CERT-FI Autoreporter

2011-12-14
Mini MetriCon 5.5

Jussi Eronen
Information Security Adviser
CERT-FI
Finnish Communications Regulatory Authority
Agenda

Background

The Autoreporter Project
Background
Mostly harmless?
The duties of the Finnish Communications Regulatory Authority are:

1) to supervise compliance with this Act and any provisions issued under it, unless otherwise provided in section 32;

2) to collect information on violations of and threats to information security in respect of network services, communications services and value added services, and on significant faults and disruptions in such services;

3) to investigate violations of and threats to information security in respect of network services, communications services and value added services, and significant faults and disruptions in such services; and

4) publicize information security matters.

Act on the Protection of Privacy in Electronic Communications (516/2004) section 31
By Finnish network services we mean:

- Autonomous Systems in Finnish soil, operated or owned by Finnish organisations or otherwise important to Finnish interests.
- Domains under .FI and .AX DNS root
- Public telephone networks with +358 prefix
- Other networks operated or owned by Finnish organisations

By Finnish network services we mean:

- Services located in Finnish networks
- Services operated or owned by Finnish organisations

Other assets we consider Finnish

- Finnish Credit Card Prefixes
- Bank Account Numbers
- Finnish Brand Names
Special about the Finnish model.

Applies to Telecommunications Operators only:

Mandatory reporting of Information Security Incidents as well as Major Faults:
- affecting the networks
- affecting users of the networks
- affecting service provider’s ability to operate it’s networks
Some Actions by FICORA

- Regulation for service providers
  - Basic security of facilities and processes
  - Mandating BCP:s
  - Block outgoing spam
- Mandatory reporting for ISP:s
- Establishing CERT-FI
  - Key point in establishment was lower the reporting threshold
Problems

- Regulation for service providers - problem: now we're being the good neighbor, but still get attacked
- Mandatory reporting - problem: Most incidents out of scope
- Establishing CERT-FI - problem: No ownership/visibility of networks, incident statistics reflect available workforce and goodness of abuse handling script framework
Some Open Questions

• How many incidents affect Finnish networks?

• Is “x incidents per year” good or bad?
  – Or: How do we compare to our neighbors?

• Are we doing the right things?

• Are things better or worse than last year?
How do we compare to our neighbors?
The Autoreporter Project
How many incidents are there?

- Since 2006, CERT-FI adopted an automated system to systematically collect Incident Reports (mostly malware infections) from various monitoring projects around the world
- **That opened our eyes!!**
- We probably still only see the tip of the iceberg..

In 2006, we enhanced automation
Daily reports

The daily reports are sent as emails with predefined and agreed-upon subjects. All reports are signed.

The reported incidents are listed in the body of the email.

- The same information is also included as an attached XML-file (IODEF-format)

From: cert-fi-autoreporter
Subject: [FICORA #123456] Daily abuse report for your network

CERT-FI has received information regarding systems on your network which may have security problems. All timestamps are according to UTC. The format is as follows:

<table>
<thead>
<tr>
<th>ASN</th>
<th>IP</th>
<th>TIMESTAMP (UTC)</th>
<th>PTR/DNAME</th>
<th>CC</th>
<th>TYPE</th>
<th>INFO</th>
</tr>
</thead>
<tbody>
<tr>
<td>90000</td>
<td>1.2.3.4</td>
<td>2008-10-01 19:00:00</td>
<td>1-2-3-4.adsl.fi</td>
<td>FI</td>
<td>Bot</td>
<td>123456</td>
</tr>
<tr>
<td>90000</td>
<td>2.3.4.5</td>
<td>2008-10-01 06:00:00</td>
<td></td>
<td>FI</td>
<td>Ddos</td>
<td>123456</td>
</tr>
<tr>
<td>90000</td>
<td>3.4.5.6</td>
<td>2008-10-01 09:00:00</td>
<td>3-4-5-6.adsl.fi</td>
<td>FI</td>
<td>Bot</td>
<td>123456</td>
</tr>
</tbody>
</table>

If more information is needed, please contact CERT-FI.
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 space/netblocks
  - Finding right contacts and their contact preferences
  - Customer expectation management
- Reporting
  - Statistics, trends, chronic cases
- Responding
Autoreporter: Sources (in practice)

• We receive the most useful abuse information from trusted 3rd parties, not-for profit “internet superheroes” that perform
  • Honeypots/nets
  • Sinkholing
  • Malware analysis
  • Spamtraps
  • Malicious URL/phishing/defacement tracking
  • Investigations
  • …
Web site vuln, attack or incident feeds

- 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.

- abusechf 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=
- cleanmxp http://support.clean-mx.de/clean-mx/xmlphishing?response=alive&format=csv&fields=url,ip,domain&domain=
Working with Data

- Incoming feeds wide and varied in format, formalism and transports
- Availability (downtime, missed reports, etc)
- Integrity of the information
- Bugs
- Update frequency: near-real-time, hourly, daily...
- Report de-duplication (overlapping refreshes)
- Timespan: last n days, specific date
- Provided details
- Terminology
- Formatting (csv, xml, etc)
- Transports (HTTP, SMTP, IRC, etc)
Finnish Victims to Data Breach Incidents
Open Questions Revisited

- What are we not seeing?
- What should I prepare for?
- Am I targeted or just collateral damage?
- Can I trust the data?
Statistics

Type of Incident
2007-2010

- Bot: 167,265
- Expected Trabot: 32,438
- 95: 1,313
- Other: 288
- None: 161
Autoreporter Statistics

Precised type of Incident
2010

Statistics
Incidents per half year (H1/2006=100), Number of broadband subscriptions
Autoreporter: Challenges

- 5 generations of CERT-FI Autoreporter and 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
- Progressing from this point might require more of a community effort → enter Abusehelper
The goal of the Abusehelper project is to provide common understanding, framework and tools for handling abuse.

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.

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.
1. Many (if not most) incidents are detected by outside parties
   - Any Infrastructure/OSINT monitoring will help in finding badness in your network. The more data you grab, the more incidents you will find

1. Working with incident data is difficult
2. Finding working incident reporting contacts is challenging
3. Collaborative use of automation not fully exploited in incident reporting
4. Customers want reports on how they are doing compared to their peers
5. Incident response process maturity
   - All by hand
   - Ad hoc (in-house) scripts
   - Hands on automata (abuse specific ticketing system)
   - Hands off automata
CERT-FI alerts and advisories are available in Finnish via:

- E-mail
- SMS (subscription fees apply)
- web pages
- RSS feed
- TELETEXT page 848 (YLE)