CVEs at CrimeBB

CrimeBB forums

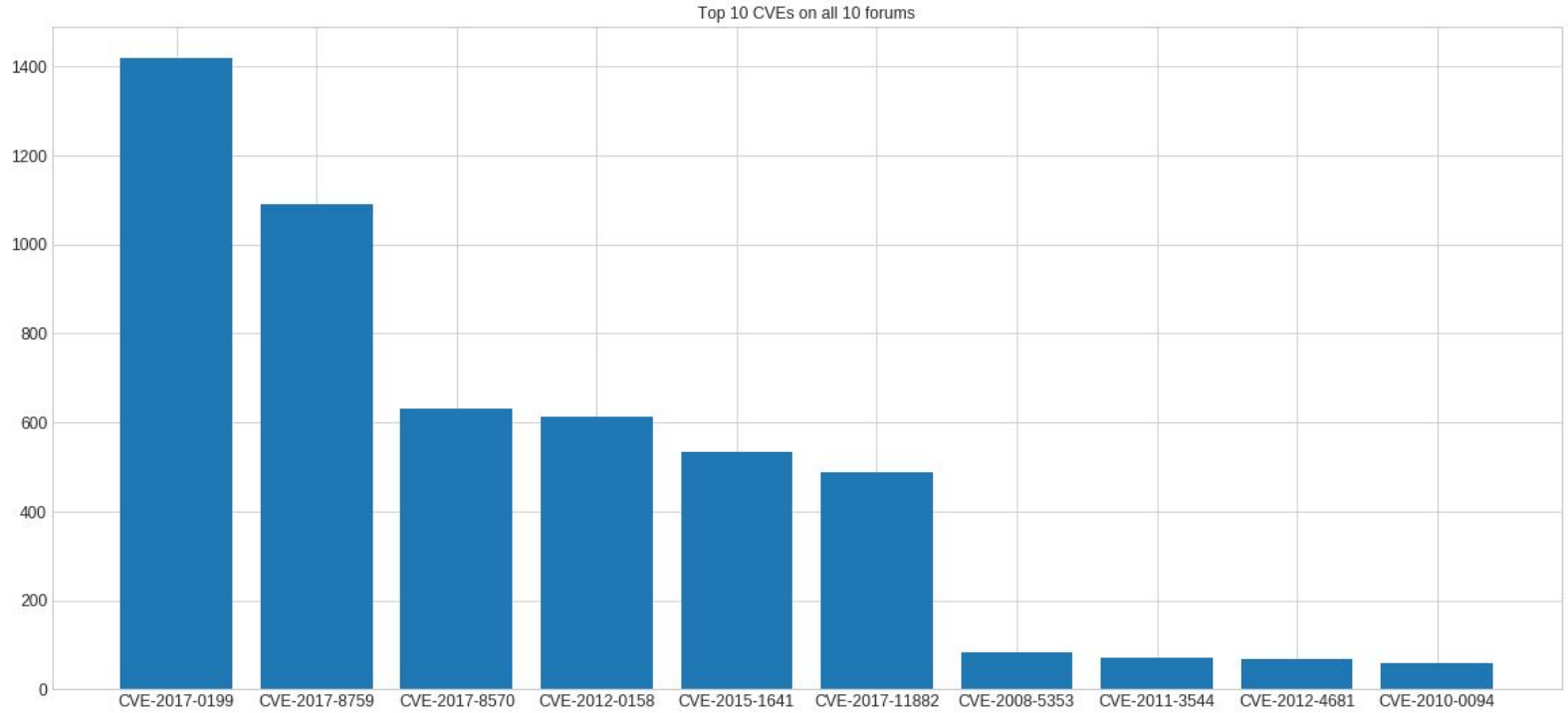
Name	Number of posts	Number of threads	Observations
Hackforums	40.218.175	3.858.661	
MPGH	8.907.938	1.479.054	Games cheats
Antichat	2.449.221	242.408	
Raidforums	214.239	33.322	
Offensive Community	58.779	18.436	
Safe Sky Hacks	26.842	12.892	
Kernel Mode	25.024	3.144	Linux kernel
Garage4Hackers	7697	1039	This forum is frozen
Streesserforum	7069	708	
Greysec	6969	1039	

General statistics

1. Amount of different CVEs = 696
2. Number of posts = 1864
3. Number of authors = 1796

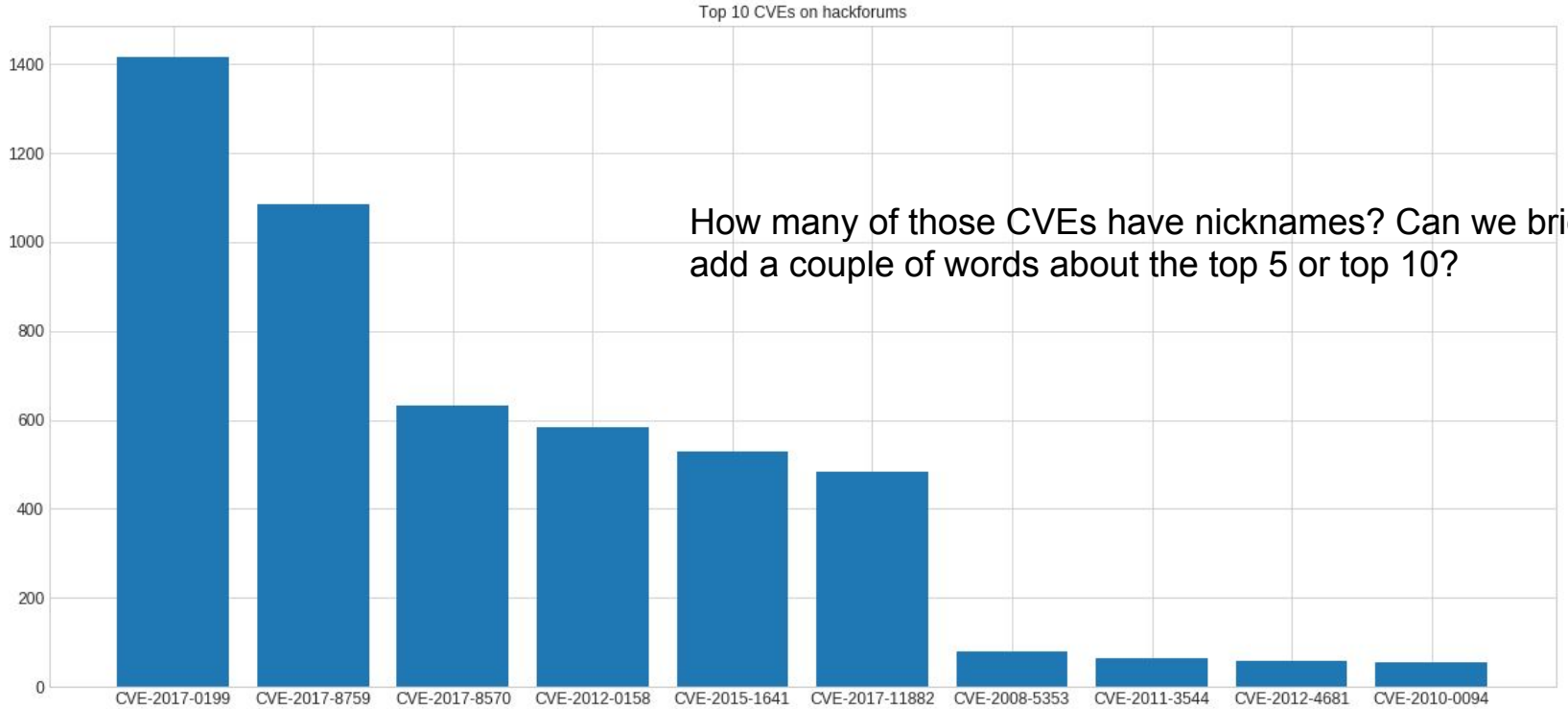
CVEs popularities

Mentions of CVE in posts across all forums



CVEs popularities on hackforums

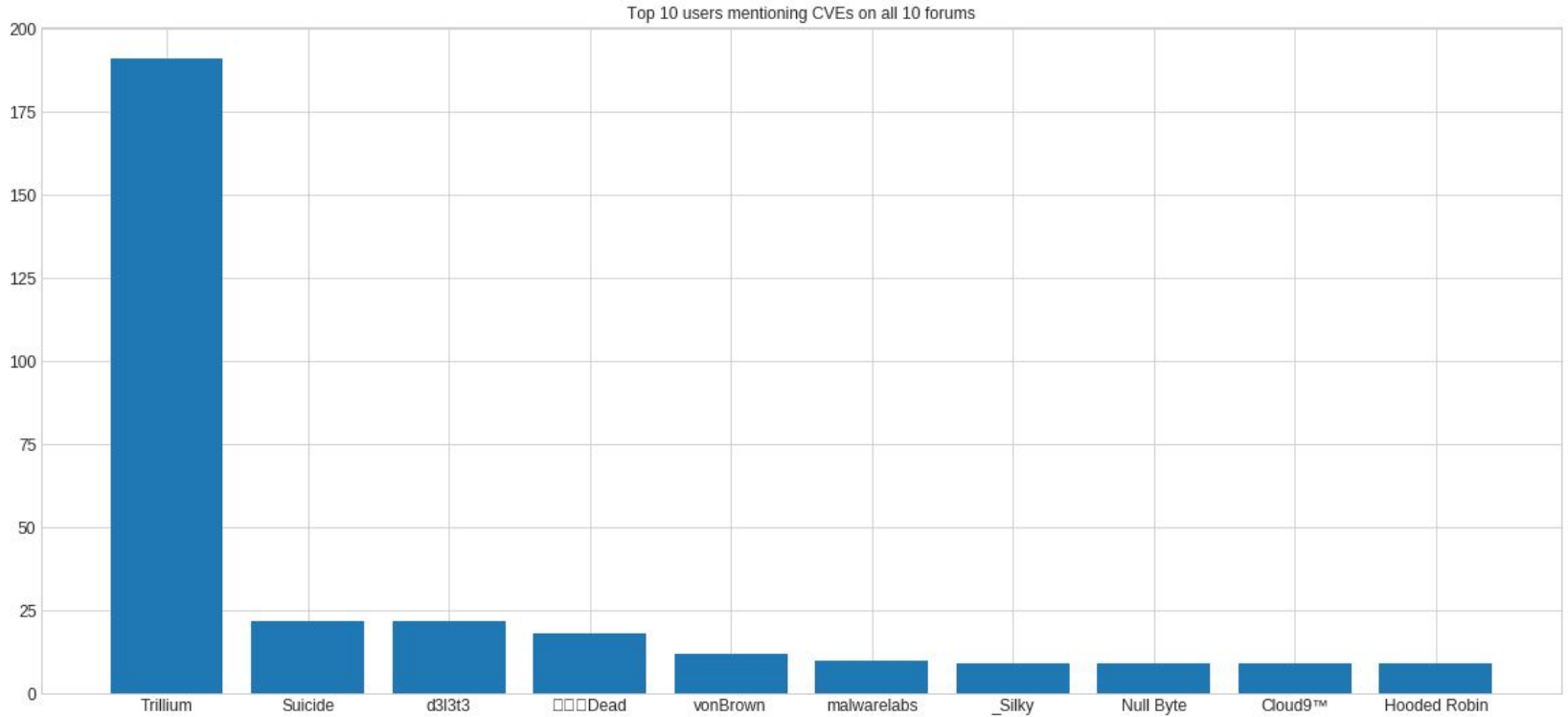
Mentions of CVE in posts on hackforums



How many of those CVEs have nicknames? Can we briefly add a couple of words about the top 5 or top 10?

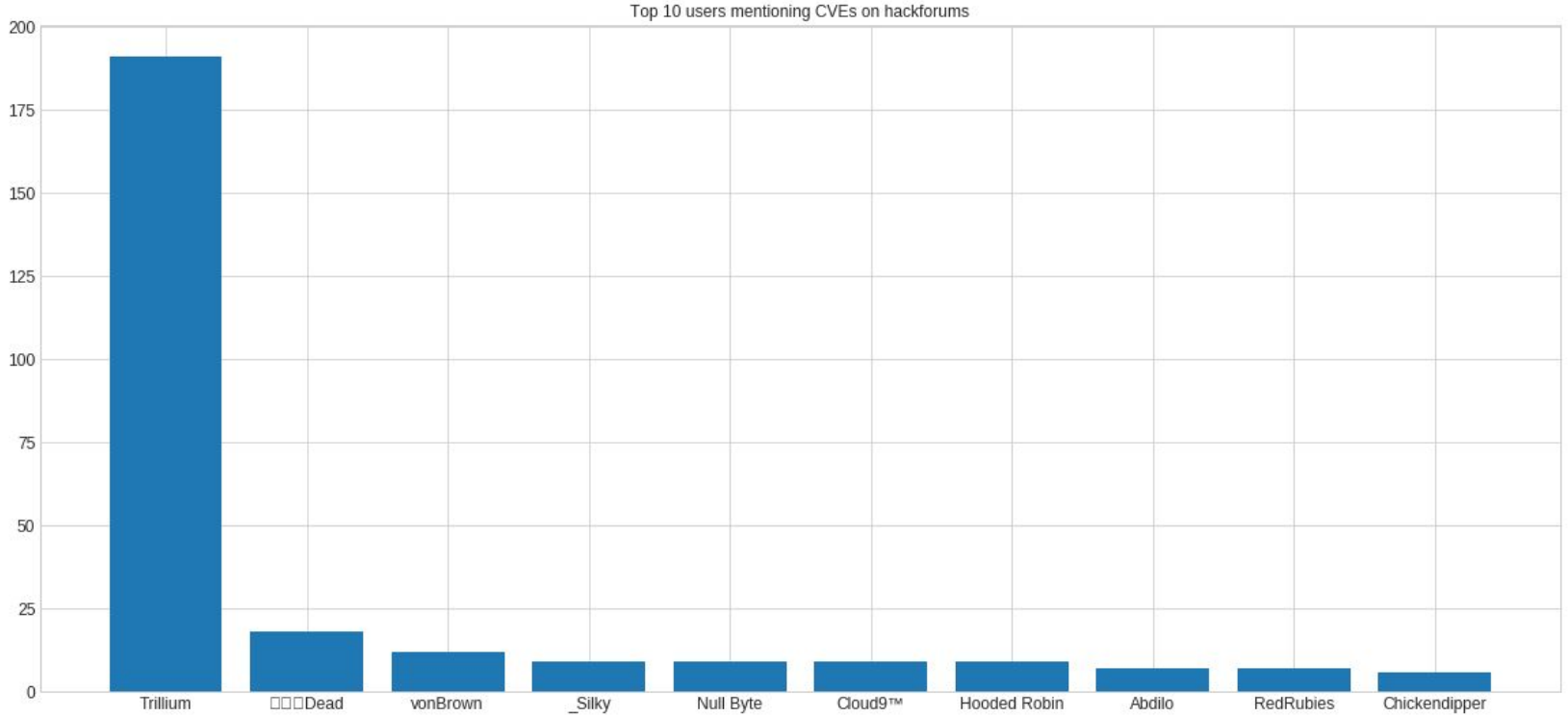
Users activity

Users mentions of CVE on all forums



Users activity on hackforums

Users mentions of CVE on hackforums



Word clouds

Word clouds for the posts related to CVEs

Word clouds

Trillium is always spamming this kind of post. He is always using the biggests words of your word cloud.

CITING[https://hackforums.net/showthread.php?pid=56682925#pid56682925]***CITING***
Hello dragonfly2014, thank you very much for your interest in my product but you should know that my product is only for lega
l educational purposes! I just sent you a PM with all details! ***IMG***[https://hackforums.net/images/smilies/blackhat.gif]*
IMG*

I am currently online and avaiable for Teamviewer Support Requests or Sell Requests and all PMs and Hardware ID Update Reques
ts are handled and I am currently working on the new big update (v6.5.3) which is in development in next coming days it will
get released. It will include much new private exploits and much other new security things.

All exploits are FUD and running great !

Best Regards ***IMG***[https://hackforums.net/images/smilies/blackhat.gif]***IMG***

Videos:

Trillium Security MultiSploit Tool v6.5 - Security Office CVE-2017-8759 Exploit Generator

IFRAME[//www.youtube.com/embed/Q8t4QybSo5s]***IFRAME***

Trillium Security MultiSploit Tool v6 - Silent Doc Exploit CVE-2017-0199 + IE-Exploit
LINKhttps://www.youtube.com/watch?v=6WuRCo-52z4&feature=youtu.be[https://www.youtube.com/watch?v=6WuRCo-52z4&featur
e=youtu.be]***LINK***

Trillium Security MultiSploit Tool v6 - Silent HTA Exploit
LINKhttps://www.youtube.com/watch?v=-uwUIrdrOXk&feature=youtu.be[https://www.youtube.com/watch?v=-uwUIrdrOXk&featur
e=youtu.be]***LINK***

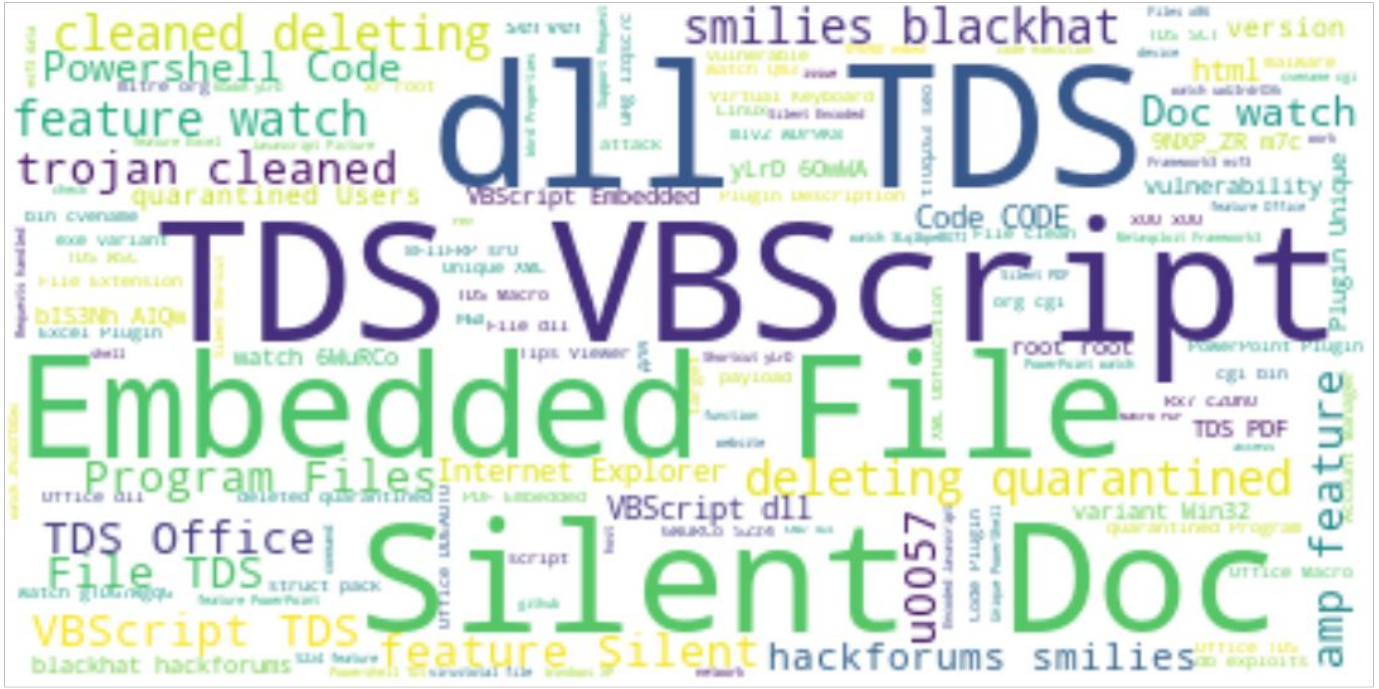
Trillium Security MultiSploit Tool v6 - Silent Doc Exploit CVE-2015-1641 + CVE-2017-0199
LINKhttps://www.youtube.com/watch?v=3LqlbpeBG7I&feature=youtu.be[https://www.youtube.com/watch?v=3LqlbpeBG7I&featur
e=youtu.be]***LINK***

Trillium Security MultiSploit Tool v6 - Silent Doc Exploit CVE-2015-1641
LINKhttps://www.youtube.com/watch?v=gTDG7WgqG-k&feature=youtu.be[https://www.youtube.com/watch?v=gTDG7WgqG-k&featur
e=youtu.be]***LINK***

Word clouds

Word clouds for the posts related to CVEs, excluding this words:

"MultSploit", "Trillium", "Tool", "generator", "Security", "Exploit", "youtube", "youtu", "v6", “CVE”



Word clouds

Word cloud for posts in which the word "exploit" appears

What are users discussing about?

Labeling of posts based on topic.

For each post we add manual labels

- ❏ improve the understanding of lifecycle of vulnerabilities PoC weaponization=> Full weaponization => Exploitation <=> market
- ❏ Check black markets

Unnamed: 0		CVE	IdPost	Time	Likes	Content
0	0	CVE-2011-1519	53287285	2016-11-30 09:21:00-02:00	nan	hello everybody\ni need some kind of experience return concerning a pentest on IBM domino server...
1	1	CVE-2016-6313	4051876	2017-02-22 03:34:00-03:00	0.00	***CITING***[goto/post?id=4013958#post-4013958]***CITING***Наверное по этому.\nПодпись\nСтандарт...
2	2	CVE-2012-1823	3130917	2012-05-05 12:40:00-03:00	0.00	На форумах Reddit опубликовали копию закрытого обсуждения критической уязвимости CVE-2012-1823 в...
3	3	CVE-2012-1823	3132319	2012-05-06 14:46:00-03:00	0.00	***CITING***[about:blank]***CITING***http://www.php-security.net/archives/9-New-PHP-CGI-exploit-...
4	4	CVE-2012-1823	4025404	2016-12-17 00:00:00-02:00	0.00	Используется следующее:\n\nCode:\n80/tcp open http Apache httpd 2.2.22 ((Ubuntu))\n\nPHP/5.3...
5	5	CVE-2012-1823	38225272	2014-02-09 10:24:00-02:00	nan	Today I will share something new with you and give you one more method for your bag of tricks wh...
6	6	CVE-2012-1823	23261704	2012-06-06 03:41:00-03:00	nan	Hi everyone, I have a site vulnerable to this exploit:\n***LINK***http://web.nvd.nist.gov/view/v...
7	7	CVE-2012-1823	30315082	2013-02-04 03:41:00-02:00	nan	I am tring to exploit CVE-2012-1823 using metasploit exploit exploit/multi/http/php_cgi_arg_inje...
8	8	CVE-2012-1823	31472896	2013-03-25 00:35:00-03:00	nan	***LINK***http://www.php-security.net/archives/9-N...ploit.html[http://www.php-security.net/arch...
9	9	CVE-2012-1823	23822	2014-09-08 23:13:00-03:00	nan	I noticed @malekal_morte & MMD guys mentioning this family recently, didn't find an existing thr...
10	10	CVE-2006-4842	569917	2008-01-21 15:02:00-02:00	0.00	URL производителя: www.sun.com\n\nSolaris 10-8\nУязвимость позволяет удаленному злоумышленнику п...
11	11	CVE-2010-3881	3939111	2016-01-11 19:18:00-02:00	0.00	Йо)\nВ общем в очередной раз когда у меня вытекли глаза от CVEDetails и его интерфейса родилась ...
12	12	CVE-2013-4854	3552924	2013-07-28 20:25:00-03:00	0.00	Опасная уязвимость в DNS-сервере BIND. В состав BIND добавлен модуль для блокирования DDoS-атак\...
13	13	CVE-2011-0920	53318541	2016-12-03 07:42:00-02:00	nan	6x66 thanks for reply but i tested all what i found for geoserver i testes xxe exploit in server...
14	14	CVE-2013-1311	54459956	2017-03-29 01:54:00-03:00	nan	Do some brief research on metasploit framework, beef xss, and CVE-2013-1311. Then, presuming you...

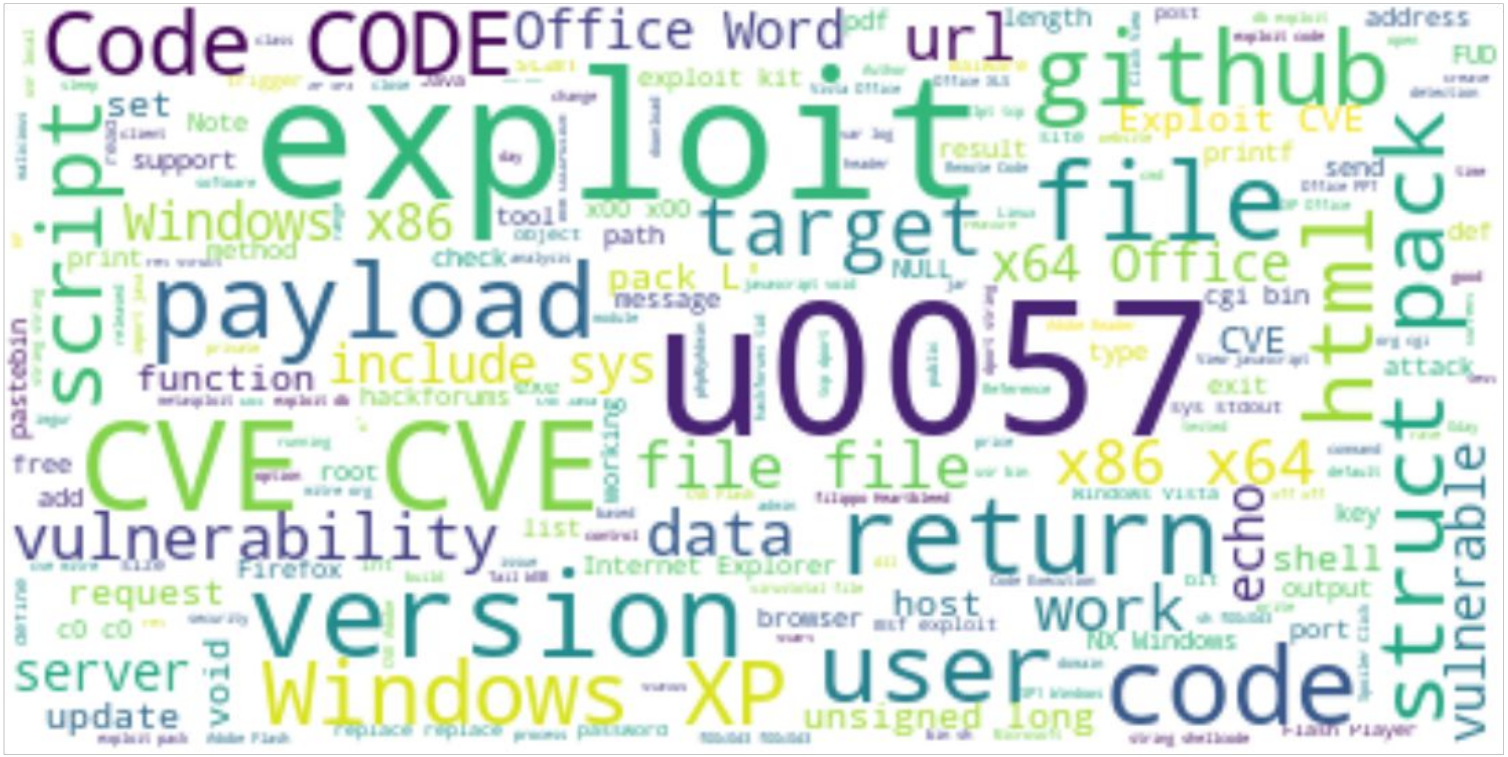
Our labels and results: 'weaponization': 408, 'others': 580, 'exploitation': 319, 'PoC': 306, 'market': 124, 'russian': 210

Early signals and their strength

Two dimensions: time and strength

- **Time**: Signals before threat feeds (early signals, but how strong are they?)
  - After someone has bought and used it
  - It will appear in threat feed
  - Analyzed by security expert
- **Strength**: Do users have steady accounts?
  - Analyze reputation?
  - Forums have reputation?
  - Spamming sellers include bunch of keywords everytime there is exploit
  - When seller includes = is it valid?
  - FUD = fully undetectable exploit kits (obfuscation is sold together with packets, most of the times they already claim it is not a 0-day)

Word clouds for posts labeled as "weaponization"



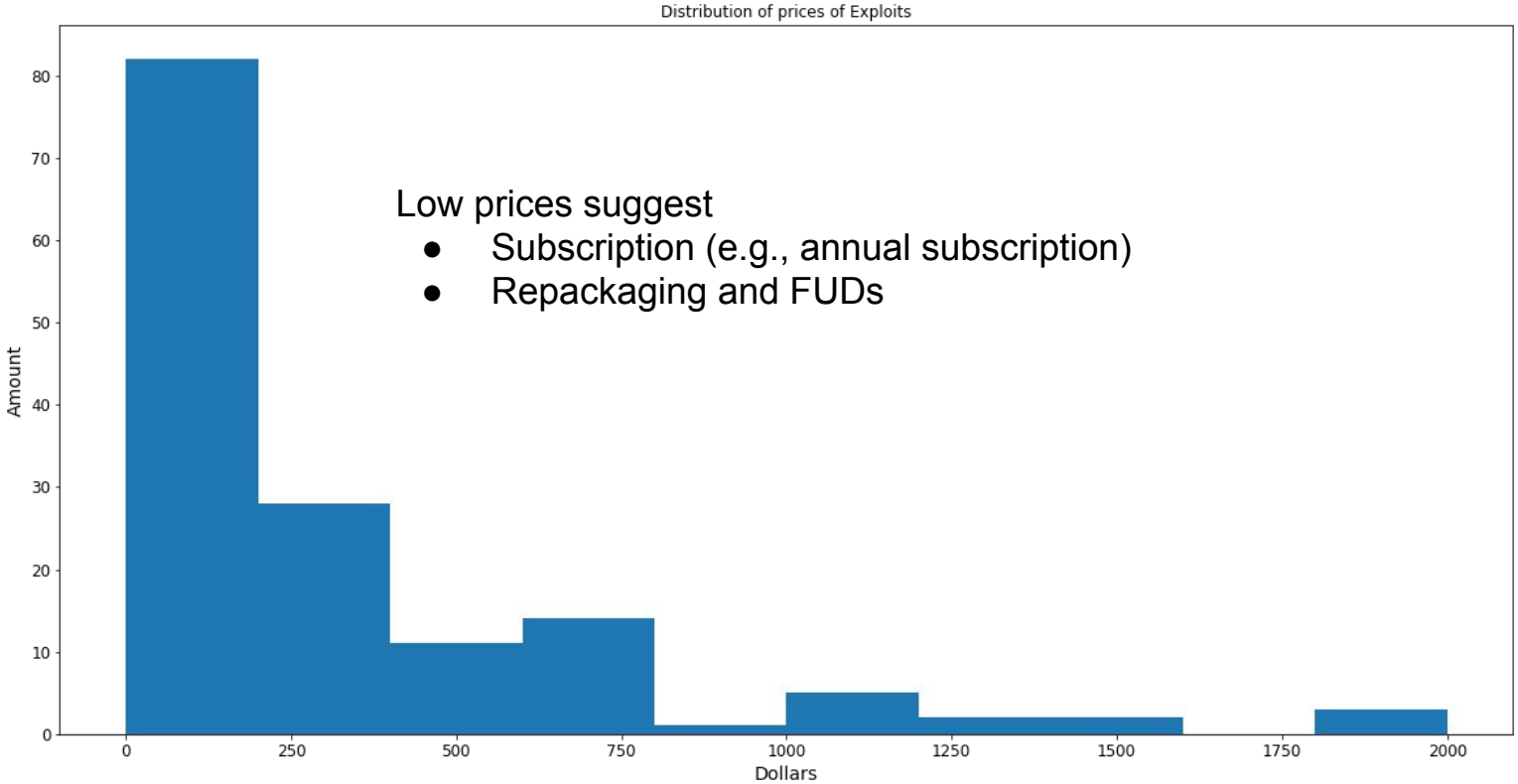
Word clouds for posts labeled as "exploitation"

Word clouds for posts labeled as "PoC"

Word clouds for posts labeled as "PoC" (but no Trillium)

Word clouds for posts labeled as "market"

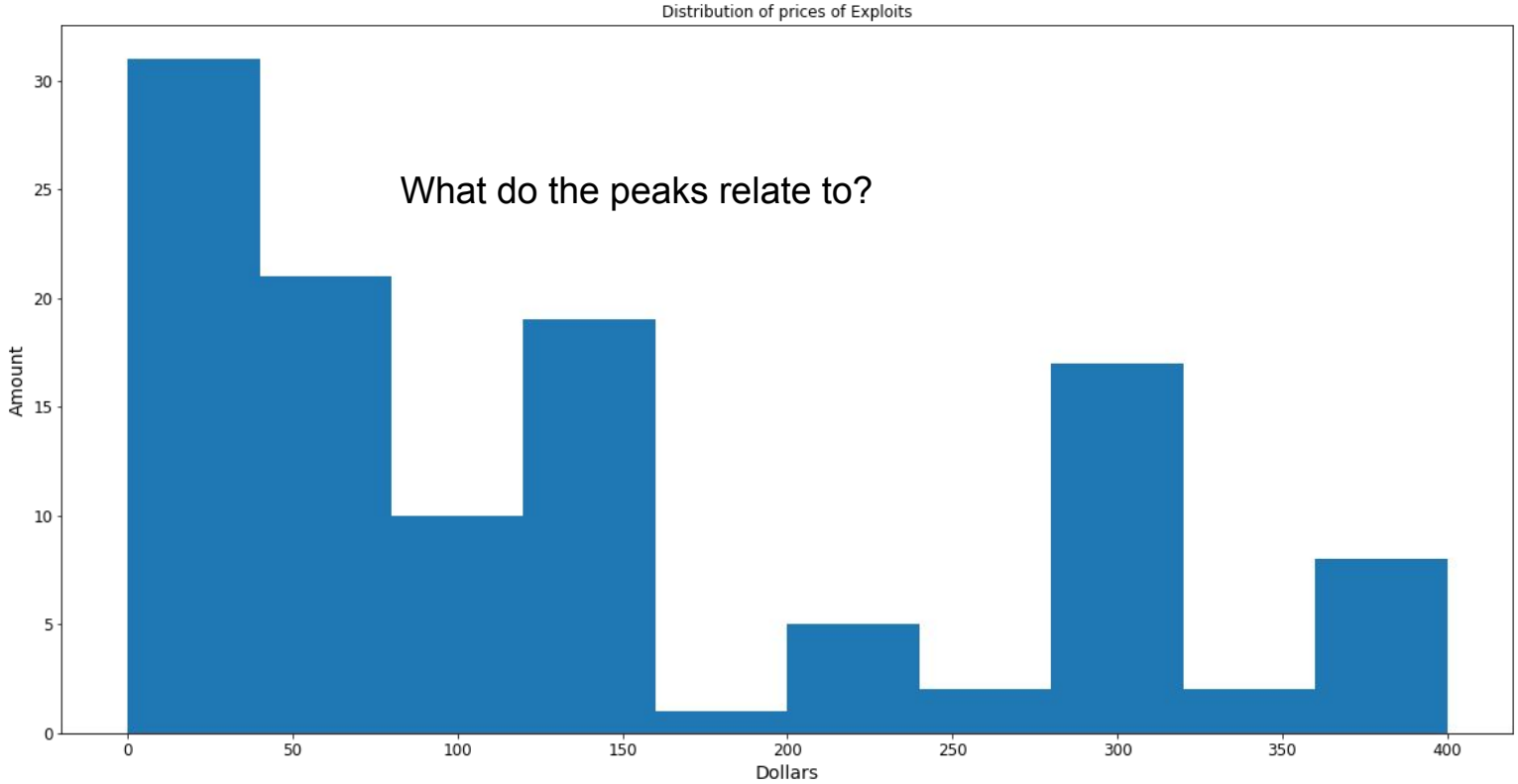
Prices of Exploits



Low prices suggest

- Subscription (e.g., annual subscription)
- Repackaging and FUDs

Prices of Exploits - prices below 400$

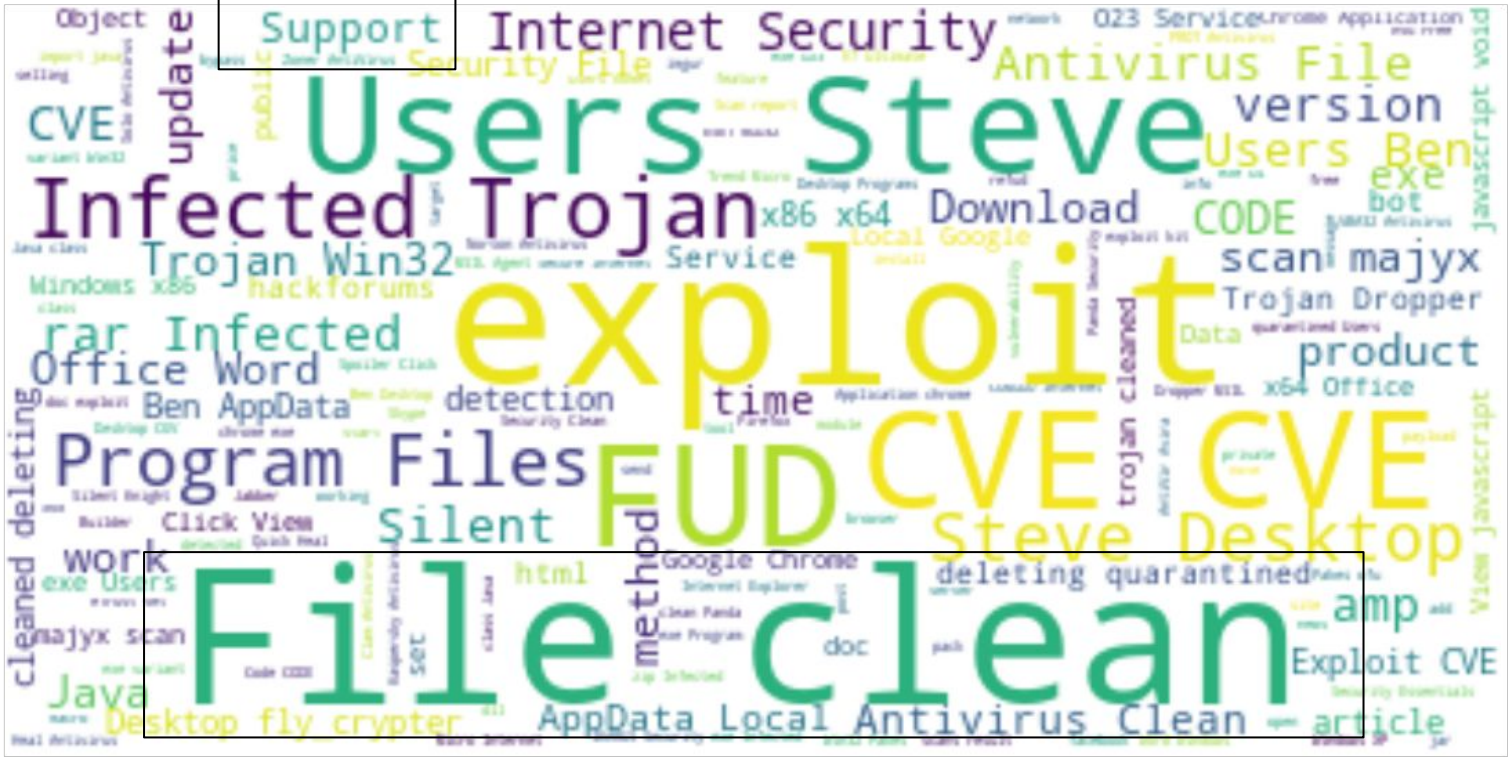


Word clouds for “FUD”(Fully UnDetectable) occurrence = 264 Posts

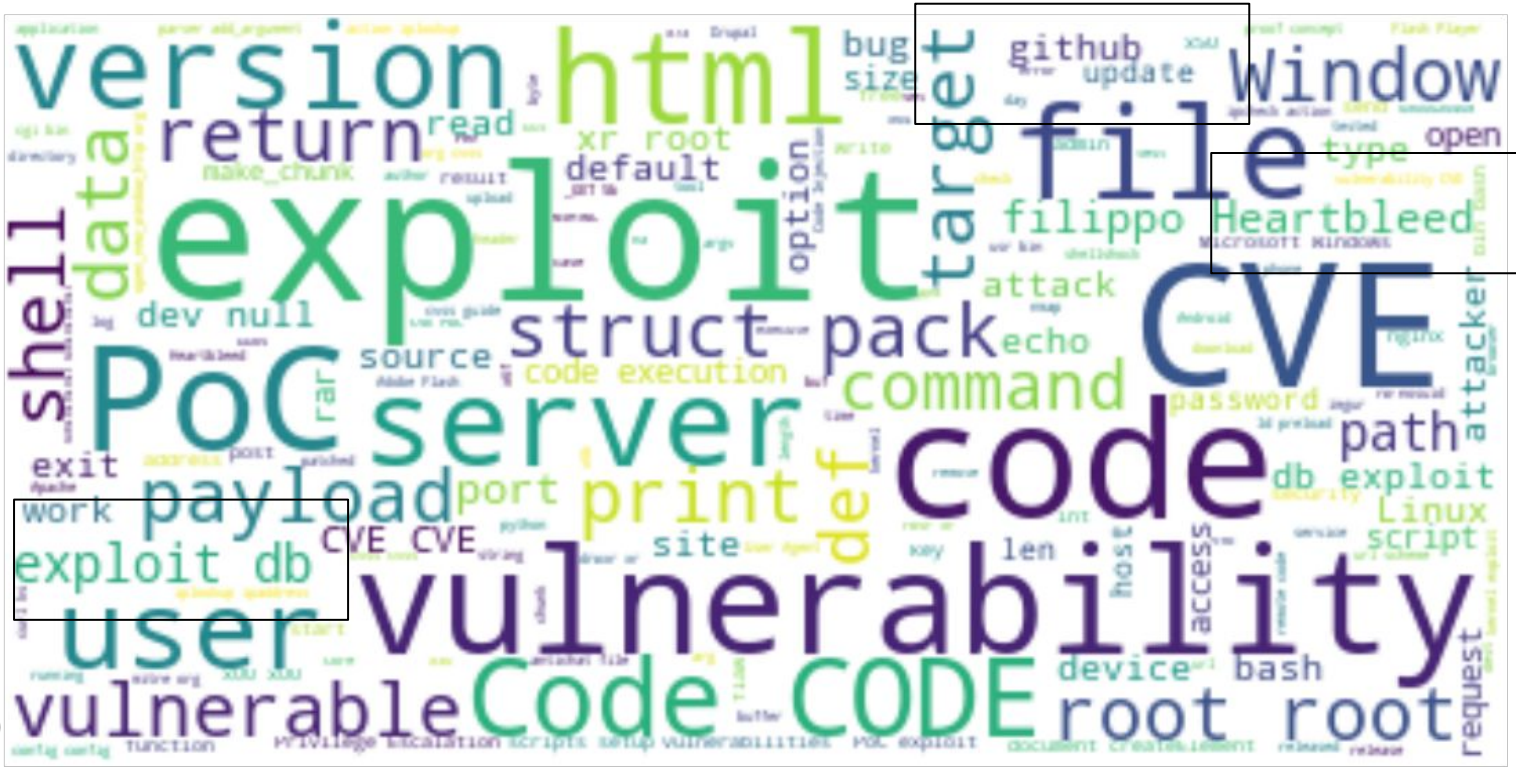
Word “FUD” occurrence (excluding Trillium) = 103 Posts

Who is Steve? :)

Clean = undetectable (double check!)



Word “PoC” occurrence = 110 Posts



Code
CODE
(remove
caption
before
running
word cloud)

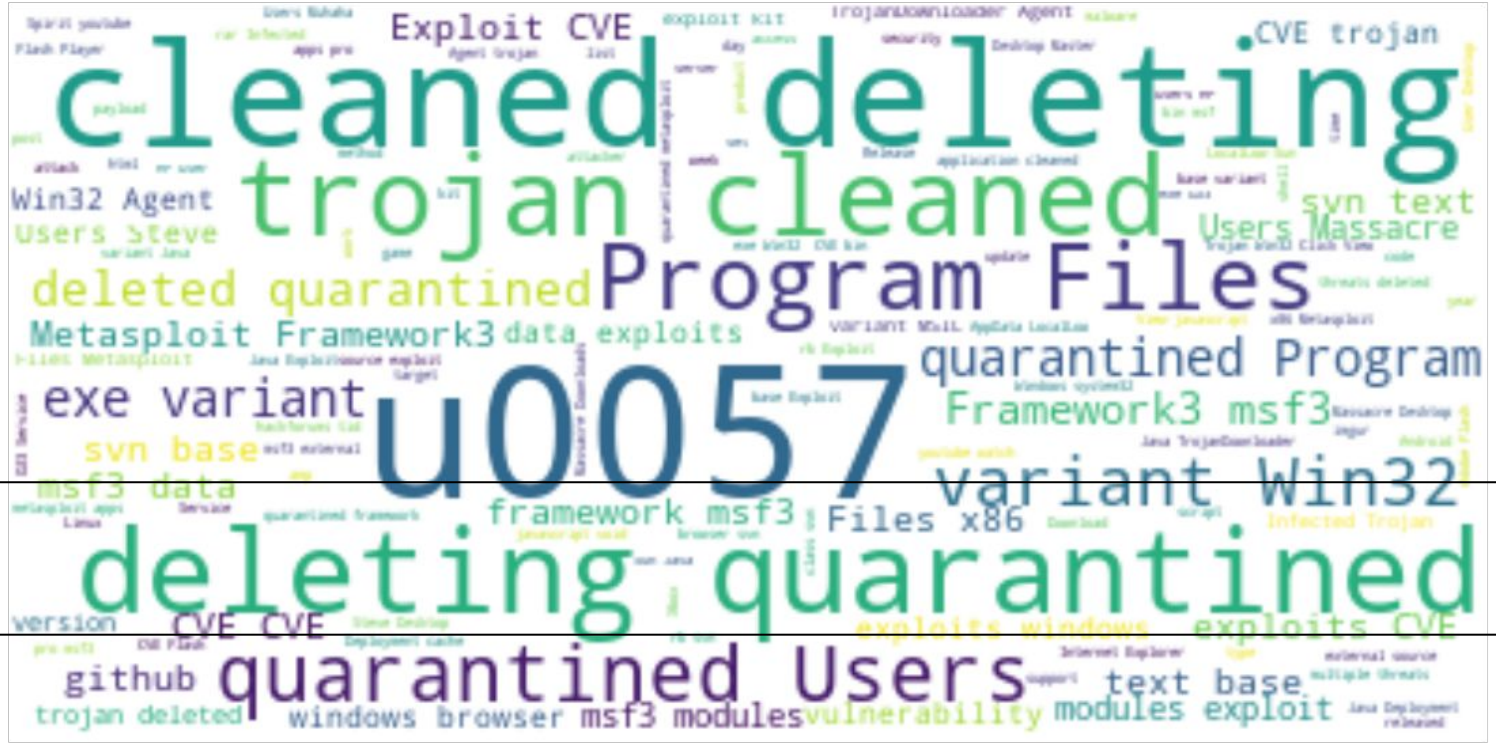
Word “0day” occurrence (excluding Trillium) = 86 Posts

Improve Regex? That will be great 0day Today is our reference website Distinguish the website from real 0days's

Word “Kit” occurrence = 141 Posts

They usually sell exploit kits.

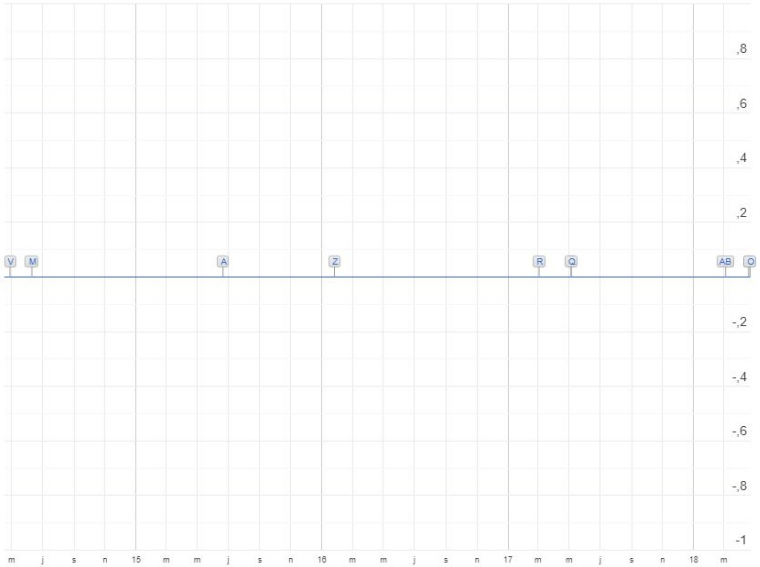
Exploit kits (look for other REGEXs)



What is this?

HeartBleed, timeline

https://docs.google.com/spreadsheets/d/1bRonl0OZyPnqkwvUZ-_KDpa8Vjl6tFM5a_UbaPWoSjs/edit?usp=sharing



Following up work

Cross-relate CrimeBB and NVD

- ❏ If you cross-relate CrimeBB and NVD, do you get useful information?
- ❏ For instance, what is the CVSS scores of the CVEs mentioned in CrimeBB?
- ❏ When were they created?
- ❏ What is the time difference between when they were created and when they are referred to in CrimeBB?

Cross-relate CrimeBB and SIEMENS blob

- ❏ Cross-relate CrimeBB events and CVEs that appear in SIEMENS blob of events (Ashton and Zubair)
- ❏ Repeat analysis above
- ❏ Predictive/classification analysis following Ashton pipeline (share dataset with Ashton)

How to recognize a scam?

symptoms
illustrative example with 0day.today

===> position paper/white paper
===> possible venue ARES

Concrete synthesis of discussion

Daniel will start writing a draft based on Bruno's presentation on evidences about scams

Another evidence = pattern in range of blocks IPs?

Analysis of lifecycle of vulnerabilities

LSA
distribution of price with respect to vulnerability (CVE)
time evolution of prices also conditioned on CVE

FUD
do some analysis about anti-virus that are typically the bottleneck
look patterns regarding the anti-virus list

distribution of number XX/YY

Mateus work on decision trees with and without temporal information