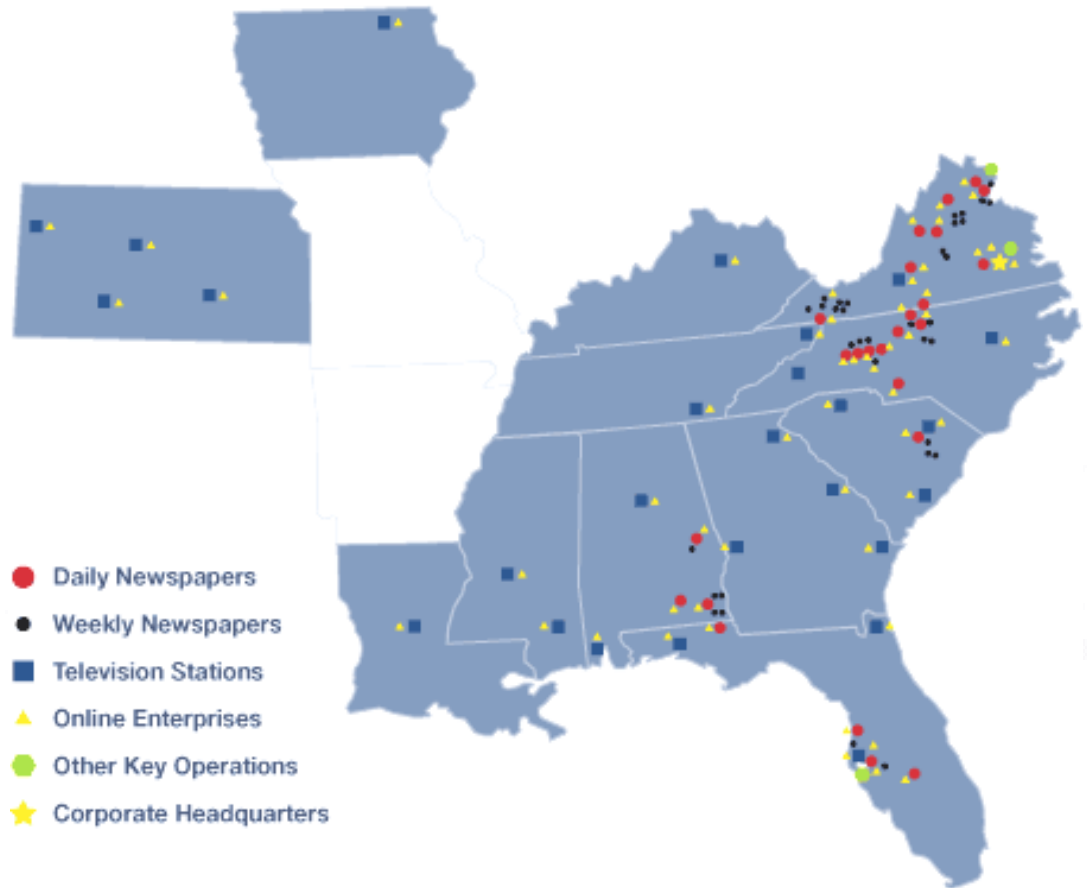


Instant Messaging at  
Media General  
or

**The Case of the  
Missing Messages**

# Background Check

## Media General



## The Setting

"Only software approved by Media General Information Technology Group (MGITG) or individually approved by MGITG, may be used on Company owned computers. Software is not to be loaded, copied, or removed from Company computers without approval from your location's Information Technology (IT) Department. Requests for using non-standard or specialized software must be coordinated with your Department Head for consideration and approval by MGITG."

## The Trouble Starts

- Jan. 2001, Media General formed the Interactive Media Division (IMD) to separate the business of our web sites from our TV stations and newspapers.
- The Division President came to Media General from another media company where he was a big user of Instant Messaging, specifically AOL's AIM client.

## The Plot Thickens

- Division President wants all his employees to be connected in real time in order to better react to news events and sales opportunities.
- He goes to the CIO and asks for AIM to be added to the list of approved software for all IMD employees.
- The CIO grants permission.

## Growing concern

### IM Worms

- W32.Choke (7/2001)
- W95.SoFunny.Worm (7/2001)
- W32.Goner.A (12/2001)
- W32.Led (1/2002)
- W32.Seesix.Worm (5/2002)

### IM Trojans

- AIMaster (10/2001)
- Trojan.msgmess (8/2002)
- IM PWSteal (4/2002)
- KrAIMer (5/2002)

## Concern Still Growing

- "ICQ logs spark corporate nightmare" CNet 3/15/2001
- "Social Engineering Attacks via IRC and Instant Messaging" CERT 3/19/2002
- "Multiple Vulnerabilities in Yahoo! Messenger" CERT 6/5/2002

## Panic Sets In

- A couple of complaints come through HR about employees losing productivity due to time spent on IM.
- 3<sup>rd</sup> hand stories of instances of application logins and passwords being sent via IM.
- In May 2003, used Snort filters to grab 1 day's worth of AIM traffic leaving our network to a handful of known AOL IM proxies. Found 282 messages. None appeared to be business related.

## The Crime Scene

- 05/02-00:16:31.360466 <[www.freeheaven.com](http://www.freeheaven.com)
- 05/02-03:20:49.038241 well..I would start by kneeling ... (*edited for content*)
- 05/02-11:32:50.901195 Me need nachos
- 05/02-16:31:35.870790 dude which Safeway are we meeting at....
- 05/02-16:59:07.072300 ETA for first beer open is 10:00

# Suspect Profiling

## Primary Goals

- Secure internal messages
- Block attachments/viruses
- Limit access to authorized users

## Preferences

- Stay with AIM client
- Implementation transparent to users

## The Investigation

- AOL at Work, Yahoo Business Messenger, and Microsoft Live Communication Server all considered immature products at the time.
- CIO not comfortable with open source alternatives like Jabber or proprietary closed systems like WiredRed.
- Most options required moving off the AIM client "standard" and were not compatible with the public IM networks.

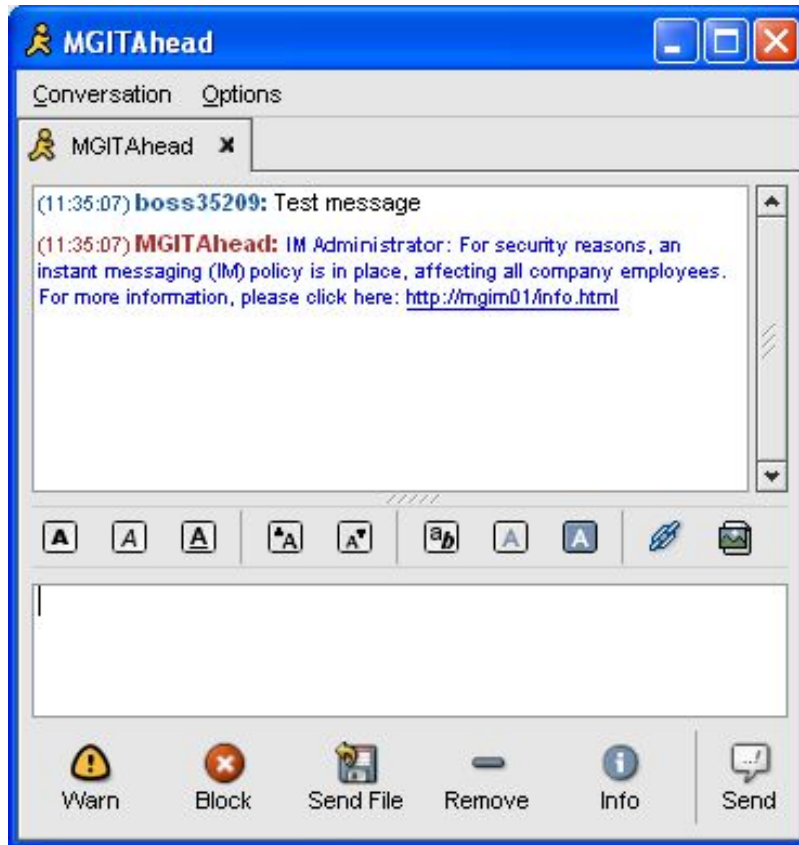
## The Prime Suspect

- Discovered IMLogic's IM Manager product mid 2003
  - Worked with Yahoo, AIM, and MSN out of the box, plus option to integrate with Live Communication Server down the road if we went that route.
  - Seemed to satisfy all our primary goals.

## The Interrogation

- Began a "stealth" test in fall 2003.
- Completely transparent to users (*watch out for HR issues*).
- Gave us a clearer picture of how much IM was really being used (*both less and more than we thought*).
- Made us consider how the IM was to be treated in terms of auditing, document retention, etc. (*same as email*)

# The Evidence



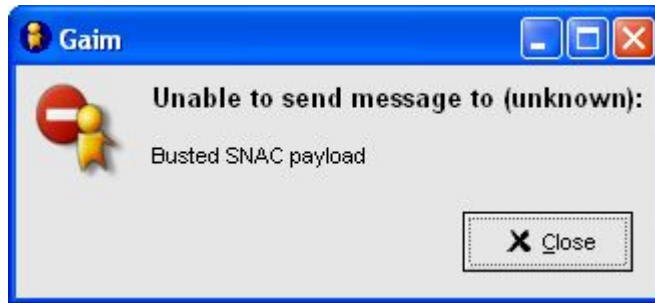
Results in client window for an unauthorized internal IM user trying to send a message.

## More Evidence



Results in client window for someone outside trying to IM an unauthorized MG user.

# The Smoking Gun



Results when  
trying to  
transfer a  
file.

**Case Closed**

SEARCHED  
SERIALIZED  
INDEXED  
MAY 19 1964  
FBI - MEMPHIS  
385111

## Your Investigation

- New IM threats emerging all the time.
- There is more of a threat today from IM than when we looked in 2003.
- The Enterprise IM Market is broader and more mature than in 2003.
- Look at your user base, try to classify their activity, and evaluate products based on your specific needs.

# Your Profiling

## Recommended basic requirements:

- Secure internal messages.
- Block attachments/viruses.
- Limit access to authorized users.

Questions?

