Cyber Security and the National Broadband Strategy

John C. Nagengast

nagengast@att.com

What is Cyber Security?

For AT&T, cyber security is the collective set of capabilities, procedures, and practices that protect our customers and the services we provide them from the full spectrum of cyber threats.

Cyber Security assures the information, applications, and services our customers want are secure, accurate, reliable, and available wherever and whenever they are desired.

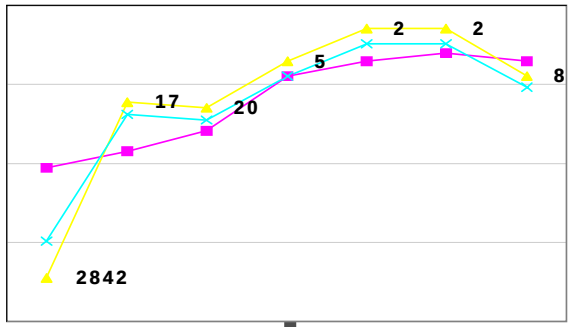
What we see every day!

- COTS Software with Bugs and Vulnerabilities
- Insecure “out-of-the-box” configurations
- Increasing speed of Zero-day Attacks
- Relentless stream of patches from Vendors
- Complexity, Complexity, Complexity

Increasingly difficult for systems administrators and users to manage complex security solutions against ever more sophisticated attacks

How AT&T Identifies Cyber Threats

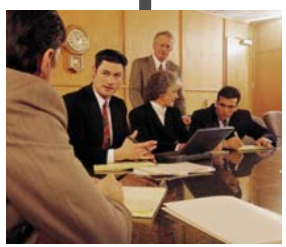
Correlation Across Network, Servers & Applications



Security Analysis
(Profile/Anomaly Based)

Real-Time Alerts & Alarms with Severity & Likely Source

AT&T Security Professionals



Profiling Engine
"What You Expect as Normal"

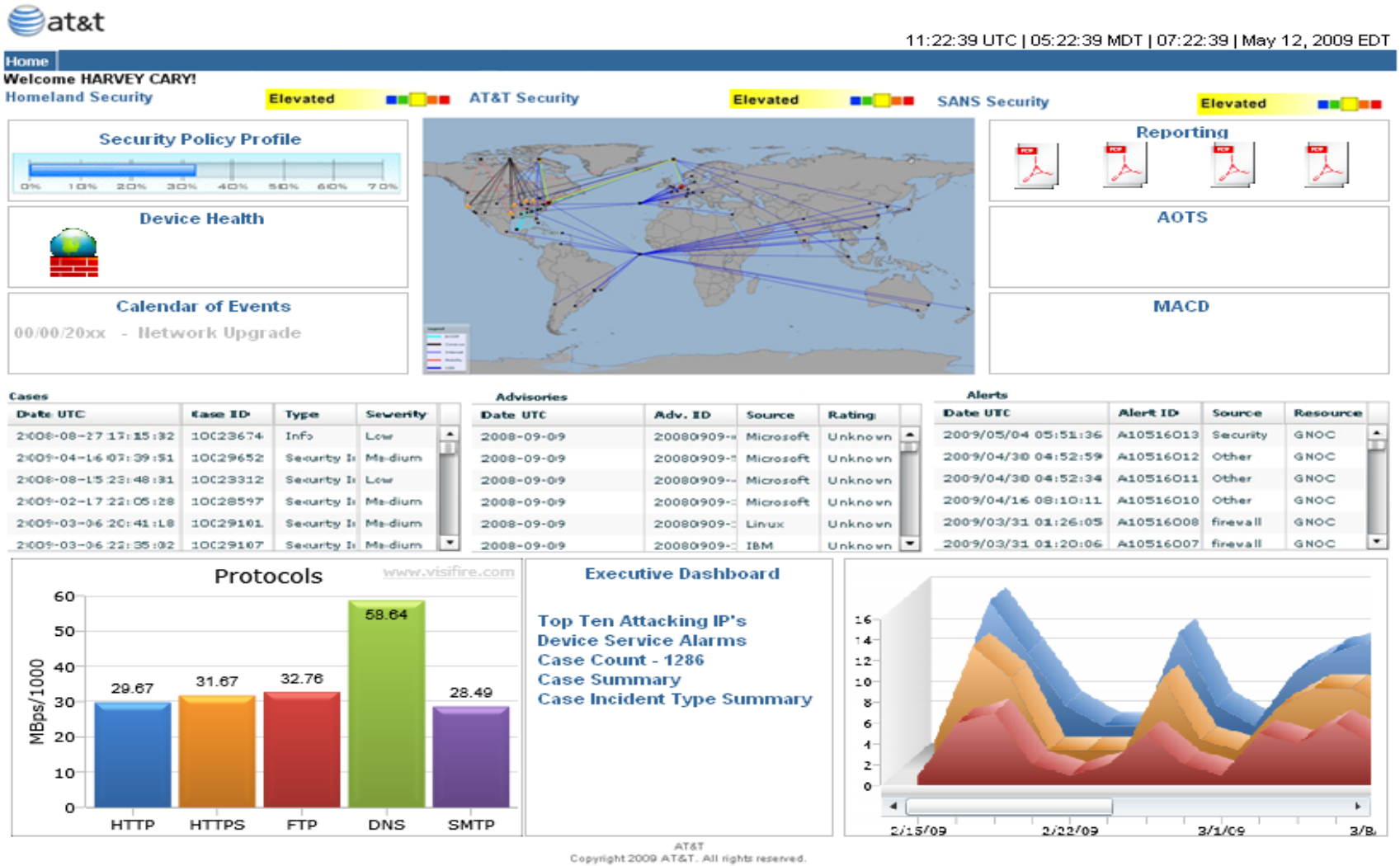
Monitoring Engine
"What you Actually See"

Correlation Engine

Normalized Database of Alerts

at&t

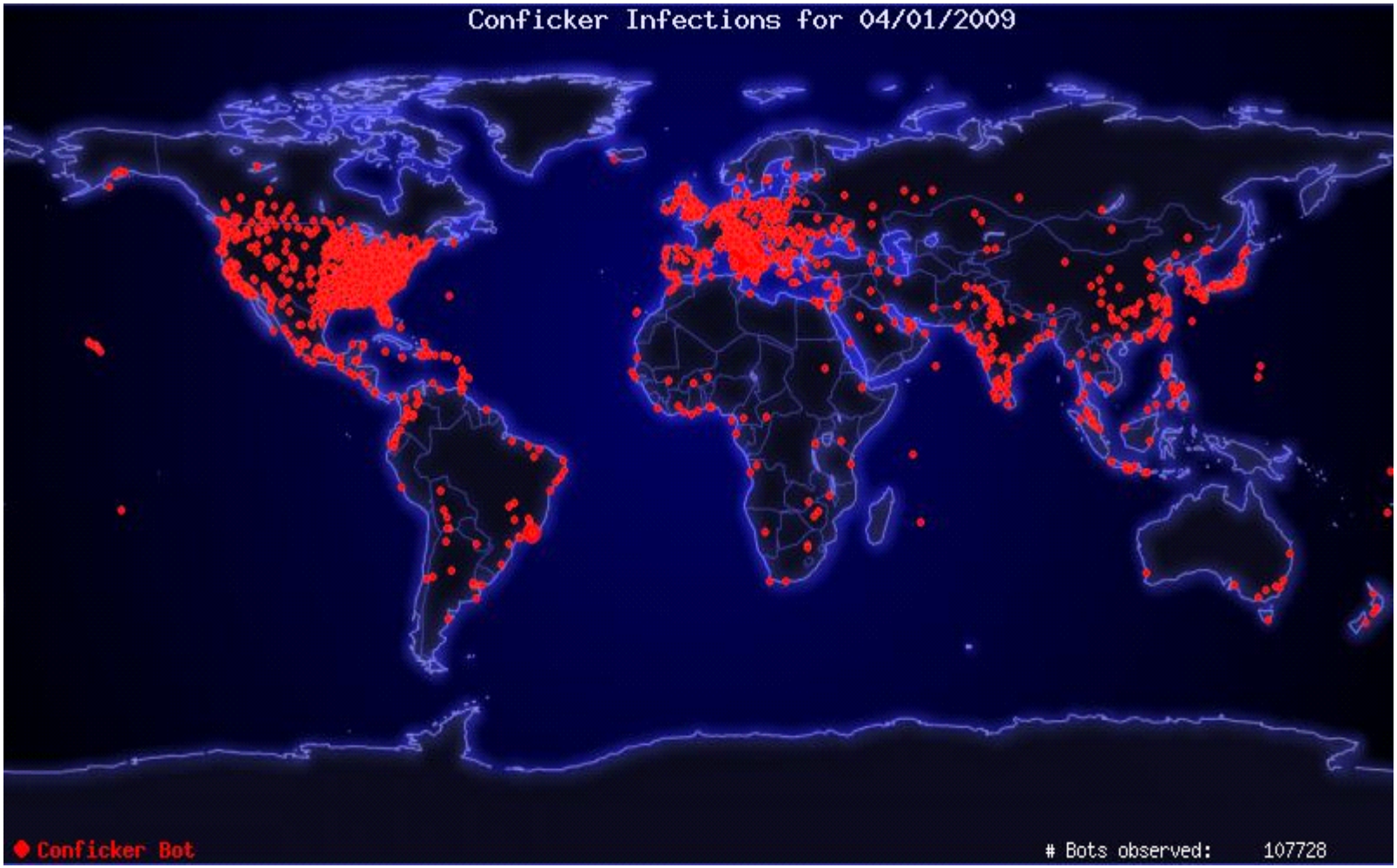
Security Event & Threat Analysis Portal



at&t

Our Cyber Security Tool Set – BotNet Tracking

Conficker Worm April 01, 2009



Page 6

Some Basic Principles – Broadband Strategy & Cyber Security

- Expand Security Education and Awareness
- Fulfill Market Needs & Demand for Cyber Security
- Spur Innovation and Investment
- Leverage Core Network Intelligence to Optimize Broadband's Security, Reliability and Efficiency
- Make Managed Security an integral part of Broadband Services
- Simplify User Experience *and* Increase Security