**蓝白蚁溯源分析报告**

## 小组成员信息

|  |  |  |
| --- | --- | --- |
| 姓名 | 学号 | 操作 |
| 罗梦霞 | 201728018670238 | 攻击事件持续过程信息收集 |
| 魏钰宸 |  |  |
| 靳泽 |  |  |
| 林业明 |  |  |
| 刘天鹏 |  |  |
| 刘勋 |  |  |

## 分析工作

所选系列：专攻日本的APT组织--蓝白蚁

上面，记录自己的信息

找一个溯源的点写一下（与课堂的内容相结合，对应到溯源的4个层次，注意提供分析流程等图表）

编辑后更新github上文档哦

## 攻击事件概述

“蓝白蚁”组织最早的攻击活动是从2013年开始的，“蓝白蚁”组织专门以日本的各大组织作为其攻击目标;他们的攻击目标大多位于日本境内。其中最主要的攻击目标就是日本的养老金服务系统,但目标名单中还包含有政府和政府机构、地方政府、公益组织、大学、银行、金融服务、能源、通信、重工业、化工、汽车、电力、新闻媒体、信息服务业、医疗保健、房地产、食品、半导体、机器人、建筑、保险、运输等产业。

2014年10月,卡巴斯基实验室开始了对“蓝白蚁”组织的研究。不幸的是,该组织的攻击活动仍然处于持续进行之中,受到攻击的行业和部门数量也在不断地增长。

#### 1.1攻击活动演变

最早的攻击从2013年开始，攻击形式不断演变，不断采用新的攻击方式并成功地扩大了他们的行动规模，图1\_1显示的是2014-8-11到2015-7-27已经检测到的C2S访问量。

2015年6月初日本养老金系统入侵事件使该攻击组织被重视，此次外泄的信息包括：基础年金号码和姓名(约3.1万份)、基础年金号码和姓名、生日(约116.7万份)、基础年金号码、姓名、生日、住址(约5.2万份)，总计约125万份。

由于新型攻击形式的出现，攻击在2015年7月中旬又有明显增长（橙色）。

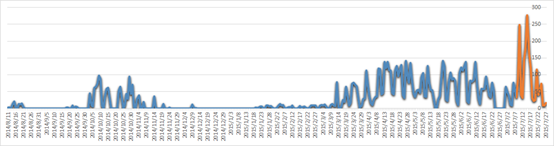
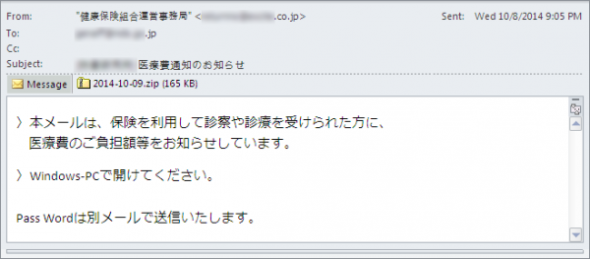


图1\_1 2014-8-11到2015-7-27已经检测到的C2S访问量

黑客组织“蓝白蚁 Blue Termite”惯用的攻击方式是钓鱼邮件：邮件都带有名为“医疗保险通知”之类的文档附件，但事实上这个文档是一个可执行的压缩文件，一旦受害者打开这个文档，隐藏在内的恶意程序就会感染用户的电脑，自动与黑客的服务器进行连接，并开始窃取用户的隐私资料。



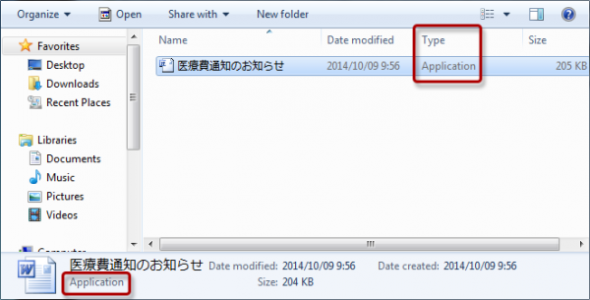


图1\_2钓鱼邮件“蓝白蚁 Blue Termite”惯用的攻击手段

#### 1.2攻击新技术的出现

通常，APT的主要感染方式是通过钓鱼邮件进行的。卡巴斯基实验室发现这个新方式是利用来自Hacking Team泄露事件中曝光的flash漏洞（CVE-2015-5119）exp，让受害者因“被迫下载”而受到感染。几个日本网站已经因为这种攻击方式而被黑，如图1\_3。



图1\_3 利用flash漏洞（CVE-2015-5119）exp的新型攻击

卡巴斯基实验室发现了一些“水管攻击”，其中包括一个属于日本政府重要议员的网站。研究者给网站管理者以及受影响站点的ISP发送了一个通知邮件，却没有收到任何回复。但是，就在大约一小时后这段恶意代码就被删除了。如图1\_4脚本过滤了大部分IP地址，除了一个是属于日本政府机构。该脚本带有变量名为“TEST”的IP信息。研究者怀疑这便是攻击者的测试IP，位于上海。



图1\_4 脚本文件

根据目标而自定义的恶意软件。卡巴斯基实验室检测发现，“emdivi t20”（后文简称“t20”）恶意软件具有根据目标而产生针对性攻击的能力。尽管t17和t20来自同一个emdivi家族，但是后者更为复杂一些。t20通常用于已经感染t17后，而此时t17充当了后门的角色。

首先，一个t20样本中包含硬编码内部代理信息，解密后的代码为"proxy.??????????.co.jp:8080"（具体代理信息网上没有公布），这种方法虽然并不新颖，但也没有被广泛应用。这是由于它可能会暴露目标，或者这并不是一个可以通用的方法，并且只有在一个特殊组织中才能运用。然而，相似的案列在其他APT攻击中也有遇到。

http://www.freebuf.com/news/75738.html

#### 1.3攻击现状

## 二、溯源分析

对下边的问题找一个点，查资料找溯源相关的材料

1. CloudyOmega是政府黑客，还是黑客主义者，还是一群坐在地下室里的脚本小子？从攻击的复杂程度来看，更像是政府黑客，或者至少是精英团体。从攻击的动机角度来看，似乎更应该是政府黑客。

2. 如果CloudyOmega是政府黑客，那应该是哪个国家的呢？中国？朝鲜？俄罗斯？还是其他的国家？

3. 日本的养老金系统入侵事件和美国人事管理局入侵事件的发生时间是如此的相近，不得不让人好奇，他们两者之间有什么样的关系？

4.IP中国 伪造？（<http://www.freebuf.com/news/75738.html>）

5. 赛门铁克和趋势科技还认为，该组织很可能与黑客组织CloudyOmega有关。

6. 该脚本带有变量名为“TEST”的IP信息。研究者怀疑这便是攻击者的测试IP，位于上海。

#### 2.1攻击针对日本且技术较新

这一特征表明更像是政府黑客。

## 三、溯源结果