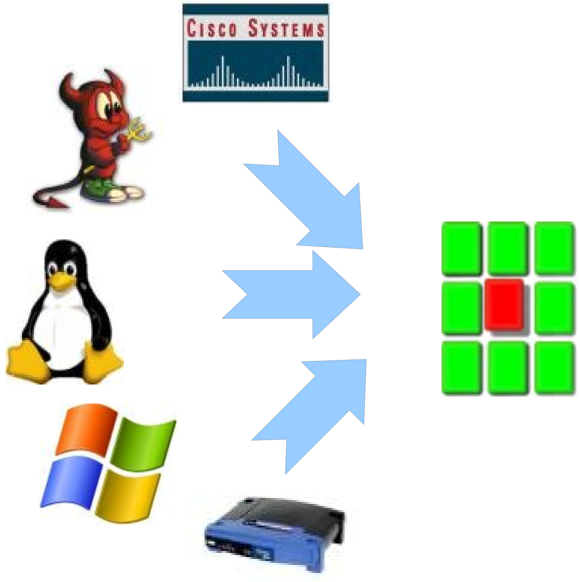
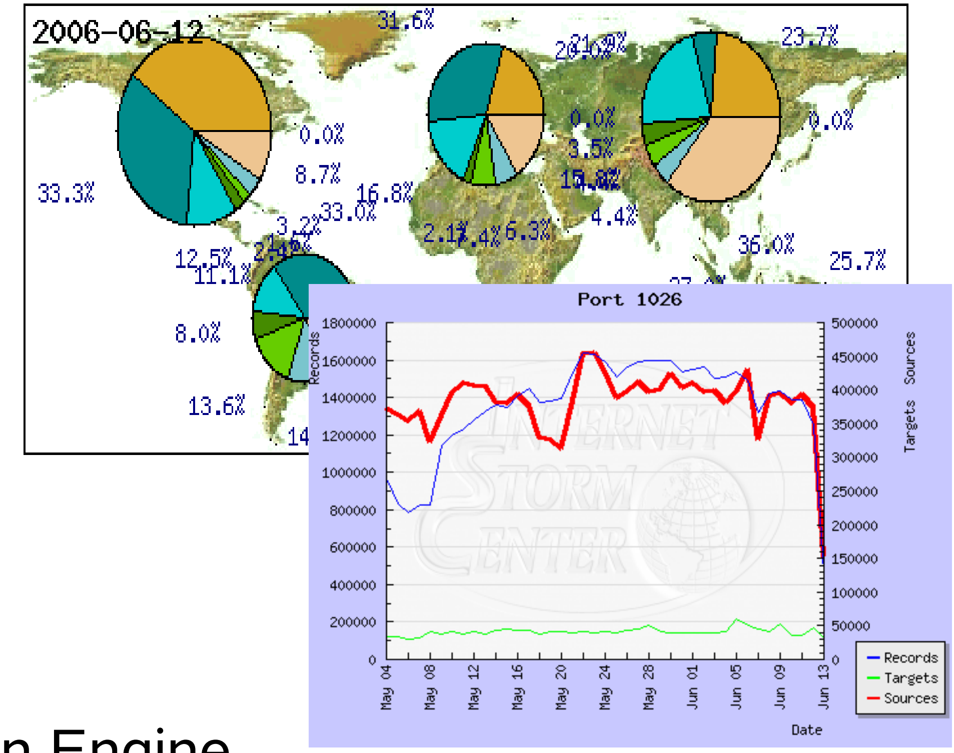
How do DShield and the Internet Storm Center work together?

Sensors → Database → Reports



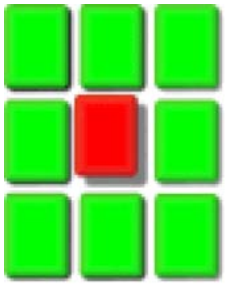


DShield: Automated Data Collection Engine.

http://isc.sans.org

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

DShield Data

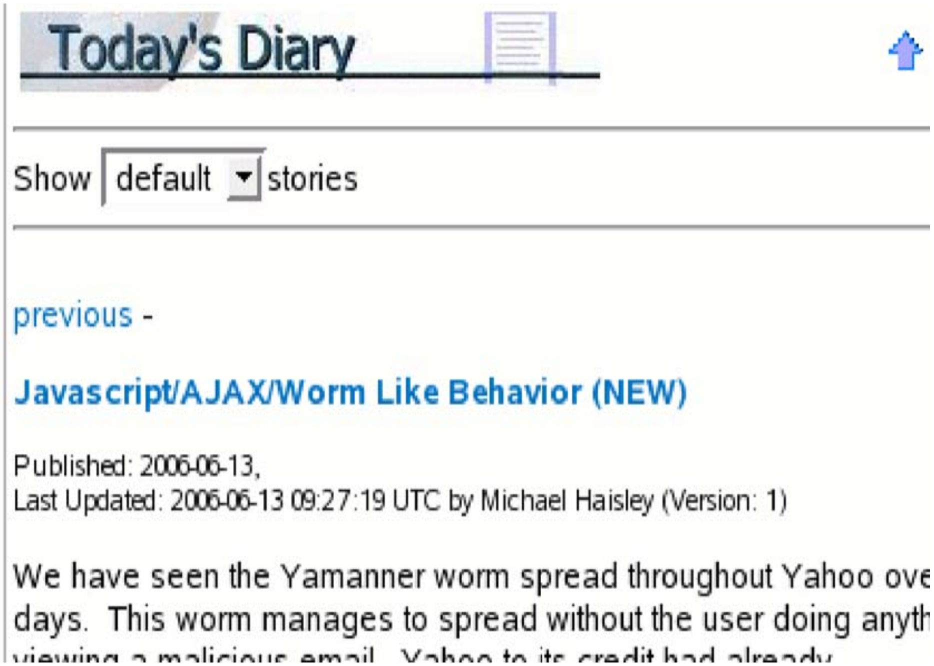


ISC Handlers

Reader Reports

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

....
```



Today's Diary

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)

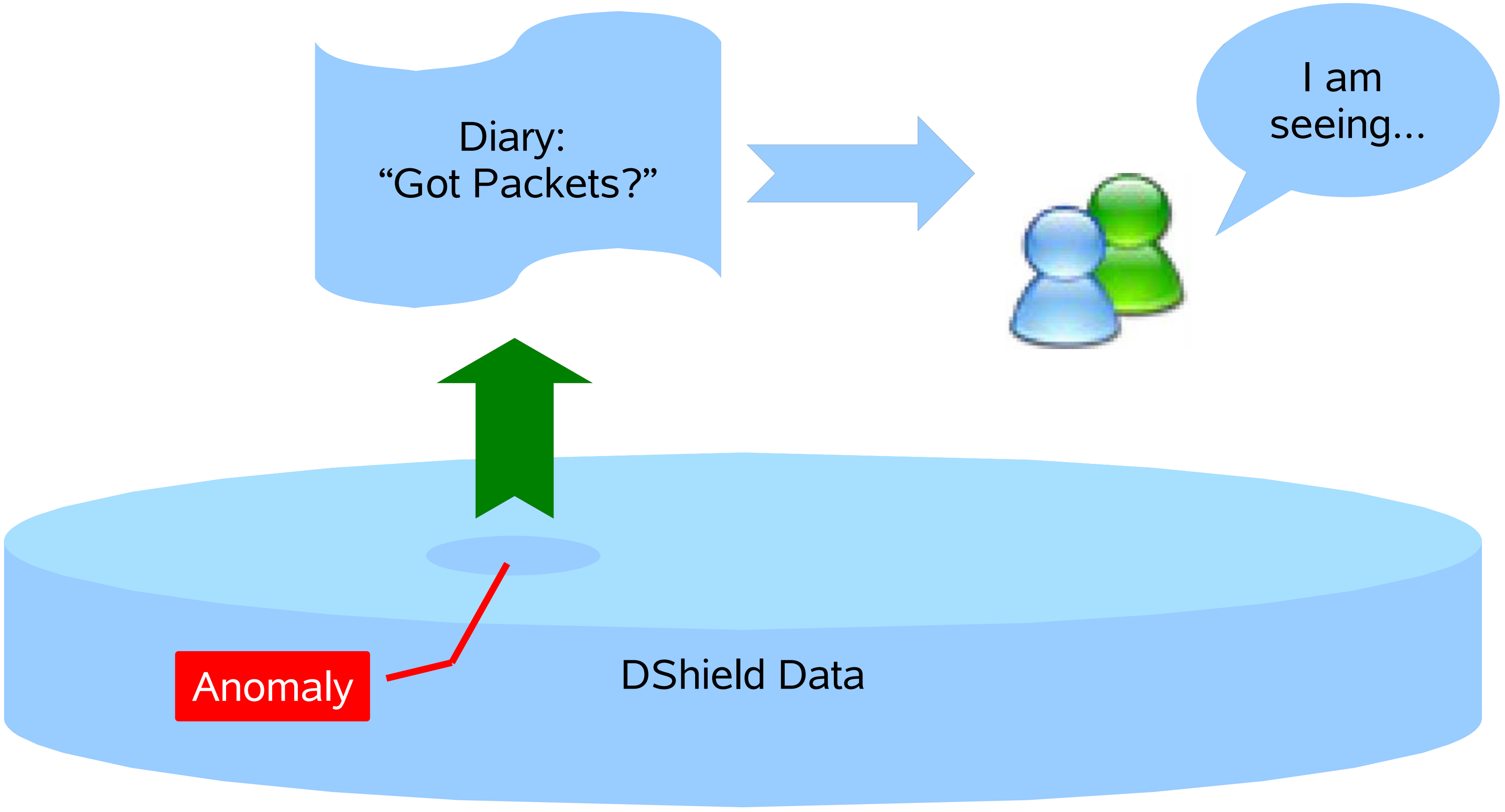
We have seen the Yamanner worm spread throughout Yahoo ove
days. This worm manages to spread without the user doing anyth
viewing a malicious email. Yahoo to its credit had already

http://isc.sans.org

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.



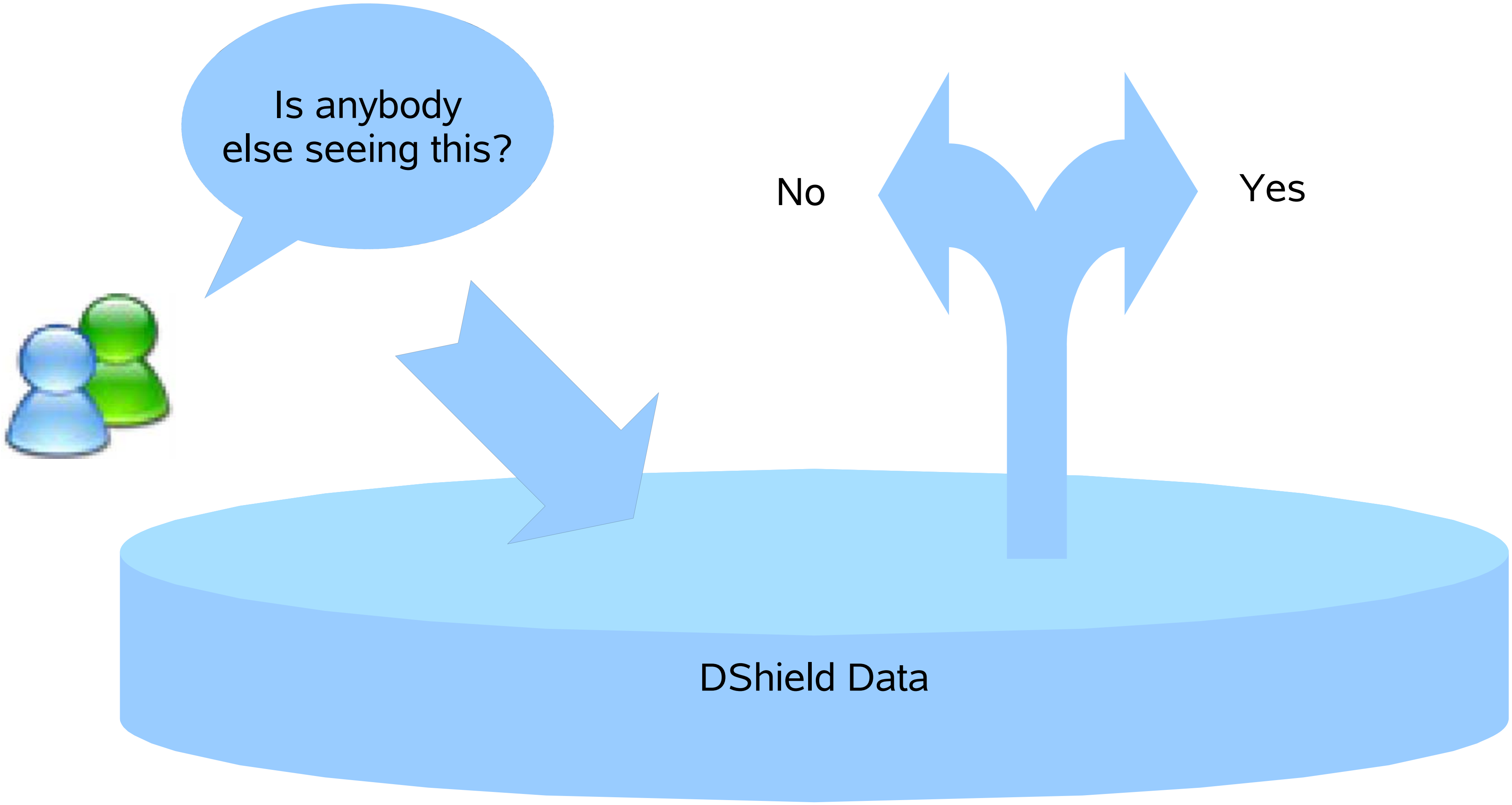
Diary:
“Got Packets?”

I am seeing…

Anomaly

DShield Data

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



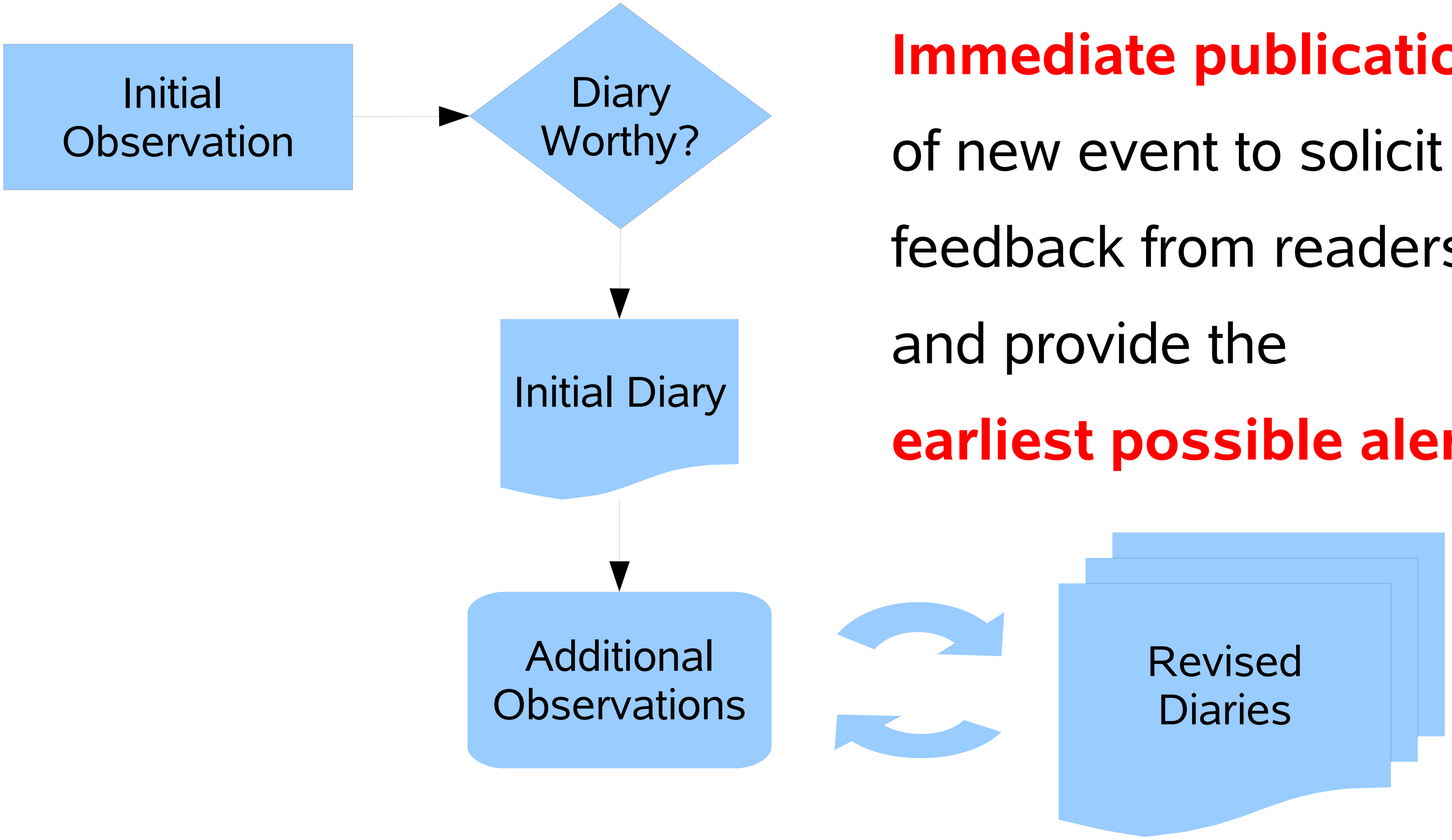
Is anybody else seeing this?

No

Yes

DShield Data

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?

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

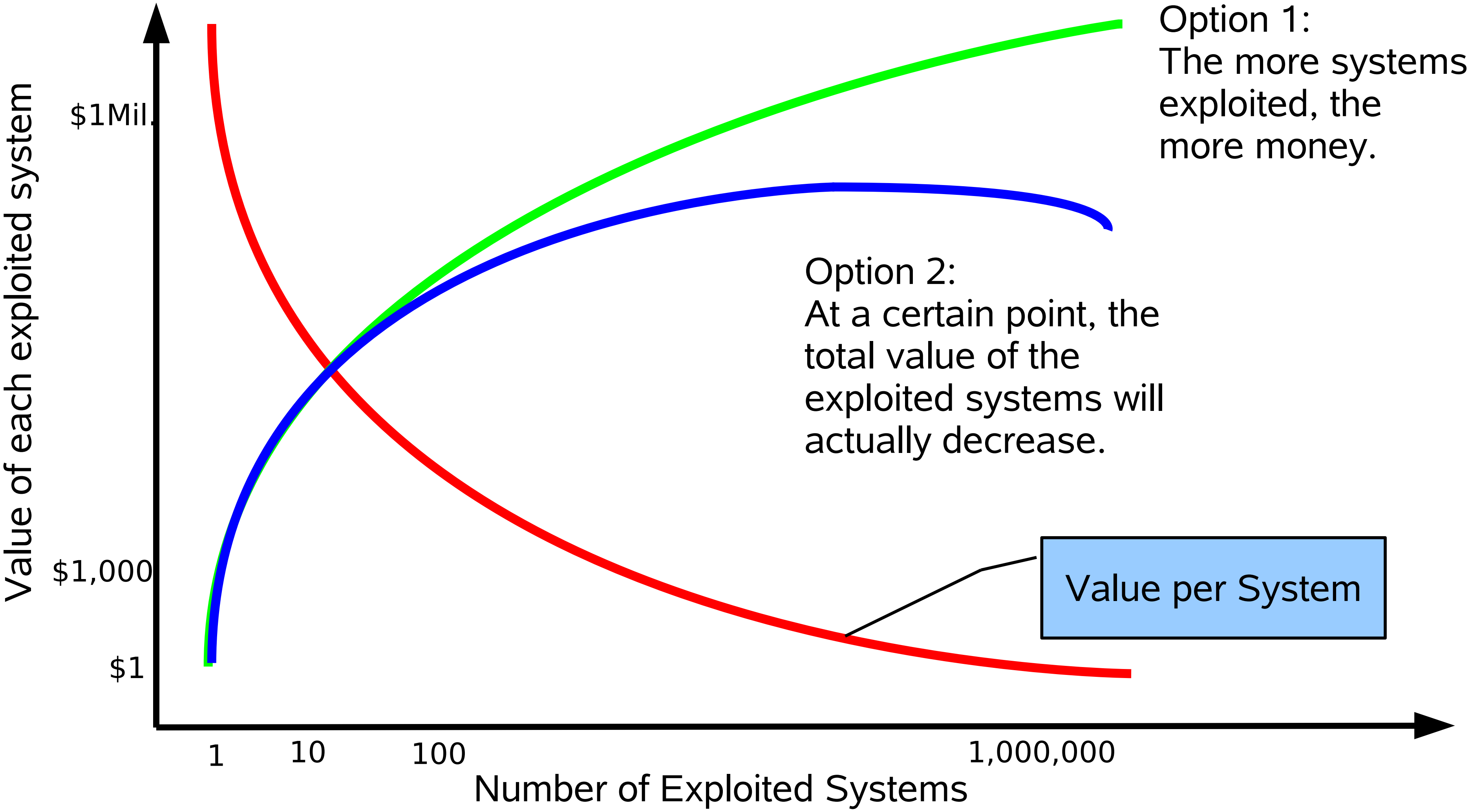
- Exploits are hard to sell on the “open market”. WMF is rumored to have sold for $5,000.
- Security companies (iDefense, 3COM) buy exploits for > $10k.
- Spyware or Adware install will bring approx. $1 per user.

➔ **0-day**

➔ **Millions of Vulnerable Users**

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

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



Option 1:
The more systems exploited, the more money.

Option 2:
At a certain point, the total value of the exploited systems will actually decrease.

Value per System

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.