

The End of Content

And the Rise of IP Analysis

Scott Petry
Founder, SVP Products & Engineering

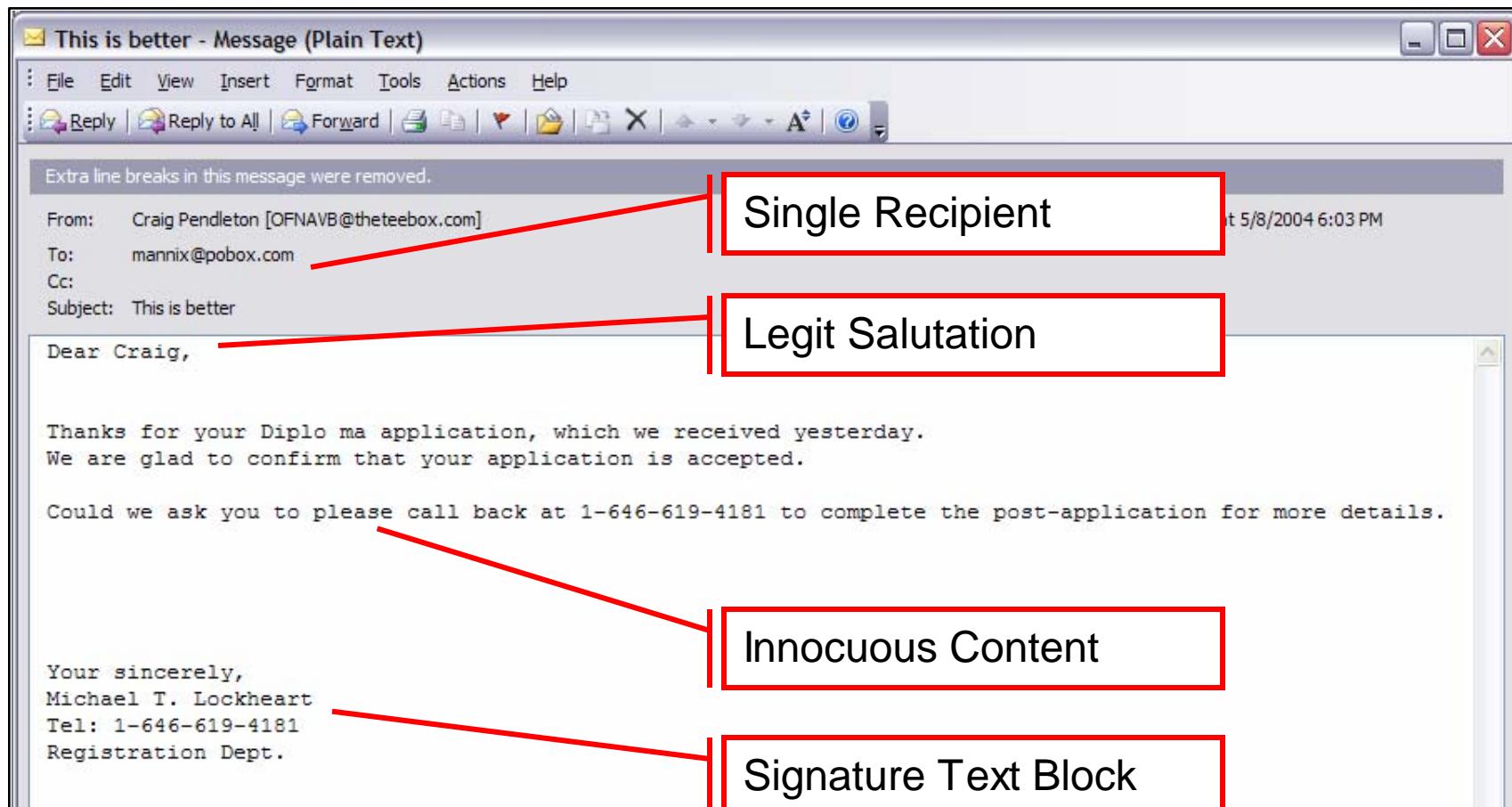


The Ever-Changing Game

- Spammers aggressively modify their messages to defeat content analysis
 - Hash busting
 - Bayesian poisoning
 - White-on-white encoding
- These are relatively easy to spot and program around
- Spammers becoming more covert

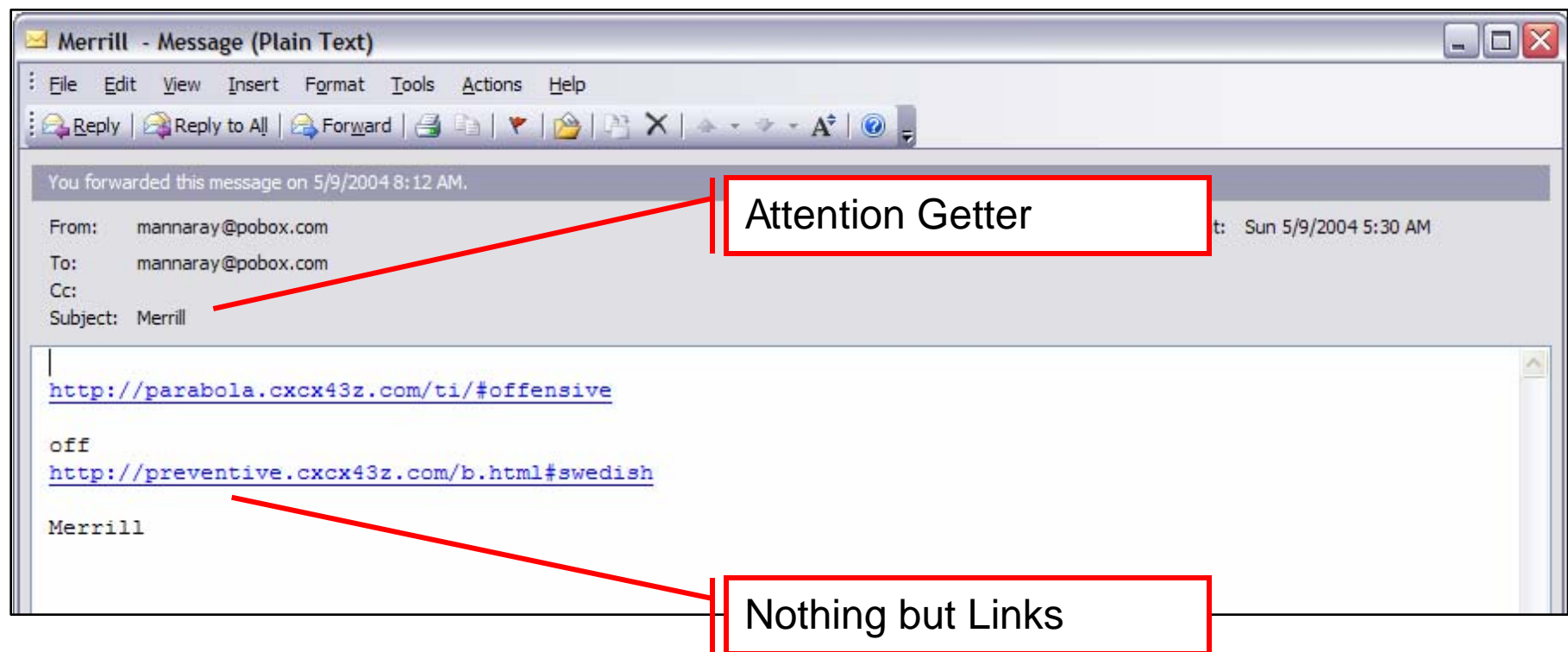
A Disturbing Trend

- Spam is becoming personalized and unique



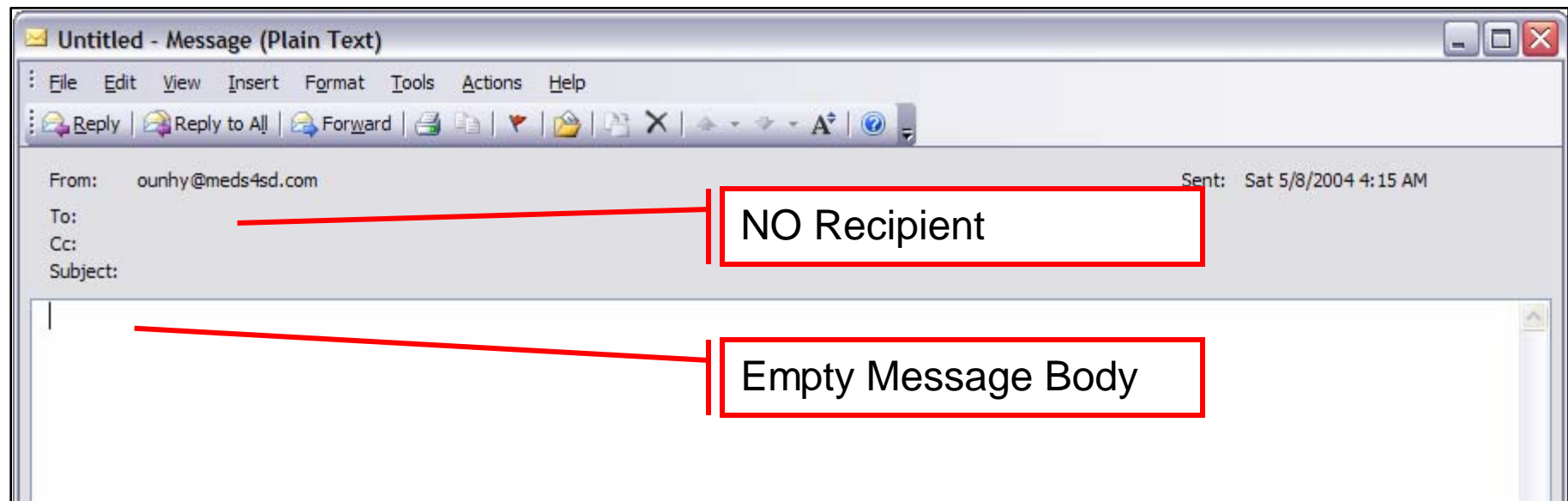
Worse Yet....

- Reduced content means reduced context

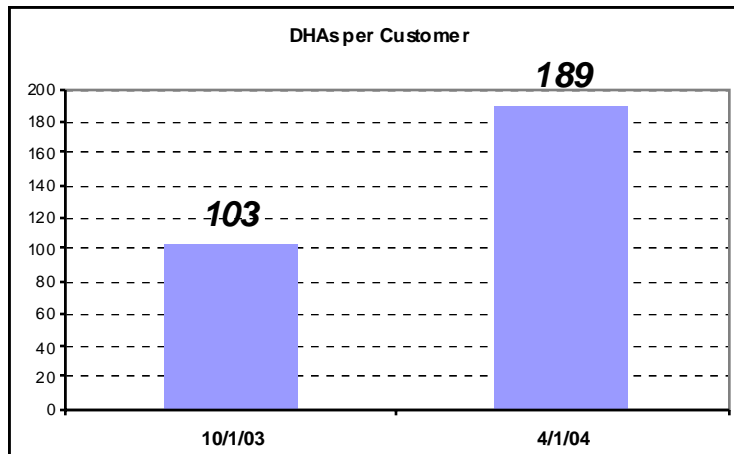


The Logical End Point

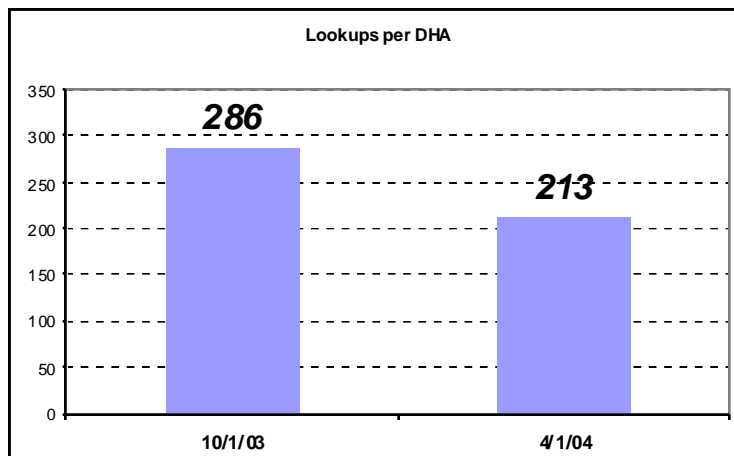
- The empty message
- But is this spam?
 - Residue from Directory Harvest Attack



Not Just a Content War



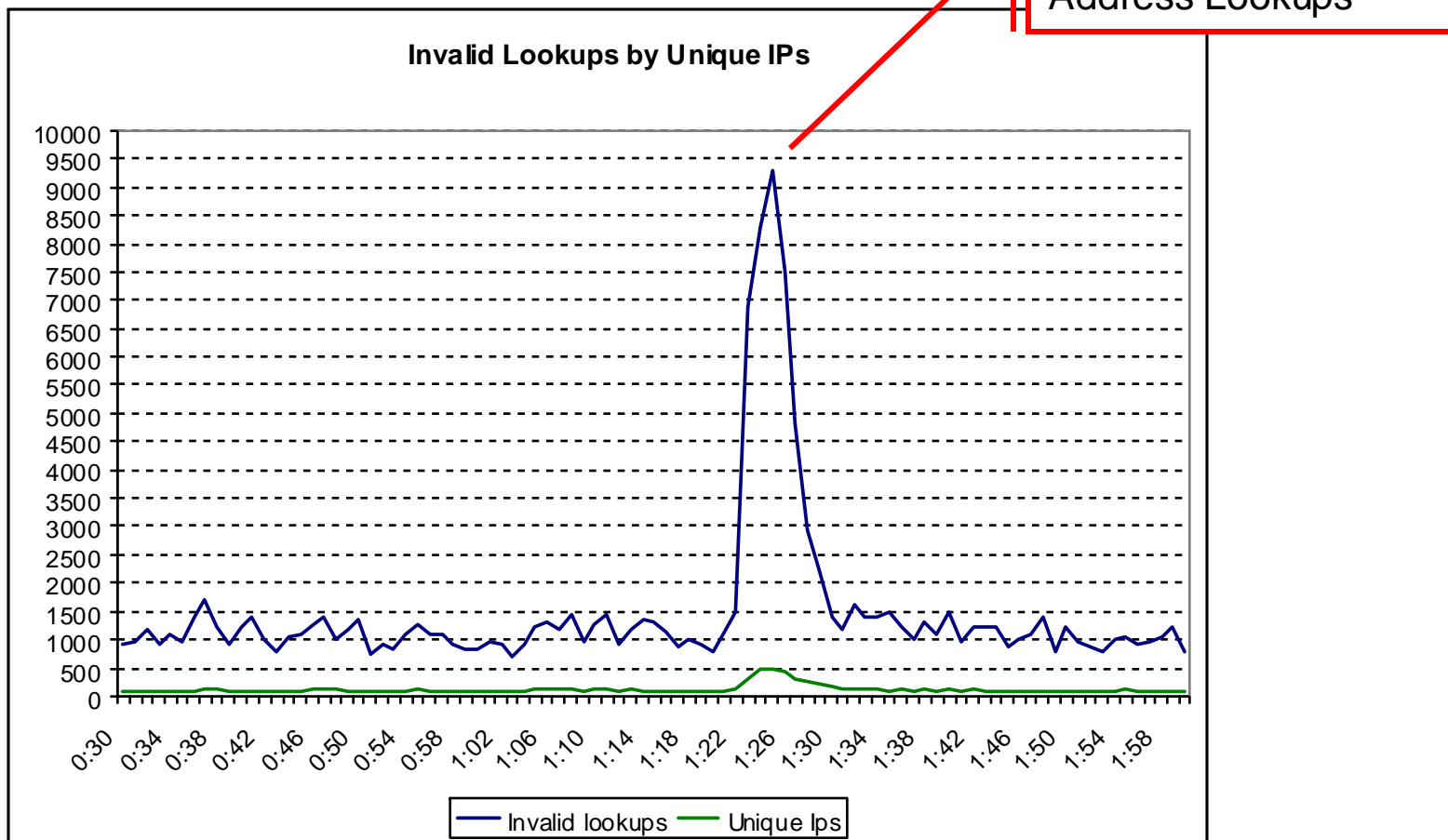
An 83% increase in Directory Harvest Attacks in the last 6 months



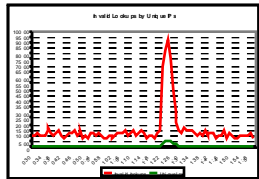
But in that time, we've tracked a 26% reduction in Recipient Address Lookups per attack

That Isn't Good News

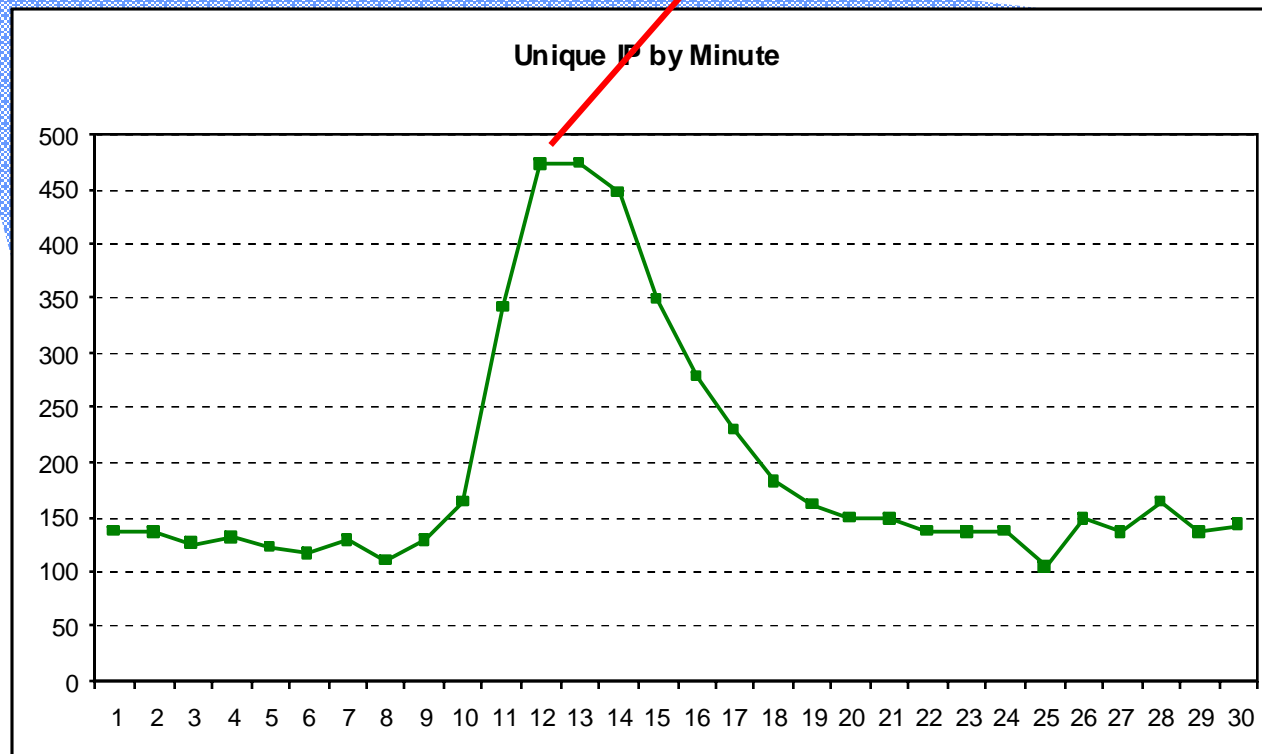
- DHAs hit hard and fast...



Coordinated Across Many IPs



472 Unique IPs. A 4x increase in minute 1



IP Transience

- Way more aggressive about moving through IPs
 - Post-facto log analysis is futile
- Moving across compromised machines
 - 36% of PTIN blocks resolve to cable modems and DSL lines, which should not be relaying SMTP directly
 - *A proxy for measuring the effectiveness of the spam zombie trojan horses like bagle, netsky, etc.*

Conclusion

- Can't just rely on message content
- IP-based intervention is required, but current methods inadequate
 - Not accurate
 - Too static
- Need to instrument and cross-correlate SMTP behavior across numerous source / destination pairs
 - In real time
 - With automated blocks and releases!
- Postini real-time Threat Identification Network is uniquely able to respond to this changing landscape
 - Based on more than 1 Billion SMTP transactions per day