Distribution Information

This presentation contains sensitive information related to procedures in use at Motorola. You may use portions within your own Information Security organization. You may not otherwise distribute this presentation in part or in whole without written permission from Motorola.
Why Monitor?

Why do we need to monitor?

• Company policy for computer use
  – What is appropriate?
    • Business related activities:
      – Support Company business goals and objectives
    • Non-business related activities:
      – as approved by management
      – negligible, not interfering with work responsibilities and required business activities
      – Examples: volunteerism, continuing education, professional development
Why do we need to monitor?

• Company policy for computer use
  – What is NOT appropriate?
    • Disclosure of confidential or sensitive data owned by
      or entrusted to Motorola to unauthorized recipients
    • Misuse of trademarks or service marks of Motorola
      or other organizations
    • Misuse of copyrighted material or other violation of
      copyrights held by Motorola or others

• Communicating in ways that disparage other companies’
  products or services (excluding objective reports of
  substantiated fact with limited internal distribution)
• Communicating information that could be perceived as
  official Motorola positions or endorsements without
  proper management approval
• Communicating using confrontational or improper
  language or using statements that are defamatory
Why do we need to monitor?

• Company policy for computer use
  – What is NOT appropriate?
    • Attempting to break into any computer (‘cracking’) without proper authorization, whether within Motorola or another organization
    • Accessing confidential information on computer resources without authorization
    • Promoting political or religious positions
    • Operating a personal business, or use for personal gain

• Creating, storing, or transmitting illegal or otherwise offensive material
• Participating in any activity which could be interpreted as harassment
• Originating or distributing chain letters
• Misrepresenting an individual’s identity or the source of communications or data
Why do we need to monitor?

• Company policy for computer use
  – What is NOT appropriate?
    • Participating or engaging in activities that violate the law, the Motorola Code of Conduct, Key Beliefs, or any Motorola policies or standards, including Human Resources, financial or security
    • Soliciting, except as provided for in the Human Resources publication “Working Together”

• Export or import of any governmentally-controlled technical data or software (such as software encryption) to or from unauthorized locations or persons without appropriate licenses or permits
Why do we need to monitor?

• Network traffic
  – Before and after “normal” hours
  – Lunch time
  – Global corporation: there is ALWAYS someone trying to be productive

• Incident response (examples)
  – Insider information posted on Yahoo message boards
  – Stalker traced back to a pager number assigned to the Corporation
  – RFP competitive results and analysis disclosed to losing bidder
  – Hacking tools, software from warez sites found running on internal network
How It All Began...

- Posting on Yahoo message board disclosed confidential company information
- Legal department enlisted our help to find out if the posting came from within our network
- Network Security Team’s RealSecure evaluation + a few Perl scripts = ad hoc system
What We Did and Did Not Find

- Did NOT find evidence that the posting came from inside
- DID find URLs for pornographic and other inappropriate sites
- Did NOT find managers who approved this inappropriate use
- DID find outraged managers ready to deal with our findings

The “System” Today
The “System” Today

- 1998 one facility
- 1999 positioned server to pick up 3 facilities
- RealSecure logs all outgoing requests to web gateway
- Weekly automated job searches through the week’s logs for activity to report

The “System” Today

- Weekly report of high-volume IP addresses (machines) - sample headings:

  Searching pattern: . in log file: ...
  Total HTTP requests: 8280520, total hits: 8280520, percentage: 100%

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Hits</th>
<th>Start-End Time Stamps</th>
</tr>
</thead>
<tbody>
<tr>
<td>------------</td>
<td>------</td>
<td>-----------------------</td>
</tr>
</tbody>
</table>
The “System” Today

• Weekly report of keyword hits on IP addresses (machines) using keywords from such categories as:
  – sex/pornography
  – racism
  – hacking/cracking
  – abuse of drugs
  – identity masking
  – etc….

• Raw log file for each IP address in the “keyword” report
• Summary file for each address showing times of activity and counts per web server (15-minute rule)
• Counts of “hits” are added to a cumulative spreadsheet, sorted by descending cumulative total
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Server/URL</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tue Sep 07</td>
<td>08:36:28</td>
<td>mtk.hotmail.msn.com</td>
<td>email</td>
</tr>
<tr>
<td></td>
<td></td>
<td>encrypted/unreadable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.cscug.org">www.cscug.org</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>209.1.112.251</td>
<td>email</td>
</tr>
<tr>
<td></td>
<td></td>
<td>archive.msn.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcl.tl.horiz.net</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.egreetings.com">www.egreetings.com</a></td>
<td>greeting cards</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.hotmail.com">www.hotmail.com</a></td>
<td>email</td>
</tr>
<tr>
<td>Tue Sep 07</td>
<td>11:17:50</td>
<td><a href="http://www.mbusa.net">www.mbusa.net</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ads16.focalink.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.picosearch.com">www.picosearch.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>209.1.112.251</td>
<td>email</td>
</tr>
<tr>
<td></td>
<td></td>
<td>admedia.xoom.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.xoom.com">www.xoom.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>classifieds.yahoo.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>gserv.zdnet.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>personal.lycos.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ad.doubleclick.net</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.angelfire.com">www.angelfire.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.egreetings.com">www.egreetings.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.hisoft.demon.co.uk">www.hisoft.demon.co.uk</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>encrypted/unreadable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>m.doubleclick.net</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>msg.yahoo.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.snap.com">www.snap.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.opera.com">www.opera.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a/1996.g.akameotech.net</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>view.avenues.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ads.msn.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>services.xoom.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>members.ad.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>www1.bluemountain.com</td>
<td></td>
</tr>
</tbody>
</table>

**Total:** 243
The “System” Today

• False hits analysis - samples:
  – abcnews.go.com (“teenyicon.gif”)
  – accommodationsexpress.com
  – www.al-anon.alateen.org
  – www.certificationshack.com
  – www.dallasexaminer.com
  – www.flowersexpress.com
  – www.jelloboy.com (“Nude teen stick figures”)

• False hits analysis - even more samples:
  – www.JoesCrabShack.com
  – www.radioshack.com
  – www.securitiesexam.com
  – www.sunglassexpress.com
  – www.texasesxes.org
  – www.uswest.net
  – xxx.lanl.gov (my favorite)
The “System” Today

- Generate weekly summary reports and charts
  - Cover page, summary and status of open cases
  - Spreadsheets of historical data by IP address
  - Charts

Inappropriate Hits

<table>
<thead>
<tr>
<th>Report Date</th>
<th>Plant 1</th>
<th>Plant 2</th>
<th>Plant 3</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10/18/99

Patti.Lawrence@Motorola.com
The "System" Today

- Cases opened for highest hitters, work our way down the list
- Find the computer
- Identify the user (whenever possible)
- Document the evidence using fill-in-the-blank template
On [date], weekly web traffic logs revealed the computer connected at IP address {IP address} had been to pornographic sites. The currently associated machine ID at this IP address is {machine ID}, assigned to {name or “multiple users” as appropriate}.

According to the web traffic log, at least one user on the machine connected at {IP address} has accessed pornographic sites on the dates and times reported in attached web traffic summaries.

The NT security log was reviewed for the dates and times in question. The security audit had not been turned on so there was no data in the security log. There are {number of user accounts} users on the computer, so to determine who was going to pornographic web sites we searched the cache and Netscape history files of all the users who had Netscape profiles on the machine.

The NT security log was reviewed for the dates and times in question. The ID shown logged in was {userID}. This ID belongs to {name}.

This machine is running Windows, is a portable computer, and has no security installed on it. It was in the docking station in {name}’s office, and the only Netscape profile on the machine was for {full email address for the user}. 
We found that the [Netscape and/or Internet Explorer] user profile associated with the following person had been used to access pornographic sites:

Upon viewing the user’s [Netscape and/or Internet Explorer] historical files, we found the following evidence the user had been to pornographic sites:

Upon viewing the user’s [Netscape and/or Internet Explorer] historical files, we found no evidence this user had been to pornographic sites, indicating web activity had been cleared from the machine some time before we went to the machine for investigation on {date}.

The hard drive of the computer contained {number of} files consuming {amount of} disk space with pornographic data with file dates ranging from {start date/time} to {end date/time}.

The user’s network home directory contained {number of} files consuming {amount of} disk space with pornographic data with file dates ranging from {start date/time} to {end date/time}.

The computer contained [executable program name] indicating the likelihood that a CD-ROM burner, jaz drive, zip drive, or other mass storage device was in use on the computer. We found [mass storage device name(s)] [in the office / attached to the machine / installed internally in the machine].

Network Security, ITSS
The “System” Today

- Investigation helps
  - Administrative account
  - Network access to machine
  - Security log from machine/ntlast.exe
  - Directory listings from machine
  - Web traffic logs and summaries
  - Web browser files and other files on machine
  - Files on user’s network drive

Netscape Cookies

www.kiss.com FALSE / FALSE 126232800 KissSearch
  PROJECTNAME=8%2F19%2F99+10%3A53%3A13+AM&PROFILEDRINK
S=&PROFILECOUNTRY=1004&PROFILERELIGION=&PROFILESEX=1&PROFILE
AGE1=&PROFILEAGE2=&PROFILEHEIGHT1=&PROFILEHEIGHT2=&PROFILEHEIGHT3=&
PROFILEHEIGHT4=&PROFILEHEIGHT5=&PROFILEHEIGHT6=&PROFILEHEIGHT7=
&PROFILEHEIGHT8=&PROFILEHEIGHT9=&PROFILEHEIGHT10=&PROFILEHE
IGHT11=&PROFILEHEIGHT12=&PROFILEHEIGHT13=&PROFILEHEIGHT14=&
PROFILEHEIGHT15=&PROFILEHEIGHT16=&PROFILEHEIGHT17=&PROFILEHE
IGHT18=&PROFILEHEIGHT19=&PROFILEHEIGHT20=
DatingClub.Com FALSE / FALSE 1249926908 DCVISIT COUNT=1
  www.kiss.com FALSE / FALSE 1293756000 WEBTRENDS_ID (IP deleted)
  .imgis.com TRUE / FALSE 1091543994 JEB2
  59f8461dd1ced1e19e3b9e8a262cfe3e15a18
  www.loveme.com TRUE / FALSE 1924992163 STRING singlesites
  carprices.com TRUE / FALSE 965860046 PARTNER SINGLE
  carprices.com TRUE / FALSE 96586046 RETURN VISITOR
  al.carprices.com FALSE / FALSE 965952104 PARTNER SINGLE
  .www-one-and-only.com FALSE / FALSE 965951522 usergroup 0
  .jobs.com TRUE / FALSE 1293699999 RMID 888062dd37b1b3c0
  snap.com TRUE / FALSE 946647999 u:version_0_0 home
  .amazon.com TRUE / FALSE 946647999 u:vid_0_0 04a891f8
  www.amcity.com/FALSE / FALSE 1563114549 Apache cache-engine-
  03.ch.aia.net:3145493454548283
  personals.yahoo.com TRUE / FALSE 949336000 L
  .amazon.com TRUE / FALSE 934963200 session-id-time 934963200
  .amazon.com TRUE / FALSE 934963200 session-id 002-9419992-6572637
  .amazon.com TRUE / FALSE 2082957304 ubid-main 002-4511810-3623549
  10/18/99 Patti.Lawrence@Motorola.com
user_pref("browser.bookmark_columns_win", "v1 1:10000 2:2996 4:1999 3:1999");
user_pref("browser.bookmark_window_rect", "132,132,929,729");
user_pref("browser.cache.disk_cache_size", 15000);
user_pref("browser.cache.memory_cache_size", 15000);
user_pref("browser.download_directory", "D:\(Download\)");
user_pref("browser.linkExpiration", 120);
user_pref("browser.print.background", true);
user_pref("browser.startup.homepage", "http://sstg.geg.mot.com");
user_pref("browser.startup.homepage_override", false);
user_pref("browserарт_history.URL_1", "www.yam.ch");
user_pref("browserарт_history.URL_10", "www.msnbc.com");
user_pref("browserарт_history.URL_11", "www.egreetings.com");
user_pref("browserарт_history.URL_12", "g:\apps\cidm\fa_sys\f3fillw\f3fillw2.exe");
user_pref("browserарт_history.URL_13", "g:\apps\cidm\fa_sys\f3fillw\f3fillw2.exe %1");
user_pref("browserарт_history.URL_14", "http://www.egreetings.com");
user_pref("browserарт_history.URL_15", "http://wms.geg.mot.com");
user_pref("browserарт_history.URL_16", "profiles.yahoo.com");
user_pref("browserарт_history.URL_17", "http://www.linuxjournal.com");
user_pref("browserарт_history.URL_18", "http://www.mfsoft.com");
user_pref("browserарт_history.URL_19", "www.arizonarepublic.com");
user_pref("browserарт_history.URL_20", "www.azrepublic.com");
user_pref("browserарт_history.URL_21", "www.uswest.com");
user_pref("browserарт_history.URL_22", "www.uswestdex.com");
user_pref("browserарт_history.URL_23", "http://www.uswest.com");
Developing Relationships

• Human Resource Management
  – Help set priorities
  – Deal with user and his/her management
  – Apply disciplinary measures
  – I never have to confront the users and usually could not identify them if I saw them

• Corporate Legal Department
  – Issues involving software licensing (freeware vs. shareware, etc.)
  – Sometimes initiate investigation request
  – Assist with decisions regarding evidence storage and retention, etc.
Developing Relationships

• Physical Security Department
  – Liaison with local, state, and federal law enforcement when required
  – Need to be informed if evidence suggests the possibility of bodily harm or destruction of property
  – Place cameras when a “public” machine does not indicate who was using it

• Law Enforcement
  – Notification of suspected illegal activity
    • Avoid changing anything on the machine (preservation of evidence)
    • Provide technical expertise in interpreting evidence (especially with local-level agencies)
Developing Relationships

- Network Architecture Team
  - Locate a machine when inaccessible over the network
  - Provide access to network services not normally required

Lessons Learned
Lessons Learned

• UNIX limitations
  – when trying to parse the data the Unix operating system (Solaris 2.6) can not handle a file size larger then 2GB. This required daily generation of a new log file and combining all at the end of the week
  – Tabling output in procedures resulted in over 40 files being open at a time

• RealSecure limitations
  – Version we are using has a memory leak, requiring us to start/stop process on an hourly basis to avoid loss of data
  – This is an older version of the software, and no longer being maintained
  – Newer versions don’t work with our processes
Lessons Learned

• Network limitations
  – We had to add two new network segments to support the Real Secure engine, which could not handle ATM.
  – We had to dual-homed the system to the monitored network and the "out of band" network used to pull the data off the system because the level of 2-way traffic caused network traffic problems (packet collisions)

Lessons Learned

• People issues
  – Habits and Impressions --> Increased activity
    • “They haven’t caught me yet”
    • “They aren’t downsizing right now”
  – Need to raise policy awareness level
    • orientation of new employees and contractors
    • reminders to existing employees and contractors
  – Manager reaction: “Now I understand why there was a productivity problem…”
Lessons Learned

• People issues
  – Creative surfing
  • “Glare screens”
  • Non-standard web browsers
  • Web sites that don’t hit keywords
  • Remote access surfing
  – If you can’t identify who is on the machine, try searching the log for web-based email!

Plans for the Future
Plans for the Future

- Evaluate, test, implement filtering software
- Continue monitoring
  - Some things will slip through filtering software
  - We expect continued historical-evidence requests outside scope of filtering software
- Automate everything that can be automated
- Analyze keywords for possible changes
- Cover more facilities/business units

Questions, Comments, Suggestions...