

成员:花十一



# 应急响应木马日志溯源画像分析

红日核心成员:花十一



# 目 录

1 入门

2 进阶

3 实战

4 总结

# 1 入门

# 1 入门

## 流程

01

前期沟通

问问题

02

事件处理

查原因

03

事件分析

应急处理

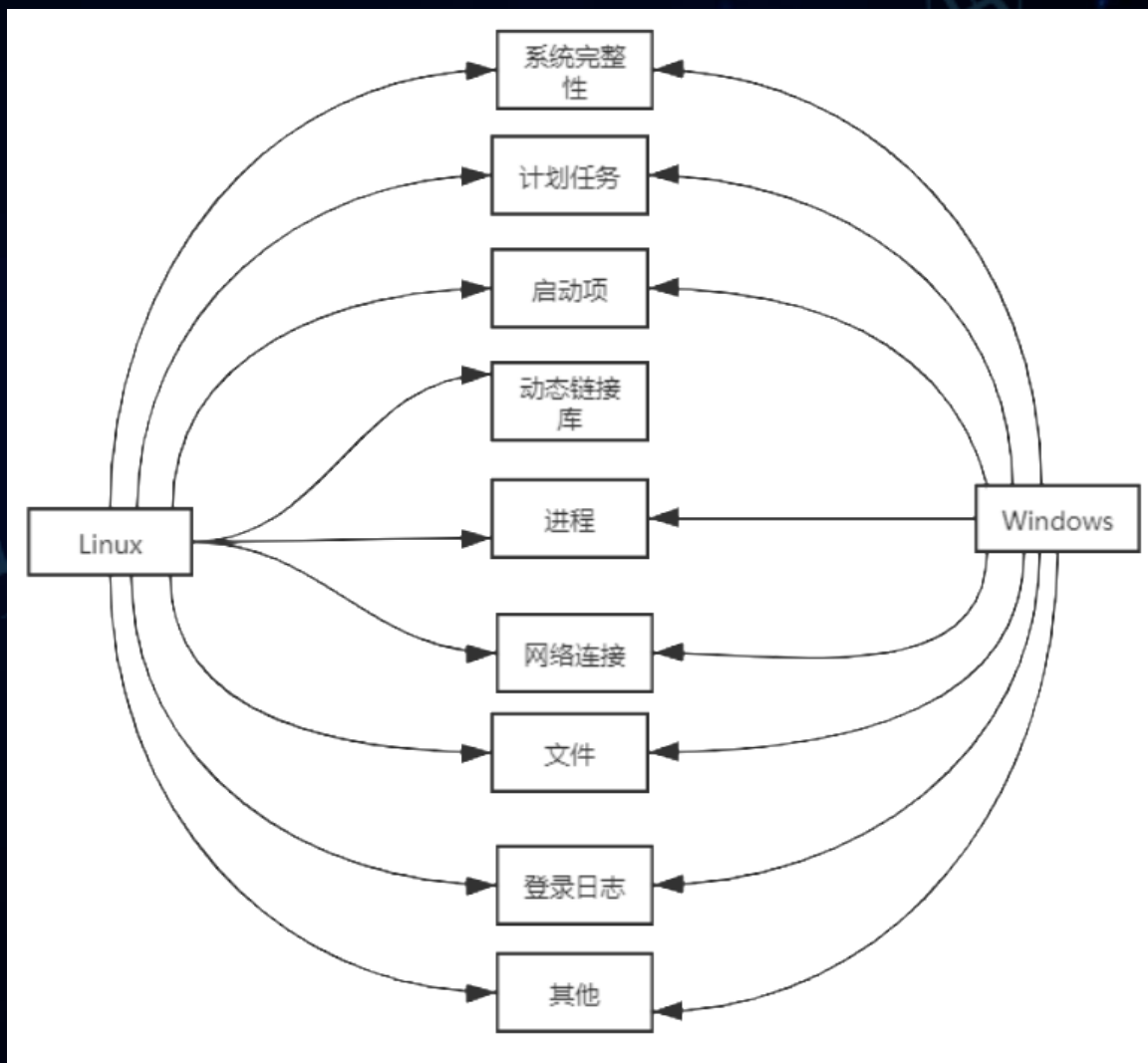
04

报告交付

产出应急响应报告

## 1 入门

# 检查项



## 1 入门

# 武器库

Linux

Windows

```
>python2 ip_info.py
success
```

IP:10.16.1.1	归属地:局域网	信息:IP
IP:172.16.1.1	归属地:美国	信息:弗吉尼亚州阿什本Psychz数据中心
IP:148.2.2.2	归属地:德国	信息: CZ88.NET
IP:77.8.8.8	归属地:希腊	信息: CZ88.NET
IP:222.222.222.222	归属地:江苏省镇江市	信息:电信IDC机房
IP:20.1.1.1	归属地:美国	信息:Microsoft数据中心
IP:138.1.1.1	归属地:德国	信息: CZ88.NET

## 2 进阶



## 2 进阶

知其然知其所以然



## 2 进阶

事件类别	详细描述
网络攻击事件	<ul style="list-style-type: none"><li>安全扫描攻击：黑客利用扫描器对目标进行漏洞探测，并在发现漏洞后进一步利用漏洞进行攻击</li><li>暴力破解攻击：对目标系统账号密码进行暴力破解，获取后台管理员权限</li><li>系统漏洞攻击：利用操作系统、应用系统中存在漏洞进行攻击</li><li>WEB漏洞攻击：通过SQL注入漏洞、上传漏洞、XSS漏洞、授权绕过等各种WEB漏洞进行攻击</li><li>拒绝服务攻击：通过大流量DDOS或者CC攻击目标，使目标服务器无法提供正常服务</li><li>其他网络攻击行为</li></ul>
恶意程序事件	<p>恶意程序主要类型及危害：</p> <ul style="list-style-type: none"><li>病毒、蠕虫：造成系统缓慢，数据损坏、运行异常</li><li>远控木马：主机被黑客远程控制</li><li>僵尸网络程序（肉鸡行为）：主机对外发动DDOS攻击、对外发起扫描攻击行为</li><li>挖矿程序：造成系统资源大量消耗</li></ul>
WEB恶意代码	<p>网站恶意代码常见类型及危害：</p> <ul style="list-style-type: none"><li>Webshell后门：黑客通过Webshell控制主机</li><li>网页挂马：页面被植入待病毒内容，影响访问者安全</li><li>网页暗链：网站被植入博彩、色情、游戏等广告内容</li></ul>
信息破坏事件	<ul style="list-style-type: none"><li>系统配置遭篡改：系统中出现异常的服务、进程、启动项、账号等等</li><li>数据库内容篡改：业务数据遭到恶意篡改，引起业务异常和损失</li><li>网站内容篡改事件：网站页面内容被黑客恶意篡改</li><li>信息数据泄露事件：服务器数据、会员账号遭到窃取并泄露</li></ul>
其他安全事件	<ul style="list-style-type: none"><li>账号被异常登录：系统账号在异地登录，可能出现账号密码泄露</li><li>异常网络连接：服务器发起对外的异常访问，连接到木马主控端、矿池、病毒服务器等行为</li></ul>

## 2 进阶

# 止损

- (1) 一般像web攻击类安全事件，处理方法就是加waf,增加攻击者的攻击成本，然后开始查找漏洞，修复漏洞，如果是CMS漏洞，需要根据官方修复建议进行修复。
- (2) 挖矿类安全事件，先暂停挖矿进程，修改远程木马下载地址为本地host。然后排查处理
- (3) 信息泄露类安全事件，要根据泄露数据样本判断是哪里存在漏洞，然后采取相应的措施。
- (4) 支付类安全事件，禁用支付密钥，关闭提现业务

## 2 进阶

- 1\_AspCMS
- 2\_Confluence
- 3\_Dede
- 4\_DZ
- 5\_ElasticSearch
- 6\_JBoss
- 7\_Joomla
- 8\_Nginx
- 9\_PHPCMSv9
- 10\_phpmyadmin
- 11\_Siteserver
- 12\_Spring
- 13\_struts
- 14\_ThinkPHP
- 15\_weblogic
- 16\_Wordpress
- 17\_禅道cms
- 18\_java
- 19\_IIS写入权限漏洞工具
- 20\_Coremail
- 21\_Seeyon
- 22\_Redis

www.anquanke.com › post ▼ [Translate this page](#)

### watchdogs挖矿木马综合分析报告- 安全客，安全资讯平台

Feb 26, 2019 - 默安科技应急响应中心接到某合作伙伴的求助电话，针对被watchdogs病毒感染的机器进行排查和分析，并最终给出了针对该类型的挖矿病毒的清除 ...

### 利用驱动人生升级通道传播的木马手工查杀记

 xiaoxinling ⌚ 2020-02-01 共28467人围观，发现 4 个不明物体 系统安全

### 一款短小精致的SSH后门分析

2018-02-28 阅读 393

#### 0x00. 引言

在《利用系统特性伪装成一个免密登陆后门》一文中，我介绍过利用系统特性伪装成一个ssh系统后门，不过，这个后门需要新开一个端口，而本文介绍的这个后门只需要系统上开放了ssh服务就行了，不需要额外的开放端口，详情见正文。

# 3 实战

### 3 实战

某天，接到客户求助说钱被刷走了

(1) 支付密钥被窃取

(2) 提现

询问业务场景

服务器上有啥服务，开了啥端口

询问业务流程

客户说，支付订单号非常规订单号码，且被盗刷的服务器存在某服务器关闭。



## 3 实战

### 验证猜想

```
GET / HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0)
Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: lang=zh-CN;
i_like_gogits=../attachment[REDACTED]
_csrf=[REDACTED]
Upgrade-Insecure-Requests:
Cache-Control: max-age=0
```

www.freebuf.com > column ▾ Translate this page

```
class="menu" tabindex="-1">
```

```
<div class="ui header">
```

```
已登录用户 <strong>[REDACTED]</strong>
```

```
</div>
```

```
<div class="divider"></div>
```

```
<a class="item" href="/cql">
```

```
<i class="octicon octicon-person"></i>
```

个人信息

```
</a>
```

```
<a class="item" href="/user/settings">
```

```
<i class="octicon octicon-settings"></i>
```

用户设置

```
</a>
```

```
<a class="item" target="_blank" href="https://gogs.io/docs" rel="noreferrer">
```

```
<i class="octicon octicon-question"></i>
```

帮助

```
</a>
```

### 3 实战

:22 [TRACE] Template: user/dashboard/dashboard

:24 [TRACE] Session ID: 2afc

:24 [TRACE] CSRF Token: -zP8e2Essc

sshd[17878]: Accepted publickey for git from port ssh2: RSA SHA256:AJx

sshd[17878]: pam\_unix(sshd:session): session opened for user hv (uid=0)

sudo: root : TTY=unknown ; PWD=/www

sudo: root : TTY=unknown ; PWD=/www

sudo: root : TTY=unknown ; PWD=/www

sudo: root : TTY=unknown ; PWD=/www

sudo: root : TTY=unknown ; PWD=/www

sudo: root : TTY=unknown ; PWD=/www

sudo: root : TTY=unknown ; PWD=/www

sudo: root : TTY=unknown ; PWD=/www

sudo: root : TTY=unknown ; PWD=/www

sudo: root : TTY=unknown ; PWD=/www

sudo: root : TTY=unknown ; PWD=/www

sudo: root : TTY=unknown ; PWD=/www

sshd[17880]: Received disconnect

sshd[17880]: Disconnected from

sshd[17878]: pam\_unix(sshd:ses

sudo: root : TTY=unknown ; PWD=/www/wwwroot/vidcontrol

35 [TRACE] Template: user/settings/sshkeys

36 [TRACE] Session ID: 2afc9732

36 [TRACE] CSRF Token: -zP8e2Essc

36 [TRACE] Template: user/settings/sshkeys

:37 [TRACE] Session ID: 2afc973



## 3 实战

# 溯源

邮箱: [xxxx@xxxx.com](mailto:xxxx@xxxx.com)

IP : xx.xx.xx.xx

The screenshot shows a web application interface for domain investigation. The top navigation bar includes links for 首页 (Home), API, Graph, 监控 (Monitoring), 招聘 (Recruitment), 情报奖励计划 (Intelligence Reward Plan), and 礼品兑换 (Gift Redemption). Below the navigation bar, there are buttons for API查询 (API Query), 加入监控 (Add Monitoring), 本地API (Local API), and 流量监测 (Traffic Monitoring). The main content area features a tabbed interface with tabs for 情报聚合 (Intelligence Aggregation), 域名解析 (Domain Resolution), 子域名 (Subdomains), WHOIS, 可视化 (Visualization), 数字签名 (Digital Signature), and 用户标签 (User Tags). The WHOIS tab is currently selected, displaying the following information:

当前注册信息	
注册者	
注册机构	
邮箱	
地址	
电话	
注册时间	1999-10-11 11:05:17
过期时间	2026-10-11 11:05:17
更新时间	2019-05-09 04:30:46
域名服务商	MarkMonitor Inc.
域名服务器	NS1.BAIDU.COM; NS2.BAIDU.COM; NS3.BAIDU.COM; NS4.BAIDU.COM; NS7.BAIDU.COM

## 4 总结

## 5 总结

应急响应是一个攻防的过程，对于攻击者其攻击手法有0day or nday，利用这些漏洞形成攻击链去攻陷目标，而防守方则需熟悉业务的场景，去还原攻击者的攻击流程。回顾一次应急响应本质上是知识点的串联。



Thanks