



**SYMANTEC  
ENGAGE  
HONG KONG** **2010**

# Technology for Today & Tomorrow's Threats

**John Bai**

Senior Manager, Security Technology & Response





**EVERY 15 MINUTES IN  
PARIS**

**A CRIME IS BEING  
COMMITTED...**



**EVERY 3½ MINUTES IN  
NEW YORK**



**EVERY 2 ½ MINUTES IN  
TOKYO**



**EVERY 2 MINUTES IN  
BERLIN**




**EVERY  $\frac{1}{4}$  OF A SECOND  
ON THE WEB**



**1 *IN* 42.000.000**



**1 *IN* 2.600.000**



1 *IN* 300



1 *IN* 31

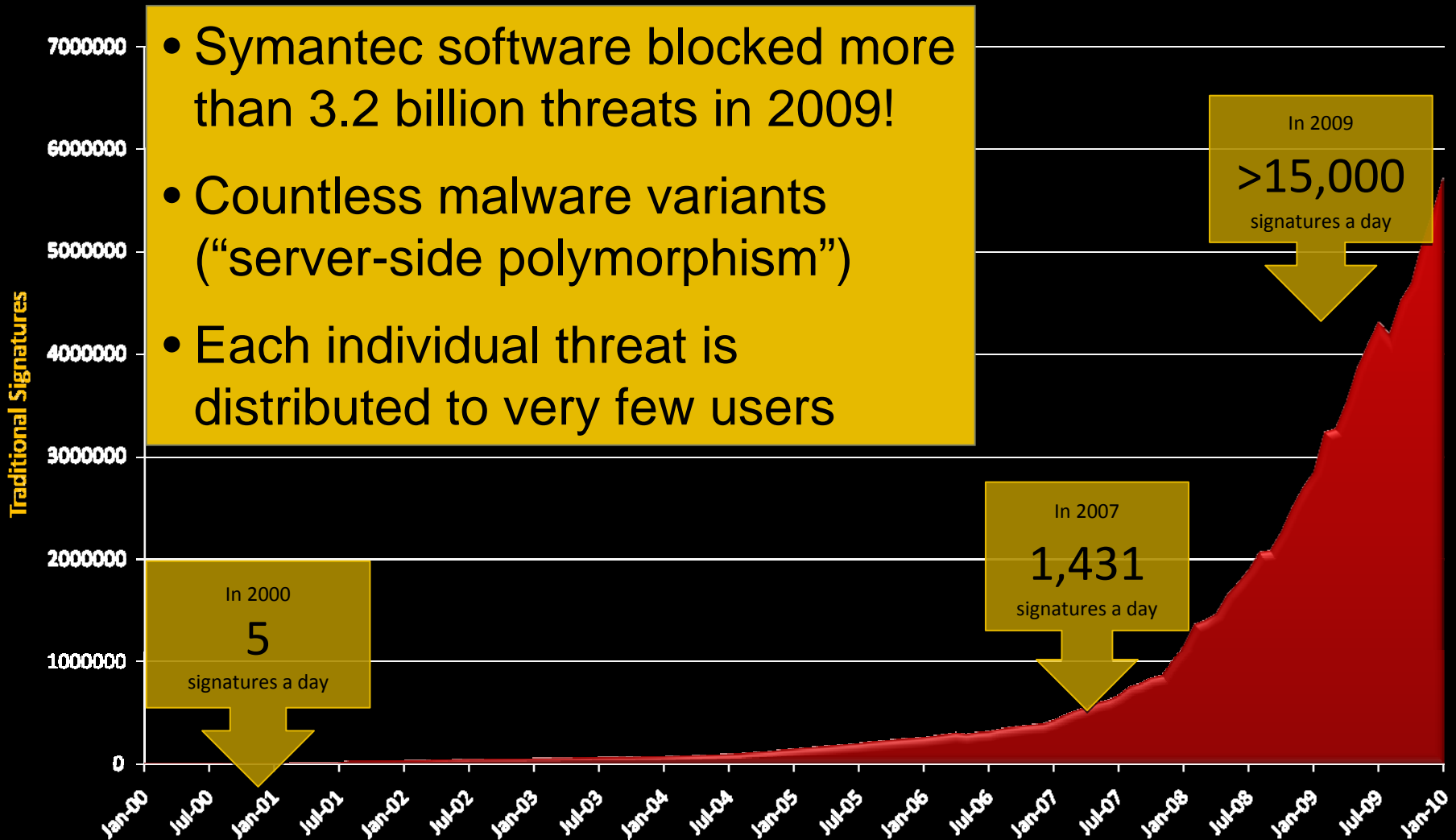
**1 *IN* 5**  
**WILL BE A VICTIM  
OF CYBERCRIME**



# Threat Landscape

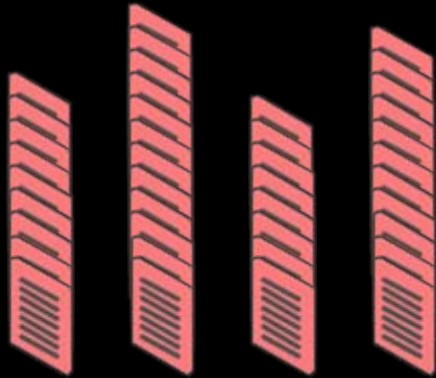
A recent explosion of malware

- Symantec software blocked more than 3.2 billion threats in 2009!
- Countless malware variants (“server-side polymorphism”)
- Each individual threat is distributed to very few users



## The Problem

# Malware authors have switched tactics



### From:

A mass distribution of a relatively few threats e.g.

- **Storm** made its way onto millions of machines across the globe



### To:

A micro distribution model e.g.

- The average **Vundo** variant is distributed to 18 Symantec users!
- The average **Harakit** variant is distributed to 1.6 Symantec users!

What are the odds a security vendor will discover all these threats?

## The Problem

# Millions of file variants (good and bad)

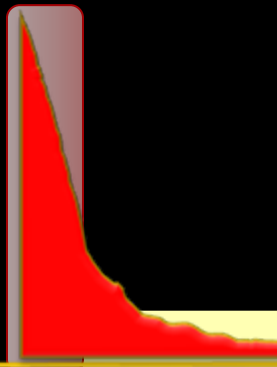
- So imagine that we know:



- about every file in the world today...
  - and how many copies of each exist
  - and which files are good and which are bad
- Now let's order them by prevalence with
    - **Bad** on left
    - **Good** on the right

# No Existing Protection Addresses the “Long Tail”

## Bad Files



Blacklisting works well here.

Unfortunately neither technique works well for the tens of millions of files with low prevalence.

(But this is precisely where the majority of today's malware falls)

For this long tail a new technique is needed.

## Good Files



Whitelisting works well here.

## Reputation

# Could Reputation be used for Security?

- It turns out this approach already works for lots of things



- Symantec has more than 100 million active users
- Couldn't we somehow leverage this massive installed user base to compute software reputations?

## What Can We Do With Reputation?



### Five important new features:

1. Drastically Improved Protection
2. Policy-Based Lockdown
3. A New Weapon Against False Positives
4. Significantly Improved Performance
5. Unique Endpoint Visibility

... now let's look at each in a little more detail

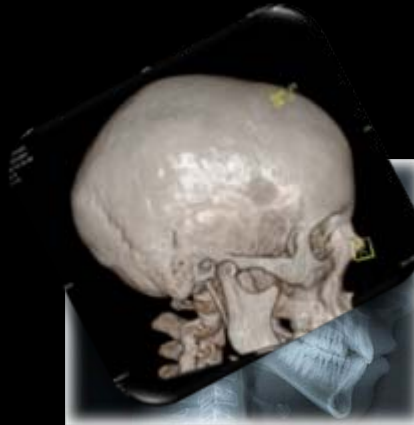
## Feature #1

# Drastically Improved Protection

Our reputation system improves protection in three ways:



- 1 It blocks entirely new malware that traditional fingerprints miss



- 2 It ratchets up the “resolution” of our heuristics and behavior blocking



- 3 It kills targeted and mutated malware, once and for all

— **Let's see why...**

## Feature #1

# Drastically Improved Protection

Attackers mutate millions of new threats to evade fingerprints

- Fingerprint-based systems like Artemis are defenseless!

**B7 93 8F 4C 15 FE ?**

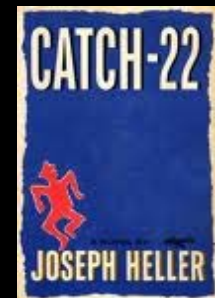
On the other hand, mutated threats stick out like a sore thumb in a reputation system

- Low prevalence + Newly generated = Low reputation!



It's a catch-22 for the virus writers

- Mutate too much = Low reputation
- Mutate too little = Easy to discover & fingerprint



## Feature #2

# Policy-based Lockdown

Traditional AV uses an innocent-until-proven-guilty strategy

- **If a file doesn't match a fingerprint**
  - Your security product assumes it's OK and allows it to run unfettered
  - Unfortunately, most malware falls into this unknown category!



- **But what if you knew that a file had...**



- **Wouldn't you like to dial up protection in these cases?**

## Feature #2

# Policy-based Lockdown

- Allows IT administrators to specify endpoint blocking policies based on their particular risk tolerance



Given that most malware strains are generated on the fly and distributed to less than 20 users, such policies could transform enterprise security!

## Feature #3

# A New Weapon Against False Positives

Reputation reduces false positives in two important ways:



- 1 Our back-end systems check the reputation of every file sent to our labs

Filters legitimate files so that analysts don't inadvertently fingerprint these

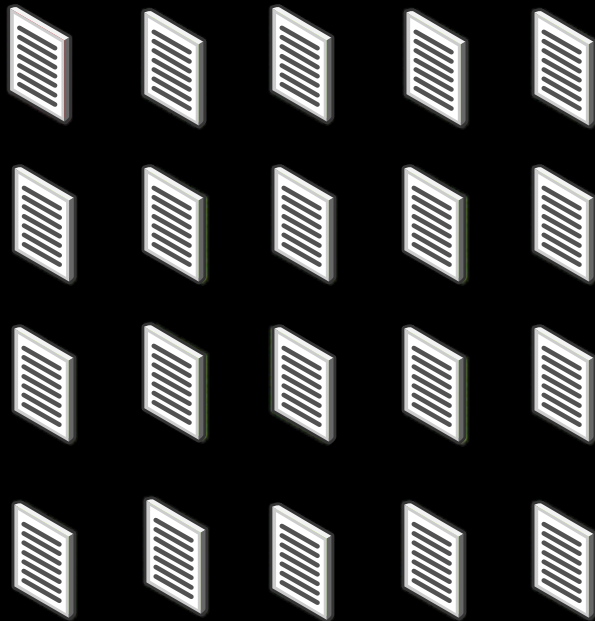
- 2 Our endpoint products consult with reputation before removing suspicious software

Greatly reduces the risk of a high prevalence FP

## Feature #4

# Significantly Improved performance

Latest products use reputation to avoid scanning trusted software!



### Traditional Scanning

Has to scan every file



On a typical system 80% of active applications can be skipped!



### Reputation- Optimized Scanning

Skips any file we are sure is good, leading to much faster scan times



## Use Case #5

# Unique Endpoint Visibility

- Have you ever wanted to understand what's actually running in your environment?
- What if you could
  - Rank order every program in your enterprise by safety, reputation or age
  - And then deploy policies to restrict apps that don't meet your standards



- Incorporate with Application and Device Control
- Investigating these and other use cases with our Altiris team

# Conclusion



## Reputation:

- Game-changing approach to securing end-points
- Leverages data on hundreds of millions of files
- Reduces reliance on signatures
- It amplifies the protection of our current protection technologies
- Shifts the odds in our favor and turns table on malware authors



# Questions?



# Thank you!

John Bai

Senior Manager, Security Technology & Response

[john\\_bai@symantec.com](mailto:john_bai@symantec.com)

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.