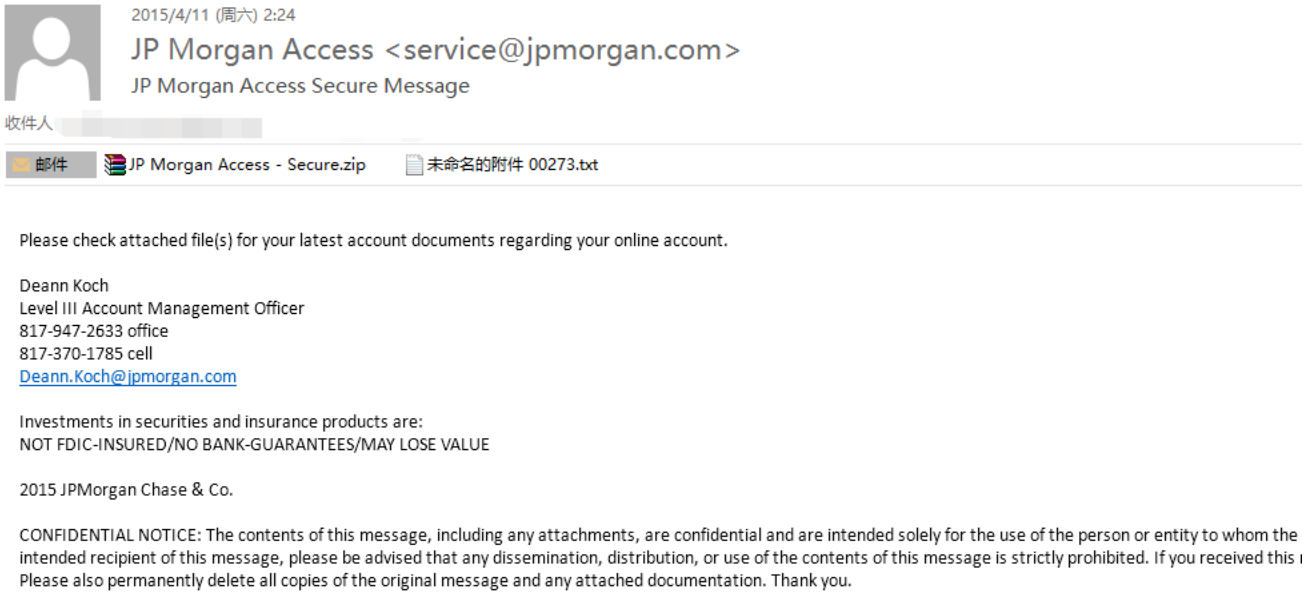
目 录

1 背景

近年来，安天诱饵信箱系统持续捕获大量利用社工技巧进行批量传播的带毒邮件。安天分析人员从诱饵信箱中随机抽取了两封附件攻击手段一致的邮件作为分析起点。其中第一封邮件的捕获时间为 2015 年 4 月 11 号，这是一封伪装成摩根大通集团的钓鱼邮件，邮件包括一个 ZIP 压缩包，压缩包解压后是一个 PDF 图标的 PE 文件，运行 PE 文件后会从后端下载其它文件，另一封邮件的捕获时间为 2015 年 4 月 13 号，这两封邮件的附件行为一致。安天 CERT 分析人员首先对第一封邮件样本进行了分析，随后对两封邮件的传播手段、附件文件的技巧方法进行了关联，最后通过提取类似特点挖掘出更多的类似攻击邮件进行了整体的关联分析与总结。

2 邮件一分析

邮件一内容：


2015/4/11 (周六) 2:24

JP Morgan Access <service@jpmorgan.com>

JP Morgan Access Secure Message

收件人

邮件 JP Morgan Access - Secure.zip 未命名的附件 00273.txt

Please check attached file(s) for your latest account documents regarding your online account.

Deann Koch
Level III Account Management Officer
817-947-2633 office
817-370-1785 cell
Deann.Koch@jpmorgan.com

Investments in securities and insurance products are:
NOT FDIC-INSURED/NO BANK-GUARANTEES/MAY LOSE VALUE

2015 JPMorgan Chase & Co.

CONFIDENTIAL NOTICE: The contents of this message, including any attachments, are confidential and are intended solely for the use of the person or entity to whom the intended recipient of this message, please be advised that any dissemination, distribution, or use of the contents of this message is strictly prohibited. If you received this
Please also permanently delete all copies of the original message and any attached documentation. Thank you.

图 1 原始邮件正文

邮件内容翻译如下：

请检查附件了解您的在线帐户的最新的帐户文件，

Deann Koch

三级账户管理主任

817-947-2633 办公

817-370-1785 分机

Deann.Koch@jpmorgan.com

证券和保险产品的投资有：

无 FDIC 保险/无银行担保/ MAY LOSE VALUE

2015 年摩根大通

特别提醒：此消息中的内容，包括任何附件，是保密的，仅发送给个人实体使用者。如果您不是此消息的预期收件人，请注意，任何传播，分发或使用该消息的内容是严格禁止的。如果你错误的接收到了此邮件，请通知发信人。同时永久删除原始邮件和任何连接文档的所有副本。谢谢。

2.1 邮件元数据提取

邮件主题	JP Morgan Access Secure Message
发送时间	2015/4/11 (周六) 2:24
发件人	JP Morgan Access [service@jpmorgan.com]
附件 1 名称	JP Morgan Access – Secure.zip
附件 2 名称	未命名的附件 00273.txt

该邮件是假冒摩根大通集团发送。

注：摩根大通集团是全球盈利最佳的银行之一，总部位于美国纽约市，2008 年总资产 20,360 亿美元，总存款 10,093 亿美元，占美国存款总额 10.51%的比例居第二，商业银行部旗下分行 5410 家。2011 年 10 月，摩根大通的资产规模超越美国银行成为美国最大的金融服务机构。(信息来源为:维基百科)

该邮件利用社会工程学技巧诱使用户打开。社会工程学攻击是一种利用人性的心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱所采取的欺骗、伤害来进行收益的手段。邮件恶意代码的社会工程学的攻击手段主要通过发送带有欺骗、伪装等主题内容的邮件，诱使受害者点击附件。该邮件利用摩根银行拥有庞大的用户群这一事实，通过在线银行的账户文件的敏感话题为诱饵，引诱用户点击附件查看账单，并且“特别提醒”声称邮件内容为机密信息。如果用户并没有摩根的在线银行或者错误的接收到此邮件，看到机密信息内容通过社会工程学特点处于好奇心也会对此附件感兴趣。

邮件附件是一个下载者病毒，邮件附件为一个 ZIP 压缩包，压缩包解压后是个以 PDF 为图标且扩展名为 src 的文件，src 为屏幕保护程序的扩展名，实际上是一个 PE 可执行程序，通过多数人对此并不了解的情况下双击之，也会自动运行 PE 文件。以下为邮件结构和行为链图。

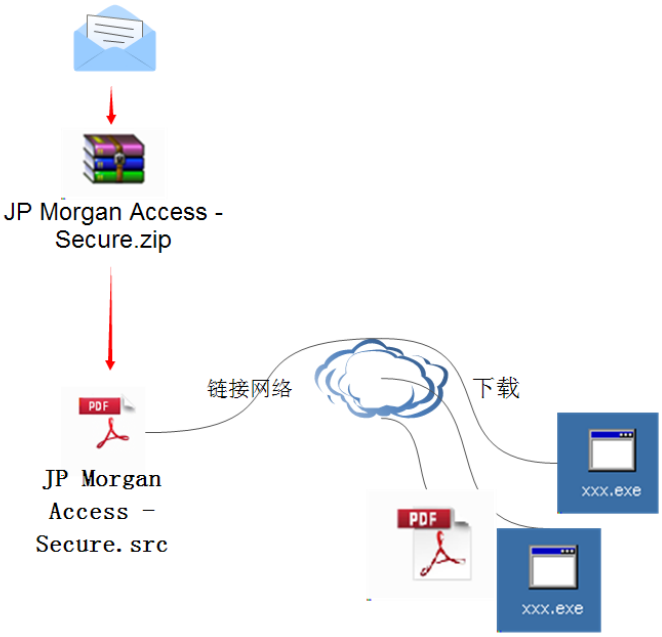


图 2 结构+行为链

2.2 样本分析

样本标签：

病毒名称	Trojan[Downloader]/Win32.Upatre
原始文件名	JP Morgan Access - Secure.src
MD5	32E1F5DED6E9C573293BB6343F785A9F
处理器架构	X86-32
文件大小	24,064 字节
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2004-09-05 12:06:14
数字签名	NO
加壳类型	无
编译语言	Microsoft Visual C++
VT 首次上传时间	2015-03-02
VT 检测结果	48 / 57
样本定性	Downloader

2.3 本地行为描述

概括描述：

样本是长度仅有 24KB 的可执行文件，并具有反调试功能，经过一系列的解密将恶意代码解密执行。样本利用 Windows 消息机制创建隐藏窗口，将恶意代码写在自定义函数中。运行后，查看临时目录是否有进程副本，如果有继续运行，如果没有将自身复制到临时目录下更名为 raturas.exe，样本运行过程中采取自修改指令方式，将关键代码以文件形式加密保存在自身进程中，运行后将加密数据进行解密后开始重新加载自身进程进行从网络上下载其他进程文件。

细节分析：

恶意代码首先创建一个线程，通过消息机制进行线程切换，将线程放在消息自定义函数中执行。在线程中恶意代码首先将加密数据放在内存 810000 中。随后经过如下解密 1 代码段进行初步解密。将解密后的数据放在 820000 内存段，此时恶意代码已经完成了初步解密，在经过第二次解密通过 403CCC 完成，完成后的代码放在 83000 中，它是一个新的 PE 可执行文件。

```
.text:00403853                inc     edx
.text:00403854                push    ebp
.text:00403855                add     esp, 4
.text:00403858                push    ecx
.text:00403859                push    ebp
.text:0040385A                push    ebp
.text:0040385B                push    eax
.text:0040385C                mov     eax, esp
.text:0040385E                pop     eax
.text:0040385F                pop     ebp
.text:00403860                pop     ebp
.text:00403861                pop     ecx
.text:00403862                test    ah, ah
.text:00403864                xor     [edx-1], al
.text:00403867                push    ebx
.text:00403868                push    ebx
.text:00403869                test    eax, 0D36A6A5Ch
.text:0040386E                pop     ebx
.text:0040386F                pop     ebx
.text:00403870                std
.text:00403871                cld
.text:00403872                push    esi
.text:00403873                rol     cl, 90h
.text:00403876                pop     esi
.text:00403877                cmp     edi, edx
.text:00403879                jnb     short loc_403853
.text:0040387B                lea     eax, byte_4040D9
```

```
.text:00403CCC              push    ebp
.text:00403CCD              mov     ebp, esp
.text:00403CCF              sub     esp, 4
.text:00403CD2              mov     [ebp+var_4], 842219FCh
.text:00403CD9              mov     eax, 1
.text:00403CDE              push    ebp
.text:00403CDF              jge     short loc_403CE7
.text:00403CE1              xor     esp, 0
.text:00403CE7
.text:00403CE7 loc_403CE7:                          ; CODE XREF: sub_403CCC+13 j
.text:00403CE7              pop     ebp
.text:00403CE8              js      short loc_403CEF
.text:00403CEA              push    0FFFFFFB5h
.text:00403CEC              add     esp, 4
.text:00403CEF
.text:00403CEF loc_403CEF:                          ; CODE XREF: sub_403CCC+1C j
.text:00403CEF              cld
.text:00403CF0              lea     ecx, [ebp+var_4]
.text:00403CF3              add     eax, ecx
.text:00403CF5              cmc
.text:00403CF6              sar     ebx, 60h
.text:00403CF9              push    esi
.text:00403CFA              and     eax, 0FFFFFFFFh
.text:00403CFF              pop     esi
.text:00403D00              cld
.text:00403D01              dec     eax
.text:00403D02              push    ecx
.text:00403D03              jnz     short loc_403D0C
.text:00403D05              jz      short loc_403D0C
.text:00403D07              push    edi
.text:00403D08              add     ebp, 0
.text:00403D0B              pop     edi
```

图 3　左侧为解密 1，右侧为解密 2

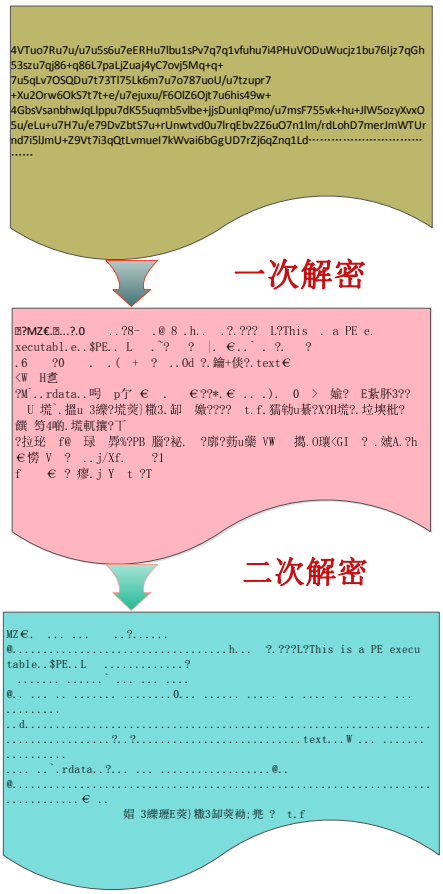

4VTuo7Ru7u/u7u5s6u7eERHu7lbu1sPv7q7q1vfuhu7i4PHuVODuWucjz1bu76Ijz7qGh
53szu7qj86+q86L7paLjZuaj4yC7ovj5Mq+q+
7u5qLv7OSQDu7t73Tl75Lk6m7u7o787uoU/u7tzupr7
+Xu2Orw6OkS7t7t+e/u7ejuxu/F6OlZ6Qjt7u6his49w+
4GbsVsanbhwJqLlppu7dK55uqmb5vlbe+jjsDunlqPmo/u7msF755vk+hu+JlW5ozyXvxO
5u/eLu+u7H7u/e79DvZbtS7u+rUnwtvd0u7lrqEbv2Z6uO7n1lm/rdLohD7merJmWTUr
nd7i5lJmU+Z9Vt7i3qQtLvmuel7kWvai6bGgUD7rZj6qZnq1Ld
一次解密
□?MZ€.□...?.0 ..?8- .@ 8 .h.. .?.??? L?This . a PE e.
xecutabl.e..$PE.. L .~? ? |. €..` . ?. ?
.6 ?O . .(+ ? ..Od ?.鑰+俠?.text€
<W H彥
?M`..rdata..呵 p疔 € . €??*.€ .. ..). 0 > 嬉? E紮胨3??
U 塭 .搵u 3纗?塭荧]糰3.卸 嬓???? t.f.猫釉u暴?X?H塭?.垃塽枇?
饒 笃4喻.塭軏攥?丁
?拉珐 f@ 琭 男%?PB 腦?裕. ?僖?勁u檑 VW 攜.O瀼<GI ? .嫉A.?h
€榜 V ? ..j/Xf. ?1
f € ? 爆.j Y t ?T
二次解密
MZ€. ... .?.....
@.....h... ?.???L?This is a PE execu
table..$PE..L .....?
.... ` ... ...
@.. ... .O... ....
.....
..d.....
.....?..?.....text...W ... .
.....
.... .. `.rdata..?... ... .@..
@.....
.....€ ..
媚 3纗壈E荧]糰3卸荧褥;凳 ? t.f
```

**图 4　解密数据还原**

当完成解密后，该恶意代码进行创建子进程，在子进程中进行申请空间、写入代码、执行代码等操作。随后子进程开始运行并连接网络。
```

2.4 网络行为描述

恶意代码运行后与远程服务器通信，进行文件下载。访问如下域名与服务器：

域名	IP	GET	result
checkip.dyndns.org	**********		本机 IP
milbrookelt d.co.uk	192.185.86.160	/cufon/sdocn.pdf	失效
nationalpalletdelivery.com	192.185.86.183	/demo/documentation/sdocn.pdf	失效
	190.111.9.129		失效

1) 恶意代码运行后首先在系统临时目录下创建文件名为 r657temp.log 的 TXT 文件，内容为：

```
C:JP Morgan Access - Secure.exe
```

随后进行调用删除命令进行文件删除，该 PE 文件是样本创建的副本。

2) 恶意代码链接 *checkip.dyndns.org* 域名，该域名是获取本地 IP 地址的功能，恶意代码是利用该域名测试网络连接是否正常。获取本地 IP 后，打开 *milbrookelt d.co.uk*、*nationalpalletdelivery.com* 域名链接进行下载指定文件。最后进行 IP（*190.111.9.129*）地址链接。循环进行此步骤。下图为整个恶意代码的流程。

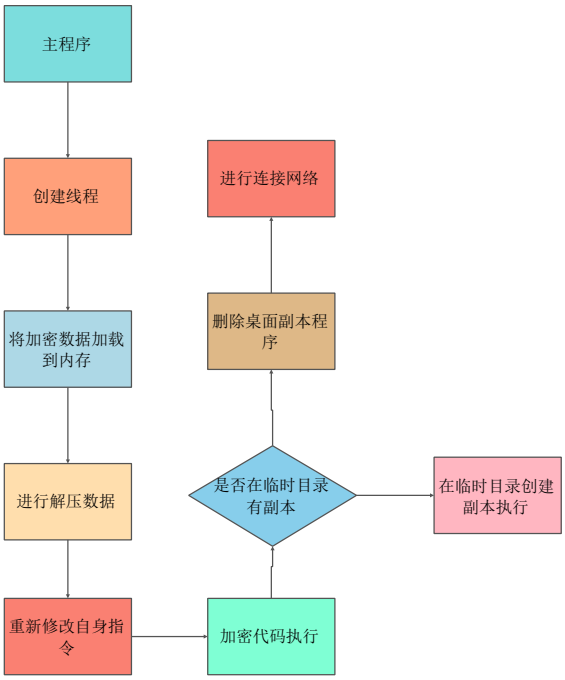


图 5 程序流程图

2.5 样本小结

该邮件首先是以社会工程学攻击为前导，当用户点击附件后，将文件副本隐匿在临时目录下进行连接网络操作，样本是一个“下载者”病毒，不涉及任何启动项功能。整体附件样本的代码技术简练而且有效。

3 邮件二分析

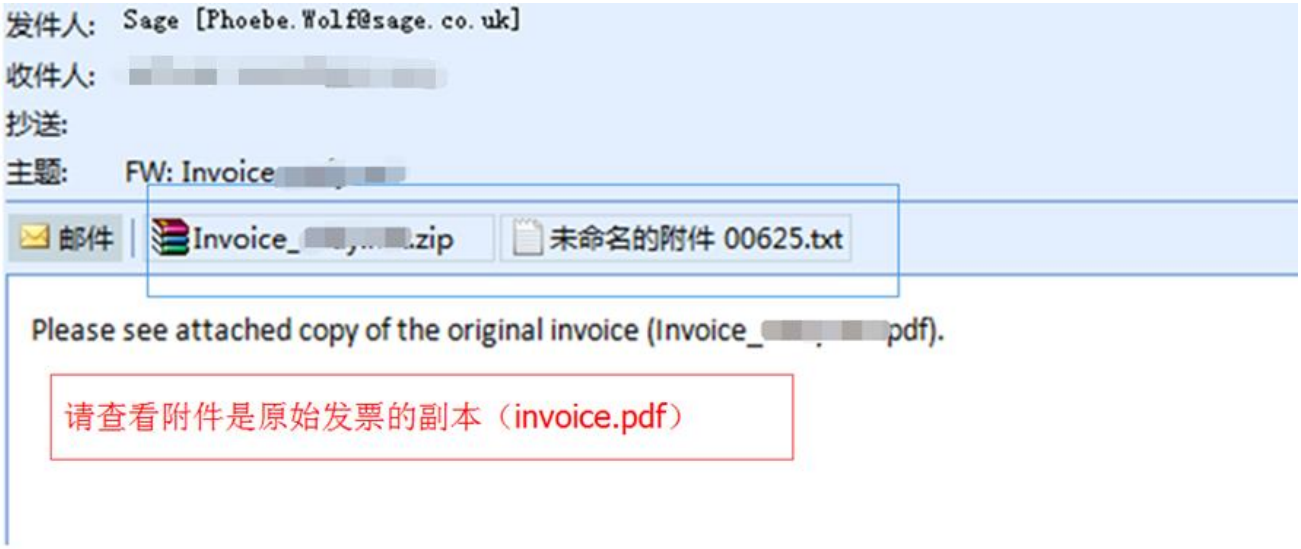


图 6 邮件正文

3.1 邮件元数据提取

邮件主题	Invoice*****
发送时间	2015/4/14 12:24
发件人	******
附件 1 名称	Invoice_***.zip
附件 2 名称	未命名的附件 00625.txt

3.2 样本标签

病毒名称	Trojan[Downloader]/Win32.Upatre
原始文件名	Invoice_004AP71
MD5	6093329DBDA17782BB8DC31CF223A188
处理器架构	X86-32
文件大小	31232 字节
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2006-05-11 20:46:41
数字签名	NO
加壳类型	无
编译语言	Microsoft Visual C++
VT 首次上传时间	2015-04-13
VT 检测结果	41 / 56
样本定性	Downloader

3.3 本地行为描述

该样本本地行为和邮件一中的样本相同。

3.4 网络行为描述

域名	IP	GET	result
checkip-iad.dyndns.com	**		本地 IP
kapil.amsinformatics.com	216.245.213.210	GET /images/monuk14.png	失效
syc.mxserver.ro	176.223.122.103	GET/wp-includes/images/monuk14.png	PDF 文件

该附件运行后，连接网络，尝试下载两个文件到本机执行，其中，一个文件下载失效，另一个样本文件下载的是 PDF 文件，如下图所示：该 PDF 文件从后端下载并且打开后，让用户觉得附件是个真正的 PDF，其实不然，当该 PDF 打开之时，附件文件已经完成了网络下载恶意代码功能。

图 7 PDF 文件

该 PDF 文件的内容可以看出和社工邮件正文内容（发票相关）并不一致，安天分析人员猜测，这种情况可能是由于邮件攻击作者批量投放多种社工技巧攻击手法邮件及与之配套的主题 PDF 文件，导致其中出现的关联混乱。但也不排除是作者手法粗略并没有考虑一致性所导致。另外一种可能是，这就是攻击者想要达成的效果，让受害人认为这不过是一封“垃圾”邮件。

4 亲缘关系分析

两个邮件均是 2015 年 4 月份捕获到的，我们通过对两个邮件的整体结构，以及附件代码的手法进行了亲缘关系分析，发现两个邮件的亲缘关系紧密，猜测属于同一作者进行的批量攻击，以下是通过三个方面的亲缘关系关联与对比。

- 结构链
- 代码行为
- 代码结构

4.1 结构链对比

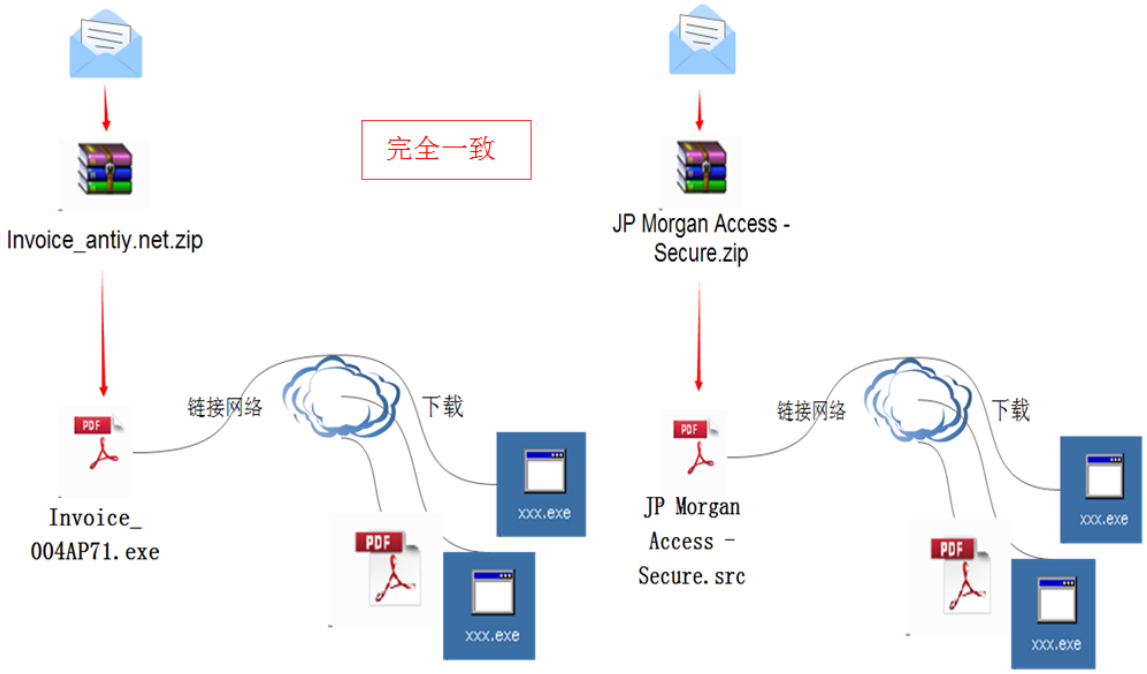


图 8 结构+行为链对比

两封邮件的结构链几乎完全一致，均是一个压缩包，压缩包解压后为一个 PDF 图标的 PE 文件，运行后在网络上下载其他文件。

4.2 代码行为

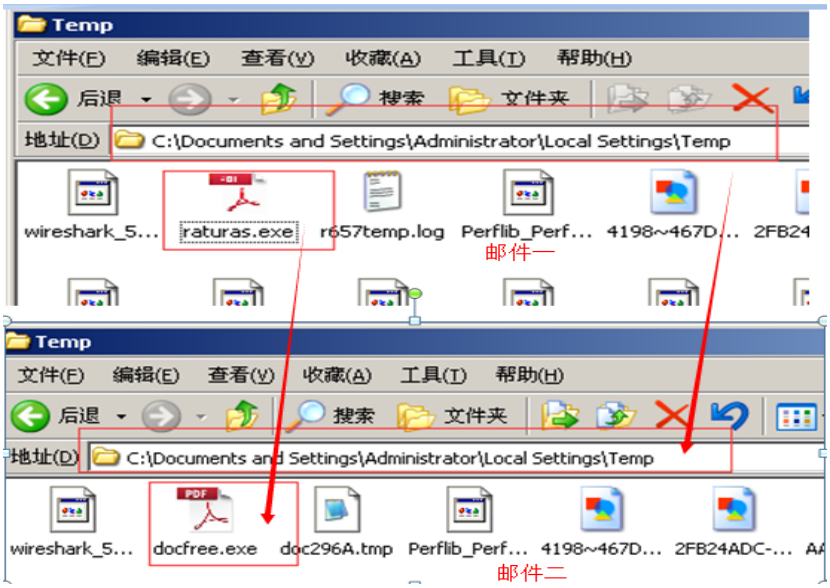


图 9 样本衍生文件目录、图标相似

如上图所示附件样本运行后均是在临时目录创建副本。邮件一，以 raturas.exe 为文件名，邮件二以 docfree.exe 为文件名，并且两个邮件均在临时目录下创建文本文件调用 CMD 命令行方式删除 C 盘副本文件。

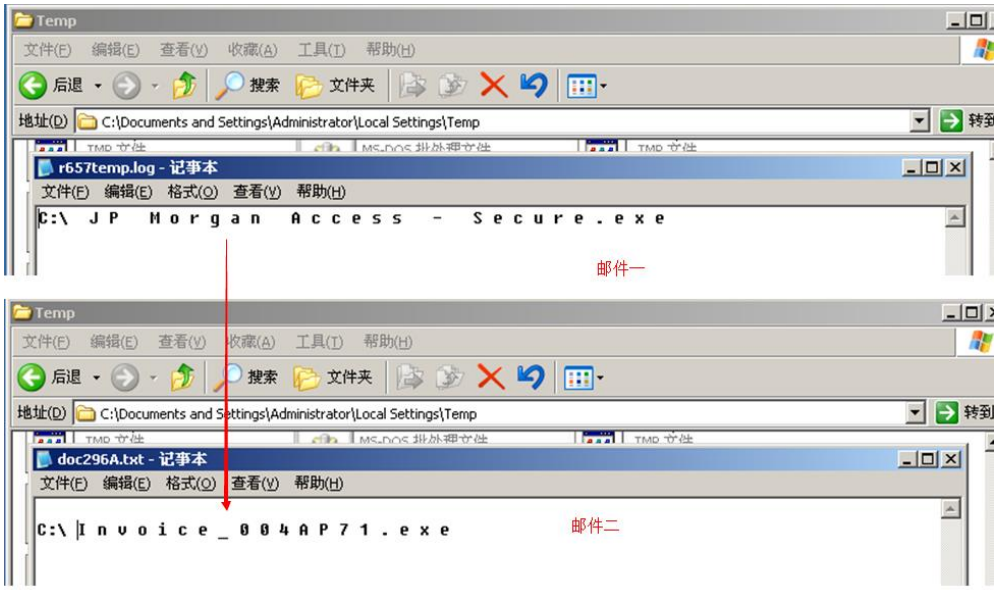


图 10 样本自删除方式

4.3 代码结构

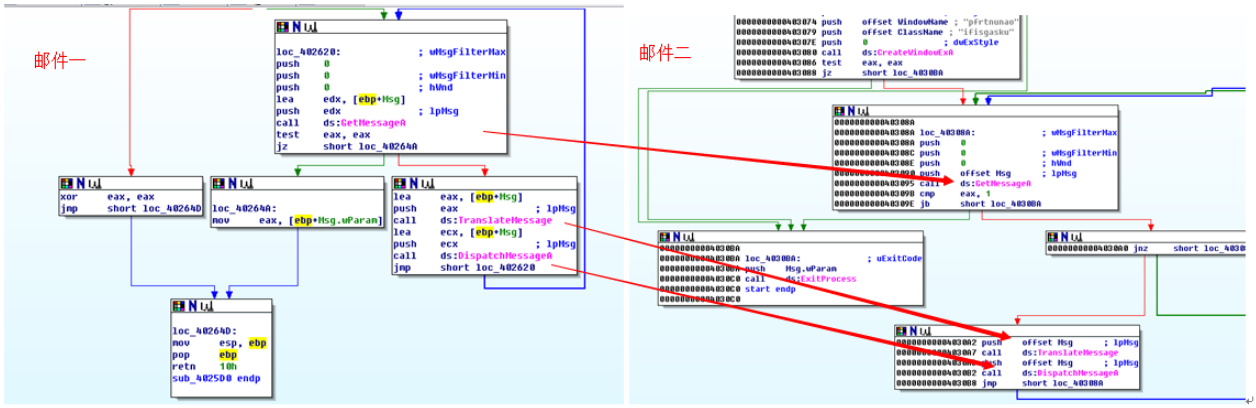


图 11 消息机制

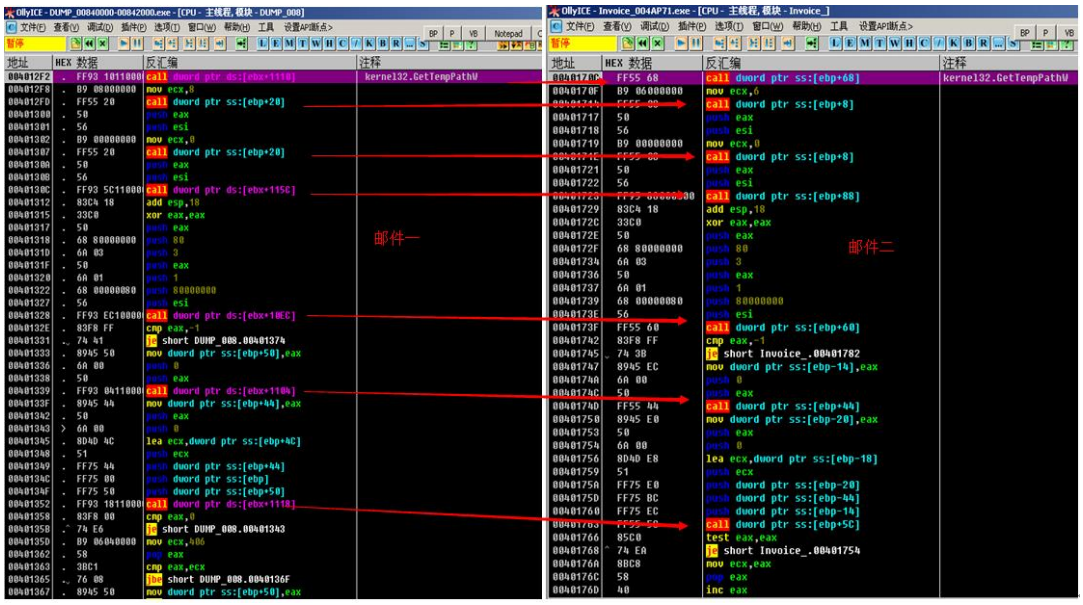


图 12　解密后代码结构

两个样本均是以消息机制为整体代码编写方式，将恶意代码写在自定义函数之中，并且两个样本均是将代码解密出来后运行，并且所有 API 均是解密动态获取。如上图所示两个样本的代码结构几乎一致。

4.3.1　网络行为

邮件一

域名	IP	GET	result
checkip.dyndns.org	[redacted]		本机 IP
milbrookelt d.co.uk	192.185.86.160	/cufon/sdocn.pdf	失效
nationalpalletdelivery.com	192.185.86.183	/demo/documentation/sdocn.pdf	失效

邮件二

域名	IP	GET	result
checkip-iad.dyndns.com	[redacted]		本地 IP
kapil.amsinformatics.com	216.245.213.210	GET /images/monuk14.png	失效
syc.mxserver.ro	176.223.122.103	GET/wp-includes/images/monuk14.png	PDF 文件

图 13　网络行为相似性

两个样本均是首先访问 *checkip-iad.dyndns.com* 域名来测试网络连通状态。可见联网方式的亲缘关系也是一致的。

4.4　小结

通过分析两封邮件的邮件结构、结构链、样本本地行为、网络行为、样本代码等多方面的关联分析得知两封邮件具有高度亲缘性。

通过上述两封邮件的分析与关联，安天 CERT 分析人员通过邮件的结构链，以及附件行为和代码结构等特征在库中抽取了更多的邮件进行批量分析。

4.5 社工手段

通过附件特征与结构的亲缘密切关系安天 CERT 分析人员抽取了 110 个类似邮件，邮件附件的大小均在 23~32kb 中间，邮件的攻击手段有的是通过银行支票作为诱饵，有的是通过扫描件作为诱饵，经过统计我们对 110 个邮件进行攻击技巧标签化，共划分为 14 个标签：

- 附件带 document 字样
- 信用检测
- 无正文内容
- 固定签名
- 问候
- 公司薪资
- 年度报告
- 扫描件
- 银行账单
- 交易类
- 汽车保险
- 合作伙伴
- 更新网上银行
- 银行密码重置

分类说明：

- **附件带 document 字样**

该类邮件使用攻击的附件名称均包括 document 名称。而邮件的主题内容不一致，有的是银行支票，有的是空内容，或者简短的内容但附件攻击代码一致。例如

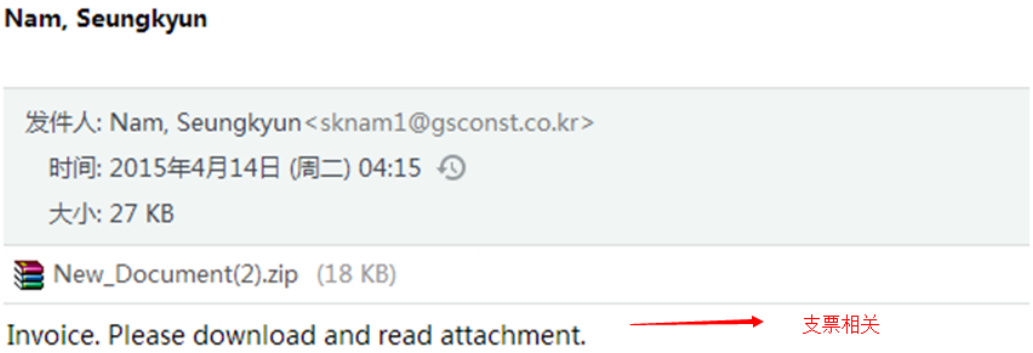


图 14 带有支票相关内容的邮件

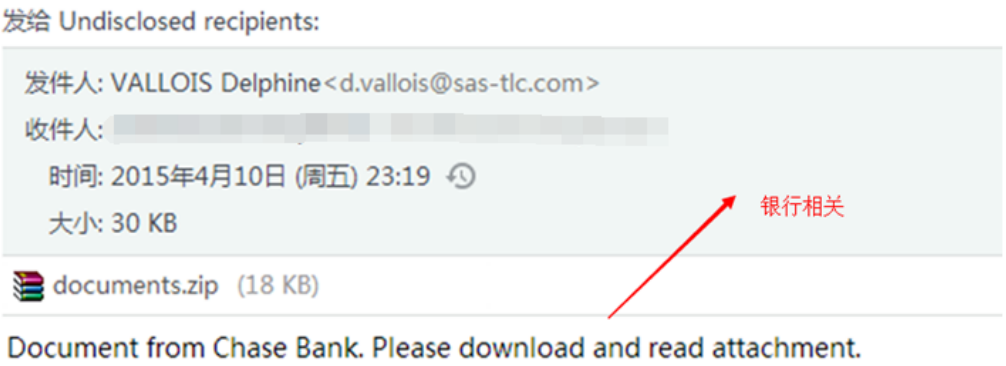


图 15　带有银行相关的邮件

- 无正文内容

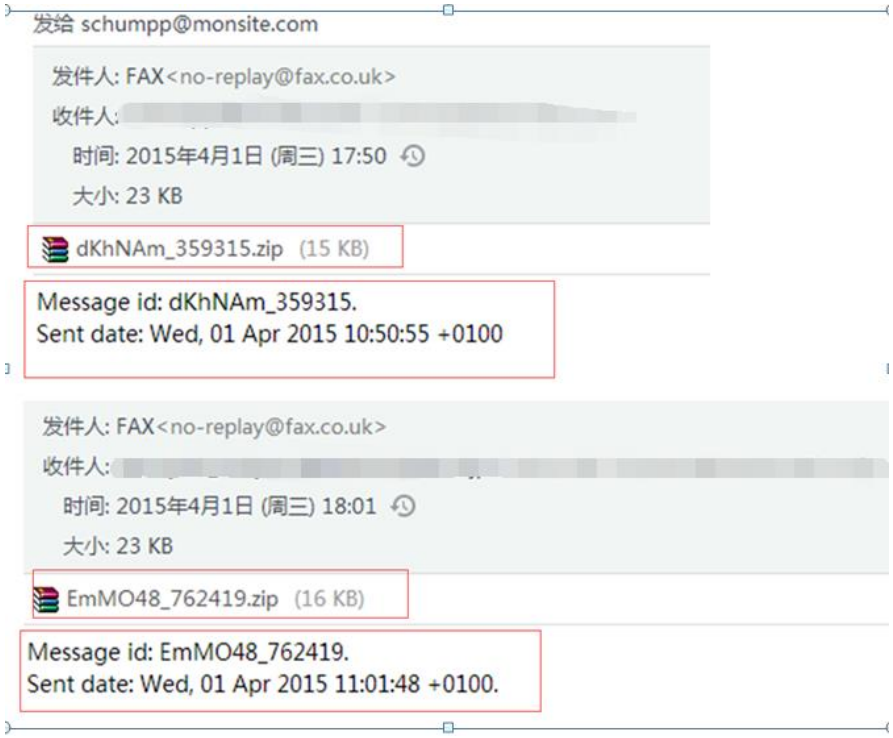


图 16　无正文内容

该类邮件无邮件内容：

Message id: EmMO48_762419.

Sent date: Wed, 01 Apr 2015 11:01:48 +0100.

邮件内容为部分邮件头内容，应该为邮件服务器在处理过程中添加。

- 固定签名

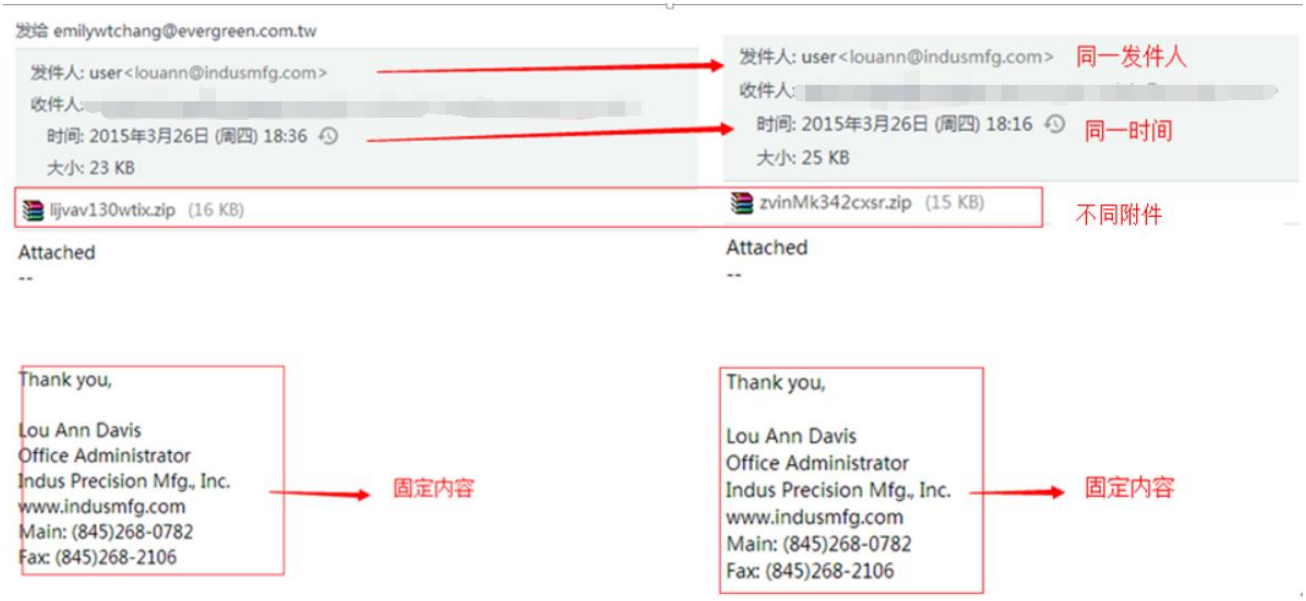


图 17　固定签名

通过分析发现，同一类邮件的攻击时间和攻击人基本是一致的，如上图所示，那么，我们的推断是否完全正确呢，下一节我们对 110 封邮件进行发送时间聚合分析。

从下图可以看出附件为 document 的攻击邮件最多，而信用检测、无内容群发、固定签名、问候等也是常用的攻击手段。

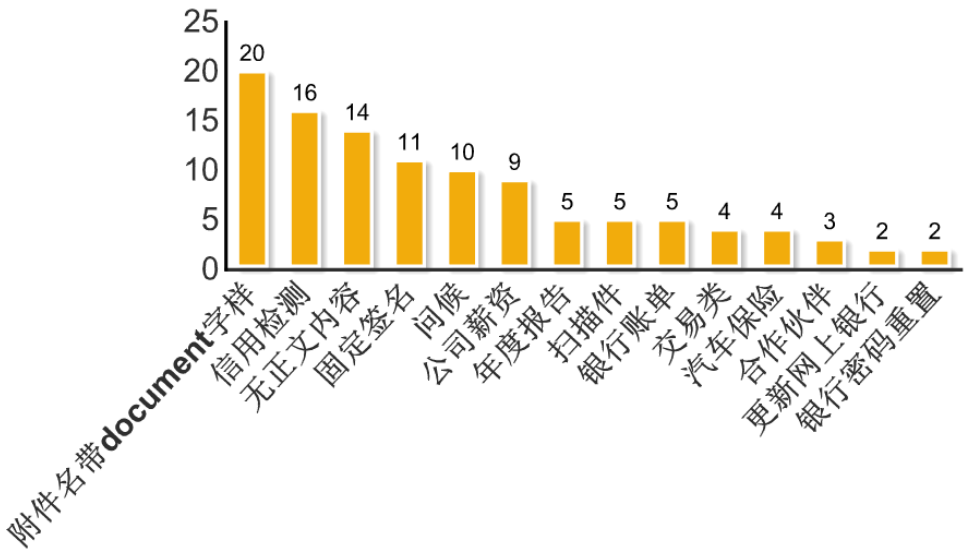
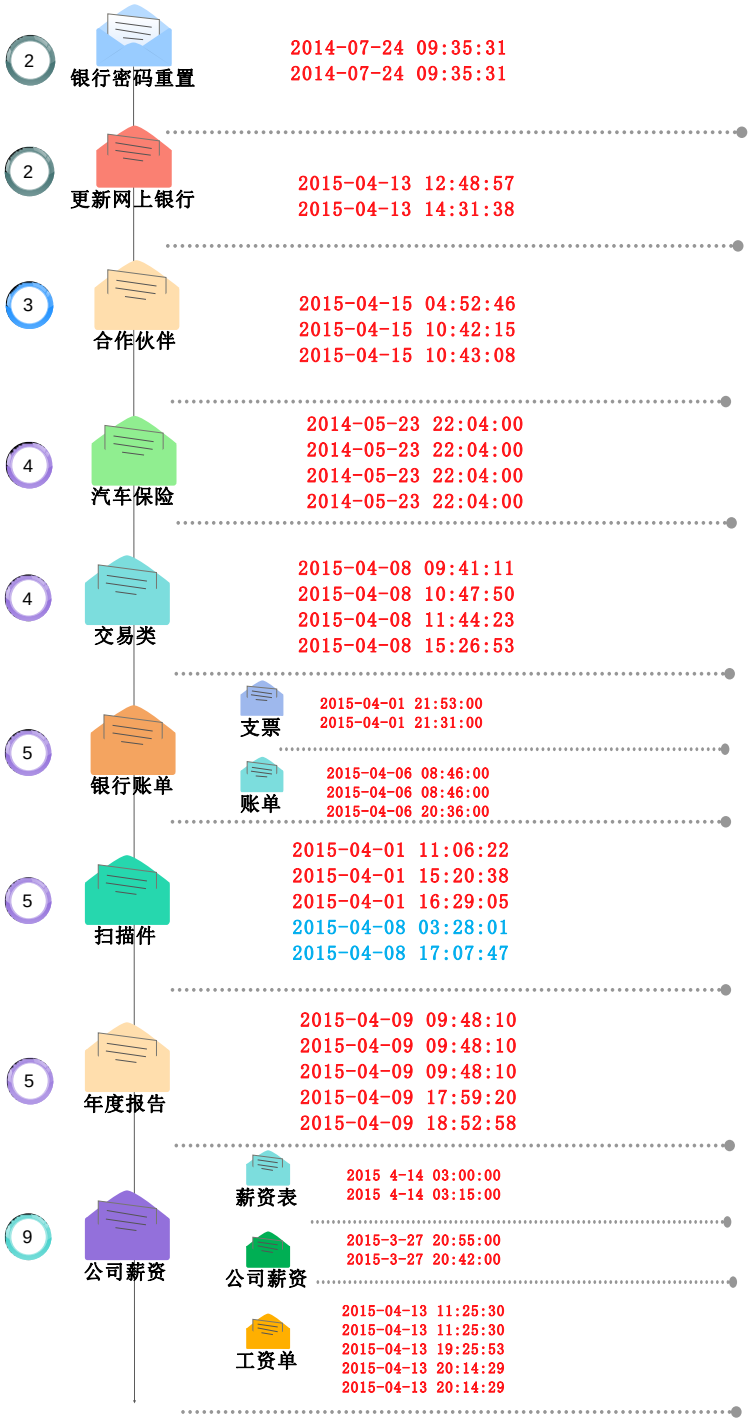
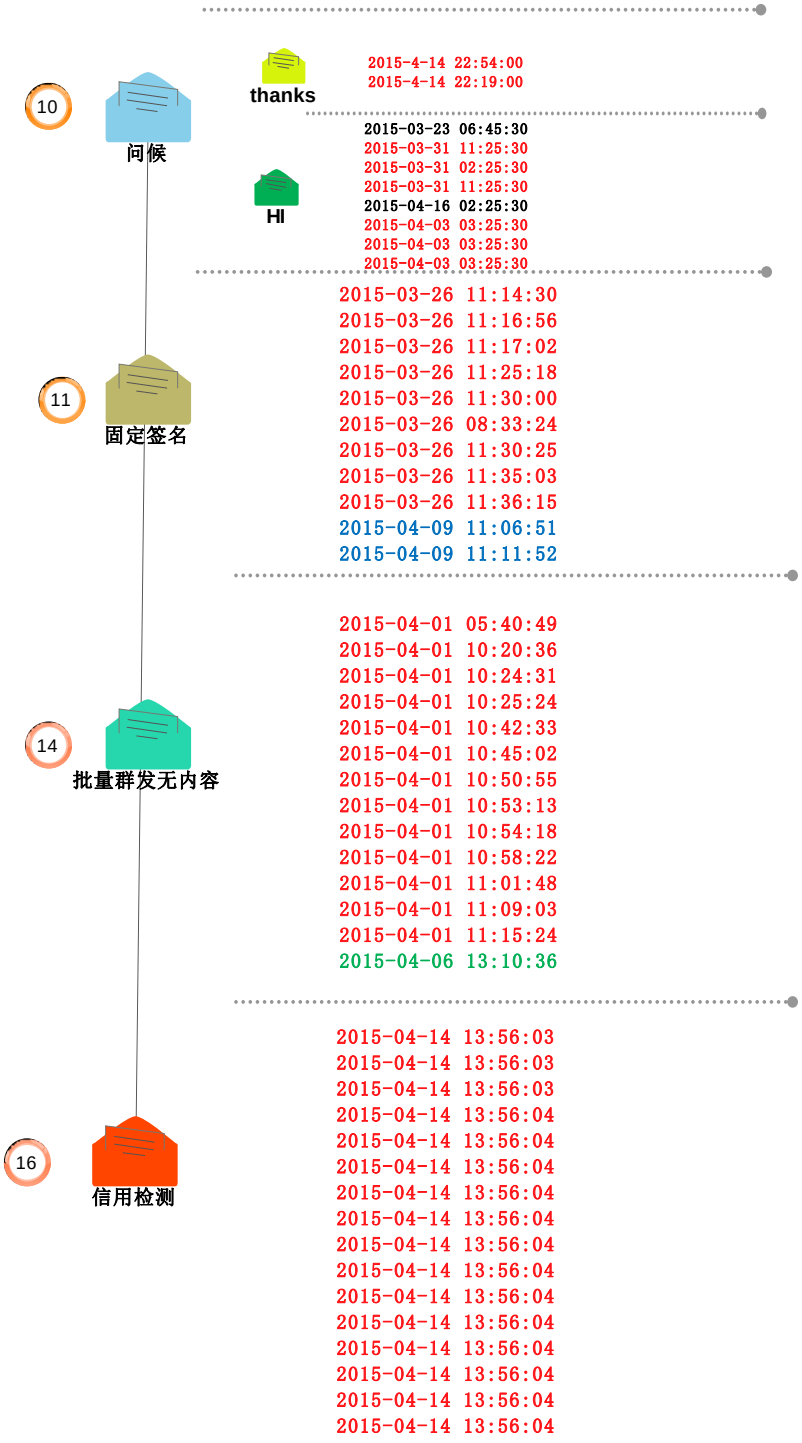


图 18　攻击手段统计

4.6　攻击时间分析

通过对 110 封邮件的社工技巧手段与发送时间的分析发现，几乎所有采用同一社工技巧的邮件都是同一时间发送，如下图所示。





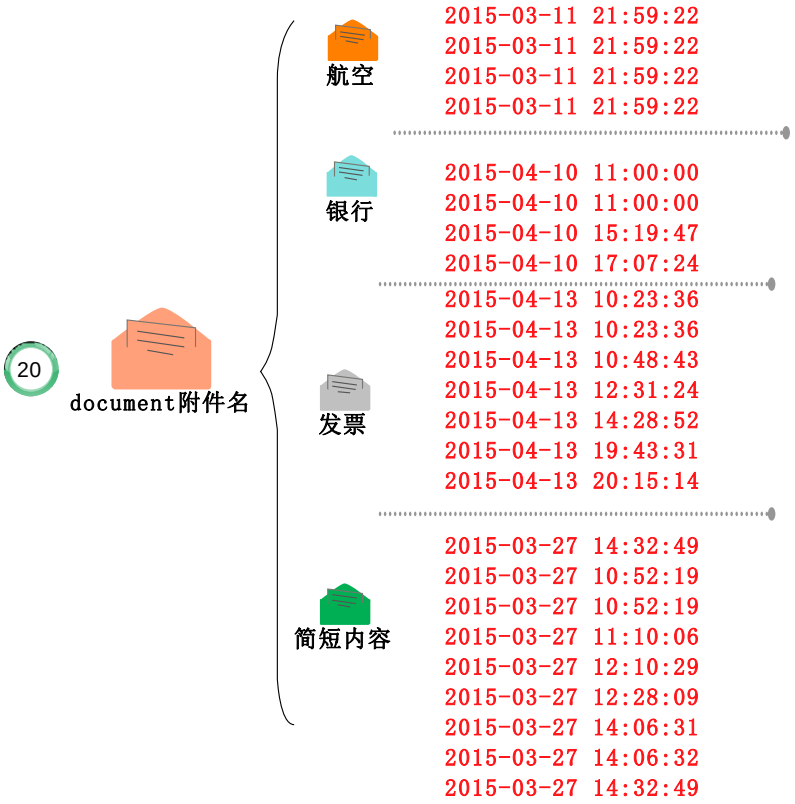


图 19　提取所有抽取邮件的攻击时间

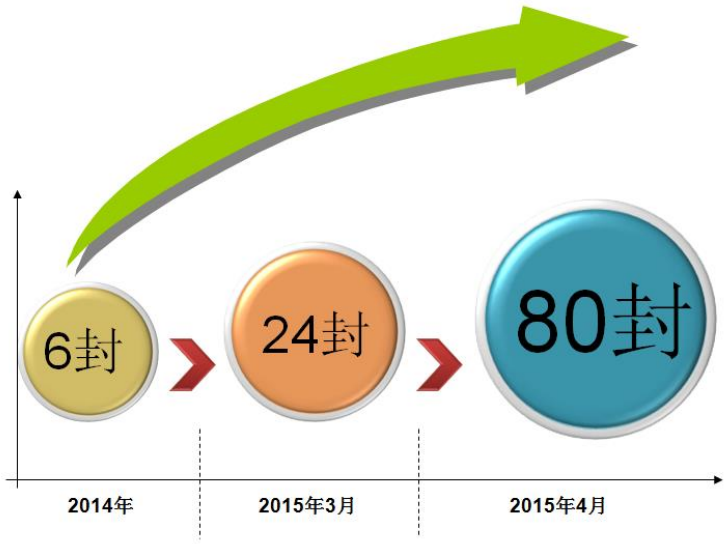


图 20　攻击时间与数目

通过对 110 个邮件的时间摘取分析发现，同一类别邮件攻击者一般采取批量攻击，也就是说在相同时间点发送批量邮件进行攻击，而且通过时间发现，这批同手法邮件的最早发送时间是 2014 年，2015 年 3 月又开始进行批量攻击，到 2015 年 4 月进行大规模性投放。

5 总结

邮件攻击在互联网时代可以说是常见而又泛滥的攻击手法，早在 1999 年爆发的 Happy99 病毒、梅丽莎（Melissa）病毒等作为邮件病毒的鼻祖，之后对照梅丽莎的“蓝本”又爆发了爱虫（LoveLetter）病毒、马吉斯（Magistr）病毒。这些病毒均属于“蠕虫”类型，具备自我扩散的能力，传播范围广，传播次数快，短时间快速传播，一方面会对网络带来很大压力，也很容易被感知和发现。但今天的邮件入口，已经完全告别了当时的“天真病毒时代”，邮件病毒从宏病毒和其他使用邮件 API 自动发送的二进制样本，到使用格式文档溢出的 APT 攻击等。攻击手法从普通的邮件攻击、钓鱼攻击、到鱼叉式钓鱼攻击。攻击手法从粗糙到精密，攻击目标从“扩散”、“扫射”到“狙击”。

尽管此次分析的相关邮件并不具有高度定向性，但其可能会呈现出小批量选择性发送的特点，但对受到欺骗的用户来说也是会造成相应的损失。在邮件采用了较为精细的社工技巧后，在批量投送中，必然有一定比例的用户会被欺骗，这种攻击对受害用户来说，达成了与定向攻击类似的效果。正如安天 CERT 在此前发布《"攻击 WPS 样本"实为敲诈者》分析报告中，所揭示的敲诈者病毒同样大量采用邮件方式进行投放一样。邮件威胁依然猖獗，毕竟，当浏览器、主机、服务器系统的安全在进一步的加固情况下，邮件对攻击者来说是个可以直达目标的上佳入口，这意味着通过邮件进行攻击的方法无论在高级威胁，还是类似扩散僵尸网络、敲诈其他的一般性的网络犯罪中，都将挥之不去。

（国家计算机病毒应急处理中心梁宏同志对本文有重要贡献）

附录一：参考信息

[1] 来源：《"攻击 WPS 样本"实为敲诈者》 http://www.antiy.com/response/CTB-Locker.html

附录二：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为拥有四个研发中心、监控预警能力覆盖全国、产品与服务辐射多个国家的先进安全产品供应商。安天历经十五年持续积累，形成了海量安全威胁知识库，并综合应用网络检测、主机防御、未知威胁鉴定、大数据分析、安全可视化等方面经验，推出了应对持续、高级威胁（APT）的先进产品和解决方案。安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，亦是 CNNVD 六家一级支撑单位之一。安天移动检测引擎是获得全球首个 AV-TEST（2013）年度奖项的中国产品，全球超过十家以上的著名安全厂商都选择安天作为检测能力合作伙伴。

关于安天反病毒引擎更多信息请访问：http://www.antiy.com（中文）

http://www.antiy.net （英文）

关于安天反 APT 相关产品更多信息请访问：http://www.antiy.cn