



black hat[®]
EUROPE 2016

Chasing Foxes by the Numbers: Patterns of Life and Activity in Hacker Forums

Christopher Ahlberg, Co-Founder & CEO

Recorded Future

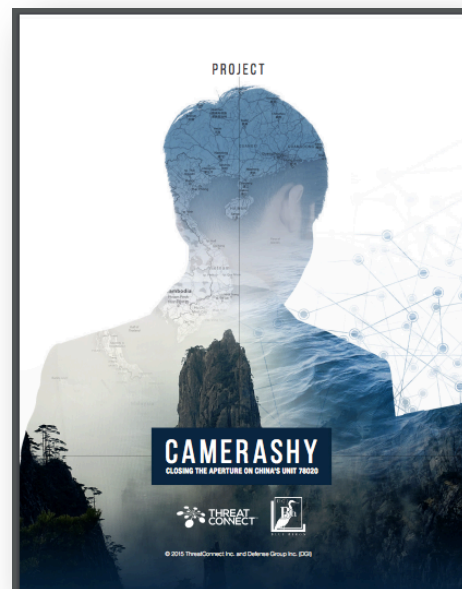
c@recordedfuture.com

[@cahlberg](https://twitter.com/cahlberg)

Attribution [Often] Based on Sloppy Handle Usage



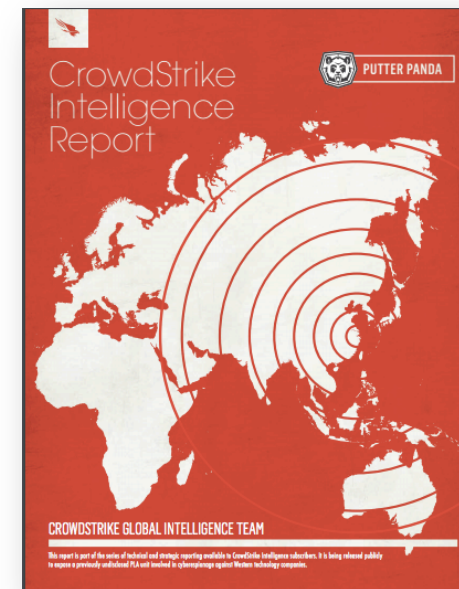
UglyGorilla
SuperHard



GreenSky27



QQ identity
5054-3533



cpyy

Handles and Forums key to attribution

"CPYY"

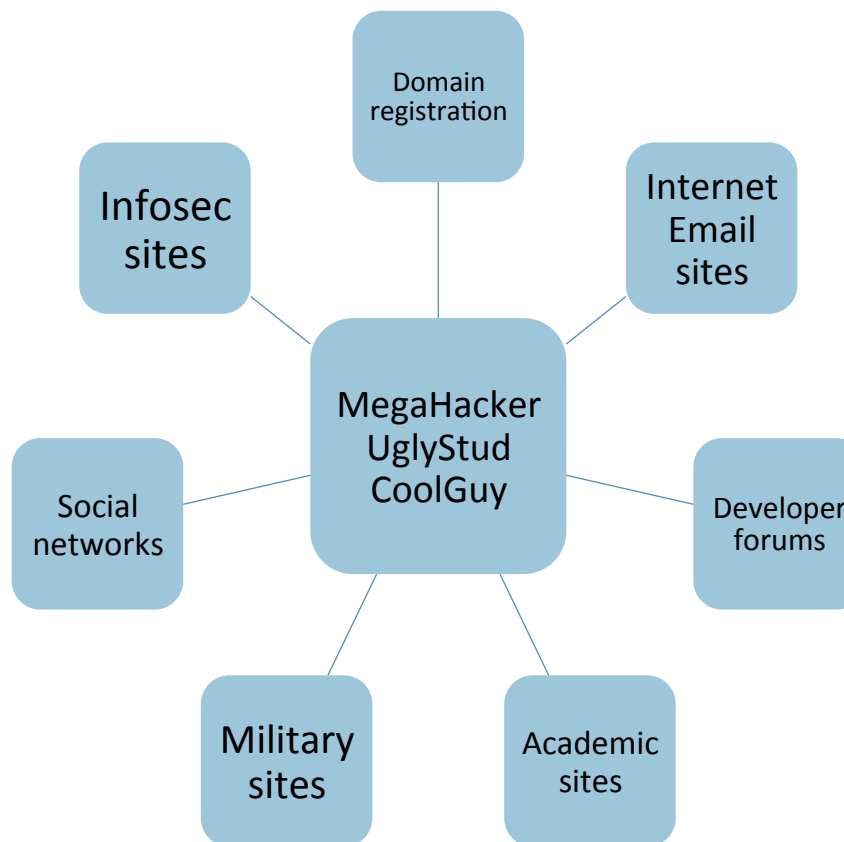
Several email addresses have been associated with cpyy, who also appears to use the alternate handles cpyy and cpyy.chen:

- cpyy@sina.com
- cpyy@hotmail.com
- cpyy.chen@gmail.com
- cpyy@cpyy.net

The cpyy.net domain lists "Chen Ping" as the registrant name, which may be cpyy's real name, as this correlates with the initials "cp" in "cpyy". A personal blog for cpyy was found at <http://cpyy.blog.163.com/>. The profile on this blog (shown in Figure 2 below) indicates that the user is male, was born on 25 May 1979, and works for the "military/police" (其他- 军人/警察).



Figure 2. cpyy Personal Blog on 163.com



If Better Actor Opsec, Then What?

Forum Targeting

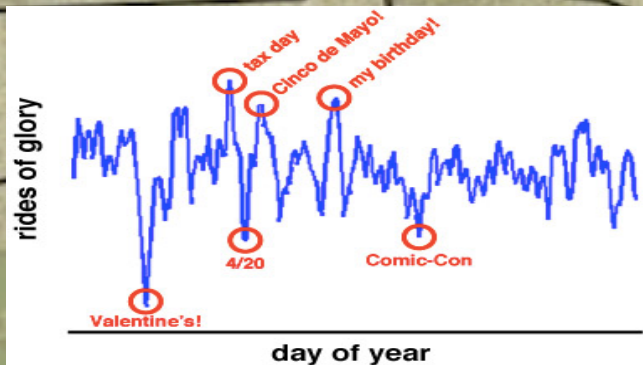
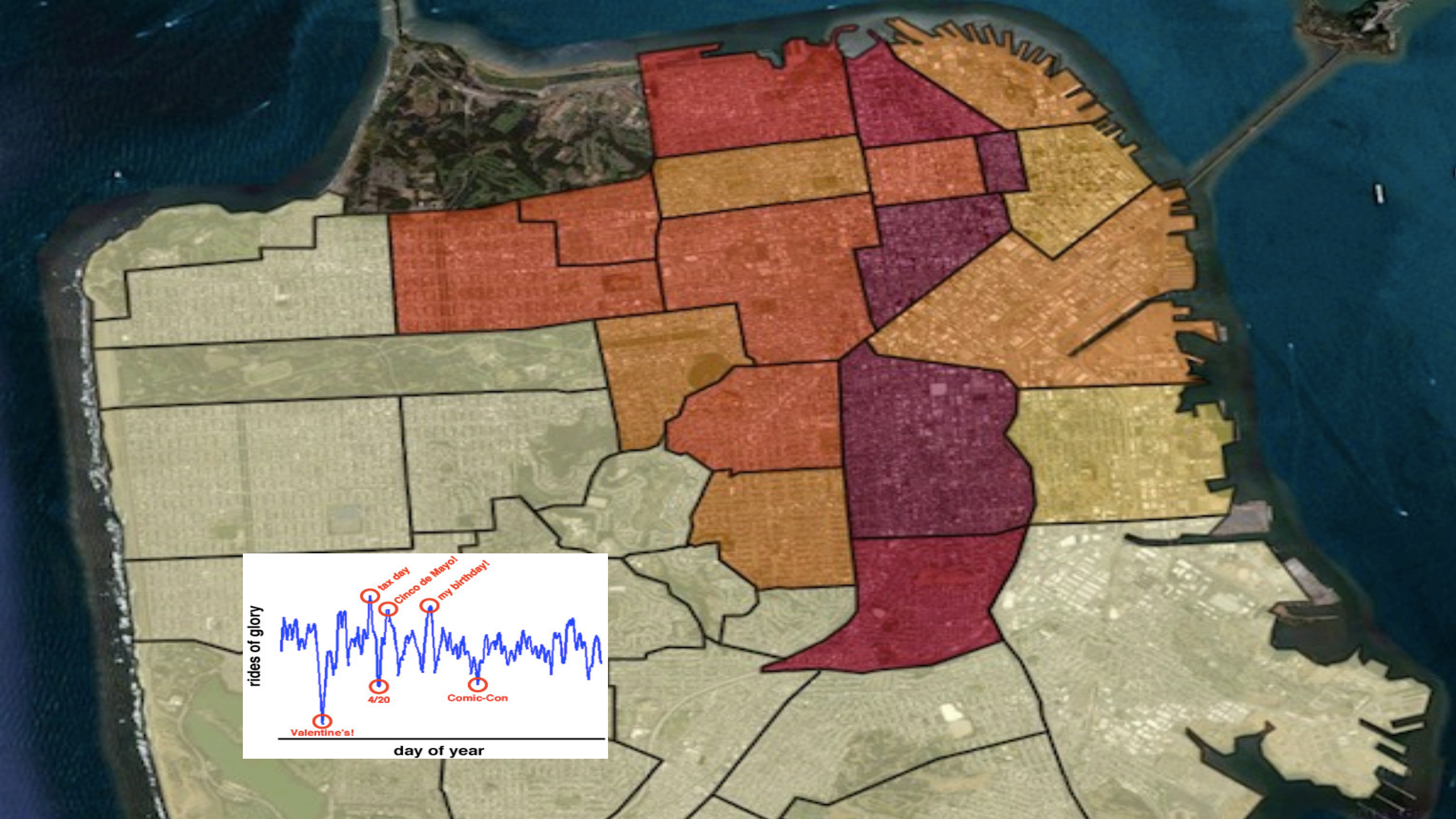
Key handles in forums

Handle hopping within and Across forums

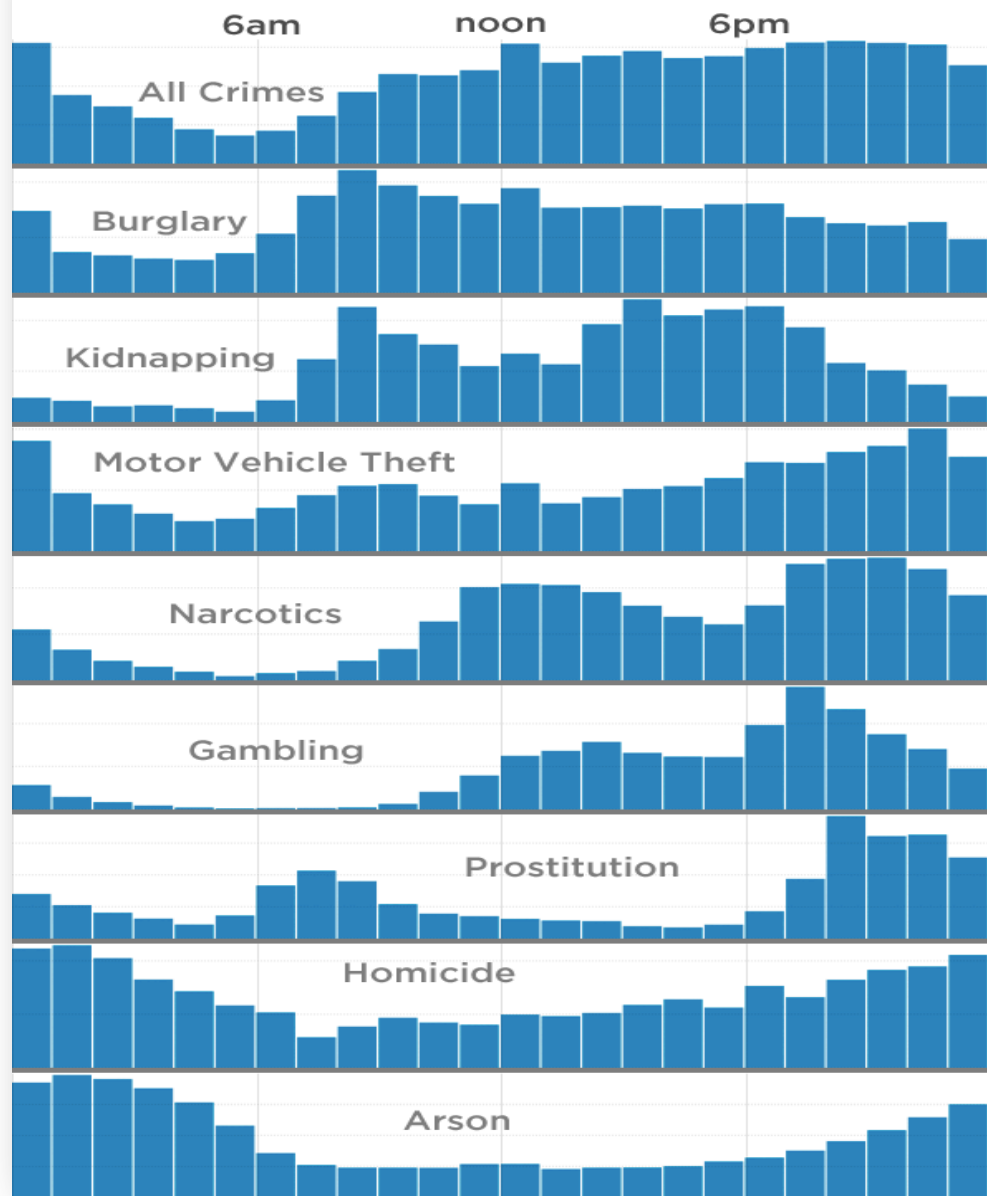
Crews of handles

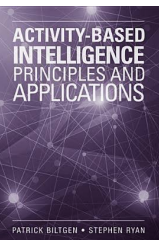
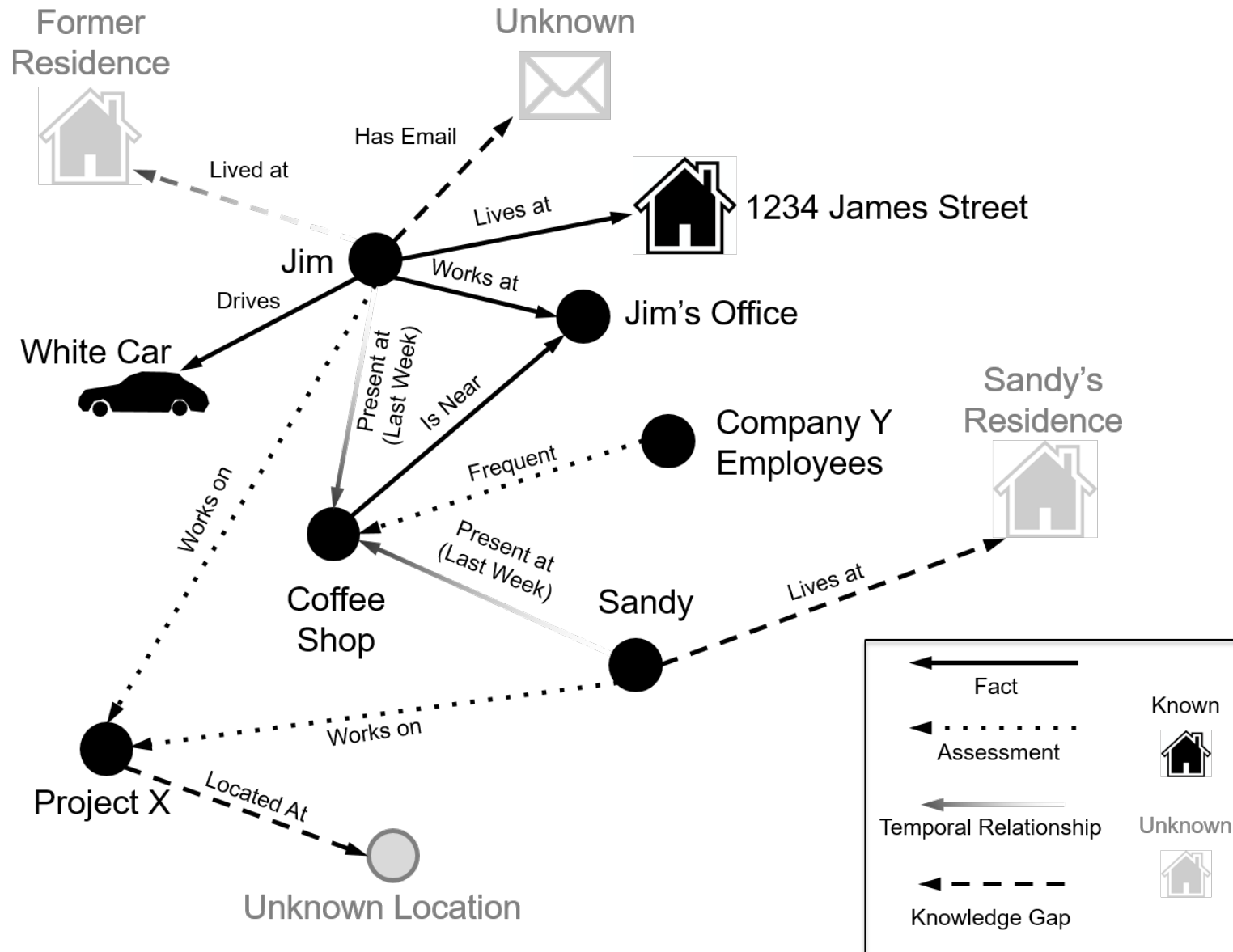
Can we apply some

$$R = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\left[\sum_{i=1}^n (x_i - \bar{x})^2 \sum_{i=1}^n (y_i - \bar{y})^2 \right]^{1/2}} \quad ?$$



The Daily Rhythm of Crime in Chicago







SHOW



منتديات شباب ليبيا

LIBIANYOUTHS.COM

مشاركات ليبيا

سبحان الله وبحمده عدد خلقه ورضا نفسه وزنة عرشه ومداد كلماته

المشاركات	المواضيع	المستخدمين
110,936	9,347	1,369
60,500	5,370	1,369
42,424	4,058	1,369

آشياء

اولين اخصائى شبكة در ايران

THE FIRST SECURITY FORUM IN IRAN

تقديم - ارسال - اخبار - الامن - تطوير - برسل و پليغ - پست هاى جديد - دوره هاى آموزشى

تقديم - ارسال - اخبار - الامن - تطوير - برسل و پليغ - پست هاى جديد - دوره هاى آموزشى

تقديم - ارسال - اخبار - الامن - تطوير - برسل و پليغ - پست هاى جديد - دوره هاى آموزشى

والصالح خير من

شبكة شموخ الإسلام

shamikh.info

مؤسسة الفرقان

فتربصوا إنا معكم متربصون

أعلنت الخلافة الإسلامية يوم الأحد 1 رمضان 1435 هـ - 29 يونيو 2014 م، ومضى عليها 556 يوماً، وستظل بالبقاء على منهاج النبوة - بإذن الله -

منتديات اسلامية

التسجيل الدخول

اسم المستخدم: *
كلمة المرور: *

هل من ترحيب بواسطة: Gana
التردد: 3 اشهر

متعدد خلفيات بدقة عالية
اسم الملف: enter
التردد: 4 ساعات

القرآن الكريم
كل ما يتعلق بالقرآن الكريم وعلموه
العضو: 118
الردود: 286

JO-SHARING.COM

الشيرينج العربى

للطباق والاستشارة
00962796726926
00962799109066

00962796726926

IP TV

جيوش الهكرز

اختراق البريد
اختراق الاجهزة
اختراق الشبكة
اختراق المواقع
ادوات الإحتراق

موقع منظمة أمن الإسلام يرحب بكم

الموقع | المنتدى

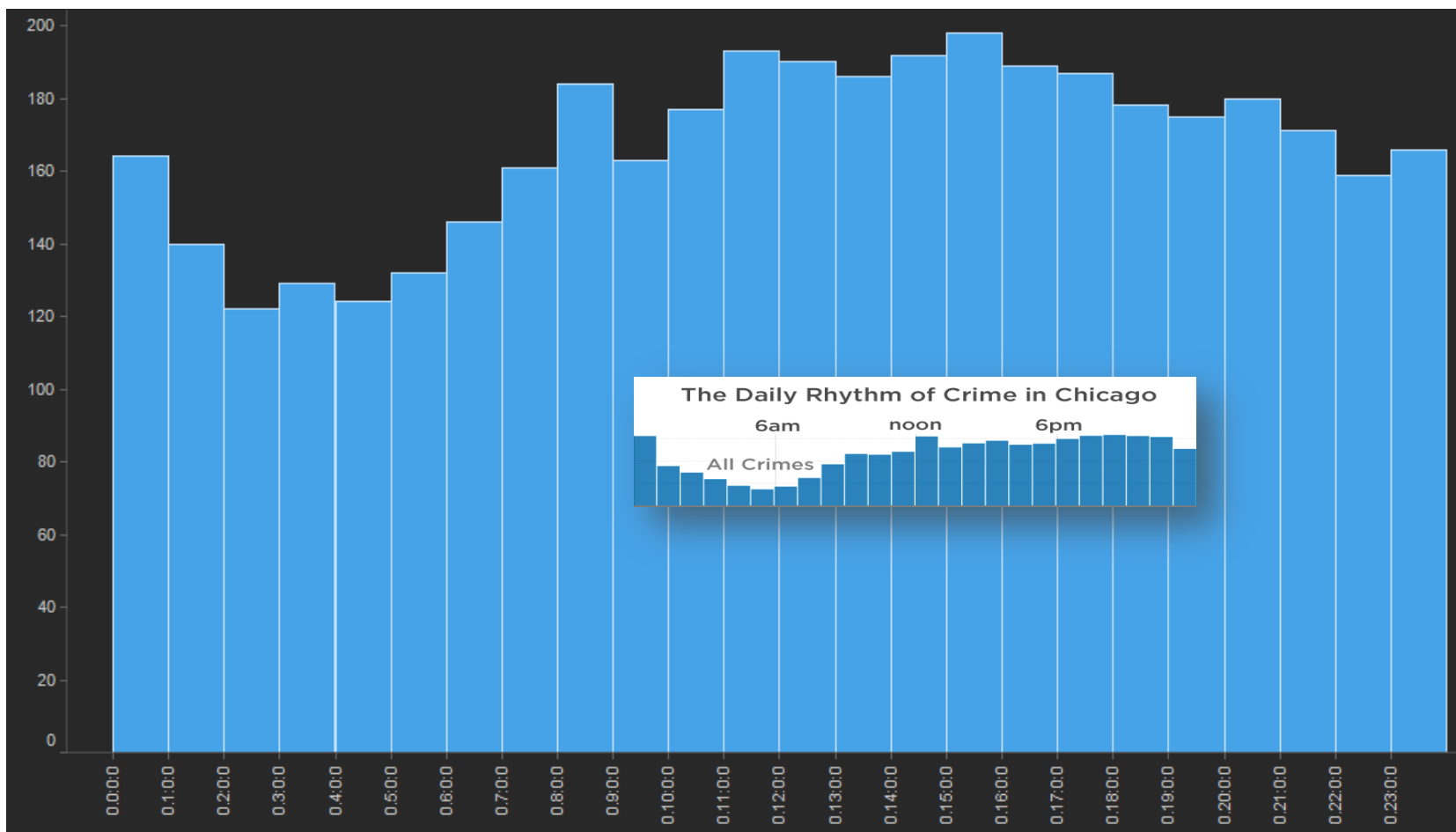
سؤال & اجابة | التبليغ عن موقع إسلامي مصاب | القرآن الكريم | راديو القرآن الكريم

تحيات [ادارة موقع منظمة أمن الإسلام]
copyright © 2010-2013 ig-sec.org, Inc.
[18]sec org

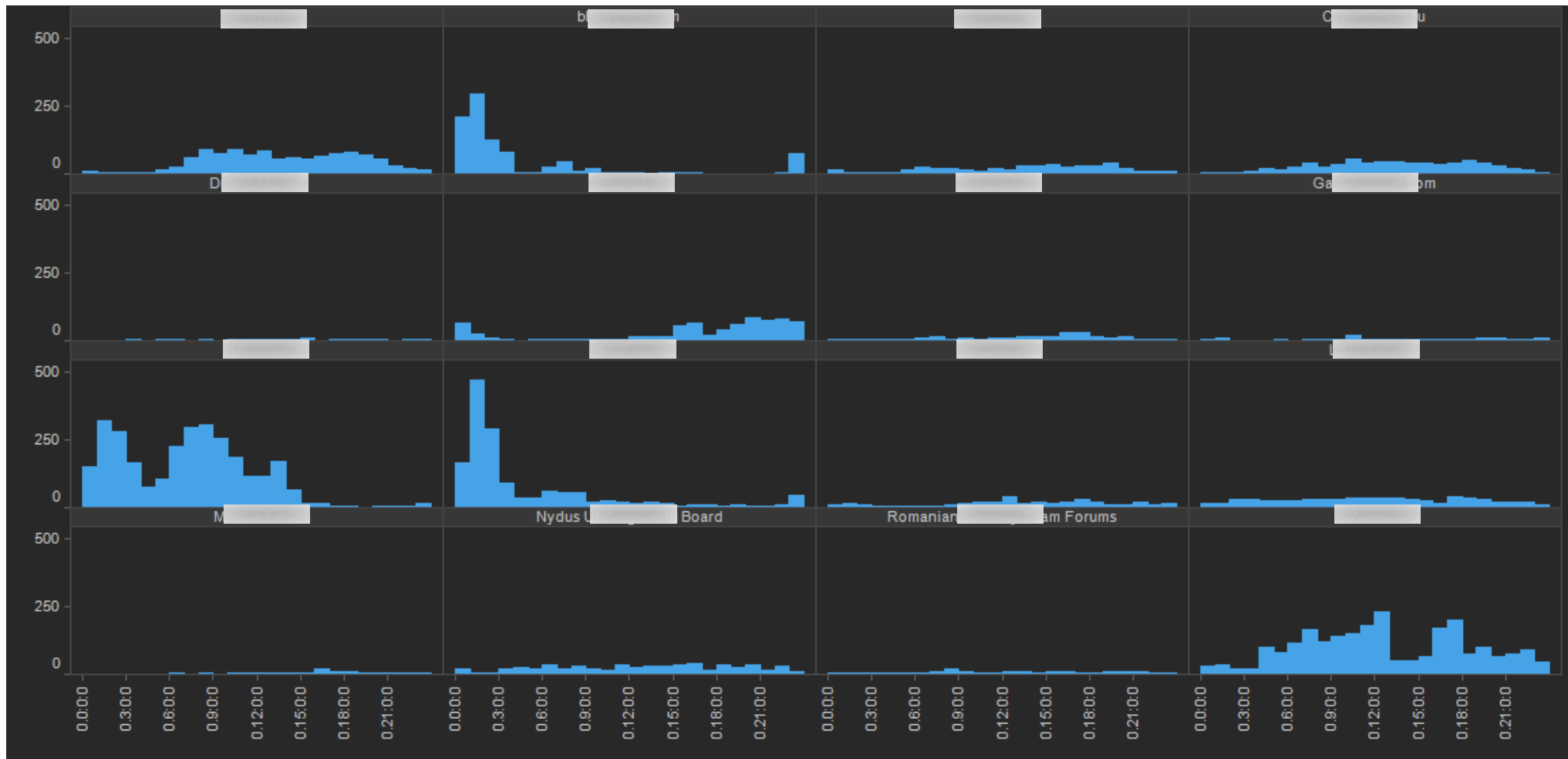
- Automated collection
- 750 hacker/criminal forums from Deep/Dark web
- 4 year collection
- 7 languages
- Indexed
- NLP/Feature extraction for cyber attacks, vulnerabilities, exploits, technical indicators, etc.

Surprisingly little handle re-use
96.6%+ used once
1,446,815 total

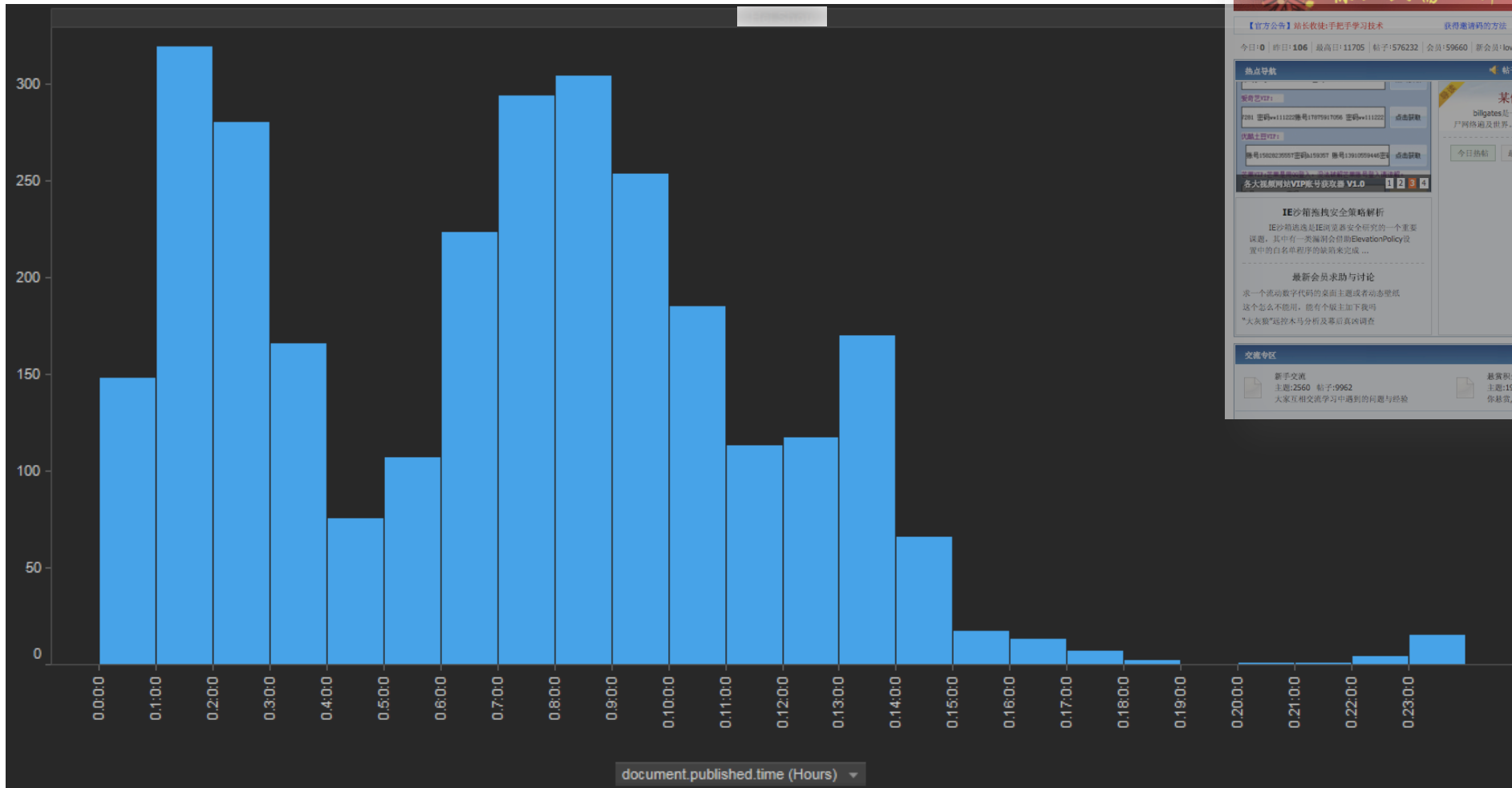
First Pattern: Hackers Have Hours



They Just Differ



Distinct Patterns



黑手安全网 www.leishou.com.cn

站长收徒&快速学技术 一对一教学,五年信誉保证 手把手指导,专攻网络安全

全站首页 社区首页 社区聚焦 社区广场 社区群组 积分升级 手机客户端

登录 注册 找回密码 帖子 搜索

震惊: 只需一部手机月入万元 立即点我 黑手安全网提示: 站外广告, 风险自担

【官方公告】站长收徒: 手把手学技术 获得邀请码的方法 【官方公告】网络交易, 风险提示 【本站广告招租】最低100元起

今日: 0 昨日: 106 最高日: 11705 帖子: 576232 会员: 159660 新会员: love123 发帖 精华

帖子内容与附件失效, 请回复本帖进行处理 15-07-16 发帖回复验证码只针对小于10帖的会员 15-07-16

某僵尸网络被控端恶意样本分析
biligates是一个近几年非常活跃的DDoS僵尸网络, 此程序组成的僵尸网络遍及世界, 网络中bot节点多是一些存在弱口令或软... 【详情】

IE沙箱检测安全策略解析
IE沙箱检测是IE浏览器安全研究的一个重要课题, 其中有一类漏洞会借助ElevationPolicy设置中的白名单程序的策略来完成...

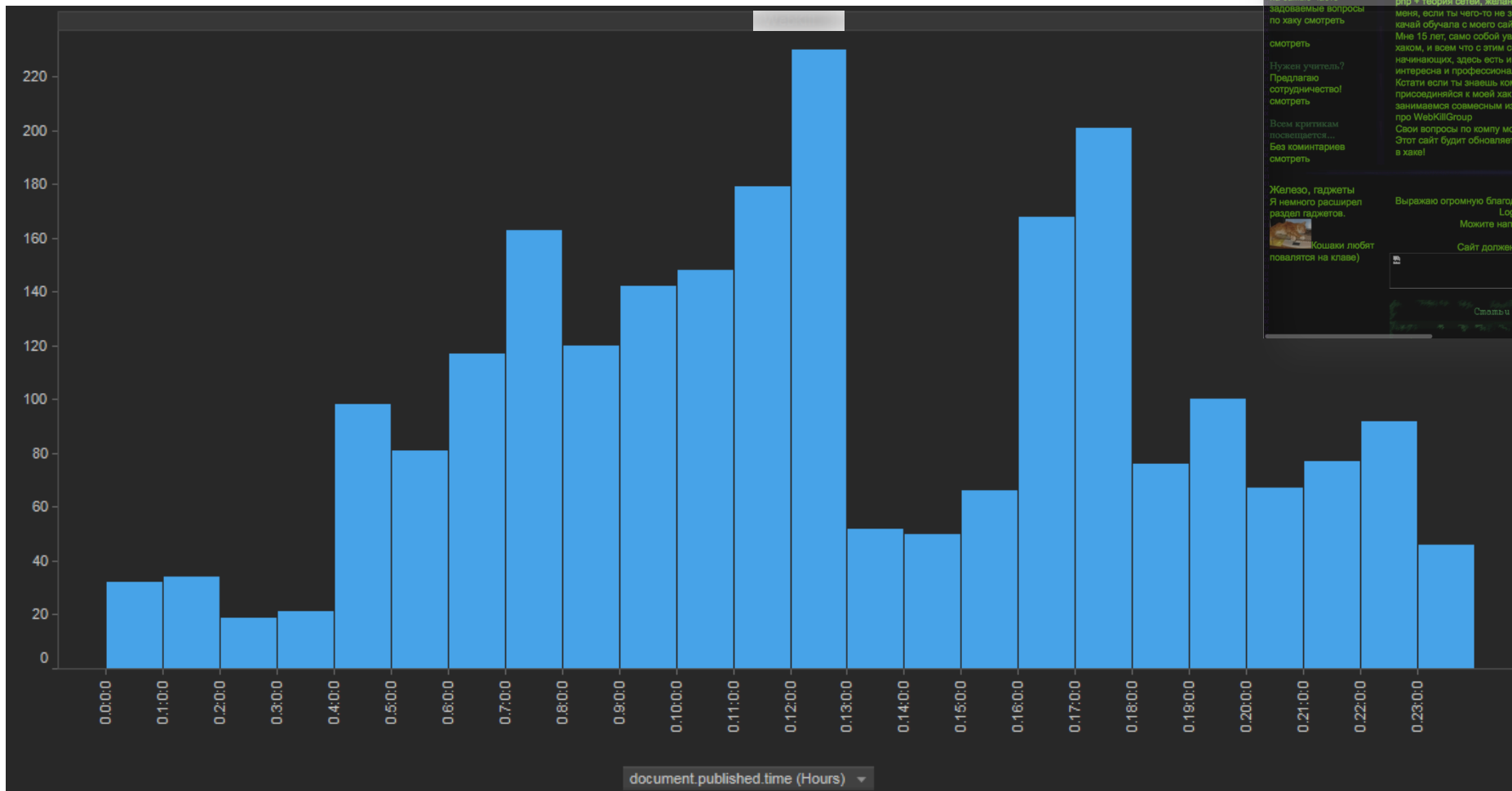
最新会员求助与讨论
求一个流动数字代码的桌面主题或者动态壁纸 这个怎么用, 能有个版主加下我吗 "大头狼" 技术分析分析及幕后真相调查

新手交流 主题: 2560 帖子: 9962 大家互相交流学习中遇到的问题与经验

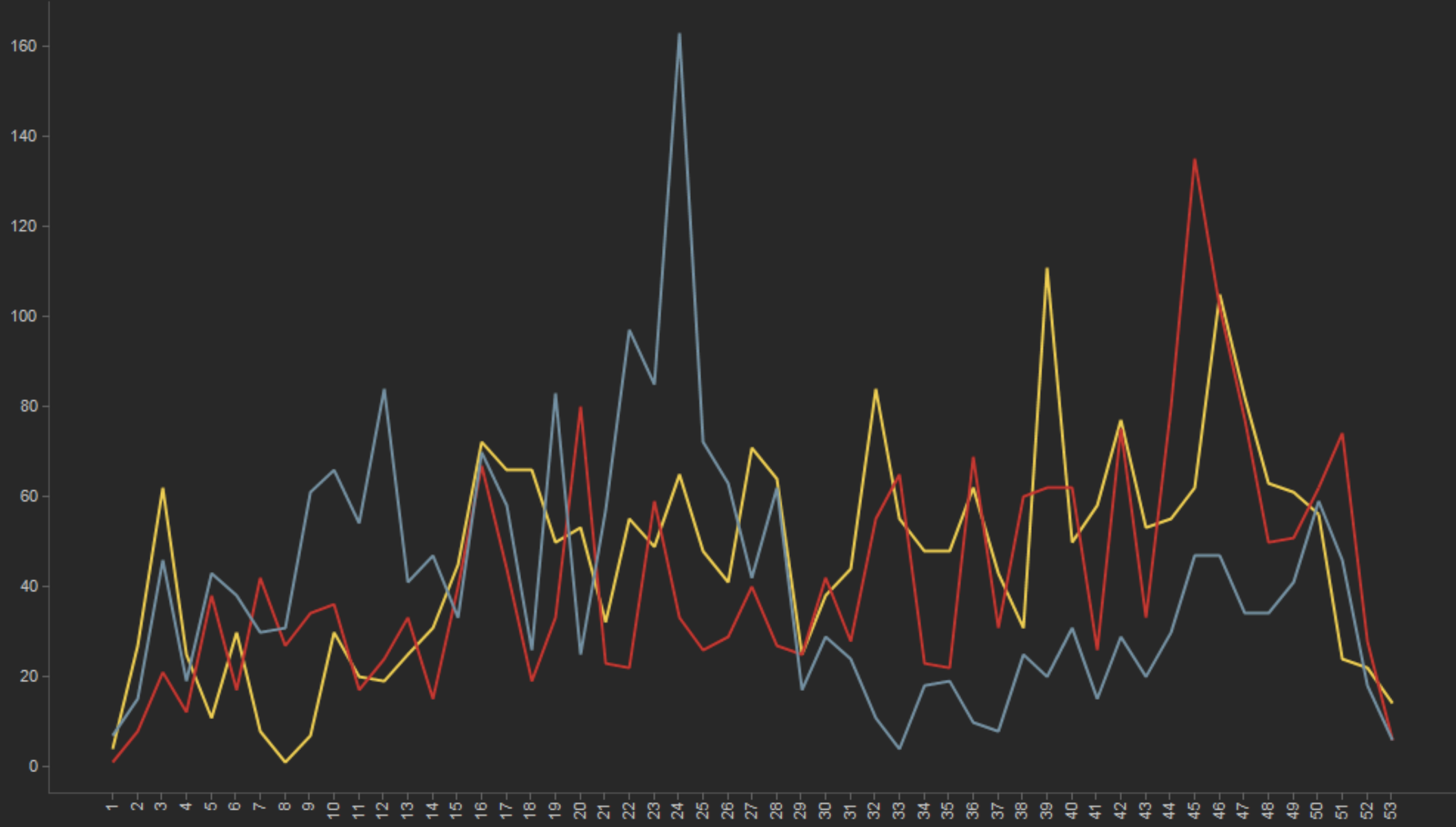
悬赏积分问答 主题: 1997 帖子: 9783 你提问, 我来答, 解决大家的学习问题

IT资讯与安全播报 主题: 12347 帖子: 14349 聚焦安全热点与事件, 揭秘业界内幕与安全人物

Multiple Geos or Crews?



count – document.published.date



Line by:
(None) ▾

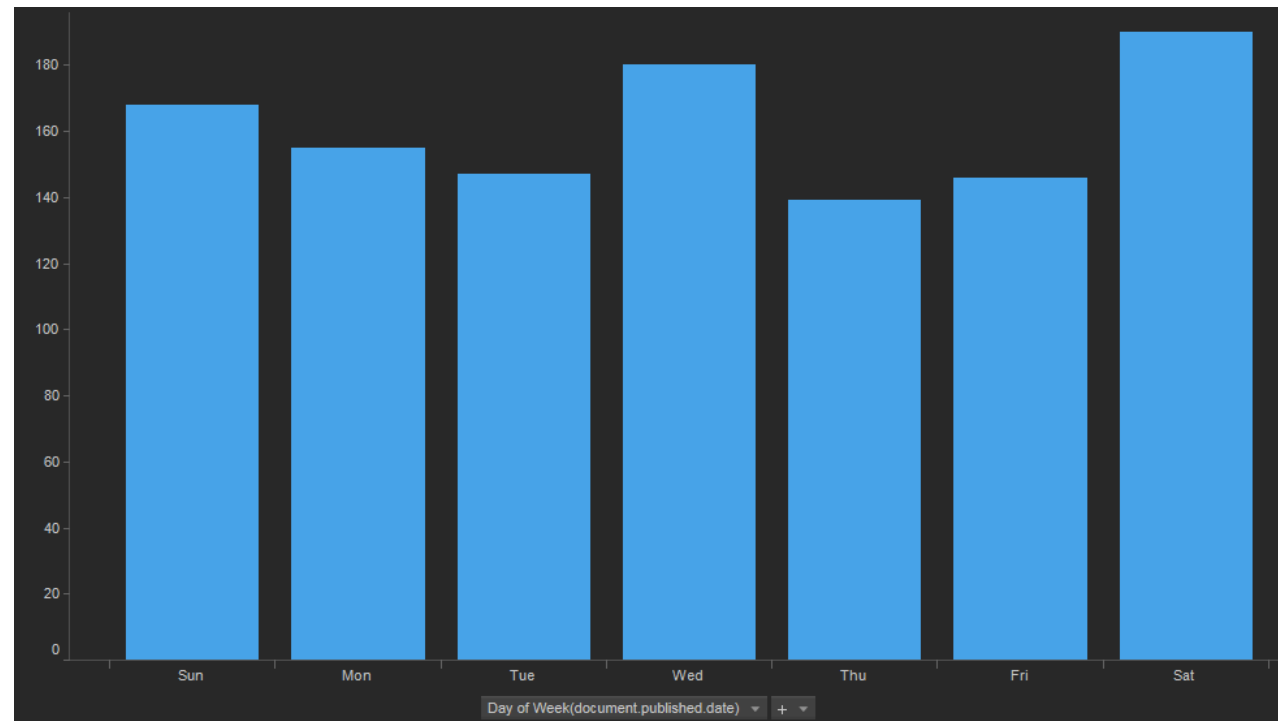
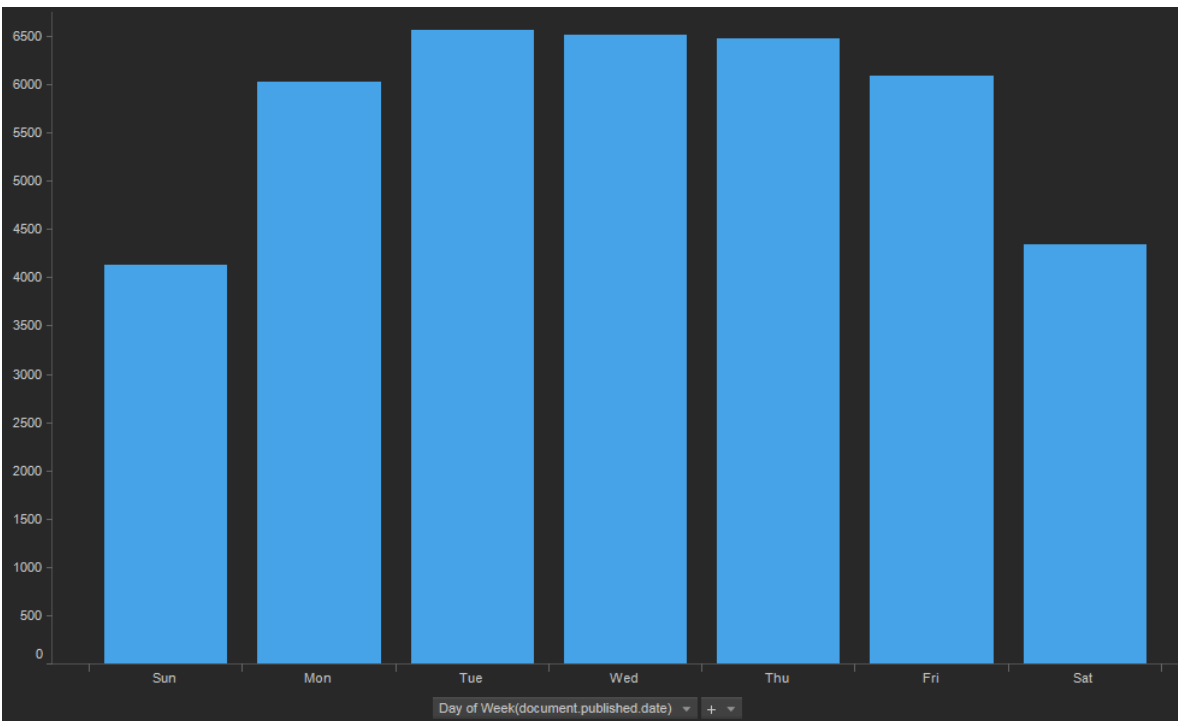
Color by:
source.na... ▾ + ▾

- Yellow
- Red
- Blue

Sum(count) ▾ + ▾

Week(document.published.date) ▾ + ▾

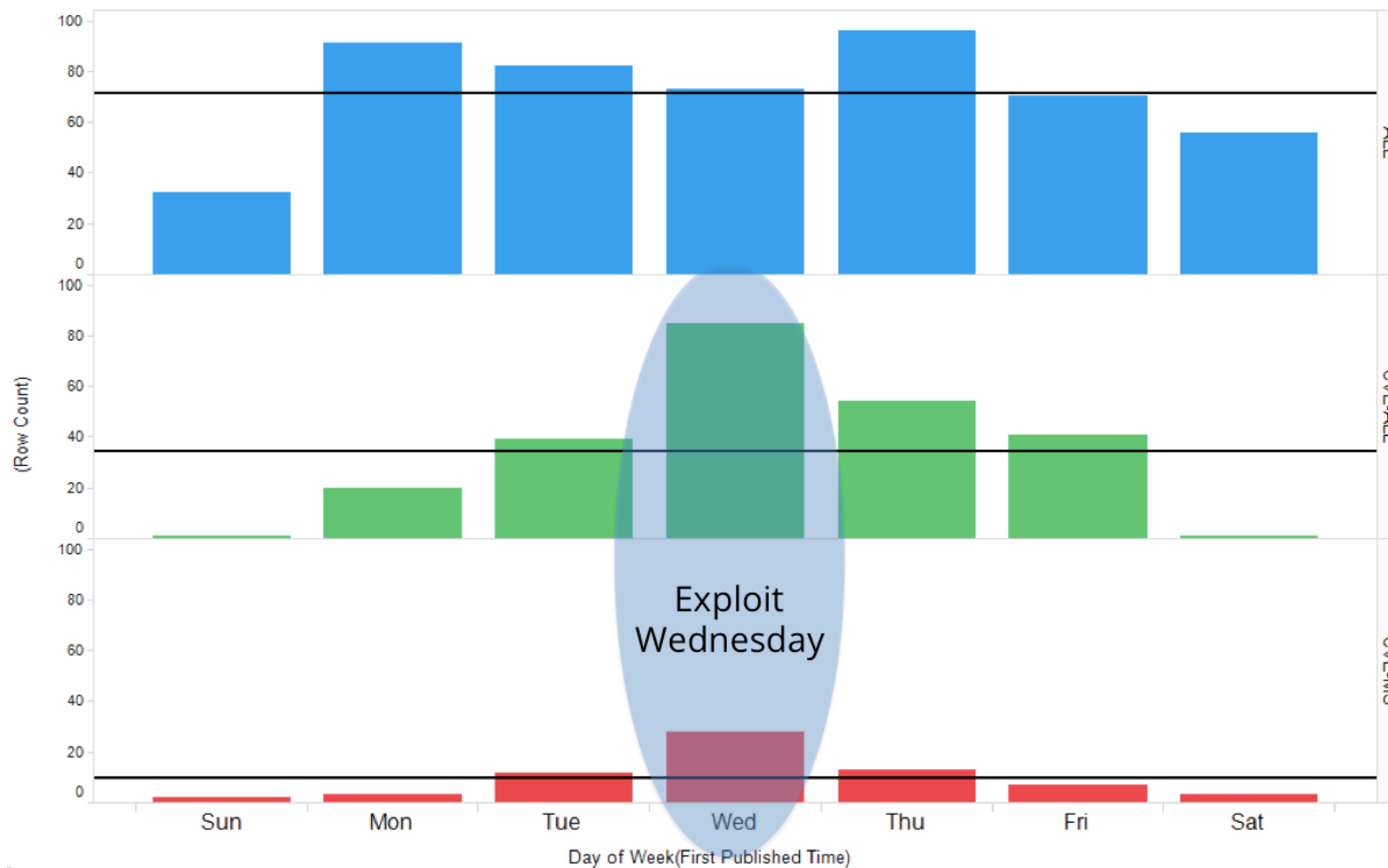
Distinct Weekly Patterns



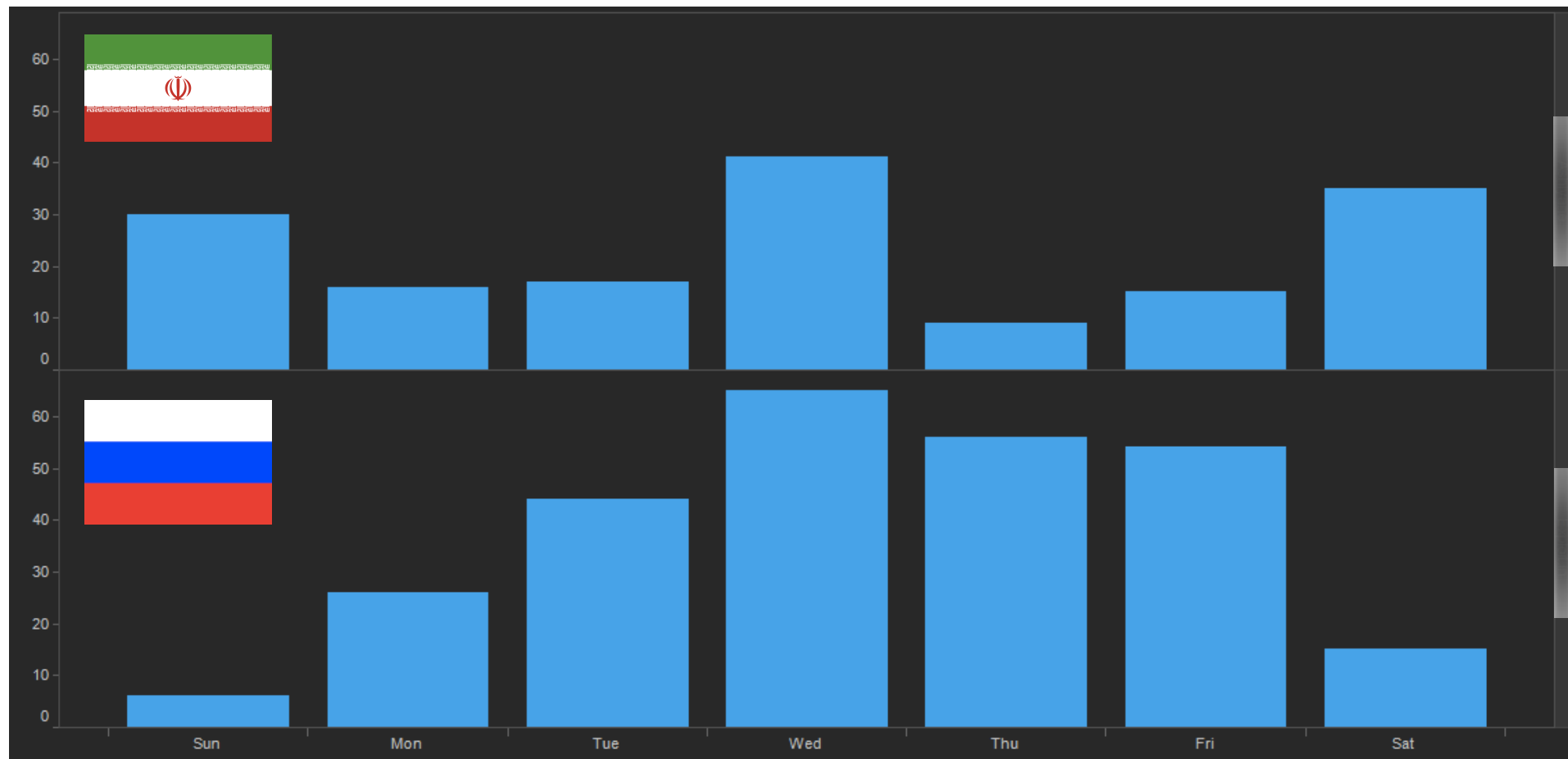
Smoking out the Rats with External Events



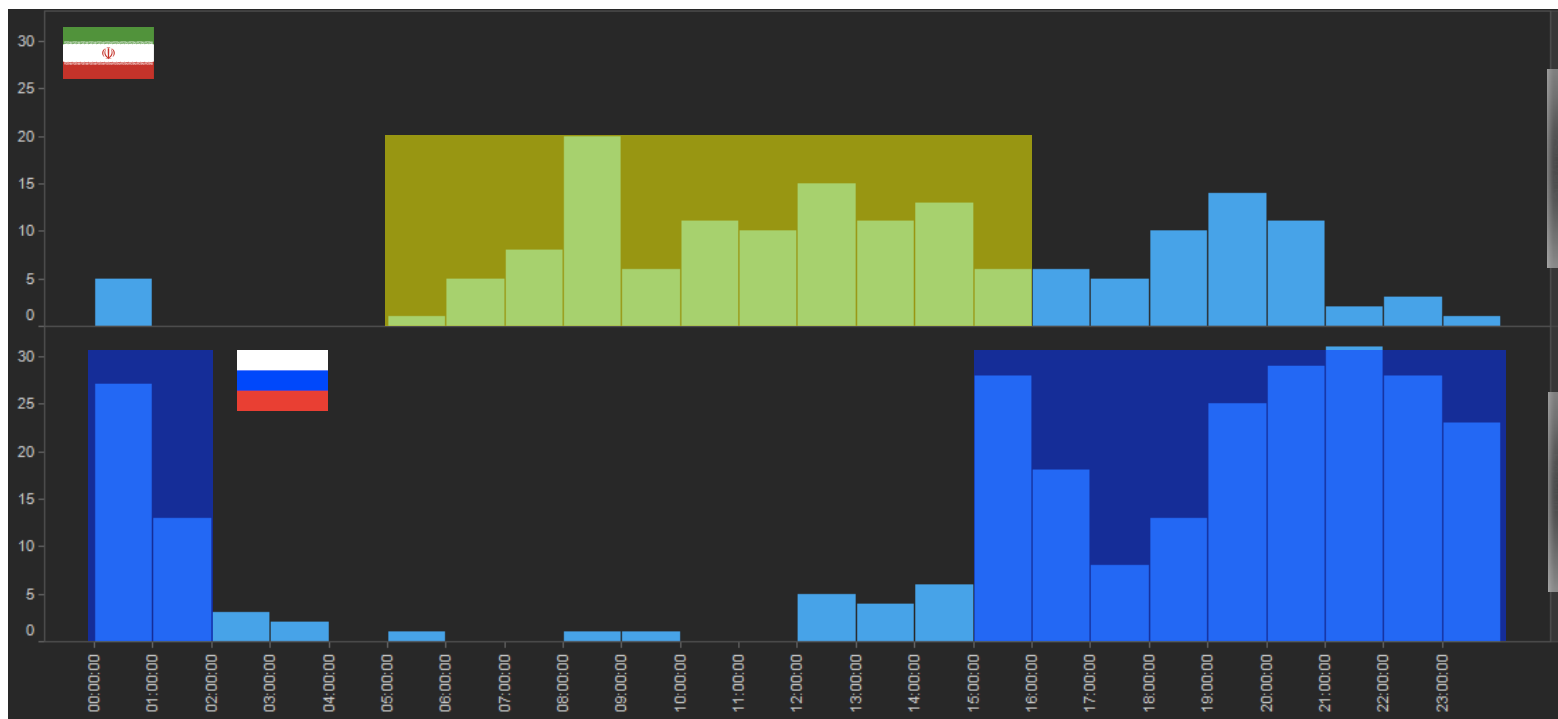
Patch Tuesday Driving Exploit Wednesday



Patch Tuesday Drives Russian and Iranians

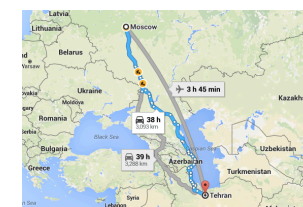


Even When Work Hours Are Different

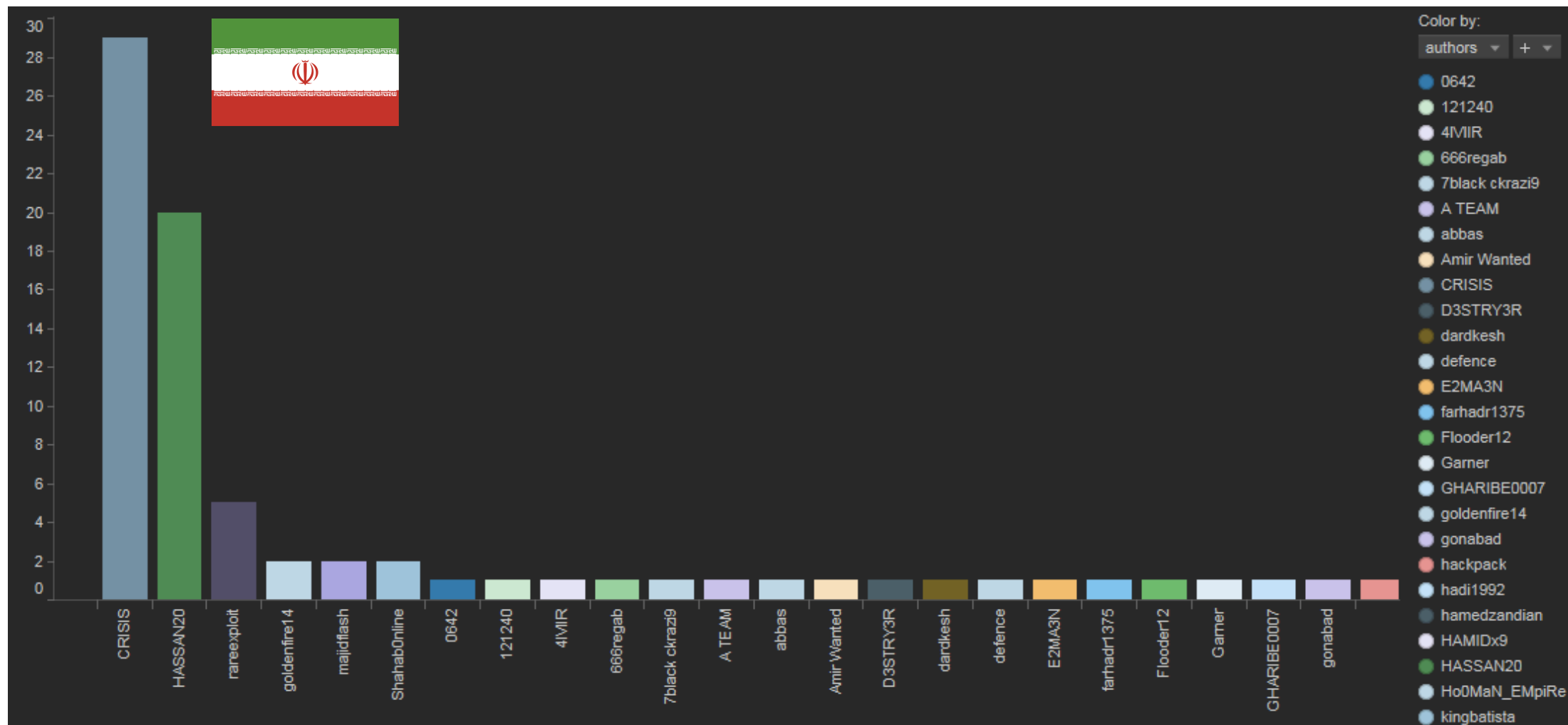


Tehran, Iran is 30 minutes ahead of Moscow, Russia

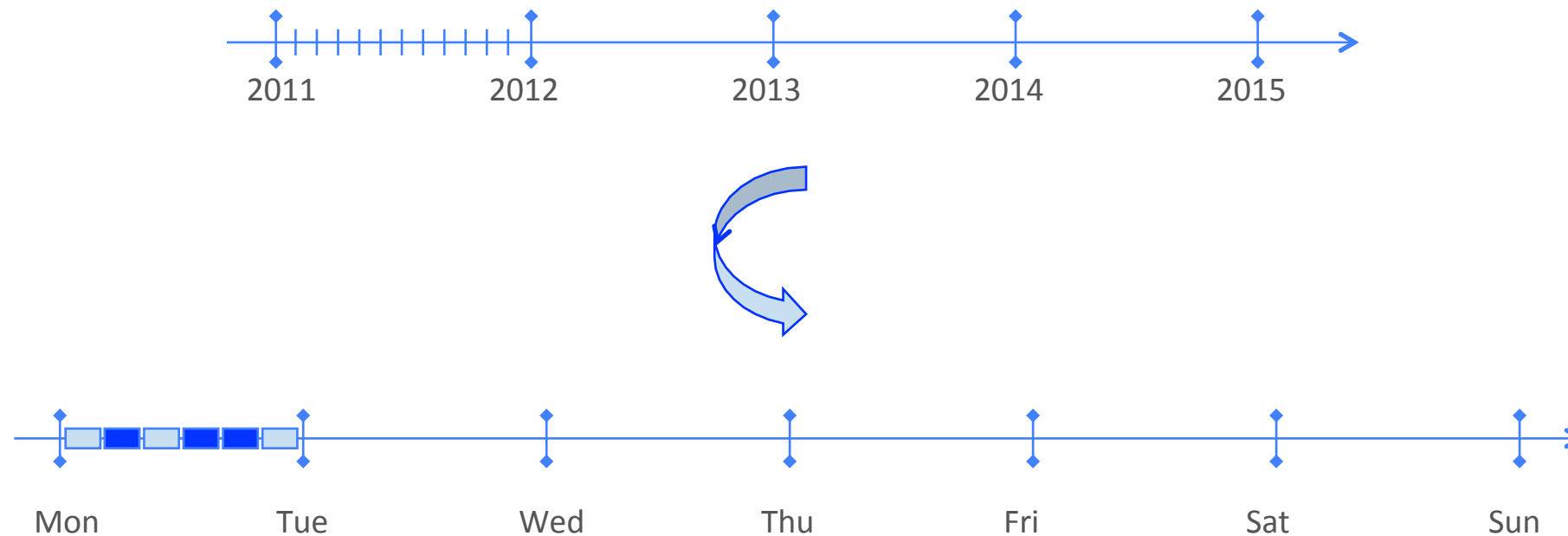
5:54 AM Saturday, in Moscow, Russia is
6:24 AM Saturday, in Tehran, Iran



Two Kings of Vulnerabilities



Clustering Pattern of Life



Understanding Behavior by Math

The *correlation* between two points, a and b , with k dimensions is calculated as:

$$\frac{cov(a, b)}{std(a) \times std(b)}$$

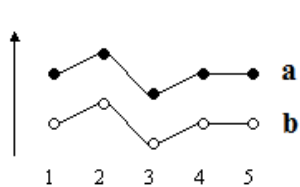
where

$$cov(a, b) = \frac{1}{k} \sum_{j=1}^k (a_j - \bar{a}) \times (b_j - \bar{b})$$

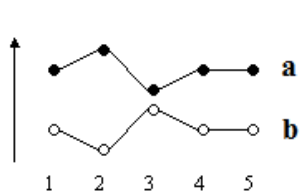
$$std(a) = \sqrt{\frac{1}{k} \sum_{j=1}^k (a_j - \bar{a})^2}$$

$$\bar{a} = \frac{1}{k} \sum_{j=1}^k a_j$$

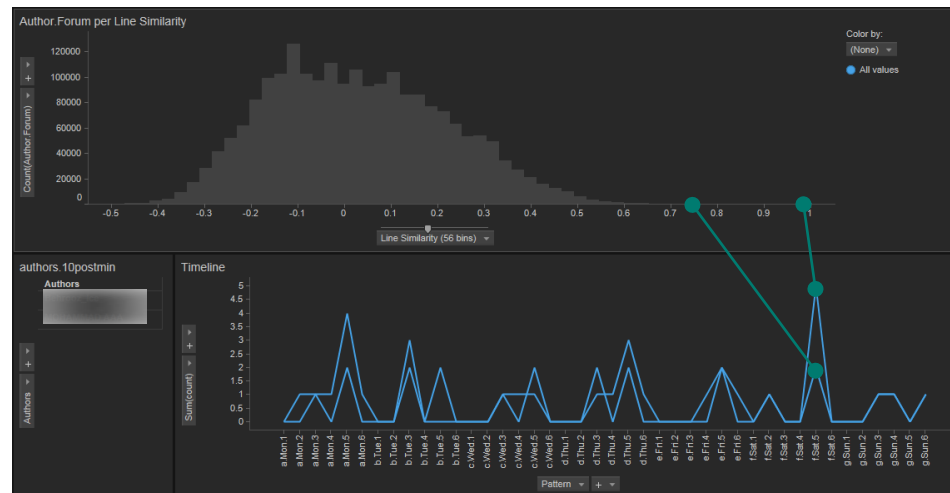
This correlation is called *Pearson Product Momentum Correlation*, simply referred to as *Pearson's correlation* or *Pearson's r* . It ranges from +1 to -1 where +1 is the highest correlation. Complete opposite points have correlation -1.



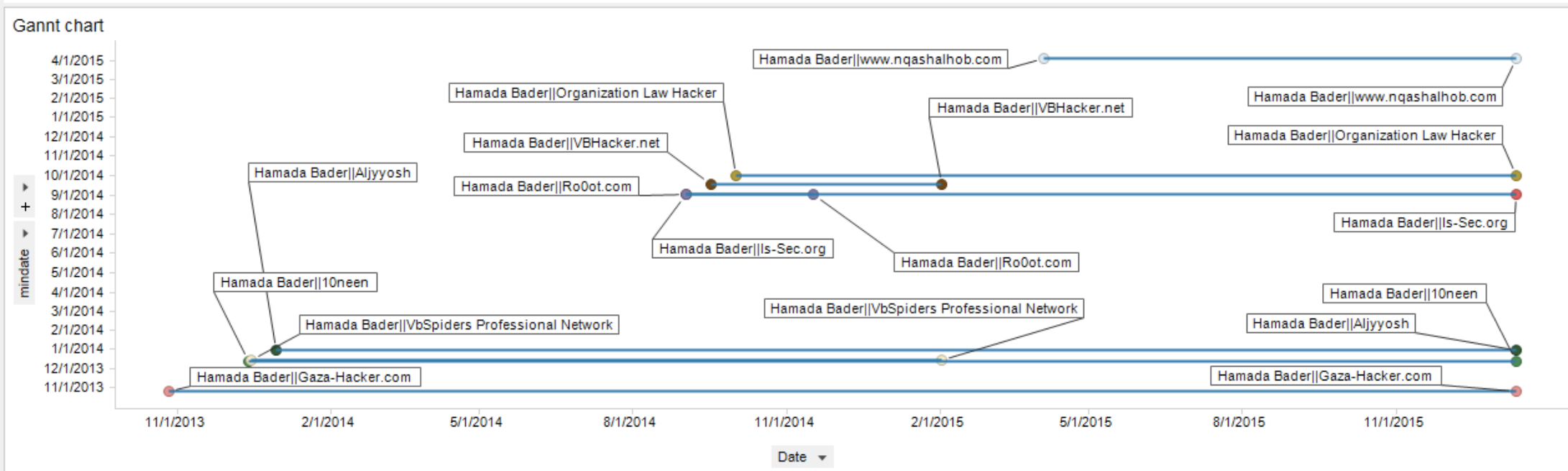
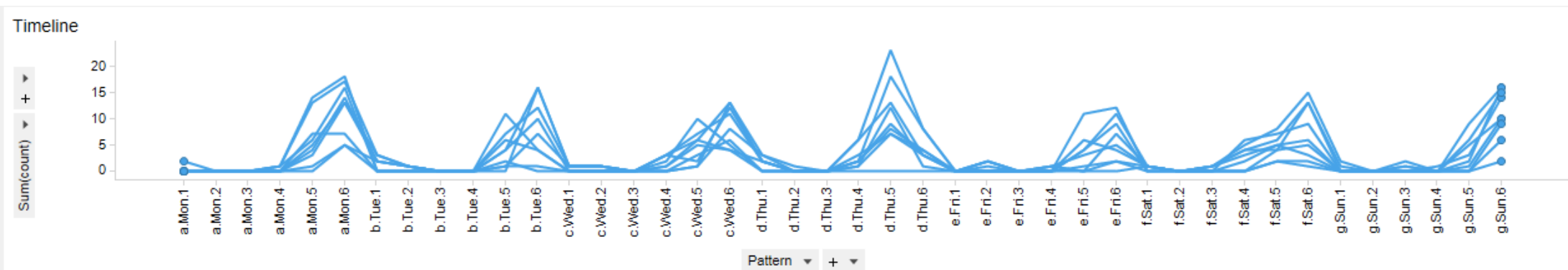
a and b are identical, which means they have maximum correlation.



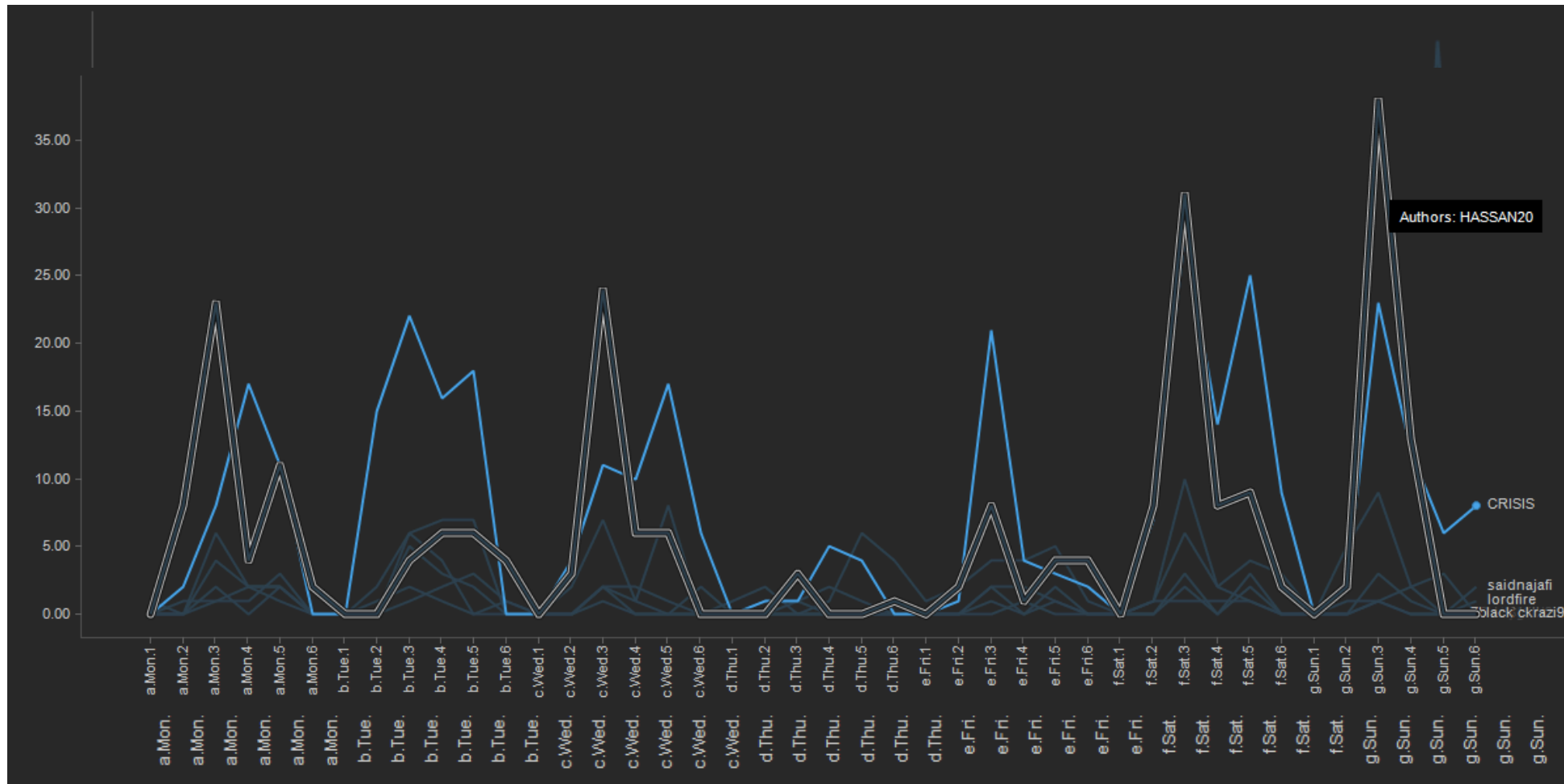
a and b are perfectly mirrored, which means they have the maximum negative correlation.



Sample: Hamada Bader (non malicious, selling IT products)



Identifying Hang Arounds

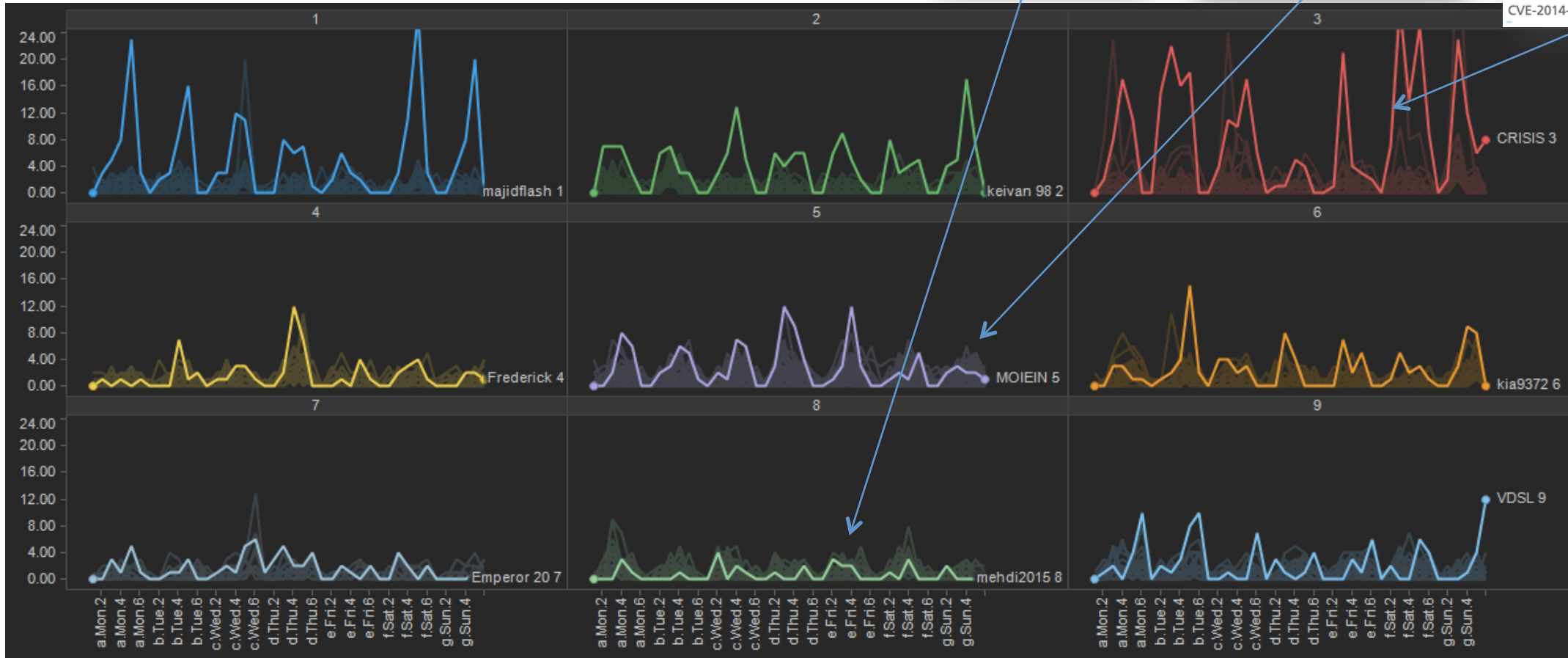


Identifying User Pods

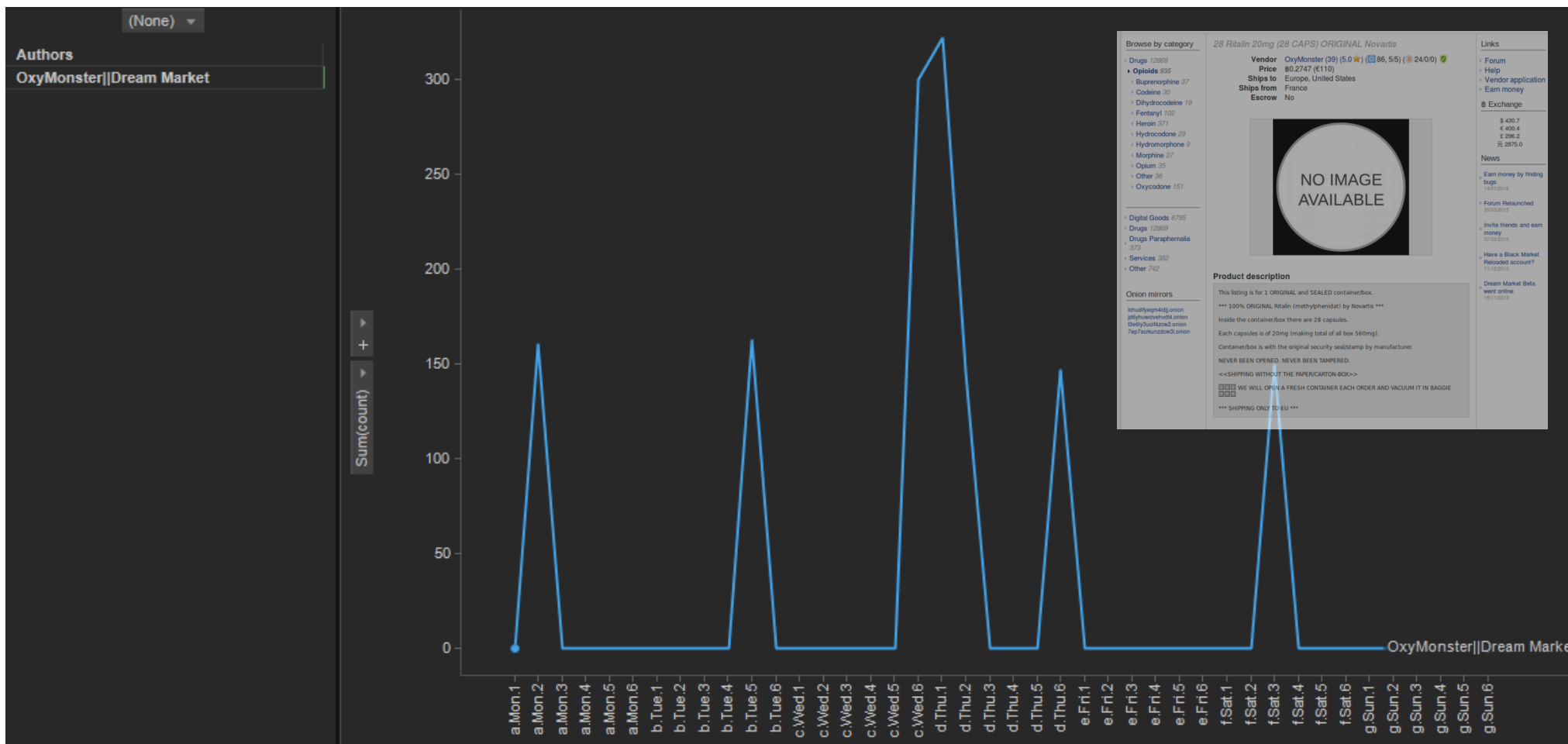
- Exploit Target Category (1)
 - Android Exploit Targets
- Malware (2)
 - AndroRAT
 - DroidJack
- Malware Category (1)
 - Remote Access Trojan ...

- Attack Vector (5)
 - Browser Targeted Cod...
 - Cross site scripting
 - Abuse of Application ...
 - Privilege Escalation
 - Cross-site Request For...

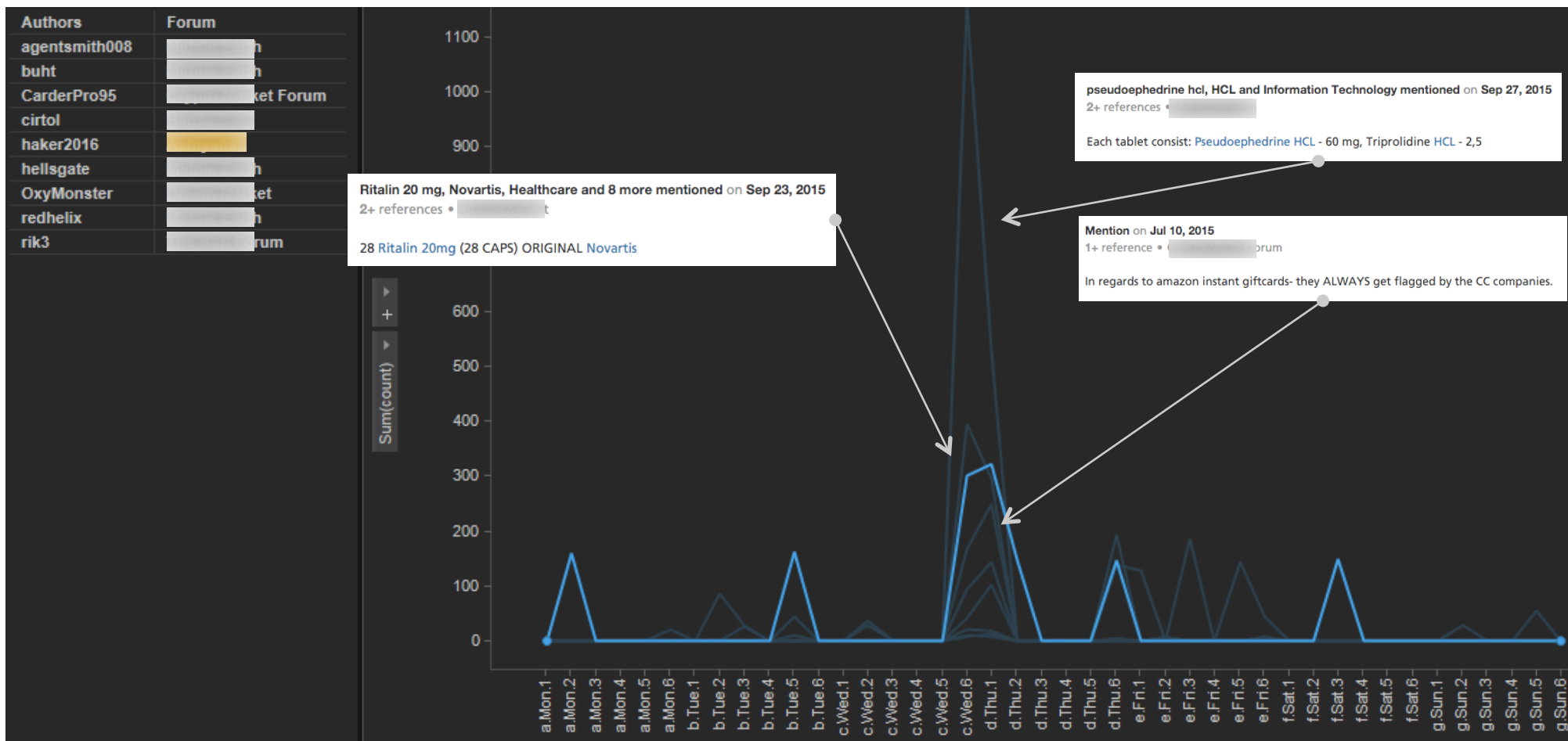
- CVE-2014-0160 (Heart...)
- CVE-2014-6271 (Shells...)
- CVE-2014-3566 (POOD...)
- CVE-2014-4114 (Sand...)
- MS14-058
- CVE-2014-0515
- MS14-056
- MS14-060
- MS14-066
- CVE-2014-4113



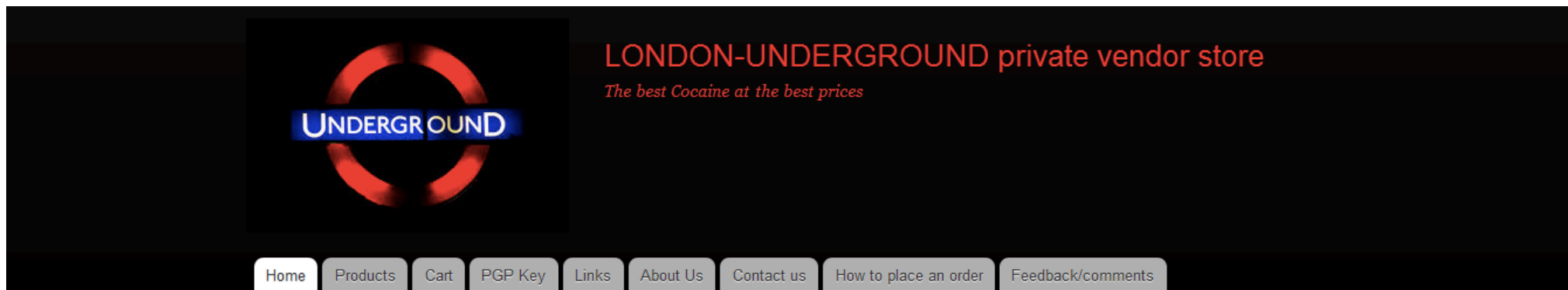
Making the Wednesday Night .Onion Rounds



Making the Wednesday Night .Onion Rounds



Profiling the Store Admin



Blog

[All order status have been updated;-\)](#)

Post date: 1 week 5 days

[Patience is a virtue;-\)](#)

Post date: 2 weeks 3 days

[All emails and orders up to date;-\)](#)

Post date: 3 weeks 7 hours

[Still working through emails](#)

Post date: 3 weeks 4 days

[QUICK UPDATE](#)

Post date: 4 weeks 13 hours

Navigation

L-U: Welcome to our private store

We are LONDON-UNDERGROUND, and we are proud to welcome you to our private vendor store.

We are here to cater to all your Cocaine needs.

We provide a fast, simple, safe way for customers across Europe to purchase high quality Cocaine using Bitcoin as a payment method.

We have 3 different product lines, so whether you are looking for an absolute bargain, or the absolute best Cocaine you can find, we will have a product for you.

Our 3 Cocaine product lines are as follows:

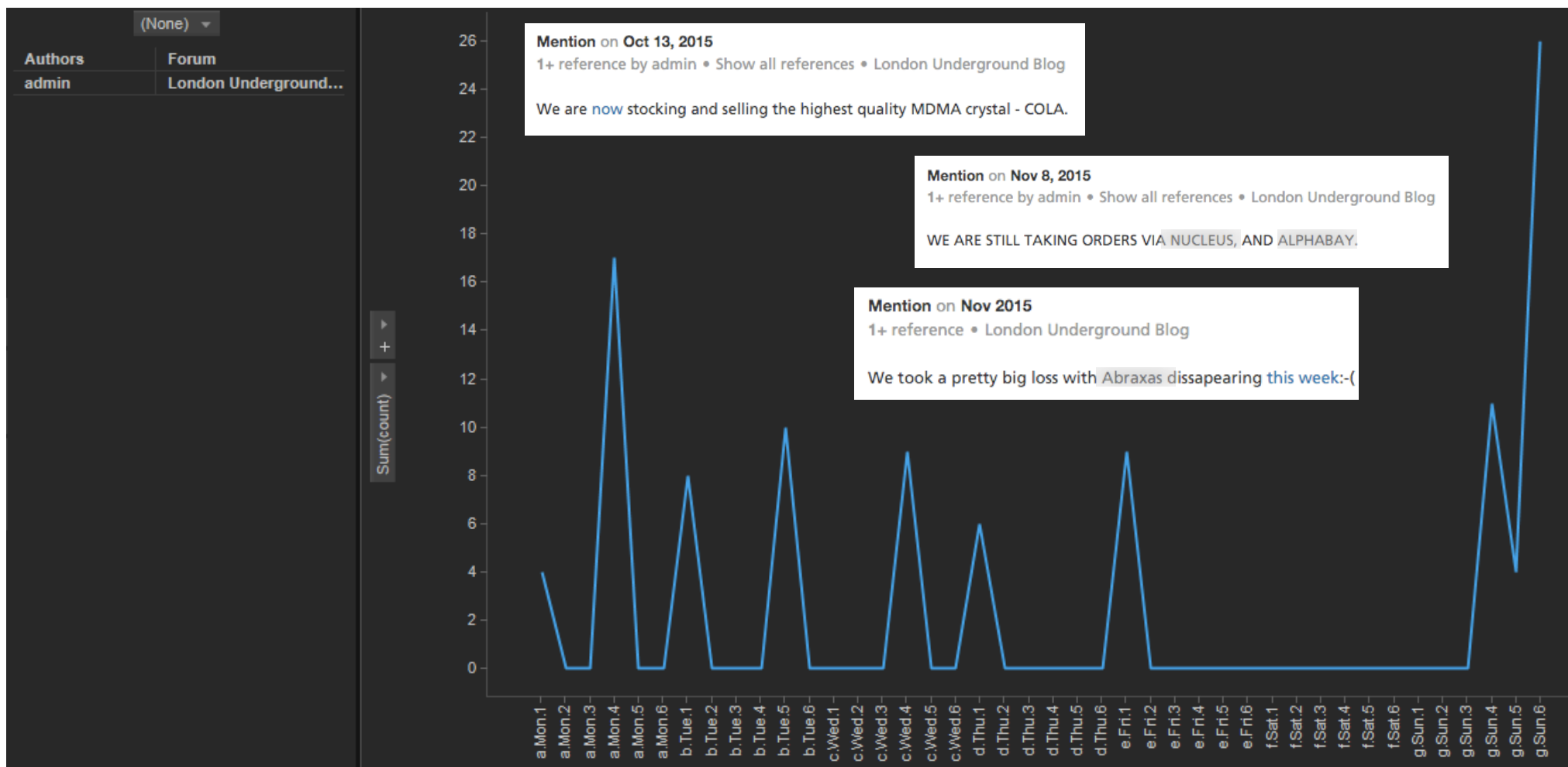
-Pure Columbiana Fishscale Cocaine (90%) £70 a gram. This is a completely untouched product.

-Columbiana MK1 (50%) £35 a gram

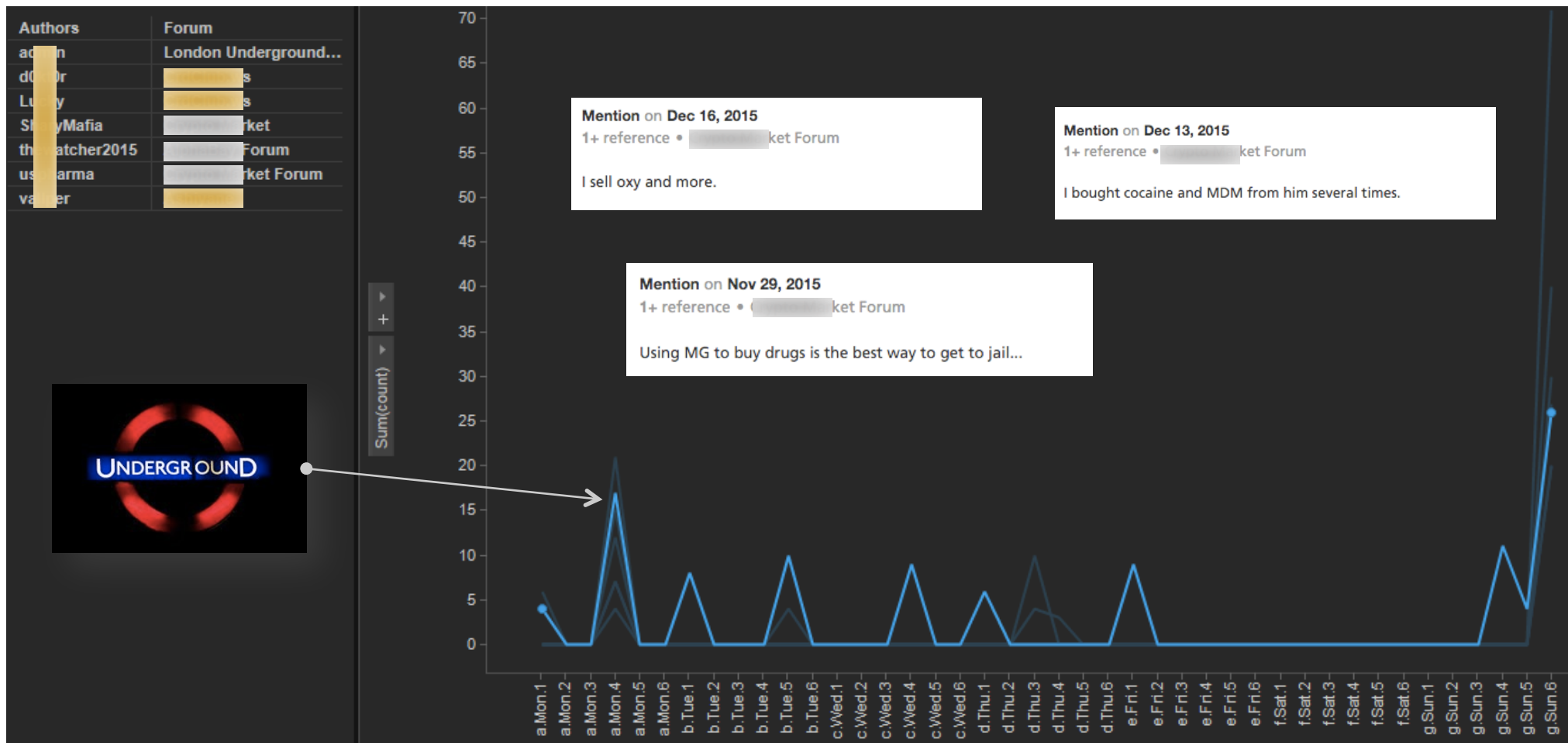
-Columbiana MK2 (30%) £20 a gram

The MK1/MK2 product lines are a mix of Columbiana Fishscale, and high quality Benzocaine, for a

Profiling the Store Admin



Profiling the Store Admin



Summary and What's Next?

- Pattern of life on metadata supports attribution
- Lead generation [duh!] requiring secondary sourcing

- Build hard analytic: “find handles like this”
- Cross validation on secondary data sources

- *Christopher Ahlberg, Co-Founder & CEO*
- *Recorded Future*
- *c@recordedfuture.com @cahlberg*