

网络溯源取证实验报告

Lazarus组织溯源分析报告

院（系）名 称：网络空间安全学院

专 业 名 称：网络空间安全

学 生 姓 名：XXX XXXX XXXX

指 导 教 师：姜政伟 杨泽明 刘宝旭

中国科学院大学

**XXX**年**XX**月

小组成员任务分配情况

|  |  |
| --- | --- |
| 姓名 | 工作情况 |
|  | 搜集资料，攻击组织刻画，溯源结果分析，论文编排，复现 |
|  | 搜集资料，攻击组织刻画，溯源结果分析，论文编排 |
|  | 搜集资料，攻击主机以及控制主机的溯源部分 |
|  | 搜集资料，攻击主机以及控制主机的溯源部分 |
|  | 搜集资料，Lazarus行动简介攻击者及攻击组织溯源部分 |
|  | 搜集资料，Lazarus行动简介攻击者及攻击组织溯源部分 |

目录

[1. 简介 1](#_Toc525903558)

[2. 行动简介 5](#_Toc525903559)

[3. 溯源的技术与流程 7](#_Toc525903560)

[4. 溯源结果分析 1](#_Toc525903561)9

[5. 复现 2](#_Toc525903562)6

[6. 结论 3](#_Toc525903563)1

[参考文献 3](#_Toc525903564)2

# 

# Lazarus组织溯源分析报告

**摘要**：Lazarus组织自2009年开始进行攻击活动。开始时仅针对韩国以及美国的政府、银行、媒体等组织。随着Lazarus组织的发展，攻击活动逐渐开始针对一些大的跨国公司以及一些国家的大银行。本文通过结合McAfee、Kaspersky、Blue Coat System等安全公司的溯源报告，对Lazarus组织进行了深入的调查。本文首先介绍了该组织进行的主要攻击行动，接着描述了对Lazarus组织的溯源技术与流程，根据该组织使用的攻击手段、攻击方法、使用的语言、所在时区等特征对该组织进行画像，最后对溯源结果的可信性进行了简要的分析。

关键词：Lazarus； Operation Troy； Dark Seoul； 溯源取证

**ABSTRACT:**Lazarus has started attacking since 2009.At first it just aimed at the organizations such as government, banks, media and so on of South Korea and the United States, with the development of the organization, it gradually began to attack some big multinationals and big banks in some countries. This paper provides an in-depth understanding of Lazarus organization by combining traceability reports from McAfee, Kaspersky and Blue Coat Systems. This paper begins with a description of the major attacks the organization has conducted,then describes the traceability techniques ,traceability processes and portrait for attackers and attacking organizations, also analyzed the credibility of the traceability results.

**Key Words:**Lazarus; Operation Troy;Dark Seoul;Traceability Forensics

## 简介

xxxx。

在本报告中我们首先在第2节中对Lazarus组织进行的攻击行动进行简要汇报；在第3节中主要针对Dark Seoul事件来描述溯源的技术以及溯源的流程；第4节我们将结合自己掌握的知识对已有溯源结果进行分析；第5节对溯源报告中提到的恶意软件信息在VirusTotal等威胁情报网站中做了一些验证。

## 行动简介

本章我们将从2009年开始按照图1中的时间线，对Lazarus组织进行的部分攻击行动进行介绍。

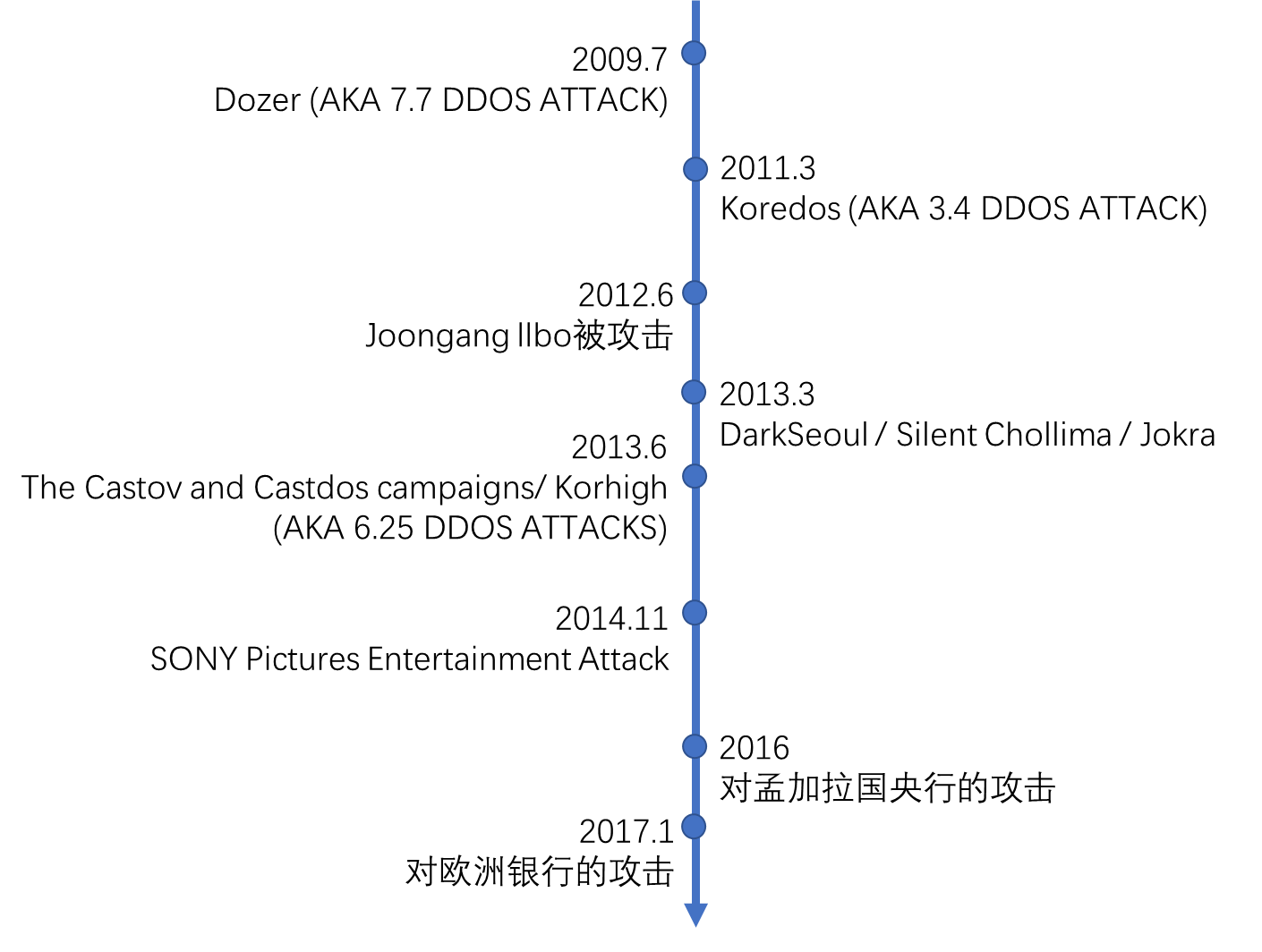


图1 Lazarus攻击行动时间线

#### 2.1 Dozer (AKA 7.7 DDOS ATTACK)( 2009.7)

这次攻击主要针对韩国的一些政府和银行网站，也针对了美国一些政府网站，包括白宫官网。整个事件分为三波攻击：第一波发生在7月4日，也就是美国独立日，攻击了包括白宫、五角大楼等27个网站；第二波发生在7月7日，攻击了韩国的青瓦台、国防部、议会等政府网站；第三波发生在7月9日，攻击包括了韩国的国家情报局、部分银行和新闻网站。此次攻击对受害主机进行了硬盘数据删除，以此抹除证据。

通过对W32.Dozer样本的分析，结合从部分僵尸机提取到的网络日志信息，推测出其攻击流程如图2所示：

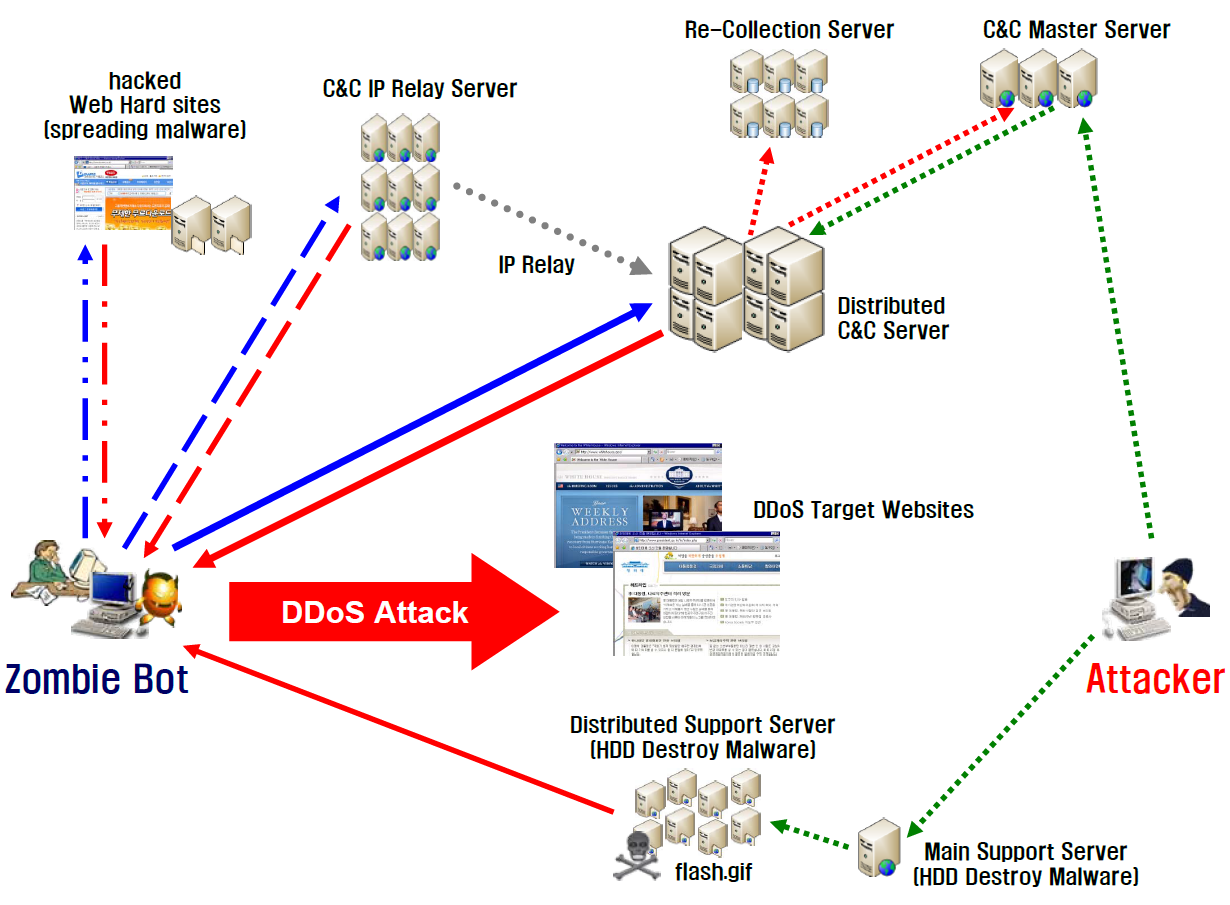


图2 Dozer攻击流程

XXXX

图3展示了issuemakerslab对此次攻击中的部分C&C的IP中继服务器溯源结果。IP中继服务器被分为三类，每一类采用了不同的加密格式和返回文件名。

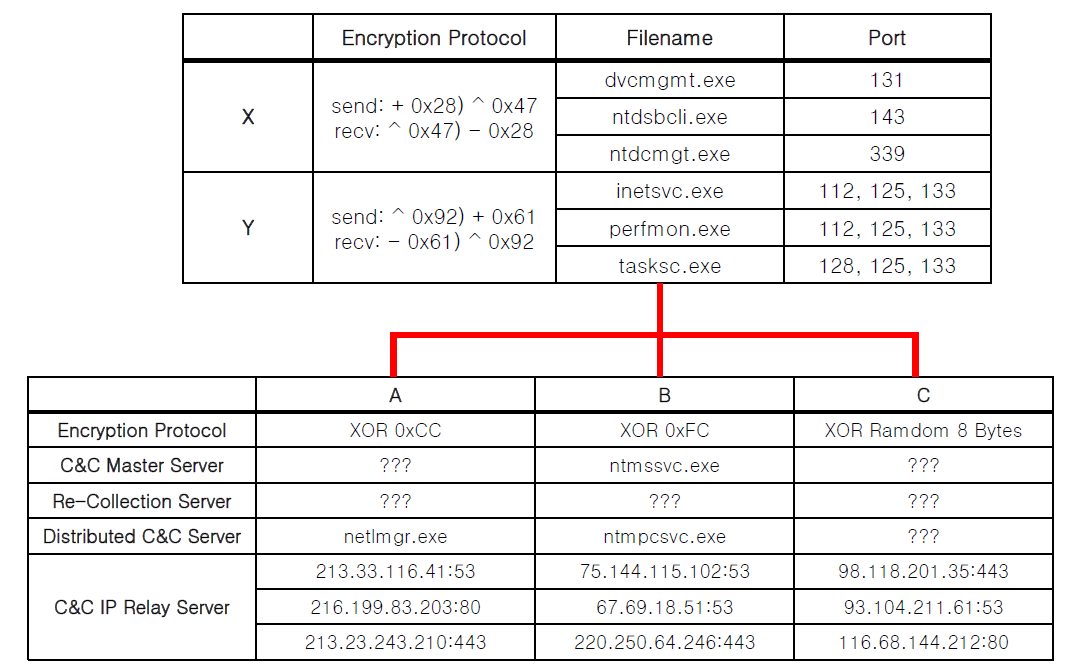


图3 Dozer溯源结果

xxx

#### 2.2 Koredos (AKA 3.4 DDOS ATTACK) (2011.3)

XXX

#### 2.3 Dark Seoul-Operation Troy(2013.3)

xxx

#### 2.4 The Castov and Castdos campaigns (AKA 6.25 DDOS ATTACKS) (2013.6)

XXX。

#### 2.5 SONY Pictures Entertainment Attack(2014.11)

XXX

#### 2.7 对欧洲银行的攻击(2017.1)

XXXX。

## 溯源的技术与流程

本节中我们主要针对Dark Seoul事件与Operation Troy中的攻击主机与控制主机进行溯源。

#### 攻击主机的溯源取证

在Dark Seoul的受害主机中，安全研究员发现在3月19日，攻击者发送了钓鱼邮件给South Korea organizations，这是一个合法的网站。邮件中包含一个木马下载器，这是攻击过程开始。通过对邮件线索的提取，可获取涉及的IP，对邮件攻击过程与投递方式分析，通过邮件头指纹比对，还原得到钓鱼的邮件路径。 xxx。

图13是Dark Seoul中存在的网络攻击的示意图，其中标有惊叹号的域名是溯源到的攻击机或者被控制的机器，这些主机在整个过程中发挥着不同的作用[1]。

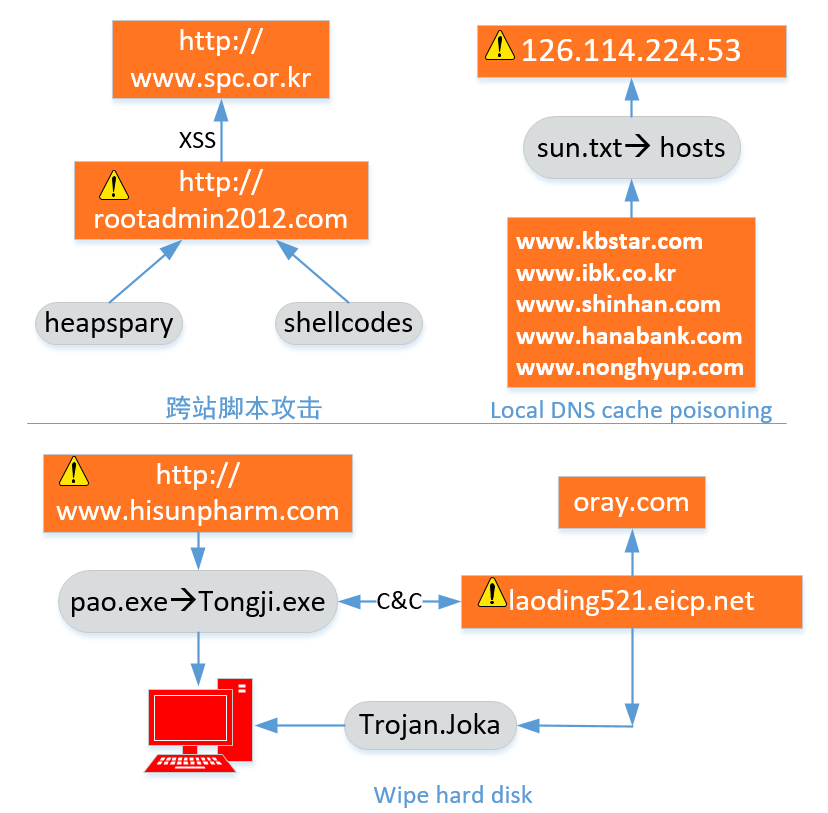


图13 Dark Seoul网络攻击示意图

#### 3.2 控制主机溯源取证

研究人员通过拼凑网络流量日志信息。分析发现，攻击者使用大量不同的地址发动了此次攻击，这些地址既有韩国境内的，也有来自国外的。不出所料的是很多地址解析为匿名代理服务器或TOR匿名网络出口节点，这使得研究人员无法判断攻击者的真实物理地址，比如使用TOR匿名网络的攻击者，其访问目标站点的数据包中，IP头部的源地址是某个 TOR 网络出口节点的 IP，它已经替换掉攻击者的ISP 为其分配的公网 IP。还有一些地址是被入侵设备，同时一些地址直接来自朝鲜。该攻击的攻击路径及溯源路径如图14所示。攻击者在攻击的每个方面都使用了不同的手段，有些使用补丁管理系统，有些则作为3RAT植入的命令和控制节点，或者借助一个恶意软件变体进行下载，这使得证据的收集变得十分困难。

XXXX。

#### 3.3 攻击者以及攻击组织溯源取证

将上述的一系列攻击溯源至同一个组织，主要依据是这一系列攻击所采用的恶意代码之间的相似性，以及攻击行为模式的相关性。

##### 3.3.1 恶意代码分析

从恶意软件代码层面上，KorDllbot最早可能来源于2009年Rbot和Mydoom在联合开发网（pudn.com）上公布的代码，它被BlueCoat命名为KorDllbot。此后的DOZER、KOREDOS、DarkSeoul、CASTOV、Korhigh、SONY Pictures Entertainment Attack几次攻击所采用的主要恶意软件的行为模式与关键特征都和这份KorDllbot高度相似，可被视为同一个代码家族的多个衍生版本。2013年的后门程序也早在2009年被编译完成。

xxx

McAfee在对Dark Seoul进行溯源的过程中发现了三个恶意软件分别是Dropper Trojan、MBR Wiper、Remote-Access Trojan，如表2所示。

表2 Dark Seoul恶意样本

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 功能 | 文件大小 | 编译时间 |
| Dropper Trojan | 安装MBR擦除器 | 418KB | March 20,2013 |
| MBR Wiper | 擦除硬盘上的MBR | 24KB | January 31,2013 |
| Remote-Access Trojan | 提供后门去攻击 | 46KB | January 26,2013 |

McAfee认为病毒生成器木马是通过一个脆弱的补丁管理器伪装成合法更新分发的。并且怀疑攻击者们在3月20日之前就攻入了目标环境，因为3月20日一天之内不太可能有3万多人被鱼叉式钓鱼攻击。一个远控木马被发现在一些脆弱的环境，特别是在被用来将更新分发给成百上千的电脑服务器。McAfee认为这个威胁像RDN/Generic PWS.y!io（McAfee的命名方式）病毒，使用Microsoft Visual C++ Version2.9编译，大小为47KB。

XXX。

##### 3.3.2 攻击行为模式分析

从行为模式上来讲，Dozer、Koredos、DarkSeoul这三次攻击都使用了基于IRC僵尸网络的DDOS攻击，并且都控制了大量计算机，并且恶意软件都表现出盗取用户信息、通过MBR删除用户磁盘数据的危害。并且，通过分析可知，Dozer和Koredos两次攻击似乎都是在为DarkSeoul以及接下来的攻击做准备，一方面扩展僵尸网络的规模，一方面窃取大量情报。在此后的Korhigh和SONY攻击中，恶意软件已经将大量目标网络的主机名、用户名、密码预先存储，就说明了这一点。这表明这一系列攻击有很强的先后关联，应为同一攻击组织所为。

XXXX

在对欧洲银行的攻击事件中，Lazarus的代码混入了俄文单词，并使用俄罗斯人开发的打包软件，但伪装效果拙劣，意味着该组织希望混淆视听，阻碍溯源过程。此外，该程序最早的KorDllbot代码源自中国国内的“联合开发网（pudn.com）”，文件命名或口令中也夹杂类似中文拼音的字符，例如某僵尸机密码为wodehaopeng，某后门文件名为pao.exe，tongji.exe，tongji2.exe，域名命名为laoding521.ecip.net，邮箱命名为xiake722@gmail.com，laohu1985@gmail.com等。这也似乎意味着该组织希望分析者将其视作一个来自中国的组织。

#### 3. 4 攻击组织刻画

##### 3. 4. 1 Lazarus组织代号汇总

XX

##### 3. 4. 2 Lazarus组织来源地域

XXX。

##### 3. 4. 3 Lazarus组织主要目标及意图

xxx。

##### 3. 4. 4 Lazarus组织攻击方法

综合上述分析我们可以得到表4，该表展示了Lazarus组织常用的攻击方法

表4 Lazarus攻击方法

|  |  |  |
| --- | --- | --- |
| 攻击方法 | 攻击载体 | 攻击描述 |
| 文档挂马 | 包含特定shellcode的文档 | 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”。 |
| 伪装为目标常用文档的文件 |
| USB蠕虫 | 包含特定shellcode的文档 | 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。 |
| 水坑攻击 | 包含恶意脚本 | 在目标人员经常访问的网站下挂马 |
| 鱼叉式钓鱼攻击 | 包含恶意代码的邮件附件 | 更快速的攻击目标人员 |
| 僵尸网络 | DeltaCharlie  恶意代码 | 基于DeltaCharlie形成僵尸网络，使用DNS反射/放大、ntp反射/放大攻击与chargen反射/放大攻击发起DDoS攻击 |

下表中包含了恶意木马与C&C通讯手段。

表5 C&C特性

|  |  |
| --- | --- |
| 通信渠道 | 渠道描述 |
| 硬编码IP | 2013 ~2014 年间，恶意木马通信C&C 均是直连硬编码的IP 地址，且地址的地理位置均位于韩国，可能是傀儡机和跳板。 |
| 暗网网桥 | 2015年开始，恶意木马的网络通讯全面升级为暗网网桥（Onion.City），这是当前APT 黑客攻击中比较高端和隐蔽的网络通信方式。 |

该组织还十分喜欢使用加密技术，表6中说明了该组织常用的加密技术。

表6 Lazarus常用加密技术

|  |  |
| --- | --- |
| 加密方法 | 加密方法描述 |
| Microsoft Cryptography API library Version 1.0 | 在Dark Seoul及之前的攻击中，该组织一直使用微软的加密API加密与C&C服务器通信的HTTP或IRC协议的流量。 |
| RC4 | 在2016年的之后的攻击事件中，攻击载荷与C&C通信时会将文本使用RC4密码算法进行加密。 |
| Gauss malware | 使用加密技术保护恶意软件。 |

##### 3. 4. 5 与Lazarus组织有关的攻击事件

XXXX

## 溯源结果分析

#### 4.1溯源方法评价

xxxx。

#### 4.2溯源结果可信性

通过从恶意软件代码、网络流量以及其余细节上的信息推断出该攻击来源于Lazarus组织，溯源的方法正确，同时溯源的过程比较详细，涉及到溯源流程的4个方面，在恶意软件代码和网络流量、网络日志分析方面分析的较完整，过程较成功。除了在溯源的手法上比较全面和详细，对于溯源得到的一些信息片段进行分析整合，攻击者所在时区UTC-8，几乎所有的恶意代码均有相似部分。攻击的目标和获取的文件信息具有相似性。

在攻击手法上，Operation Troy与SONY Pictures Entertainment Attack存在很大的相似性。这些活动首先利用水坑攻击进入目标系统，通过收集的信息使用鱼叉式钓鱼攻击进行大规模攻击，用最少的时间收集和窃取尽可能多的数据。如果入侵目标有价值，Lazarus就会立刻使用另外的工具，转而采用长期隐藏策略，长时间的收集情报。除了这些大规模的活动，Lazarus同时还在不停的实施一些小规模活动，这些活动的针对性更强，使用了不同的工具。这些针对性活动已经至少持续了8年。其目标和持续时间都与朝鲜有关。同时各大安全团队的溯源报告在不能确定攻击组织确切的所在地的情况下，没有在证据不足的情况下就断定是由那个国家或者攻击团队所为，这也使得这些溯源结果更为可信。

## 复现

#### 5.1 SONY Pictures Entertainment Attack恶意软件分析

#### 5.1.1 Dropper

XXXX。

##### 5.1.2 Wiper

xxx

##### 5.1.3 Web Server

XXX

##### 5.1.4 Backdoor

xxx

##### 5. 1. 5 SMB worm

XXX

#### 5.2 Kaspersky对东南亚某国央行溯源中发现的恶意软件

##### 5. 2. 1 SWIFT transactions Information Harvester (New Runoff)

xxx

##### 5. 2. 2 Session Hijacker

XXX

##### 5. 2. 3 Active Backdoors

xxx

#### 5. 3 总结

在复现的过程中我们尝试在微步、Virus Total、hybrid-analysis等威胁情报网站下载恶意样本或者网络数据包，但是网络样本大都下载不成功网络数据包中也没有什么有价值的东西，如下图27和图28所示。因此我们仅在Virus Total中查询了在溯源报告中出现个恶意样本的hash值。

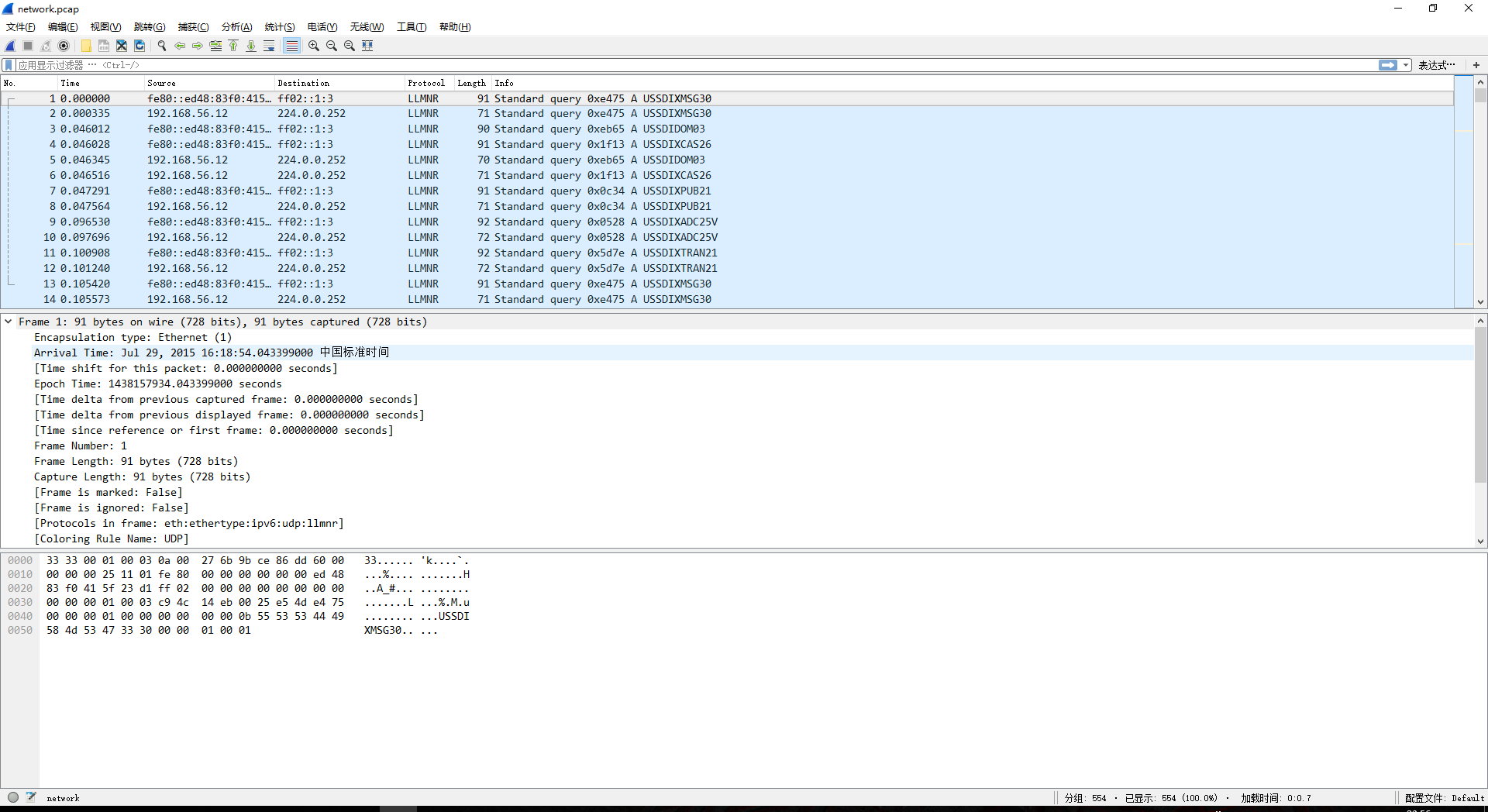


图27 从hybrid-analysis中下载的pcap包



图28 在Virus Total下载恶意样本界面

## 结论

xxx。

# 参考文献

[1] https://blog.avast.com/2013/03/19/analysis-of-chinese-attack-against-korean-banks/

[2] David M. Martin. Tracing the Lineage of DarkSeoul, 2015.

[3] Snorre Fagerland, From Seoul to Sony:The Histoty of the DarkSeoul Group and the Sony Malware Destover, 2016.

[4] Jonathan A.P,HoonJae Lee,Dark Seoul Cyberattack, 2013.

[5] Ryan Sherstobitoff,Itai Liba,James Walter, Dissecting Operation Troy: Cyberespionage in South Korea, 2014.

[6] Kaspersky Lazarus Under The Hood, 2017.

[7] sionics & kaientt, DDoS: Unknown Secrets and Botnet Counter-Attack, 2013

[8] Ji-Young Lee, 7.7 DDOS Attack in Korea, 2009

[9] Youm H Y, SG I. Korea’s experience of massive DDoS attacks from Botnet[J]. ITU-T SG, 2011, 17.

[10] DongJoo Ha, SangMyung Choi, TaeHyung Kim, SeungYoun Han, Check your zombie devices! Analysis of the DDoS cyber terrorism against the country and future attacks on various devices, 2011

[11] Rights R F. SANS Institute InfoSec Reading Room[J]. GIAC, 2002.

[12] 6.25 DNS DDoS 공격 악성코드 분석 , (cfile5.uf.tistory.com/attach/2555EE4E51EE1AB4228292), 2013