Agenda: Coordinating Attack Response at Internet Scale (CARIS) Workshop

19 June 2015, InterContinental Berlin, Charlottenburg Room

9:00 AM: Introduction – Level setting

- Challenges that we are facing/goals for the workshop (Kathleen Moriarty) – 15 minutes

9:15 AM: 5 minute lightning talks on data exchanges/attack type mitigations described in template submissions.

- Describe your use case?
- Where they are focusing?
- How can others engage with them?
- Who participates?

Presenters:

- Rossella Mattioli
- Foy Shiver
- Wes Young
- Tom Millar
- Cristine Hoepers
- Sharifah Roziah Mohd Kassim
- Roman Danyliw

10:00-10:45 AM: Mat Ford – Moderated discussion: Challenges organizations are facing and opportunities for collaboration.

- Where do good connections exist and how can more be facilitated?
- How did your group overcome legal challenges?
- Does vendor/law enforcement participation have an effect on your operational efforts?

10:45-11:00: 15 minute break

11:00 AM: Dave Dittrich. With great power comes great responsibility: Scaling Responses to DDoS and BotNets Effectively and Safely.

Agenda: Coordinating Attack Response at Internet Scale (CARIS) Workshop

11:30 AM: Panel on Scaling Attack Response for DDoS and BotNets

Lightning Talk by each panelist (one per paper) followed by a discussion

- Nik Teague. DOTS DDoS Open Threat Signaling.
- Liang Xia, Tianfu Fu, Cheng He, Tobias Gondrom and Danping He. An Elastic and Adaptive Anti-DDoS Architecture Based on Big Data Analysis and SDN for Operators.
- Ulrich Seldeslachts. ACDC – Advanced Cyber Defence Center pilot action results and activities.
- John Kristoff. An Internet-wide BGP RTBH Service.

12 or 12:30-1:30: Lunch. Food is provided – Attendees may attend closing FIRST talks

1:30-2:45 PM: DNS & RIRs: Attack Response and Mitigation Methods

Lightning talks followed by a panel.

- Mirjam Kuehne, **Ivo Dijkhuis**. RIPE NCC: Useful Data and Tools for Operators and Abuse Handlers.
- Merike Kaeo. Leveraging DNS to Help Counter DDoS, Malware, Phishing, Spam, and Other Attacks.
- John Graham-Cummings, **Michael Daly** and Olafur Gudmundsson. CloudFlare is at the center of internet attacks.
- Graciela Martinez, LACNIC. The Role of the Regional Internet Registries in Global Incident Management.
- John Crain. ICANN Template Submission.

Panel Lead: Mirjam Kuehne (RIPE)

Answering the questions:

- What attacks are most prevalent and what mitigation methods are most effective?
- Does collaboration between RIRS and TLDs impact effectiveness? Can it be improved?
- Discussion of challenges and possible solutions.
- Interactions with country-level CSIRTs and operators, what works and what can be improved?

Agenda: Coordinating Attack Response at Internet Scale (CARIS) Workshop

Papers (not speaking):

- Nick Biasini and Craig Williams. Exploit Evolution and Advanced Threats.
- Gonzalo Romero. How the .CO ccTLD handles cybersecurity – Cooperate Action on Colombian and Global cybersecurity and cyberdefense issues.

2:45 PM:

Mio Suzuki, Daisuke Inoue and Takeshi Takahashi. Cross-Organizational Incident Information Sharing using a Darknet Monitoring System (10 Minutes, 5 minutes of questions).

3:00 PM:

Mohamed Boucadair, Christian Jacquenet and **Linda Dunbar**. Integrating Hosted Security Functions with On-Premises Security Functions — Joint Force to Mitigate Internet attacks (5 minute talk and 10 questions).

3:45 PM:

- Pat Cain – Trust, Privacy and data markings (20 minutes)
- Privacy/Sharing discussion (Andrew Sullivan & Ted Hardie) 40 minutes
  - How to manage scale and scope of information sharing
  - How to get into these communities
  - Does the operator-driven sharing get you away from this problem because it's more of a broker model?
  - How do vendors fit in?

Panel for discussion on 'Trust and Privacy'

Panel Members: Pat Cain, Chris Morrow, Nancy Cam-Winget, Dave Cridland

Reading list:

- Patrick Cain. Technical Formats and Laws are not the Barriers to Improved Attack Data Sharing.
- Joseph Hall. The Technical Gap in Information Sharing Policy.
- Chris Morrow. Operations Security Administration Template Submission.
- Nancy Cam-Winget, Syam Appala and Scott Pope. Enabling Security Information Sharing.

Agenda: Coordinating Attack Response at Internet Scale (CARIS) Workshop

- Dave Cridland and Nick Leaver. Countering the Cyber Threat through Trusted and Secure Cross-Domain Collaboration.

4:45 PM: Break

5:00 – 6:00 PM

- How the Internet architecture helps or hurts their cause, and what operators and CSIRTS need from the IAB (Eliot Lear)
  - Permission models, encryption, identity, privacy etc.
  - WEIRDS, how do these changes affect incident responders?

Reading list for discussion:

- Jessica Steinberger, Anna Sperotto, Harald Baier and Aiko Pras. Exchanging Security Events of flow-based Intrusion Detection Systems at Internet Scale.
- Scott Pinkerton and Chris Strasburg. Coordinating Attack Response at Internet Scale.
- Dave Cridland and Nick Leaver. Countering the Cyber Threat through Trusted and Secure Cross-Domain Collaboration.
- Paweł Pawliński and Adam Kozakiewicz. Lowering Cost of Data Exchange for Analysis and Defence.
- Nancy Cam-Winget, Syam Appala and Scott Pope. Enabling Security Information Sharing.

Conclusions and next steps

Socialize – we'll head out for cocktails/beer and food

Supplemental Reading

- Eric Burger. Barriers to Automated Threat Intelligence Sharing.
- Arnold Sykosch and Matthias Wuubbeling. STIX 2 IDS.
- Tomas Sander. Human Aspects of Security Collaboration.

Lunch and breaks sponsored by EMC

Evening social sponsored by the Internet Society (boat river tour with dinner)