ISE® SOUTHEAST EXECUTIVE FORUM

Nominee Showcase Presentation

EarthLink

BotRadar™: Invisible Protection from Malicious Attacks

Pete Chronis

Chief Security Officer

Company Overview

EarthLink provides managed network, security and cloud solutions for multi-location businesses. We help thousands of specialty retailers, restaurants, financial institutions, healthcare providers, professional service firms and local governments deliver a reliable and engaging customer experience in their stores and branch offices.

Key Facts:

- Headquarters: Atlanta, GA
- >1M customers
- $1.2B in Annual Revenue
- EarthLink celebrated its 20th anniversary in 2014!

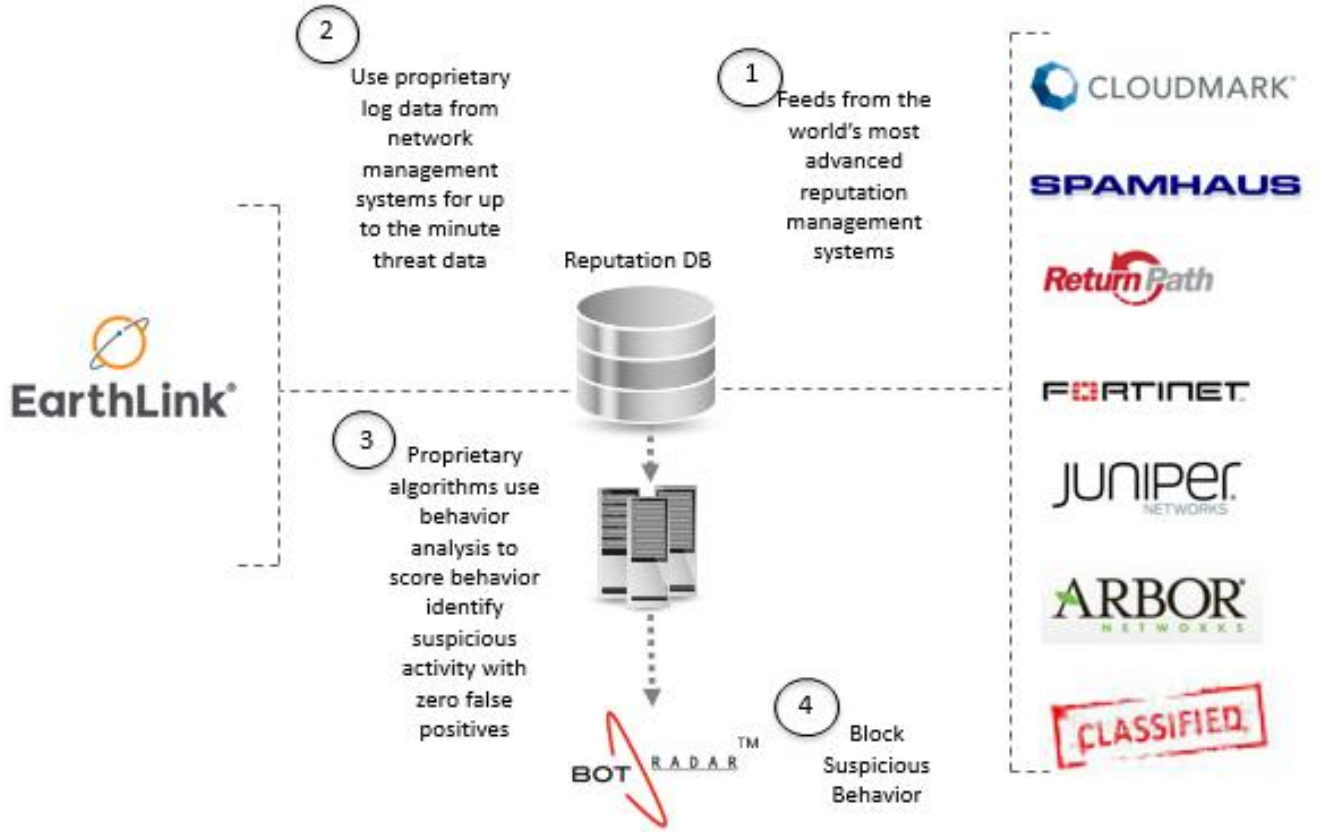
Presentation Overview

What is EarthLink's BotRadar™?

- EarthLink's proprietary threat reputation platform designed to identify suspicious and malicious events.
- Compiles raw log data from firewalls, IPS, application logs and DDoS prevention systems.
- Log data is automatically analyzed for malicious behavior, anomalous activity or high risk application specific events.
- EarthLink uses BotRadar™ across multiple platforms to proactively block threats.
- Custom modules within BotRadar™ block spam, identify advanced persistent attacks or block fraudulent authentications
- Blocks over 200M threats a day; contains 1.2B attack vectors; protects 1M customers

Presentation Slide

The Secret Sauce. How does EarthLink's BotRadar™ work?



Presentation Slide

What Business Problems Were We Trying to Solve?

- Brute force account log in attempts were causing account lock outs
- Account lockouts, although necessary, were very disruptive to customers
- Lockouts generated high volumes of customer calls, driving up call center costs and impacting product margins
- Could we create a custom module in BotRadar to block brute and suspicious log in activity before it impacted customers?

What were the Results?

- Account lockouts were reduced by 92%
- Customer support calls declined by over 80% (Q3 2013 vs. Q4 2014) saving over $200K in annual call center and support costs
- Blocked an additional 10M threats a day

Lessons Learned/Best Practices

What Surprises Did We Encounter?

- Infected mobile devices were being used in brute force attacks (to an alarming degree) – Mobile companies use of proxies made threat blocking difficult
- Traffic analysis across multiple systems helped us identify for-rent botnets activity – DDoS attacks from one source today, spam from the same IP tomorrow

What were the Most Valuable Team Experiences?

- Leveraged commercial technology + proprietary know how
  - Cross-functional knowhow included infrastructure, network, customer service, security, software development teams