Known Networks

Non-Actionable Network Filtering

Wayne Wheeles

Release 2 Innovation (R2i)

July 2016

Deny. Detect. Defeat.

About Release 2 Innovation

Founded in early 2014, Release 2 Innovation is a provider of Service Provider Intelligence (SPI) products collected from across the globe and delivered in the form of databases and services.

Release 2 Innovation provides Service Provider Intelligence through the Known Networks brand. Some of the largest healthcare provider networks and fortune 500 clients use Known Networks to focus resources on threats that are actionable. Clients can derive invaluable insights into internet infrastructure and environments which often cloud the efforts of security analysts and analytics.

Release 2 Innovation products and services enable clients to isolate and filter different classes of activity present on networks and minimize manual intervention. Our commitment is on delivering higher fidelity, lower costs results and analysis optimization.

Release 2 Innovation is a Service Disabled Veteran Owned Small Business (SDVOSB) and Veteran Owned Small Business (VOSB) privately held and based in Lothian, Maryland.

Deny. Detect. Defeat.

An Introduction to Known Networks

Known Networks is a database of Service Provider Networks that enables clients of all sizes the ability to isolate and filter network blocks by class based on their unique requirements:

- Analysts and analytics can quickly filter out “non-actionable” entities from the analysis process by applying pre-defined categories provided by **Known Networks** to result sets.

- Provides the ability to isolate entire classes of network activity with use of a single predicate for inclusion or exclusion from results.

- Comes with complete data structures that provide access to both classes and sub-classes of all filters.

- Customized Known Networks data sets can be developed and delivered as required based on client requirements.

- Database is updated monthly for subscribers.

Deny. Detect. Defeat.

Release2Innovations

The Analysis/Analytic Dilemma

Ever increasing Data Rates

- Network Usage is always increasing
- More end points and BYODs
- Social networking is everywhere
- More Entertainment and Videos

More to Analyze….

Demand for Measurable Results

- Quicker situational awareness and reporting
- Better blocking; less collateral damage
- Smarter signature development and deployment
- Focused metrics to measure effectiveness

More Reporting and actions required….

Limited Resources and Budgets

- Too few qualified analysts
- Not enough hours in the day
- Cyber budget is too small

Doing More with Less….

Demand for High Fidelity Results

- Less False Positives
- Less research spent on “non-actionable” entities
- Higher quality triage and production process

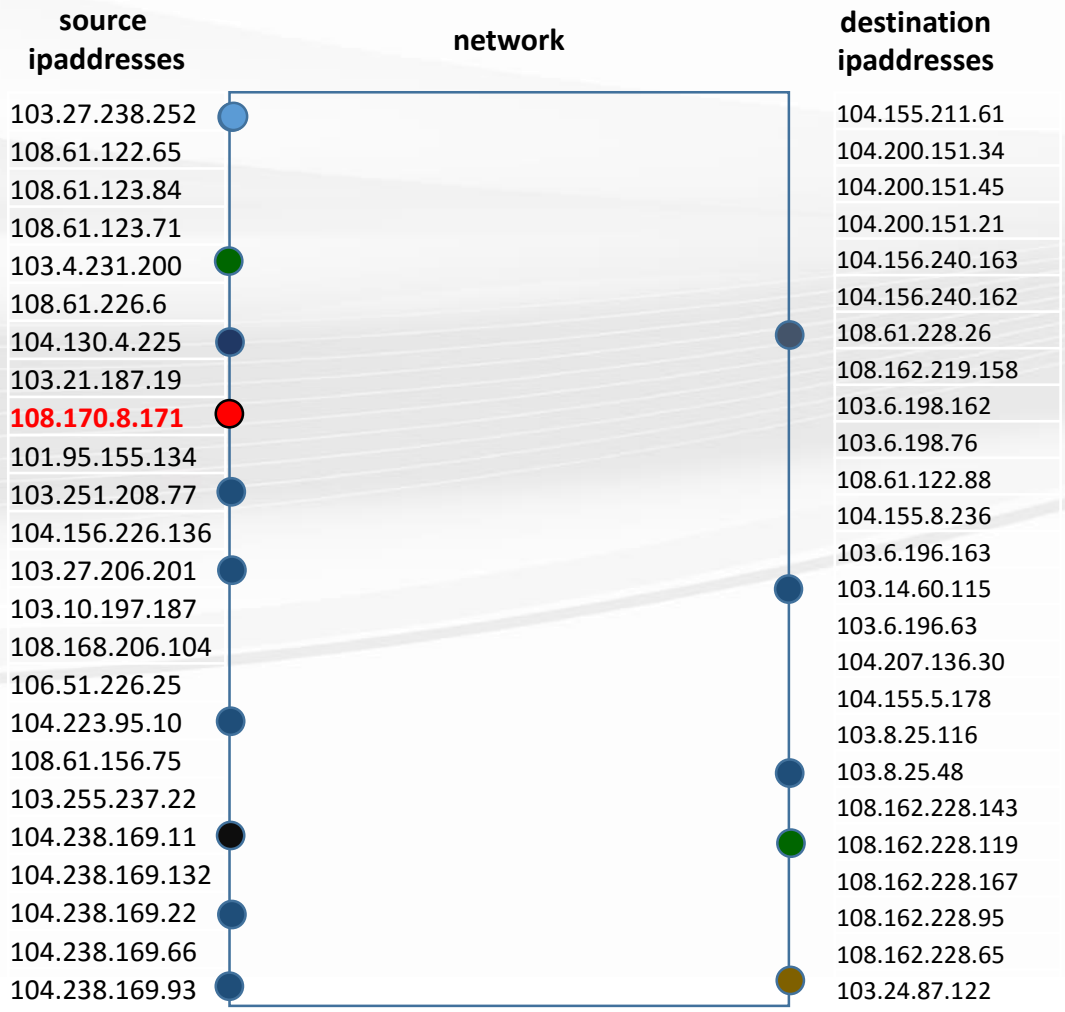
Making what is produced action ready….

Deny. Detect. Defeat.

Release2Innovations

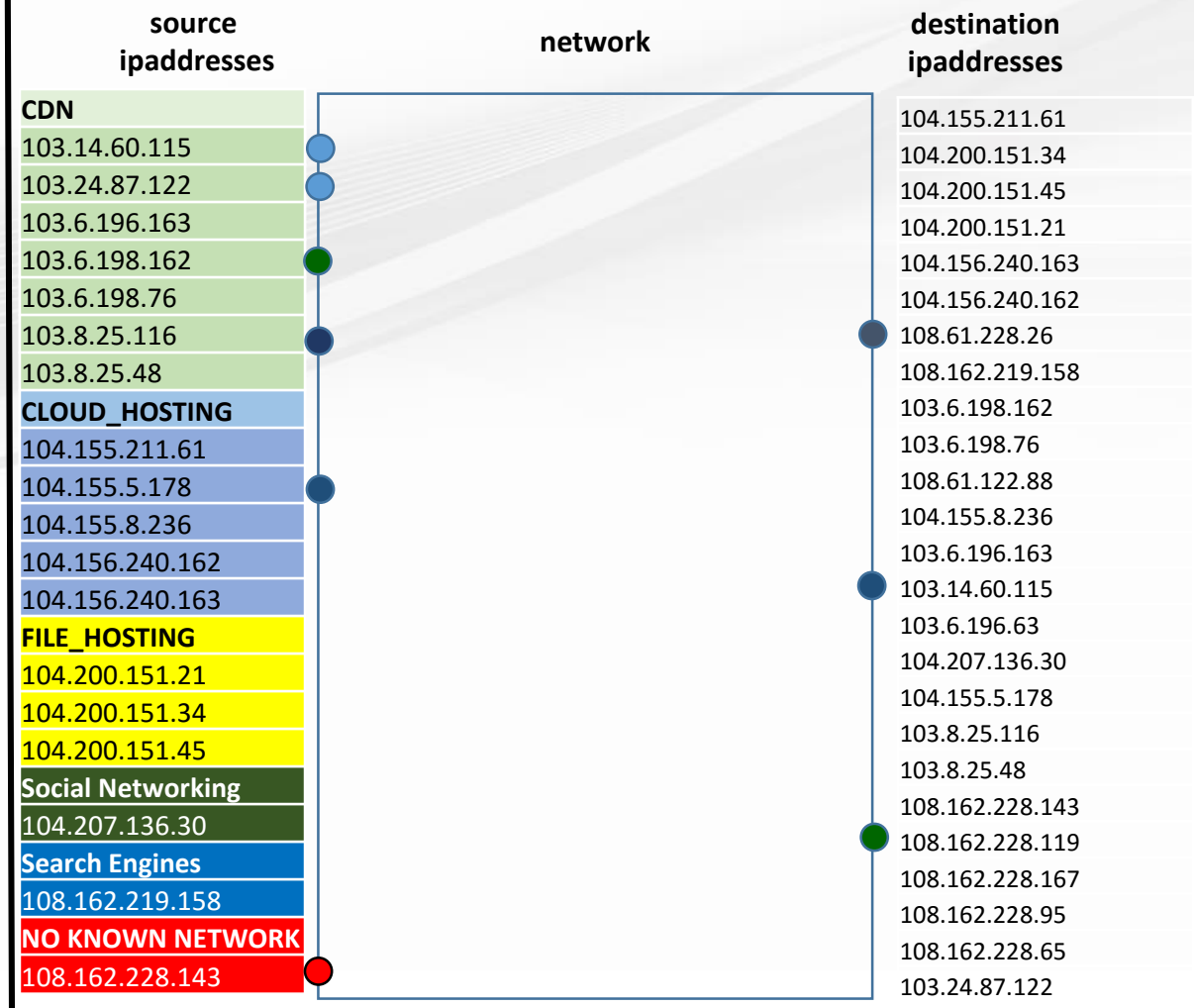
Analysis on Network Centric Data

Without Known Networks



Malicious Actor

Using Known Networks



The Solution: Known Networks "Network Types"

Clients in both the health care and manufacturing industries use **Known Networks** to make analysts more efficient by providing the ability to filter or isolate Service Provider networks using the following filters:

- Government (Federal)
- Academia (Universities, Schools, Labs, Institutes)
- Content Delivery Networks (Commercial, P2P, Free)
- Search Engines (Commercial)
- Cloud Hosting Environments (Cloud Hosting, Web Hosting)
- Social Networking (Commercial)
- File Hosting Services (Commercial)
- Internet Security Firms (Commercial)
- Entertainment (Music, TV, Video Sharing, Gaming)
- Internet Related Authorities (Government, Non-Profit, International)

Note: Additional data sets are available under strict NDA;
custom data sets can be created based on client requirements

Based on Known Networks Version 3.1

Deny. Detect. Defeat.

Release2Innovations

Known Networks: Data Model

The Known Networks data model was designed to provide maximum flexibility providing multiple levels of detail:

Network Type – Top level network type: CDN, Government, Cloud Hosting, Academia, Search Engine, Social Networking, File Hosting, Internet Security Firms, Entertainment, Internet Related Authorities

Network Group – Subset of the Network Type for Example: Cloud Hosting, Web Hosting are groups associated with the Cloud Hosting Network Type.

Network Name – The name of the organization associated with the ipaddress range

Address Range – The lower and upper bounding ipaddresses for a Organization

Deny. Detect. Defeat.

Release2Innovations

Simplification of Analysis: Known Networks

When tasked to develop an analytic that will not include any results from Content Delivery Networks:

Without Known Networks:

Select * from network_traffic where network_name not like '%INCAPSULA' or network _name not like '%CLOUDFARE%' or … (14 more)

- it would require a predicate for each statement calling into question efficiency and accuracy

Using Known Networks:

Select * from network_traffic where network_type <> 'CDN';

- Greater accuracy, great efficiency, speed, resulting in 35 – 50% reduction in "non-actionable" events.
- Simplicity with filtering

Deny. Detect. Defeat.

Release2Innovations

Platform Support and Data Set Formats

Platform and Distribution Support:

- MySQL, Maria DB, Oracle, IBM PureData for Analytics (Netezza)
- Hadoop: IBM Big Insights, Cloudera, Hortonworks
- HBASE, HIVE, Accumulo

Format Support:

- JSON
- Csv
- Stacked list (python-silk)
- Formatters for proprietary sets can be generated based on client specifications

Deny. Detect. Defeat.

Release2Innovations

Who is currently using Known Networks

- Department of Homeland Security
- US based Large Healthcare Network located in the US northwest
- US based Large Healthcare Network located in the US mid-west
- US based Large scale Manufacturer located in the Southeast

What is Known Networks being used for:

- Security Operations Analysis (SECOPS)
- Network Operations Analysis (NETOPS)
- Web traffic analytics

Deny. Detect. Defeat.

Demonstration: Known Networks

Demonstration 1 – 7 days of firewall data which was processed using their standard internal workflow, results were enriched with Known Networks and exported in Excel format.

Demonstration 2 – Client provided netflow data which was processed and exported as an extract for Visualization using Tableau.

Deny. Detect. Defeat.

Questions & Discussion

For **Known Networks** related information on other available data sets, questions or information on purchasing a subscription for **Known Networks** please contact us at knownnetworks@release2innovation.com

Known Networks – Simplifying the analysis and analytics process for network-centric data

Deny. Detect. Defeat.