Metrics@Google

John “Four” Flynn and Steve Weis

Security@Google

- Who are we?
- Secops
- ISE
- Appsec
- Safebrowsing
  - Anti-phishing
  - Anti-malware

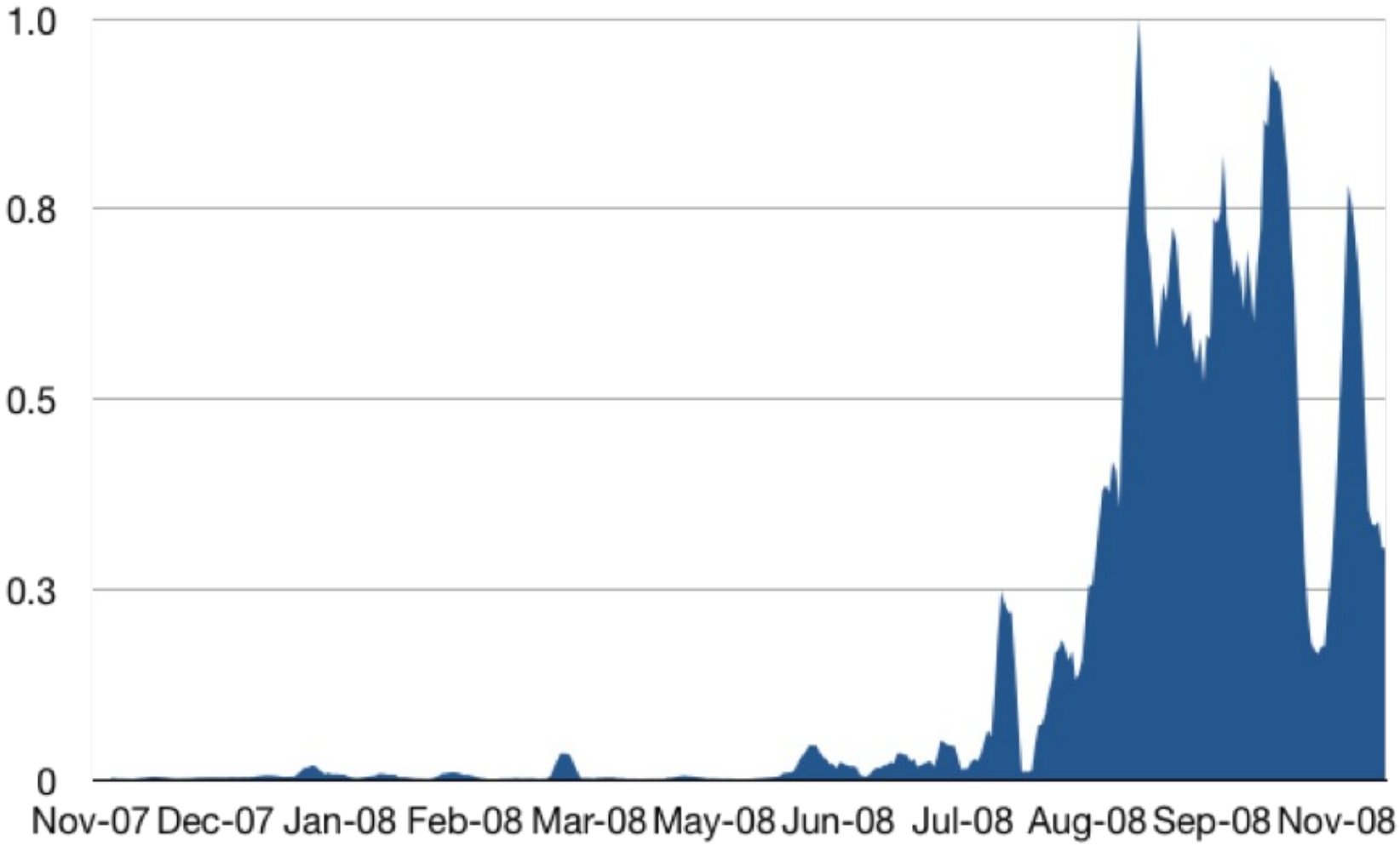
Security Metrics Motivation

- Google is highly data driven
- “How do I determine where to spend effort?”
- “How do we measure our value to our organization?”
- “How can we take a more quantitative approach to security?”

About the Data

- All internal data are normalized on a 0-1 scale
- All data are 7-day moving averages
- The maximum value over the time period is a 1
- When comparing two trends, we will explain the difference in scale verbally and in slide notes.
- This is a presentation of long-term observed trends with limited analysis.

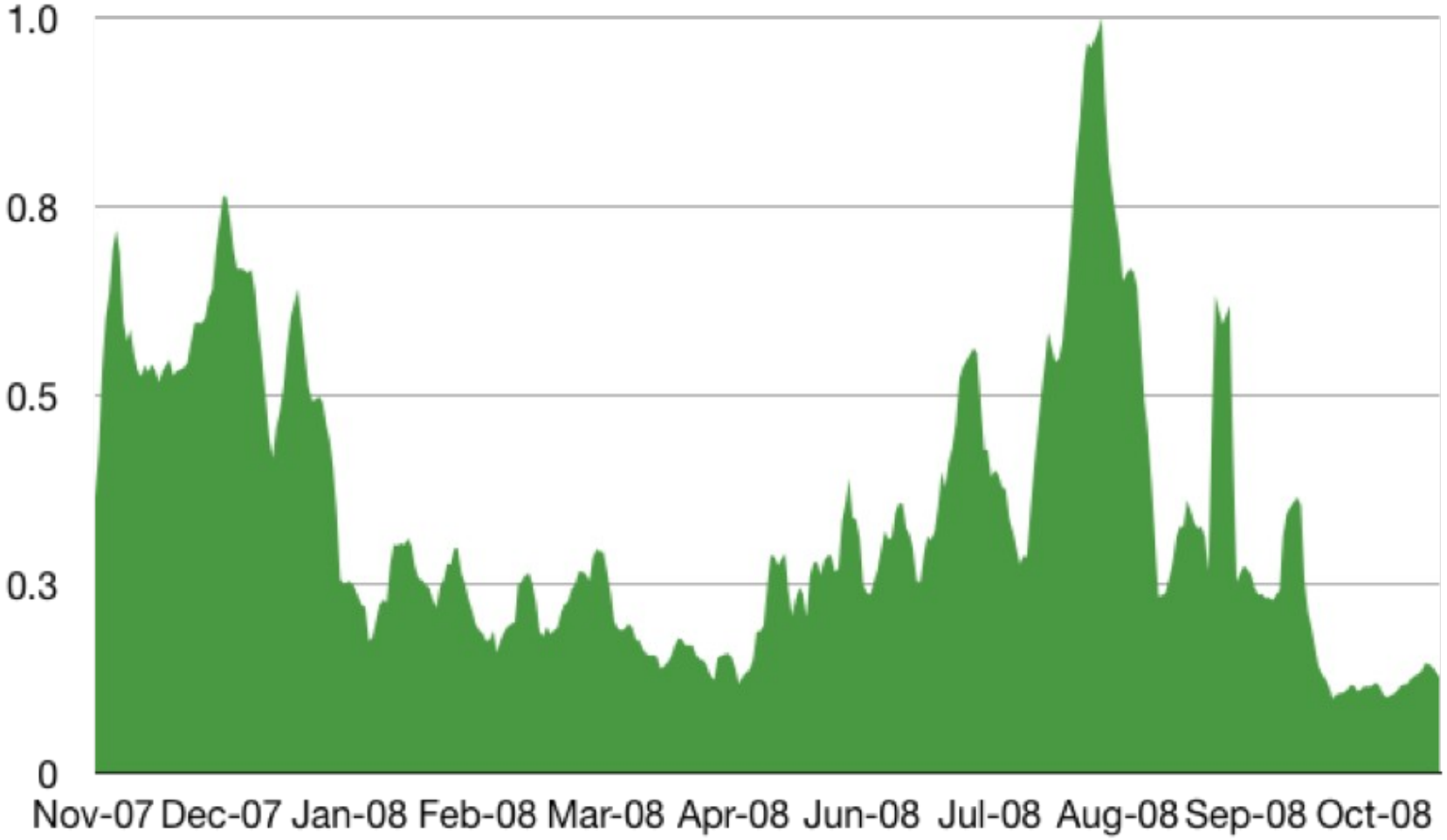
Suspected Account Hijack Signals



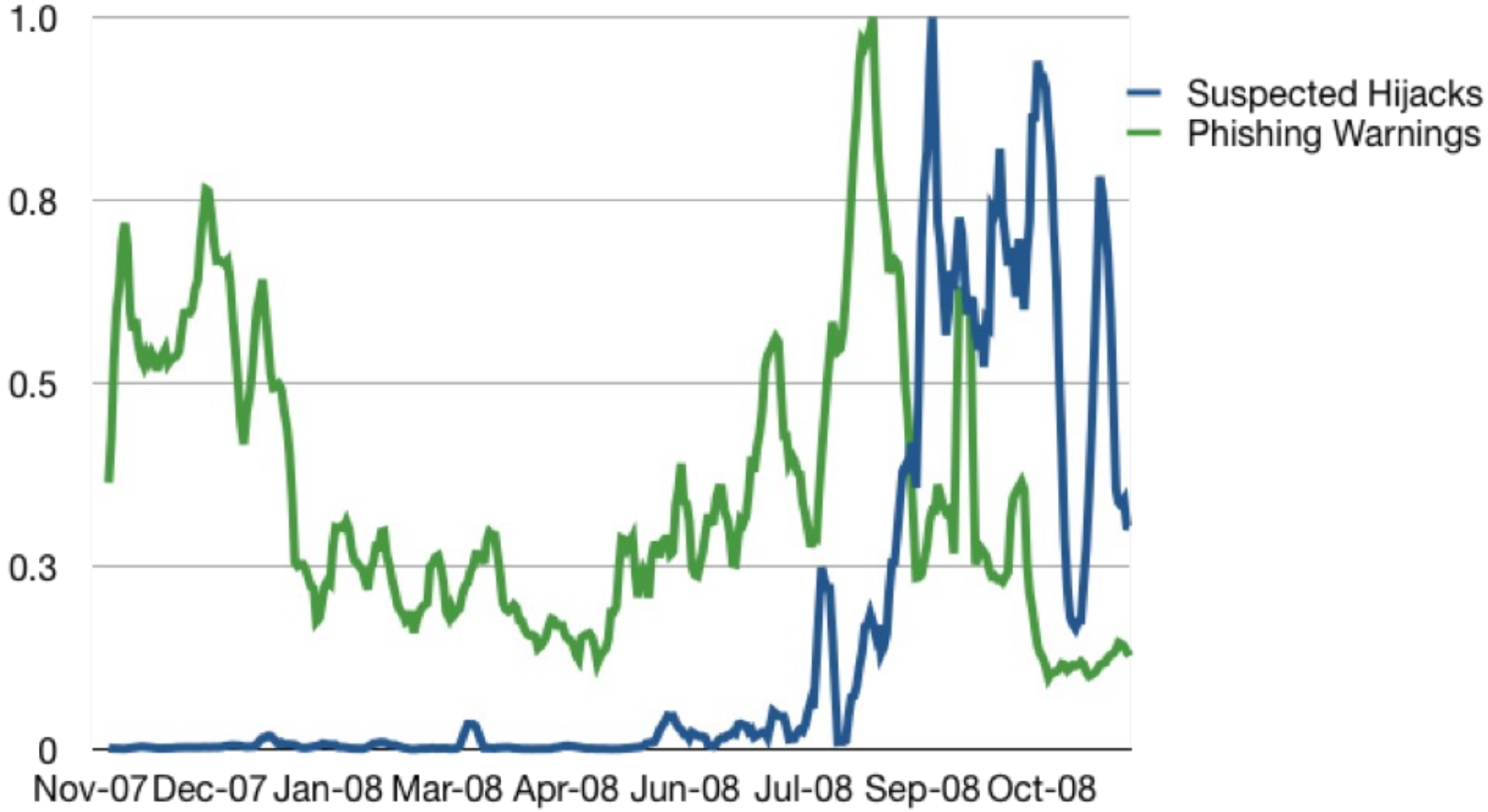
Anti-phishing

- Automated system to find phishy sites on the web

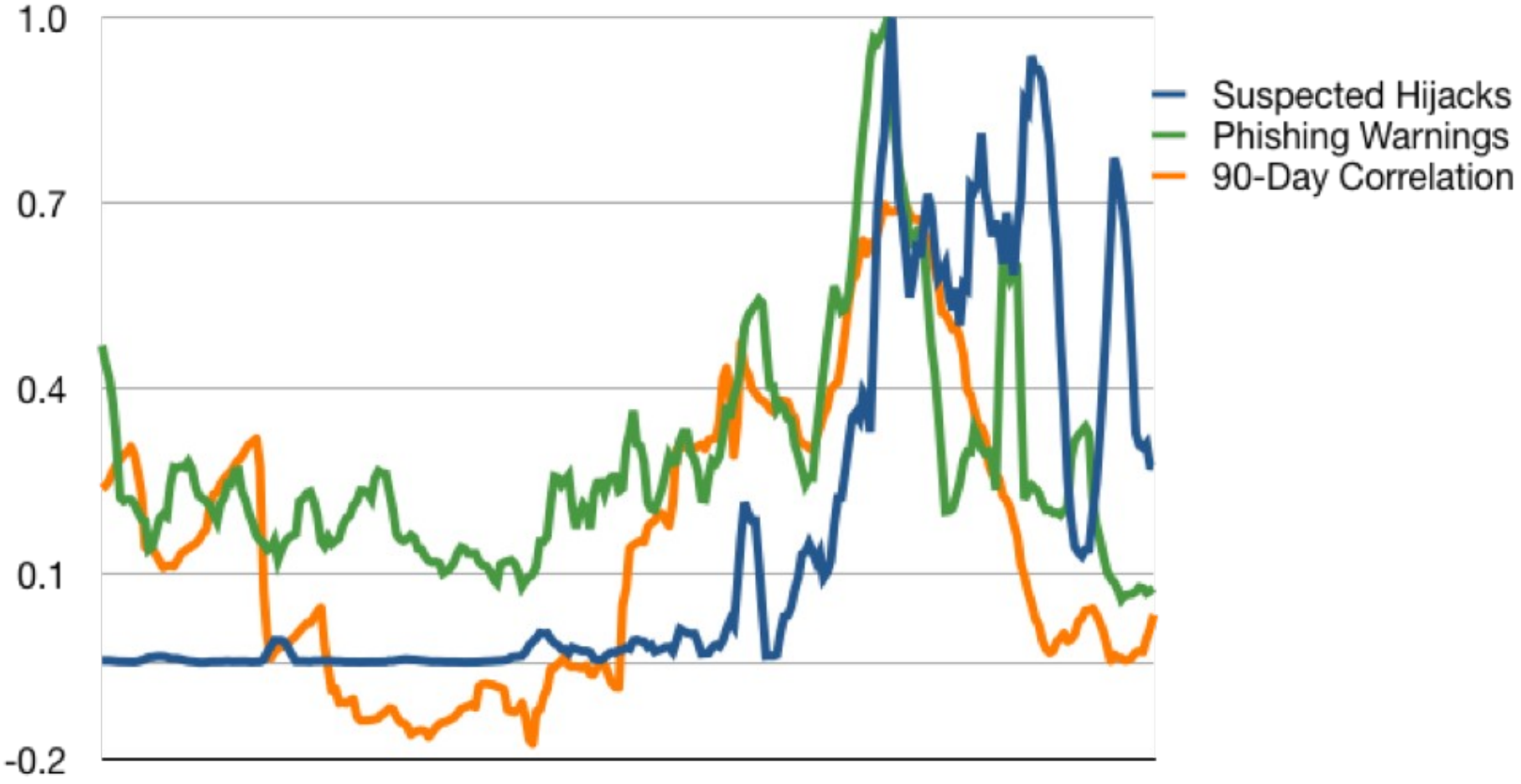
Phishing Warnings Displayed



Hijack and Phishing Comparison

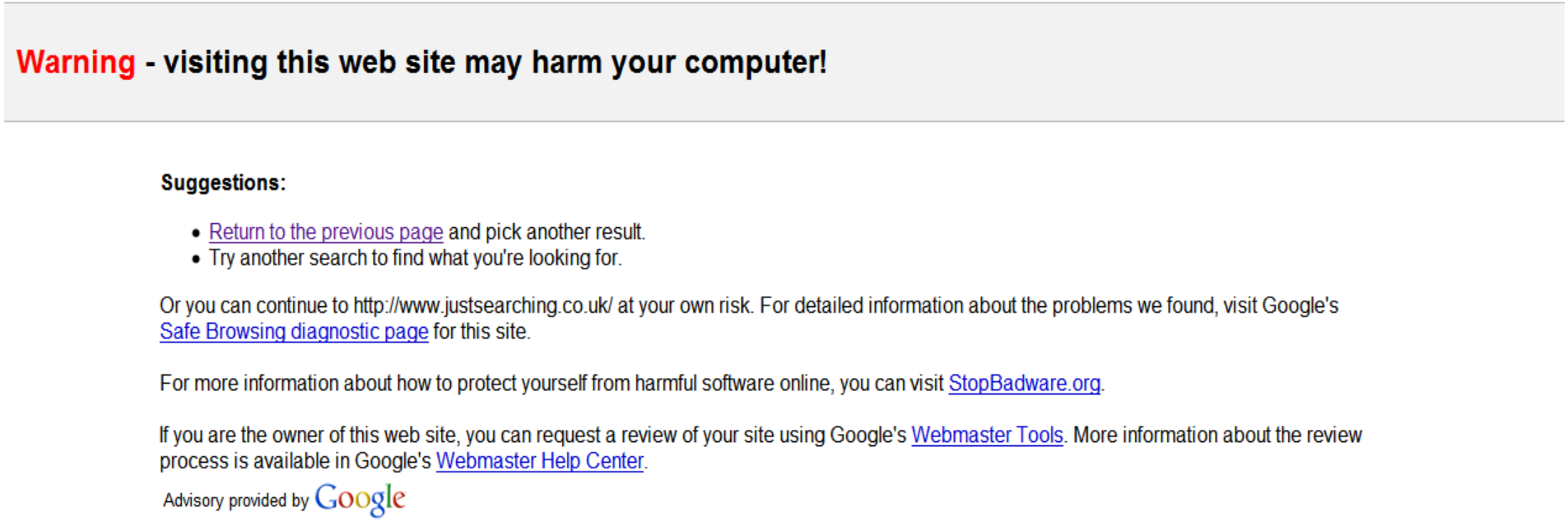


Time-Shifted Correlation

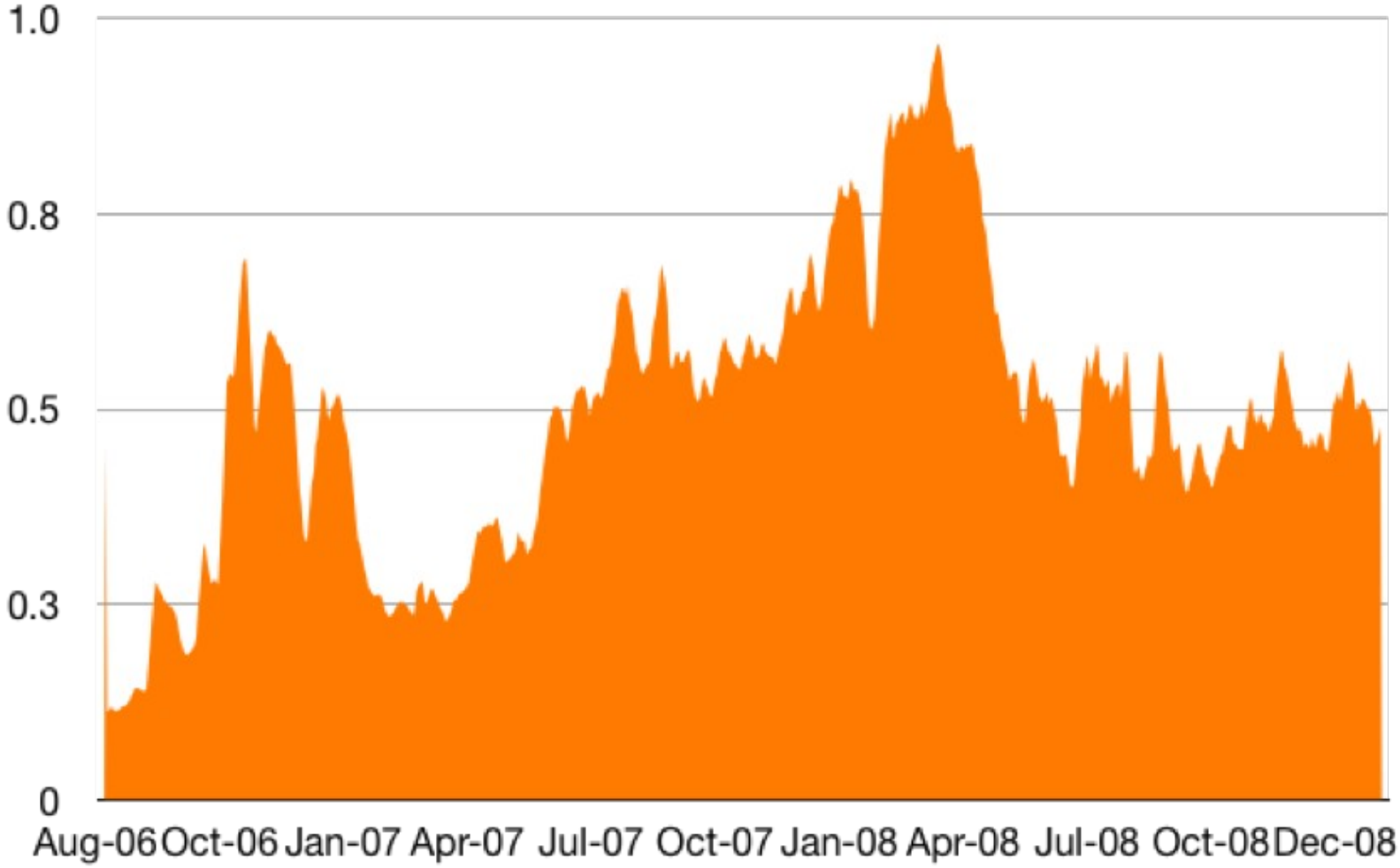


Anti-malware

- Ghost in the browser
- Automated analysis to find malicious sites

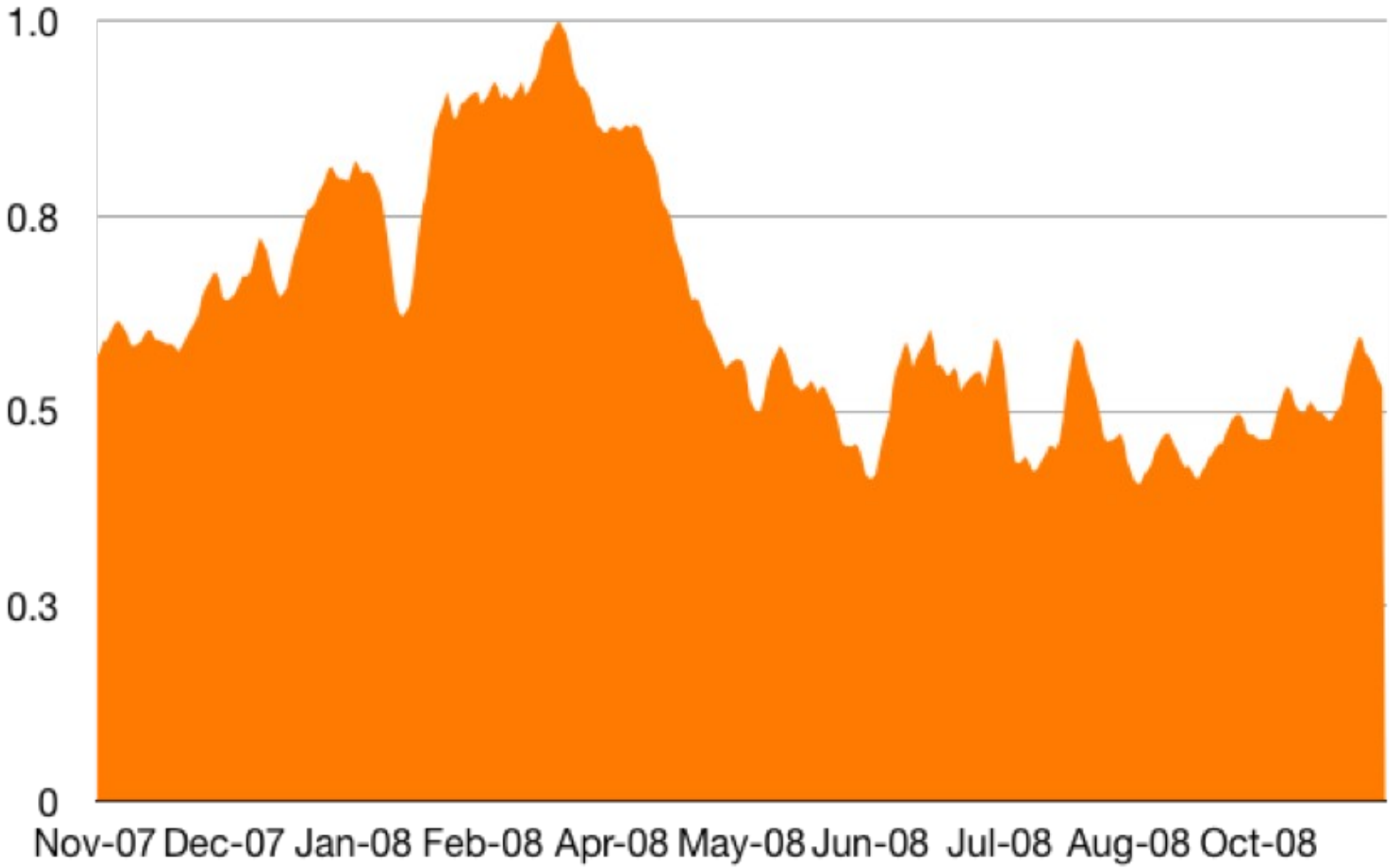


Malware Impressions 2006-2009



Malware Warnings Gone Wrong

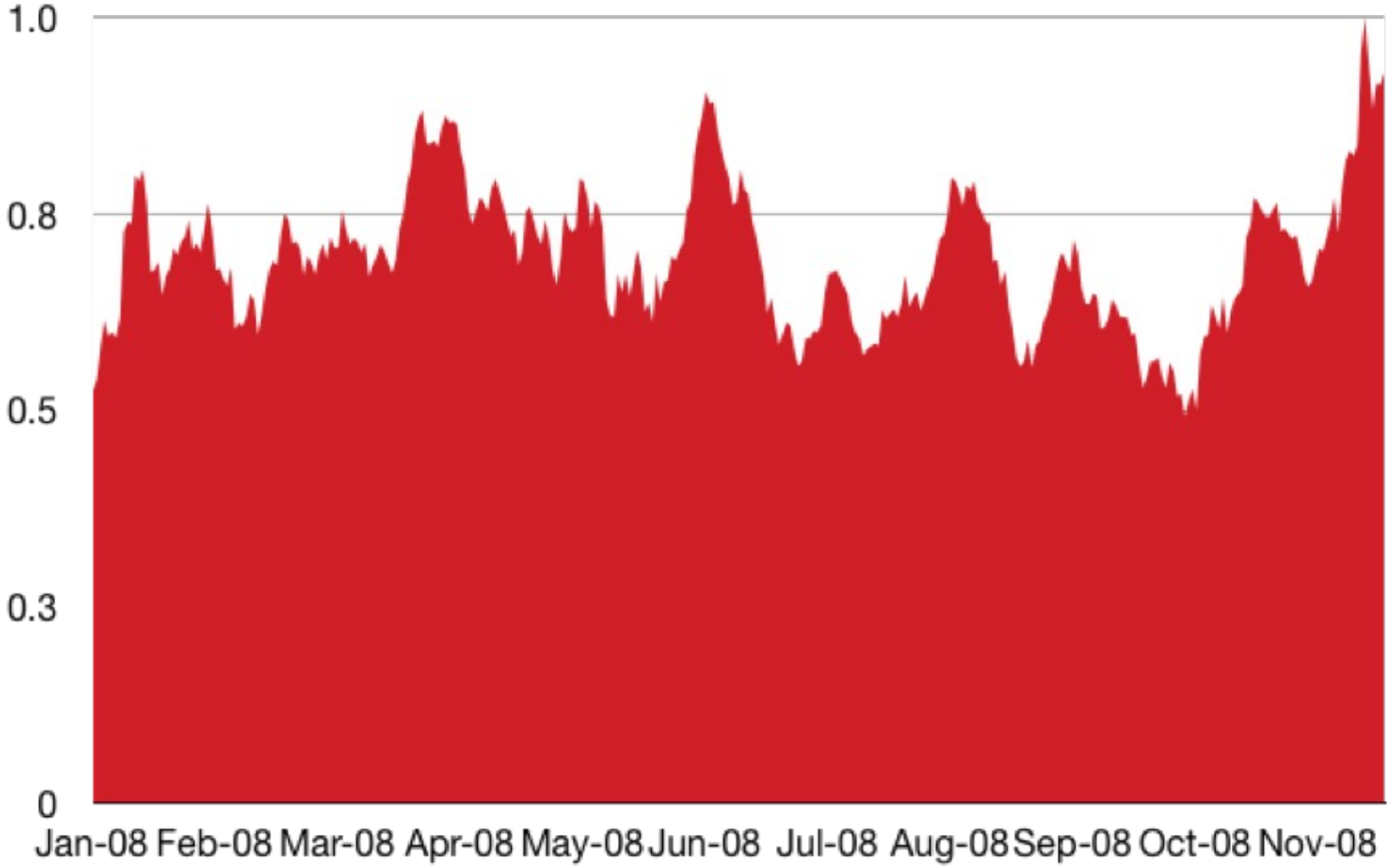
One Year of Malware Impressions



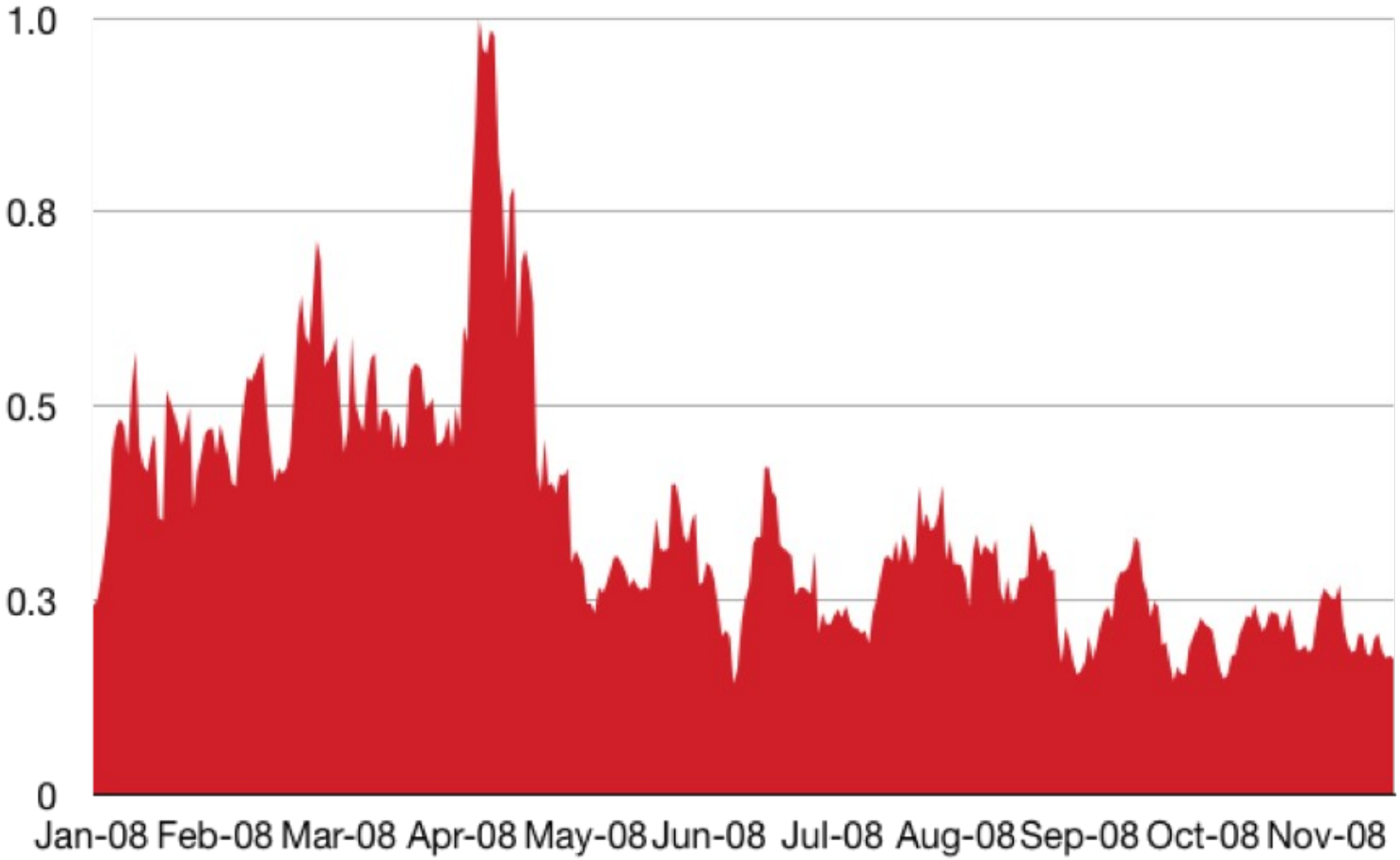
Checkout Fraud

- What is Checkout?
- Not click fraud, but Payment fraud

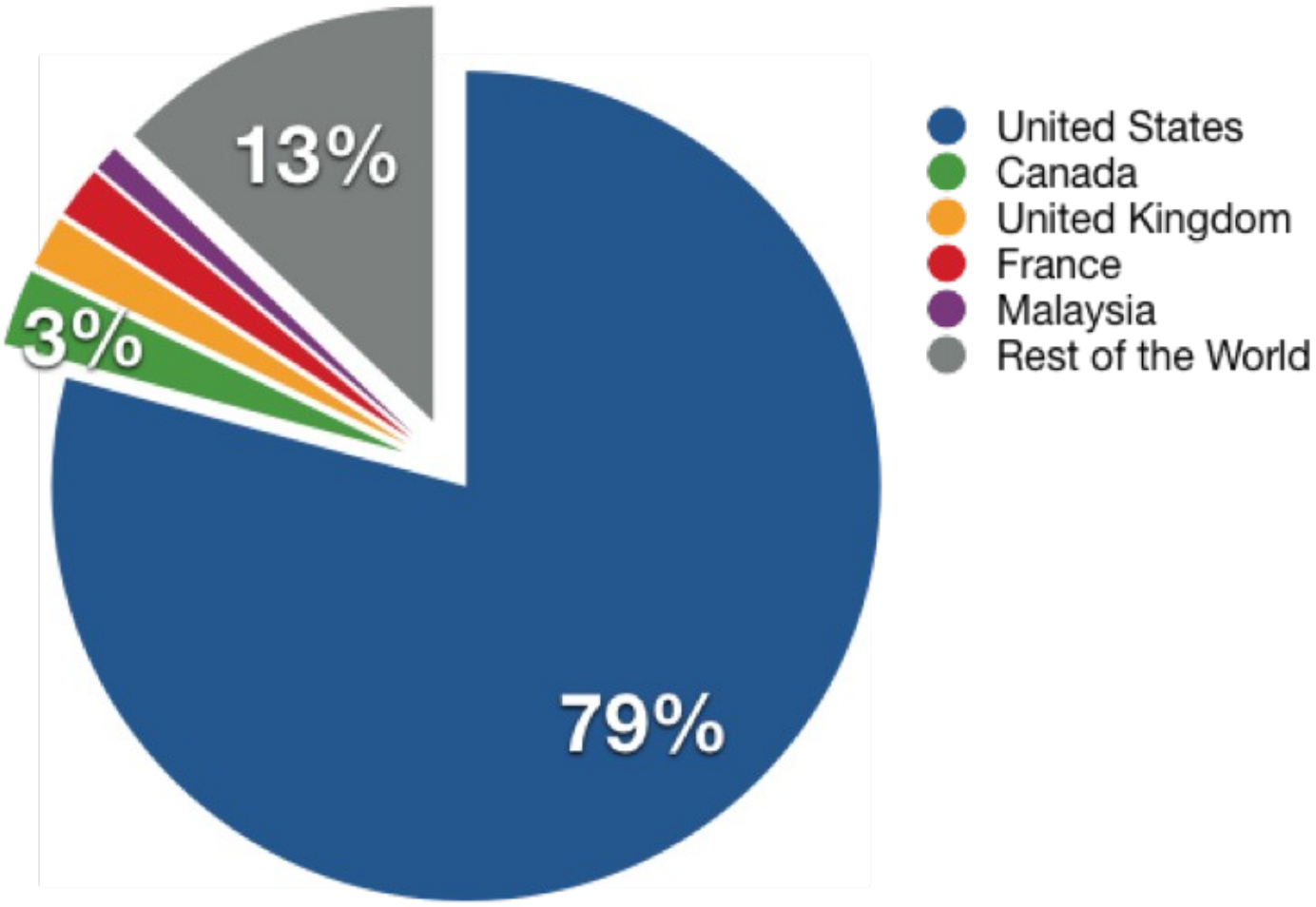
Unsuccessful Payment Fraud 2008



Detected Payment Fraud 2008



Fraud Sources by Country



Conclusions and Questions

- Observe long-term attack trends to diagnose sources of attacks and effectiveness of countermeasures.