CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS’

Real-time Protocol Shepherds

Raytheon BBN technologies

Ron Watro

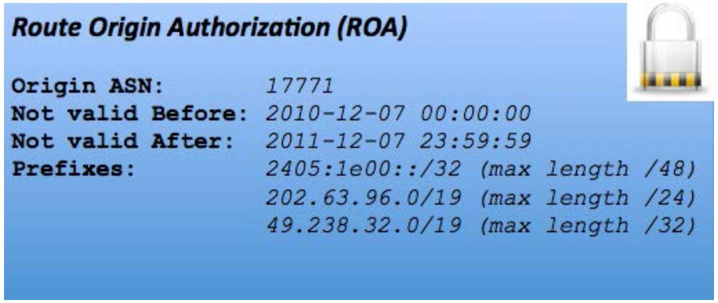
17 September 2013

Homeland Security

Science and Technology

Raytheon BBN Technologies

First Internet router

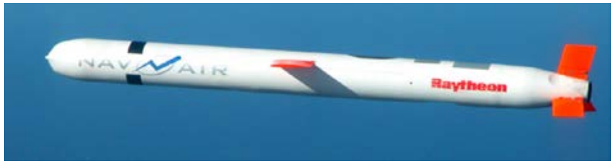


Route Origin Authorization (ROA)

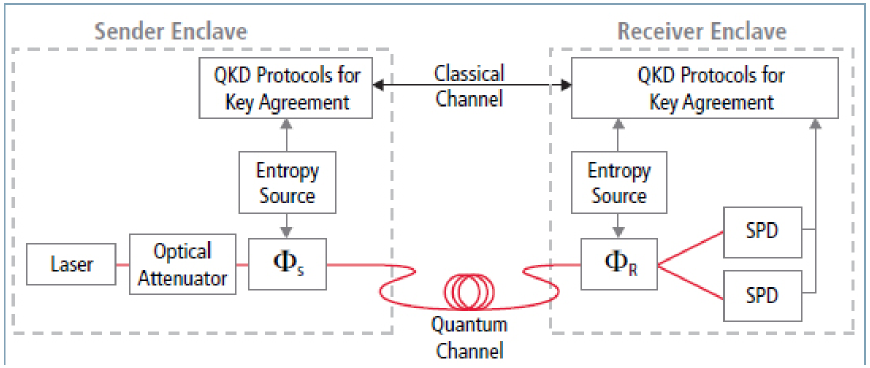
```
Origin ASN:          17771
Not valid Before:    2010-12-07 00:00:00
Not valid After:     2011-12-07 23:59:59
Prefixes:            2405:1e00::/32 (max length /48)
                     202.63.96.0/19 (max length /24)
                     49.238.32.0/19 (max length /32)
```

BGP Routing Security

National Technology Medal



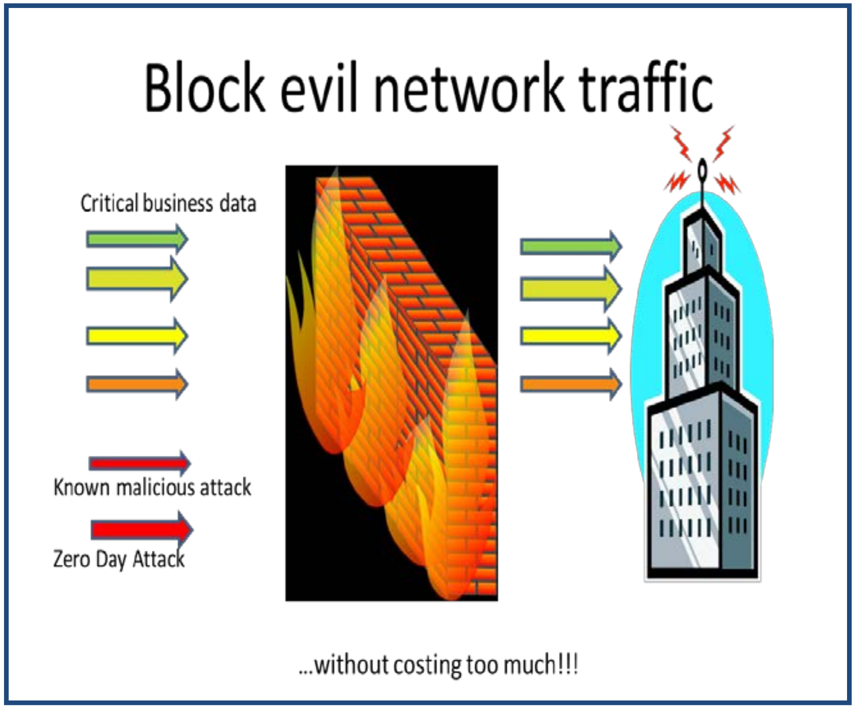
Acquired by Raytheon in 2010



First deployment of Quantum Key Distribution

Current programs: PlanX, ICAS, VET, CSFV, APAC, CRASH, CyberGenome, PROCEED, SAFER, MilNetP, …

Customer Need



Customers need automated, faster-than-human, response to sophisticated attacks

Attacks are commonly novel enough to bypass conventional signature checking

Advanced Persistent Threat (APT) does not announce itself; rather, it …

- Penetrates an enclave
- Remains resident and exfiltrates data
- Damage can be long lasting

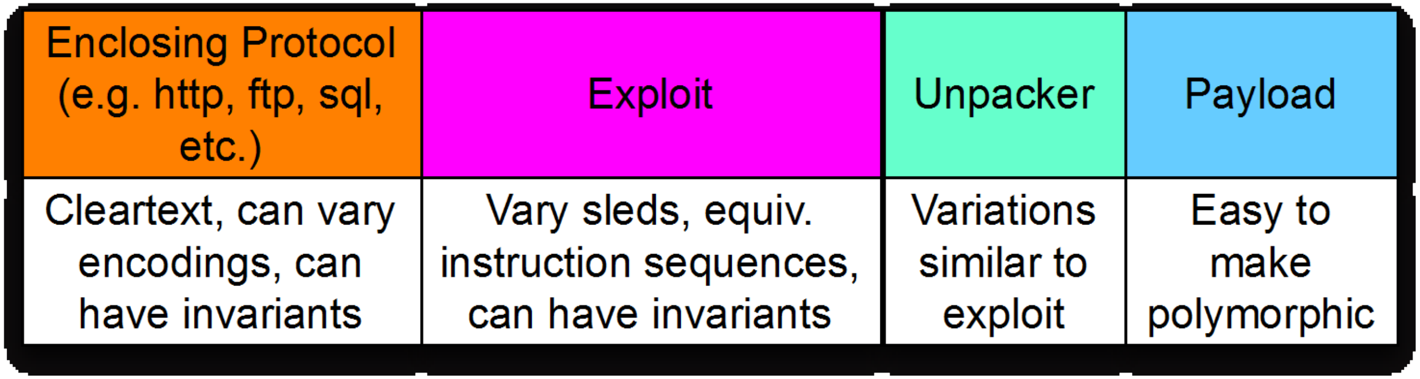
Approach

- RePS uses “inherent anomaly detection” as a basis for finding zero-day attacks
  - “Inherent” implies no training required
  - Based on detectors developed by BBN on the DARPA Scalable Network Monitoring (SNM) program
  - Deploying the sensors into existing open source programs
- Using a signature creation algorithm to create polymorphic signatures for the detected attacks
- Integrating Suricata (in-line mode) and Bro to deploy the tool

Sensors Deployed

	Name	Description
1	ICMP	The ICMP monitor checks for unreasonable packet lengths, strange/illegal IP headers, and use of unused or deprecated packet types and codes. The monitor checks for signs of a covert data channel (traffic tunneled over ICMP). It also checks for misuse of ICMP Redirects and ICMP Destination Unreachable (DU).
2	DNS	New sensors to support detection of DNS churning, poisoning, Kaminsky-style attacks, Akamai-like redirection/load-balancing, and detection evasion attempts
3	Flow Analysis	Detects long-term flows, traffic rates, "fat" flows, wrong-way traffic (out greater than in for client), overall traffic rates
4	Host Peering Characteristics	Sensors for sudden wide peering changes, half-peering, long-term peers.
5	Host / Ext Address Block Characterization	Tracks connection aspects of internal hosts and external host blocks. Estimate coarse-granularity traffic flow rates inbound and outbound.
6	Replicated Content Detection	Generates a signature from a set of suspected attack packets. This capability supports detection of polymorphic attacks by using a signature scheme that recognized specific small patterns (called n-grams) in varying locations in the attack.
7	Detection Correlations	A capability to combine the basic detections (1-5) into a range of required detection sequences, in order to obtain higher confidence in the results.

Attack Anatomy and Polymorphism/Metamorphism

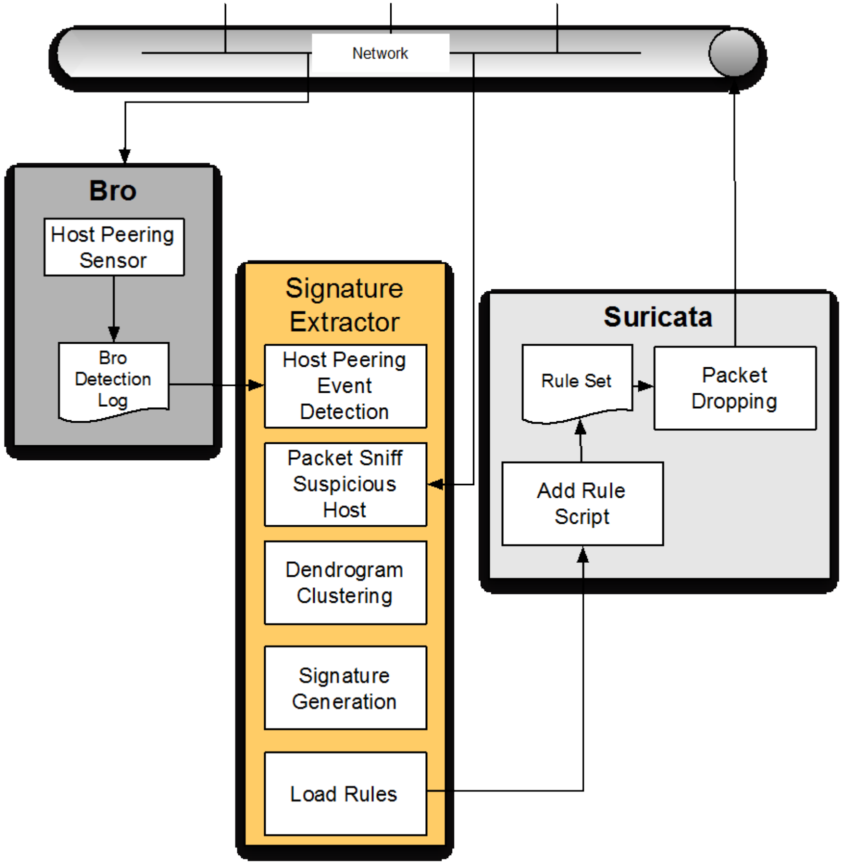


Enclosing Protocol (e.g. http, ftp, sql, etc.)	Exploit	Unpacker	Payload
Cleartext, can vary encodings, can have invariants	Vary sleds, equiv. instruction sequences, can have invariants	Variations similar to exploit	Easy to make polymorphic

- Polymorphic/Metamorphic malware changes between instances of an infection to avoid detection
- Worms make heavy use of this behavior
- Attack invariants – some portions of packet content that are used before the unpacker can have some of their content changed, but some elements are unchanged (e.g. required for the exploit)

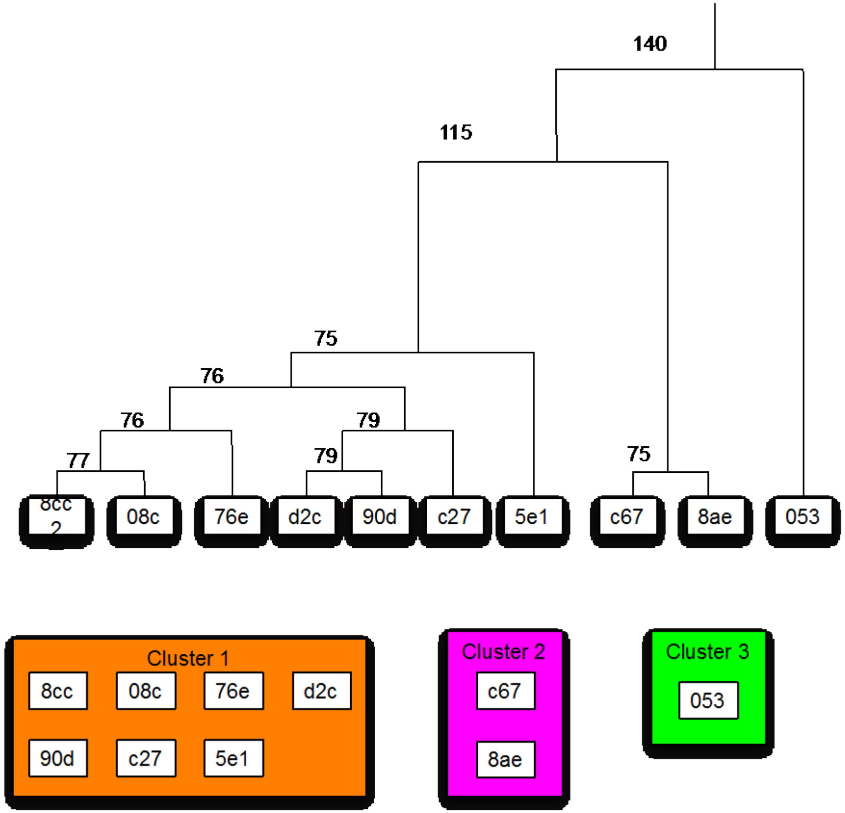
Signature Generation Architecture

- Bro
  - Host Peering sensor added to Bro and writes detections to Bro log
- Signature Extractor
  - Trigger on new Bro log event
  - Start collecting packets from suspicious host
  - Cluster packets
  - Generate signature for each cluster
  - Load rules into Suricata by calling script
- Suricata
  - Rules dynamically added
  - Rules loaded and inline packet blocking is enabled



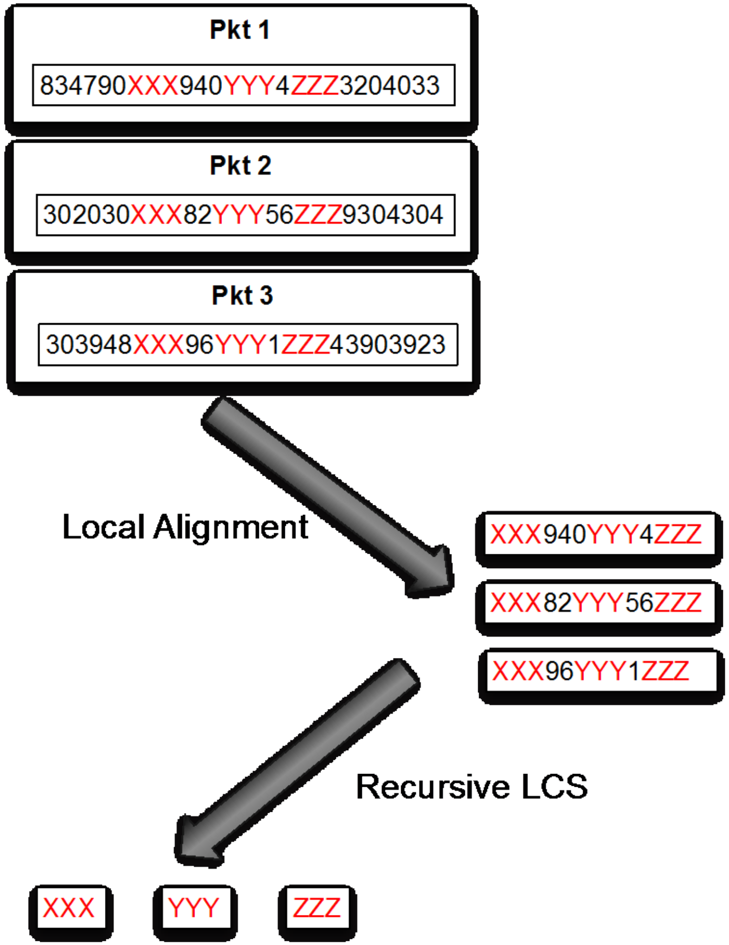
Dendrogram Clustering

- Technique borrowed from DARPA DECODE program
- Start with clusters of size one
- Distance metric is local alignment edit distance
- Find closest cluster and merge
- Distance between multi-element clusters is shortest between any two
- Cluster is broken off when next merge involves big jump



Signature Extraction

- Extract all Local Alignment (LA) pairs for a cluster and add to String of Interest (SI) list
- Apply recursive Longest Common Substring (LCS) algorithm to find all string sequence chunks common to all SI elements
- Signature consists of string chunks in sequence



Pkt 1

834790XXX940YYY4ZZZ3204033

Pkt 2

302030XXX82YYY56ZZZ9304304

Pkt 3

303948XXX96YYY1ZZZ43903923

Local Alignment

XXX940YYY4ZZZ

XXX82YYY56ZZZ

XXX96YYY1ZZZ

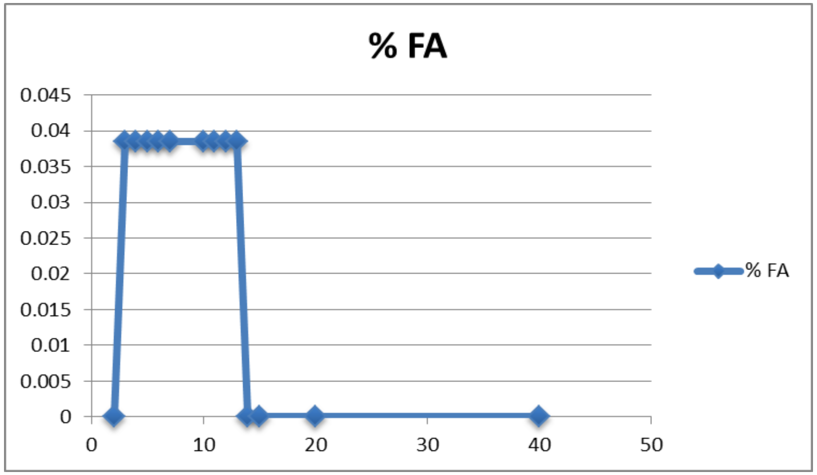
Recursive LCS

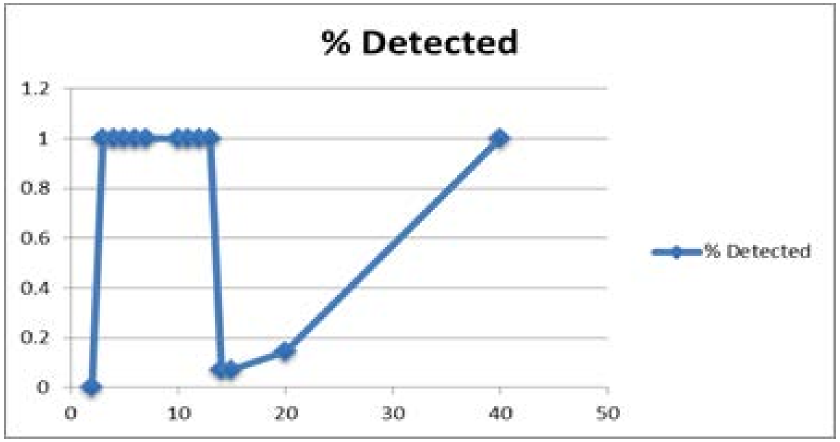
XXX

YYY

ZZZ

Sample Results for FTP attack





X-axis is number of packets used for signature generation

Benefits

- What is the value that your solution provides?
  - Adds new detection capacity to Suricata and Bro
  - Provides ability to generate highly accurate attack signatures in an automated manner
  - Fits well into an open source approach
  - Is expandable and works well with other approaches

Competition

	Signature	Anomaly	RePS
Coverage			
Known signatures	✓	🟥	🟥
Deviations from trained	N/A	✓	N/A
Deviations from normal	🟥	✓	✓
Encrypted attacks	🟥	Some	Some
Extensible	✓	🟥	✓
Scales w/ population	✓	🟥	✓
Scales w/ traffic	🟥	🟥	✓
Scales w/ attack type	✓	🟥	✓
Detection score	Tunable		
High Bandwidth	Costly	No	Yes
Zero Day Attacks	Few	Some	More!
Identify Attack	Specific	General	General
Determine Attack Success	No	Yes	Yes

Current Status

- Prototype capability has been developed
- Additional testing is underway
- Current work ends in November
- Follow-on opportunities being pursued

Next Steps

- What are your plans for the remainder of the effort?
  - Complete testing
- Technology Transition Activities?
  - Coordinate with Suricata and Bro
  - Reach out to commercial partners
  - Work the ideas inside Raytheon

Contact Information

- Ron Watro, rwatro@bbn.com
- Dan Wyschogrod, dwyschog@bbn.com
- David Mandelberg, dmandelb@bbn.com