MIS|TI™ PRESENTS InfoSecWorld Conference & Expo 2018

YOU CAN'T FIX IT IF YOU CAN'T FIND IT

10 Techniques to Becoming the Ultimate Cyber Hunter

Dr. Vincent Berk & Dr. John Murphy

FlowTraq

WHAT IS CYBER HUNTING?

1. The Art of Looking for Trouble (in network data)

2. Human brain is still the best pattern matching tool out there

3. Cyber hunters combine knowledge of a specific network and knowledge of cyber threats to go exploring through data

> **“Like any hunt, can be targeted or opportunistic”**

FlowTraq

InfoSecWorld
Conference & Expo 2018

“WHY CYBER-HUNT?”

1. Automated tools are best-suited to finding pre-defined patterns
   - Zero-day exploits, by definition, aren’t pre-defined

2. Anomaly detection works best at large scales or on small well-defined systems

3. Danger signs are often only visible in retrospect, when:
   - breach is identified
   - vulnerability finally disclosed
   - new information provides context

4. Your employer has invested a lot of time and money making YOU an expert on your network
   - Cyber hunting is the single most effective way of directly applying that knowledge for a security benefit

Data Sources for Cyber Hunting

WHY CYBER-HUNT?

FlowTraq

InfoSecWorld
Conference & Expo 2018

FULL FIDELITY DATA

1. What is full-fidelity?

2. Why is it important?

   ❑ The most important clues are often the smallest: DNS queries, unsuccessful SSH attempts, single SYN packets sent to non-responding ports

   ❑ “Aggregation” and “sampling” are euphemisms for “we delete data”

WHY NOT FULL PACKET CAPTURE?

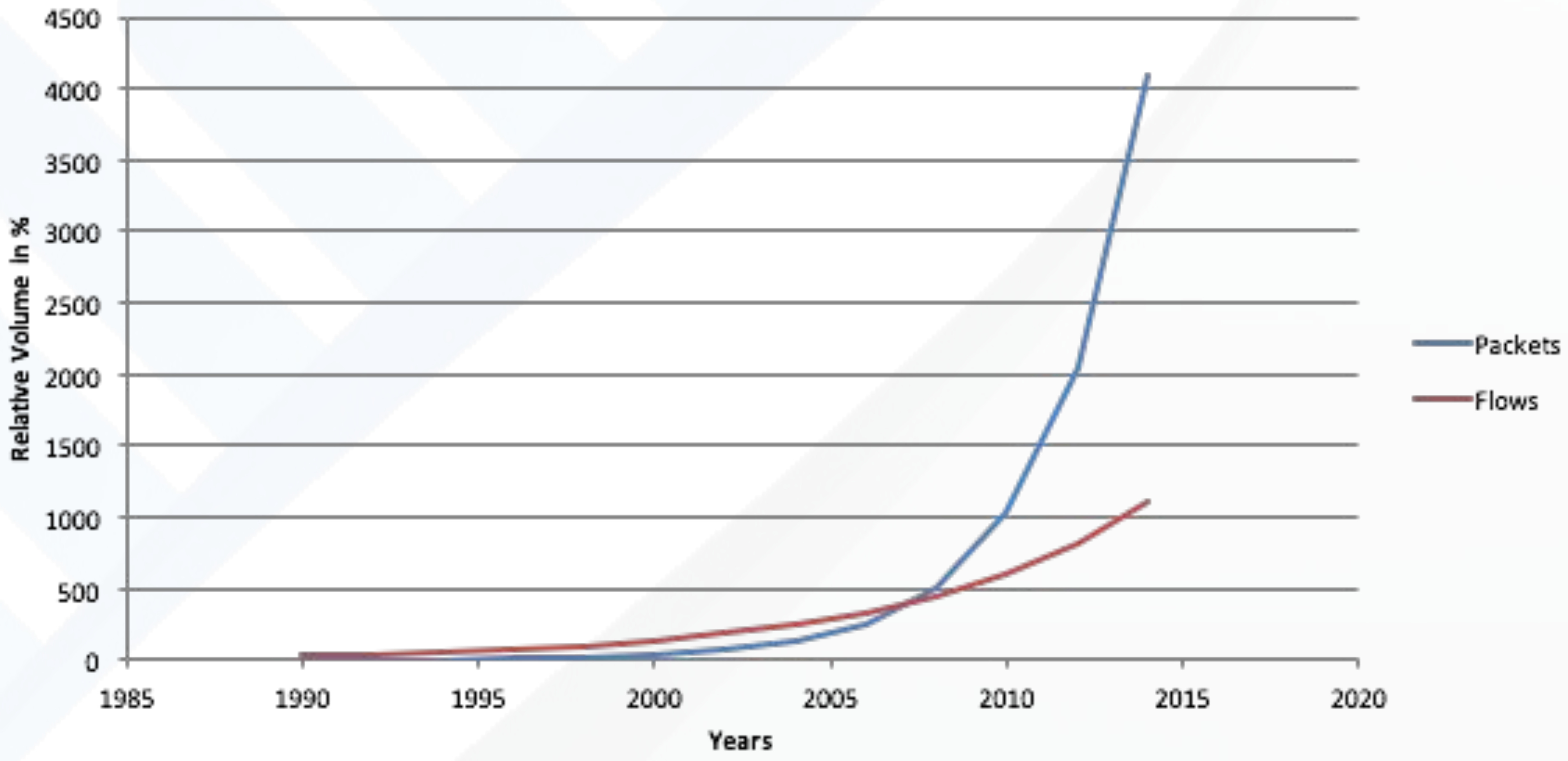
1. Packet capture is valuable as an investigation proceeds, but doesn’t work for cyber hunting: too information-rich, too hard to see the forest for the trees
2. Lends itself poorly to visualization and pivoting
3. Scales very poorly
4. Increased use of SSL and tunneling greatly reduce its benefit

WHY NETFLOW?

1. NetFlow and related technologies scale much more easily than packet capture

2. Unsampled data sources still commonly available from most vendors

3. Can be visualized and searched in real time without lengthy or expensive processing



FlowTraq

InfoSecWorld
Conference & Expo 2018

WHY PERFORMANCE MATTERS

1. Often the number one budgetary intangible: analysts know they need performance, but often struggle to articulate why

2. Cyber hunters require responsive systems – not just a “nice to have”

3. Hard to quantify “train of thought” but vital to pursuing a consistent hunt and maintaining a mental narrative of the items identified so far

4. Studies have shown that response time has a massive impact on operator responsiveness (think “first person shooter” video games as an extreme example, where network lag strongly affects performance)

TERMINOLOGY USED IN THIS LAB

“flow” – the record of a transfer of data from one host to another over a computer network

“session” – the record of at least one flow of data and optionally the return flow, defined by the host IPs, host ports, protocol, and exporting device

“partition” – a collection of session records defined by selected exporting devices, segregated for separate analysis to maintain differences between physically- and logically-distinct networks

“traffic group” – sometimes also called “host groups” or “managed objects”; groups of logically-organized IP addresses or CIDR blocks; e.g. “All Internal IPs”, “All my Web Servers”, “Accounting Department Desktops”

“alert” – a single tracked event, which may evolve over time, identified automatically

TOOL USED IN THIS LAB

1. FlowTraq Flex
   - free tool for small offices

2. Open source substitutes include the popular SiLK package from CERT, and YAF

Lab Overview

SECTION 1

SECTION 1 OBJECTIVES

1. Interpret and quickly navigate full-fidelity flow data
2. Find positive indicators of compromise such as outbound ddos attacks, cryptocurrency mining (bitcoin and monero)
3. Identify scanning and reconnaissance behaviors, brute forcing behaviors, large data movements and data theft and/or communication with command and control server
4. Effectively use data and threat feeds to identify overall patterns and abnormalities quickly

SECTION 2 OBJECTIVES

1. Identify common pivot techniques used by cyber-hunters when identifying the scope and severity of security incidents
2. Identify 'needle in a hackstack' search techniques and iterative drill-down methods
3. Identify important pre-incident context
4. Locate patterns post-incident

SECTION 3 OBJECTIVES

1. Follow the hackers' trail and identify compromised systems through multiple hops

2. Map the full extent of the compromise, and learn why shutting the bad guys out might not be the best first step

MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Dr. Vincent Berk & Dr. John Murphy

FlowTraq