Ruby trunk - Bug #8945

Unmarshaling an Array containing a Bignum from a tainted String returns a frozen, tainted Bignum

09/24/2013 01:07 PM - brixen (Brian Shirai)

Status:	Closed		
Priority:	Normal		
Assignee:	matz (Yukihiro Matsumoto)		
Target version:	2.2.0		
ruby -v:	ruby 2.1.0dev (2013-09-24 trunk 43025) [x86_64-darwin13.0.0]	**Backport:**	1.9.3: REJECTED, 2.0.0: UNKNOWN

Description

In 2.1, Symbol, Fixnum, Bignum, and Float (at least) have been changed to frozen by default. Consequently, calling #taint on an instance of those classes raises a RuntimeError because a frozen object cannot be modified to be tainted. However:

```
sasha:rbx brian$ ruby -v
ruby 2.1.0dev (2013-09-24 trunk 43025) [x86_64-darwin13.0.0]
sasha:rbx brian$ irb
irb(main):001:0> a = 0xffff_ffff_ffff_ffff
=> 18446744073709551615
irb(main):002:0> a.class
=> Bignum
irb(main):003:0> a.frozen?
=> true
irb(main):004:0> a.tainted?
=> false
irb(main):005:0> str = Marshal.dump([a]).taint
=> "\x04\b[\x06l+\t\xFF\xFF\xFF\xFF\xFF\xFF\xFF\xFF"
irb(main):006:0> str.tainted?
=> true
irb(main):007:0> aa = Marshal.load(str)
=> [18446744073709551615]
irb(main):008:0> aa.first.class
=> Bignum
irb(main):009:0> aa.first.frozen?
=> true
irb(main):010:0> aa.first.tainted?
=> true
irb(main):011:0>
```

The behavior above is inconsistent with the results of performing the same operations on instances of Symbol, Fixnum, Float. For example:

```
irb(main):014:0> :a.frozen?
=> true
irb(main):015:0> :a.tainted?
=> false
irb(main):016:0> str = Marshal.dump([:a]).taint
=> "\x04\b[\x06:\x06a"
irb(main):017:0> aa = Marshal.load(str)
=> [:a]
irb(main):018:0> aa.tainted?
=> true
irb(main):019:0> aa.first.frozen?
=> true
irb(main):020:0> aa.first.tainted?
=> false
```

Associated revisions

Revision cc1910b5 - 02/08/2014 05:13 PM - nobu (Nobuyoshi Nakada)

marshal.c: Numerics are not tainted

- include/ruby/ruby.h (OBJ_TAINTABLE, OBJ_TAINT, OBJ_INFECT), marshal.c (r_entry0): all Numerics never be tainted now. [ruby-core:57346] [Bug #8945]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@44891 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 44891 - 02/08/2014 05:13 PM - nobu (Nobuyoshi Nakada)

marshal.c: Numerics are not tainted

- include/ruby/ruby.h (OBJ_TAINTABLE, OBJ_TAINT, OBJ_INFECT), marshal.c (r_entry0): all Numerics never be tainted now. [ruby-core:57346] [Bug #8945]

Revision 44891 - 02/08/2014 05:13 PM - nobu (Nobuyoshi Nakada)

marshal.c: Numerics are not tainted

- include/ruby/ruby.h (OBJ_TAINTABLE, OBJ_TAINT, OBJ_INFECT), marshal.c (r_entry0): all Numerics never be tainted now. [ruby-core:57346] [Bug #8945]

Revision 44891 - 02/08/2014 05:13 PM - nobu (Nobuyoshi Nakada)

marshal.c: Numerics are not tainted

- include/ruby/ruby.h (OBJ_TAINTABLE, OBJ_TAINT, OBJ_INFECT), marshal.c (r_entry0): all Numerics never be tainted now. [ruby-core:57346] [Bug #8945]

Revision 44891 - 02/08/2014 05:13 PM - nobu (Nobuyoshi Nakada)

marshal.c: Numerics are not tainted

- include/ruby/ruby.h (OBJ_TAINTABLE, OBJ_TAINT, OBJ_INFECT), marshal.c (r_entry0): all Numerics never be tainted now. [ruby-core:57346] [Bug #8945]

Revision 44891 - 02/08/2014 05:13 PM - nobu (Nobuyoshi Nakada)

marshal.c: Numerics are not tainted

- include/ruby/ruby.h (OBJ_TAINTABLE, OBJ_TAINT, OBJ_INFECT), marshal.c (r_entry0): all Numerics never be tainted now. [ruby-core:57346] [Bug #8945]

Revision 44891 - 02/08/2014 05:13 PM - nobu (Nobuyoshi Nakada)

marshal.c: Numerics are not tainted

- include/ruby/ruby.h (OBJ_TAINTABLE, OBJ_TAINT, OBJ_INFECT), marshal.c (r_entry0): all Numerics never be tainted now. [ruby-core:57346] [Bug #8945]

History

#1 - 01/30/2014 04:18 AM - hsbt (Hiroshi SHIBATA)

- Target version changed from 2.1.0 to 2.2.0

#2 - 02/07/2014 12:57 PM - nobu (Nobuyoshi Nakada)

- Category set to core

- Status changed from Open to Assigned

- Assignee set to matz (Yukihiro Matsumoto)

As Bignum instances are frozen now, it feels reasonable that they never be tainted, IMO.

#3 - 02/08/2014 01:05 PM - matz (Yukihiro Matsumoto)

Agreed. It should be consistent here.

Matz.

#4 - 02/08/2014 05:14 PM - nobu (Nobuyoshi Nakada)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

Applied in changeset r44891.

marshal.c: Numerics are not tainted

- include/ruby/ruby.h (OBJ_TAINTABLE, OBJ_TAINT, OBJ_INFECT), marshal.c (r_entry0): all Numerics never be tainted now. [ruby-core:57346] [Bug #8945]

#5 - 02/14/2014 04:15 AM - usa (Usaku NAKAMURA)

- Backport changed from 1.9.3: UNKNOWN, 2.0.0: UNKNOWN to 1.9.3: REJECTED, 2.0.0: UNKNOWN

IMO this is a feature change, although it is close to a bug infinite.
So, I decided this not to backport into 1.9.3.