ARBOR NETWORKS
SPECTRUM™

Epic Range, Faster Proof

02.05.2016
Your Driver Today

• Paul Bowen aka Pablo!  pbowen@arbor.net
  – Manager Global Security Estee Lauder 10 years
    • This is where Pablo had his inception
  – Employee #200 for 9 years at ArcSight Pre and Post HP Strategic Security Evangelist
  – SecurOnix Principal Architect
  – Mandiant Principal Architect TAP Threat Analytics Platform
  – Fortinet Principal Sales Engineer SandBox
  – Arbor Principal Security Technologist

• I Am a Dog Lover and currently working on my line of British Labs
Arbor Overview: 15 Years of Network Excellence

Leading Network Traffic Expertise
- 15 years of understanding the world’s most complex and demanding service provider and enterprise networks.
- Deployed everywhere on the planet (107 countries).
- See more Internet traffic than any other service provider.

Premier Global Security Visibility
Hourly updates from 330+ providers on attack traffic across the Internet.
- World class security research team analyzing traffic patterns and reverse engineering malware and its infrastructure with ATLAS/ASERT.

Proven Scale Across Blue Chip Installed Base
- 3/5 Top Global Banks.
- Deployed largest financial institution in 28 countries.
- 9/10 of largest online brands and hosting providers.
- 100% Tier 1 Service providers.

Live Digital Attack Map
Powered by: Arbor Networks
The Arbor Spectrum Approach

Prove and resolve threats on your network 10x faster.

Designed with the security user in mind, real-time workflows and analytics to empower & scale security teams to investigate and prove threats 10x more efficiently than existing solutions today.

Visualize global attack campaigns in real-time in your network.

Arbor’s real-time global threat intelligence from its service provider network is automatically correlated with an organization’s internal traffic to detect highest risk, most damaging threats.

Search and surface anything within the network.

Automatic IOC-based forensics for both packets and flows delivers complete visibility into past and present network activity at a fraction of cost & complexity of traditional network forensics.
How Arbor Spectrum Works

**PROVE**
- Respond with Confidence
- Automatic PCAP on IOC
- Fast search into months of network data

**INVESTIGATE**
- Automatic correlation of IOCs to network activity
- Real-time hunting workflows
- Investigation workbench
- Tie malicious host to attacks
- Conversations search

**ViDETECT**
- Global Internet Threats
- Internal network conversations
- Third party intelligence

**ViDETECT**
- Atlas
- ASERT
- 330+ Providers
- Global internet threats
- Internal network conversations
- Third party intelligence

**Flow Traffic Collection**
- Botnet
- Darknet
- Trojan

**Packet Traffic Collection**
- Custom or intelligence feeds

©2016 ARBOR® CONFIDENTIAL & PROPRIETARY
The Network Sees the Entire Attack Campaign

**ORGANIZATION'S NETWORK**

**STAGE 1**
“Gets In”
Initial Entry Point
Detected or Missed Threat

**STAGE 2**
Delivery
Exploits Privileges or Vulnerabilities

**STAGE 3**
Lateral Movement

**STAGE 4**
Command/Control

**STAGE 5**
Exfiltration

**STAGE 6**
Mission Complete
Use Forensics to detail incident

**STAGE 7**

---

Unsupervised Consultant
Bypasses Firewall & Sandbox

Remote Subsidiary

Sandbox

Headquarters

Desktop of CFO

Server Calling Out to Botmaster

Sensitive Assets

Headquarters

Unsupervised Consultant

Desktop of CFO

Server Calling Out to Botmaster

Sensitive Assets

Headquarters
Where Arbor Spectrum Fits