**LARGE-SCALE INCIDENTS**

*a threat to private and national assets*

- **Large-scale Internet incidents**
  - BGP hijacks, connectivity outages, spam and fishing campaigns, botnet activities, large-scale bug exploitation, …
  - A major threat to public safety and to both public and private strategic and financial assets
- **often unnoticed**
- **hard to understand** (dynamics, motivation, infrastructure used, source, target)
  - hard to mitigate, prevent, etc.
  - hard to assess the impact
  - hard to assess restoration

**DHS CISA:** “there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend.”
Cybersecurity Analytics PaaS and SaaS

• Distributed infrastructure (PaaS) and software frameworks (SaaS)
  • for ingestion and correlation of streams of diverse cybersecurity data

• Web-based collaborative environment (SaaS) with trusted user groups
  • enabling analysis with interactive and visual tools, dashboards, ...
THE Hi³ APPROACH

three key concepts

1. Combination and correlation of diverse Internet cyber-security data streams...
   • Unwanted traffic, prefix hijacks, outages, DoS, spam, ...
   ..around a set of common dimensions
   • Time, geography, and Internet Coordinates (IP, BGP, DNS, …)

2. Data analytics in the form of interactive exploratory data analysis and configurable event detection

3. Trusted realtime collaborative environment
ARCHITECTURE
“EXPLORER” INTERFACE

Interactively transform, aggregate, compare, and visualize time series-based Internet data

• Last year’s demo shows how it can be used to investigate a potential massive bug exploitation

• 13th Oct 2015 - from 5.40pm UTC for about **25 minutes** a large spike in source IPs from all continents

• but among top 5 **US providers** we see it coming **only from TWC**!

• backscatter from UPnP machines that received spoofed packets to their **UDP port 1900 (UPnP)** originating from UDP port 80

FEATURED DATA FEEDS

Example: CAIDA’s BGP Hijacks Observatory

• Detects potential BGP Hijacking events by monitoring the Internet 24/7
  • Detects sophisticated attacks (NewEdge, Defcon)
  • Executes traceroutes during the event
  • Filters out many legitimate events
  • Assigns informative tags to events
  • Provides visualization of AS paths and traceroutes

• Y2: time series for correlation w/ outages, spam

https://dev.hicube.caida.org/feeds/hijacks
WHY “BUY”?  

What does the user (e.g., CISA) get

• **Benefits**
  • Enhances our ability to detect and understand large-scale incidents
    • The whole is better than the parts
      • Ability to correlate/combine/compare multi-type data on various dimensions
    • Provides live streams of data
    • Enables collaborative analysis
    • Access through a single entry point
  • Some “exclusive” data analytics. E.g., BGP Hijacking Observatory

• **Risks/Challenges**
  • Developing complex infrastructure
  • Incentivizing data sharing
WHY “INVEST” YOUR DATA & TIME?

Adding Data Feeds and Analytics Platforms

• Increase the **outreach** of your project/platform
  • Critical Mass adoption model

• **Lowers costs** to for data/analytics provision (leveraging existing UI, Visualization frameworks, DB infrastructure, Auth/Auth system, …)

• Research/Investigation: leverage combining your data with other data and using tools to quickly correlate/compare/etc.

• Creates opportunities for **collaboration**
COMPETITION

and synergy

- Internet telemetry data analysis and event detection systems typically
  - focus on a single type of data or one class of events
  - are non-collaborative

- Potential synergy with
  - DHS IMPACT performers
  - Threat intelligence platforms
MATURITY LEVEL

hicube.caida.org — dev.hicube.caida.org

• Prototype & development sites are both online

• Data Feeds:
  • Now: **Outages, BGP Hijacking, Network Telescopes** (UCSD, MERIT)
  • Soon: **MapKIT**: relevance of Autonomous Systems in a country’s Internet topology; identification of structural topological weaknesses of interest to an adversary state
  • Soon: **DoS** attack events

• Interfaces available now:
  • **Time Series Explorer** (transformation, detection, geographical viz, …)
  • Various project-specific interfaces

• Authorization and Authentication system deployed
THANKS