



Vulnerabilis

Aghast

HOMO
Awarensis

Dexterous

Securis

OTRS: Issue Management System Meets Workflow of Security Team

Pavel Kácha, 2007
CESNET, z. s. p. o.

History

- postmaster@, hostmaster@, abuse@
- Mailbox
 - Reply-To problem
- Later shared mailbox (IMAP)
 - Strict coordination needed (1 RW, others RO)
 - Handover summary of open incidents needed
 - Mail threading problem - incidents scattered through mailbox
 - No scaling

What now?

- Most incidents do not need professional erudition - routine work
- Reach target faster - we're part time
- 1. line - Monitoring Centre
 - They can handle usual cases, rest may go to us
- They have to:
 - Identify type and severity of incident
 - Identify responsible administrator (or team)
 - Pass incident on

Needs

- Whois (RIPE)
- Keep messages of one incident together
- Action originator
- Metadata (to store responsible network)
- Templates for forwarding and replying
- PGP, S/MIME
- Libre, or at least reasonably open source
- Issue management system

Alternatives

OTRS, Trac, Mantis, RTIR, RoundUp, Thunderbird + IMAP + extensions, Bugzilla, Sirios, Issue Tracker, Issue Tracking Product, Issue Management Tool, phpticket, batts, Ticketsmith, whups, Keystone, phpSupport, DCL, frontdesk, JitterBug, Teacup PRMS, CLC, OcoMon, Techtables, PHPTasks, Gedeon, WebCall, WREQ, PEST, oTasks, EdenCRM, urqm, PHPHelpdesk, openTicket, BugIn, PHPSAT, GNATS, IssueDealer...

See <http://www.cesnet.cz/doc/techzpravy/2006/tickets-review/>



[Queue: Certs]

Tickets shown: 1-6 - Page: [1](#) - Tickets available: 6 - All tickets: [6](#)Queues: [My Queues \(7\)](#) - [Certs \(6\)](#) - [Certs-IDS \(4\)](#) - [Certs-Masters \(7\)](#) - [Certs-Scrap \(39\)](#) - [MDS \(410\)](#) - [Misc \(4\)](#) - [Spam \(3113\)](#)**[Ticket#: 2007050247000075] [SpamCop
(<http://bgvgeos.roundlearn.hk/?718999297160>) id:227[.]****[Age: 3 hours 4 minutes]**[Lock](#) - [Zoom](#) - [History](#) - [Priority](#) - [Note](#) - [Close](#)**Created:**05/02/2007 08:54:52**From:** "BigD" <2270478406@reports.spamcop.net>
To: abuse@cesnet.cz
Subject: [SpamCop (<http://bgvgeos.roundlearn.hk/?718999297160>) id:2270478406]Check out th[.]**State:** new
Priority: 3 normal
Queue: Certs**CustomerID:** [2270478406@rep\[.\]](#)
Escalation none
in:
NETNAME: UPOL-TCZ
IP: 158.194.183.102
ADMIN: abuse@upol.cz**[Ticket#: 2007050247000084] [SpamCop
(<http://eltdpa.whetherproper.hk/?625295560451>) id:2[.]****[Age: 2 hours 27 minutes]**[Lock](#) - [Zoom](#) - [History](#) - [Priority](#) - [Note](#) - [Close](#)**Created:**05/02/2007 09:32:03**From:** "Guido Bienhaus" <2270515243@reports.spamcop.net>
To: abuse@cesnet.cz
Subject: [SpamCop (<http://eltdpa.whetherproper.hk/?625295560451>) id:2270515243]Cheap / I [.]**State:** new
Priority: 3 normal
Queue: Certs**CustomerID:** [2270515243@rep\[.\]](#)
Escalation none
in:
NETNAME: UPOL-TCZ
IP: 158.194.183.102
ADMIN: abuse@upol.cz**[Ticket#: 2007050247000093] [SpamCop (<http://repeatmusic.hk/>)
id:2270517341]Don't miss t[.]****[Age: 2 hours 24 minutes]**[Lock](#) - [Zoom](#) - [History](#) - [Priority](#) - [Note](#) - [Close](#)**Created:**05/02/2007 09:34:17**From:** "Guido Bienhaus" <2270517341@reports.spamcop.net>
To: abuse@cesnet.cz
Subject: [SpamCop (<http://repeatmusic.hk/>) id:2270517341]Don't miss this unique chance**State:** new
Priority: 3 normal
Queue: Certs**CustomerID:** [2270517341@rep\[.\]](#)
Escalation none
in:
NETNAME: UPOL-TCZ
IP: 158.194.183.102
ADMIN: abuse@upol.cz

OTRS - Pros

- Handles directly email messages (stores MIME)
- LDAP authentication
- Metadata
- Dynamic templates
- Stable mail identifiers
- Detailed log of all actions
- PGP, S/MIME
- Perl

OTRS - Cons

- Templates only for Reply, not for Forward
- Only inline forward
- Subject: Re/Fwd
- Not exactly glaring performance
- Live project, but only handful of developers
- Project lists usually help only with basic problems
- Perl

States/Queues

- New, Open, Update
- Resolved, Unresolved
- Warn, IDS, Informed
- Scrap, Organizing
- Certs - main queue
- Certs-Masters - us
- Certs-IDS - LaBrea
www.cesnet.cz/doc/techzpravy/2006/ids/
- Certs-Scrap - unusable complaint
- Spam, MDS

Pavel Kácha, CSIRTmaster of the day
CESNET Computer Security Incident Response Team
Zikova 4
160 00 Prague 6
The Czech Republic

Vážení kolegové,

CESNET Computer Security Incident Response Team obc zprávu o nedoručitelnosti elektronické pošty ze str 147.33.15.5, který je ve Vaší správě.

Autorům stížnosti se nelíbí, že tyto zprávy neodmit server už v průběhu SMTP konverzace: RCPT TO -> odp

Příloha:

Následující stav tiketu:

Doba čekání na vyřízení (pro stavy čekání na vyřízení*):

Jednotky času(jednotky práce):

- uzavřeno - vyřešeno
- uzavřeno - nevyřešeno
- otevřít
- uzavřeno - automat
- uzavřeno - hlášení IDS
- uzavřeno - jsme informováni
- uzavřeno - odpad
- uzavřeno - organizační
- uzavřeno - upozornění

IP harvesting

- How to integrate *whois*?
 - Web? Special interface?
- Complaint goes through module, which
 - Extracts from mail everything reminding IP address
 - Determines, if it belongs into Cesnet network
 - If yes, asks RIPE for details
 - Appends IP address, Netname and Administrator contact as metadata

IP harvesting II

- When forwarding, recipient goes from metadata
- More or no IP address - needs human
 - But rarely happens
- For majority of incidents monitoring has all needed info, if not, hands incident over to us

Od: Netvigator Postmaster <postmaster@netvigator.com>
Komu: abuse@cesnet.cz
Předmět: Spamming IP: 195.113.79.75
Vytvořeno: 06/04/2007 19:47:44

Dear Sir/Madam,

The spammer below is either using your resources to send out bulk unsolicited commercial e-mail ("spam") or is deceptively trying to make it look like he is. In either case, a legitimate company like yours probably would not approve. The information below should be all you need.

Please take the necessary actions to stop the spam.

Thanks for your cooperation !

uova.
Stupňování -
v:
Vlastník: andrea (Andrea Kropáčová)
Linked (Normální):
Linked (Parent):
Linked (Child):
NETNAME: UZSI-TCZ
IP: 195.113.79.75
ADMIN: abuse@uzsi.cz

Forwarding templates

- Homemade patches, Forward rewritten
(trying to push upstream)
- Now uses same templates as Reply
- Recipient filled in from metadata
(network abuse contact)

Choose an incident:

[OTRS] Pavel Kácha (ph@rook.cz) Thu May 03 11:43:04 2007

[Logout](#) [QueueView](#) [Phone-Ticket](#) [Email-Ticket](#) [Search](#) [Preferences](#) [Customer](#) [Bulk-Action](#) | [Stats](#) [Admin](#) [New message](#) [Locked Tickets](#)

[\(0\)](#) [\(0\)](#)

[Queue: Certs]

Tickets shown: 1-3 - Page: [1](#) - Tickets available: 3 - All tickets: [3](#)

Queues: [My Queues \(7\)](#) - [Certs \(3\)](#) - [Certs-IDS \(4\)](#) - [Certs-Masters \(7\)](#) - [Certs-Scrap \(39\)](#) - [MDS \(410\)](#) - [Spam \(3147\)](#)

[Ticket#: 2007050247000101] [SpamCop (http://repeatmusic.hk/) id:2270535498]SPAM-LOW: D[.] **[Age: 1 day 1 hour]**

[Lock](#) - [Zoom](#) - [History](#) - [Priority](#) - [Note](#) - [Close](#)

Created: 05/03/2007 08:18:34

From: "Jacob Chiong" <jacob@farexmarketing.com>	State: aktualizace	CustomerID: 2270535498@rep[.]
To: "Cesnet Certs" <certs@cesnet.cz>	Priority: 3 normal	Escalation none
Subject: Re: [Ticket#2007050247000101] [SpamCop (http://repeatmusic.hk/) id:2270535498]SP[.]	Queue: Certs	in:
		NETNAME: UPOL-TCZ
		IP: 158.194.183.102
		ADMIN: abuse@upol.cz

[Ticket#: 2007050347000153] [SpamCop (http://puusn.payhold.hk/?804331472279) id:22717048[.] **[Age: 1 hour 0 minute]**

[Lock](#) - [Zoom](#) - [History](#) - [Priority](#) - [Note](#) - [Close](#)

Created: 05/03/2007 10:42:57

From: 2271704881@reports.spamcop.net	State: new	CustomerID: 2271704881@rep[.]
To: abuse@cesnet.cz	Priority: 3 normal	Escalation none
Subject: [SpamCop (http://puusn.payhold.hk/?804331472279) id:2271704881]\$1.59 a pill is t[.]	Queue: Certs	in:
		NETNAME: UPOL-TCZ
		IP: 158.194.183.102
		ADMIN: abuse@upol.cz

Review and pick template:

[Zoom Ticket#: 2007050347000153] [SpamCop (<http://puusn.payhold.hk/?804331472279>) id:22717048[.]

[Age: 1 hour 2 minutes]

[Back](#) - [Lock](#) - [History](#) - [Print](#) - [Priority](#) - [Free Fields](#) - [Link](#) - [Owner](#) - [Customer](#) - [Note](#) - [Merge](#) - [Pending](#) - [Close](#)

Created:05/03/2007 10:42:57

|-->>> **1. customer (email-external) (plain) 2271704881@repor[.]: [SpamCop ([http://puu\[.\]](http://puu[.]))-05/03/2007 10:42:57**

From: 2271704881@reports.spamcop.net
To: abuse@cesnet.cz
Subject: [SpamCop (<http://puusn.payhold.hk/?804331472279>) id:2271704881]\$1.59 a pill is the best price for V1agr@ ever pro..
Created: 05/03/2007 10:42:57

[SpamCop V630]

This message is brief for your comfort. Please use links below for details.

Spamvertised web site:

<http://puusn.payhold.hk/?804331472279> [#####
#####2]<http://puusn.pauhold.hk/?804331472279> is
158.194.183.102; Thu, 03 May 2007 08:42:40 GMT

[Offending message]

Return-Path: <Melinda@vc.netyou.jp>

X-Spam-Flag: YES

X-Spam-Checker-Version: SpamAssassin 3.1.5 (2006-08-29) on
bpa09de.bpaserver.net

X-Spam-Level: *****

X-Spam-Status: Yes, score=31.6 required=5.0 tests=DRUGS_ERECTILE,
DRUGS_ERECTILE_OBFU,FUZZY_VPILL,HELO_DYNAMIC_HCC,HTML_IMAGE_ONLY_16,
HTML_MESSAGE,HTML_SHORT_LINK_IMG_2,MIME_HTML_MAINLY,MPART_ALT_DIFF,
PART_CID_STOCK,PART_CID_STOCK_LESS,RAZOR2_CF_RANGE_51_100,
RAZOR2_CF_RANGE_E4_51_100,RAZOR2_CF_RANGE_E8_51_100,RAZOR2_CHECK,
STOCK_IMG_HDR_FROM,STOCK_IMG_HTML,SUBJ_DOLLARS,TVD_FW_GRAPHIC_ID1,
URIBL_BLACK,URIBL_JP_SURBL,URIBL_OB_SURBL,URIBL_SC_SURBL
autolearn=disabled version=3.1.5

X-Spam-Report:

* 3.3 HELO_DYNAMIC_HCC Relay HELO'd using suspicious hostname (HCC)
* 0.4 SUBJ_DOLLARS Subject starts with dollar amount

State: new
Priority: 3 normal
Queue: Certs
Locked: unlock
CustomerID: 2271704881@reports[.]
Accounted 0
time:
Escalation -
in:
Owner: root@localhost (Admin OTRS)

Linked
(Normal):
Linked
(Parent):
Linked
(Child):

NETNAME: UPOL-TCZ
IP: 158.194.183.102
ADMIN: abuse@upol.cz

Customer Info:

Compose Answer (email):

- ◆ [Empty](#)
- ◆ [FWD upozornění - Abuse](#)
- ◆ [FWD upozornění - Bounce](#)
- ◆ [FWD upozornění - Spam](#)

Pick state and pass incident along:

From: Cesnet Certs <certs@cesnet.cz>
To: 2271704881@reports.spamcop.net
Cc:
Bcc:
Subject: Re: [Ticket#2007050347000153] [SpamCop (http://puusn.payhold.hk/?804331472279) id
Options: [[Address Book](#)] [[Attachments](#)]
Text:
Dear Administrator,

the CESNET Computer Security Incident Response Team has received attached e-mail notice regarding spam abuse originating at computer 158.194.183.102 which belongs to your network/domain.

Would you please check the integrity of this computer and solve the problem (if any) as soon as possible?

With best regards

Attachment:

Next ticket state:
closed successful
closed unsuccessful
open
uzavřeno - automat
uzavřeno - hlášení IDS
uzavřeno - jsme informováni
uzavřeno - odpad
uzavřeno - organizační
uzavřeno - upozornění

Pending Date (for pending* states):

Time units (work units):

https://rt.cesnet.cz/otrs-2.1.2...&ResponseID=4&TicketID=9758&ArticleID=11...

Dealing with spam

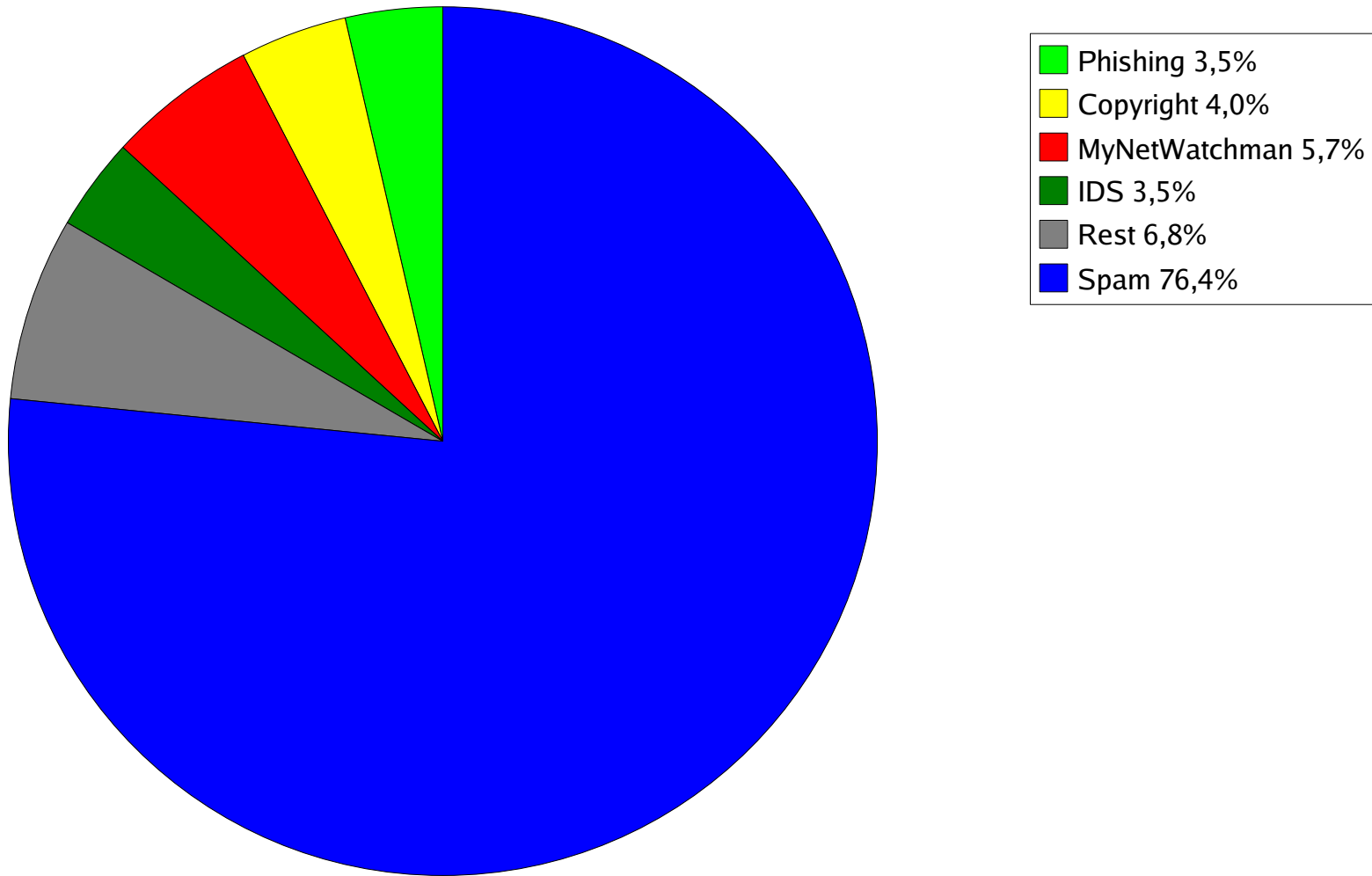
- SpamAssassin...
 - ... but incident complaint can itself contain spam and be marked as such!
- Keyword whitelist

```
/abuse mail|abuse-mail|abuse of|abuse report|abuse spam|  
e-mail spam|multiple spam|received spam|report abuse|  
reported spam|reporting spam|returned spam|spam:|spam  
abuse|spam complaint|spamcop|spam from|spam mail|  
spammails|spam mails|spammer|spamming|spam-rbl|stop the  
spam|ube:|ube-uce|ube\/uce|uce:|uce-ube|uce\/ube|ube  
from|uce from|\[uce\]|\[spam\]|spam received|uce  
complaint|ube complaint|phish|fraud/
```

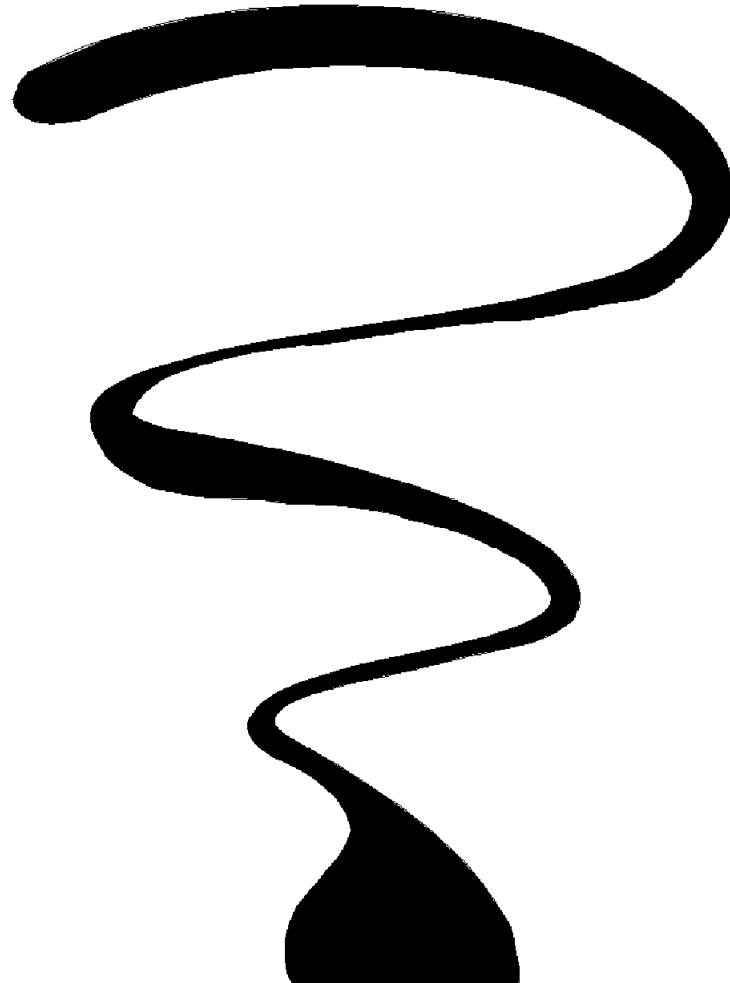
Useful

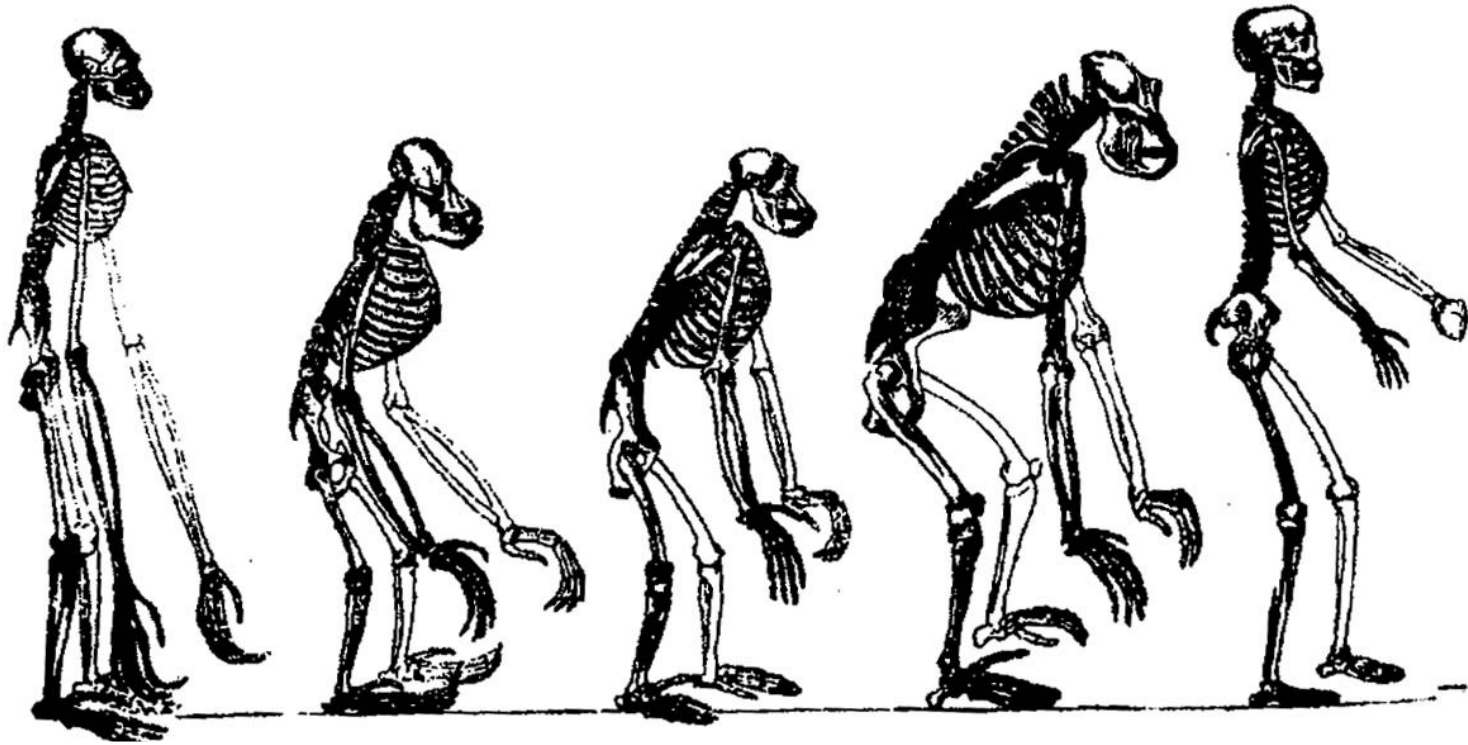
- PGP signing
- We're able to verify PGP and S/MIME
- FollowUpSearchIn*
(pairs even mail delivery notification reports)
- Complex, but transparent database model
 - Statistics is just bunch of clever SQL queries
 - We plan detection of repeated complaints
 - We plan auto escalation of incidents with no response

Incident types in 2007



Questions





Big Bang

Pine

We and OTRS

Monitoring
and OTRS

Us on
Hawaii

Thank you for you attention