Instant Messaging Parental Control

Massimo Bernaschi, IAC-CNR
Antonio Grillo, DISP
Alessandro Lentini, DISP
Gianluigi Me, DISP

Virtual Parent

Gianluigi Me, Ph.D.
me@disp.uniroma2.it

Instant Messaging Parental Control

http://isgm.iac.cnr.it
http://www.virtualparent.eu
Project’s Partner

Consiglio Nazionale delle Ricerche

Istituto per le Applicazioni del Calcolo "Natale Piccioni"

IAC Cnr (http://www.iac.cnr.it)

ECPAT Italia (http://www.ecpat.it)

ECPAT Italia ONLUS
End Child Prostitution, Pornography and Trafficking

Da schiavi a bambini

LAND (http://www.land.it)
**Key Terms**

- **Parental Control**: a software/service used to access the Internet, that allows a parent to monitor or limit what a child can see or do; and/or time-limit restricted activities.

- **Instant Messaging Control**: software used to monitor or limit the use of chats (any kind of).
Purpose

System goals concern with:

- **Execute** on the target machine in an hidden way
- **Collect** the raw instant messaging network data
- **Reconstruct and organize** the raw data applying the instant messaging protocol
- **Identify** potential suspicious conditions
- **Present** the rebuilt data in a smart way
- **Allow** an interactive consultation of the rebuilt data
- **Allow** a local/remote consultation of the rebuilt data
# Competitors analysis

<table>
<thead>
<tr>
<th>Rank</th>
<th>Software</th>
<th>Type</th>
<th>IM Control</th>
<th>Efficacy</th>
<th>Vote</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Windows Vista Parental Control</td>
<td>OS Module</td>
<td>No</td>
<td>80%</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>Optenet</td>
<td>Application</td>
<td>Yes</td>
<td>62%</td>
<td>7.5</td>
</tr>
<tr>
<td>3</td>
<td>Windows Live One Care Family Safety</td>
<td>Application Service</td>
<td>Yes</td>
<td>74%</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>K9 Web Protection</td>
<td>Application</td>
<td>No</td>
<td>62%</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>Net Nanny</td>
<td>Application</td>
<td>Yes</td>
<td>58%</td>
<td>6.5</td>
</tr>
<tr>
<td>6</td>
<td>Stopalporno.net</td>
<td>ISP Service</td>
<td>No</td>
<td>73%</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>ZOT</td>
<td>Application</td>
<td>No</td>
<td>60%</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>Davide.it</td>
<td>ISP Service</td>
<td>No</td>
<td>58%</td>
<td>6</td>
</tr>
<tr>
<td>9</td>
<td>Norton Internet Security 2008</td>
<td>Application</td>
<td>No</td>
<td>44%</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>KEYfamily</td>
<td>Application</td>
<td>Yes</td>
<td>n.d.%</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>Naomi</td>
<td>Application</td>
<td>No</td>
<td>n.d.%</td>
<td>4</td>
</tr>
</tbody>
</table>

Source: [www.elis.org](http://www.elis.org) (data test: 2008-08-12)
### Competitors analysis

<table>
<thead>
<tr>
<th>Type of control</th>
<th>Windows Vista compatibility</th>
<th>Antivirus alert</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>VirtualParent</td>
<td>Proactive</td>
<td>Medium</td>
<td>Yes</td>
</tr>
<tr>
<td>IM Lock Home ED</td>
<td>TBC*</td>
<td>None</td>
<td>No</td>
</tr>
<tr>
<td>KEYfamily</td>
<td>TBC*</td>
<td>High</td>
<td>No</td>
</tr>
<tr>
<td>Optenet</td>
<td>TBC*</td>
<td>High</td>
<td>No</td>
</tr>
<tr>
<td>Net Nanny</td>
<td>TBC*</td>
<td>High</td>
<td>No</td>
</tr>
<tr>
<td>Skypito</td>
<td>Preventive</td>
<td>Low</td>
<td>No</td>
</tr>
<tr>
<td>Windows Live One Care Family Safety</td>
<td>Preventive</td>
<td>High</td>
<td>No</td>
</tr>
</tbody>
</table>

*: Total block of protocol based on filter rule applied over the port number.
## Competitors analysis

<table>
<thead>
<tr>
<th>Products Features</th>
<th>Virtual Parent</th>
<th>MSN Chat Monitor</th>
<th>MSN Checker Sniffer</th>
<th>MSN Spy Monitor</th>
<th>MSN Track Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Textual Message</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Emoticons</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>File transfer</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Contact Details</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Contact List</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Conversation Reconstruction</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Remote data Consultation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>History</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Search Function</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Statistics</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Cost</td>
<td>$69.95</td>
<td>$29.99</td>
<td>$39.99</td>
<td>$49.85</td>
<td></td>
</tr>
</tbody>
</table>
# Competitors analysis

<table>
<thead>
<tr>
<th>Products Features</th>
<th>Virtual Parent</th>
<th>Golden Eye</th>
<th>Colasoft MSN Monitor</th>
<th>EtherBoss MSN Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Textual Message</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Emoticons</td>
<td>Yes</td>
<td>Yes*</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>File transfer</td>
<td>Yes</td>
<td>Yes*</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Contact Details</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Contact List</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Conversation Reconstruction</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Remote data Consultation</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>History</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Search Function</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Statistics</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cost</td>
<td></td>
<td>$29.95</td>
<td>$29.95-$59.95</td>
<td>$99</td>
</tr>
</tbody>
</table>

*: Timed-Screenshot configurable behaviour.
**System Overview**

Virtual Parent is a **distributed** system.

**4+2 Module Architecture:**
- 4 main modules
- 2 support modules

**Main Modules:**
- [L] Launcher Module
- [C] Capture Module
- [A] Analysis Module
- [P] Presentation Module

**Support Modules:**
- [U] Upload Module
- [D] Download Module

Date: 23/10/2008
System Overview

Remote Consultation Scenario:

Target PC

MSN Community

Remote PC

Market Available Grid Computing

23/10/2008
System Information Flow

MSN Application

Raw Network Data (PCAP)

Instant Messaging Data (PCAP)

Account History (XML)

Account Histories (XML)

Account History (MXML)

Remote Repository

Remote Scenario
Launcher Module Features

- **C#** windowed application.
- **Provide** the configuration form for the app’s modules.
- **Monitor** the status (alive/dead) of the app’s modules.
- **Resume** the modules that appear to be dead.
- **Set** the “Start on boot” feature into the OS Registry.
Capture Module Features

- **C#** windowed application.
- **Capture** TCP/UDP traffic from all the NIC installed on the target machine (based on WinPcap library).
- **Filter** TCP/UDP traffic; the filter rules are based on the ports effectively opened by the instant messaging application (not only tcp/udp port 1863!).
- **Trace** chat messaging windows opened during the capture session.
- **Dynamically modify** capture session timelength with respect to the real instant messaging application usage.
Analysis Module Features

- **C#** windowed application.
- **Organize** TCP traffic detecting out of order, lost, and repeated packets.
- **Recover** all existent files for the account (messengerCache, objectStore)
- **Rebuild** all the chat information (account information, chat-text, emoticons, file transfers, ...)
- **Recognize** the MIME-Type of many file formats.
- **Create/Update** an account library (XML Based) for each account detected.
Upload Module Features

- C# windowed application.
- **Mantain** an updated account library on the remote repository.
- **Upload** periodically the account library updated by the analysis module.
- **Upload** only the new/modified files for reducing the target PC network overhead.
All the local modules can be hidden from the screen.

All the local modules can be restored with a configurable hotkey.

All the local modules show their operative state with a simple graphical indicator.
Download Module Features

- **Adobe Flex** module of the Presentation application.
- **Maintain** an updated account library on the local site.
- **Retrieve** the list of the account libraries relative to a specific user.
- **Obtain** only the new/modified files for reducing the remote PC network overhead.
Download Module Screenshots

Local Account Consultation

Remote Account Download
Presentation Module Features

- **Adobe Flex** application (MXML for the graphic with AS3-logic).
- **Access** to both local and downloaded library.
- **Consult** the library with a usable/high-hyperlinked interface.
- **Alert** the user for suspicious conditions identified by the analysis module (anonymous proxy file transfers, new contacts, ...).
- **Allow** to mark contacts for monitoring their activity (new conversations/new file transfers).
- **Allow** to mark/tag conversation for remind.
Presentation Module Screenshots

Interesting Contacts

Sorting/filtering tools
Presentation Module Screenshots

All Contacts

Contacts sorting options
Presentation Module Screenshots

Contacts filtering options

Contacts sorting options

Search Results

Contacts Card
Presentation Module Screenshots

Contact last information

Contact alert box

Contact edit notes

Contact current notes
Presentation Module Screenshots

Date-tree view (e.g. the conversations)

<table>
<thead>
<tr>
<th>Date</th>
<th>Durata</th>
<th>Messaggi</th>
<th>File Trasmessi</th>
</tr>
</thead>
<tbody>
<tr>
<td>13/11/12</td>
<td>65998</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>13/11/12</td>
<td>40000</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>13/11/12</td>
<td>10000</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>13/11/12</td>
<td>10000</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

Example:
- amico1@tiscali.it
- amico2@tiscali.it
- amico3@outlook.com
- amico4@hotmail.com
Presentation Module Screenshots

Datagrid view (e.g. the file transfers)

Sorting/filtering tools
Presentation Module Screenshots

Graph view (e.g. the file transfers type)
**Presentation Module Screenshots**

- **Statistics Summary**
- **Statistics details** (e.g. the file transfers)
- **Other Info:**
  - Conversations statistics
  - Contacts statistics
  - File transfers statistics
  - Notes history
  - Alert history
- **Sorting/filtering tools**
Q&A