

Research Access to Shared Darknet Data

Agreement to Conditions of Use

Background

The Shared Darknet¹ (SD) is a project under the auspices of REN-ISAC² (RI). The SD objective is to develop a persistent and evolving darknet resource using combined data contributions of participating sites and joint efforts in analysis and analytics development. SD enables the discovery of operationally actionable information regarding sources of threat, the understanding of attacks, malware, threat evolution, and miscreant behavior, and is a source of real-world data for innovative research.

The purpose of the Research Access to Shared Darknet Data program (Program) is to provide a framework for making SD data available for research purposes, under Conditions of Use.

Rationale for the Conditions of Use

Dark IP address space is indispensable for the reasons outlined in *Background*. Dark space is useful only as long as miscreants are unaware of the dark address specifics. Darknets trap threat. Miscreants alter their systems and behaviors to avoid known traps. The specifics of darknet addressing should never be disclosed outside the immediate operators of the darknet.

In addition to avoiding the outright disclosure of specifics, security researchers and practitioners must exercise caution and restraint regarding publishing results from analysis of darknet data. Dark space can be easily mapped by patterned probing, forcing signatures in otherwise innocuous analysis results.

Definitions

“SD participant” is the operator of a darknet sensor that is feeding data to the SD. Individual SD participants must opt-in to share their data in the Program. SD participants have control of the disposition of their data within the Program.

“Data” is the raw event data collected in SD participant darknets and stored in the SD repository.

“Provided Data” is data that is provided to Researchers under this Agreement.

“Researcher” is a faculty member at an accredited institution, or a threat researcher at an RI-affiliated organization, who is a consumer of Provided Data, and is party to the Agreement.

“Results” refers to information product derived by Researchers from analysis of Provided Data.

“RI-SDB” is the REN-ISAC Shared Darknet Board. It consists of the REN-ISAC Technical Director, Principal Security Engineer, and a limited number of SD participants. Researchers are not included in the RI-SDB

¹ http://www.ren-isac.net/shared_darknet

² <http://www.ren-isac.net>

because the group will be privy to proposed activities and pre-publication results of other Researchers. The RI-SDB may at times seek guidance from the REN-ISAC Technical Advisory³ and Executive Advisory⁴ Groups, and will seek input and feedback from Researchers.

Notices

Notices to REN-ISAC and RI-SDB regarding this Agreement should be sent in e-mail to soc@ren-isac.net. Emergency communications can be made 24x7 to the REN-ISAC Watch Desk⁵. Notices to the Researcher will be sent by e-mail to the Researcher and signatory department head or dean.

Instructions

Proposed research activity(s) must be vetted by the RI-SDB as specified in *Conditions*. The Researcher may, but is not required to, discuss proposed activities with RI-SDB before formally submitting a proposal.

The Researcher, Researcher's department head or dean, and the REN-ISAC Technical Director must each sign the Agreement.

Each proposed research activity must be individually described in Appendices. The Researcher and Technical Director must each sign Appendices. Accordingly, signature is not required of the Researcher's department head or dean during the lifetime of the Agreement when new research activities are added, or the substance of an already proposed activity changes (e.g. additional subordinate researchers.)

Agreement

This Agreement is not intended to introduce a legal liability on the Researcher, the Researcher's employer, the SD participants, the REN-ISAC organization, its host, sponsoring organizations, or officers.

Data shared under the Program relates to IT security measures and is proprietary and confidential.

Data shared under the Program is shared in good faith. There are no explicit or implied guarantees or warranties to the quality of the data. SD participants and REN-ISAC accept no responsibility for negative impacts that result from the use of Provided Data.

This Agreement is executed among the parties and on the date identified in *Signatures*. The term of this Agreement is one year. Data access will be terminated immediately upon expiration. Renewal notices will be sent one month in advance of expiration.

REN-ISAC, the Researcher, or the Researcher's employer can terminate this Agreement with sole discretion, without prior notice. Any violation of the *Conditions* will result in immediate termination for cause. Notification and reason for termination shall be communicated among the parties identified in *Notices*. If termination is due to cause, the Researcher must securely delete all Provided Data. If the

³ <http://www.ren-isac.net/advisory.html#technical>

⁴ <http://www.ren-isac.net/advisory.html#executive>

⁵ <http://www.ren-isac.net/watch.html>

termination is for convenience, the Researcher must securely delete all Provided Data that is not required for underpinning of completed research. Any Provided Data that is so retained must be stored encrypted.

Recognized Researchers from accredited institutions may have access to Provided Data under the following *Conditions*.

Conditions

1. The Conditions survive expiration or termination of the Agreement. The Researcher commits to remain bound by the Conditions following termination or expiration of the Agreement.
2. Provided Data, in whole or in part, must not be redistributed, published, or made public under any circumstances.
3. Provided Data is for non-commercial use only.
4. An academic Researcher's institution must meet the guideline for REN-ISAC institutional membership. Although the Researcher's home institution is not required to be a REN-ISAC member, the institution is strongly encouraged to become a member.
5. Candidate Researchers will be vetted by the RI-SDB. Research requests may be turned down at the sole discretion of the RI-SDB.
6. Subordinate researchers, e.g. graduate students, may be given access to Provided Data, but only under the conditions that they (a) are named in a Research Activity Appendix to the Agreement, (b) work under the direct supervision of the Researcher, and (c) have been thoroughly apprised of the Agreement *Conditions* by the Researcher.
7. Access is provided only for specific activities identified in appendices to this Agreement. Each research activity making use of Provided Data must be uniquely identified and agreed to by RI-SDB. Blanket access is not granted. General classroom use is not granted. When a new research activity arises during the lifetime of the Agreement, the new activity must be described in appendix to the Agreement, vetted by the RI-SDB, and signed by the Researcher and REN-ISAC Technical Director.
8. Responsibility for safeguarding Provided Data is the responsibility of the Researcher.
9. All reasonable care must be taken to safeguard Provided Data. Individuals who are not party to or identified in the Agreement must not have access. Care must be taken to safeguard against accidental or malicious access by unauthorized parties. Researchers must inform RI-SDB personnel as soon as they become aware of any unauthorized access or disclosure of the data.
10. Provided Data should be stored encrypted. Provided Data that is not required for further analysis or for the underpinning of Results must be securely deleted. Upon completion of the research activity or termination of the Agreement, Provided Data that is retained to support Results must be encrypted.

11. Provided Data will never contain destination addresses (i.e. the addresses in the dark space.) The contributing dark IP addresses will be mapped to non-routable addresses in the 10.0.0.0/8 space. The mapping will not be persistent over long periods of time. Mappings will retain locality, i.e. two addresses in the same /24 in "real" IP space will be in the same /24 in the anonymized space. Researchers planning studies that require persistent mapping should contact RI-SDB personnel.
12. Researchers must not make any attempt to map the transformed dark IP addresses back to real addresses, must not attempt to locate the dark IP addresses in any other way, and must not publish any Results likely to allow third parties to map the dark IP addresses.
13. Researchers must submit a description of the Results they hope to achieve and publish. A description must be submitted for each unique research activity, and attached as an appendix to the Agreement. The purpose is to check for the potential for leakage of information counter to the interests of RI members and/or SD participants. RI-SDB will treat the information in strict confidence.
14. Researchers must permit the RI-SDB to review pre-publication Results derived from Provided Data. The purpose of the review is to check for leakage of information counter to the interests of RI members and/or SD participants. RI-SDB will treat the Results with strict confidence. RI-SDB may decline the opportunity to conduct this review at their sole discretion, in which case the researcher is free to publish. If RI-SDB does not raise an objection or request additional time with 10 calendar days of receiving a researcher's manuscript, the researcher shall also be free to publish.
15. Researchers will not take any action against traffic sources identified by the SD as (potential) threat sources. No probes, take-down attempts, etc., except with the cooperation of REN-ISAC.
16. Published Results should acknowledge the "Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)", and must include the statement: "The content is the responsibility of the authors and does not necessarily represent official views of the REN-ISAC."
17. The terms of the Agreement, along with a list of current and historical participating Researchers, will be maintained and available to SD participants.
18. In the event a Researcher is required, by open records, freedom of information, subpoena, or any other law or regulation, to disclose Provided Data, or Results that may put the specifics of darknet addressing at risk, the Researcher shall promptly notify REN-ISAC before responding to the request, consult regarding whether there are legitimate grounds to narrow or contest disclosure, and disclose only information that the Researcher, determines with sole discretion, is legally obligated to disclose.

Signatures

REN-ISAC

Name:

Title:

Phone:

E-mail:

Signature:

Date:

Notices: soc@ren-isac.net

Researcher

Institution:

Name:

Title:

Phone:

E-mail:

Signature:

Date:

Researcher's Department Head or Dean

Institution:

Name:

Title:

Phone:

E-mail:

Signature:

Date:

Appendix A. #___: Research Activity

Each research activity must be individually described according to the following template, and attached to the Agreement as Appendix A.x. Each must be individually signed by REN-ISAC and Researcher.

This Appendix is supplement to the master Agreement signed on:

Name of Researcher:

Name of Research Activity:

Description of the Intended Results: The description must provide sufficient information to permit the RI-SDB to check for potential leakage of information counter to the interests of RI and SD participants.

Subordinate Researchers: Must provide the name and e-mail address of all subordinates (e.g. grad students) involved in the research activity. Subordinate Researchers must initial their name, indicating that they have read and agree to abide the conditions.

Signatures

REN-ISAC

Name

Signature

Date

Researcher

Name

Signature

Date