



# Why Your AV Solution is Ineffective Against Today's Email-borne Threats

**Greg Leah**

Malware Analyst

Symantec Hosted Services (formerly MessageLabs)

# Motivation

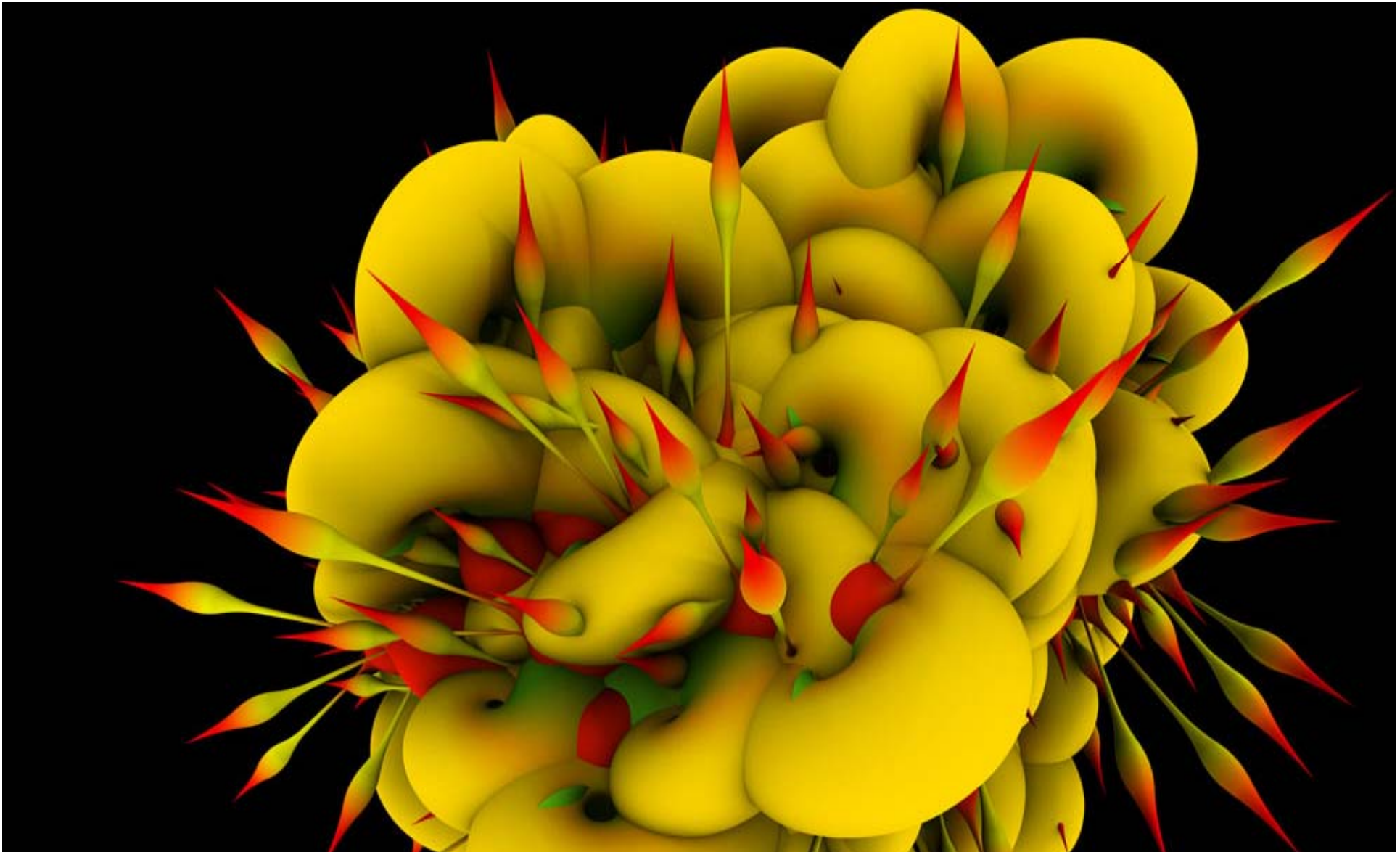
- Many recent high profile attacks on into major software companies, public sector institutions and international organizations
  - Aurora attack on Google and 32 other companies last year
  - All cases: malicious email was sent to victim

# Introduction

- Email-borne threats fall into two general categories:
  - Mass-email attacks
  - Targeted attacks
- Traditional AV increasingly ineffective
- Heuristic engine is necessary

# Skeptic™

- MessageLabs Heuristic Anti-Virus engine
- Deployed as part of our Software-as-a-Service (SaaS) solution across all of our mail towers
- Used to scan customer emails for malicious content



## Bredolab (Trojan.Sasfis)

Your AV Solution is Ineffective...

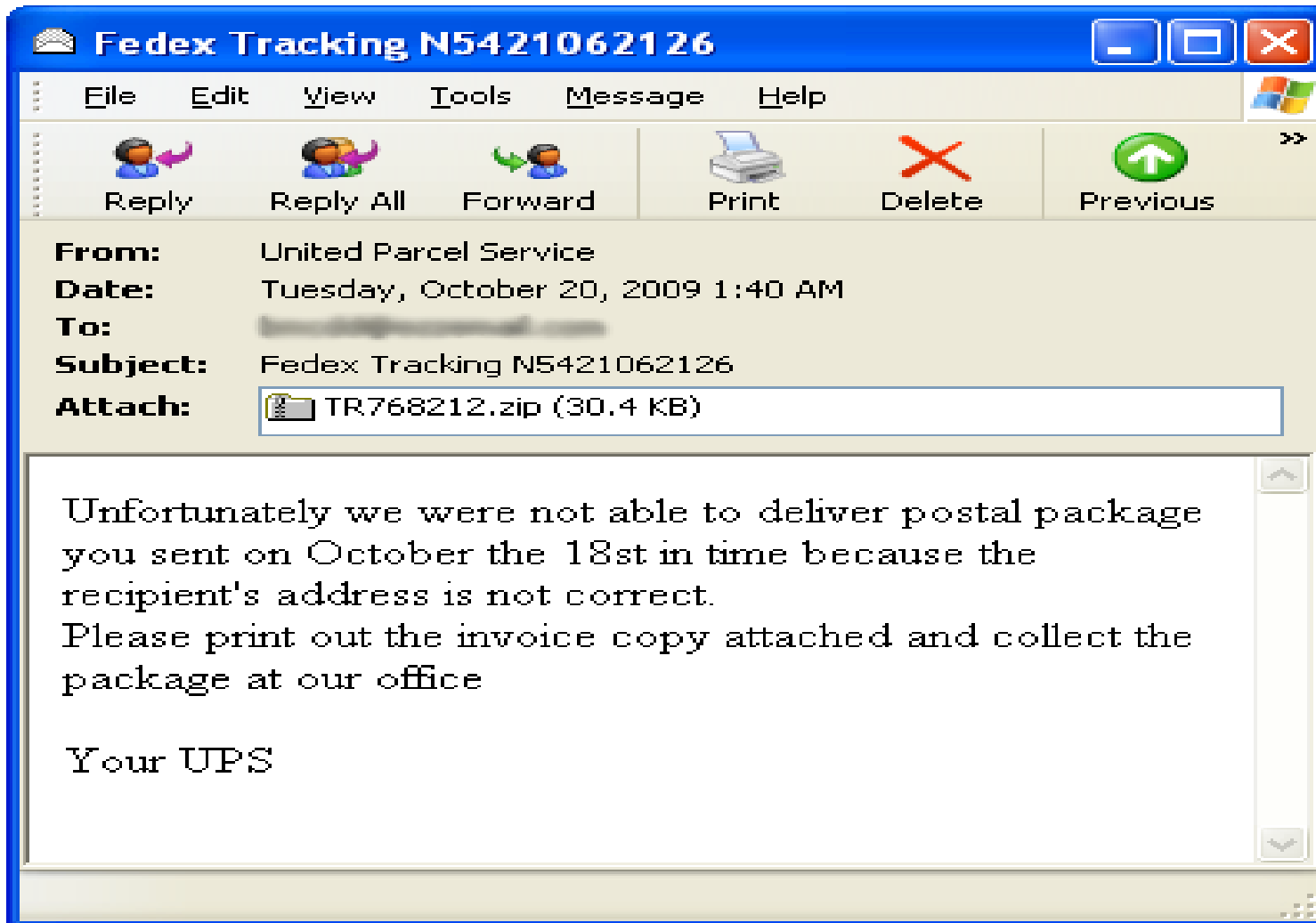
SYMANTEC HOSTED SERVICES™

5

## Bredolab/Trojan.Sasfis

- Most prolific family of mass-mailed threats
- Mass email attacks with executable attachment
- Social engineering lures:
  - *Facebook password reset*
  - *Western Union or UPS invoice*
  - ‘You have received an E-Card!’

# Typical Bredolab Email

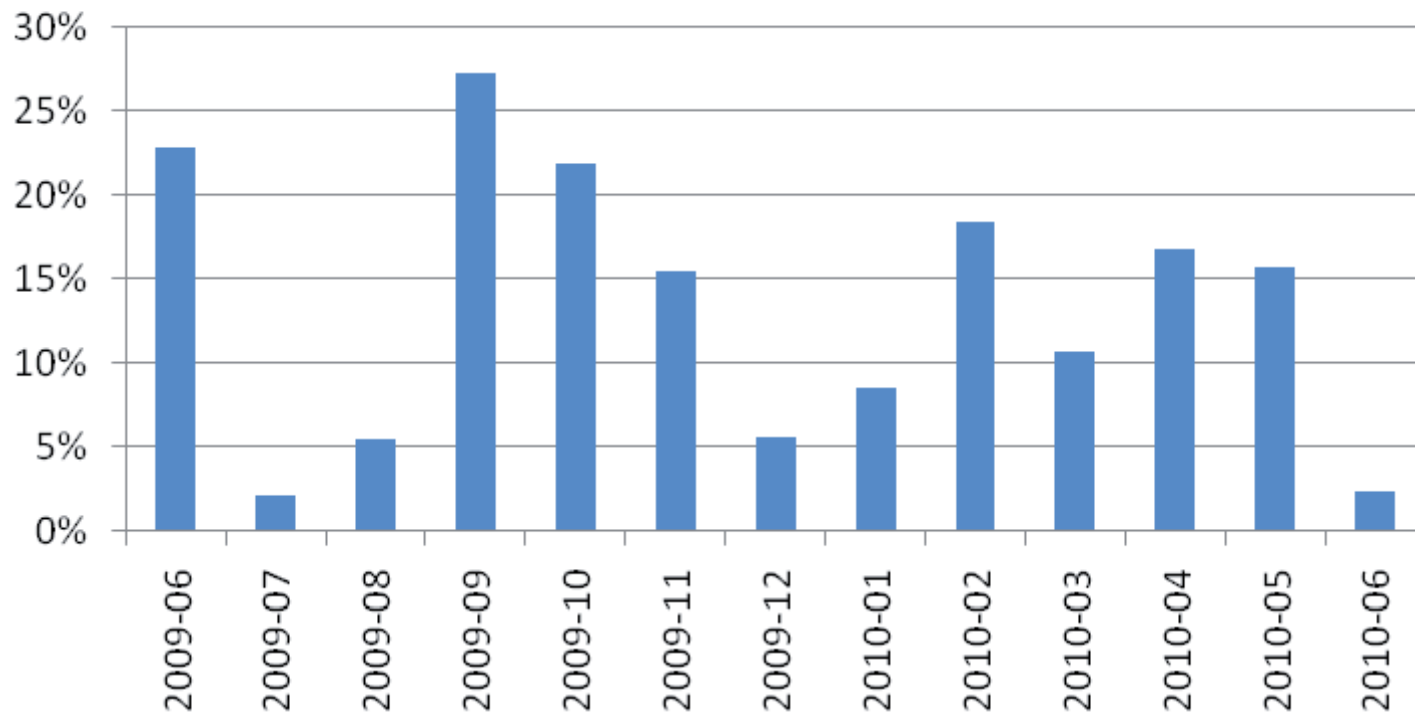


## Some Bredolab Details

- Spammed out in very large numbers
  - Cutwail botnet
- Many different payloads
- 13.3% of all Malware stopped by Skeptic
  - between June 2009 and June 2010 (excluding Phish and links)
- Typically low AV detection (< 10 on VT)



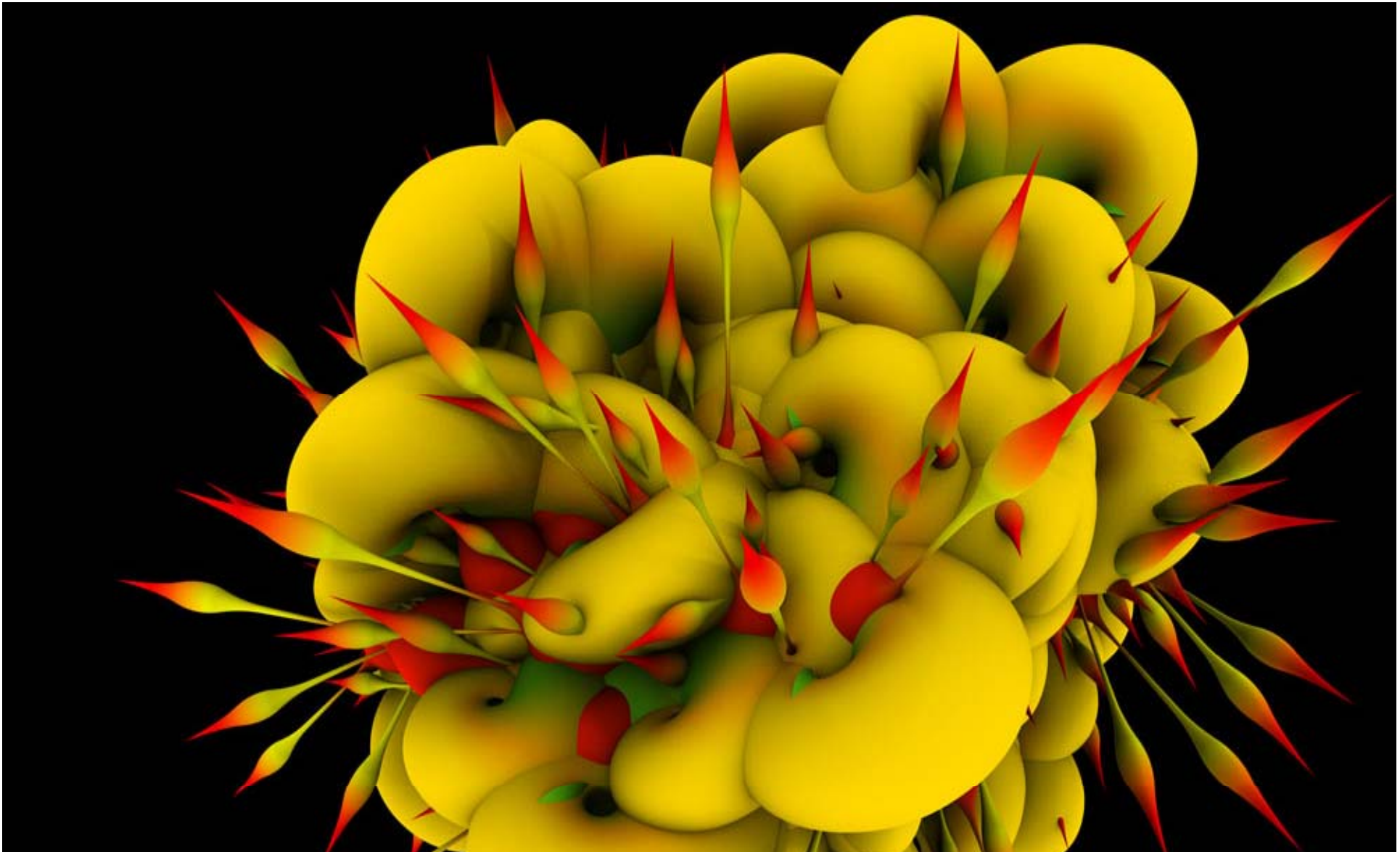
## Bredolab: % of Malware



## Bredolab Effectiveness

- Good social engineering tactics
  - Use of Word or Excel icons
  - Spoof prolific companies
    - Facebook, UPS, Fedex
- Heavy use of **server-side polymorphism (SSP)** to evade signature-based AV
- High volume





## Signature- vs. Heuristic-Based Detection

Your AV Solution is Ineffective...

SYMANTEC HOSTED SERVICES™

11

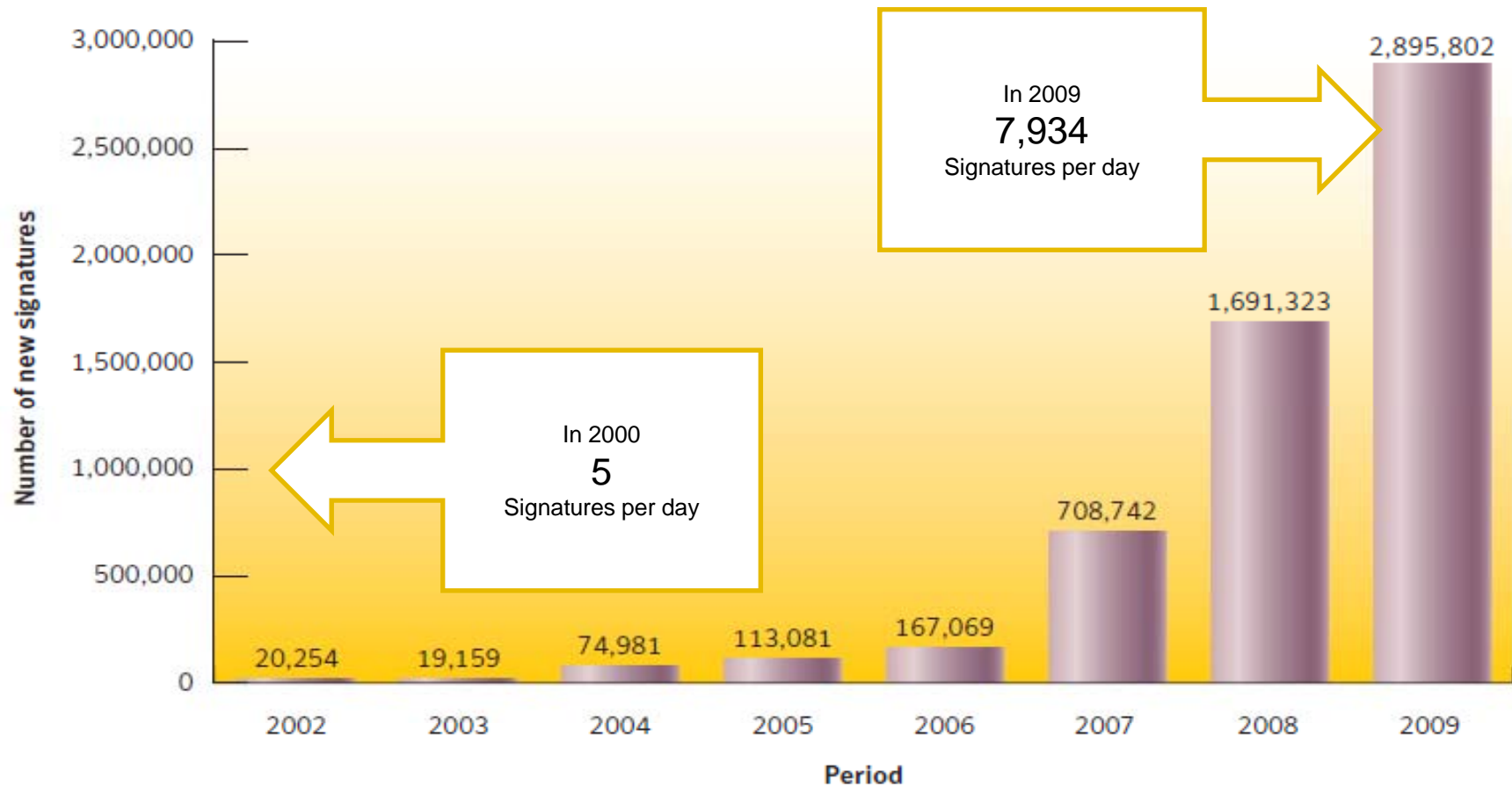
## Signature-based AV

- Create a “signature” for a piece of Malware
- String(s) of bytes
- Checksum(s)
- Very specific

## Signatures – by the numbers

- Evidence of increased use of SSP
- In 2008, Symantec created 1,691,323 new malicious code signatures
- In 2009, 2,895,802 new signatures were created
  - 71% increase!
- 139% increase from 2007 to 2008
- **Not sustainable!**
- Solution: heuristic-based approach

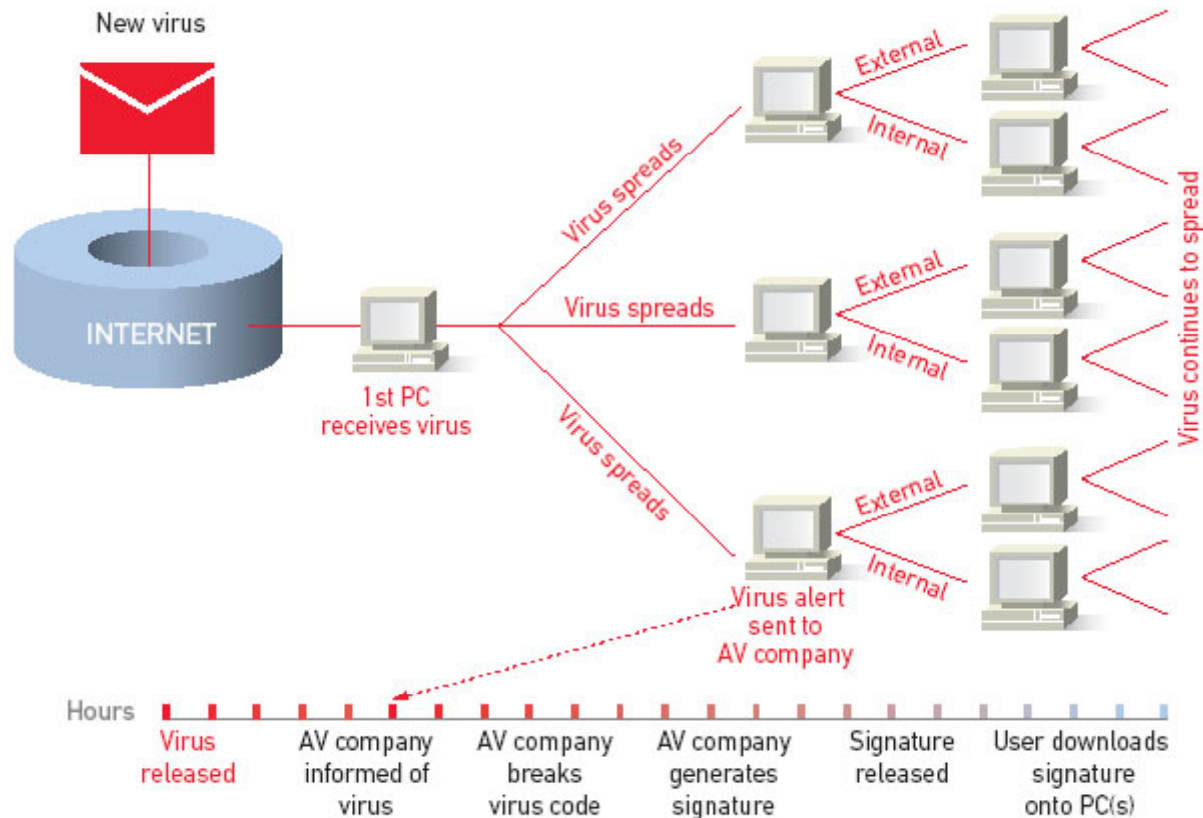
# Signatures released per year rapidly increasing



Total: 5,724,106

# Signature development process

How traditional anti-virus software works



Your AV Solution is Ineffective...

SYMANTEC HOSTED SERVICES™

## Signatures - shortcomings

- Reactionary
- 1-1 correlation
- Time consuming
  - Sample -> analysis -> sig -> deploy
    - takes around an hour in the absolute best case
  - Data on this later

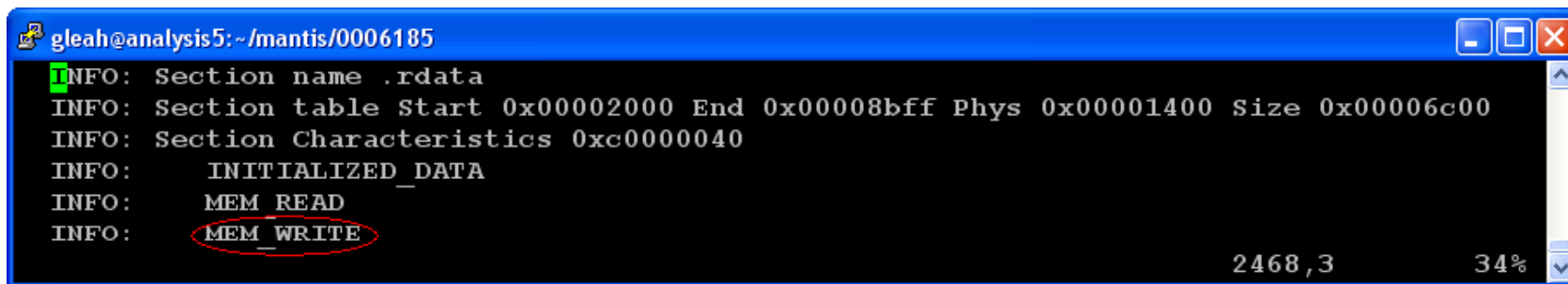


## Heuristic-based approach

- Generic detection
- Features known to exist in Malware
- Decision based on extracted features
- Weighted
- Cloud based
  - no reactive signature deployment delays

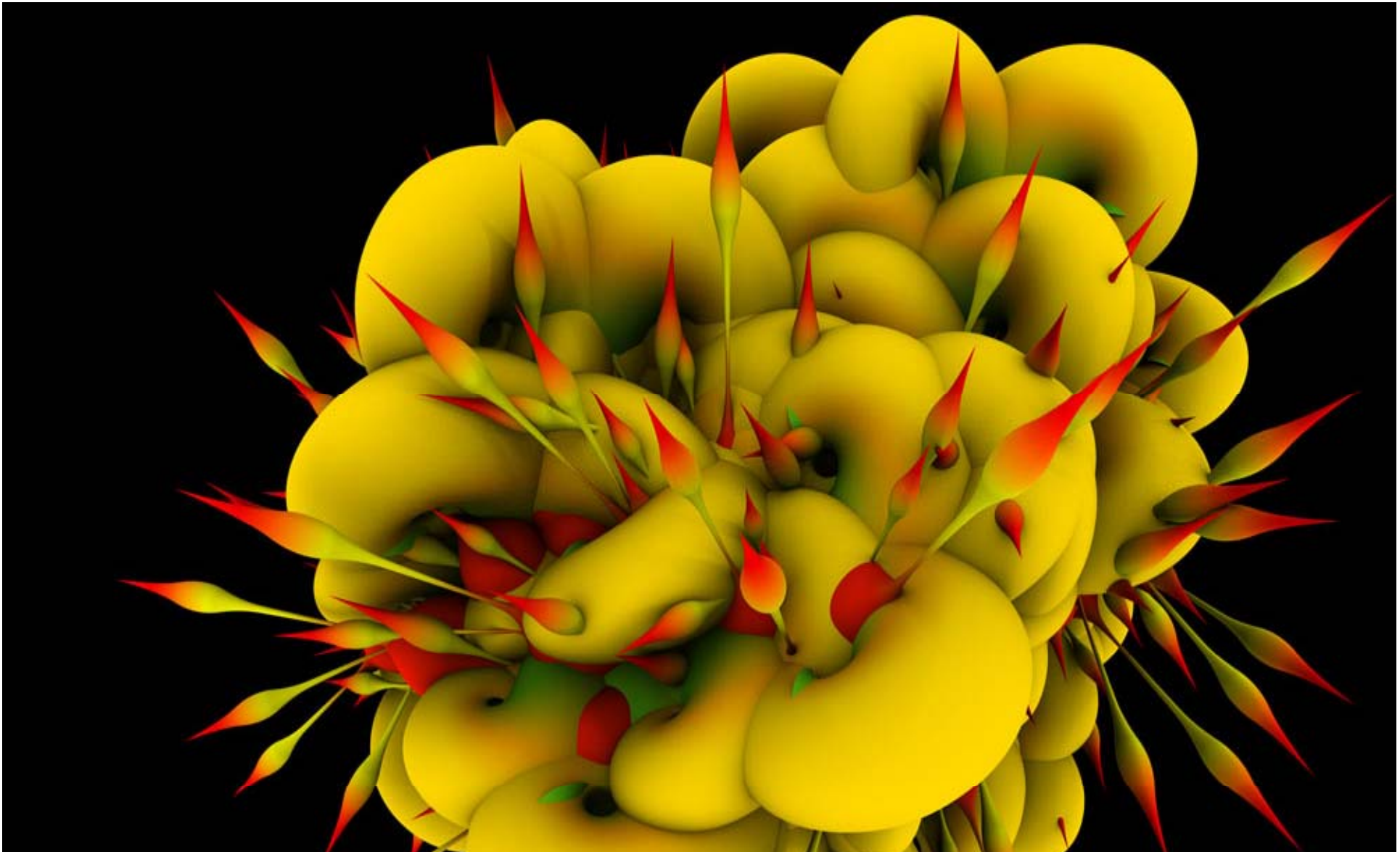
# Heuristic examples

- Writable .rdata section (read-only data)
  - rarely will happen in clean files or – strong heuristic



```
gleah@analysis5: ~/mantis/0006185
INFO: Section name .rdata
INFO: Section table Start 0x00002000 End 0x00008bff Phys 0x00001400 Size 0x00006c00
INFO: Section Characteristics 0xc0000040
INFO:     INITIALIZED_DATA
INFO:     MEM_READ
INFO:     MEM_WRITE
2468,3 34%
```

- Calls IsDebuggerPresent()
  - happens all the time in clean files – weak heuristic



## Server-side Polymorphism

Your AV Solution is Ineffective...

SYMANTEC HOSTED SERVICES™

19

“ [Viruses that] can mutate its decryptor to a high number of different instances ”

*Peter Szor*

# Polymorphic Viruses

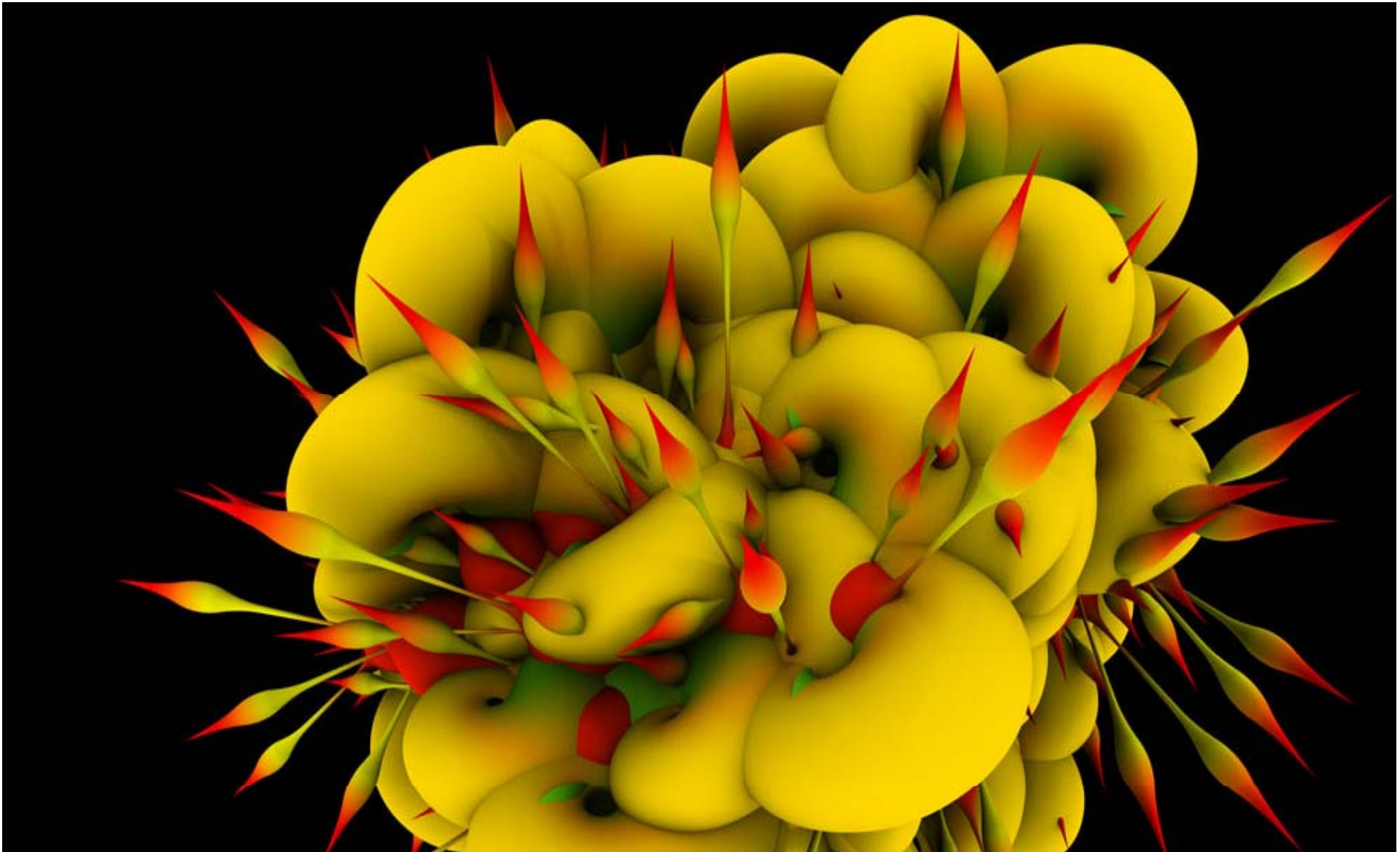
- Big problem for AV
  - Many different variants
  - Functionally equivalent
  - Signatures required for each variant
- Solution: emulation
  - Emulate past decryptor stub
  - Sig the static virus body

# Server-side polymorphism (SSP)

- Custom encryption routine
  - Decrypt at runtime
- Generated by a polymorphic engine
- Hundreds or perhaps thousands of unique variants
- Random junk instructions
  - API calls
  - Arithmetic
  - EP

## Use in mass-email attacks

- Attackers generate a number of unique binaries
- Change the binary being spammed throughout the attack
- Problem for any vendor without proactive protection in place



## Bredolab Case Study

Your AV Solution is Ineffective...

SYMANTEC HOSTED SERVICES™

24

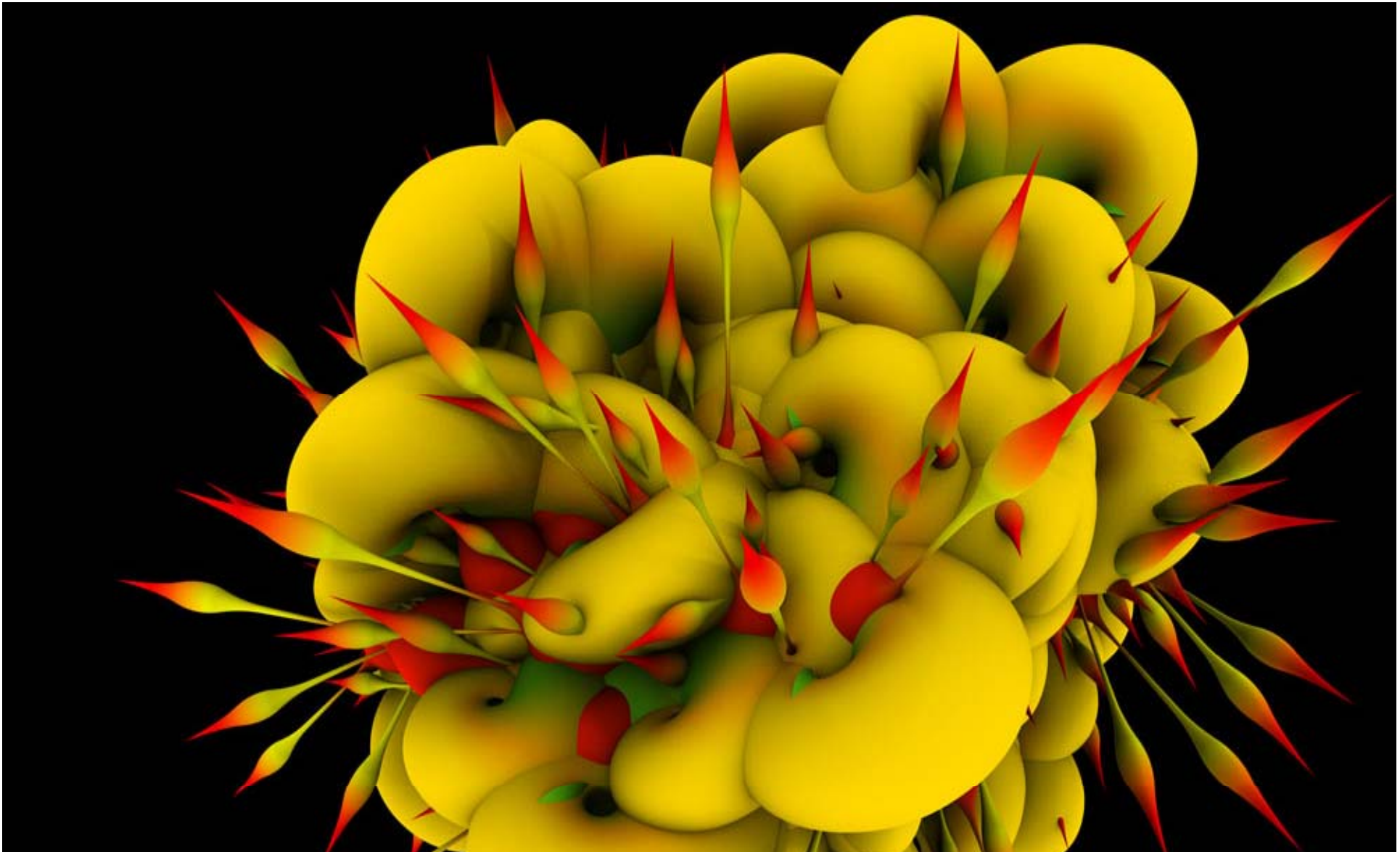


## Bredolab Case Study – 30 March 2010

- Standard Bredolab run:
  - Subject: variation of ‘UPS Delivery Problem NR 18800’
  - Attachment: similarly named ‘UPS\_invoice\_1845.exe’
  - relatively small (only 56 observed copies)
- Started at 19:08:33 GMT (time 0)
- Last observed sample at 19:36:31
  - total of 27 min 59s

## Case Study - AV Detection & Response Time

- At time 0, AV detection was 0
- Average response time?
  - 661 minutes (11 hours and 1 minute) !!!
- Remember that the attack only lasted 28 mins...
- This is the **average** response time
- INEFFECTIVE



## Aurora and Targeted Attacks (Spear-Phishing)

Your AV Solution is Ineffective...

SYMANTEC HOSTED SERVICES™

27

“ [Google was the victim of] a highly sophisticated and targeted attack’ on its corporate infrastructure on 12 January 2010 ”

*David Drummond, Senior Vice  
President of Corporate  
Development and Chief Legal  
Officer, Google*

## Aurora/Hydraq

- Up to 34 different companies compromised in same period using similar techniques
  - Email links to malicious web pages
  - Flaws in Adobe Acrobat Reader
- Google hackers are back?
  - CVE-2010-2883



“ 102 breaches of the Pentagon’s agencies, partners and contractors in a two-year period ending August 2009 ”

*Steve Shirley, Director, US  
Department of Defense Cyber  
Crime Center*

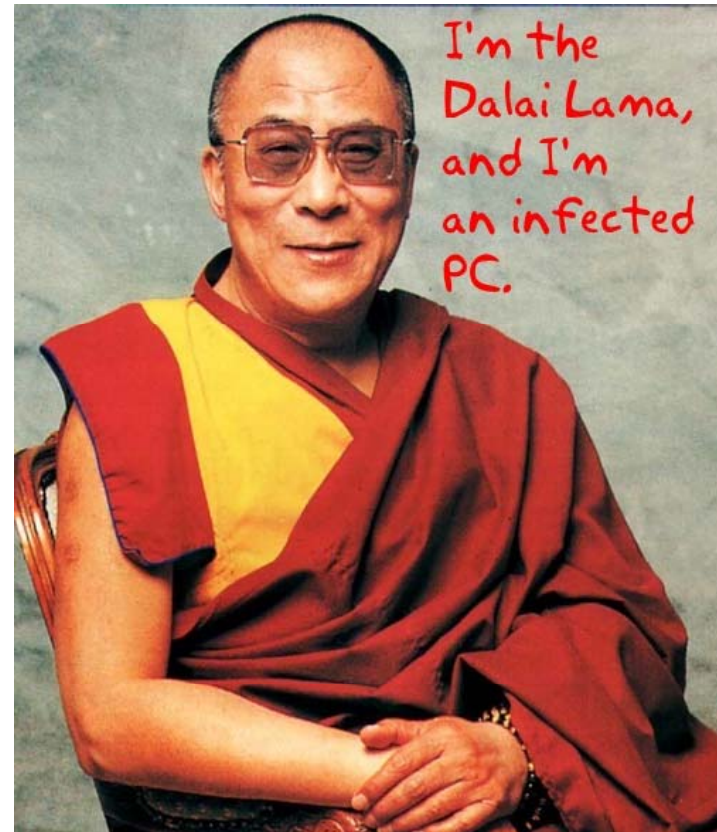
## Other High Profile Targeted Attacks - Pentagon

- Targeted emails with malicious attachments
- Vulnerabilities in unpatched software



## Other High Profile Targeted Attacks - *Ghostnet*

- Cyber espionage ring discovered by mostly Canadian researchers from UofT
- Infected at least 1,295 computers in 103 countries
  - Close to 30% could be considered high-value diplomatic, political, economic and military targets
- Dalai Lama & other Tibetan targets



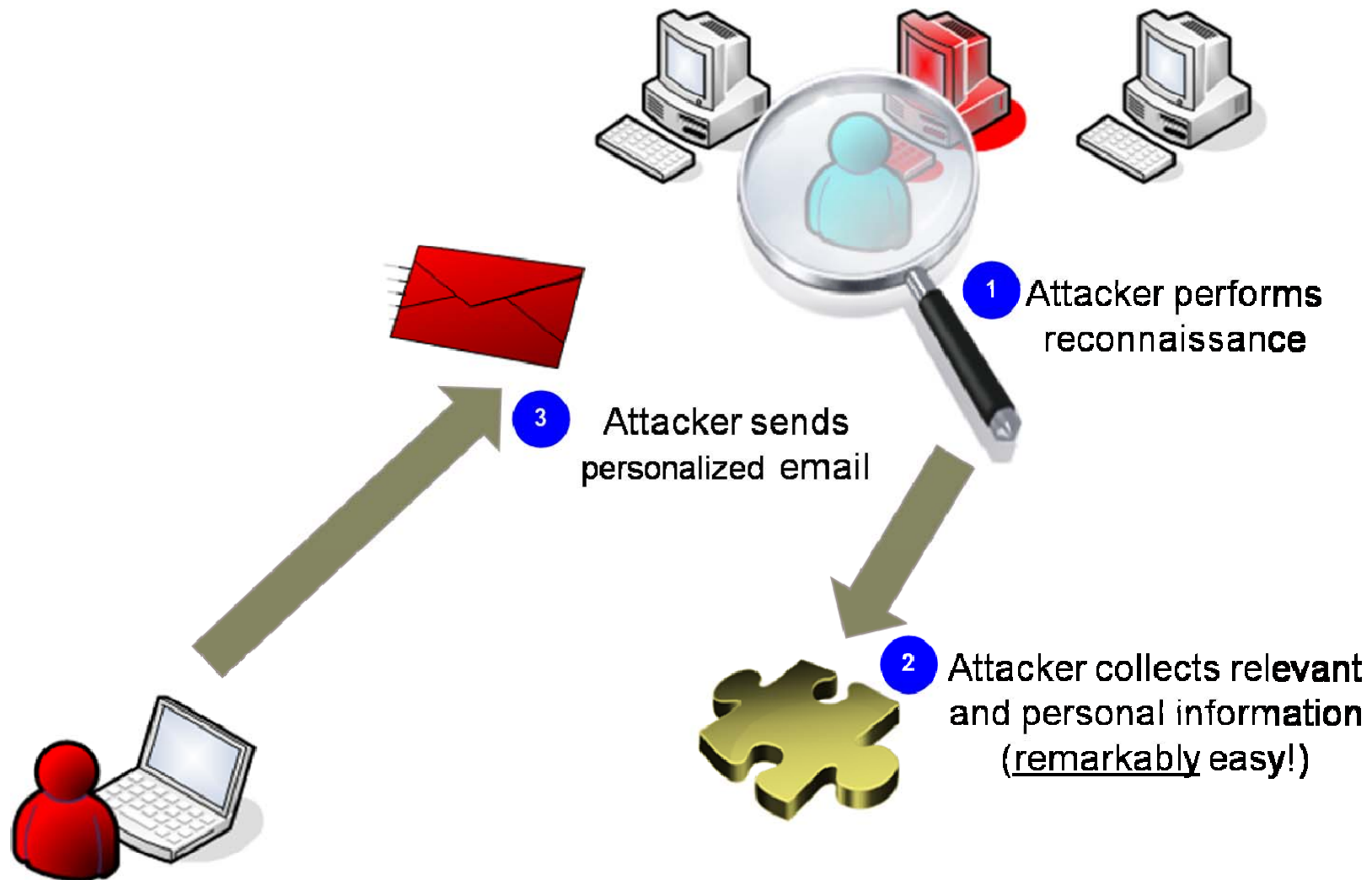


# Targeted Attacks - Motivation

- Aurora/Hydraq
  - Access Gmail accounts
  - Pilfer source code, defense technology and other intellectual property
- In general:
  - Exfiltration of sensitive information



# Targeted Attack - Illustration

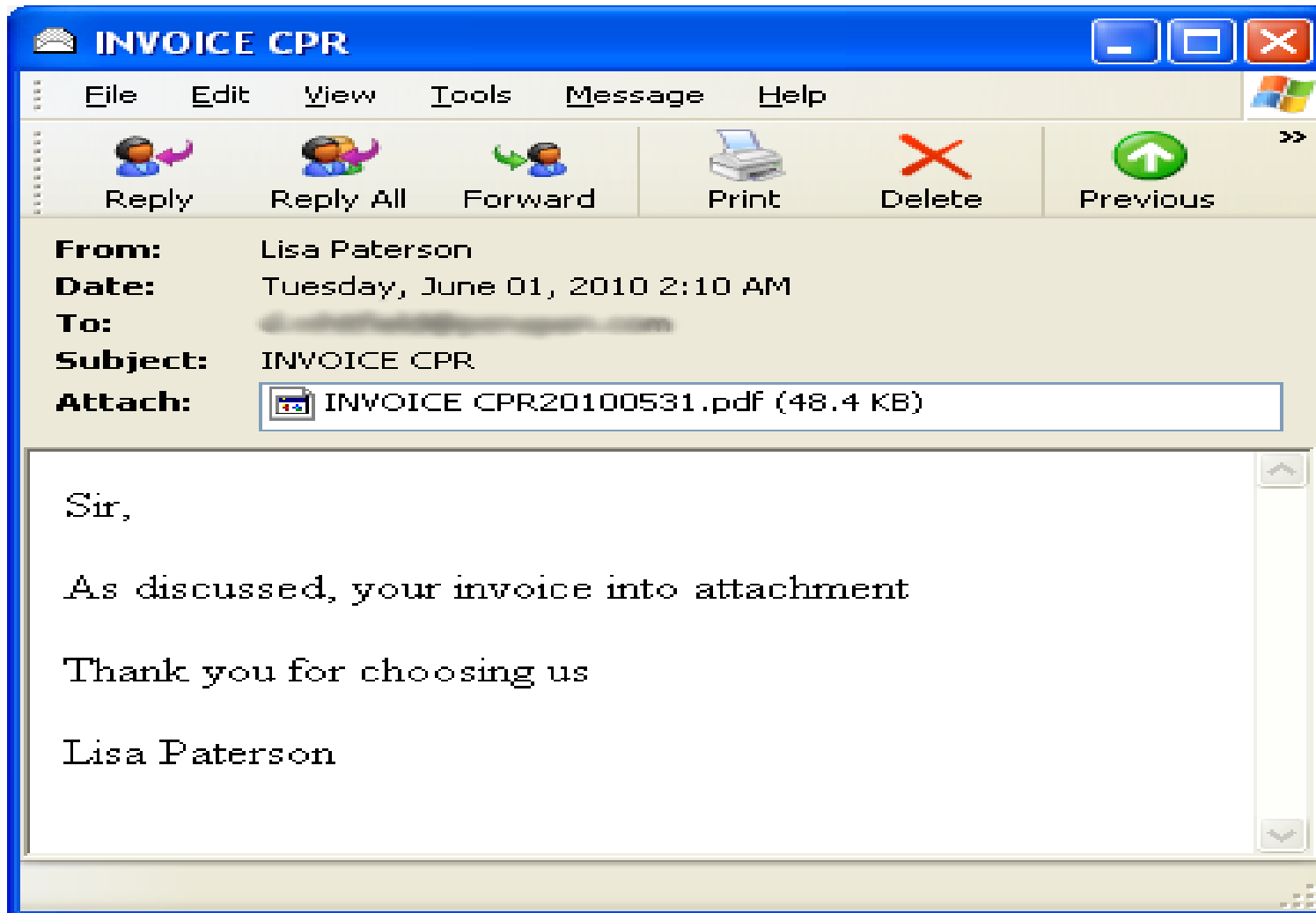


# Effectiveness of Targeted Attacks

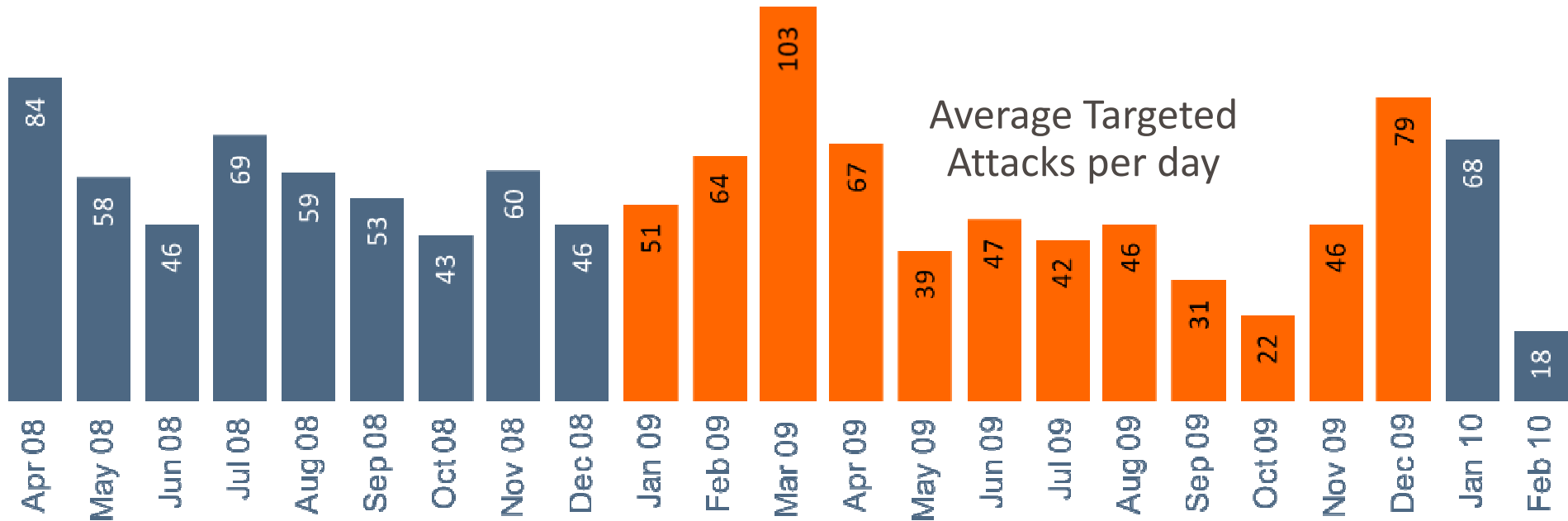
- 'Innocent' file formats
  - .doc, .xls, .ppt, .pdf
- Passive reconnaissance
  - Public websites
  - Social networks
- Sophisticated social engineering
  - “Invoice” email to Accounting department
  - Newsworthy events
- Sent in very low numbers to ‘fly in under the radar’



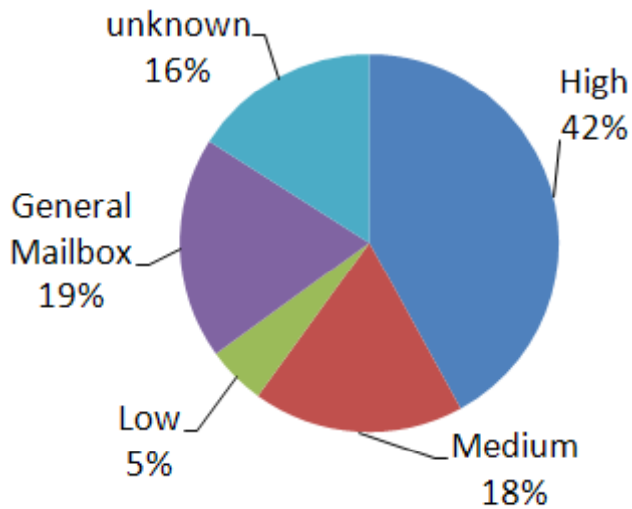
# Targeted Email Example



# Low Volume, Highly Damaging



## Seniority of Target



- Of around 500,000 malicious emails blocked per day, typically <100 targeted attacks per day
- 60% of recipients are of a high/medium seniority
- Watch out Public Sector.... 34% of all attacks

## Targeted Attack Case Study – 24 March 2010

- Targeted attack blocked attempting to exploit CVE-2010-0188 (libTiff)
- Single copy sent to an individual in a major international organization
  - Co-ordinates governments from around the world
- Trojanized a clean PDF from a World Cup travel site

## Case Study - AV Detection & Response Time

- AV detection was 0
- One week later, AV detection at **33%**
  - Sample sharing, blogged
- Average response time?
  - **3631 minutes (two and a half days) !!!**
- Only takes into account the 33% of vendors that were actually detecting the threat
- INEFFECTIVE

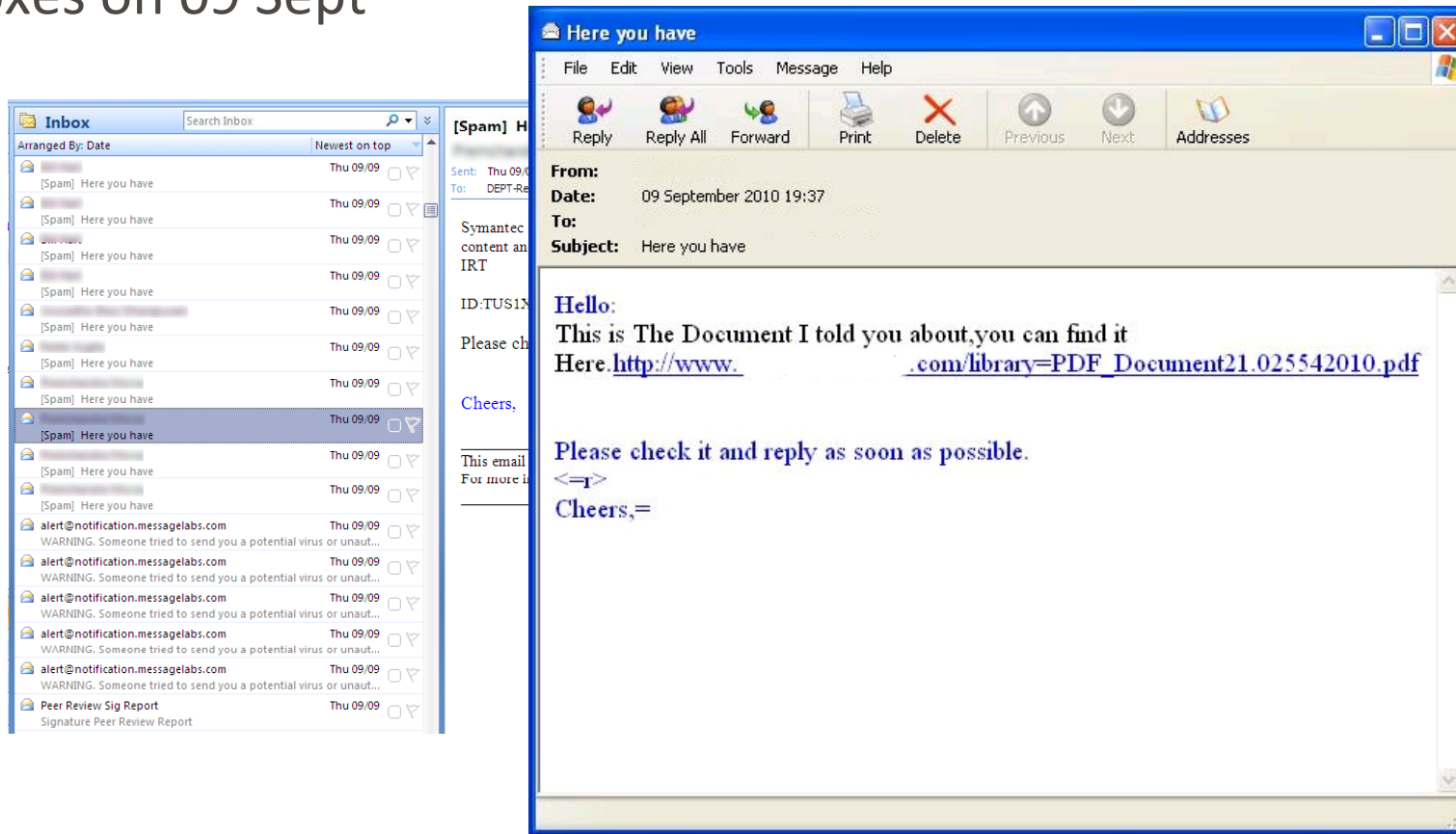
## Oday Example of Heuristic Effectiveness: CVE-2009-4324 (Doc.media.newPlayer)

- Announced 14 December 2009
- Patched 12 January 2010
- First known attack using this vulnerability was blocked on *MessageLabs'* infrastructure on 20 November 2009
  - LONG before the attack was made public
- Blocked based on shellcode and presence of encrypted executables



# Imsoik.B “Here you have”

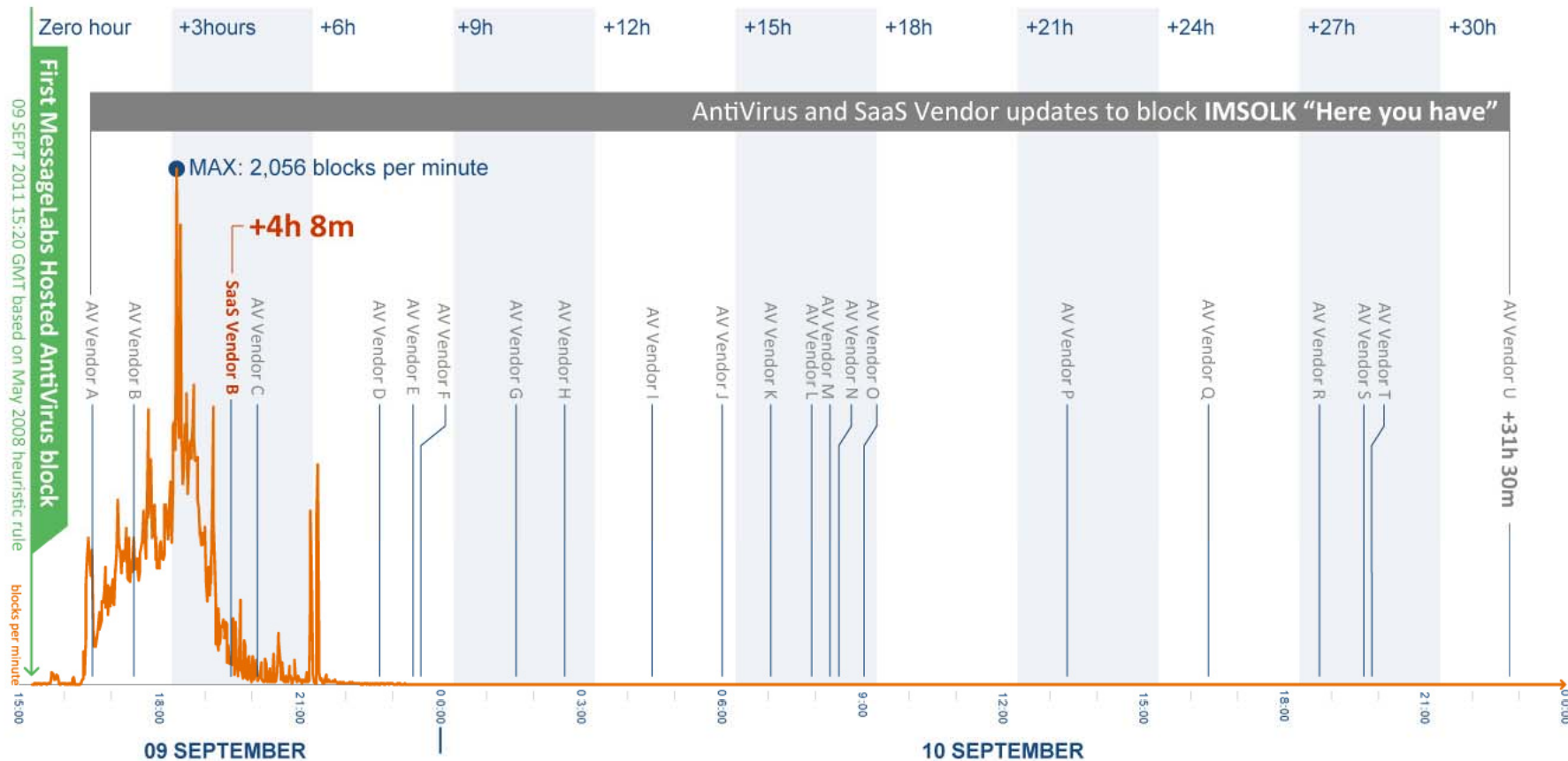
- Many business users likely saw something like this in their inboxes on 09 Sept



## Heuristic effectiveness vs. Imsolk.B

- All copies of the Imsolk.B mass mailer worm were stopped
- Heuristic in place since May 2008
- While a few AV solutions stopped the worm at zero-hour the – up to 31 hours later

# Window of vulnerability: Imsolk.B “Here you have” worm



Source: Outbreak graph Symantec Hosted Services; AV Signature times as reported by AVTest.org; SaaS vendor time via vendor site Note: All times GMT

Your AV Solution is Ineffective...

SYMANTEC HOSTED SERVICES

43

# Conclusion

- Heuristics > Signatures



# Thank you!

Greg Leah


[gleah@messagelabs.com](mailto:gleah@messagelabs.com)

416-774-0275

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.

# Bredolab Variants

**From:** SLP Ltd.  
**Date:** 19 August 2008 07:42  
**To:** [REDACTED]  
**Subject:** Open an account  
**Attach:**  contract\_2.zip (231 bytes)

Good afternoon,  
We have prepared a contract and added the paragraphs that you wanted to see in it.  
Our lawyers made alterations on the last page. If you agree with all the provisions we are ready to make the payment on Friday for the first consignment.  
We are enclosing the file with the prepared contract.

If necessary, we can send it by fax.  
Looking forward to your decision.

AUGUST 2008