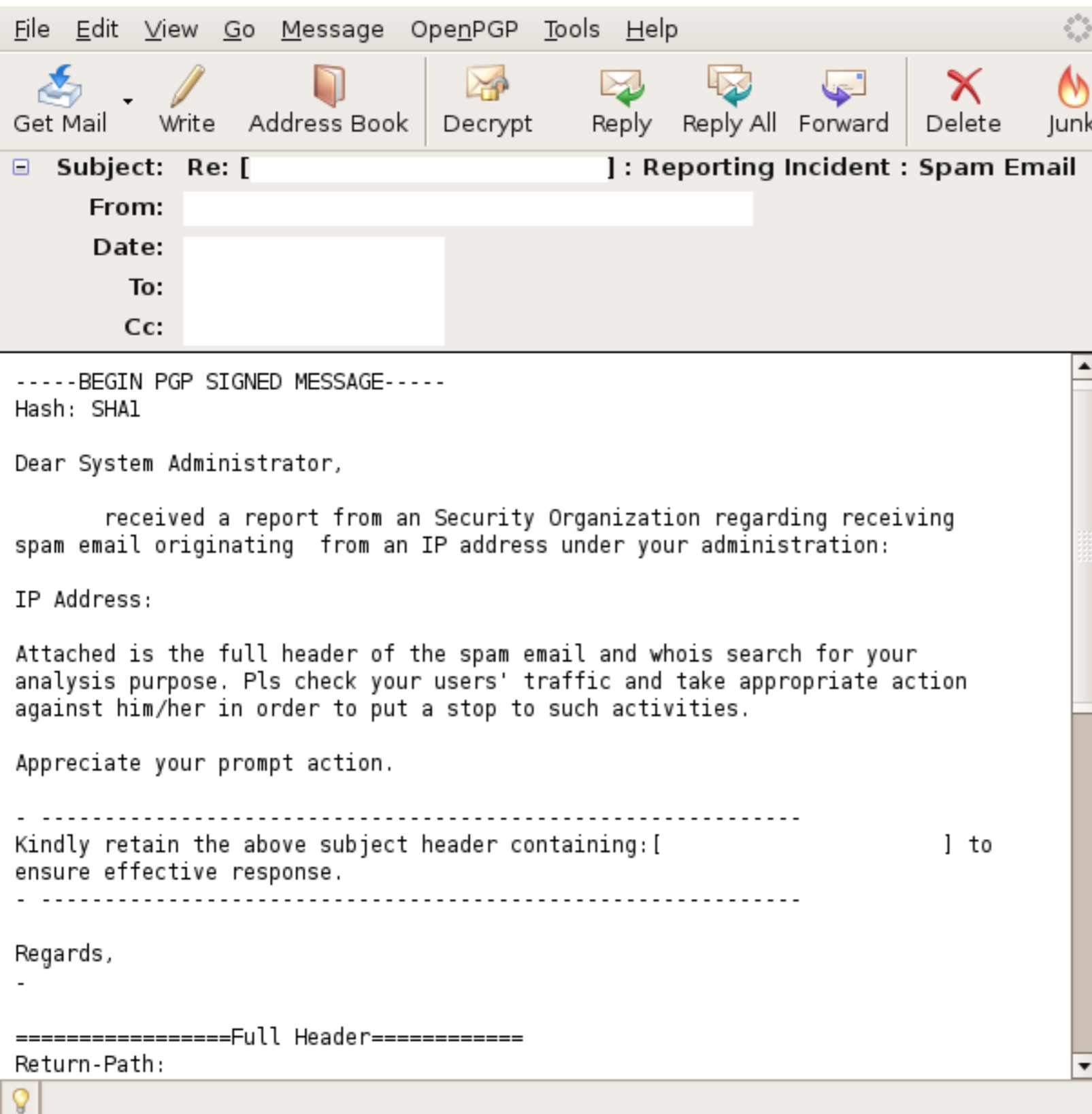


A Framework to understand and handle Internet Abuse Incidents

This is abuse?



The screenshot shows an email client window with a menu bar (File, Edit, View, Go, Message, OpenPGP, Tools, Help) and a toolbar with icons for Get Mail, Write, Address Book, Decrypt, Reply, Reply All, Forward, Delete, and Junk. The email subject is "Re: [redacted] : Reporting Incident : Spam Email". The message body is a PGP signed message with the following content:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Dear System Administrator,

I received a report from an Security Organization regarding receiving
spam email originating from an IP address under your administration:

IP Address:

Attached is the full header of the spam email and whois search for your
analysis purpose. Pls check your users' traffic and take appropriate action
against him/her in order to put a stop to such activities.

Appreciate your prompt action.

-----
Kindly retain the above subject header containing:[redacted] to
ensure effective response.
-----

Regards,
-

=====Full Header=====
Return-Path:
```

Abuse Ground Zero: At the wrong end of the stick



Source: <http://upload.wikimedia.org/wikipedia/commons/c/c6/Botnet.svg>



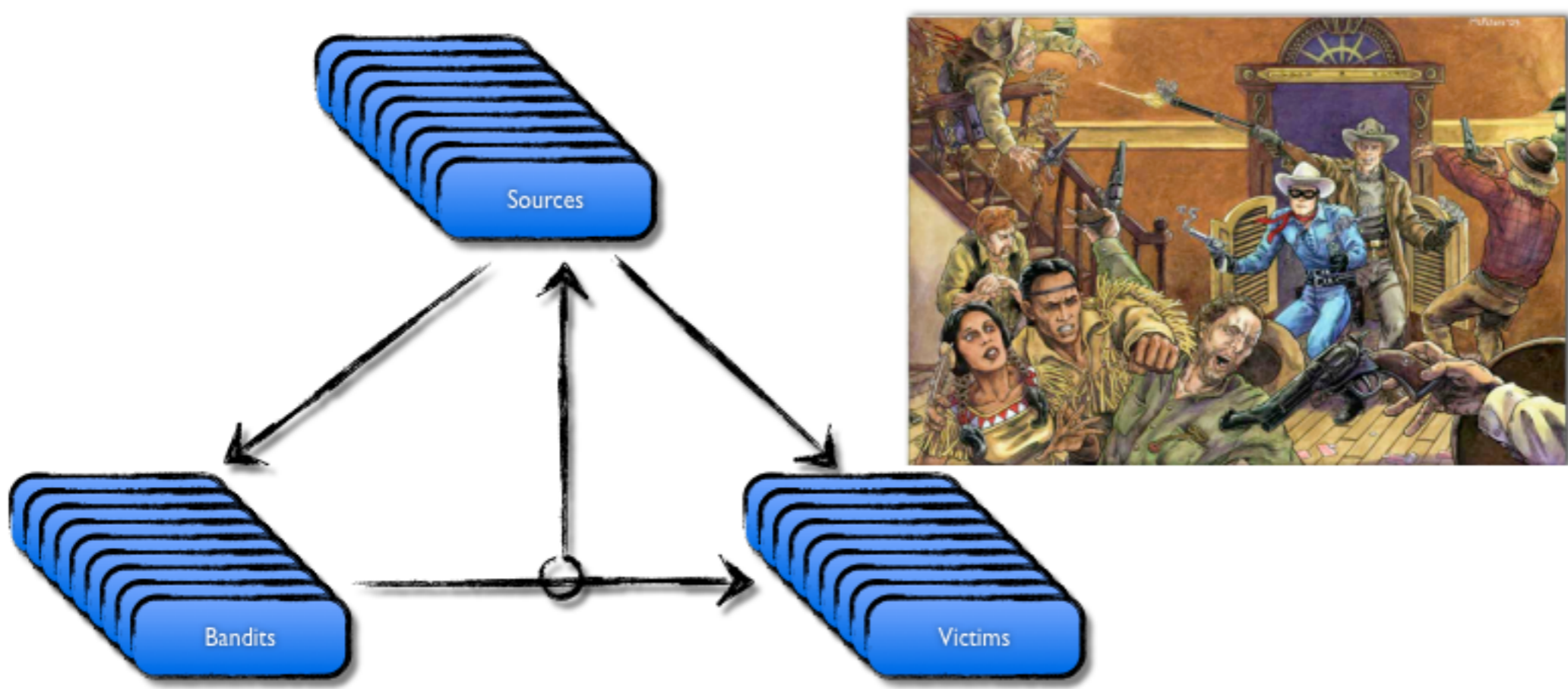
Abuse 1st Floor: Keeping our eyes open and fighting back

Feeds - abusehelper Collab

22nd An... AusCER... ToBeNa... Feeds - ... Lessons ... The Lon... >> +

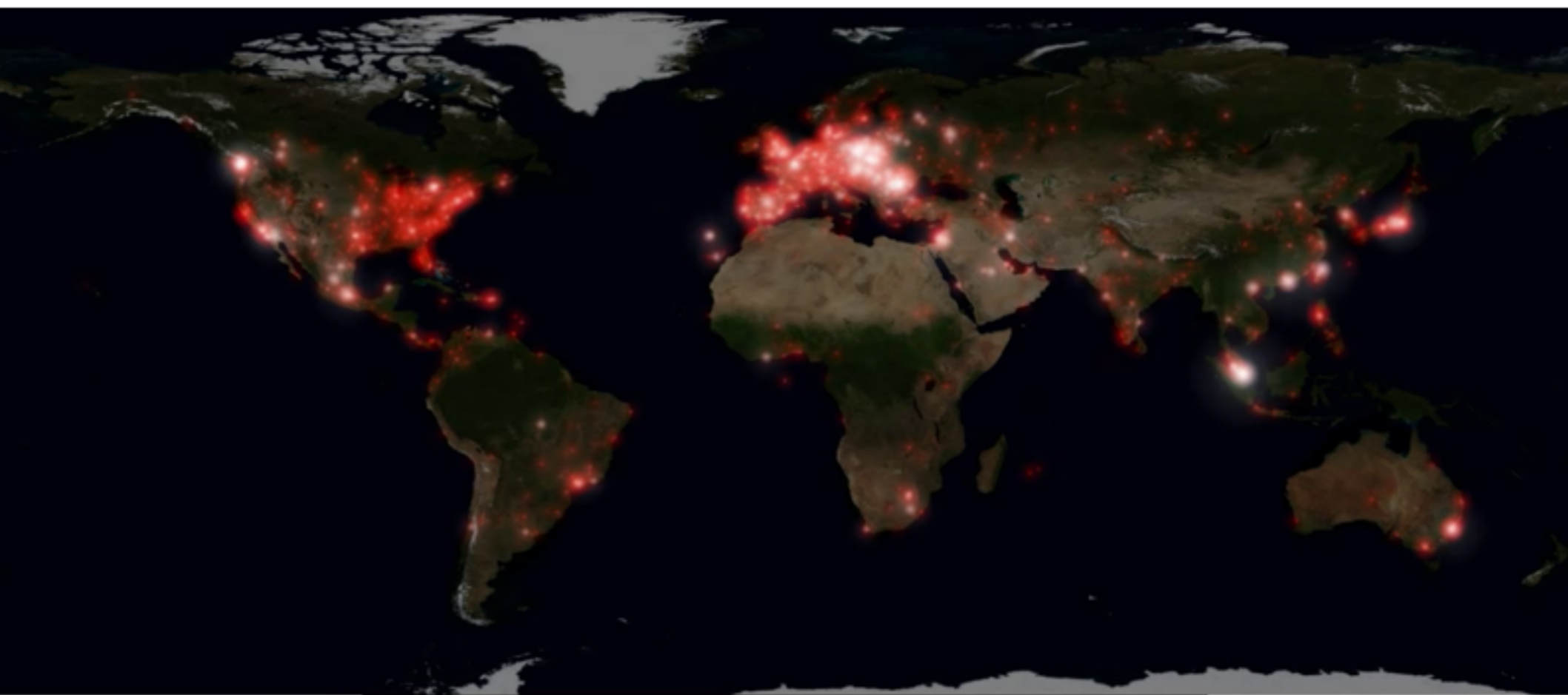
Web site vuln, attack or incident feeds

- Good list: <http://www.okamalo.com/2009/11/malicious-ips-and-url-free-databases.html>
- Defacements: <http://zone-h.org/archive/special=1>
- XSS incidents: <http://www.xssed.com/archive/special=1>
- Some wepawet JS deobfuscation analyses contain CVE:s <http://wepawet.cs.ucsb.edu/static/torpig-twitter.html>
- Various attack data: http://barometer.interoute.com/barom_stat_alerts.php
- IP blacklists: <http://whatismyipaddress.com/staticpages/index.php/is-my-ip-address-blacklisted>
- sources of malicious IPs.
 - abusechff <http://dnsbl.abuse.ch/fastfluxtracker.php>
 - abusechweb <http://dnsbl.abuse.ch/webabusetracker.php>
 - arbor http://atlas-public.ec2.arbor.net/public/ssh_attackers
 - autoshun <http://www.autoshun.org/files/shunlist.csv>
 - badguys <http://www.t-arend.de/linux/badguys.txt>
 - blacklisted <http://www.infiltrated.net/blacklisted>
 - brawg <http://www.brawg.com/hosts.deny>
 - cleanmxv <http://support.clean-mx.de/clean-mx/xmlviruses?response=alive&format=csv&fields=url,ip,domain&domain=>
 - cleanmxx <http://support.clean-mx.de/clean-mx/xmlphishing?response=alive&format=csv&fields=url,ip,domain&domain=>



• *Ideally: Security data is collected and either shared or made readily accessible in a trusted community in real time. Today: Security data is mostly discarded or at least not shared in a common framework.*

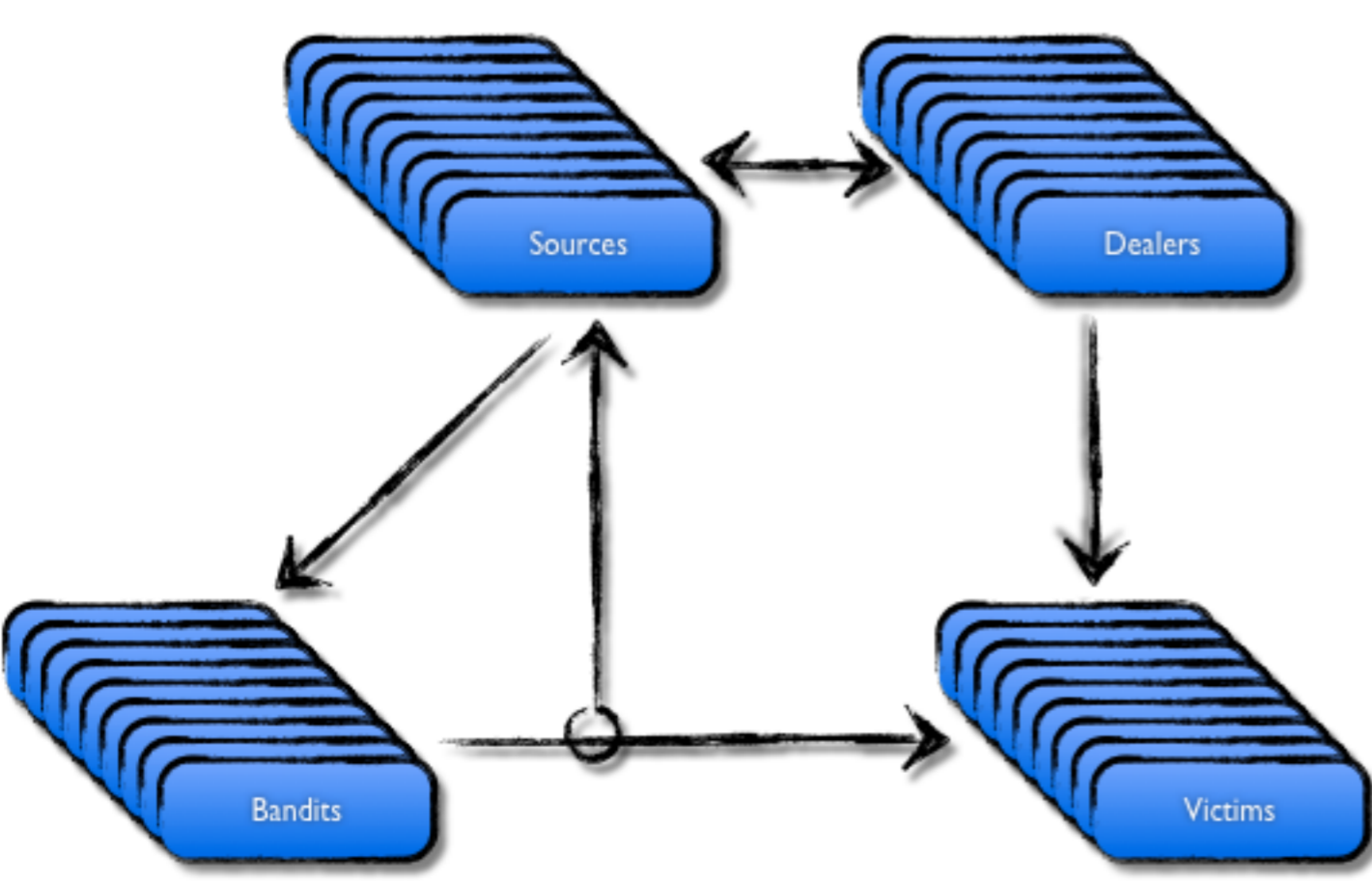
-- Paul Vixie, Andrew Fried, Dr. Chris Lee - Stalking Badness Through Data Mining



F-SECURE® 2008-09-01 16:50:36 Clarified NETWORKS

CERTs in Europe

- Germany:** BFK, CERT-BUND, CERTBw, CERTCOM, CERT-VW, ComCERT, dCERT, DFN-CERT, ESACERT, FSC-CERT, GNS-CERT, PRE-CERT, RUS-CERT, S-CERT, SAP CERT, SECU-CERT, Siemens-CERT, Telekom-CERT, KIT-CERT
- United Kingdom:** BP DSAC, BTCERTCC, Cisco PSIRT, CITIGROUP (UK), CSIRTUK, DAN-CERT, DCSIRT, E-CERT, EUCS-IRT, GovCertUK, JANET-CSIRT, MLCIRT (UK), MODCERT, OxCERT, Q-CIRT, RBSG-ISIRT, RM CSIRT
- Netherlands (The):** AAB GCIRT, AMC-CERT, CERT-IDC, CERT-KUN, CERT-RUG, CERT-UU, GOVCERT.NL, KPN-CERT, ING Global CIRT, SURFCERT, UVA-CERT, RABOBANK SOC
- Belgium:** BELNET CERT, CERT.BE
- France:** CERTA, Cert-IST, CERT-LEXSI, CERT-Renater, CERT-Societe General, ISIRT, APOGEEsec Watch
- Portugal:** CERT.PT, CERT-IPN, CSIRT.FEUP
- Spain:** CCN-CERT, CSIRTCV, e-LC CSIRT, esCERT-UPC, INTECO-CERT, IRIS-CERT
- Luxembourg:** CIRCL, CSIRT-LU, RESTENA-CSIRT
- Switzerland:** CC-SEC, CERN CERT, IP+ CERT, OS-CIRT, SWITCH-CERT
- Italy:** CERT-Difesa, CERT ENEL, CERT-IT, CERT-RAFVG, GARIR-CERT, GovCERT.IT, S2OC, SICEI-CERT
- Sweden:** SITIC, SUNet CERT, TS-CERT, SIST
- Finland:** CERT-FI, Ericsson PSIRT, Funet CERT, Nokia NIRT, FSLabs
- Denmark:** CSIRT.DK, DK-CERT, KMD IAC, SWAT, SECUNIA
- Norway:** NorCERT, UIO-CERT, UniNett CERT
- Iceland:** RHnet CERT
- International:** NCIFRC CC, EGEE OSCT
- Estonia:** CERT-EE, SKY-CERT
- Latvia:** DDIRV, CERT NIC.LV
- Lithuania:** CERT-LT, LITNET CERT, IST-SVDPT
- Russia:** RU-CERT, WebPlus ISP
- Poland:** CERT GOV PL, CERT POLSKA, PIONIER-CERT, TP CERT
- Czech Republic:** CESNET-CERTS, CSIRT.CZ, CZNIC-CSIRT, CSIRT-MU
- Ukraine:** CERT-UA
- Hungary:** CERT-Hungary, HUN-CERT, NIIF-CSIRT
- Slovenia:** SI-CERT
- Romania:** RoCSIRT
- Georgia:** CERT-GE
- Azerbaijan:** CERT AzEduNET
- Croatia:** CARNet CERT, CERT ZSIS, HR-CERT
- Bulgaria:** CERT Bulgaria
- Turkey:** TR-CERT, Ulak-CSIRT
- Cyprus:** CYPRUS
- Austria:** ACOnet-CERT, CERT.AT, GOVCERT, R-IT CERT
- Greece:** AUTH-CERT, FORTH CERT, GRNET-CERT
- Malta:** mtCERT



Everybody's Different, Nobody's Perfect



- Incoming feeds wide and varied in format, formalism and transports -> can't have generic automata
 - Availability (downtime, missing daily reports etc)
 - Integrity of the information (Different sources have different opinions for example on IP<->ASN mapping)
 - Bugs (ask report for ASN1, get report for ASN2)
 - Update frequency: near-real-time, hourly, daily, request/response
 - Timespan: last n days, specific date
 - Provided details: IP, ASN, badness type, firstseen, lastseen, geolocation...
 - Used terminology,
 - Formatting (csv with varying delimiter policies, textual, XML etc)
 - Required pre-knowledge (ASN, IP, fetch URL..)
 - Transports (HTTP, SMTP, IRC)



Abuse Handling Process

- Detecting Abuse
 - Receiving Reports
 - Email, phone, fax, ...
 - Stalking Badness Through Data Mining
 - Scraping Feeds
 - Normalizing Data
 - Correlating Data
- Dealing with Badness
 - Mapping events to address spaces and netblocks
 - Finding right contacts and their contact preferences
 - Customer expectation management
 - Reporting
 - Statistics, trends, chronic cases
 - Responding



State of CERT-FI/CERT-EE abuse handling process

- Previous Processes and Tools
 - 5 generations of CERT-FI Autoreporter (running since 2006)
 - 2 generations of CERT-EE Abuse Killer
- Common challenges
 - Works for me / my sources / my processes / my tools
 - Integration with other "worksforme" processes and tools
 - Customer requirements, processes, involvement, commitment
 - Report reliability, well-formedness, reliability

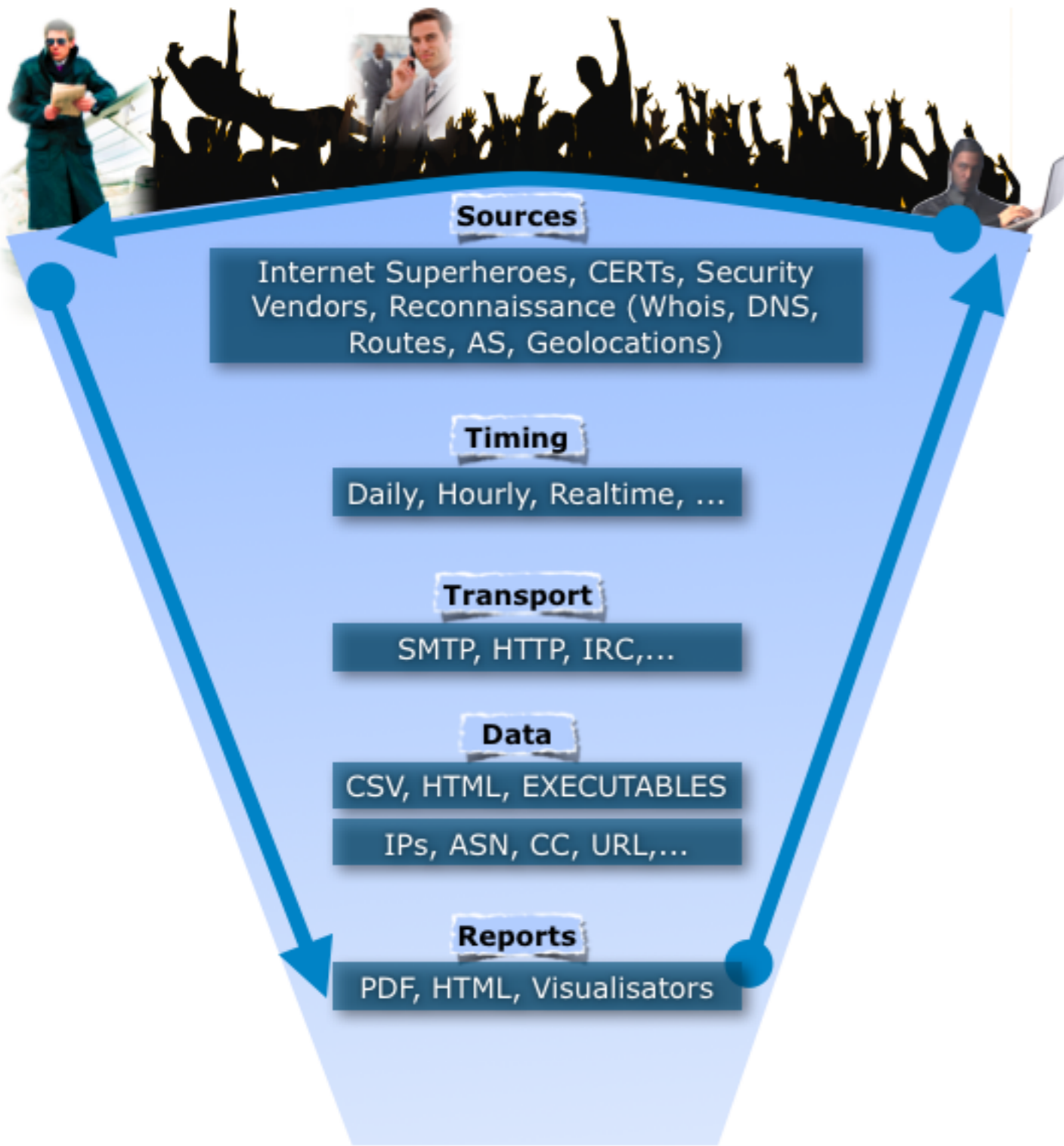
Abuse Helper Goals



- Socio/Economical goal: to bring further focus to somewhat scattered Internet Abuse Handling scene
 - documenting and unifying abuse related terminology
 - documenting assumptions
 - taking into account different needs
 - enabling the creation of processes and workflows
- Technical goal: to take the next step in maturity, from works-for-me information systems to
 - modular,
 - scalable (with regards to performance and usability),
 - commonly developed, and
 - shared one.

- In short, provide common understanding, framework and tools for handling abuse

What is Abuse Helper?



- Abuse Helper is a modular, scalable and (hopefully) robust machine to help you in your abuse handling.
 - Modular:
 - Accept information from several feed sources,
 - via several transports,
 - using several formats, and
 - with several timings (near-real-time, hourly, daily).
 - The same applies to reporting
 - Bots are independent from each other, saving you from complex configurations
 - Scalable:
 - XMPP allows distributing the work to several different machines and geolocations
 - Robust:
 - One bot failing does not mean the whole engine stops working. (See [Screaming Expert approach](#)).
 - The heart, XMPP server is Ejabberd, which is a cross-platform, fault-tolerant, clusterable and modular piece of software.



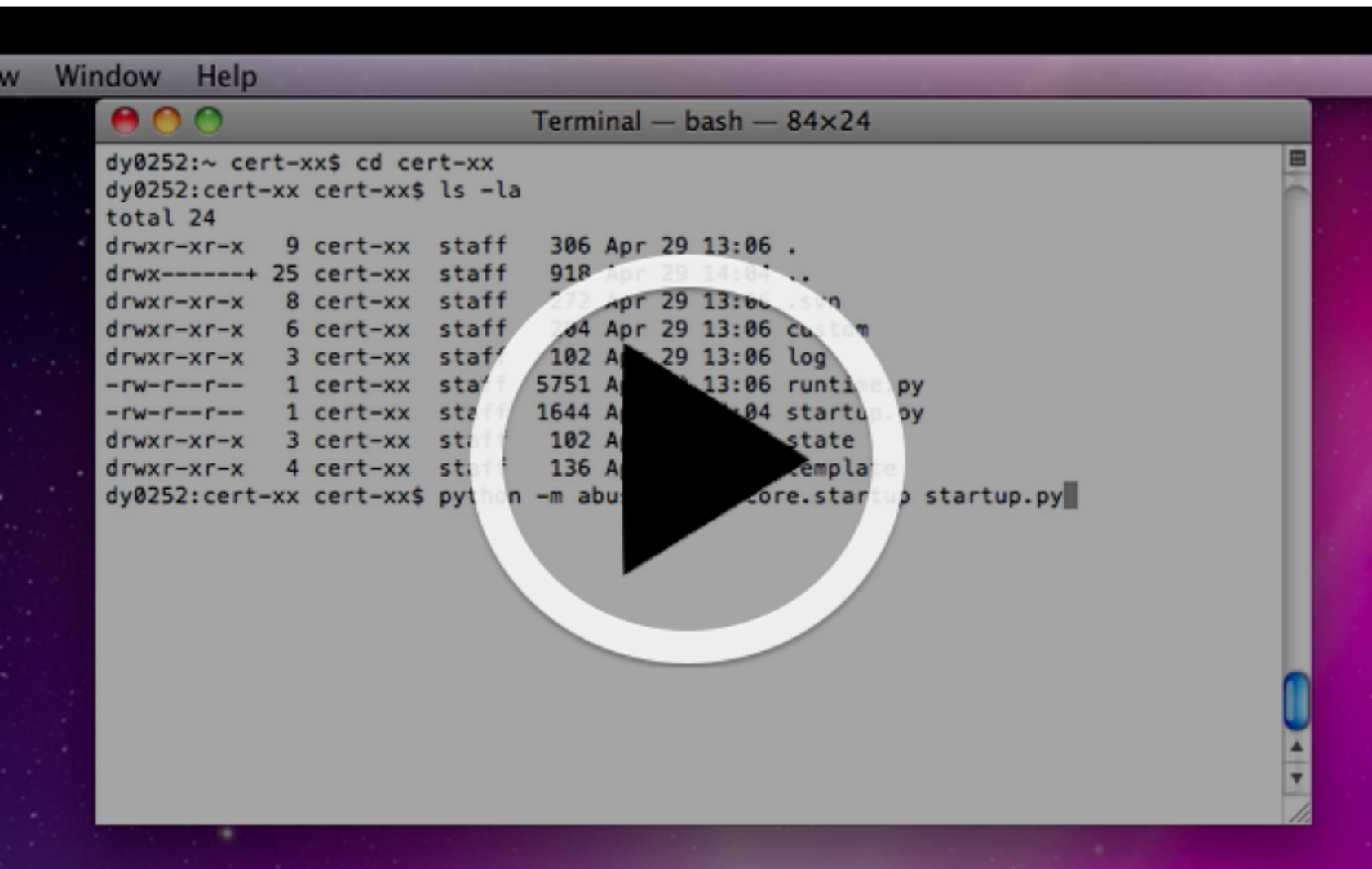
Components

<<	Description <<	See also <<
Bots	One isolated module performing one specific action. The bots should be blissfully unaware of each other. The communication between bots is typically done via MUCs.	
CouchDB	Apache CouchDB is a document-oriented database that can be queried and indexed in a MapReduce fashion using JavaScript. CouchDB is written in Erlang for building concurrent distributed systems. P.S. CouchDB is not a relational database.	http://couchdb.apache.org/
Ejabberd	Ejabberd is an cross-platform, fault-tolerant, clusterable and modular open-source Jabber/XMPP instant messaging server. It is the heart of Abuse Helper	http://www.ejabberd.im/
Idiokit	A simple XMPP library designed for robustness/scalability.	http://code.google.com/p/idiokit

There is a Bot for That

«	Description «	See also «
AtlasSRFBot	AtlasSRFBot takes download URL and a list of AS numbers, downloads badip information from AtlasSRF and throws the information to a XMPP channel(s)	
ConfigBot	Reads configuration from somewhere (for currently we have one implementation, reading customers.ini) and creates Sessions for different Services.	Service , Session
CSV2XMPP	Reads CSV from file or URL and throws the data to XMPP channel.	
CymruWhois	Cymru IP2ASN Whois service expert	
DShieldBot	DShieldBot takes a list of AS numbers, downloads badip information from DShield and throws the information to a XMPP channel.	http://www.dshield.org/indexd.html
Historian	Bot: Historian sits on MUCs, and stores all the events it sees. Bots and humans can then search for all the events in that channel., Term: Historian can be queried about historical events. If he does not know about them, historian turns to Archivist, to get data to analyze and to come up with some answer. Like any other good Historian, our one has some memory about QA and can answer quickly without turning to Archivist 😊	Archivist , Bot
IMAPBot	IMAPBot works as follows: Out-of-the-box: retrieve URLs to CSV files in supported by Python 2.5.4 csv module in default settings. You may customize the bot to: a) Retrieve CSV attachments b) Change CSV format to non-default.	Bot
IRCFeedBot	IRCFeed bot can join to a specific Feed channel on a specific IRC server and relay the messages to the XMPP server.	Bot , Feed
Reporter	Watches specific channel, builds its worldview in a real-time manner and reports as configured.	Bot
Roomgraph	Roomgraph is an implementation of Backoffice Manager role. The term graph comes from the fact that between the rooms, dataflow can be modeled as graph. E.g. Dshield -(split by ASN&CIDR)-> n x Customer rooms.	Backoffice Manager , Customer

DEMO: Basic operation out of the box



A terminal window titled "Terminal — bash — 84x24" showing a directory listing and file operations. A large play button icon is overlaid on the terminal output.

```
dy0252:~ cert-xx$ cd cert-xx
dy0252:cert-xx cert-xx$ ls -la
total 24
drwxr-xr-x  9 cert-xx  staff   306 Apr 29 13:06 .
drwx-----+ 25 cert-xx  staff   918 Apr 29 14:04 ..
drwxr-xr-x  8 cert-xx  staff   272 Apr 29 13:06 bin
drwxr-xr-x  6 cert-xx  staff   204 Apr 29 13:06 custom
drwxr-xr-x  3 cert-xx  staff   102 Apr 29 13:06 log
-rw-r--r--  1 cert-xx  staff  5751 Apr 29 13:06 runtime.py
-rw-r--r--  1 cert-xx  staff  1644 Apr 29 13:04 startup.py
drwxr-xr-x  3 cert-xx  staff   102 Apr 29 13:06 state
drwxr-xr-x  4 cert-xx  staff   136 Apr 29 13:06 template
dy0252:cert-xx cert-xx$ python -m abusecore.startup startup.py
```



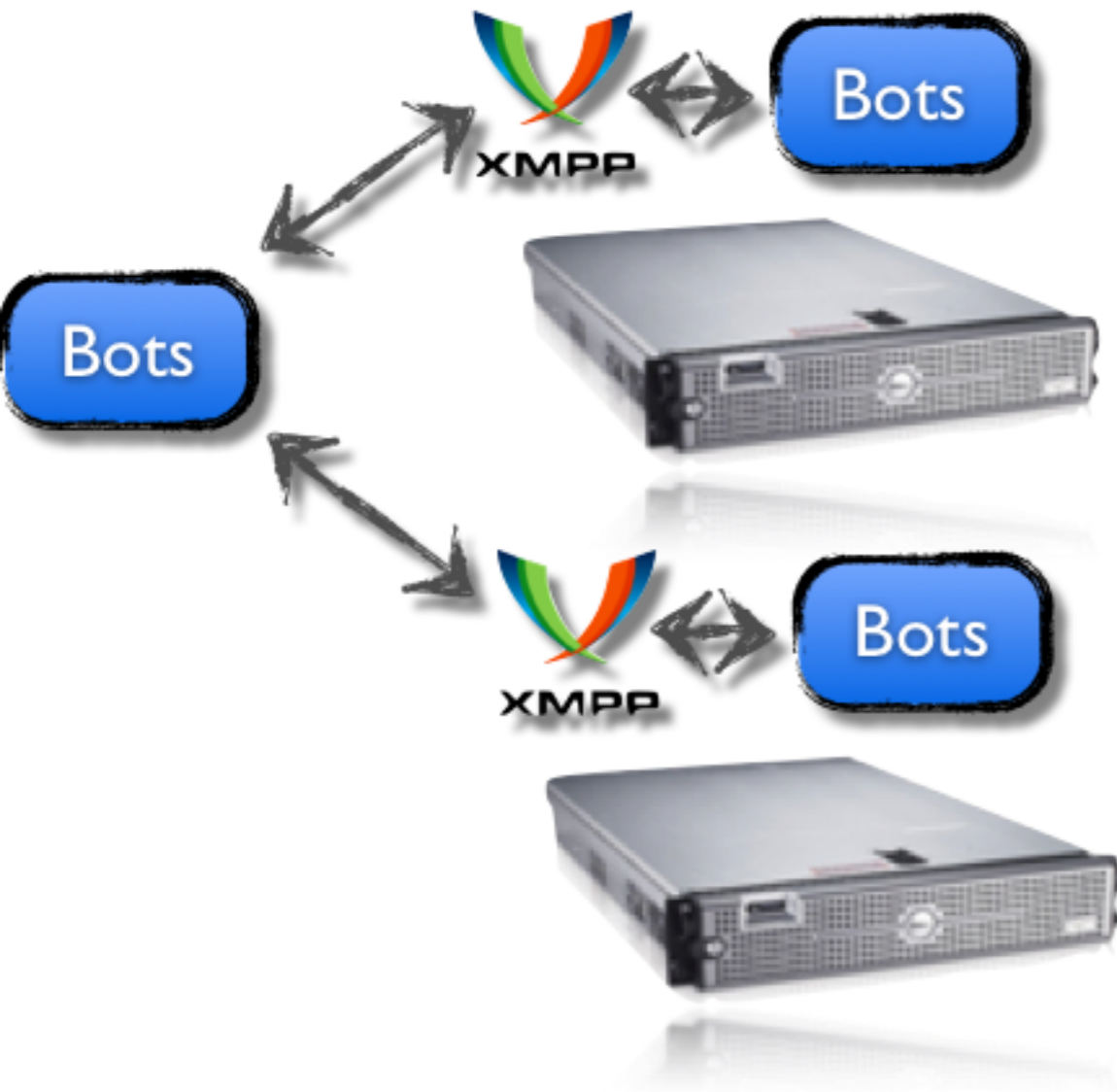

Different Means for Collaboration

- Bridged Collaboration
- Federated Collaboration
- Legacy Collaboration



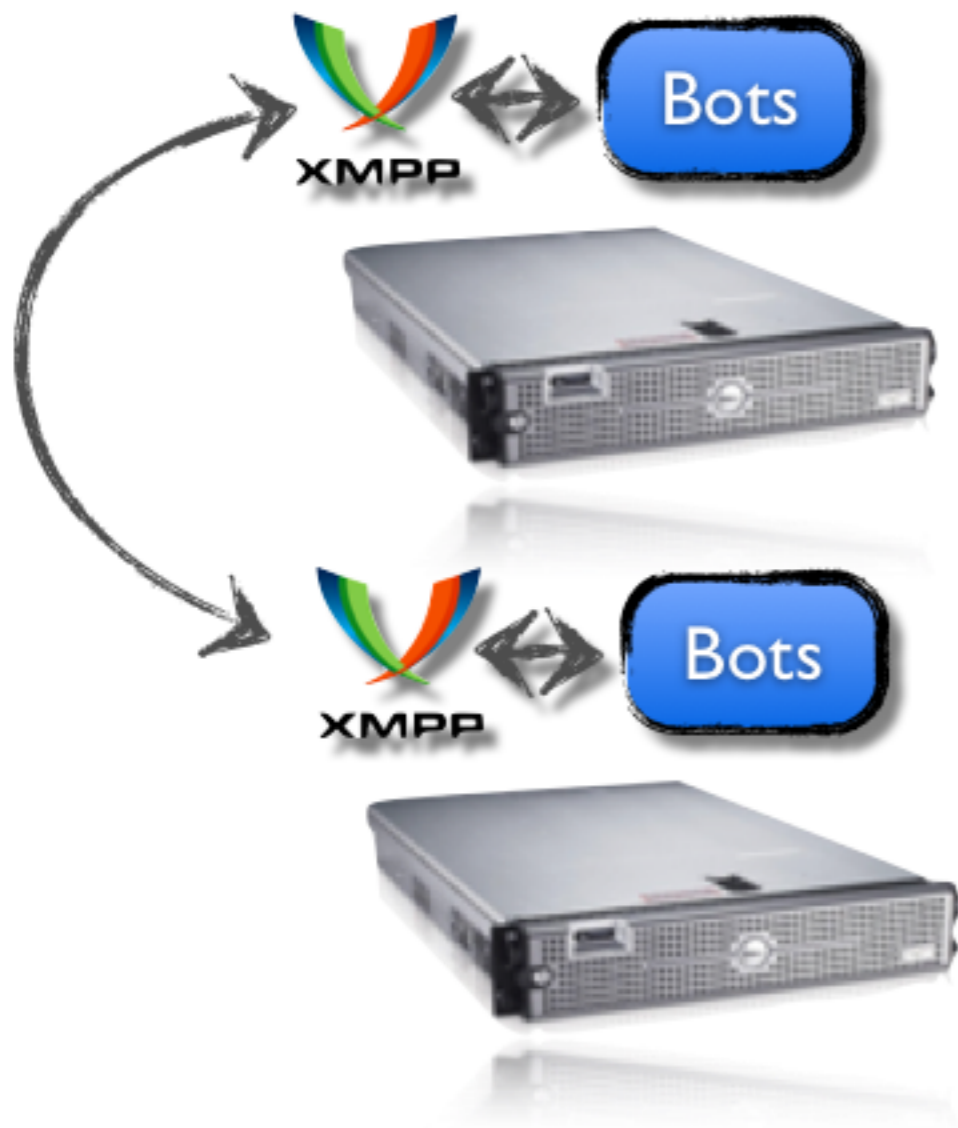


Bridged Collaboration



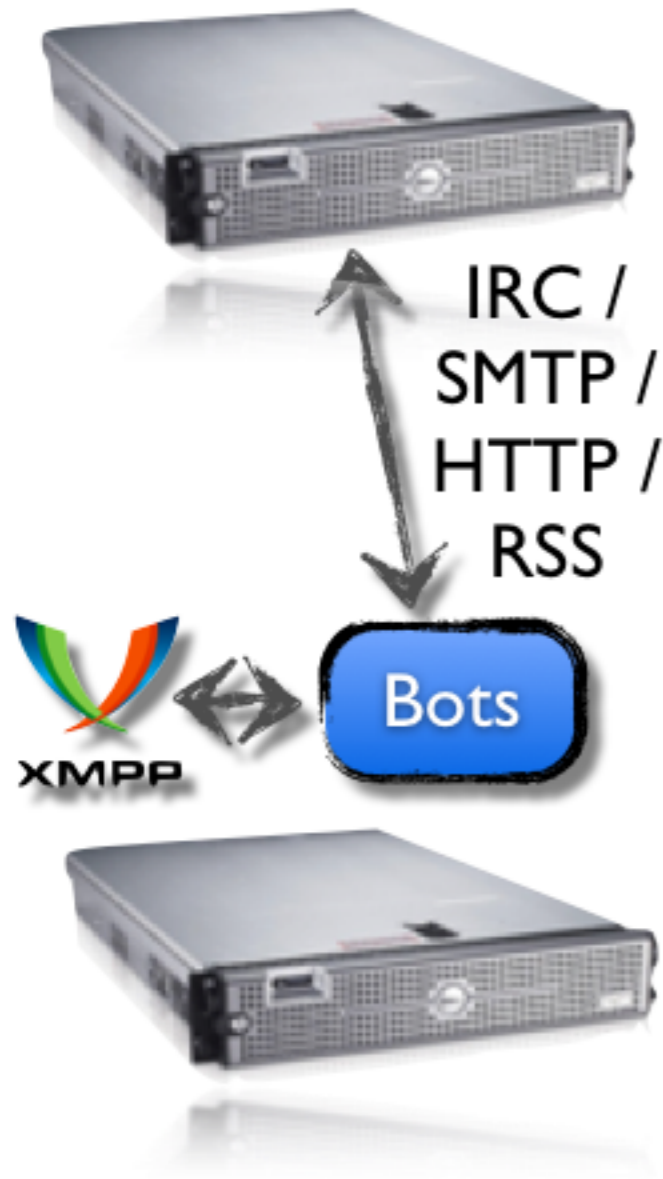
- With Bridged Collaboration collaborators (such as different national CERTs) just join their bots to each others specific MUCs (channels).
- For example CERT-EE may receive information that is relevant to CERT-FI
 - CERT-FI will join a bridge/collector/reportert bot to finland@conference.cert.fi MUC
 - CERT-EE will use splitterbot to throw all information relevant to CERT-FI to the finland MUC

Federated Collaboration



- In federated collaboration collaborators unleash the flexibility of XMPP, federating their servers.
- If CERT-EE receives information relevant to CERT-FI, CERT-EE bot will report directly to finland@conference.cert.fi.
- Another scenario, CERT-FI's bot connects to cert.fi-server and joins channel finland@conference.cert.ee.
- XMPP federation will take care of routing the messages.

Legacy Collaboration



- If none of the previous collaboration mechanisms do not fit to you, we have legacy collaboration.
- Bots can connect via several mediums [1](#) to legacy reporting mediums.
 - Near-real-time: for example IRC
 - Polling: SMTP/HTTP/RSS
- You can recycle the feed and reporting bots.

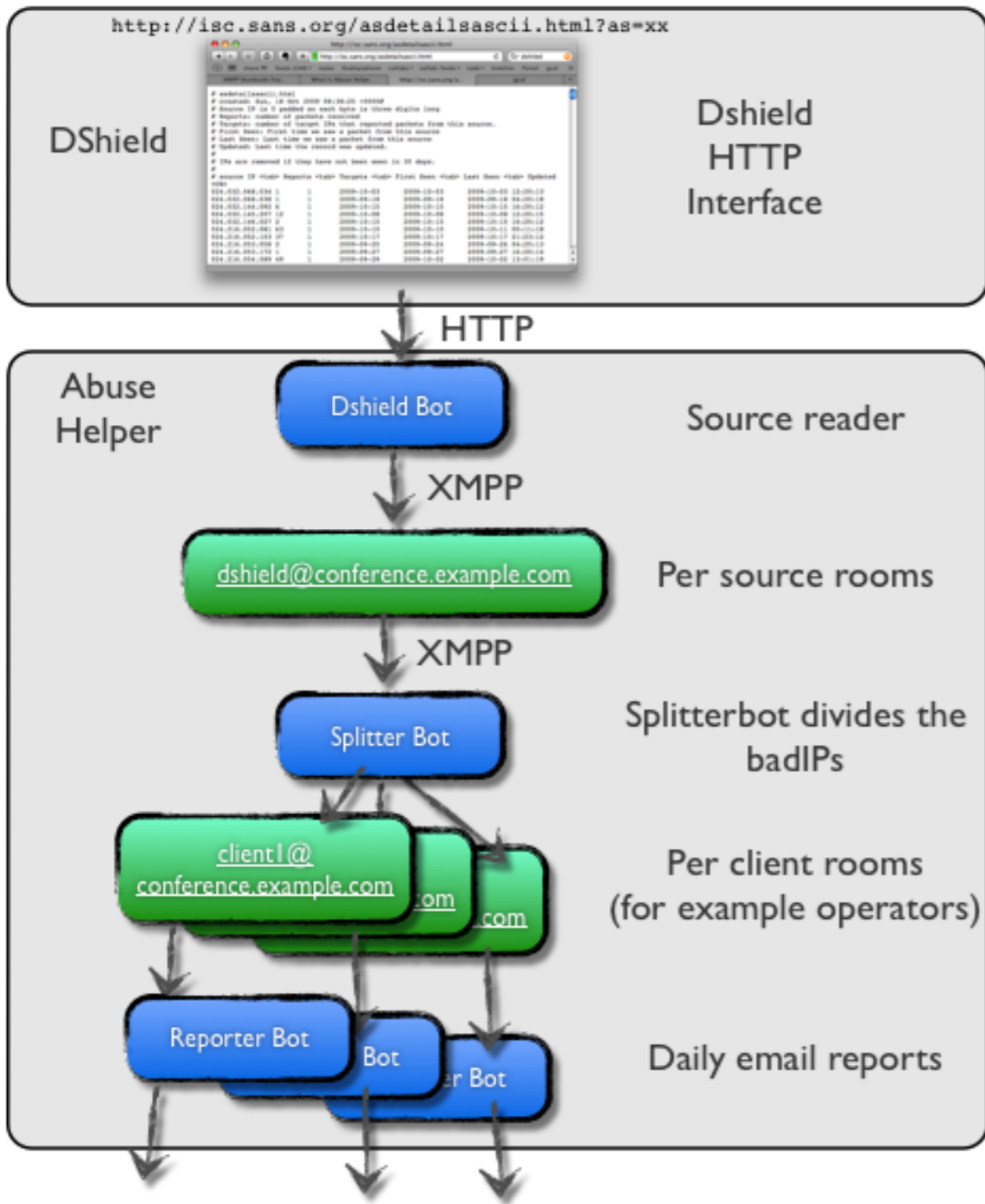
1. Not all are available right now, but nothing prevents you creating your own bots. ([1](#))

Use Case Examples



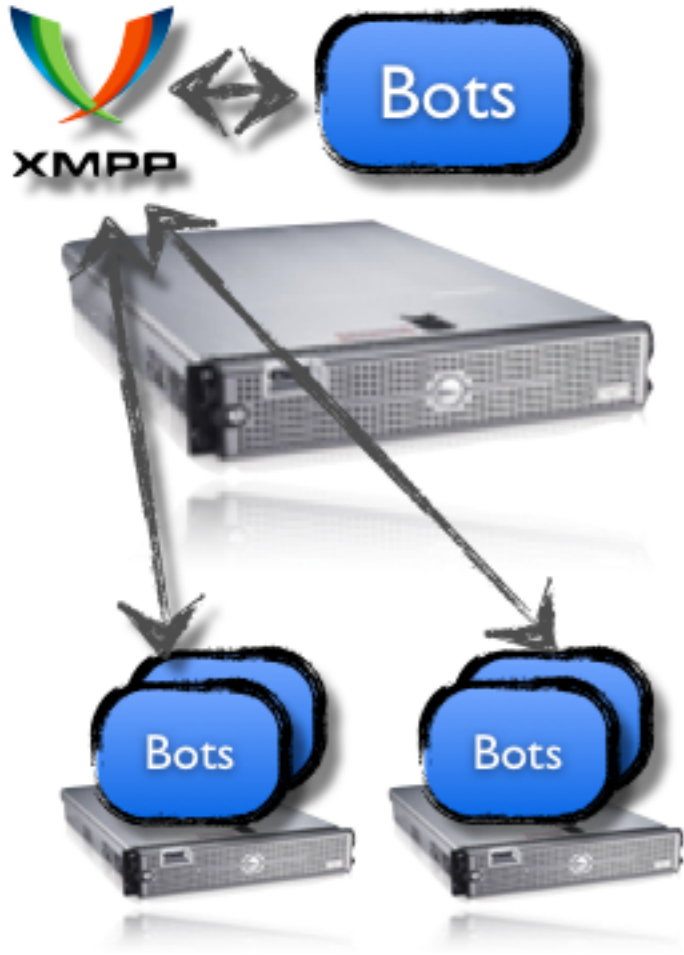
- How you deploy your abuse helper is your choice:
 - **No XMPP:** You have few sources and 1-3 clients, forget the XMPP and make your bots talk to each other via [Idiokit](#) pipes.
 - **Single machine with XMPP:** You have more than 2 sources and several clients, use single machine with XMPP to enable flexibility and observability.
 - **Distributed:** Distribute the workload by running the bots in several machines. Run reconnaissance bots in different geolocations and ASes.

Single Machine With XMPP - DShield Use Case

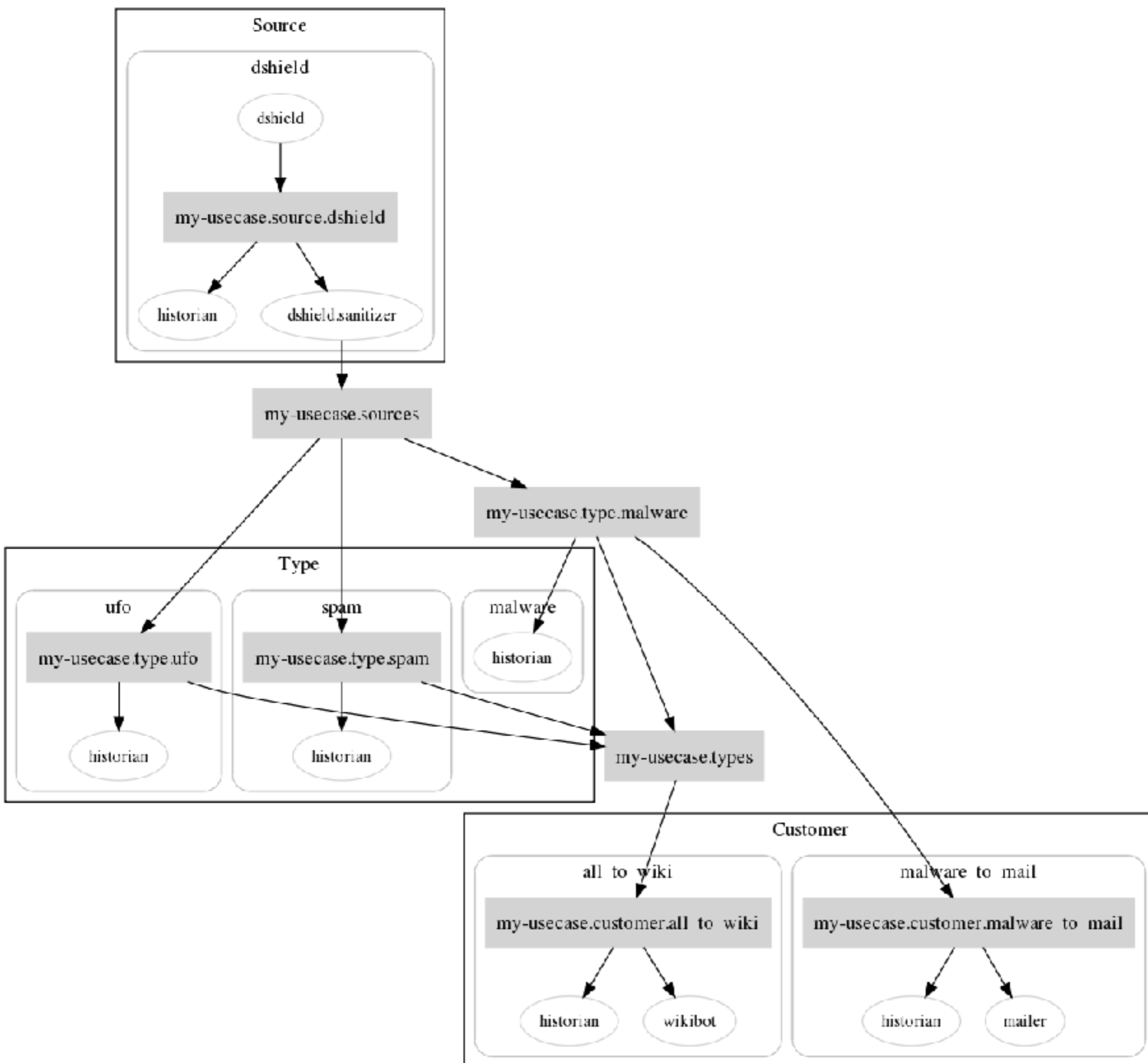


Distributed Setup

- With XMPP, distributing your work load is simple:
 - just launch some of the bots in different machines



Simple example customer setup





DEMO: Simple config, handling feeds



Abuse Helper: Simple Benefits

Enabling Abuse Feed Usage

- Several feed types supported out of the box
- Integration with in-house malicious activity detection tools (darknets, sandnets etc)
- Ease of customisation to differing environments has been a key in the development

Raising Process Maturity

1. All by hand
2. Ad hoc (in-house) scripts
3. Hands on automata (abuse specific ticketing system)
4. Hands off automata

Use Cases

End Users (Victims)

- More readily understand Internet Abuse (and fighting it)
- Receive timely information on actualised threats and vulnerabilities
 - Feedback loop to risk management
- Receive information pertaining to your assets
- Integrate with existing monitoring information to enhance network protection

CSIRTs (Dealers)

- Collaborate with other CSIRT teams more efficiently
- Get trends and statistics for networks you observe
- Identify high risk networks
 - Focus efforts on chronic infections or possible organised malicious activity
- Have a consisted terminology and workflows for Abuse Reporting
- Reduce reporting effort

Feed Providers (Sources)

- Have a consisted terminology and workflows for Abuse Reporting
- Have readily-thinked access control and visibility to your data consumers
- Streamline your feeds to near-real-time



Advanced Use Cases

- Handling of infected customers
 - Integration with ticketing system, walled garden, CRM, provisioning, ...
- Investigative aid in Incident Handling
 - Using historical data, active and passive data gathering, integration with network monitoring, ...
- Network protection
 - integration with endpoint monitoring, audit findings, network monitoring and risk management

Simple Examples

How to Get Started

- SVN checkouts: <http://code.google.com/p/abusehelper/source/checkout>
 - Downloadable package available later in Sourceforge and Google code.
- [User documentation](#) (installation/configuration etc)
- Talk with contributors in CollabChat, in [✉ abusehelper@conference.clarifiednetworks.com](mailto:abusehelper@conference.clarifiednetworks.com).
 - Our server is federated with Google and Jabber.org, but for MUC access you need to use your collab account (the one you logged in to this environment), see instructions to join at [CollabChat](#) -page.



Contributing

- Content contribution: Feel free to contribute to this wiki-based collaboration environment
- Social contribution: Contribute community members by [inviting](#) them.
- Code contributions
 - Ask commit access from [Jukke](#) ([✉ contact@clarifiednetworks.com](mailto:contact@clarifiednetworks.com))
 - Guidelines for the repository structure:
 - `./abusehelper` - Abuse Helper core features, commits go through [Jukke](#), [Sebastian](#) and [Mika](#)
 - `./contrib` - anyone can contribute
 - See some code [Examples](#)
- Process contribution: Promote, regulate, motivate, mandate!