

Networks under Fire!

The SANS Internet Storm Center



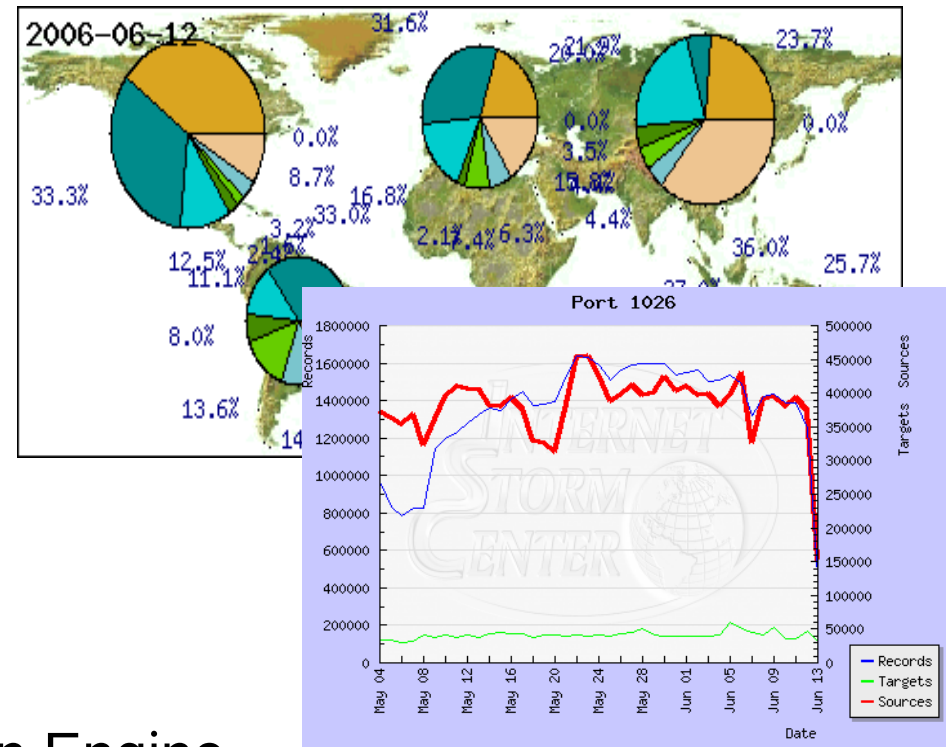
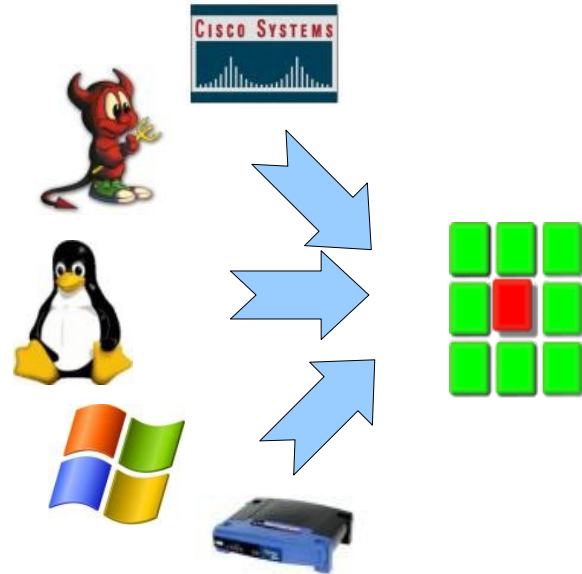
Johannes B. Ullrich, Ph.D.
SANS Institute



Outline

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

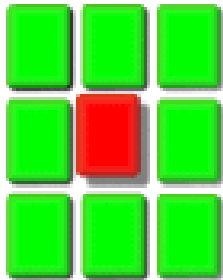
How do DShield and the Internet Storm Center work together?



DShield: Automated Data Collection Engine.

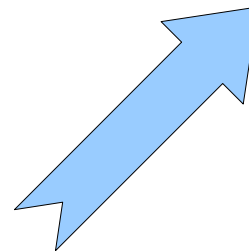
The Internet Storm Center uses DShield and reader reports to create daily diaries.

DShield Data

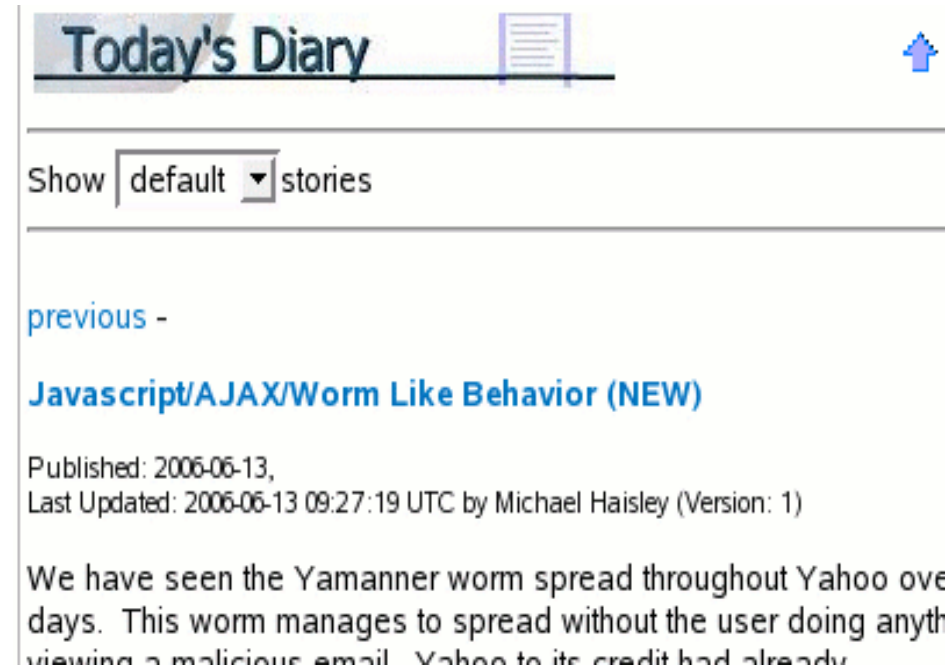


Reader Reports

```
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)

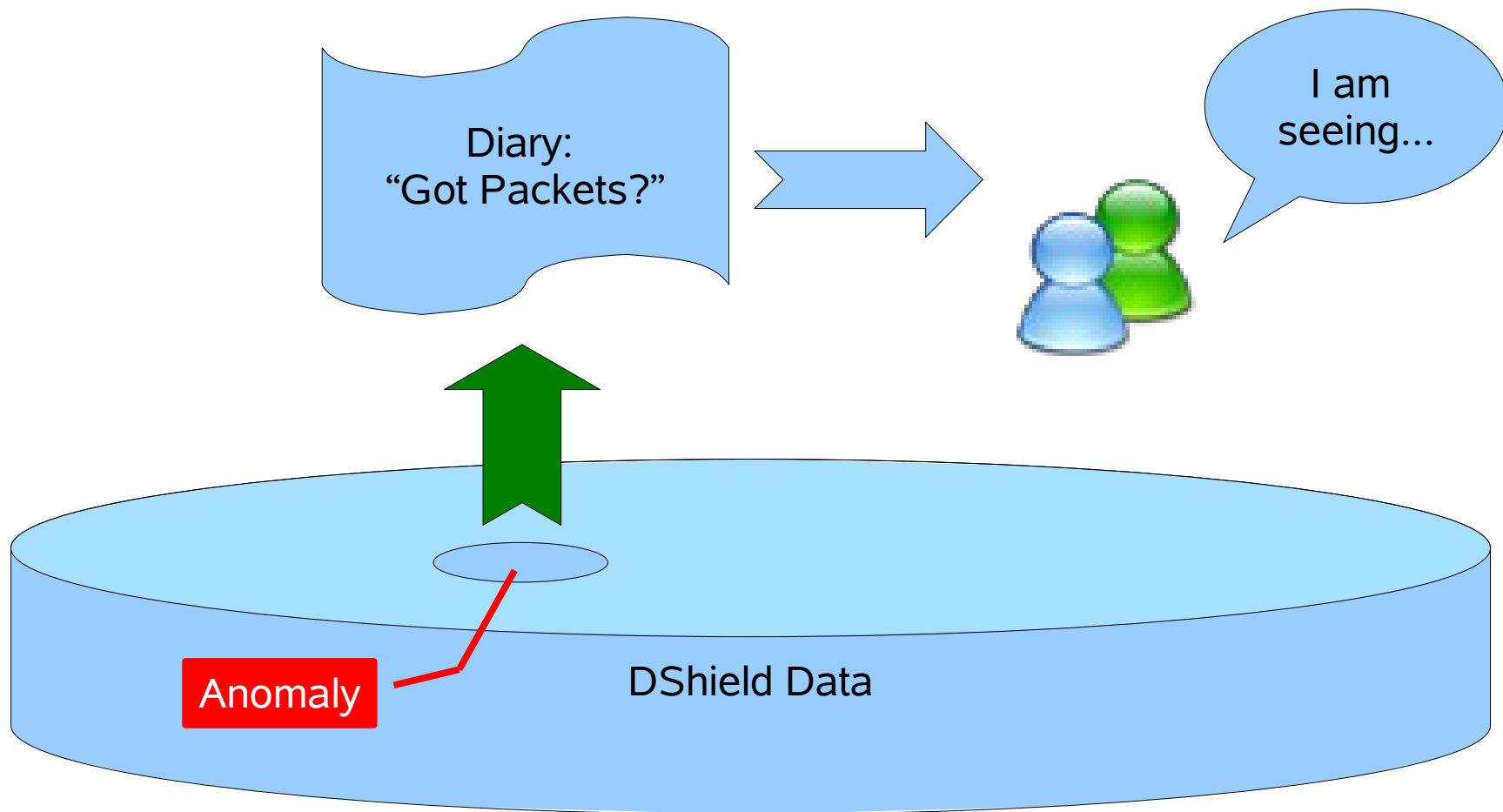
We have seen the Yamanner worm spread throughout Yahoo over days. This worm manages to spread without the user doing anything...



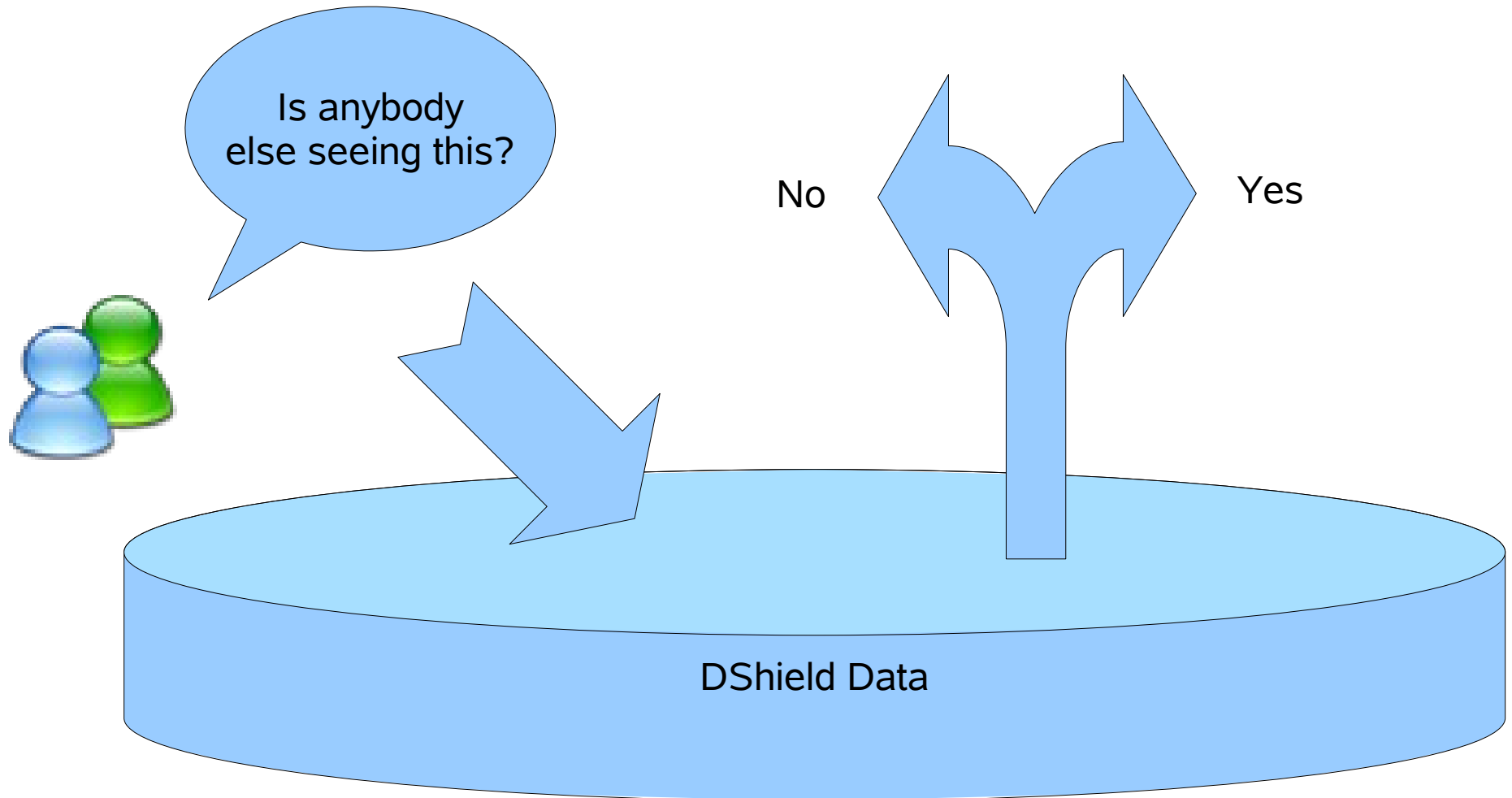
The ISC Handlers are a diverse group of network security professionals

- 40 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.

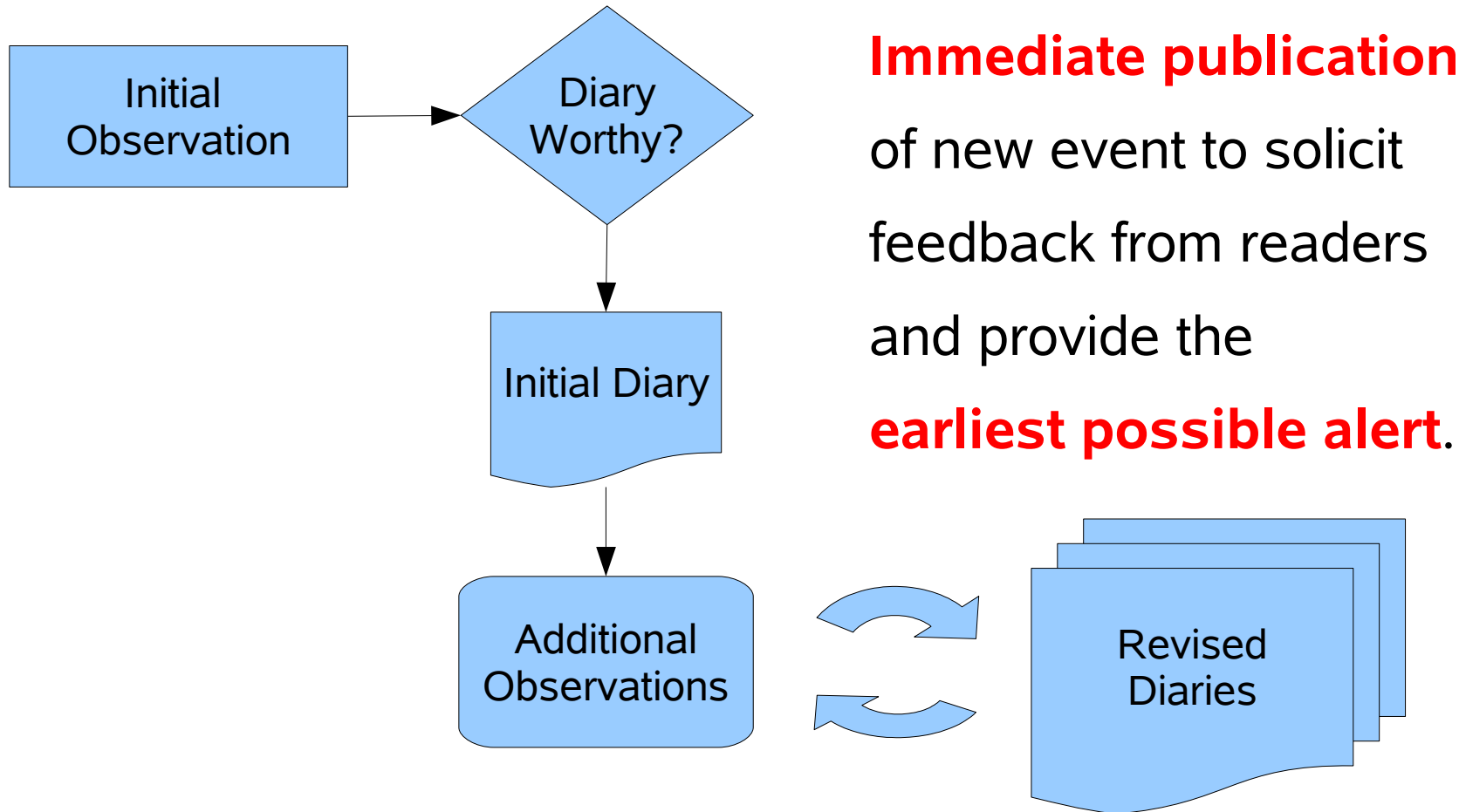
Data from DShield allows us to “zoom in” on new trends and solicit more details from users.



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.





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?



The WMF exploit showed that 0-day exploits are no longer used to attack only high value targets.

DEC
28
2005

Phone Call:

“I went to Knoppix-STD.org, and it looks like adware was installed on my system”

Verification:

- ✓ Visit knoppix-std.org
- ✓ “Fax Viewer” pops up
- ✓ Anti Spyware Ad is installed.

Initially, the WMF 0-day exploit is used to install fake anti-spyware.

**Step 2
Spyware scan**



WinHound

hunt
down
malware

Spyware scan process control

▶

Process overview

Current object: C:\Documents and Settings\Test User\Cookies\test

Filesystem		Registry	
Files scanned	4044	Keys scanned	141421
Files infected	9	Keys infected	3
Folders scanned	969	Values scanned	16178
Folders infected	1	Values infected	9
Total scanned	162612	Host entries scanned	0
Total found	99	Hosts entries found	0

Microsoft Internet Explorer [Close]

System scan was finished.
WinHound detected malicious programs on your computer.
Please take your action and then proceed to Step 3 -> SmartCleanup

OK

						Status
+ []	File	SpySheriff	Critical	Delete	Found	Found
+ []	File	SpySheriff	Critical	Delete	Found	Found
+ []	Folder	SpySheriff	Critical	Delete	Found	Found
+ []	RegKey	Trojan.InternetUpdate	Critical	Delete	Found	Found

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?

Disable shimvw.dll works ok.



User Education?

Too late, and wouldn't work.

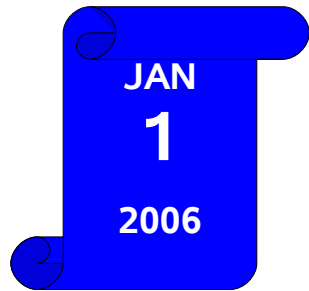


Why did Anti Virus not work well?

- Rapid delivery of obfuscation tools (e.g. Metasploit).
- Anti Virus recognized payload, but not exploit.
 - Multi-payload exploit: Only partially discovered and removed.
- New payloads released hourly.

> 500 distinct versions after few days !

The situation escalates as more and more sites attempt to exploit the vulnerability.



YELLOW

- The race is on by malware writers to capture as many vulnerable systems as possible.
(SPEED COUNTS!)
- Spam used to disseminate exploit.
- Exploit can be triggered by desktop search programs.
- **Ifak Guilfanov releases patch!**



Is it ok for the Internet Storm Center (or anybody) to release or recommend an unofficial patch?

- Patch has been validated.

Tom Liston verified that the patch is “ok”.

- Risks are communicated to the user.

The patch was clearly labeled as “unofficial”

- No good mitigation method is available.

disabling shimvw.dll causes many problems.

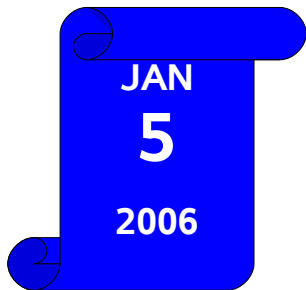
- Widespread use of exploit.

500 versions found in the wild, large botnets built.

- No vendor patch is available.
-

Even with patch and workarounds, the battle against WMF exploit continues.

- several 1,000 e-mails over the new year weekend.
- Microsoft releases WMF patch by mistake.



Microsoft releases official patch ahead of its scheduled January patch day.



Recent reports to the ISC show the following threats as important and current.

- 0-day exploits (“commodity” as well as targeted).
- The Age of the Bot.
- Client (and more targeted) attacks.
- Diminishing utility of signature based Antivirus solutions.



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

- 0-day: 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.

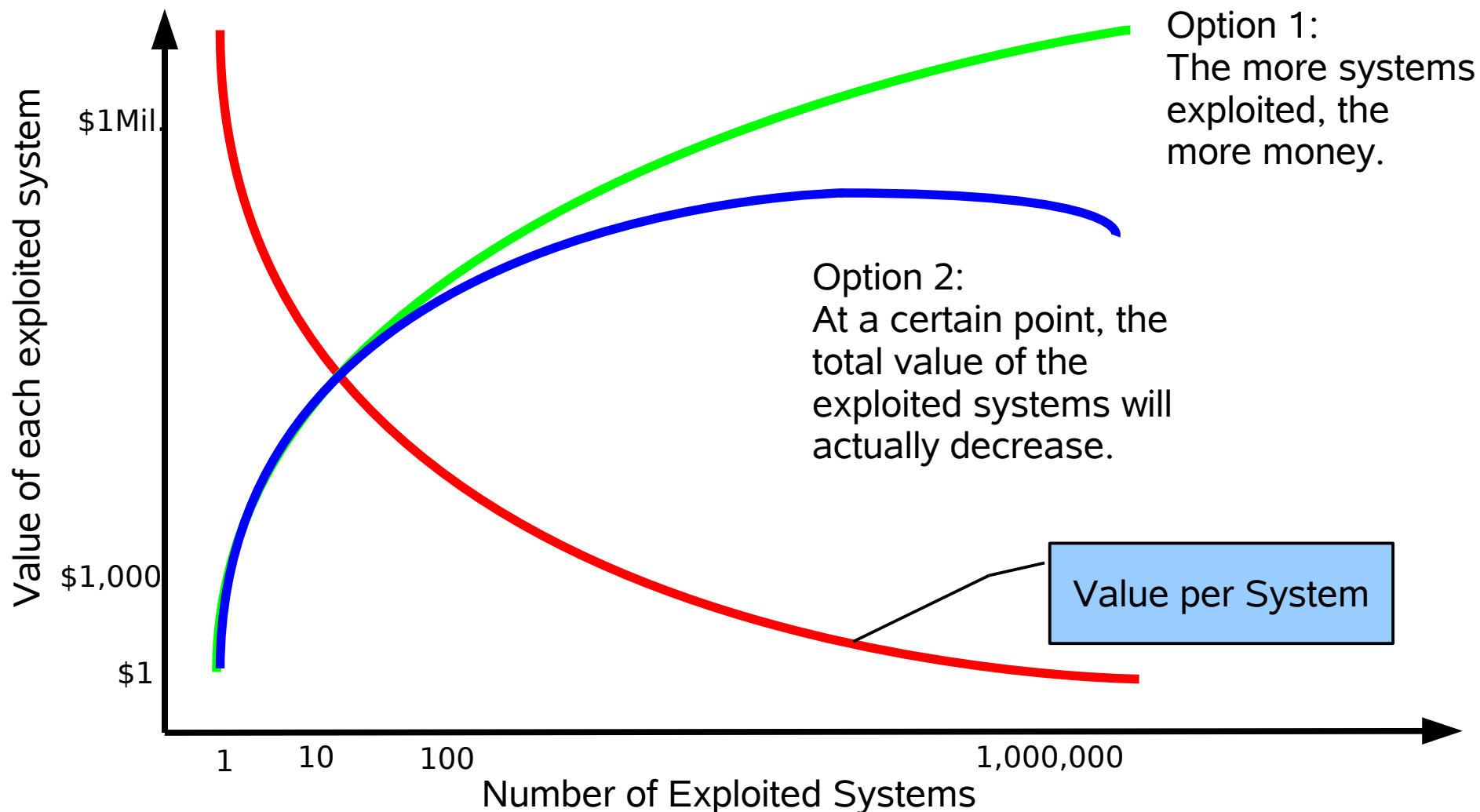


Vendors have a hard time responding to 0-day exploits.

-
- 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.



It is the goal of a malware writer to maximize the return from a particular exploit.





What does it mean for the malware world if there is an optimum number of exploited systems?

- Worm: Unlimited exploit delivery to very larger number of hosts.
- Bot: Semi-targeted and controlled exploit delivery with good post-exploit control over infected hosts.

> **Bots win!**



Why would additional systems actually lower the value of the total “Botnet”?

- If an exploit is too wide spread, high value systems are likely to be patched and the exploit will be removed. (“CNN Effect”).
- Larger networks are harder to maintain. It will be harder to fully take advantage of the few high value systems.



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 Targeted e-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:

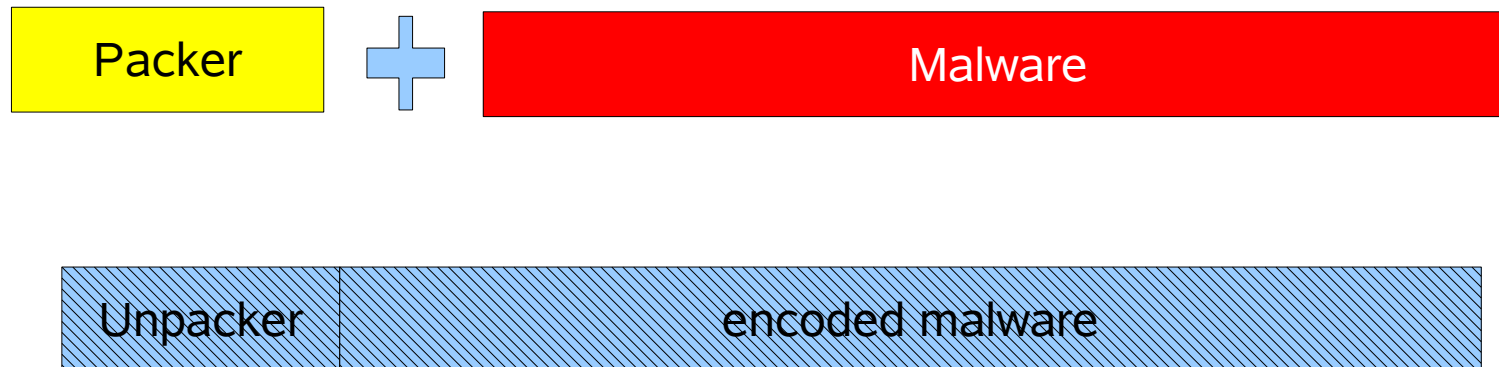
From: Alice's Bot
To: Bob
Subject: Meeting

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

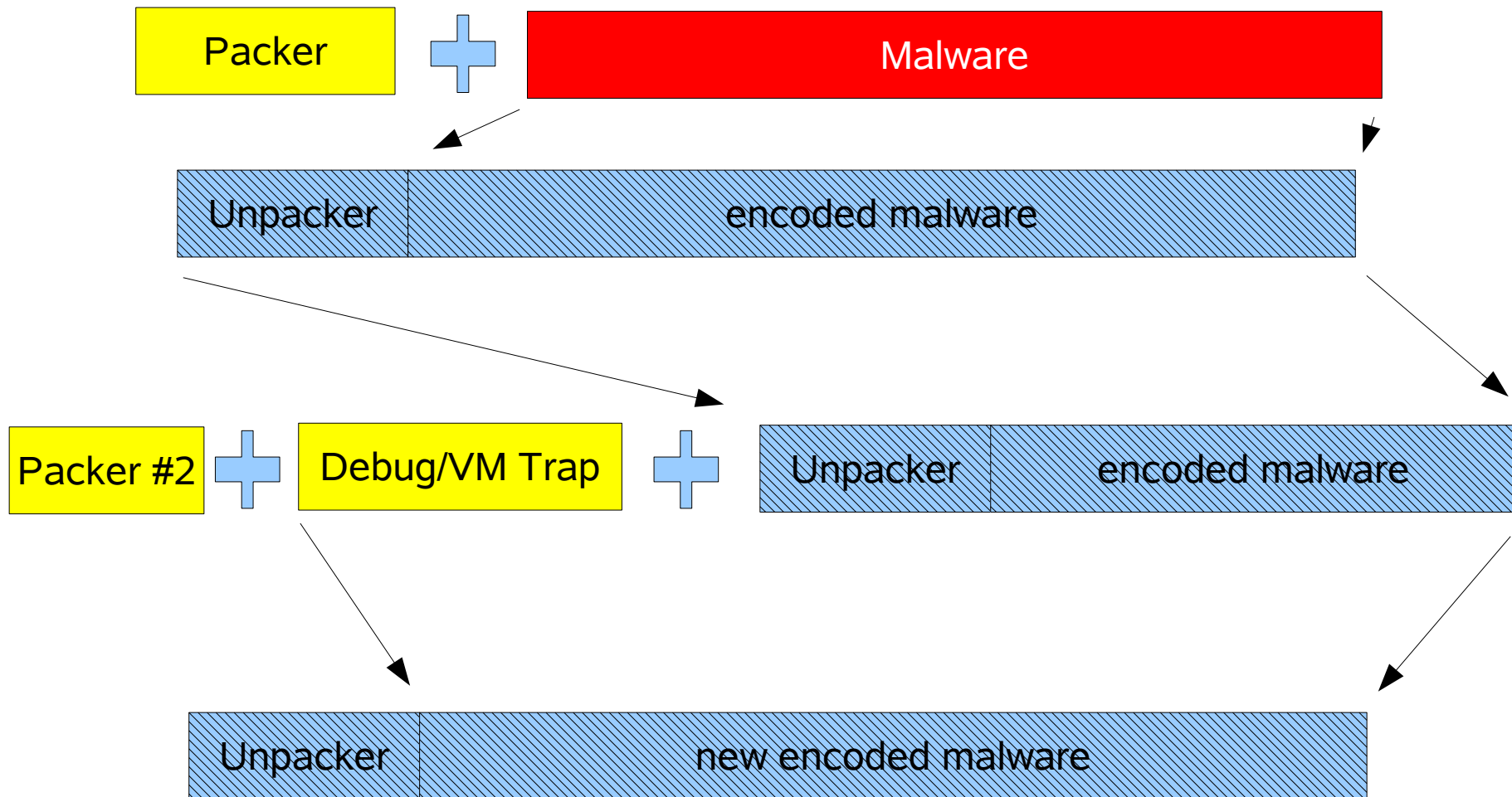
Alice

Packers allow for rapid mutation of existing malware, making it very hard for AV products to keep up.

- Zotob: Every 4 hrs a new version.
- New Version: Old code repacked.
- No need to write new malware.



Packers can use different “keys”, debugger traps, or they can be nested.





Anti Virus writers are working on defenses, but so far the defenses fall short.

-
- “Sandbox”: Still essentially pattern based and requires unpacking the code to analyze.
 - “Unpackers”: Packers again are easily modified and it is hard to keep up. Implementation can introduce new problems (Remember: ZIP/RAR... vulnerabilities in AV Products)



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.php>

- Send us your observations:

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

handlers@sans.org

- Send us your malware:

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

<http://isc.sans.org/seccheck>



Now it's your turn to ask questions!

Thanks!

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

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