vulnerabilis    aghast    hominid    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...

[ Ticket#: 2007050247000075 ] [SpamCop (http://bgvgeos.roundlearn.hk/?718999297160) id:227[...]

State: new
Priority: 3 normal
Queue: Certs

[ Ticket#: 2007050247000084 ] [SpamCop (http://elftdpa.whetherproper.hk/?625295560451) id:2[...]

State: new
Priority: 3 normal
Queue: Certs

[ Ticket#: 2007050247000093 ] [SpamCop (http://repeatmusic.hk/) id:2270517341]Don't miss t[...]

State: new
Priority: 3 normal
Queue: Certs
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
- Certs-Scrap - unusable complaint
- Spam, MDS
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
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:

<table>
<thead>
<tr>
<th>Ticket#</th>
<th>Subject</th>
<th>From</th>
<th>To</th>
<th>Priority</th>
<th>State</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007050247000101</td>
<td>Re: [Ticket#2007050247000101] [SpamCop (<a href="http://repeatmusic.hk/">http://repeatmusic.hk/</a>) id:2270535498]SPAM-LOW: D[...]</td>
<td>&quot;Jacob Chiong&quot; <a href="mailto:jacob@farexmarketing.com">jacob@farexmarketing.com</a></td>
<td>&quot;Cesnet Certs&quot; <a href="mailto:certs@cesnet.cz">certs@cesnet.cz</a></td>
<td>3 normal</td>
<td>aktualizace</td>
<td>05/03/2007 08:18:34</td>
</tr>
<tr>
<td>2007050347000153</td>
<td>[SpamCop (<a href="http://puusn.payhold.hk/?804331472279">http://puusn.payhold.hk/?804331472279</a>) id:2271704881]$1.59 a pill is t[...]</td>
<td><a href="mailto:2271704881@reports.spamcop.net">2271704881@reports.spamcop.net</a></td>
<td><a href="mailto:abuse@cesnet.cz">abuse@cesnet.cz</a></td>
<td>3 normal</td>
<td>new</td>
<td>05/03/2007 10:42:57</td>
</tr>
</tbody>
</table>
Review and pick template:

Spam advertised web site: 
http://puusn.payhold.hk/?804331472279

Offending message:

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.

Spam advertised web site: 
http://puusn.payhold.hk/?804331472279

Offending message:

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.
Pick state and pass incident along:

Dear Administrator,

the CESNET Computer Security Incident Response Team has received attached e-mail notice regarding spam abuse originating at computer 158.194.183.182 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 options]

Next ticket state:
- open
- closed successful
- closed unsuccessful

Pending Date (for pending* states):

Time units (work units):
- uzavřeno - automat
- uzavřeno - hlášení IDS
- uzavřeno - jsme informováni
- uzavřeno - odpad
- uzavřeno - organizační
- uzavřeno - upozornění

Submit
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|spammcop|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
Questions
Thank you for your attention