Table of content

1. Introduction

2. The infrastructure
   - ADMF Client and Infection GUI
   - Administration: ADMF
   - iProxy: NDP01/02
   - Radius Probe: RP01/02
   - Communication

3. Use Case Infection

4. System handling

5. Technical details

6. Incident handling
1. Introduction
Who we are
Delegates:

Nicolas Mayencourt  
Head of Dreamlab Technologies AG  
Member of the Board of Directors, ISECOM  
Member OWASP

Richard Sademach  
Head of Operations Dreamlab Technologies AG
2. The infrastructure
Overview & components
1. ADMF-Client & Infection GUI
2. ADMF
3. iProxy NDP01/02
4. Radius Probe RP01/02
1. ADMF Client and Infection GUI

- ADMF Client
- Graphical User Interface for managing Infections
- Configuring Infections
- Selection of Infection method
- Realtime status information
- Management of all components
1. ADMF Client → Infection GUI

Separate Training

Figure 1: Welcome Screen

Figure 2: License Information

Figure 3: Select Install Folder

Figure 4: Start Installation
1. ADMF Client and Infection GUI

**Hardware:**

- HP Compaq 8000 Elite Business PC
- 1 x Copper 10/100/1000

**Software:**

- FinFly ISP GUI
- XMPP Client
- Windows 7 Ultimate
2. ADMF - Central Administration Function

- Core component of the FinFly ISP infrastructure
- Realtime communication with all components → NDP, RP, FinFly Gui
- Configuration and initiation of infections on the ADMF
- Provisioning of the ADMF Client, iProxy and RP
- Realtime exchange of information and states → Targets coming online, being infected, etc
- RFC XMPP protocol used for secure and encrypted communication (TLS based)
2. ADMF - Central Administration Function

Hardware:

• HP DL380 G6
• 2x Intel(R) Xeon(R) CPU X5550 @ 2.67GHz
• Memory: 12 GB
• 3 x 146 GB SAS 2,5" (Raid 5)
• 4 x Copper 10/100/1000
• 1 x ILO (Integrated Lights Out)
• OS:Linux GNU (Debian 5.0), hardened by Dreamlab best practices

Software:

• ADMF → Administration function
• Ejabberd (XMPP server)
ADMF Configuration

Name: instance.conf
Path:

/home/iproxy/service/admf/etc/

```bash
# coding: utf-8
export VERBOSE=0

# ADMF
export ADMF_INSTANCE_DIR="${INSTANCE_DIR}"
export ADMF_DATA_DIR_PATH="${INSTANCE_DIR}/data"
export ADMF_DB_FILE_NAME="admf.db"

# ADMF manager
export ADMF_JID="admf@admf"
export ADMF_SECRET="xxyyzz"

# ADMF<>NDP
export NDP_JIDs="ndp01@admf ndp02@admf"

# ADMF<>GUI
export GUI_JID="gui@admf"

# ADMF<>RPROBEes
export RP_JIDs="rp01@admf rp02@admf"

# settings below this line are autogenerated by the provision script
# and should need no change unless you know what you are doing
export PYTHONPATH="/home/iproxy/code/home/iproxy/code/lib/python"
export EXEC_PATH="/home/iproxy/code/finfoy/admf.py"
export INSTANCE_NAME="admf"
```
3. NDP01 / NDP02 → iProxy

- Network data processing component
- Infections remotely activated/deactivated via the ADMF/ADMF GUI
- Provisioning of the actual target IP-Address from the RP via the ADMF
- Each NDP bridge is equipped with a carrier grade 10GB/s fiber bypass module
- In case of hardware or logical failures this module switches automatically to bypass-mode. Thus traffic will never be interrupted.
- Attention this is a highly dynamic bridge / fw environment: **DO NOT change any configuration manually**

The NDP has been specifically configured for this network. Any configuration change of the network i.e. protocolstacks, media, failover features etc must be tightly coordinated with Dreamlab. Not doing so most probably will lead to an unusable system.
3. NDP01 / NDP02 → iProxy

Hardware:

- HP DL380 G7
  2x Intel(R) Xeon(R) CPU X5650 @ 2.67GHz
- Memory: 12 GB
- 3 x 146 GB SAS 2,5" (Raid 5)
- 4 x Copper 10/100/1000
- 1 x Fiber Multimode Bypass NIC
- 1 x ILO (Integrated Lights Out)
- OS: Linux GNU (Debian 5.0), hardened by Dreamlab best practices

Software:

- NDP → Network Data Processor
- IPProxy → infection Proxy
- ADMF Client
### NDP Configuration

**Name:** instance.conf

**Path:**

```
/home/iproxy/service/ndp0[12]/etc/
```
4. RP01 / RP02 → Radius probe

- Realtime monitoring of the AAA processes: Targets coming online, receiving IP addresses, changing IP addresses, going offline
- Recording of the RADIUS authentications and accounting dialogues
- Being always up-to-date of the target IP address
- RP sends information to the ADMF
- The ADMF provisions the NDP's
- For statically configured IP addresses this is not needed

The target identification has been specifically configured for the local setup. Any configuration changes of the AAA / Radius setup must be tightly coordinated with Dreamlab. Failure to do so will most probably lead to an unusable system.
4. RP01 / RP02 → Radius probe

**Hardware:**

- HP DL380 G6
- 2x Intel(R) Xeon(R) CPU X5550 @ 2.67GHz
- Memory: 12 GB
- 3 x 146 GB SAS 2,5" (Raid 5)
- 4 x Copper 10/100/1000
- 1 x Intel quad port 1G copper
- 1 x ILO (Integrated Lights Out)
- OS: Linux GNU (Debian 5.0), hardened by Dreamlab best practices

**Software:**

- RP → Radius Probe
- ADMF Client
RP Configuration

Name: instance.conf

Path:

/home/iproxy/service/rp0[12]/etc/
The communication of all components always is initiated towards the ADMF:

- RP → ADMF
- NDP → ADMF
- Inf.SW → NDP → ADMF
- ADMF-Client → ADMF

Once the communication is established the information flow is bidirectional (red arrows).
## Communication: Traffic matrix

<table>
<thead>
<tr>
<th>from / to</th>
<th>ADMF</th>
<th>ADMF-GUI</th>
<th>NDP</th>
<th>RP</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMF</td>
<td>none</td>
<td>none</td>
<td>TCP 62200</td>
<td>TCP 62200</td>
</tr>
<tr>
<td>ADMF-GUI</td>
<td>TCP 62200  / TCP 7990 / TCP 443 / TCP 23</td>
<td>none</td>
<td>TCP 62200 / TCP 7990 / TCP 443 / TCP 23</td>
<td>TCP 62200 / TCP 7990 / TCP 443 / TCP 23</td>
</tr>
<tr>
<td>NDP</td>
<td>TCP 62200  / TCP 5222</td>
<td>none</td>
<td>none</td>
<td>TCP 62200</td>
</tr>
<tr>
<td>RP</td>
<td>TCP 62200  / TCP 5222</td>
<td>none</td>
<td>TCP 62200</td>
<td>none</td>
</tr>
</tbody>
</table>
3. Use Case
Infection
<table>
<thead>
<tr>
<th>Step</th>
<th>Direction</th>
<th>Action content</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GUI -&gt; ADMF</td>
<td>Infect a target</td>
<td>Send infection information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Target information / infection mode</td>
</tr>
<tr>
<td>2</td>
<td>ADMF -&gt; Radius probe</td>
<td>Start monitoring and set a trap on this target</td>
<td>Actual IP address of target is known</td>
</tr>
<tr>
<td>3</td>
<td>Radius -&gt; ADMF -&gt; NDP / iProxy</td>
<td>Handover actual IP address</td>
<td>IP address</td>
</tr>
<tr>
<td>4</td>
<td>iProxy -&gt; NDP</td>
<td>Iproxy requests NDP to analyse the datastream on IP address and „interesting“ traffic</td>
<td>Target IP address</td>
</tr>
<tr>
<td>5</td>
<td>NDP -&gt; iProxy</td>
<td>Handover traffic matching the request</td>
<td>Stream is redirected to iProxy</td>
</tr>
<tr>
<td>6</td>
<td>iProxy</td>
<td>changes the traffic and modifies the data by adding the infection parts</td>
<td></td>
</tr>
</tbody>
</table>
## Use Case → Infection

<table>
<thead>
<tr>
<th>Step</th>
<th>Direction</th>
<th>Action content</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>iProxy</td>
<td>changes the traffic and modifies the data by adding the infection parts</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>iProxy -&gt; NDP</td>
<td>iProxy sends the modified traffic back to NDP</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>NDP Reinject</td>
<td>NDP recalculates checksums, resequences TCP/IP packets and reinjects the traffic into the stream</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Target infection done</td>
<td>Data successfully sent to target</td>
<td></td>
</tr>
</tbody>
</table>
10. Infection succeeded → Start operating the target

Seperate training
3. System handling

Management network
ILO access
The iProxy components can either be accessed via SSH or ILO. These interfaces are solely made available on the management network.

- SSH:

  Secure shell is being used to directly access the iProxy components for all configuration changes, operation and debugging on system-level.

- ILO:

  Integrated lights out management is the dedicated access being used to manage system HW-components. i.e.: stop/start of the system hardware, hardware-monitoring, remote system console, etc.
SSH access

```
user system[-] ssh host -l user -p 62200
user@host's password:
Linux raftier 2.6.26-2-686 #1 SMP Tue Mar 9 17:35:51 UTC 2010 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Sep 16 12:34:35 2010 from raftier
user system[-] []
```

SSH : secure shell maintenance access on system level
ILO access

Integrated Lights-Out 2
HP ProLiant

Login name: 
Password: 

Log In  Clear

© Copyright 2008 Hewlett-Packard Development Company, L.P.

Contains security software licensed from RSA Data Security Inc.

FontList Copyright 1989, 1993, 1994 by Carleton W. Willan University

Edition 3.0, 2005-2006 Copyright 2005, 2006 The Regents of the University of California
ILO access

ILO Power: button press for “power on/power off”

Attention: It really works!
System Health

- **Fans:** Ok; Fully Redundant
- **Temperatures:** Ok
- **VRMs:** Ok
- **Power Supplies:** Ok; Fully Redundant
ILO access

Integrated Lights-Out 2
HP ProLiant

System Status
Remote Console Virtual Media Power Management Administration

Fan Health

Summary
System Information

ILO 2 Log
IML
Diagnostics
ILO 2 User Tips
Insight Agent

<table>
<thead>
<tr>
<th>Location</th>
<th>Status</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan 1: I/O Board Zone</td>
<td>Ok</td>
<td>45%</td>
</tr>
<tr>
<td>Fan 2: I/O Board Zone</td>
<td>Ok</td>
<td>45%</td>
</tr>
<tr>
<td>Fan 3: CPU Zone</td>
<td>Ok</td>
<td>42%</td>
</tr>
<tr>
<td>Fan 4: CPU Zone</td>
<td>Ok</td>
<td>42%</td>
</tr>
<tr>
<td>Fan 5: CPU Zone</td>
<td>Ok</td>
<td>42%</td>
</tr>
<tr>
<td>Fan 6: CPU Zone</td>
<td>Ok</td>
<td>42%</td>
</tr>
</tbody>
</table>

© GAMMAGROUP
## Temperature Health

<table>
<thead>
<tr>
<th>Location</th>
<th>Status</th>
<th>Reading</th>
<th>Thresholds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp 1: I/O Board Zone</td>
<td>Ok</td>
<td>38°C</td>
<td>Caution: 70°C; Critical: 75°C</td>
</tr>
<tr>
<td>Temp 2: Ambient Zone</td>
<td>Ok</td>
<td>18°C</td>
<td>Caution: 30°C; Critical: 44°C</td>
</tr>
<tr>
<td>Temp 3: CPU 1</td>
<td>Ok</td>
<td>30°C</td>
<td>Caution: 127°C; Critical: 127°C</td>
</tr>
<tr>
<td>Temp 4: CPU 1</td>
<td>Ok</td>
<td>30°C</td>
<td>Caution: 127°C; Critical: 127°C</td>
</tr>
<tr>
<td>Temp 5: Power Supply Zone</td>
<td>Ok</td>
<td>41°C</td>
<td>Caution: 77°C; Critical: 82°C</td>
</tr>
<tr>
<td>Temp 6: CPU 2</td>
<td>Ok</td>
<td>30°C</td>
<td>Caution: 127°C; Critical: 127°C</td>
</tr>
<tr>
<td>Temp 7: CPU 2</td>
<td>Ok</td>
<td>30°C</td>
<td>Caution: 127°C; Critical: 127°C</td>
</tr>
</tbody>
</table>
### ILO access

**Integrated Lights-Out 2**

- **HP Proliant**

#### Integrated Management Log

<table>
<thead>
<tr>
<th>Severity</th>
<th>Class</th>
<th>Last Update</th>
<th>Initial Update</th>
<th>Count</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repaired</td>
<td>Power</td>
<td>07/14/2009 19:39</td>
<td>07/14/2009 19:17</td>
<td>1</td>
<td>System Power Supplies Not Redundant</td>
</tr>
<tr>
<td>Critical</td>
<td>ASR</td>
<td>05/30/2009 11:37</td>
<td>05/30/2009 11:37</td>
<td>1</td>
<td>ASR: Detected by System POM</td>
</tr>
<tr>
<td>Caution</td>
<td>POST Message</td>
<td>05/20/2009 20:21</td>
<td>05/20/2009 20:21</td>
<td>1</td>
<td>POST Error: 1615-Power Supply Failure or Power Supply Unplugged In Bay 2</td>
</tr>
<tr>
<td>Caution</td>
<td>POST Message</td>
<td>05/20/2009 20:15</td>
<td>05/20/2009 20:15</td>
<td>1</td>
<td>POST Error: 1615-Power Supply Failure or Power Supply Unplugged In Bay 2</td>
</tr>
<tr>
<td>Caution</td>
<td>Power</td>
<td>05/20/2009 20:20</td>
<td>05/20/2009 20:15</td>
<td>2</td>
<td>System Power Supply: General Failure (Power Supply 2)</td>
</tr>
<tr>
<td>Caution</td>
<td>POST Message</td>
<td>05/20/2009 19:09</td>
<td>05/20/2009 19:09</td>
<td>1</td>
<td>POST Error: 1615-Power Supply Failure or Power Supply Unplugged In Bay 2</td>
</tr>
</tbody>
</table>

Log information from low level hardware components
ILO access

ILO System remote console information: choose the remote console

- **Integrated Remote Console**: Access the system KVM and control Virtual Power & Media from a single console under Microsoft Internet Explorer.

- **Integrated Remote Console Fullscreen**: Re-size the Integrated Remote Console to the same display resolution as the remote host. Exit the console to return to your client desktop.

- **Remote Console**: Access the system KVM from a Java applet-based console requiring the availability of a JVM.

- **Remote Serial Console**: Access a VT320 serial console from a Java applet-based console connected to the ILO 2 Virtual Serial Port. This console requires the availability of a JVM.
ILO access

ILO: access the OS via the ILO remote console
6. Technical Details

Commonly used SW components
System and Bios Hardening
Commonly used SW components

- Daemontools:
  - Used to provide a high level of availability for the installed core SW components

- Ssh:
  - Remote secure command-line access to the iProxy components for management purposes

- Ntp:
  - Being used for synchronizing the time on the iProxy components

- Syslog-ng:
  - Used for collecting all system and application events
  - Possibility to send a copy of the events to a defined e-mail address

- Shorewall (Except the NDP-Component):
  - High level configuration user-land frontend for the onboard firewalls
System and Bios Hardening

· System:
  · Firewall configured deny all, allow specifically
  · Removed unnecessary services
  · Disabled Ipv6
  · No direct root login allowed
  · Minimal software stack
  · Security optimized configuration for all services

· Bios:
  · Boot order and media
  · Bios password
  · In case of power failure: Auto power on
7. Incident Handling

Hands on / System Training
SSH access

Secure shell / SSH is used for accessing the iProxy-components:

Command:    ssh host -l user -p 62200

Parameters: host: hostname
             -l username
             -p portnumber
The command `id` is used for identifying the active user:

Command: id
Parameters: n.a.
Output: uid (user-id), gid (group-id), groups (groups the user belongs to)
The command `su` is used to gain root-privileges:

**Command:** su -
**Parameters:** - (to start the root-shell from home-path)
**Output:** n.a.

Attention: You are working on live systems, you may break things!
The command `dmesg` is used for displaying kernel debug messages:

**Command:** `dmesg`  
**Parameters:** n.a.  
**Output:** see above
Dir containing all system logs

The command `ls` lists the directory containing all system log files:

Command:     ls
Parameters:  i.e: -lah
Path:        /var/log
Important Log Files: daemon.log, messages, kern.log, auth.log, dmesg, syslog
List log directory by date:

Command: `ls -laht`

Parameters: 
- `-l = list`
- `-a = all`
- `-h = human readable`
- `-t = sort by date`

Output: all files sorted by date
The messages file contains all important system logs:

Command:   cat
Parameters: /var/log/messages
Output:   see above
The ADMF log file contains all messages from the admf service:

Log File Path: /home/iproxy/service/admf/service/log/logfiles/current
Command: less
Parameter: /home/iproxy/service/admf/service/log/logfiles/current
Output: see above
The NDP log file contains all messages from the ndp service:

Log File Path: /home/iproxy/service/ndp/service/log/logfiles/current
Command: less
Parameter: /home/iproxy/service/ndp/service/log/logfiles/current
Output: see above
The RP log file contains all messages from the rp service:

Log File Path: /home/iproxy/service/rp/service/log/logfiles/current
Command: less
Parameter: /home/iproxy/service/rp/service/log/logfiles/current
Output: see above
The command `ps` lists processes running on the system:

**Command:** ps -aux

**Parameters:** -a = all processes, -u = list by user-id, -x = list by tty

**Output:** all running processes, see above
The command `top` lists in realtime all processes running on the system:

**Command:**

```
top -d1
```

**Parameters:**

`-d = delay in seconds (here = 1 second)`

**Output:**

`see above`
The command `scp` is used for copying files from one server to another via ssh:

Command: `scp -P 62200 files.tar.bz2 user@host:/directory`

Parameters: 
- `-P 62200` (Portnumber to be used),
- `files =` the filename to be copied,
- `user@host =` user who logs into the target system,
- `/directory: where to copy the file`

Output: see above
The command `ifconfig` is used for listing active nic configurations:

**Command:** `ifconfig`

**Parameters:** n.a.

**Output:** see above
The network configuration is stored in configuration files on the systems. The file is on /etc/network/interfaces.
List active routing configuration

The command `route` is used for listing the active routes:

Command:   route
Parameters: -n = do not resolve IP addresses
Output:    routing table
The command `netstat` is used for listing network statistics:

Command: netstat
Parameters: -t = tcp-connection, -u = udp, -l = list, -p = program, 
e = extended output, -n = do not resolve IP address
Output: Network statistics
The command `tcpdump` is used to analyze network packets:

Command:  tcpdump
Parameters:  -n= do not resolve IP address, -i = interface name to dump
Output:  see above
The command `tcpdump` is used to analyze network packets:

Command: `tcpdump`
Parameters: `-n` = do not resolve IP address, `-i` = interface name to dump, `host` = hostaddress to filter on
Output: see above

```
root@system(-)~# tcpdump -ni eth0 host 192.168.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
13:03:06.795248 IP 192.168.59690 > 192.168.53: 25655+ AAAA? mail. (22)
13:03:06.801993 IP 192.168.53 > 192.168.59690: 25655 NXDomain 0/0/0 (22)
13:03:06.801993 IP 192.168.45287 > 192.168.53: 22123+ A? mail. (22)
^C
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```
The command `tcpdump` is used to analyze network packets:

Command: tcpdump
Parameters: -n = do not resolve IP address, -i = interface name to dump, port = port to filter on
Output: see above
Analyze contents of packets on a network

The command `tcpdump` is used to analyze network packets:

Command: `tcpdump -ni eth0 port 53 and proto UDP`

Parameters: `-n= do not resolve IP address, -i = interface name to dump, port = Port to filter on, proto = Protocol to filter on`,

Output: `see above`
Daemon Tools Usage

Daemon Tools is used for starting / stopping the iProxy services

a Daemon Tools File structure is needed:

/home/iproxy/service/admf

/data/
/etc/instance.conf
/service
/log/
/run
/supervise/

→ To activate the service admf, the /home/iproxy/service/admf/service directory has to be linked in to the /etc/service folder
Daemon Tools Usage

Daemon Tools is used for starting / stopping the iproxy services

Once the service is linked and activated it constantly restarts itself when having problems

The activated service can be controlled via the “svc” command:

- `svc -t /etc/service/admf`: sends a TERM Signal, and automatically restarts the daemon after it dies
- `svc -d /etc/service/admf`: sends a TERM Signal, and leaves the service down
- `svc -u /etc/service/admf`: brings the service back up
- `svc -o /etc/service/admf`: runs the service once
Hands on experience on demand

What would you like to explore in greater detail?

- Collecting network traces
- Collecting logs
- Collecting evidence
- More system training
- Tell us
Incident handling

Basically the systems just work. In case something does not work or you are not sure:

1) Collect data, evidences, log files
2) Contact our helpdesk
3) More details (including contact) in the system manual
4) We fix things together
Questions ?

Thank you for your attention !