Botnet Detection with HCP

Presented By:
Greg Phillips
Carolyn Duby
Amol Thacker
Ramasamy Baskaran
Vikas Sawhney

September 2018

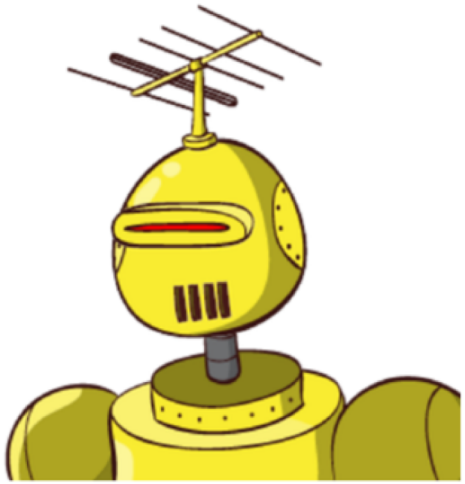
Agenda

- What is a botnet?
- Why is botnet detection valuable?
- How can we detect it with HCP?

HORTONWORKS

What is a botnet?

- Hosts infected with malware
- Report to command and control (C&C)
- C&C instructs them to do harm
  - Distributed Denial of Service (DDOS)
  - Spam
  - Social Media
  - Exfiltration
- Unsecured IOT devices present new challenges

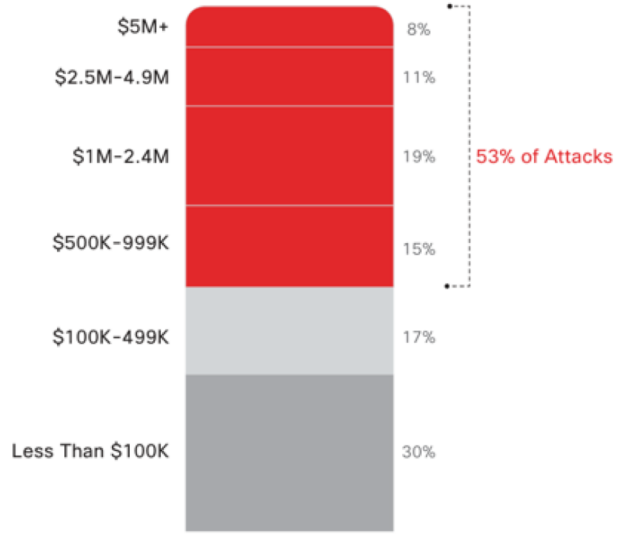


HORTONWORKS

Why is botnet detection valuable?

- Significant attack vector for organizations
- IOT use is expanding
- IOT security is weak
  - difficult or impossible to patch
  - lack of agents or security software
- Easier to take over than a PC
- Always on and can be called to action anytime
- **53% of attacks cost $500K or more**

Figure 40 Fifty-three percent of attacks result in damages of $500,000 or more



Source: Cisco 2018 Security Capabilities Benchmark Study

Download the 2018 graphics at: cisco.com/go/acr2018graphics

HORTONWORKS

Detecting Botnets with Metron

Ingest DNS and NetFlow data

- Tracking: Source, Destination, Duration, Size, Protocol & Port

Apply botnet threat intelligence

- Domain / IP Blacklists for known attackers

Profilers detect anomalous traffic

- Failed DNS queries
- Anomalous levels of IRC traffic
- DNS activity at predictable intervals

Machine learning algorithms

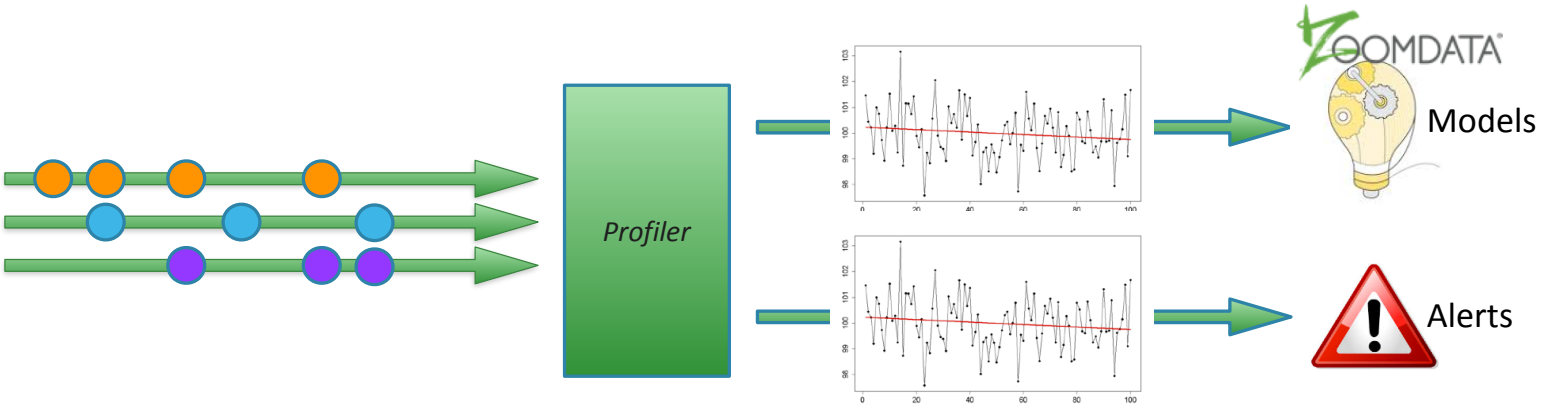
- NLP analysis to find suspicious and/or generated domains

Ensemble algorithms

- Combining several models for improved predictions

HORTONWORKS

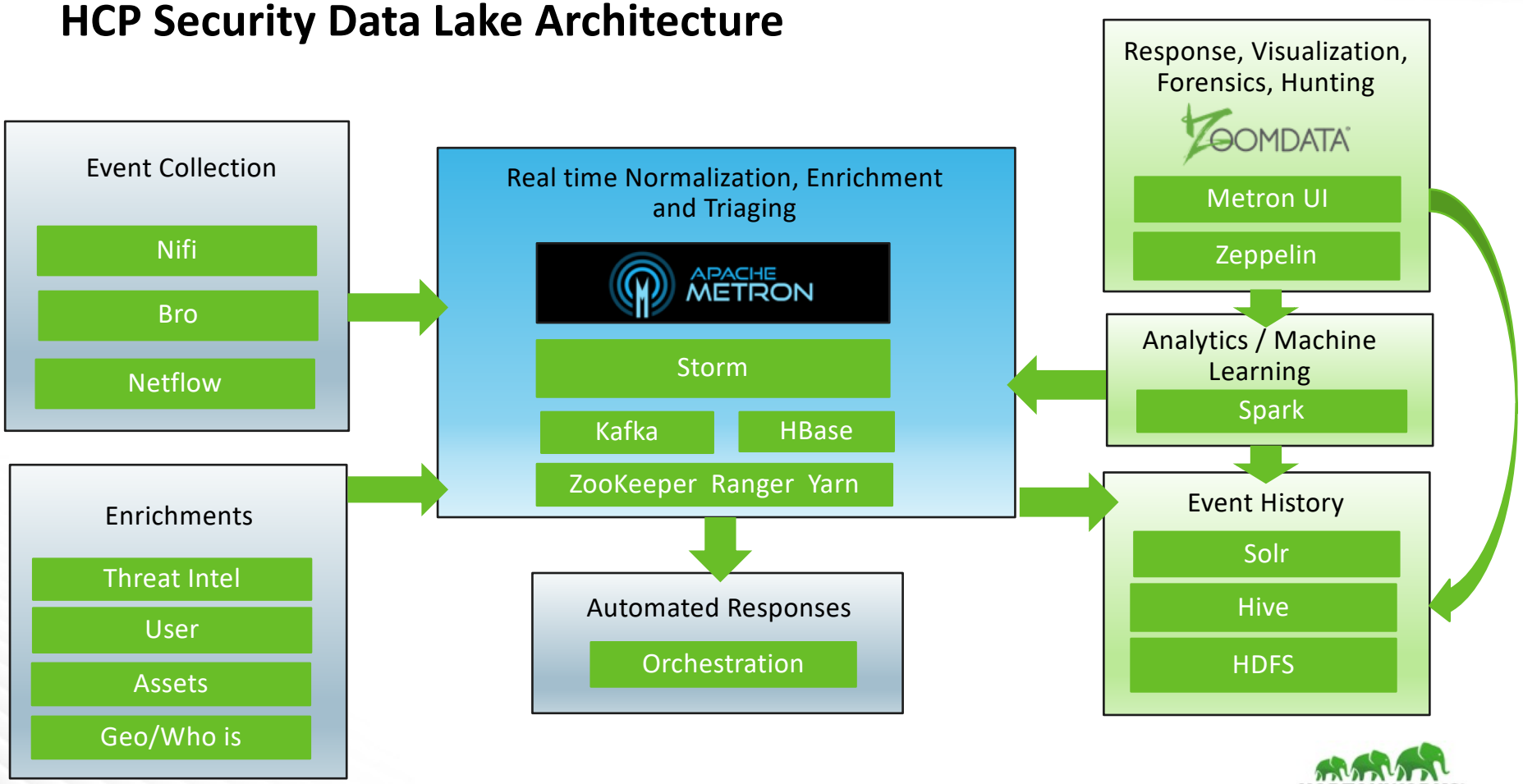
The Profiler



- A generalized, extensible solution for extracting feature sets from high throughput, streaming data
- Generates a profile describing the behavior of an entity; a host, user, subnet or application
- A foundational component for both security model building and alerting in Metron

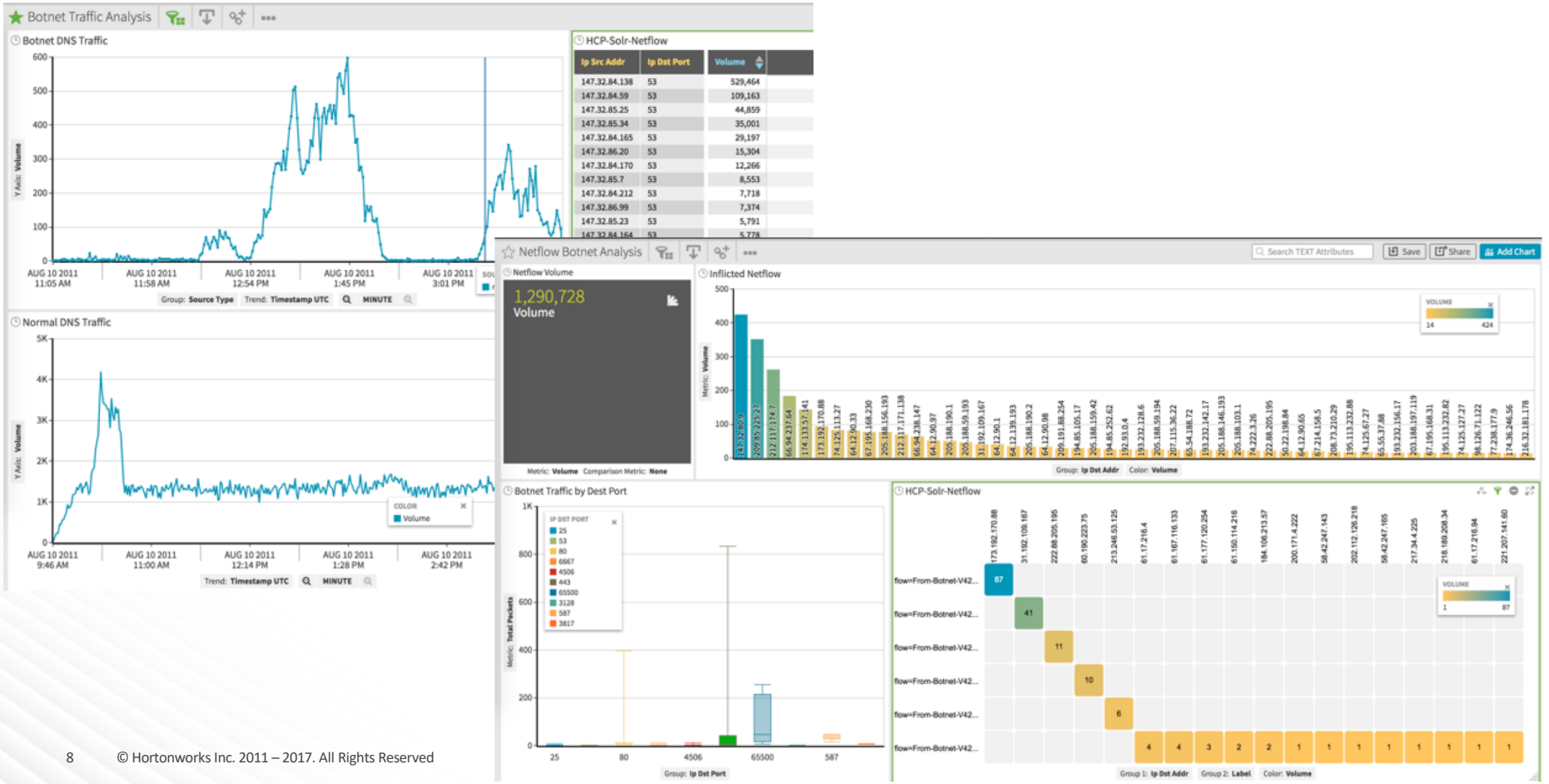
HORTONWORKS

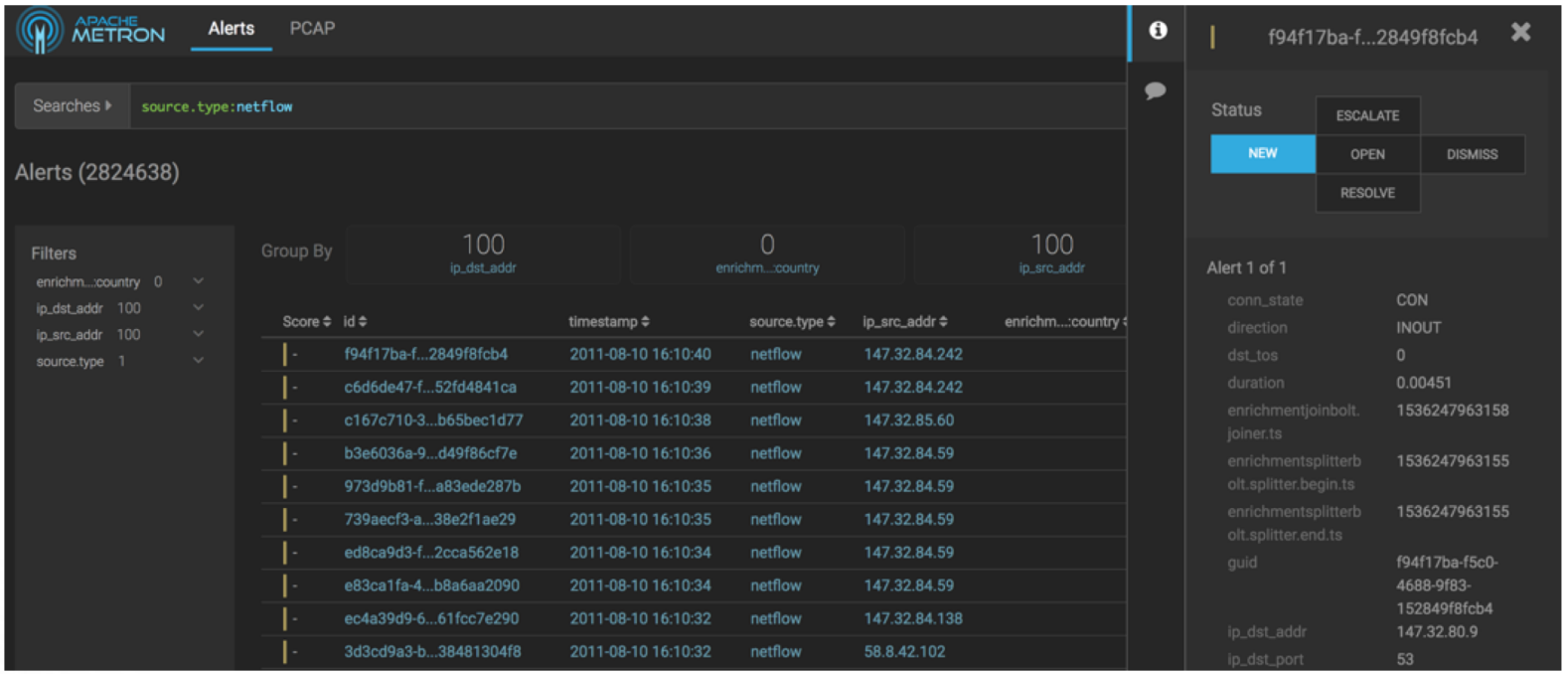
HCP Security Data Lake Architecture



HORTONWORKS

Peek at the Solution





HORTONWORKS

Thank you