



宜信安全应急响应中心

CreditEase Security Response Center

FREETALK

2018 北京站

可扩展的分布式安全扫描与响应平台

REEBUF





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

公司介绍：

- 宜信——创立于2006年，从事普惠金融和财富管理事业的金融科技企业。在支付、网贷、众筹、机器人投顾、智能保险、区块链等前沿领域积极布局，通过业务孵化和产业投资参与全球金融科技创新。
- 成立十二年以来，始终坚持以理念创新、模式创新和技术创新服务中国高成长性人群、大众富裕阶层和高净值人士，真正的让金融更美好。



宜信财富
CreditEase

宜信普惠
CreditEase

宜人贷
www.yirendai.com

宜信博诚保险服务
CreditEase Insurance Agency

宜农贷
www.yinongdai.com

投米RA
让机器人帮你理财

GOOD & HOPE
好望角咨询

指旺

星火金服
xinghuo.yixin.com

China Growth Capital
华创资本

宜信租赁
CreditEase Leasing

宜信惠民

商通贷

翼启云股
YIQIFIN

REEBUF

宜人宜己，美好生活





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK
2018 北京站

部门介绍：

- 宜信安全部直属于宜信总公司，承接总部及所有子公司的安全需求，为公司的业务安全保驾护航。
 - ※安全部成4年以来，弥补了公司安全基础建设的缺失，发展至今组建了覆盖网络、应用、主机、终端、数据逐层渗透的前沿安全架构，每一步都凝聚着肩负亿万用户信息和财产安全的责任。
 - ※ 2018年我们在传统安全架构上引入了当前热点科技，将人工智能与大数据技术融合到当前的安全架构中，将资产、漏洞、风控和管理有机结合到一起，构建用户画像，为实现安全态势感知与威胁情报预警奠定了基础。
 - ※ 自研的【洞察】漏洞管理平台在GitHub上进行了开源，借此帮助更多金融科技的行业伙伴，完成自动化风险全生命周期的管理并实现风险的可量化，共建互联网金融行业的安全生态。





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

问题和痛点

安全产品学习和运维成本高

- 产品、工具种类繁多，学习和切换成本较高
- 人工使用工具获取资产数据和进行结果处理耗时耗力
- 安全工具功能单一，且无法协同使用



安全检测网络环境多样化

- IDC (多IDC) ,办公网，公网.....单一扫描节点无法满足复杂的需求





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

解决思路



疲于工具的学习和使用



乐于技能提高，专注风险本身





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

0x01 谈谈分布式





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

基于任务队列的分布式扫描

1. 难以将扫描功能解耦合
2. 分发后聚合实现比较繁琐
3. 扫描模块调用接口不统一





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

基于MapReduce模型分布式扫描

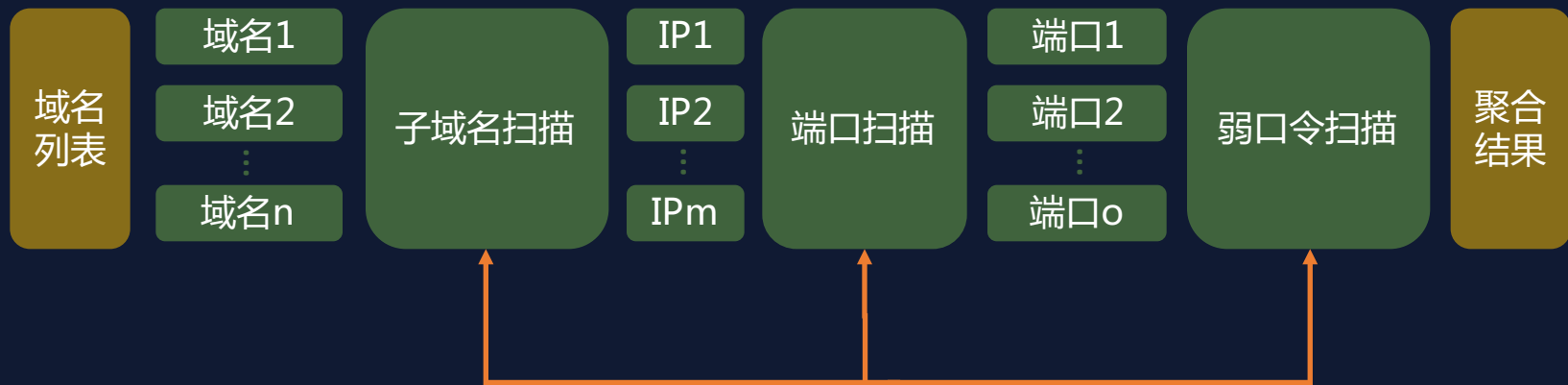
1. 易于任务数据分片和结果聚合
2. 调用链使用简单
3. P2P方式进行数据传输，效率高





举个栗子

- 举例说明任务数据分片和任务链过程: 子域名扫描->端口扫描->弱口令扫描



异步执行





举个栗子

- 举例说明任务数据分片和任务链过程: 子域名扫描->端口扫描->弱口令扫描





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

0x02 功能可扩展（易于开发）





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

插件开发

- 开发过程简化
- 将重复的工作抽象出来封装起来，例如安全通信，任务监控，数据传输等等
- 提供协程，线程，进程任务执行粒度支持
- Python依赖自动检测并安装
- 结果保存为JSON方便后续使用





HelloWorld示例

```
class TestPlugin(Plugin):  
    '''  
    测试插件  
    '''  
  
    def operate(self, **param):  
        '''执行操作'''  
  
        url_list = param['url_list']  
  
        for url in url_list:  
            html = urllib.urlopen(url).read()  
            m_title = re.search(r'<title>(.*?)</title>', html, flags=re.I)  
            title = m_title and m_title.group(1) or 'UNKNOWN'  
            self.logger.info('URL: %s , TITLE: %s' % (url, title))  
            self.push({'DATA': {'TITLE': title, 'URL': url}})
```





任务状态

CRON表达式, 任务参数, 执行次数, 执行花销时间, 优先级等信息

计划任务管理

新建计划任务

ID	名称	描述	插件	CRON	参数	次数	权重	AGENT	操作	方式	状态	策略	耗时	消耗
6666C	数据库备份	备份	SysPlugin	0 0 18 * * *	显示	0	默认	显示	backup_db	终端	启用	+	0	0(秒)
ARACD	WebGIS守护进程	WEB	MinotaurPlugin	@reboot	显示	12	默认	显示	alarm_webgis	终端	启用	+	0	0(秒)
CdRax	敏感目录扫描	敏感字	DirScanPlugin	0 0 15 * * *	显示	30	高	显示	默认	终端	启用	+	0	17小时9分钟50
h7wqg	域名存活判断	通过改	DomainAlivePlugin	0 0 15 * * *	显示	180	默认	显示	默认	终端	启用	+	0	28分钟18秒
HmpgQ	ASVS-Web扫描	使用A	ASVSPPlugin	@reboot	显示	14	内网	显示	默认	终端	启用	+	0	0(秒)
e7CWX	镜像流量数据同步	更新U	MinotaurPlugin	0 0 18 * * *	显示	248	内网	显示	update_data	终端	启用	+	0	17秒
OnuqV	DNS扫描	DNS	DNSQueryPlugin	0 0 15 * * *	显示	36	默认	显示	dns_scan	终端	启用	+	0	1小时29分钟4
uRuLJ	被动式扫描	SQL	PassiveScanPlugin	@reboot	显示	0	默认	显示	默认	终端	禁用	+	0	1分18秒
wkduTs	端口扫描	使用H	PortScanPlugin	0 0 15 * * *	显示	27	默认	显示	默认	终端	启用	+	0	6小时27分钟4
wxU2s	Wall防护检测	Wall	SiteUnderWallPlugin	0 0 9 * * *	显示	20	内网	显示	默认	终端	启用	+	0	28分钟17秒

每页显示行数: 10 显示第 1 至 10 条记录, 共 10 条数据

每页显示行数: 10 显示第 1 至 10 条数据, 共 10 条数据





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

Blade扫描器与分布式平台

调度器

Scheduler

集群

Agent

Agent

...

Agent

单机

Agent

Blade





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

Blade扫描器-命令行模式

```
root@2018-08-08 10:00:12:/# python2.7 plugin_manager.py line 170 | INFO | Available Plugins: ['DnsQueryPlugin',  
, 'PassiveScanPlugin', 'PortScanPlugin', 'MasscanPlugin', 'DirScanPlugin', 'SysPlugin', 'ArkPlugin']  
=====
```

Welcome to Big Sword 0.9.99

BLADE

```
=====
```

BLADE > s

- sysinfo
- SysPlugin
- SubdomainBrutePlugin





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

Blade扫描器-Web模式





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

插件易于分发

- 复用，一键打成Zip包和Zip包导入
- vs PoC 偏向于功能级别的插件





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

多种响应方式

- 平台响应
- 邮件响应
- 第三方即时通讯接口响应





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

平台响应

漏洞名称，描述以及扫描和更新时间

PoC扫描

POC同步

POC选择

POC扫描

📄

🔍

漏洞名称	漏洞描述	扫描结果	扫描时间	更新时间	状态	操作
Nginx源header信息泄露漏洞	CVE-2017-7529整数溢出漏洞,可利用获取源站返回信息。	存在	2017-07-20 18:45:56	2017-09-18 17:44:28	存在	📄
Nginx源header信息泄露漏洞	CVE-2017-7529整数溢出漏洞,可利用获取源站返回信息。	存在	2017-07-24 13:27:42	2017-09-18 17:36:36	未处理	📄
Nginx源header信息泄露漏洞	CVE-2017-7529整数溢出漏洞,可利用获取源站返回信息。	存在	2017-07-24 13:27:45	2017-09-18 17:37:51	未处理	📄
Nginx源header信息泄露漏洞	CVE-2017-7529整数溢出漏洞,可利用获取源站返回信息。	存在	2017-07-24 13:27:48	2017-09-18 17:37:54	存在	📄
Nginx源header信息泄露漏洞	CVE-2017-7529整数溢出漏洞,可利用获取源站返回信息。	存在	2017-07-24 13:28:18	2017-09-18 17:39:18	未处理	📄
Nginx源header信息泄露漏洞	CVE-2017-7529整数溢出漏洞,可利用获取源站返回信息。	存在	2017-07-24 13:28:18	2017-09-18 17:39:18	未处理	📄
Nginx源header信息泄露漏洞	CVE-2017-7529整数溢出漏洞,可利用获取源站返回信息。	存在	2017-07-24 13:28:27	2017-09-18 17:39:39	未处理	📄
Nginx源header信息泄露漏洞	CVE-2017-7529整数溢出漏洞,可利用获取源站返回信息。	存在	2017-07-24 13:29:00	2017-09-18 17:41:03	未处理	📄
Nginx源header信息泄露漏洞	CVE-2017-7529整数溢出漏洞,可利用获取源站返回信息。	存在	2017-07-24 13:29:03	2017-09-18 17:41:06	未处理	📄
Nginx源header信息泄露漏洞	CVE-2017-7529整数溢出漏洞,可利用获取源站返回信息。	存在	2017-07-24 13:29:03	2017-09-18 17:41:06	未处理	📄

每页显示行数: 10

显示第 1 至 10 条结果, 共 56 条数据

<

>

回到顶部

每页显示行数: 10 * 显示第 1 至 10 条结果, 共 56 条数据 < > 刷新





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

邮箱响应

任务运行时的异常

计划任务执行异常 AWVSPugin

```
{
  'TASK_ID': 'u' HmpgZi7nZBFj+vKcnbb8hnujXYfYqwGg36U4iBIW9/s=',
  'ERROR': 'Traceback (most recent call last):\n File "../cesec_host_agent/core/plugin.py", line 136, in
init_thread\n self.operate(**param)\n File "/app/agent/cesec_host_agent/plugins/AWVSPugin.py", line 129, in
operate\n if wvs.is_finished(item):\n File "/app/agent/cesec_host_agent/plugins/AWVSPugin.py", line 354, in
is_finished\n req = requests.post(url, headers=self.headers, data=json.dumps(data), verify=False)\n File
"/usr/lib/python2.7/site-packages/requests/api.py", line 112, in post\n return request(\'post\', url,
data=data, json=json, **kwargs)\n File "/usr/lib/python2.7/site-packages/requests/api.py", line 58, in
request\n return session.request(method=method, url=url, **kwargs)\n File "/usr/lib/python2.7/site-
packages/requests/sessions.py", line 502, in request\n resp = self.send(prepare, **send_kwargs)\n File
"/usr/lib/python2.7/site-packages/requests/sessions.py", line 612, in send\n r = adapter.send(request,
**kwargs)\n File "/usr/lib/python2.7/site-packages/requests/adapters.py", line 504, in send\n raise
ConnectionError(e, request=request)\nConnectionError: HTTPConnectionPool(host=\'10.143.128.77\', port=9999): Max
retries exceeded with url: /api/getScanHistory (Caused by NewConnectionError(\' : Failed to establish a new
connection: [Errno 111] Connection refused\'))\n',
  'RUNNING_STATUS': 'FAILURE',
  'LAST_START_TIME': 1524128960.601824,
  'LAST_FINISH_TIME': 1524260380.443133,
  'DATA': [], 'OPERATION': False,
  'PLUGIN_NAME': 'AWVSPugin',
  'LAST_TIME': 131419.8413090706}
```



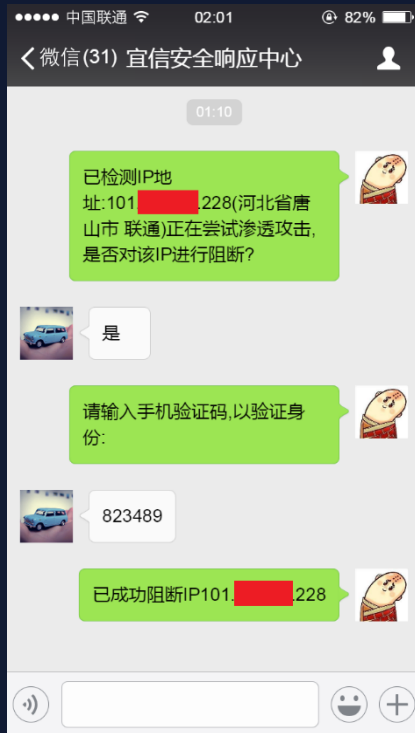


宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

第三方即时通信响应





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

0x03 架构可扩展





分布式架构



宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站



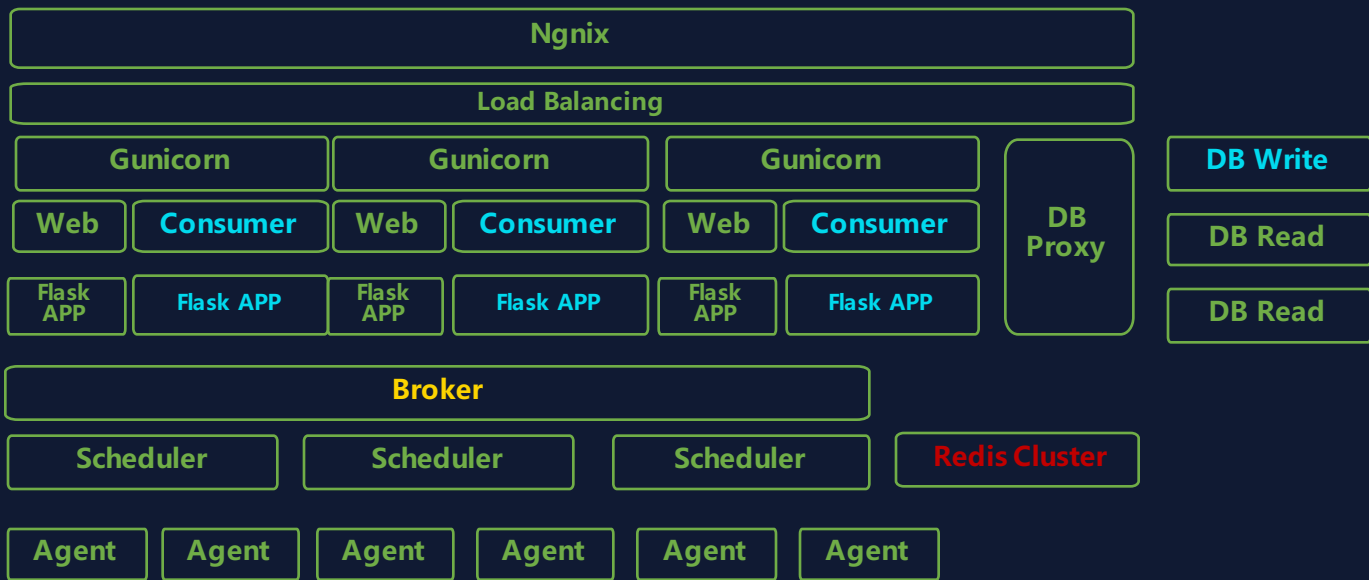


宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

架构扩展





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

0x04 节点可扩展





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

节点简单部署

- 1. 一键安装 `pip install blade.whl`
- 2. 配置Scheduler Server地址并启动，如 `192.168.1.2:5559`
支持配置文件，方便使用自动化运维分发部署



如有环境依赖：提供Docker file生成





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

节点授权与通信

- TCP+JSON通信，自定义协议
- Scheduler授权，Token认证





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

节点授权与通信

Agent管理															
ID	名称	位置	CPU	负载	核数	内存	磁盘	SALT	任务	授权	注册	最后心跳	状态	操作	
显示	URL_28 SERVER	内网	0	0	4	48.4	显示	显示	1	授权	2017-10-23 18:44:24	2018-4-27 18:24:30	在线	授权	删除
显示	阿里云	公网	0	0.13	4	9.7	显示	显示	2	授权	2017-10-23 19:14:17	2018-4-27 18:24:30	在线	授权	删除
显示	邮件服务器	内网	0	0	2	31.8	显示	显示	2	授权	2017-12-8 16:27:51	2018-4-27 18:24:30	在线	授权	删除
显示	移动扫描服务器	内网	36.8	0.63	2	56.7	显示	显示	1	授权	2017-12-26 14:14:32	2018-4-27 18:24:30	在线	授权	删除
显示	天翼云	公网	0	0.05	1	27.3	显示	显示	0	授权	2018-4-17 16:56:29	2018-4-27 18:24:30	在线	授权	删除

每页显示行数: 10 | 显示第 1 至 5 条结果, 共 5 条数据 | [<](#) [>](#) 排序

节点位置, CPU使用率, 负载, 内存使用率, CPU核数位置等





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

节点超时重传机制

- 支持节点与调度器之间进行单向通信
- 如果网络故障可保存数据尝试重连
- 超时时间可配置





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

0x05 展望





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

展望

- 1. 失效转移
- 2. 阻塞方式的数据转发（分布式同步请求服务）





宜信安全应急响应中心
CreditEase Security Response Center

FREETALK

2018 北京站

Get more information ↓

☆本宝宝求关注☆

好看的人都关注啦



再不关注我！

(¬^¬)ゞ你会后悔哒！

