

# Github敏感信息泄露监控

止介 <feei@feei.cn>



- ▶ 白帽子
- ▶ 美丽联合集团 安全项目总监
- ▶ 专注漏洞自动化发现与防御



- ▶ 背景
- ▶ 爬取方案
- ▶ 特征思路
- ▶ 规则设计
- ▶ 报告
- ▶ 误报
- ▶ 未来

# 背景

以**技术手段**杜绝由于**员工意识**问题导致的**Github敏感信息泄露**

## 爬取方案

Proxy+Page vs Token+API

## 准实时与频率限制的取舍

$$\text{CORP} * \text{RULES}(\text{N1}) * (\text{SEARCH} + \text{PAGES}(\text{N2}) + (\text{PAGE\_LIST} + \text{HTML\_URL} + \text{SHA} + \text{PATH} + \text{FULL\_NAME} + \text{CONTENT}) * \text{PER\_PAGE}(\text{N3}))$$

$$\text{N1} = ?, \text{N2} = 20, \text{N3} = 50$$

Token Max Requests(5000) / Single Rule

$$\text{Requests}(320) = \text{Rules}(15)$$




内部特征 - 域名反查

whois查询 邮箱反查 注册人反查 电话反查 域名批量反查 域名抢注 历史查询								
dugu@mogujie.com					查看分析	查询记录		
序号	域名	注册者	电话	注册商	DNS	注册时间	过期时间	更新
1	juandou.net	yue xu qiang	--	ENAME TECHNOLOGY C O., LTD.	NS1.DREAMHOST.COM NS2.DREAMHOST.COM	2010-04-27	2018-04-27	🔄
2	juangua.cn	杭州卷瓜网络科技有限公司	--	厦门易名科技股份有限公司	dns13.hichina.com dns14.hichina.com	2010-08-17	2018-08-17	🔄
3	juangua.com	yue xu qiang	--	ENAME TECHNOLOGY C O., LTD.	F1G1NS1.DNSPOD.NET F1G1NS2.DNSPOD.NET	2010-01-17	2018-01-17	🔄
4	juangua.org	yue xu qiang	--	eName Technology Co. L td.	DNS13.HICHINA.COM DNS14.HICHINA.COM	2010-08-09	2018-08-09	🔄
5	kolsocial.com	yue xu qiang	--	HICHINA ZHICHENG TEC HNOLOGY LTD.	DNS10.HICHINA.COM DNS9.HICHINA.COM	2016-01-10	2018-01-10	🔄
6	linglang.com	yue xu qiang	--	ENAME TECHNOLOGY C O., LTD.	F1G1NS1.DNSPOD.NET F1G1NS2.DNSPOD.NET	2004-08-31	2018-08-31	🔄
7	linkeye.net	yue xu qiang	--	ENAME TECHNOLOGY C O., LTD.	F1G1NS1.DNSPOD.NET F1G1NS2.DNSPOD.NET	2010-06-08	2018-06-08	🔄
8	linlang.cn	杭州卷瓜网络科技有限公司	--	厦门易名科技股份有限公司	flg1ns1.dnspod.net flg1ns2.dnspod.net	2008-05-31	2023-05-31	🔄
9	meili-inc.com	yue xu qiang	--	ENAME TECHNOLOGY C O., LTD.	F1G1NS1.DNSPOD.NET F1G1NS2.DNSPOD.NET	2016-03-28	2019-03-28	🔄
10	mogucdn.com	yue xu qiang	--	ENAME TECHNOLOGY C O., LTD.	NS3.DNSV5.COM NS4.DNSV5.COM	2013-10-28	2018-10-28	🔄
11	mogujie.cn	杭州卷瓜网络科技有限公司	--	厦门易名科技股份有限公司	flg1ns1.dnspod.net flg1ns2.dnspod.net	2010-08-18	2023-08-18	🔄
12	mogujie.com	yue xu qiang	57188867550	eName Technology Co.,L td	ns3.dnsv5.com ns4.dnsv5.com	2010-08-18	2023-03-25	🔄
13	mogujie.com.cn	杭州卷瓜网络科技有限公司	--	厦门易名科技股份有限公司	flg1ns1.dnspod.net flg1ns2.dnspod.net	2010-08-18	2020-08-18	🔄
14	mogujie.org	yue xu qiang	--	eName Technology Co. L td	F1G1NS1.DNSPOD.NET F1G1NS2.DNSPOD.NET	2010-08-18	2018-08-18	🔄

通用内网域名特征

.net	<u>alipay.net</u> <u>taobao.net</u> <u>qihoo.net</u> <u>elenet.me</u>
后缀	<u>mogujie.org</u> <u>tuniu.org</u> <u>dianrong.io</u> <u>bilibili.co</u>
inc	<u>meili-inc.com</u> <u>sohu-inc.com</u> <u>alibaba-inc.com</u> <u>cainiao-inc.com</u>
corp	<u>ctripcorp.com</u>
相似	<u>wemomo.com</u>






[Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)

[Repositories](#) **Code 2K** [Commits](#) [Issues 1](#) [Wikis 145](#) [Users](#)


**2,749 code results** Sort: Best match ▾

 **wenling-lichao/tt-cli – mogu**  
Showing the top five matches Last indexed 25 days ago

```
1 registry=http://npm.f2e.mogujie.org/  
2 npm.f2e.mogujie.org/:_password="WGNfMm9wdGlqbTI="  
3 npm.f2e.mogujie.org/:username=xincan  
4 npm.f2e.mogujie.org/:email=xincan@meili-inc.com  
5 npm.f2e.mogujie.org/:always-auth=true
```

**FEEI wufeifei/GSIL – test.java** Java  
Showing the top two matches Last indexed 6 days ago

```
1 xxx.mogujie.org  
2 top.meili-inc.com  
3 jd.local  
4 qiyi.domain
```

 **rusonding/muse – TaskReporter.java** Java  
Showing the top three matches Last indexed on Aug 16

```
1 /*  
2  * 蘑菇街 Inc.  
3  * Copyright (c) 2010-2015 All Rights Reserved.  
4  *  
5  * Author: wuya  
6  * Create Date: 2015年10月9日 上午9:58:47  
7  */  
8  
9 package com.mogujie.jarvis.core;  
10  
11 import com.mogujie.jarvis.core.domain.TaskDetail;
```

## 通用模糊搜索词

domain.tld corp  
domain.tld dev  
domain.tld inc  
domain.tld pre  
domain.tld test  
domain inc  
domain copyright



## Meili-Inc

内部域名

mogujie.org / meili-inc.com

对外邮箱

mail.mogujie.com



代码注释	IQIYI Inc
内部域名	qiyi.domain
主机	qiyi.virtual
数据库	qiyi.db
对外邮箱	mail.iqiyi.com

# Baidu

代码注释	@baidu.com Baidu, Inc
内部域名	<u>vm.baidu.com</u> / <u>epc.baidu.com</u> iwm.name
主机	<u>vm.baidu.com</u> / <u>nj01.baidu.com</u> sh01.dba-nuomi-bgoods.sh01
数据库	xdb.all.serv db-dba-dbbk-001.db01
对外邮箱	<u>smtp.baidu.com</u>

Other

京东	jd.local	携程	<u>ctripcorp.com</u>
360	<u>qihoo.net</u>	去哪儿	<u>qunar.net</u>
搜狐	<u>sohuno.com</u>	支付宝	<u>alipay.net</u>
苏宁	<u>cnsuning.com</u>	淘宝	<u>taobao.net</u>
陌陌	wemomo.com	小米	<u>mioffice.cn</u>
饿了么	<u>elenet.me</u>	菜鸟	cainiao-inc

企业邮箱	<u>exmail.qq.com</u> <u>qiye.163.com</u> <u>263.net</u> <u>mxhichina.com</u> <u>icoremail.net</u> ...
私密文档	<u>账号 密码</u>
微信密钥	<u>appid appsecret</u>
QCloud密钥	privatekey publickey



强制搜索	<u>加引号，比如"meili-inc.com"</u>
横杠默认不匹配	<u>使用"meili-inc.com"搜索不出，使用"meili inc.com"则可以</u>
分词特性	<u>appsecret</u>

Keywords	<p>多个关键词可以用空格，比如‘账号 密码’；</p> <p>某些关键字出现的结果非常多，所以需要精确搜索时可以用双引号括起来，比如“<a href="#">ele.me</a>”；</p>
Mode	<p>normal-match(default): 匹配包含keyword的行，并记录该行附近行</p> <p>only-match:仅匹配包含keyword行</p> <p>full-match: 搜出来的整个问题都算作结果</p> <p>mail wechat qcloud</p>
Extension	<p>多个后缀可以使用英文半角逗号 (,) 分隔，比如‘java,php,python’</p>

## 邮件

调快客户端收信的时间间隔

imap模式，保证各平台统一处理已读状态

可以提交或者可研究的打上标记

误报删除到垃圾桶，定期针对垃圾桶优化规则减少误报

对于邮件发送频率限制，可以多配置多个不同运营商的发件账号

# Exclude Repository Name

Github博客	<u>github.io</u> <u>github.com</u>
Android项目	app/src/main
爬虫	crawler spider scrapy 爬虫
插件	surge adblock .pac
无用	linux_command_set domains jquery sdk linux contact readme hosts authors .html .apk

# Exclude Codes

**Link**

<a href  
<iframe src  
](

**无用**

DOMAIN-SUFFIX 文档 接口 友情链接 官网



1. 持续提升准确性
2. 实时性对抗
3. 扩充通用类规则
  1. DB
  2. REDIS
  3. SSH

