



每个威胁都不是独立存在的

# 1. 引言



漏洞  
IP  
威胁情报  
恶意文件

烽火台安全威胁情报联盟  
FengHuTai CTI Alliance

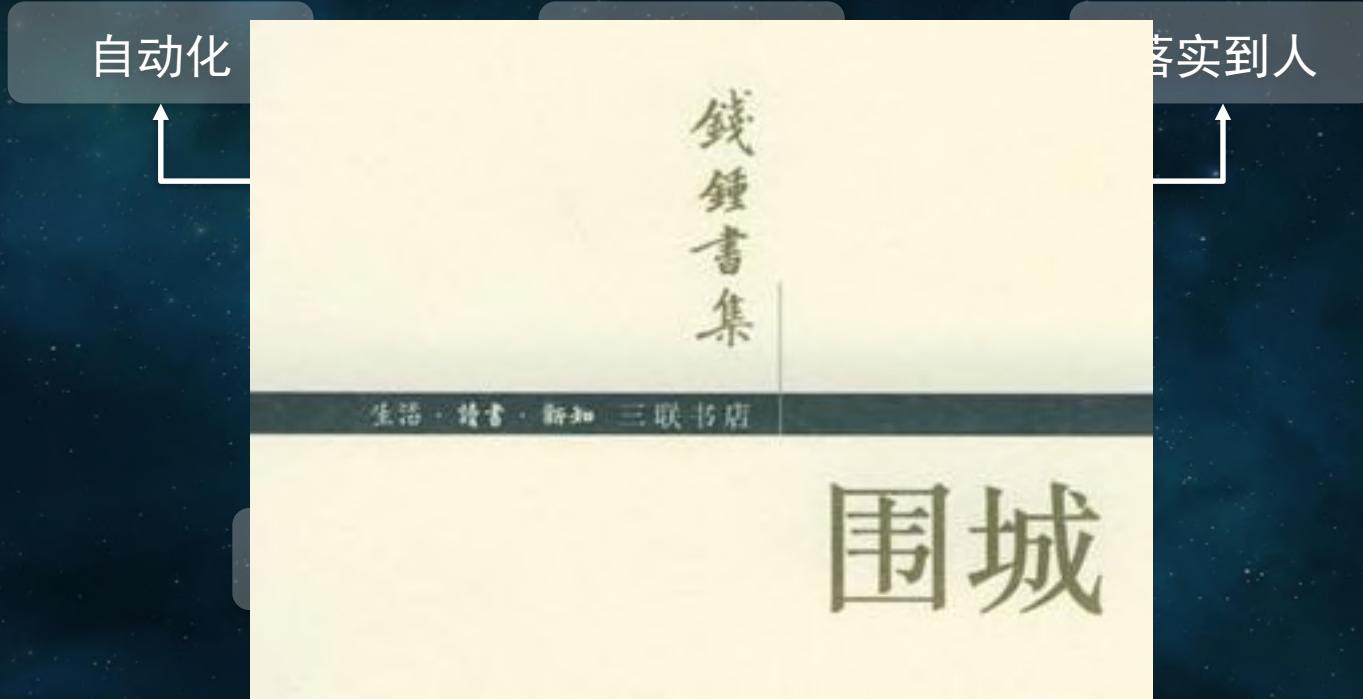
时间：2016/6/26  
Feed获取方式：<http://feed.watcherlab.com/>  
更新提醒：  
最近我们开放了Feed API 内测功能，在Alice平台上注册账户并通过审核后可以使用。  
每日热点事件

事件描述	来源	IOCs数	更新频度
宏基电子商务网站发现一个数据泄露的漏洞并已经存在长达一年，该漏洞可用来获取消费者的信用卡信息，好消息是目前没有明确的数据泄露迹象	<a href="https://blog.malwarebytes.com/security-world/2016/06/acs-lengthy-data-breach-discovered/">https://blog.malwarebytes.com/security-world/2016/06/acs-lengthy-data-breach-discovered/</a>	12	24h
每日常规更新			
分类	分类说明	IOCs数	更新频度
watcherlab-proxy	代理服务器IP Feed: 本Feed包含众多的HTTP/HTTPS、SOCKS等方式的代理服务器IP地址。	31092	24h
watcherlab-fastflux	快速进行过IP地址和域名绑定更换的IP地址，通常我们认为这些IP地址是有潜在威胁的	10	24h
watcherlab-botnet	包含全球的僵尸网络和僵尸主机相关的IP Feed。	28682	24h
watcherlab-c2	包含全球范围内的C2主机信息，通常这些IP也为受害者。	949	24h
watcherlab-on-ipv4	中国地区的恶意行为IP地址Feed:本Feed是我们为中国地区推出的特殊版本。包含了一系列具有常见恶意行为的IP数据,这些数据有可能为受害者也有可能来自攻击者本身。	949	24h
watcherlab-ipv4	全球的恶意行为IPv4地址Feed	21203	24h
watcherlab-ipv6	全球的恶意行为IPv6地址Feed	0	24h

## 2. 传统的漏洞管理



### 3. 平台式漏洞管理



#### 4. 利用威胁情报发现漏洞



## 5. 一次利用外部威胁的入侵

github

© 2015-08-26T07:19:51Z.

关键字: web.xml config.xml config web.config ssh

```

# -*- coding: utf-8 -*-
...
Parallels Cloud Module
=====

The Parallels cloud module is used to control the Parallels VPS system.

Set up the cloud configuration at ``/etc/salt/cloud.providers.d/parallels.conf``

.. code-block:: yaml

my-parallels-config:
# Parallels account information
user: myuser
password: mypassword
url: ...
provider: parallels

...
# Import python libs
from __future__ import absolute_import
import copy
import time

```

网易邮箱

百度为您找到相关结果约9,020个

了搜索工具

### 如何评价网易邮箱[过过过](#)数据泄露? - 程序员 - 知乎

2015年10月23日 - 主要是一堆游戏账号都是网易的。。真是烦,知乎也是用的网易的邮箱。刚才知乎系统...5亿的数据,如果要撞库,那得是多大的库?而且光网易出事儿? 撞库十有...

[www.zhihu.com/question... - 百度快照 - 1135条评价](http://www.zhihu.com/question/1135)

### 5亿条[网易邮箱](#)数据疑似泄露!这几招救命-网易,邮箱,泄露,黑客,乌云...

2015年10月19日 - 乌云称,根据白帽子报告,网易邮箱的用户数据库疑似泄露,数量多达5亿条,...的这份数据库记录多达5亿条,不太可能是简单的“撞库”,更像是“撞库”。

[news.mydrivers.com/1/4\\_1 - 百度快照 - 41条评价](http://news.mydrivers.com/1/4_1)

### 撞库还是撞库?[网易邮箱](#)罗生门 | 雷锋网

从乌云吉之菌匿的报告和网友的如潮控诉来看,网易邮箱信息泄露,似乎已经被坐实。然而,对于数据泄露的方式,网易和乌云存在着一定的分歧。那么,乌云在说...

[www.leiphone.com/news/... - 百度快照 - 52条评价](http://www.leiphone.com/news/... - 百度快照 - 52条评价)

### 【公告】[网易邮箱](#)密码被撞库,使用[网易邮箱](#)注册的JRS建议立即修改...

11条回复 - 发帖时间: 2015年10月20日

2015年10月20日 - 得到最新消息,网易邮箱密码被撞库,使用网易邮箱注册的用户建议立即修改密码! 以免账号丢失,给您的财产和生活造成不必要的损失和麻烦。不用网易邮箱也...

[bbs.hupu.com/144075 - 百度快照 - 260条评价](http://bbs.hupu.com/144075)

## 6. 利用威胁情报分级漏洞



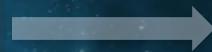
## 7. 威胁情报和漏洞管理的初步结合



威胁情报



漏洞

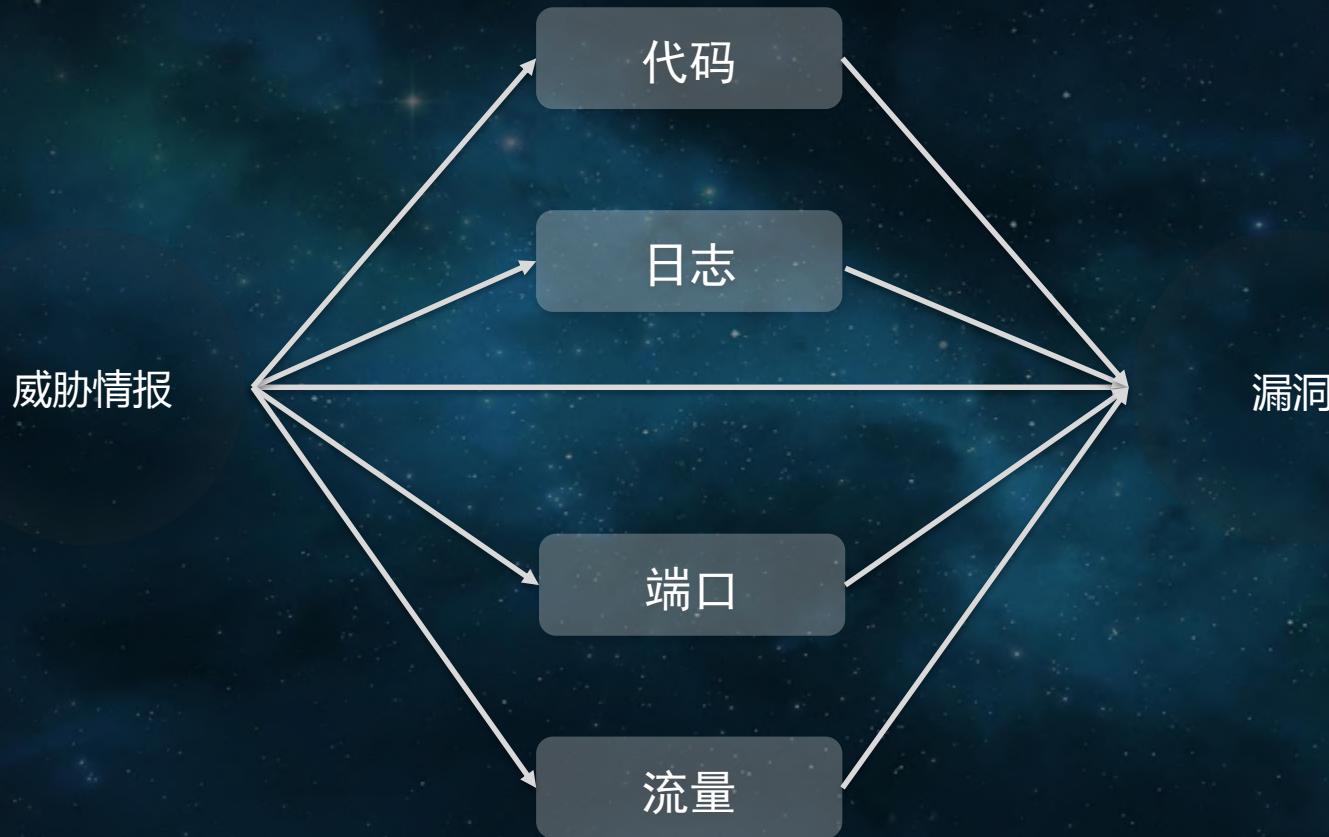


人

## 8. 企业里不同维度的关联



## 9. 多元化关联方式



## 10. 一次威胁处置



Welcome 123456@163.com Log out

https://www.virustotal.com/en/file/b938fdb60b6c228d21ce2d06c4403c536991431f98/a485abf6395494bcf1ca4/

SHA256: 50386db50b6c228d21ce2d06c4403c536991431f98/a485abf6395494bcf1ca4

File name: yhqlxxzini

Detection ratio: 19 / 43

Analysis Additional information Comments Votes

Antivirus	Result
AI Yar	Trojan Linux Xorddos.B
AVG	Linux/DDoS.XCR.16
Ad-Aware	Trojan Linux Xorddos.B
Arcabit	Trojan Linux Xorddos.B
BitDefender	Trojan Linux Xorddos.B
CAT-QuickHeal	TrojanXor Linux EDDos.A
ClamAV	Unix/Trojan.Kemmis-1
ESET-NOD32	a variant of Linux/Xorddos.D
Immunet	Trojan Linux Xorddos.B (B)
F-Secure	Trojan Linux Xorddos.B

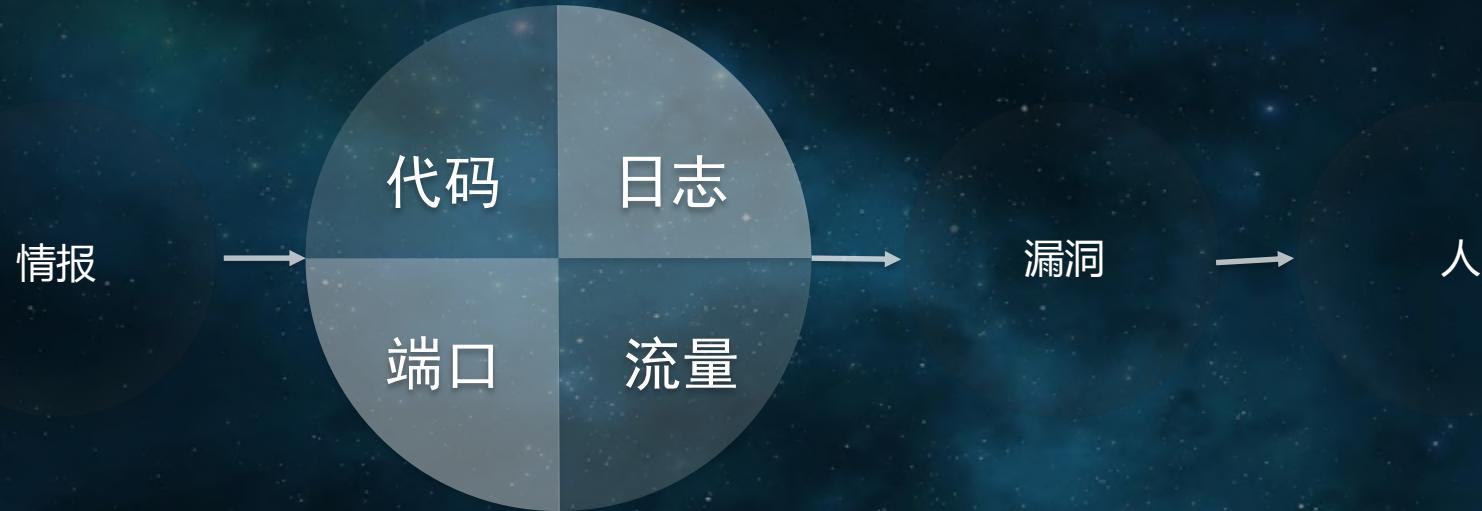
2016-01-08 13:23:16

```
graph TD; 端口 --- 二级域名; 二级域名 --- 应急申请; 应急申请 -.-> 20160108132316[2016-01-08 13:23:16]
```

## 11. 应急和威胁情报的结合



## 12. 安全威胁管理



观星台

星规

外网安全威胁管理

内网安全漏洞管理

THANKS

