

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.

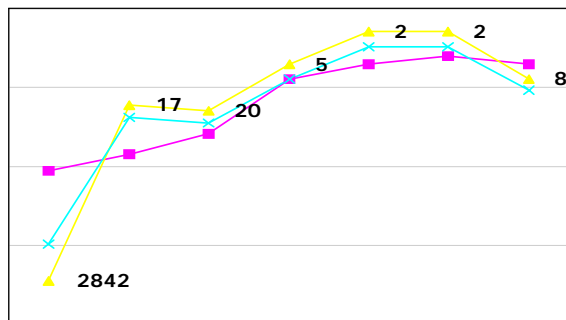
What we see every day!

- 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

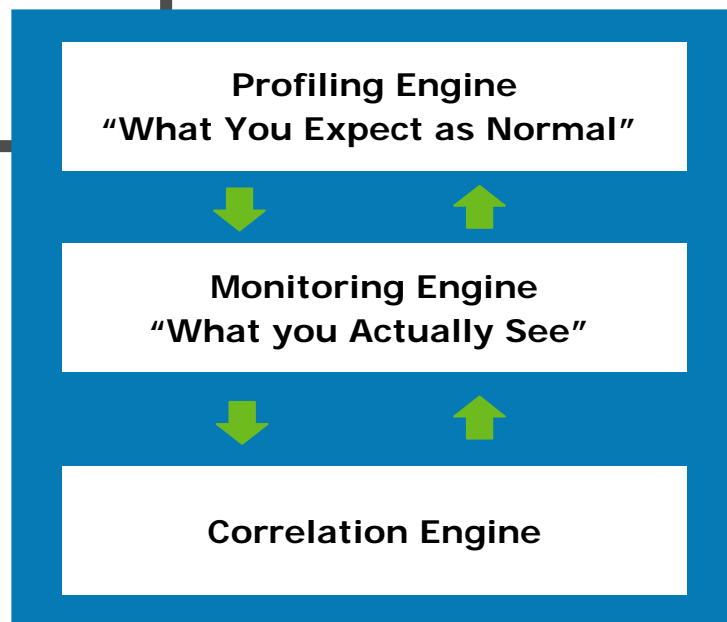


Security Analysis
(Profile/Anomaly Based)

Real-Time Alerts & Alarms with Severity & Likely Source



AT&T Security Professionals



Normalized Database of Alerts

Security Event & Threat Analysis Portal



11:22:39 UTC | 05:22:39 MDT | 07:22:39 | May 12, 2009 EDT

Home | Welcome HARVEY CARY! | Homeland Security

Elevated [Progress Bar] **AT&T Security** | **Elevated** [Progress Bar] **SANS Security** | **Elevated** [Progress Bar]

Security Policy Profile

Reporting

AOTS

MACD

Device Health

Calendar of Events

00/00/20xx - Network Upgrade

Cases

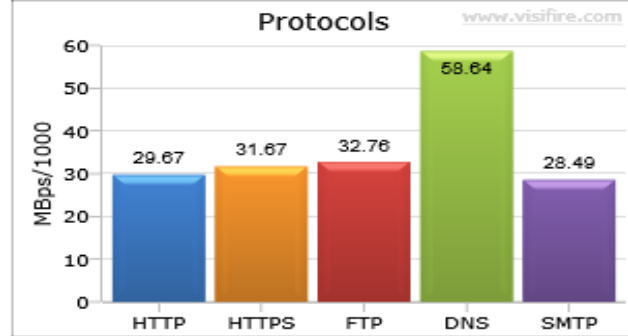
Date UTC	Case ID	Type	Severity
2008-08-27 17:15:32	10C23674	Info	Low
2009-04-16 07:39:51	10C29652	Security I	Medium
2008-08-15 23:48:31	10C23312	Security I	Low
2009-02-17 22:05:28	10C28597	Security I	Medium
2009-03-06 20:41:18	10C29101	Security I	Medium
2009-03-06 22:35:02	10C29107	Security I	Medium

Advisories

Date UTC	Adv. ID	Source	Rating
2008-09-09	20080909--	Microsoft	Unknown
2008-09-09	20080909--	Microsoft	Unknown
2008-09-09	20080909--	Microsoft	Unknown
2008-09-09	20080909--	Microsoft	Unknown
2008-09-09	20080909--	Linux	Unknown
2008-09-09	20080909--	IBM	Unknown

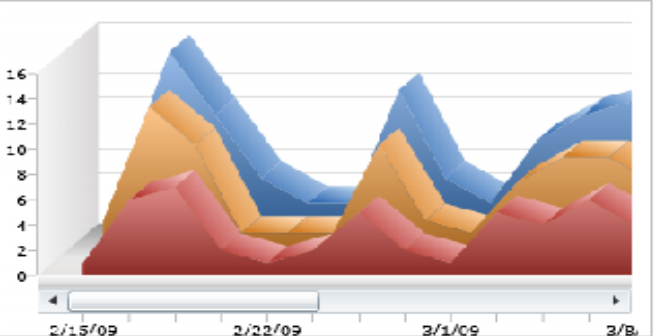
Alerts

Date UTC	Alert ID	Source	Resource
2009/05/04 05:51:36	A10516013	Security	GNOC
2009/04/30 04:52:59	A10516012	Other	GNOC
2009/04/30 04:52:34	A10516011	Other	GNOC
2009/04/16 08:10:11	A10516010	Other	GNOC
2009/03/31 01:26:05	A10516008	firewall	GNOC
2009/03/31 01:20:06	A10516007	firewall	GNOC



Executive Dashboard

Top Ten Attacking IP's
 Device Service Alarms
 Case Count - 1286
 Case Summary
 Case Incident Type Summary

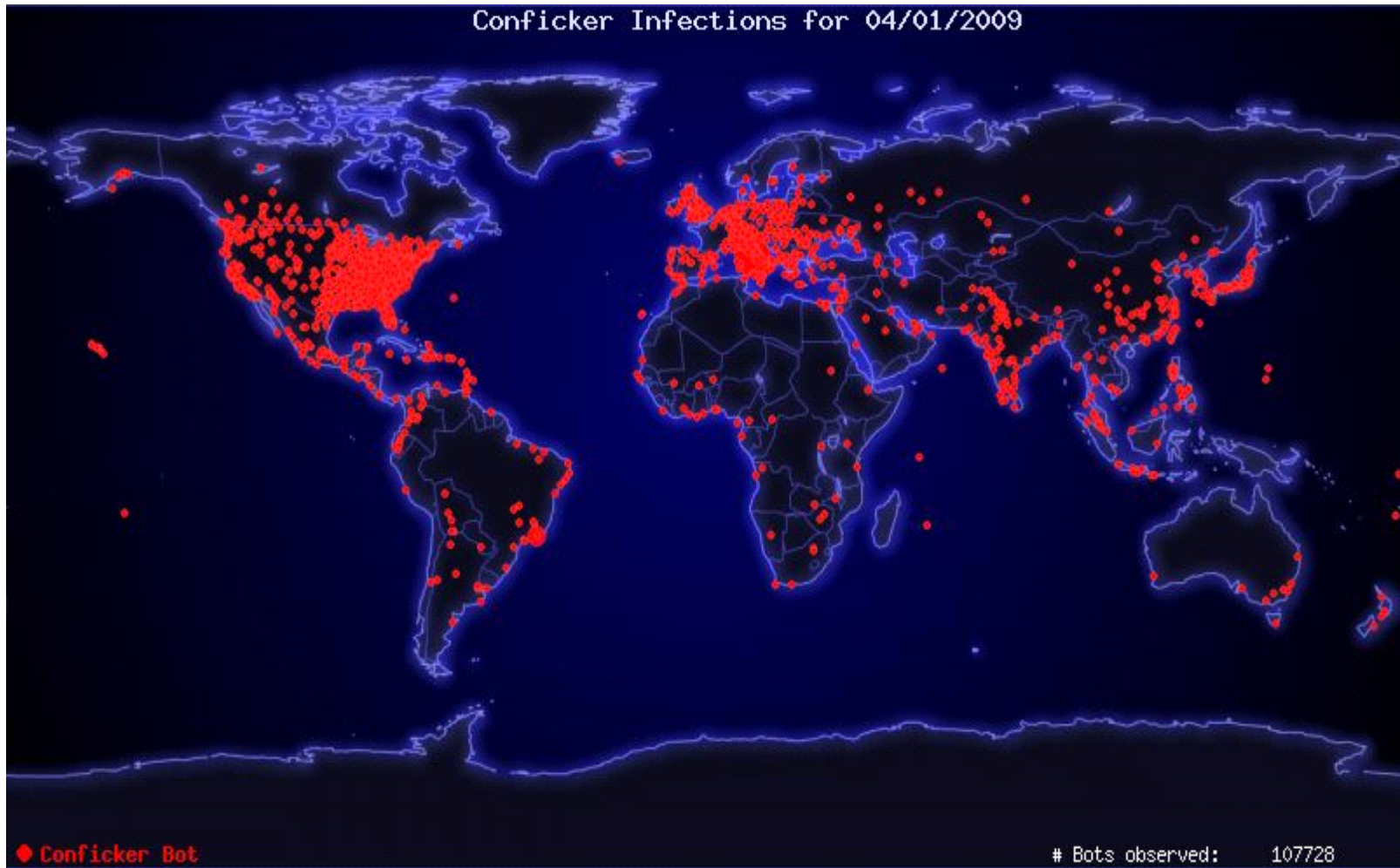


AT&T
 Copyright 2009 AT&T. All rights reserved.



Our Cyber Security Tool Set – BotNet Tracking

Conficker Worm April 01, 2009



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