– Paul Vixie, co-founder

Overview:

The Security Information Exchange of Europe (SIE-Europe.NET) is a managed network facilitating the sharing of real time network telemetry by cooperating Data Participants with trusted data analysts. These trusted analysts include academic entities and other Data Participants. The purpose of SIE-Europe is to make the Internet safer by improving European visibility. Supported data types within SIE-Europe will eventually include network telescope output, spam trap output, honeypot output. This document concerns primarily Passive DNS.

Details:

A Data Participant who operates one or more recursive domain name system (RDNS) servers will install SIE-Europe's open-source software-based Passive DNS sensors on or nearby each such server. This can be done by adding a passive network tap to the name server, or by adding a "span port" on the name server's upstream Ethernet switch, or by installing the Passive DNS sensor software directly on the name server itself, or by using the open source *dnstap* protocol to reach a nearby telemetry collection server.

The output of the software sensor is a stream of DNS transactions including the query, the response, and various measurements such as the total transaction time. By design and intent, no end-user personally identifiable information (PII) will be present in this output stream. The sensor only monitors upstream traffic resulting from RDNS cache miss events, and has no access to downstream traffic which would show the end-user's IP address and identifying frequency of re-use patterns.

Sensor output can either be transmitted directly to SIE-Europe using the *trampoline* protocol, or can be first collected at the Data Participant's Security Operations Center (SOC) where it can be stored and analyzed in addition to being transmitted to SIE-Europe for wider data sharing purposes. SIE-Europe advises all Data Participants to collect, store, and analyze this traffic to improve their knowledge of its own network. SIE-Europe requests that this data, once collected, also be forwarded to SIE-Europe to facilitate external analysis by other Data Participants.

Status:

More than a hundred (100) enterprise, service provider, academic, and research entities around the world have installed this Passive DNS software sensor and are sharing their real time DNS transaction streams. Every Data Participant receives access to either the real-time or at-rest data shared by others, with the result that all participating networks are better observed, and better able to observe, both nominal and anomalous traffic within the European digital economy.

Next Steps:

SIE-Europe and a new Data Participant must first execute a Data Participant Agreement which sets out the rights and responsibilities of each party. There is no fee for participation.

Technical activities can then begin, including consultation as to topology and method, delivery and installation of sensor software, exchange of authentication keys, initial startup, and setting conditions and methods for ongoing monitoring and break-fix.

Topology: