

Botnet Detection with HCP

Presented By:

Greg Phillips

Carolyn Duby

Amol Thacker

Ramasamy Baskaran

Vikas Sawhney

September 2018

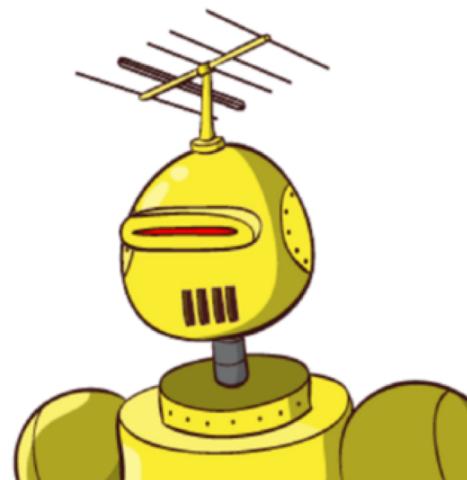


Agenda

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

What is a botnet?

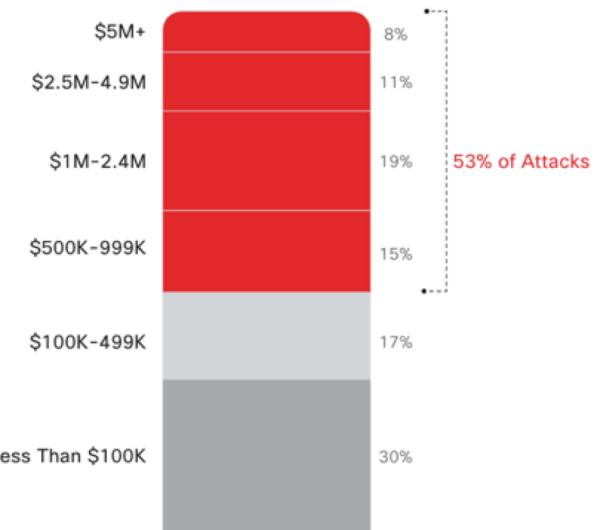
- ◆ Hosts infected with malware
- ◆ Report to command and control (C&C)
- ◆ C&C instructs them to do harm
 - Distributed Denial of Service (DDOS)
 - Spam
 - Social Media
 - Exfiltration
- ◆ Unsecured IOT devices present new challenges



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**

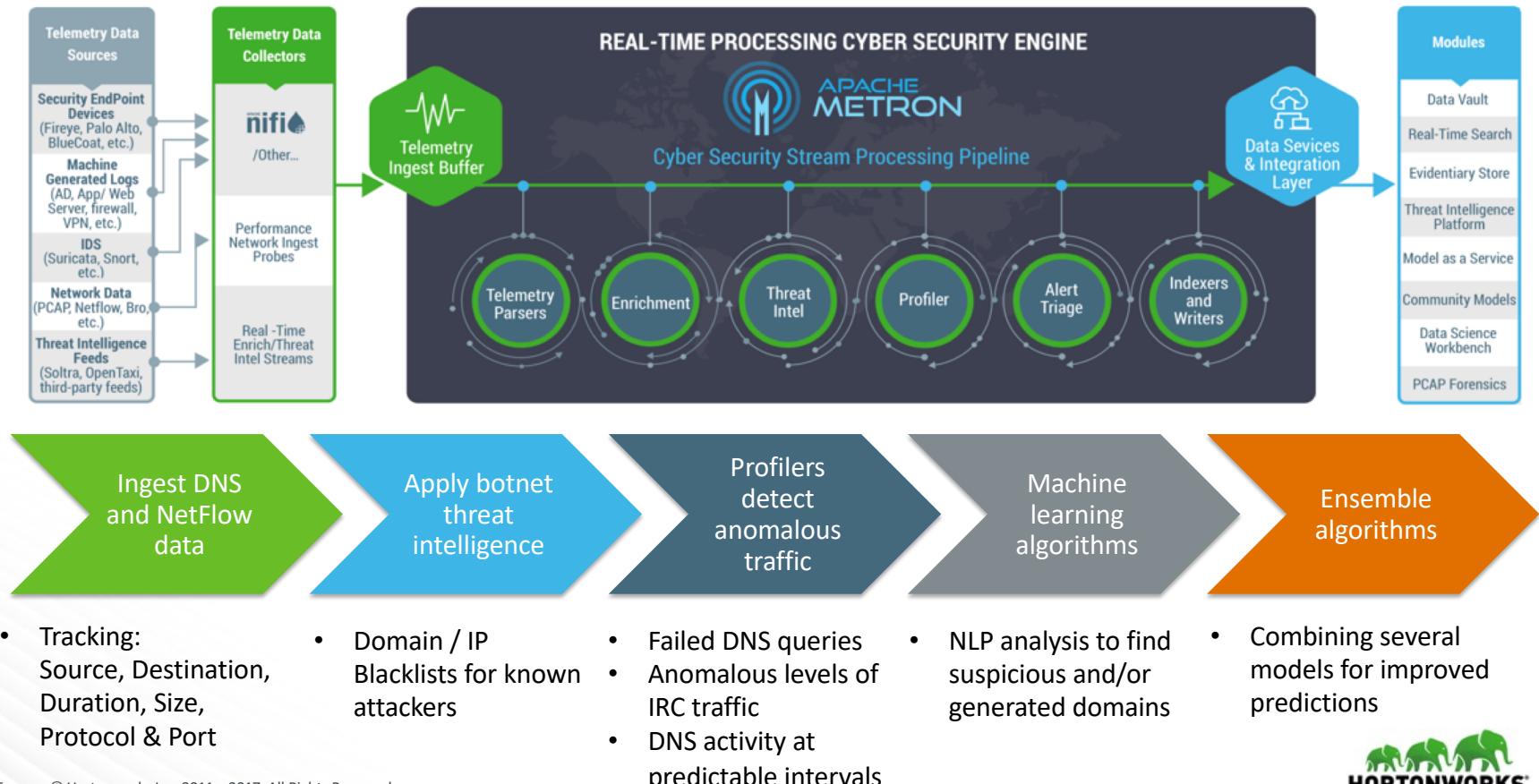
Figure 40 Fifty-three percent of attacks result in damages of \$500,000 or more



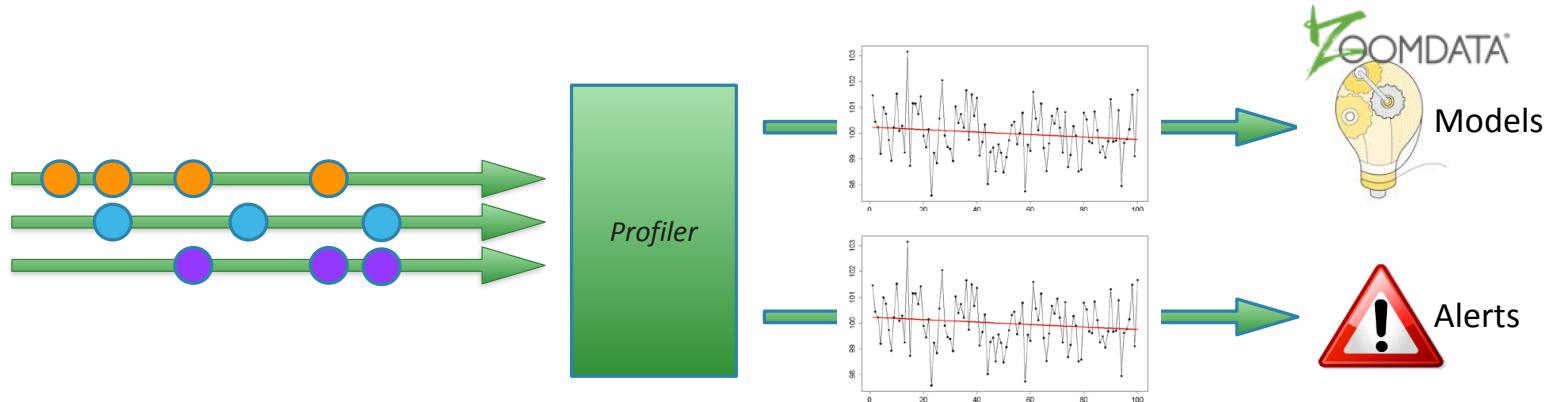
Source: Cisco 2018 Security Capabilities Benchmark Study

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

Detecting Botnets with Metron

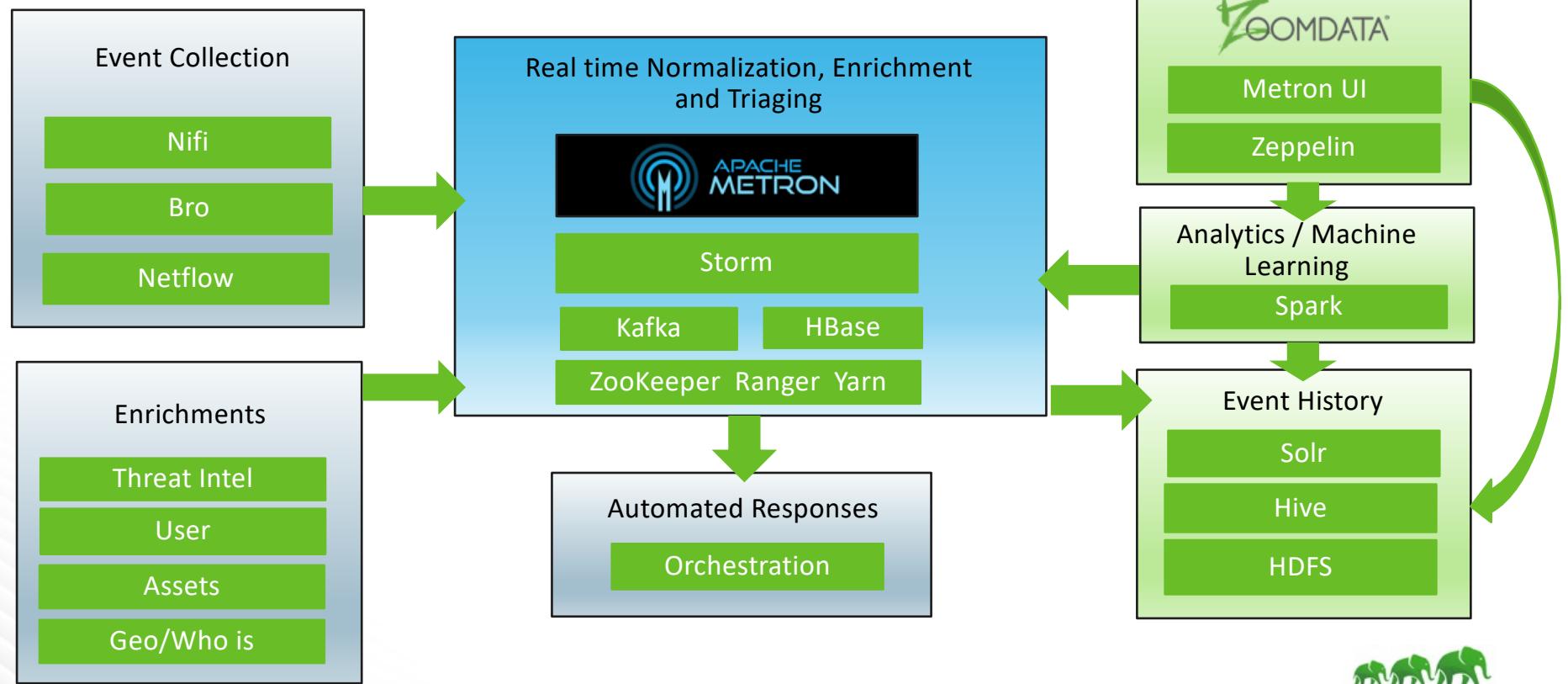


The Profiler

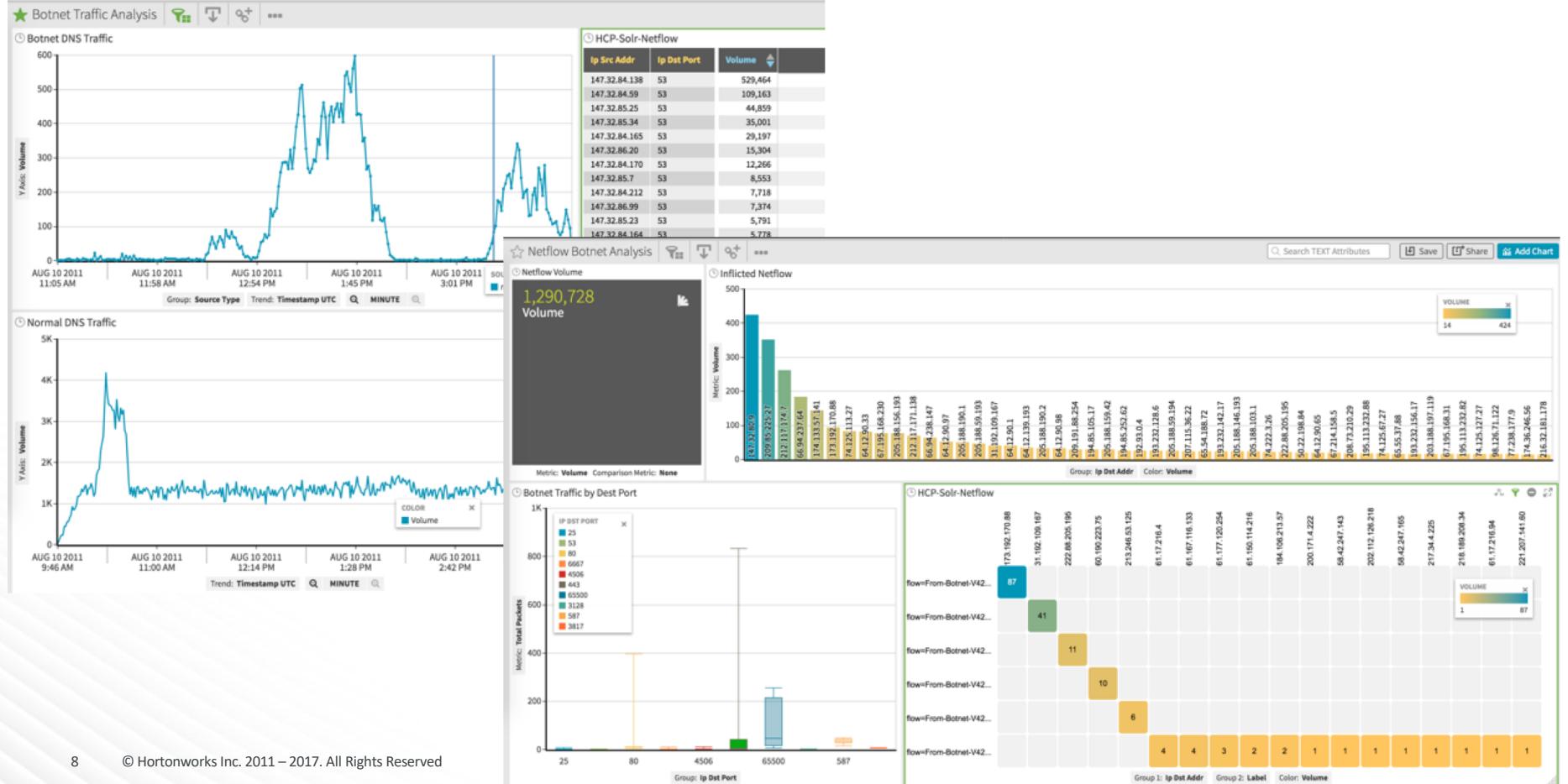


- ◆ A generalized, extensible solution for extracting feature sets from high throughput, streaming data
- ◆ Generates a profile describing the behavior of an entity; a host, user, subnet or application
- ◆ A foundational component for both security model building and alerting in Metron

HCP Security Data Lake Architecture



Peek at the Solution





APACHE METRON

Alerts PCAP

Searches ▾ source.type:netflow

Alerts (2824638)

Filters

enrichm...country 0 ▾
ip_dst_addr 100 ▾
ip_src_addr 100 ▾
source.type 1 ▾

Group By

	100 ip_dst_addr	0 enrichm...country	100 ip_src_addr
Score ↴ id ↴	timestamp ↴	source.type ↴	ip_src_addr ↴
- f94f17ba-f...2849f8fc4	2011-08-10 16:10:40	netflow	147.32.84.242
- c6d6de47-f...52fd4841ca	2011-08-10 16:10:39	netflow	147.32.84.242
- c167c710-3...b65bec1d77	2011-08-10 16:10:38	netflow	147.32.85.60
- b3e6036a-9...d49f86cf7e	2011-08-10 16:10:36	netflow	147.32.84.59
- 973d9b81-f...a83ede287b	2011-08-10 16:10:35	netflow	147.32.84.59
- 739aecf3-a...38e2f1ae29	2011-08-10 16:10:35	netflow	147.32.84.59
- ed8cae9d3-f...2cca562e18	2011-08-10 16:10:34	netflow	147.32.84.59
- e83ca1fa-4...b8a6aa2090	2011-08-10 16:10:34	netflow	147.32.84.59
- ec4a39d9-6...61fcc7e290	2011-08-10 16:10:32	netflow	147.32.84.138
- 3d3cd9a3-b...38481304f8	2011-08-10 16:10:32	netflow	58.8.42.102

Status

ESCALATE
NEW OPEN DISMISS
RESOLVE

Alert 1 of 1

conn_state	CON
direction	INOUT
dst_tos	0
duration	0.00451
enrichmentjoinbolt.joiner.ts	1536247963158
enrichmentsplitterb.olt.splitter.begin.ts	1536247963155
enrichmentsplitterb.olt.splitter.end.ts	1536247963155
guid	f94f17ba-f5c0-4688-9f83-152849f8fc4
ip_dst_addr	147.32.80.9
ip_dst_port	53

Thank you