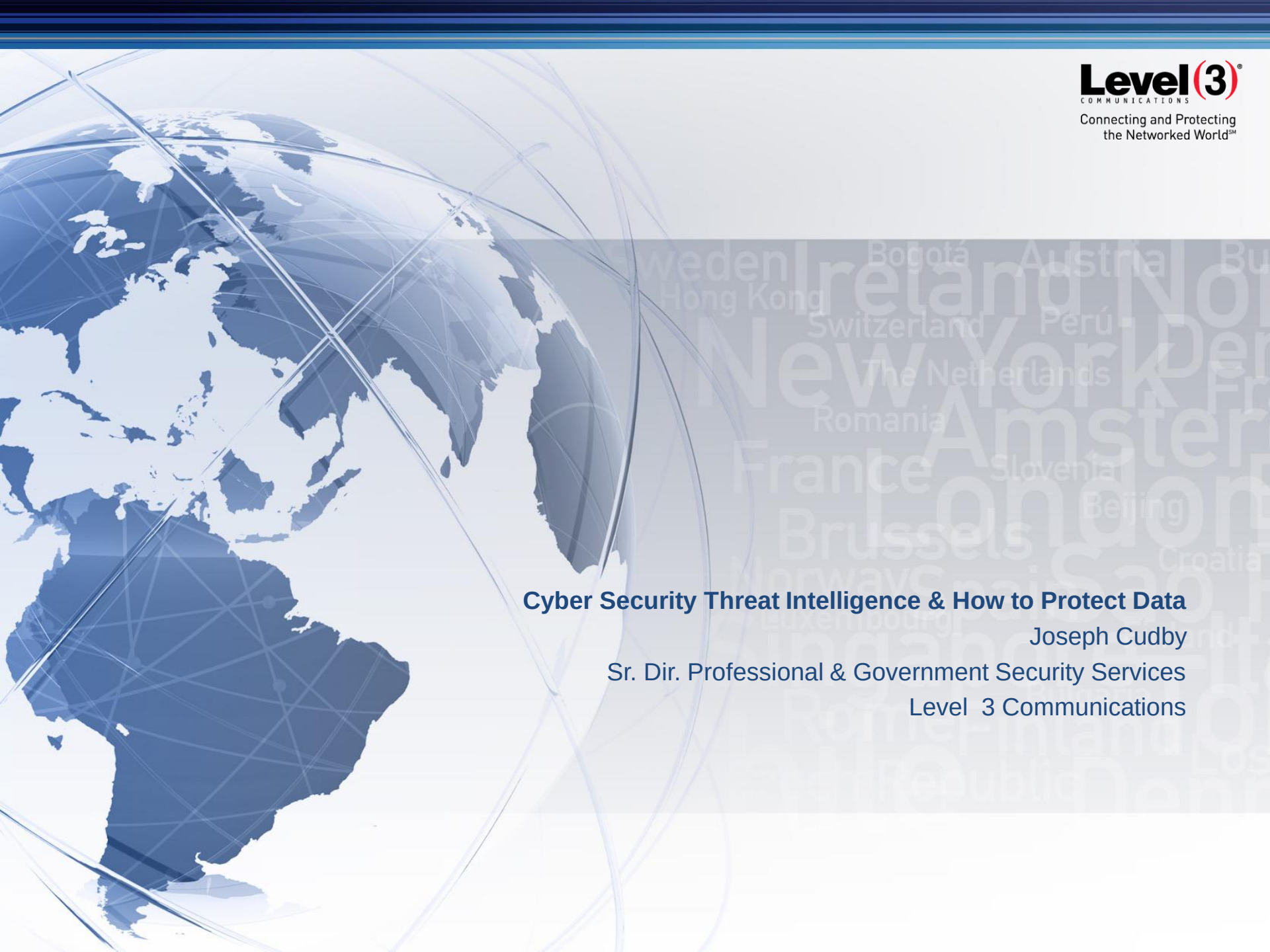


Level (3) COMMUNICATIONS
Connecting and Protecting the Networked World℠

Cyber Security Threat Intelligence & How to Protect Data

Joseph Cudby
Sr. Dir. Professional & Government Security Services
Level 3 Communications

A little about Level 3…

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Over **$8B** In Annual Revenue

~12,500 Employees

Hallo
もしもし
Bonjour Olá
Hola Hello 你好

Connecting **60+** Countries and Counting

200,000+ Route Miles of Fiber Globally

Approx. **360** Multi-tenant Datacenters

Security from Our Lens

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

We **monitor**
~1.3 billion
Security events per day

We **respond** to and
mitigate ~120
DDoS attacks a day

We **identify** and **remove**
at least **one C2**
network a month

We **monitor** over
45 billion
NetFlow sessions per day

We **collect**
~87 TB
of data per day

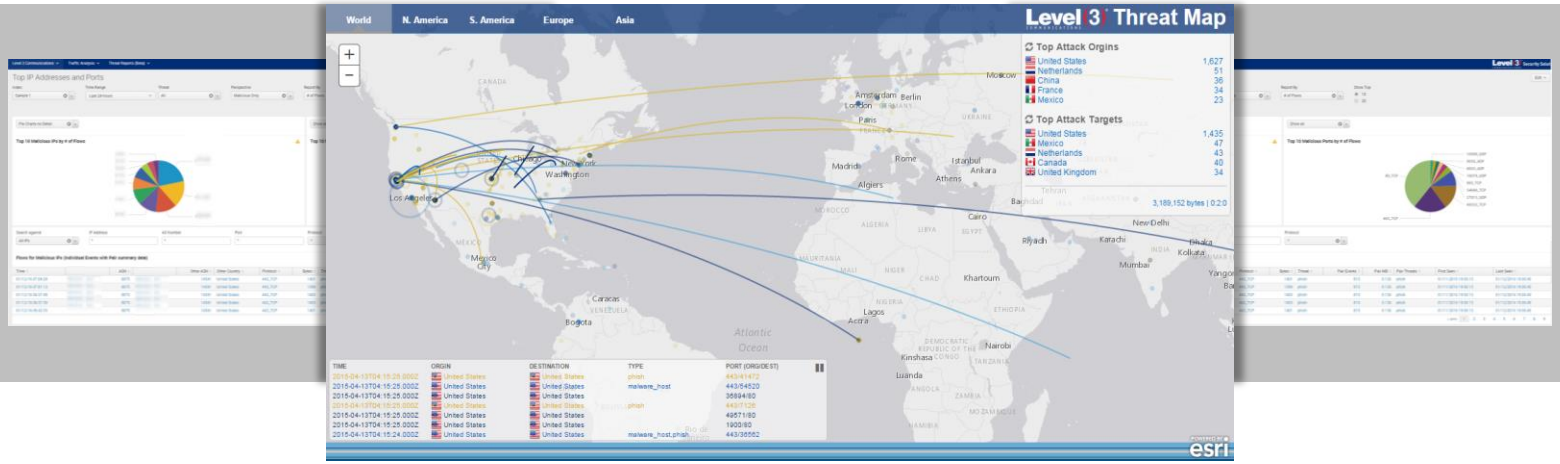
We perform
daily audits,
protect and monitor
all our products & systems

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Threat Intelligence – Process & Technology

Protection Approach

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠



KNOW WHAT YOU ARE PROTECTING

- Inventory your data, systems, applications and locations
- Know the importance of your intellectual property
- How is it being accessed and by whom

THREAT INTELLIGENCE

- Global Threat View
- Behavior Monitoring
- Internal and External Honeypots
- Social Honeypots

ADVANCED PROTECTION

- Segmentation
- DDoS Protection
- SandBoxing

MONITORING

- Independent security layer monitoring
- Invest in SOC, Incident Response and Forensic analysis

Threat Intelligence Data

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Collected and curated data driving reputation

- Automated retrieval of publicly published lists.
- Manual retrieval of OSINT data.
- Purchases of non-public lists.
- Real matches from our sensor network (Q3)

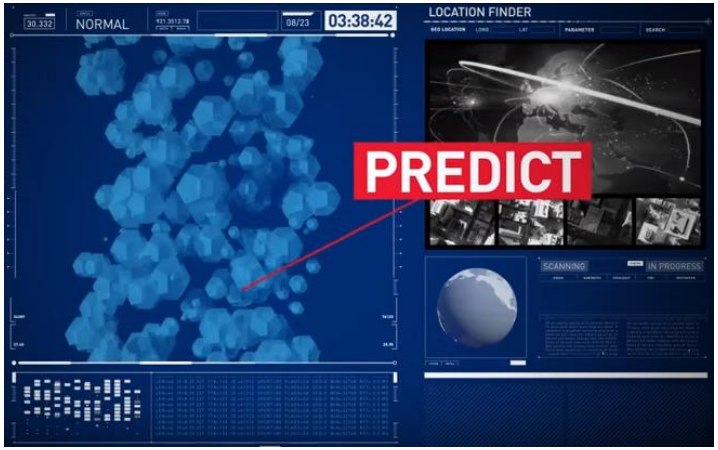
Developed data driving reputation

- Proprietary Level 3 algorithms.
- Tracking of new IOCs from campaigns/botnets.
- Machine-learning-driven models finding new IOCs.
- Anomaly detection on the Internet-feeding models (Q3).
- Detailed analyst-driven analytics on events and risks.
- Aggregated risk scoring, driving focused response.

Level 3 obtains approximately

45 billion

sampled NetFlow **records per day.**



Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Threat Intelligence - Process & Technology - Some Lessons Learned

Deriving Value from Big Data

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Lessons Learned

Life Cycle of Data Operation

- Identify Sources of Data
  - Where are they?
  - What are they?
  - What format is the data in?
  - How much data is there?
- Verify that YOUR systems are generating clean data
  - How do you verify that the data stream is correct and reliable?
- Verify that collaborative systems are generating clean data
  - How are you verifying that?
  - Must continue to monitor and refine the data
  - Reports must continue to provide **actionable information**
- Value of reports over time
  - Must evolve or will eventually be ignored

Deriving Value from Big Data

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Lessons Learned continued

- **Very easy to underestimate resource requirements**
  - You will need 5x more than you think of everything…
- **Time is a real factor**
  - Writing queries across a huge volume of data (billions of rows) potentially in multiple repositories takes time (days!)
  - Running queries takes time
- **Developer and Analyst skill sets are hard to find**
  - Tenacity is key as well as willingness to “come up empty”
  - Analysts must be able to write code – not just SQL queries
  - Developers and analysts must work together to be successful

Enterprise Privacy Concerns

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

- Intellectual Property
- Market Share Data
- Competitive Data
- Financial Information
- Strategic Information
- Employee Privacy
- Customer/CRM Data
- Test and Development

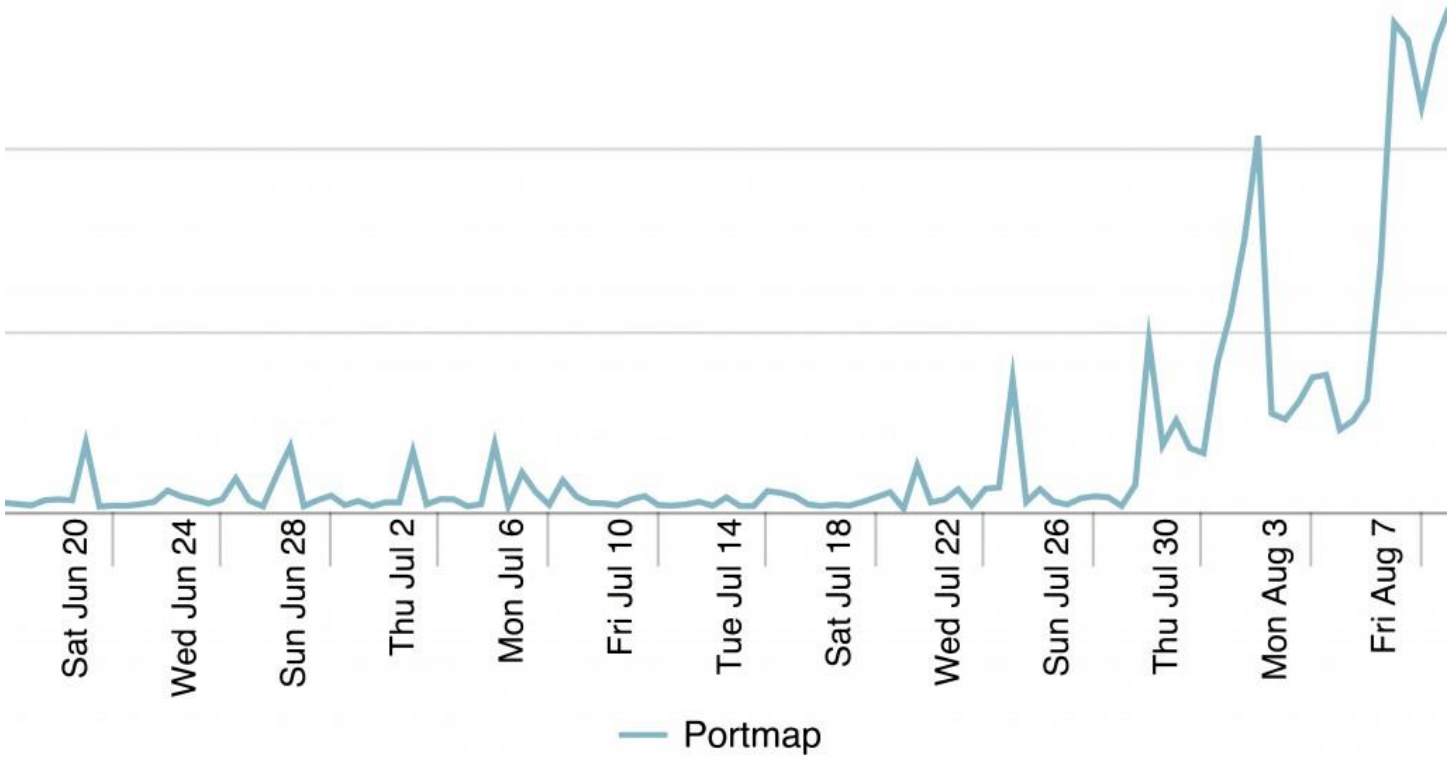
Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Threat Intelligence - How the Information can be used to protect yourselves and others

Old Playgrounds for New Tricks

DDoS Attack Vector: Portmapper

Level (3) COMMUNICATIONS
Connecting and Protecting the Networked World℠

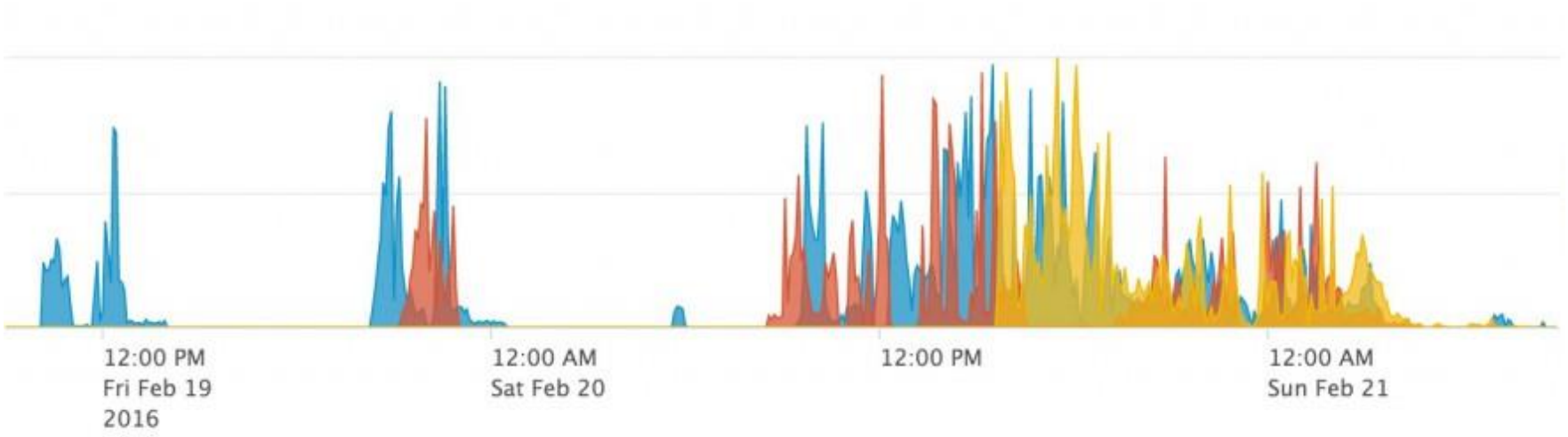


- **News Articles:** US-Cert, SC Magazine, threatpost, The Register, eWeek, TechRadar, TechWorld, IT World Canada

New Playgrounds for Old Tricks

The Linux Mint Backdoor: Kaiten Dos Bot

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠



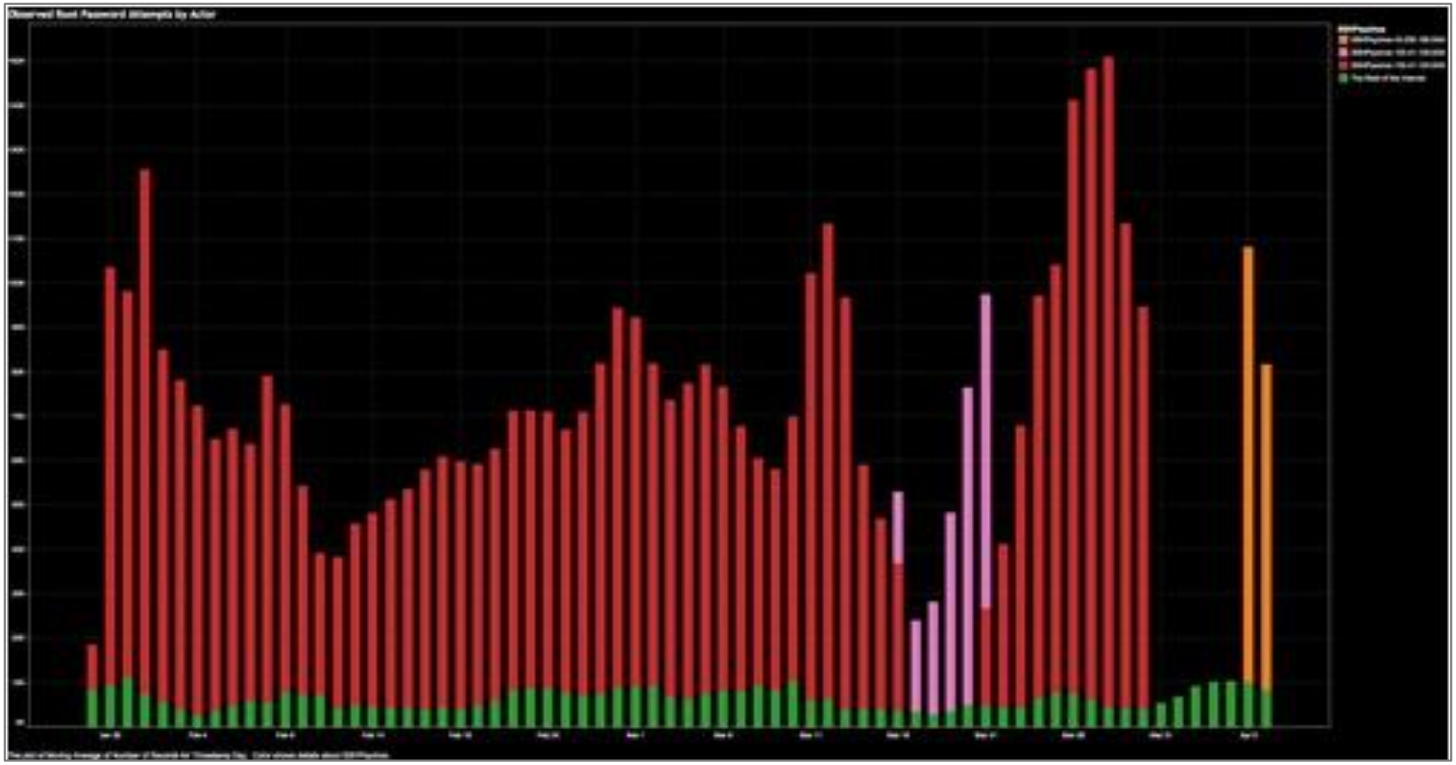
5.104.175.212
5.104.175.214
5.104.175.216

Using Threat Intelligence to Take Action

SSH Psychos

Level (3) COMMUNICATIONS
Connecting and Protecting the Networked World℠

SSH Psycho Traffic Vs. Rest of the Internet



- A visual depiction of the SSHPyscho traffic verses SSH traffic of the rest of the Internet

Threat Intelligence - To share or not to share ?

The Power of a Collective Response

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

InformationWeek DARKReading

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

"Researchers Disrupt Angler Exploit Kit, Ransomware Operation… estimate Angler is making **$60 million per year** from ransomware alone."

"Cisco, Level 3 Disrupt SSH Brute Force Attacks Used to Deliver DDoS Bot…at times, the attackers' activities accounted for **more than a third** of the total Internet SSH traffic."

Collaborate with Service Providers and Peers

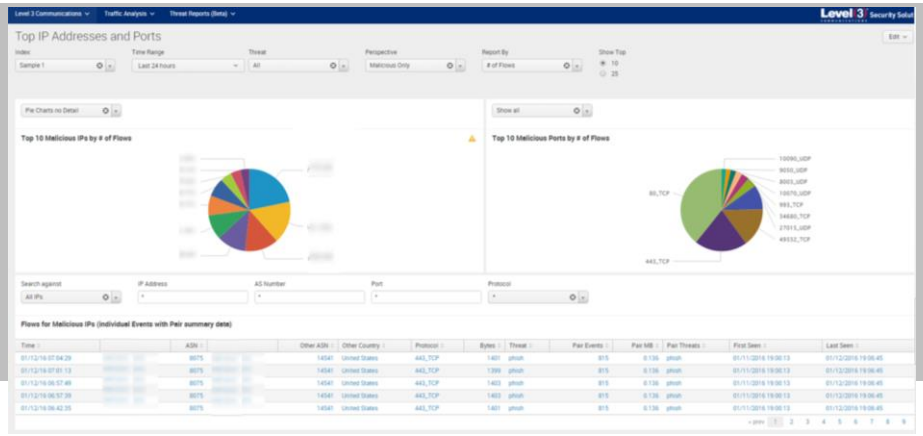
Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

- The threat landscape is evolving rapidly
- Collaboration with peer organizations is vital
- Determine core competencies, perform functions that you do well, outsource others
- Some security functions must be done in partnership with your service provider(s)
- Take advantage of government resources: standards, programs, events, consortiums, services
- Information sharing partnerships are essential

Barriers To Collaboration

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

SHARED
Threat Data



NOT SHARED
Victim Data

- Consumer and enterprise concerns about privacy
- Victim organizations concern of damage to brand reputation
- Threat research industry concern of eroding commercial value of threat data or security services
- Lack of resources to put toward threat collaboration
- Not a priority: focus is on blocking, not removing threat

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Thank You