US IN NUMBERS

**Clarified 2010:**
- Estonia (gov & NATO CCDCOE), Russia, Finland, Sweden
- CERTs, Banks, Large teleoperators, Large enterprises, other gov orgs.
- 1.5x growth, profitable, AAA-rating

**Clarified 2011 - Joining forces with Codenomicon**, sales rep now includes:
- UK, Canada, Japan, Sweden, Netherlands, US
- Operating in US/European/APAC market
- As a whole: 70 person R&D community producing innovative solutions to protect you and your constituencies
1. Analyzer used in Bredolab botnet takedown, Dutch TV-channel covers

2. White House still remembers our research results from 2002, Chief of Defense Command Finland tweets about it after his visit. (Clarified Networks and Codenomicon are spin-offs from Oulu University Secure Programming Group).

3. Virtual Situation Room deployment for Estonian Government

4. Situation rooms for NATO Baltic Cyber Shield exercise, covered by Swedish national TV (SVT)

5. Clarified Visualization in Mikko Hyppönen’s TED talk, 300 000 views as of 2011-09

6. News coverage of CERT.be fighting against website hacks, AbuseHelper’s TV-premiere.
ABUSE SITUATION AWARENESS

Jani Kenttälä, Clarified Networks Oy, part of Codenomicon Group
CHALLENGE: ABUSE IS REALITY

Screenshot of a real-time visualization showing abuse events.

Monday, November 7, 11
AID, AND A NEW CHALLENGE: A LOT OF FEEDS TELLS US ABOUT IT
AID, AND A NEW CHALLENGE: A LOT OF FEEDS TELLS US ABOUT IT
THE PROCESS

We help our customers to deal with Cyber threats (malware, spam, botnets etc) by:
• fully automating the data collection from external sources,
• enabling actionable reporting to stakeholders, and
• visualizing the collected information for risk management and decision support
• Additionally we enable cross-organizational collaboration
RAISING THE MATURITY OF ABUSE HANDLING

UP TO THE FULL AUTOMATION

• Manual
• Ad hoc (in-house) scripts
• Hands on automata (abuse specific ticketing systems)
• **Hands off automata**
• Investigative capability
"The infection rates and other metrics for Finland have consistently been below the world-wide averages, and we have often wondered ourselves what the reason is for this"  

— Kimmo Bergius, Microsoft’s Chief Security Advisor
HOW DID IT WORK FOR CERT-FI?

- That opened our eyes!!
- We probably still only see the tip of the iceberg..

In 2006, we enhanced automation

1000 manually handled cases
100,000 automatically handled cases

From: abuse-report.certi-fi@gmail.com
Subject: Daily Abuse Report for SecurityInsecure Inc.
Date: August 16, 2011 21:44:11 GMT+03:00
To: Jani Kostas (jani@certifi-networks.com)

Abuse Helper found reports regarding your network. See the data below, or click the attachment.

<table>
<thead>
<tr>
<th>time</th>
<th>ip</th>
<th>typ</th>
<th>cc</th>
<th>asa</th>
<th>asname</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-08-16 18:44:05 UTC</td>
<td>71.94.146.92</td>
<td>drone</td>
<td>US</td>
<td>2015</td>
<td></td>
</tr>
<tr>
<td>2011-08-16 18:44:05 UTC</td>
<td>71.94.146.93</td>
<td>drone</td>
<td>US</td>
<td>2015</td>
<td></td>
</tr>
<tr>
<td>2011-08-16 18:44:05 UTC</td>
<td>71.94.146.94</td>
<td>drone</td>
<td>US</td>
<td>2015</td>
<td></td>
</tr>
</tbody>
</table>

Regards,
Abuse Helper

report 23
WHY THIS HASN’T BEEN DONE EARLIER?

- Each feed is different in terms of timing, transport, data format, data content etc.

- On the other hand, reporting requirements may be very specific.
COMMUNITY HAS CALLED FOR IT

• 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 presented at Black Hat USA -09
TOOLS FOR DEALING WITH ABUSE

• AbuseHelper
  • A tool for collecting and sharing suspected malicious activity
  • Collect and process Abuse Information
  • Sent out actionable reports

• Virtual Situation Room
  • Gain situational awareness over Abuse Information
  • Real-time visualizations from your perspective
ABUSEHELPER

• A tool for collecting and sharing suspected malicious activity
• Botnet inspired architecture
  • Distributed
  • Modular
• Bot for each specific task
• Build for various feed formats, download mechanisms, augmenting, sanitizing, normalizing, reporting
• Based on 6 CERT-FI and 2 CERT-EE generations of abuse handling automata
• **Fully automatic**
ABUSEHELPER BENEFITS

• Handle more Abuse with less effort:
  • With AbuseHelper you are able to consume more information sources than ever!

• Stay up to date with newest feeds:
  • New Abuse Feeds pop up on monthly basis. Some of them are specializing on latest threats, which you want to be aware of. In typical case you have incorporated new feed to your AbuseHelper within a week from discovery.

• Save time & effort:
  • Automate mundane tasks, such as abuse & incident data collection and reporting. Skip the bootstrapping time needed to build your own solution from the ground-up.

• Modularity & extensibility:
  • Bring together information from sources with wildly varying qualities (e.g. streaming real time data, daily mail reports, periodically polled HTTP resources, different data formats).

• Robustness & scalability:
  • With its botnet inspired architecture AbuseHelper is an extremely robust and scalable solution.

• Sharing & collaboration:
  • Benefit from the know-how of other similar actors, share yours to benefit them.

• Open source for a closed community:
  • Scalable, robust and actively developed open core, while still allowing non-publicly available extensions.
VSROOM

• Taps into stream of events and provides real-time visualizations
• Map based views, classification views, text based views.
• Benefits:
  • See up-to-date situation from your perspective:
    • National: how different nations are coping with abuse
    • Organizational: how large enterprises suborganizations and subcontractors are doing.
HOW IS THIS DIFFERENT FROM IDS/IPS?

The world watches you. AbuseHelper helps you to stay on top of what others know about our security incidents.

Based on real incidents and known badness, less false positives than IDS.

Sensor based solutions are expensive and they take long time to deploy. In national context, often plagued with legal and organizational.

Others do the most work-intensive part - staying technically up to date with latest threats.

- Botnets
- Dropsites
- Scan source/target
- Malware
- Spamming
- Phishing
- Your critical assets
HOW IS THIS DIFFERENT FROM IDS/IPS?

The world watches you. AbuseHelper helps you to stay on top of what others know about our security incidents.

Based on real incidents and known badness, less false positives than IDS.

Sensor based solutions are expensive and they take long time to deploy. In national context, often plagued with legal and organizational issues.

Others do the most work-intensive part - staying technically up to date with latest threats.

Abuse.ch

Malware

Spamhaus

ShadowServer

Commercial Abuse Feeders

SecretOrgs

Your critical assets

IDS

FW

Spamming

Phishing

Botnets

Dropsites

Scan source/target

Malware

Your critical assets

IDS

FW

Spamming

Phishing

Botnets

Dropsites

Scan source/target

Malware
• Reports are fully tailorable
• For example add inter-organizational details
• Report timing (real time, periodic), document templates, distribution methods - all tailorable as well
Maturity

0 - Abuse

1 - Pilot capability

2 - Production automation

3 - Situational awareness and collaboration

4 - Private sensors

Activity

Manual or no abuse handling

Critical assets, feeds and constituencies mapped and pilot setup implemented.

Feeds processed and actionable reports produced

Trends and situation visualized, timely collaboration enabled

Private sensors confirm and extend 3rd party reports

Impact

Loss

Benefit demonstrated and work scoped

Dirt removed from your network more efficiently

Decision makers and experts collaborate on exact intelligence

Incidents confirmed, coverage improved

Monday, November 7, 2011
ROADMAP IN PRACTICE

• Pilot (maturity level 1)
  • sufficient integration to your environment to present tangible results
  • with CSIRT/CERT/Security team and decision makers
• Production (maturity levels 2-4)
  • full integration,
  • 24/7 operation,
  • reaching all stakeholders
• Typically done in 4 sprints