Internet Architecture Board (IAB)
Request for Comments: 8073
Category: Informational
ISSN: 2070-1721

K. Moriarty
M. Ford

March 2017

Coordinating Attack Response at Internet Scale (CARIS) Workshop Report

Abstract

This report documents the discussions and conclusions from the Coordinating Attack Response at Internet Scale (CARIS) workshop that took place in Berlin, Germany on 18 June 2015. The purpose of this workshop was to improve mutual awareness, understanding, and coordination among the diverse participating organizations and their representatives.

Note that this document is a report on the proceedings of the workshop. The views and positions documented in this report are those of the workshop participants and do not necessarily reflect IAB views and positions.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Architecture Board (IAB) and represents information that the IAB has deemed valuable to provide for permanent record. It represents the consensus of the Internet Architecture Board (IAB). Documents approved for publication by the IAB are not a candidate for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8073.

Table of Contents

1. Introduction

The Internet Architecture Board (IAB) holds occasional workshops designed to consider long-term issues and strategies for the Internet, and to suggest future directions for the Internet architecture. This long-term planning function of the IAB is complementary to the ongoing engineering efforts performed by working groups of the Internet Engineering Task Force (IETF), under the leadership of the Internet Engineering Steering Group (IESG) and area directorates.

The Internet Architecture Board (IAB) and the Internet Society (ISOC) hosted a day-long Coordinating Attack Response at Internet Scale (CARIS) workshop on 18 June 2015 in coordination with the Forum for Incident Response and Security Teams (FIRST) Conference in Berlin. The workshop included members of the FIRST community, attack response working group representatives, network and security operators, Regional Internet Registry (RIR) representatives, researchers, vendors, and representatives from standardization communities. The key goals of the workshop were to improve mutual awareness, understanding, and coordination among the diverse participating organizations. The workshop also aimed to provide the attendees with greater awareness of existing efforts to mitigate specific types of attacks, and greater understanding of the options available to collaborate and engage with these efforts.

The day-long workshop included a mix of invited talks and panel discussion sessions with opportunities to collaborate throughout, taking full advantage of the tremendous value of having these diverse communities with common goals in one room. There were approximately 50 participants engaged in the CARIS workshop.

Attendance at the workshop was by invitation only. Prior to the workshop, existing attack-mitigation working groups were asked to complete a survey. The data gathered through this questionnaire, including how third parties can participate in or contribute to the attack-mitigation working group, was shared with all of the participants at the workshop to better enable collaboration [ISOC]. Attendees were also selected from submissions of two-page position papers that included some key insight or challenge relevant to the broader group. Paper topics included research topics related to attack mitigation or information sharing/exchange, success stories, lessons learned, and more in-depth studies on specific topics such as privacy or trust.

The program committee received 25 papers and 19 template submissions. The template submissions will be maintained by the Internet Society, and as a result of the workshop, they will be amended to provide

additional value to the Computer Security Incident Response Teams (CSIRTs) and attack response communities/operators on their information exchange capabilities. The CARIS participants found the template submissions to be very useful in coordinating their future attack mitigation efforts. This initiative is a new, open for the global community, and hosted in a neutral location. All submissions are available online and are linked from the agenda [AGENDA].

The workshop talks and panels involved full participation from attendees who were required to read all the submitted materials. The panels were organized to spur conversation between specific groups to see if progress could be made towards more efficient and effective attack mitigation efforts. See [KME] for additional information on possible approaches to accomplish more effective attack response and information exchanges with methods that require fewer analysts.

The workshop was run under the Chatham House Rule to facilitate the exchange of sensitive information involved with incident response. As such, there was no recording, but minutes were taken and used to aid in the generation of this report. Comments will not be attributed to any particular attendee, nor will organizations be named in association with any discussion topics that were not made public through submission templates or papers by the submitter and organization.

2. Sessions and Panel Groups

After an initial presentation to set the stage and elaborate the goals of the workshop, the day was divided into five sessions as follows:

1. Coordination between CSIRTs and attack-response mitigation efforts

2. Scaling response to Distributed Denial-of-Service (DDoS) and botnets effectively and safely

3. Infrastructure: DNS and RIR providers and researchers

4. Trust and Privacy with the exchange of potentially sensitive information

5. Implications for Internet architecture and next steps

The remainder of this report will provide more detail on each of these sessions.

2.1. Coordination between CSIRTs and Attack Response Mitigation Efforts

The first panel session on Coordination between CSIRTs and attack mitigation efforts included representatives from several organizations that submitted templates describing their organization's attack mitigation efforts. This panel was purposefully a cross section of organizations attending to see if there were new opportunities to collaborate and improve efficiency, thereby better scaling attack mitigation. The panelists described their efforts with the following questions in mind:

- What is the use case for their organization?
- Where are they focusing their efforts?
- How can others engage with their organization?
- Who participates in their organization today?

For each of the following organizations, additional information can be found in their template submissions [ISOC].

The following summaries are to be read in the context of the workshop and not as standalone descriptions for each organization. These summaries are a result of the workshop discussions.

- ENISA is the European Network and Information Security Agency [ENISA]. While ENISA provides support for the community in the form of education, training, and collaboration on security and attack mitigation, it does not offer a service for attack response or mitigation.
- The Anti-Phishing Working Group (APWG) offered examples of operator-driven exchanges focused on specific use cases that involve hundreds of participating organizations daily. The APWG operates a data clearinghouse and provides infrastructure to support meaningful data exchanges and maintains a current set of data through these interactions. More can be learned on the APWG website [APWG] in addition to their template submission.
- The Research and Education Networking Information Sharing and Analysis Center (Ren-ISAC) employs an interesting operational model that scales well through automation, exchanging actionable information between 500 universities and automatically implementing controls. Since many universities cannot respond to incidents in real time due to a scarcity of resources, REN-ISAC leverages a small number of analysts to accomplish the task of protecting many universities through automation. The key to the

success of their project is providing tools that allow organizations to make use of incident data operationally. They are currently working to develop open-source tools to track metrics more formally [REN-ISAC].

- CERT.br is the Brazilian Computer Emergency Response Team (CERT) that has made impressive progress in a short amount of time. CERT.br is the national focal point for incident reporting, collection, and dissemination of threat and attack trend information in Brazil. CERT.br works to increase awareness and incident-handling capabilities in the country as well as assisting to establish new CSIRTs. In addition to providing training and awareness campaigns, they distribute network security honeypots and have a primary focus on network monitoring. CERT.br requires active participation from third parties wishing to collaborate and exchange data with them [CERT.BR].

- MyCERT's mission is to address the security concerns of Malaysian Internet users and reduce the probability of successful attacks [MYCERT]. They have been operational since 1997. MyCERT is responsible for incident handling of unauthorized intrusions, identity theft, DDoS attacks, etc. MyCERT handles computer security incidents in Malaysia, provides malware research, and technical coordination. In addition to incident response and coordination activities, MyCERT members provide talks and training, as well as local and regional security exercises. MyCERT also provides incident alerts and advisories on vulnerabilities, breaches, etc.

- The CERT Coordination Center (CERT/CC) has been operational since 1998 on an international and national scale [CERTCC]. They have long been known for their software vulnerability work and the national vulnerability database in the US (Common Vulnerabilities and Exposures -- CVEs) and informing organizations of vulnerabilities. CERT/CC helps to coordinate between vendors and researchers for improved collaborations. CERT/CC provides guidance on dealing with the aftermath of incidents, risk assessment best practice, bug bounties, and other incident-related areas.

Highlights from the panel discussion:

- Passive surveillance by state actors has impacted incident response activities due to the erosion of trust between communities.

- Government involvement in information exchange efforts has not been productive. Despite lots of discussion, there have not been useful outcomes.
- There is more interest in consuming feeds of information than sharing information.
- Ego has been a big issue for improving data sharing, as have reputation-related concerns when sharing or receiving data.
- There is a perception of weakness around organizations that share attack information in some regions.
- Sharing in isolation doesn't help, it must lead to operational return on investment.
- Language barriers have been an issue for some national CSIRTs.
- Sharing too much information leads to capacity and resource issues for receiving organizations. Organizations directly receiving feeds can often misinterpret data and think they are under attack when it is not the case. Operational models are preferred where data exchanges have a direct impact on improving the efficiency of a small number of analysts to impact many.
- Privacy regulations restricting some organizations from sharing IP address information have had an impact on the effectiveness of incident data exchanges. ENISA is currently running a study on this impact (this point was raised by several attendees).
- Too many efforts are using data just for blocking attacks and not for operational mitigation and elimination of vulnerabilities as part of their incident response effort. Note: Operational efforts stand out in that they do eliminate threats and update data warehouses.
- Involvement of vendors is needed to better scale attack response. This is not seen as a need by all groups, but some sharing groups with an operational focus are looking for improved efficiencies to leverage a small number of analysts more productively. Analysts are a limited resource in this technical area of expertise.
- Enterprises don't want more security boxes in their networks as they don't have the resources to manage them, so involving vendors doesn't mean deploying more equipment, but improving automated controls and the elimination of threats wherever possible. False positives are still an issue, which can be problematic for some automation activities.

2.2. Scaling Response to DDoS and Botnets Effectively and Safely

The first invited talk at the workshop provided an interesting history of Distributed Denial-of-Service (DDoS) attacks and the evolution of botnets as well as the methods to combat these threats. The paper by Dave Dittrich [DD1] is available to learn more of this history. This section of the report will focus on the workshop discussion in an effort to benefit from the workshop attendees' thoughts concerning how to better scale our response to these threats.

Key points from the discussion:

- Of the attack types discussed, DDoS and botnets appear to be the furthest along in terms of efficient and effective response. Other efforts can learn from this experience. There has not been any interaction between these two attack types that may benefit from information exchange tied to remediation activities since botnets can be the source of DDoS attacks.

- There is a disparity between short-term mitigation goals and actual eradication of DDoS and botnet threats. The question was raised: how do we normalize the same data in different ways to serve different goals? In other words, DDoS traffic is often the result of botnets, but the data is not shared between the service providers and vendors responding to DDoS threats and those actively mitigating and eradicating botnets.

- There are ad hoc trust groups within the operations security (OPSEC) community today. The Cybercrime Response Advisory Group (CRAG) is one example.

- Filtering and triage is an issue, but this is a solvable problem.

- The IETF DDOS Open Threat Signaling (DOTS) working group was discussed and compared to a previous effort, Real-time Inter-network defense (RID) [RFC6545]. It was stated that the two are similar, except DOTS makes use of current data formats and protocols and has the support of multiple DDoS vendors. One of the goals of DOTS is to have this solution be the "glue" between vendors to communicate shared data using standard formats and protocols developed in open-source tools.

- The IETF Interface to Network Security Functions (I2NSF) effort was discussed to explore ways of leveraging infrastructure to combat DDoS attacks.

- Vendors discussed existing capabilities for DDoS mitigation, while data-sharing groups discussed their mitigation activities related to botnets (see the submissions under the heading "Panel on Scaling Attack Response for DDoS and BotNets" in the workshop agenda [AGENDA]).

- Trust and reputation of data sources is still a concern.

- One of the exchange groups has a goal of "automated takedowns" for botnets. However, they think they will always have a need for manual intervention.

- The need for multiple levels of trust seemed to be prevalent among those participating in the panel discussion. Intelligence agencies erode trust (this was also mentioned in the first panel in terms of surveillance activities from governments).

- Although trust was discussed in this panel and there are concerns, it was noted that trust is not as big a barrier for DDoS and botnet mitigation, and this is likely due to the operational experience of the participants.

2.3. DNS and RIRs: Attack Response and Mitigation

This session was a shift from other sessions in the day as the panelists were infrastructure providers for those combating attacks. This session was of interest to see how attack and incident responders could better collaborate with DNS infrastructure organizations and RIRs. These groups have not interacted in the past, and it was interesting to see the collaboration opportunities since the workshop participants rely on these services to do their jobs. From the panelists' perspective, DNS and RIRs are separate worlds where they spend a lot of time trying to educate policy makers about how they work together to make the Internet work.

Key discussion points:

- The use of passive DNS in attack mitigation was described.

- RIRs discussed the data they maintain and provide, including worldwide BGP update data and root DNS server data. These datasets are available to share with researchers and could be of interest to those working on attack response. The current way the data is made available does not scale, and ideas were discussed in the workshop to improve the scalability should this become a more widely used resource.

- Some of the global RIRs already actively coordinate with incident responders in their region. In some cases, they do facilitate information sharing as well as provide education and training. Data shared out by RIRs is anonymized.

- A concern was raised regarding overlapping efforts and a request was made for the IETF and ISOC to pay attention to this and help. This workshop was one step toward that in bringing together this diverse community. The participants wished to see this type of event repeated for future cross area collaboration between the diverse set of groups that often only meet within their silo.

- Standards for APIs to access data consistently from RIRs and scoring methods were discussed as possible ways to scale trust. Questions were raised as to how this might be possible. One might receive unverifiable data about a network. They may be able to verify the source's identity, verify route origins, but won't be able to verify the provenance of data.

2.4. Trust Privacy and Data Markings Panel

Why don't organizations share data? The answer seems to be a mix of privacy, legal, technical/mundane, cultural, and communication issues. There are also concerns about sharing proprietary data with competitors. Having said that, most of these reasons were dismissed as bogus by the more operationally focused participants in the workshop. Lawyers need contextual education for the intersection of law and technology. Sensitive data is still an issue as one can't control what others do with data once it is shared.

Key points from the panel discussion:

- Operationally focused groups do retain/rate/re-mark confidence levels based upon the submitter's reputation.

- The Traffic Light Protocol (TLP) [TLP] was discussed. While TLP is useful to some groups who exchange data, others find that it is not granular enough for their needs.

- In many cases, when data is shared, the user never knows, and there is no way to manage that disclosure.

- Trust is personal. When sharing circles get too large, trust breaks down. The personal relationship aspect of information sharing communities was emphasized by several who are actively exchanging data. This was a very prevalent theme.

- A point of comparison was made with consumer goods, and it was observed that trademarks are a byproduct of the Industrial Revolution. The question was raised: does trust need branding?

- Observing participants noted that there appear to be cabals operating the groups based on the current trust notions. This was not disputed.

- Transparency is vital to maintain trust.

- Participants working on automation have found a need to share with organizations of all sizes as well as a need to share both synchronously and asynchronously. In an automated model, they must ensure data sources are "authorized" and these efforts have encountered questions about anonymization as well as regional regulatory perspectives as they vary.

- Another automation effort found that people have different upper limits for trust group scale, which is sometimes based on individualized knowledge of other participants and having a comfort level with them. Social interaction (beer) is a common thread amongst sharing partners to build trust relationships. The relationships are formed between individuals and not necessarily between organizations.

- It's rare for any single piece of information to be clearly identifiable as private or public. The temptation is to say that information isn't Personally Identifiable Information (PII). In aggregate, however, non-PII can become PII.

- There was common agreement that reputation is fundamental.

3. Workshop Themes

During the course of the day, a couple of themes recurred in the discussions. Firstly, in order to better scale attack response through improvements to the efficiency and effectiveness of information exchanges:

1. Exchanging data should not be just for the purpose of creating blacklists that could be redundant efforts.

2. Involving service providers and vendors to better coordinate and scale response is key.

Secondly, information security practitioners are a scarce resource:

1. Training and education was discussed to improve this gap, both to train information security professionals and others in IT on basic network and system hygiene.

2. Leveraging resources to better scale response, using fewer resources is critical.

4. Next Steps

4.1. RIR and DNS Provider Resources

Workshop participants expressed an interest in expanded information about the resources and assistance offered by the RIRs and DNS providers. Participants are going to define what is needed.

4.2. Education and Guidance

Another recurring theme was the lack of knowledge in the community about basic security principles such as ingress and egress filtering explained in BCP 38 [RFC2827]. The CSIRTs, operators, and vendors of attack mitigation tools found this particularly frustrating. As a result, follow up activities may include determining if security guidance BCPs require updates or to determine whether there are opportunities to educate people on these basic principles already documented by the IETF.

4.3. Transport Options

One of the more lively discussions was the need for better transports for information exchange. Real-time Inter-network Defense (RID) [RFC6545] was published 5 years ago. While the patterns established in RID still show promise, there are updated solutions being worked on. One such solution is in the IETF DOTS working group that has an approach similar to RID with updated formats and protocols to meet the demands of today's DDoS attacks. While Trusted Automated eXchange of Indicator Information (TAXII -- another transport option) is just in transition to Organization for the Advancement of Structured Information Standards (OASIS), its base is similar to RID in its use of SOAP-like messaging, which will likely prevent it from scaling to the demands of the Internet. Vendors also cited several interoperability challenges of TAXII in workshop discussions. Alternatively, XMPP-Grid has been proposed in the IETF Security Automation and Continuous Monitoring (SACM) working group and it offers promise as the data exchange protocol for deployment at scale. Extensible Messaging and Presence Protocol (XMPP) [RFC6120] inherently meets the requirements for today's information exchanges

with features such as publish/subscribe, federation, and use of a control channel. XMPP-Grid is gaining traction with at least 10 vendors using it in their products and several more planning to add support [APPALA]. Review and discussion of this document would be helpful as it transitions to the Managed Incident Lightweight Exchange (MILE) working group as an outcome of the workshop. Representational State Transfer (REST) was also brought up as a needed interface because of the low barrier to use [REST]. The IETF MILE Working Group has discussed a document detailing a common RESTful interface (ROLIE) that could be used with any data format and this may also be of interest [ROLIE].

4.4. Updated Template for Information Exchange Groups

One of the submission options was for organizations actively exchanging data to submit a form describing their work to reduce computer security incidents. The CSIRTs, in particular, liked having access to this information in a neutral location like the Internet Society. However, they wanted to see amendments to the format to improve its usefulness. There was a desire to have this used by additional information exchange groups, thereby creating a living library to improve awareness about how to become a member, benefit from, or contribute to the success of the attack response and CSIRT information exchange platforms.

5. Security Considerations

The CARIS workshop was focused on security and methods to improve the effectiveness and efficiency of attack response to enable better scaling. This report provides a summary of the workshop discussions and identifies some outcomes to improve security. As such, no additional considerations are provided in this section.

6. Informative References

[AGENDA] "Agenda: Coordinating Attack Response at Internet Scale (CARIS) Workshop", 2015, <https://www.iab.org/activities/workshops/caris/agenda/>.

[APPALA] Cam-Winget, N., Ed., Appala, S., and S. Pope, "XMPP Protocol Extensions for Use with IODEF", Work in Progress, draft-ietf-mile-xmpp-grid-01, October 2016.

[APWG] "APWG Homepage", <http://www.antiphishing.org>.

[CERT.BR] "Brazilian National Computer Emergency Response Team Homepage", <http://www.cert.br/en/>.

[CERTCC] "CERT Coordination Center Homepage", <https://www.cert.org>.

[DD1] Dittrich, D., "Taking Down Botnets - Background", April 2015, <https://www.iab.org/wp-content/IAB-uploads/2015/04/CARIS_2015_submission_21.pdf>.

[ENISA] "European Union Agency for Network and Information Security Homepage", <https://www.enisa.europa.eu>.

[ISOC] "CARIS Workshop Template Submissions 2015", <https://www.internetsociety.org/doc/caris-workshop-template-submissions-2015>.

[KME] Moriarty, K., "Kathleen Moriarty Blog Series", July 2015, <http://blogs.rsa.com/author/kathleen-moriarty/>.

[MYCERT] "Malaysia Computer Emergency Response Team Homepage", <https://www.mycert.org.my/en/>.

[REN-ISAC] "Research and Education Networking Information Sharing and Analysis Center Homepage", <http://ren-isac.net>.

[REST] Fielding, R., "Architectural Styles and the Design of Network-based Software Architectures", Ph.D. Dissertation, University of California, Irvine, 2000, <http://www.ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf>.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <http://www.rfc-editor.org/info/rfc2827>.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <http://www.rfc-editor.org/info/rfc6120>.

[RFC6545] Moriarty, K., "Real-time Inter-network Defense (RID)", RFC 6545, DOI 10.17487/RFC6545, April 2012, <http://www.rfc-editor.org/info/rfc6545>.

[ROLIE] Field, J., Banghart, S., and D. Waltermire, "Resource-Oriented Lightweight Information Exchange", Work in Progress, draft-ietf-mile-rolie-06, March 2017.

[TLP] "Traffic Light Protocol (TLP) Matrix and Frequently Asked Questions", <https://www.us-cert.gov/tlp>.

Appendix A. Workshop Attendees

In alphabetical order by first name, workshop attendees were: Adli Wahid, Alexey Melnikov, Andrew Sullivan, Arnold Sykosch, Brian Trammell, Chris Morrow, Cristine Hoepers, Dario Forte, Dave Cridland, Dave Dittrich, Eliot Lear, Foy Shiver, Frank Xialiang, Graciella Martinez, Jessica Stienberger, Jim Duncan, Joe Hildebrand, John Bond, John Graham-Cummings, John Kristoff, Kathleen Moriarty, Klaus Steding-Jessen, Linda Dunbar, Marco Obiso, Martin Stiemerling, Mat Ford, Merike Kaeo, Michael Daly, Mio Suzuki, Mirjam Kuehne, Fu TianFu, Nancy Cam-Winget, Nik Teague, Pat Cain, Roland Dobbins, Roman Danyliw, Rosella Mattioli, Sandeep Bhatt, Scott Pinkerton, Sharifah Roziah Mohd Kassim, Stuart Murdoch, Takeshi Takahashi, Ted Hardie, Tobias Gondrom, Tom Millar, Tomas Sander, Ulrich Seldeslachts, Valerie Duncan, and Wes Young.

IAB Members at the Time of Approval

The IAB members at the time this memo was approved were (in alphabetical order):

Jari Arkko
Ralph Droms
Ted Hardie
Joe Hildebrand
Russ Housley
Lee Howard
Erik Nordmark
Robert Sparks
Andrew Sullivan
Dave Thaler
Martin Thomson
Brian Trammell
Suzanne Woolf

Acknowledgements

Thanks are due to the members of the program committee (in alphabetical order) for their efforts to make the CARIS workshop possible and a productive session with cross area expertise: Matthew Ford (Internet Society, UK), Ted Hardie (Google, USA), Joe Hildebrand (Cisco, USA), Eliot Lear (Cisco, Switzerland), Kathleen M. Moriarty (EMC Corporation, USA), Andrew Sullivan (Dyn, USA), and Brian Trammell (ETH Zurich, Switzerland).

Thanks are also due to the CARIS workshop sponsors:

- FIRST provided a room and excellent facilities in partnership with their annual conference in Berlin.
- The Internet Society hosted the social event, a boat ride through the canals of Berlin.
- EMC Corporation provided lunch, snacks, and coffee throughout the day to keep the attendees going.

Authors' Addresses

Kathleen M. Moriarty
176 South Street
Hopkinton, MA
United States of America

Email: Kathleen.Moriarty@dell.com

Mat Ford
Galerie Jean-Malbuisson 15
Geneva
Switzerland

Email: ford@isoc.org