Quel est l'OS de Kim Jong-un ?

Conclusions hâtives et mauvaise foi

Pierre Capillon
pierre@30cm.fr

SSTIC 2013
Rump session

http://java-0day.com

Days since last known Java 0-day exploit

Previous high score: 46

General info

Java-related CVEs:
web.nvd.nist.gov

No glove, no love:
How to be safe?

```
navigator.javaEnabled() == true
```

Latest patch:
Java 7u21 / 6u45

Latest 0-day(s) info

Is it still a threat? istherejava0day.com
a.k.a. "is the latest patch useless yet?"

Fulldisclosure
http://seclists.org/fulldisclosure/2013/Apr/194
(SE-2012-01 issue #61)

This bypass has been fixed in the latest patch, thus doesn't count as a 0-day.

Stéphanie Ouillon
@steph_ouillon

Follow

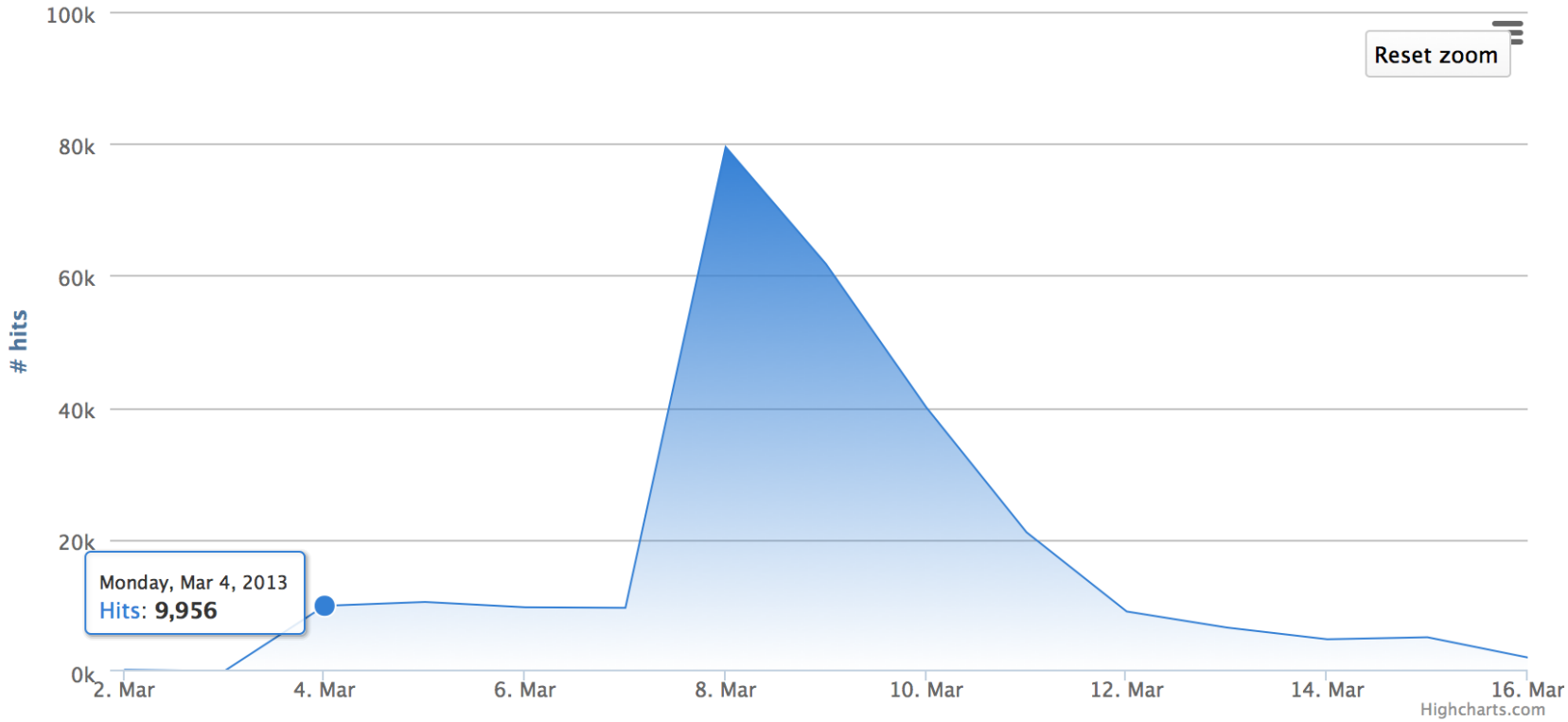
How many days since last known java oday exploit ? java-oday.com

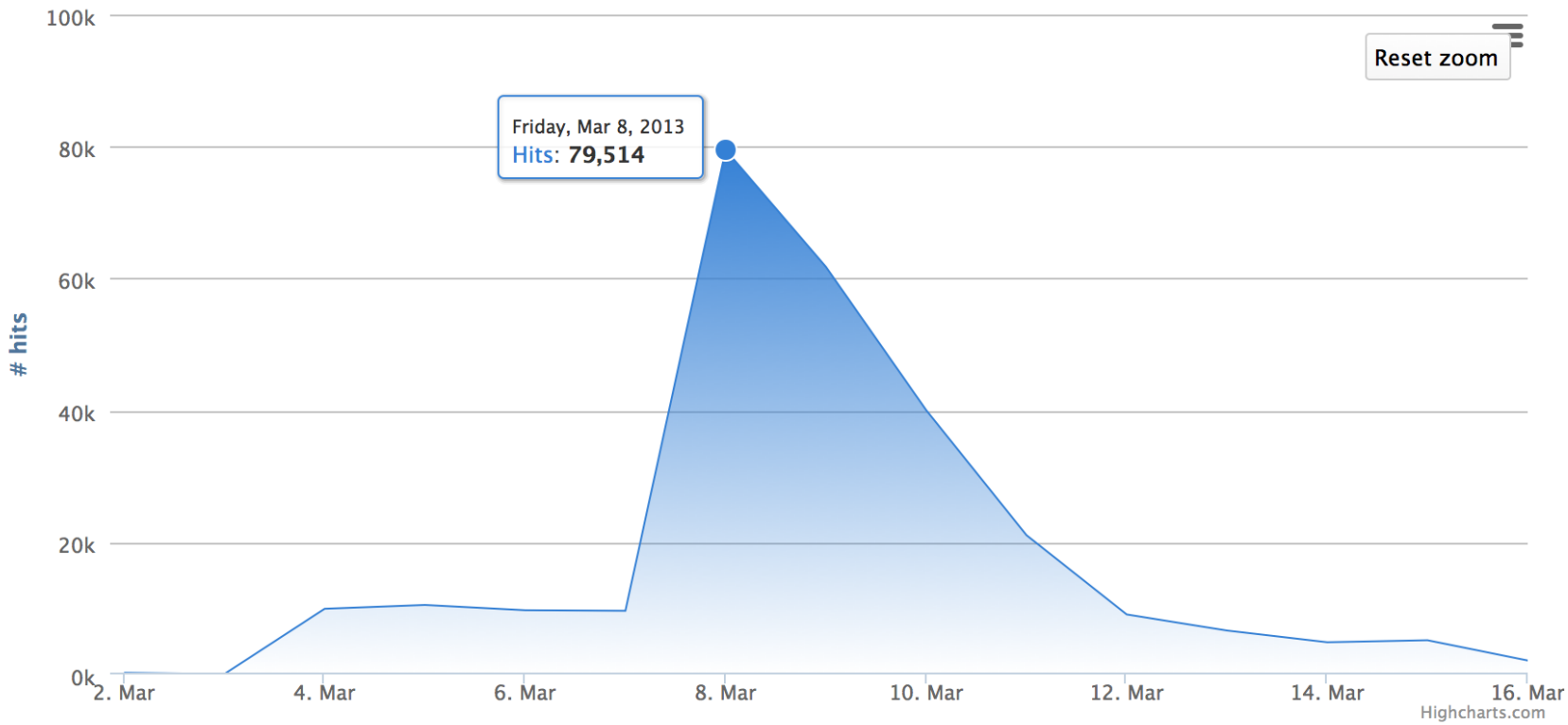
Reply Retweet Favorite More

2
RETWEETS

1:42 AM - 4 Mar 13

https://twitter.com/steph_ouillon/status/308512806414741504


100k
80k
60k
40k
20k
0k
hits
Reset zoom
Monday, Mar 4, 2013
Hits: 9,956
2. Mar
4. Mar
6. Mar
8. Mar
10. Mar
12. Mar
14. Mar
16. Mar
Highcharts.com


100k
80k
60k
40k
20k
0k
hits
Reset zoom
Friday, Mar 8, 2013
Hits: 79,514
2. Mar
4. Mar
6. Mar
8. Mar
10. Mar
12. Mar
14. Mar
16. Mar
Highcharts.com

Certains tremblent déjà...

```
# hits IP hostname
     [...]
   4 196.15.16.100 resolves to inet-idcmc01-o.oracle.co.in
   4 196.15.16.101 resolves to inet-idcmc02-o.oracle.co.in
   4 196.15.16.103 resolves to inet-idcmc04-o.oracle.co.in
   4 202.45.129.181 resolves to inet-jpmc02-ext.oracle.co.jp
   4 202.45.129.184 resolves to inet-cnmc02-pri-ext.oracle.co.jp
   9 202.45.129.180 resolves to inet-jpmc01-ext.oracle.co.jp
     [...]
  31 148.87.19.222 resolves to inet-hqmc08-o.oracle.com
  33 193.9.13.137 resolves to inet-emmc05-o.oracle.co.uk
     [...]
  47 193.9.13.139 resolves to inet-emmc07-o.oracle.co.uk
  54 148.87.19.198 resolves to inet-hqmc02-o.oracle.com
  60 193.9.13.135 resolves to inet-emmc03-o.oracle.co.uk
```

... peut-être à raison

- 193.9.13.135
  "Mozilla/5.0 (X11; **SunOS i86pc**; rv:6.0.2)
  Gecko/20100101 **Firefox/6.0.2**"
- 148.87.67.212
  "Mozilla/5.0 (Macintosh; **Intel Mac OS X 10.6**;
  rv:19.0) Gecko/20100101 Firefox/19.0"
- 148.87.19.206
  "Mozilla/5.0 (Windows NT 5.1; rv:18.0) Gecko/20100101
  Firefox/18.0"
- 137.254.4.6
  "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
  rv:1.9.1.18) Gecko/20110319 **Firefox/3.5.18**

Un fanboy java !

stackoverflow Questions Tags

Chas. Owens less info

36,764
reputation

5 56 140

bio	website	wonkden.net
	location	Sterling, VA
	age	38
visits	member for	4 years, 2 months
	seen	4 hours ago
stats	profile views	2,551

De l’argent !

[−] **todu** 11 points 2 months ago

+tip 1 USD verify

permalink

[−] **bitcointip** [🏦] 13 points 2 months ago

[✔] **Verified**: todu ---> ฿0.02151463 BTC [$1 USD] ---> Thebestfrenchie [**help**]

permalink **parent**

[−] **Comment removed** 2 months ago

[−] **todu** 12 points 2 months ago

I just donated 1 USD to the post submitter using the "bitcoin" currency, because I wanted to give him a little monetary support for the cost of registering a domain name in order to make a joke that I found to be funny :). If you click the "help" link in the message from the "bitcointip" user, you can read more about it.

permalink **parent**

[−] **Katana__** 8 points 2 months ago

...are you even sure that OP is the site creator?

permalink **parent**

[−] **Thebestfrenchie** [S] 6 points 2 months ago

Thanks for the healthy skepticism: I'm not the creator.

See this post.

permalink **parent**

Les vieux

- **1154 hits MSIE 6.0**

```
 63 204.13.200.8 resolves to aip-8.trustwave.com
  7 204.13.202.8 resolves to aip-8.trustwave.com
  5 212.73.202.122 resolves to h3-c04-v.eset.com
  8 187.162.232.236 resolves to 187-162-232-236.static.axtel.net
 18 62.90.140.132 resolves to 62-90-140-132.barak.net.il
 24 62.90.140.132 resolves to 62-90-140-132.barak.net.il
  2 80.120.162.10 resolves to mail.wassenaar.org
    [...]
```

- dont 1 qui vient tous les jours à heures fixes

Reverse DNS

- **6 reports urlquery.net**
- 191 .gov
- 107 .mil
- 22 .cn
- **1 .gouv.fr**

Best-of

- **92.103.133.164 resolves to mail.defense.gouv.fr**
  `"Mozilla/5.0 (Windows NT 5.1; rv:20.0) Gecko/20100101 Firefox/20.0"`

Best-of

- **president.whitehouse.gov**
  "Mozilla/5.0 (**X11; Ubuntu; Linux i686;** rv:17.0) Gecko/20100101 Firefox/17.0"

Best-of

- **osd.mil (Office of the Secretary of Defense)**
  "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3)"

Best-of

- **host-134-11-73-69.ptr.hqda.pentagon.mil**
  `"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0"`

Best-of

- **GenericHost.kuwait.swa.army.mil**
  `"Mozilla/5.0 (Windows NT 6.1; rv:20.0) Gecko/20100101 Firefox/20.0"`

APT1 Rebirth

40 Hits depuis les IP des méchants du rapport Mandiant :

- 2 hits 101.85.121.126
- 2 hits 112.64.71.171
- 2 hits 114.85.197.143
- 2 hits 116.231.244.196
- 2 hits 116.231.246.46
- 2 hits 116.232.93.200
- 2 hits 116.233.108.210
- 2 hits 116.237.16.215
- 2 hits 222.67.137.194
- 3 hits 114.94.75.3
- 4 hits 116.232.168.40
- 7 hits 143.89.190.40
- 8 hits 112.64.161.162

APT1

- 112.64.161.162 **CN, China (APT1)**
  - "Mozilla/5.0 (**X11; Linux x86_64**) AppleWebKit/537.22 (KHTML, like Gecko) Chrome/25.0.1364.97 Safari/537.22"
  - "Mozilla/5.0 (Macintosh; **Intel Mac OS X 10_8_3**) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.11 Safari/537.36"

Pays amis d'Internet

```
91.144.8.16 @ GeoIP: SY, Syrian Arab Republic
94.252.208.206 @ GeoIP: SY, Syrian Arab Republic
94.252.229.111 @ GeoIP: SY, Syrian Arab Republic
95.159.59.91 @ GeoIP: SY, Syrian Arab Republic
190.6.74.249 @ GeoIP: CU, Cuba
200.55.145.11 @ GeoIP: CU, Cuba
109.162.221.104 @ GeoIP: IR, Iran, Islamic Republic of
109.162.225.94 @ GeoIP: IR, Iran, Islamic Republic of
109.162.231.20 @ GeoIP: IR, Iran, Islamic Republic of
[... 33 hits d'Iran ...]
```

Pays amis d'Internet

- 95.159.59.91 **SY, Syrian Arab Republic**
  - "Mozilla/5.0 (compatible; **MSIE 10.0; Windows NT 6.2**; Trident/6.0)"

Pays amis d'Internet

- 112.64.161.162 **IR, Iran, Islamic Republic of**
  - "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.11 (KHTML, like Gecko) **Ubuntu/10.04** Chromium/23.0.1271.64 Chrome/23.0.1271.64 Safari/537.11"

Pays amis d'Internet

- 190.6.74.249 **CU, Cuba**
  - "**Opera/9.80 (Windows NT 6.2; WOW64)** Presto/2.12.388 Version/12.14"

Pays démocratiques

202.144.184.147 @ GeoIP: **LA, Lao People’s Democratic Republic**
175.45.176.140 @ GeoIP: **KP, Korea, Democratic People’s Republic of**

Pays démocratiques

- 175.45.176.140 **KP, Korea, Democratic People's Republic of**
  - `"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/537.22 (KHTML, like Gecko) Chrome/25.0.1364.152 Safari/537.22"`

Questions ?

Game of Thrones