This is abuse?

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

Dear System Administrator,

I received a report from a 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: [ ] to ensure effective response.
-------------------------------

Regards,

-----------Full Header-----------
Return-Path:
Abuse Ground Zero: At the wrong end of the stick

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

Web site vuln, attack or incident feeds

- Defacements: http://zone-h.org/archive/special=1
- XSS Incidents: http://www.xs3ed.com/archive/special=1
- Some wepawet JS deobfuscation analyses contain CVEs http://wepawet.cs.ucsb.edu/static/toppig-twitter.html
- Various attack data: http://barometer.interoute.com/barom_stat_alerts.php

- sources of malicious IPs.
  - abusechiff http://idsbl.abuse.ch/fastfluxtracker.php
  - abusechweb http://idsbl.abuse.ch/webabusetracker.php
  - arbor http://atlas-public.ac2.arbor.net/public Sadly attackers
  - autoshun http://www.autoshun.org/files/shunlist.csv
  - badguys http://www.l-taron.de/linux/badguys.txt
  - blacklisted http://www.infiltrated.net/blacklisted
  - brawg http://www.brawg.com/hosts.deny
  - cleanmx http://support.clean-mx.de/clean-mx/xmlviruses?response=alive&format=csv&fields=uri,ip,domain&domain=
  - cleanmxp http://support.clean-mx.de/clean-mx/xmlphishing?response=alive&format=csv&fields=uri,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
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.
<table>
<thead>
<tr>
<th><strong>Components</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bots</strong></td>
</tr>
<tr>
<td><strong>CouchDB</strong></td>
</tr>
<tr>
<td><strong>Ejabberd</strong></td>
</tr>
<tr>
<td><strong>idiokit</strong></td>
</tr>
<tr>
<td>Bot</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td><strong>AtlasSRFBot</strong></td>
</tr>
<tr>
<td><strong>ConfigBot</strong></td>
</tr>
<tr>
<td><strong>CSV2XMPP</strong></td>
</tr>
<tr>
<td><strong>CymruWhois</strong></td>
</tr>
<tr>
<td><strong>DSHieldBot</strong></td>
</tr>
<tr>
<td><strong>Historian</strong></td>
</tr>
<tr>
<td><strong>IMAPBot</strong></td>
</tr>
<tr>
<td><strong>IRCFeedBot</strong></td>
</tr>
<tr>
<td><strong>Reporter</strong></td>
</tr>
<tr>
<td><strong>Roomgraph</strong></td>
</tr>
</tbody>
</table>
DEMO: Basic operation out of the box
Different Means for Collaboration

- Bridged Collaboration
- Federated Collaboration
- Legacy 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/reporterbott 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 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

http://iso.sone.org/anddetailsasoci1.html?as=ex

DShield

Dshield HTTP Interface

HTTP

Abuse Helper

Dshield Bot

Source reader

Per source rooms

XMPP
dshield@conference.example.com

Splitter Bot

Splitterbot divides the badIPs

Per client rooms (for example operators)

XMPP

Reporter Bot

Daily email reports

client@conference.example.com

Bot

Bot
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
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-thought 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

- 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!