校園資訊安全之威脅與因應

劉乙 Jim Liu
Technical Director
Fortinet.Taiwan
0912214906
jimliu@fortinet.com
Agenda

- Fortinet 簡介
- 資訊網路潛在威脅之探討分析
- ASIC Base防毒防駭即時防護系統
- 網路安全報表統計與分析工具
Fortinet 簡介 --- Who is Fortinet ?
A History of Rapid Growth and Achievement

- Developed World’s First ASIC-Accelerated Antivirus/Content Security Technology
- Fortinet Founded
- FortiGate Family Introduced
- Recognized by Gartner as Visionary
- $50 Million Financing

Cumulative Unit Shipments
Fortinet Company Overview

- Founded October, 2000 by Ken Xie
  - Founder, former Pres. & CEO of NetScreen (NASDAQ: NSCN)
- Over 350 employees; HQ in Sunnyvale, CA
  - Offices throughout Americas, Asia, and EMEA
    - Tokyo, Seoul, Beijing, Shanghai, Hong Kong, Taipei, Singapore, KL, Melbourne, etc.
    - Belgium, France, Germany, Italy, Sweden, UK
- Creators of world’s only ASIC-powered antivirus systems
  - Addressing the need for real-time network protection
- Achieved >10x revenue growth in 2003 vs. 2002
  - Over 50,000 units shipped in under 2 and half of years
- Completed $50 million mezzanine financing Feb 2004
  - Positioned for continued rapid growth
Fortinet is Driving a Major Shift in the Evolving Security Market

“...Firewalls must provide a wider range of intrusion prevention capabilities, or face extinction...”

“Fortinet has demonstrated its investment in powerful network processing technology by filtering viruses in-line, which requires an unprecedented level of packet assembly and filtering.”
The FortiGate Family Scales from SOHO to Service Provider

FortiGate Product Family

- **FortiGate-100**: SOHO
- **FortiGate-300**: Branch Office
- **FortiGate-400**: Medium Enterprise
- **FortiGate-4000**: Large Enterprise
- **FortiGate 500 Multi-Zone**: Service Provider/Telco

**Capabilities**

- Virus/Worm Scanning, Firewall, VPN, Intrusion Detection & Prevention, Content Filtering
- DMZ port, traffic shaping
- Enhanced remote client capacity
- Integrated Logging (20 Gbyte)
- Dual USB ports; integrated 4 managed switch ports; Dual WAN connection
- Redundant power
- Gigabit performance
- Multi-Zone (12 10/100 ports)
- High Availability
- FortiManager System
- FortiLog System
- FortiGate-100
- FortiGate-200
- FortiGate-300
- FortiGate-400
- FortiGate-500
- FortiGate-800
- FortiGate-1000
- FortiGate-3000
- FortiGate-3600
- FortiGate-4000
- FortiWiFi-60

**Performance (Mbps)**

- 30
- 95
- 120
- 200
- 300
- 4G
- 2G
- 1G
- 300
- 120
- 90
- 60
- 30
- 15
- 10
- 5
- 3
資訊網路潛在威脅之探討分析
The Nature of Threats Has Evolved…

Major Pain Points for Organizations of all Types


PHYSICAL

CONNECTION-BASED

CONTENT-BASED

SPEED, DAMAGE ($)

Hardware Theft

Intrusions

Viruses

Trojans

Worms

Intrusions

Spam

Banned Content

Anti-spam

Anti-virus

Content Filter

IDS

VPN

Firewall

Lock & Key

PHYSICAL

SPEED, DAMAGE ($)

Firewalls Don’t Analyze Contents so they Miss Content Attacks

**STATEFUL INSPECTION FIREWALL**

Inspects packet headers only – i.e. looks at the envelope, but not at what’s contained inside.

DATA PACKETS

Packet “headers” (TO, FROM, TYPE OF DATA, etc.)

Packet “payload” (data)

CONFIDENTIAL

http://www.freesurf.com/downloads/Gettysburg

Four score and **BAD CONTENT** our forefathers brought forth upon this continent a new nation, liberty, and dedicated to the proposition that all
Some Firewalls Claim to do “Deep Packet Inspection” – But They Still Miss a Lot

DEEP PACKET INSPECTION
Performs a packet-by-packet inspection of contents – but can easily miss complex attacks that span multiple packets

http://www.freesurf.com/downloads/Gettysburg

Four score and eight years ago our forefathers brought forth upon this continent a new nation,

 liberty, and dedicated to the proposition that all...
To Stop Content-Based Threats Requires More than Deep Packet Inspection

COMPLETE CONTENT PROTECTION

1. Reassemble packets into content

   http://www.freesurf.com/downloads/Gettysburg

   Four score and **BAD CONTENT** our forefathers brough

   Four score and seven years ago our forefathers brought forth upon this
continent a new nation,

   liberty, and dedicated to the proposition that all…

2. Compare against disallowed content and attack lists

   **DISALLOWED CONTENT**

   **BAD CONTENT**

   **NASTY THINGS**

   **NASTIER THINGS**

   **ATTACK SIGNATURES**
使用網路銀行防毒、防駭缺一不可

記者歐陽宜珊／台北報導
2004-4-01 18:40

針對日前台灣出現網路銀行帳號被木馬程式竊取密碼而盜領的犯罪案例，雖然銀行立即向警方報案，且查證之後發現只有少數幾位受害者。若消費者的電腦被植入後門或是因為中毒，必須自行負擔損失。另外，若是習慣使用簡單密碼的用戶也要注意，駭客隨時可猜中密碼，而盜領銀行的錢。因此加強電腦防毒、防駭及強化身份認證機制成了當前重要的一環。

此次出現的案例，駭客是透過電子郵件或惡意網站等手法將木馬或後門程式植入受害者電腦，當使用者登入網路銀行時，木馬程式就將受害者的在鍵盤上輸入的帳號及密碼等資料予以記錄，接著再將竊取到的資料，透過電子郵件或檔案傳送等手法傳至指定的網址，歹徒再透過「非約定帳戶」轉帳功能，盜領成功。

如果加裝用戶端數位憑證，也不能杜絕所有木馬或後門問題。只能增加入侵的複雜度，駭客還是有可能透過木馬竊走使用者密碼、數位憑證與私密金鑰。若使用IC卡或「一次密碼器」(Token)，也無法完全避免駭客利用木馬或後門進行盜領。駭客還是有可能在背景發出假交易或竄改交易內容，甚至可讓IC卡對假冒的交易內容進行數位簽章，除了利用此方式取得帳號外，多數人常用懶人密碼設定，雖然連續三次不對，帳號會被鎖定，不過若使用破解密碼的軟體，一次即可猜中。因此，如果要避免被駭客盜取密碼帳號，消費者在設定時，必須英文、數字混合使用，且至少應包含2個大小寫英文字母或符號、密碼與代號間不可相同。
網銀用戶須防堵木馬程式開後門竊密碼盜存款

（中央社記者韋樞台北四日電）

日前傳出數家網路銀行的客戶遭駭客盜領，事實上，此事件責任釐清後網路銀行並沒有安全疏失，主要原因是個人的安全防護出現大缺口，資訊安全廠商已經掌握到肇禍的木馬程式是Backdoor.Powerspider.B，駭客利用鍵盤側錄功能盜取存戶的密碼，將存戶的存款提領一空。

Backdoor.Powerspider.B，這類程式會偽裝成IE的名稱iexpore.exe，駭客透過電子郵件或網頁，甚至是p2p程式等多種方式將此程式植入受害者電腦，利用鍵盤側錄的功能(keylogger)竊取機密資訊，再透過電子郵件的方式傳回駭客的電腦裡，駭客登入網路銀行後，透過「非約定轉帳」方式盜領存款。

至於駭客是如何植入後門及木馬程式，林育民分析，駭客利用病毒（Beagle、MyDoom、Bugbear系統漏洞）電子郵件，或透過色情、軟體破解或其他惡意網站，偽裝成可吸引使用者執行或下載的應用程式，或利用社交工具如MSN、Yahoo、Messenger、ICQ等途徑，植入或散布木馬程式。

網路銀行用戶要防杜被盜領，必須確認個人電腦的網路安全防護，除可偵測掃除木馬程式、鍵盤側錄程式的防毒功能外，進階型的個人防火牆，入侵偵測機制則是整合防護的標準配備，缺一不可。

對習慣性使用網路銀行的消費者而言，務必要養成良好的使用習慣，不任意開啓不明的電子郵件或附件，不隨意安裝或執行來路不明的軟體，不任意瀏覽色情或可能有惡意的網站，並關閉移除不必要的服務與程式，唯有確實在電腦安全防護和個人使用習慣上強化安全性，才能一面享受網路銀行的便利，一面照顧好自己的財物安全。930404
IPS can Protect everything --- Post-Sasser.
IPS Vendors Speak up ---- Post-Sasser

• Block worm & exploit viruses is trend
  – Antivirus is not important
  – Even NetSky can be blocked by IPS
• IPS is enough
  – Can block exploit worm, Trojans and Backdoor
• IF true, why TrendMicro, Symantec … focus on protocol-based AV?
  http, FTP, Email
What is IDS?

What does IDS work?
Performs specific packets inspection and behavior analysis.

1. Signature

2. Behavior

CONFIDENTIAL
The Fact is ......... (1/2)

Only one level compression
The Fact is ........ (2/2)

Or attached a email with Viruses
Conventional/Single Point Security Solution Do Not Solve these Problems

If it is sasser, then

Spam
Viruses, worms
Intrusions
Banned content

Do Not Examine The Content of Data Packets – Threats Pass Through
Protocol-based Antivirus Benefits

• According to protocol
  – to adapt different kinds of file format or Characteristic of different application.
  i.e. like compression file type, ZIP, RAR,… outlook, outlook express or Unix Mailbox
World-Wide based Real time Update Center
Ensure Rapid Response to New Threats

Fortinet Threat Response Team and Update Distribution Servers

FortiProtection Center Web Portal & email Bulletins

Automatic Updates Can Reach All FortiGate Units Worldwide in Under 5 Minutes
Dynamic Real time Attack Response Combines the Best of AV, NIDS and IDP

- Multiple detection mechanisms
  - AV signatures (application layer, content scan)
  - Intrusion signatures (protocol layer, content & behavior)

- Reduction in false positives and the amount of data analysis
  - Policy-based IPS applies scanning only where needed

- Multiple prevention mechanisms
  - Packet drop
  - Port closure
  - TCP reset
  - Traffic limit (e.g. P2P apps)
  - File delete/quarantine

*All dynamically updatable via the FortiProtection Network*
NIPS Signatures

Edit Predefined NIDS Signature

- Group Name: apache
  - Signature Name: Apache-DoS
    - Revision: 10
    - Enable: ✔
    - Logging: ✔
    - Action: Pass
    - Details: view
  - Signature Name: Chunked-Encoding.vorm
    - Revision: 10
    - Enable: ✔
    - Logging: ✔
    - Action: Pass
    - Details: view

- Group Name: pop2
  - Signature Name: pop2
    - Revision: 2
    - Enable: ✔
    - Logging: ✔
    - Action: Pass
    - Details: view

- Group Name: pop3
  - Signature Name: pop3
    - Revision: 5
    - Enable: ✔
    - Logging: ✔
    - Action: Pass
    - Details: view
A New Approach for Content filtering
Limitations of Conventional Software-Based Web Filtering Solutions

- Requires a dedicated server
- Requires periodic update of large (multi-megabyte) URL database
- Missed and incorrect ratings between updates
- High cost
The Fortinet Solution: FortiGate Antivirus Firewalls + FortiGuard Service

- No additional hardware required
- No need to download large database to FortiGate units
- URL ratings are always up to date
- Local FortiGate caching of ratings greatly improves performance
- FortiGate solution also scans HTML content for keywords/phrases
- Lower cost
- Multi-language recognition
- Reduction in false positives
  - Policy-based IPS applies scanning only where needed

FortiGuard Web Filtering Solution

Internet

FortiGuard URL Database

FortiGuard Hosting Sites (data mining) (Worldwide)

URL requests from users are checked against internal cache in FortiGate unit – if not yet rated, FortiGate unit sends rating request to FortiGuard hosting site

FortiGate unit allows or denies page based on requestor’s Content Profile

www.cnn.com = ?

“www.cnn.com matches the NEWS category.”
Web Profiles Support 80 Content Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Action</th>
<th>Category</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abortion</td>
<td>Allow</td>
<td>Pro-Choice</td>
<td>Allow</td>
</tr>
<tr>
<td>Pro-Life</td>
<td>Allow</td>
<td>Adult Content</td>
<td>Allow</td>
</tr>
<tr>
<td>Lingerie and Swimsuit</td>
<td>Allow</td>
<td>Nudity</td>
<td>Allow</td>
</tr>
<tr>
<td>Sex</td>
<td>Allow</td>
<td>Sex Education</td>
<td>Allow</td>
</tr>
<tr>
<td>Advocacy Groups</td>
<td>Allow</td>
<td>Business and Economy</td>
<td>Allow</td>
</tr>
<tr>
<td>Financial Data and Services</td>
<td>Allow</td>
<td>Abused Drugs</td>
<td>Allow</td>
</tr>
<tr>
<td>Marijuana</td>
<td>Allow</td>
<td>Prescribed Medications</td>
<td>Allow</td>
</tr>
<tr>
<td>Supplements and Unregulated Compounds</td>
<td>Allow</td>
<td>Cultural Institutions</td>
<td>Allow</td>
</tr>
<tr>
<td>Educational Institutions</td>
<td>Allow</td>
<td>Educational Materials</td>
<td>Allow</td>
</tr>
<tr>
<td>Reference Materials</td>
<td>Allow</td>
<td>Entertainment</td>
<td>Allow</td>
</tr>
<tr>
<td>MP3</td>
<td>Allow</td>
<td>Gambling</td>
<td>Allow</td>
</tr>
<tr>
<td>Games</td>
<td>Allow</td>
<td>Government</td>
<td>Allow</td>
</tr>
<tr>
<td>Military</td>
<td>Allow</td>
<td>Political Organizations</td>
<td>Allow</td>
</tr>
<tr>
<td>Health</td>
<td>Allow</td>
<td>Illegal or Questionable</td>
<td>Allow</td>
</tr>
<tr>
<td>Information Technology</td>
<td>Allow</td>
<td>Computer Security</td>
<td>Allow</td>
</tr>
<tr>
<td>Abortion</td>
<td>Allow</td>
<td>Pro-Choice</td>
<td>Allow</td>
</tr>
<tr>
<td>Pro-Life</td>
<td>Allow</td>
<td>Adult Content</td>
<td>Allow</td>
</tr>
<tr>
<td>Lingerie and Swimsuit</td>
<td>Allow</td>
<td>Nudity</td>
<td>Allow</td>
</tr>
<tr>
<td>Sex</td>
<td>Allow</td>
<td>Sex Education</td>
<td>Allow</td>
</tr>
<tr>
<td>Advocacy Groups</td>
<td>Allow</td>
<td>Business and Economy</td>
<td>Allow</td>
</tr>
<tr>
<td>Financial Data and Services</td>
<td>Allow</td>
<td>Abused Drugs</td>
<td>Allow</td>
</tr>
<tr>
<td>Marijuana</td>
<td>Allow</td>
<td>Prescribed Medications</td>
<td>Allow</td>
</tr>
<tr>
<td>Supplements and Unregulated Compounds</td>
<td>Allow</td>
<td>Cultural Institutions</td>
<td>Allow</td>
</tr>
<tr>
<td>Educational Institutions</td>
<td>Allow</td>
<td>Educational Materials</td>
<td>Allow</td>
</tr>
<tr>
<td>Reference Materials</td>
<td>Allow</td>
<td>Entertainment</td>
<td>Allow</td>
</tr>
<tr>
<td>MP3</td>
<td>Allow</td>
<td>Gambling</td>
<td>Allow</td>
</tr>
<tr>
<td>Games</td>
<td>Allow</td>
<td>Government</td>
<td>Allow</td>
</tr>
<tr>
<td>Military</td>
<td>Allow</td>
<td>Political Organizations</td>
<td>Allow</td>
</tr>
<tr>
<td>Health</td>
<td>Allow</td>
<td>Illegal or Questionable</td>
<td>Allow</td>
</tr>
<tr>
<td>Information Technology</td>
<td>Allow</td>
<td>Computer Security</td>
<td>Allow</td>
</tr>
</tbody>
</table>
A Range of Logging and Reporting Options

• **Logging**
  – FortiGate unit logs the source IP, destination IP, requested URL, action (allowed/denied), and content category

• **Built-in reporting**
  – Graph in the FortiGate GUI shows web usage by category

• **Additional reporting**
  – Logs are compatible with 3rd party reporting tools, such as eIQnetworks Firewall Analyzer / SecureExp
A BASIC Anti-SPAM skill
Email Content Filtering (Antispam) Enhancements

- Check & Mark Messages with Signs of SPAM:
  - Keywords & phrases in message body and subject line
  - Blacklist of known bad spam senders
  - Invalid return email address (DNS check)
  - Spoofing (MIME header check)

- Block SMTP Messages based on:
  - IP address Black/White list
  - IP-based checks against the Real-time Blackhole list (RBL) and the Open Relay Database (ORDB)
  - Reverse DNS lookups
Anti-Spam

```
C:\WINDOWS\System32\cmd.exe - nslookup
C:\Documents and Settings\Jim Liu>nslookup
Default Server:  dns.hinet.net
Address:  168.95.1.1

> set type=MX
> msn.com
Server:  dns.hinet.net
Address:  168.95.1.1

msn.com MX preference = 5, mail exchanger = mx1.hotmail.com
msn.com MX preference = 5, mail exchanger = mx2.hotmail.com
msn.com MX preference = 5, mail exchanger = mx3.hotmail.com
msn.com MX preference = 5, mail exchanger = mx4.hotmail.com
mx1.hotmail.com internet address = 65.54.166.99
mx1.hotmail.com internet address = 64.4.50.50
mx1.hotmail.com internet address = 65.54.252.99
mx1.hotmail.com internet address = 64.4.50.99
mx2.hotmail.com internet address = 65.54.190.50
mx2.hotmail.com internet address = 65.54.252.230
mx2.hotmail.com internet address = 65.54.190.7
mx2.hotmail.com internet address = 65.54.166.230
mx3.hotmail.com internet address = 64.4.50.179
mx3.hotmail.com internet address = 65.54.253.99
mx3.hotmail.com internet address = 65.54.167.5
```
### Anti-Spam

**郵件選項**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>郵件設定</strong></td>
<td><strong>安全性</strong></td>
</tr>
<tr>
<td>重要性</td>
<td>敏感度</td>
</tr>
<tr>
<td>高</td>
<td>普通</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>追蹤選項</strong></td>
<td></td>
</tr>
<tr>
<td>索取此郵件的傳送回條(R)</td>
<td>索取此郵件的閱讀回條(R)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>傳送選項</strong></td>
<td></td>
</tr>
<tr>
<td>預設郵件回覆收件者(T):</td>
<td>Ready</td>
</tr>
<tr>
<td>□ 截止於(截止至)</td>
<td>晚上 12:00</td>
</tr>
</tbody>
</table>

**連絡人(C)...**

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

**類別(1)...**

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Internet標題(出):**

```plaintext
by mail:fortinet.com (8.12.8/8.12.8) with SMTP id 12KSSL Lo006427
for <apex_support@fortinet.com>; Sun, 20 Mar 2004 11:28:30 -0800
Message-ID: <200403201928.12KSSL Lo006427@mail:fortinet.com>
From: "Ready" <Tiller@msn.com>
Reply-To: "Ready" <Tiller@msn.com>
To: apex_support@fortinet.com
Subject: Re: Card Declined, app_d... 062054
```

---

34
RBL Server-List

- rbl.maps.vix.com
- dul.maps.vix.com
- relays.orbs.org
- bl.spamcop.net
- cbl.abuseat.org
- dnsbl.njabl.org
- dnsbl.sorbs.net
Why everybody talk about ASIC?
The ASIC-Based FortiGate Platforms Provide Better Protection and Higher Performance

Throughput

- Stateful Inspection
- Deep Packet Inspection
- Complete Content Protection

ASIC-BASED FIREWALL APPLIANCE

ASIC-BASED FORTIGATE PLATFORM
What’s real hardware-based Security Box?

Content processor is needed !!!
Fortinet Developed a Unique Architecture for Complete, Real-Time Network Protection

CORE TECHNOLOGY

- FortiASIC™ Content Processor
  - Proprietary Fortinet Chip
  - Hardware scanning engine
  - Hardware encryption
  - Real-time content analysis

- FortiOS™ Operating System
  - Real-time networking OS
  - High performance
  - Robust, reliable
What is the weakest point for point solution? (Why policy based management is needed?)

FortiASIC Content Processor Chip

*Note: Blocks can be used in multiple combinations, e.g. firewall, AV, and other functions can be applied to decrypted VPN tunnels
安全網路架構
A Real Case for Education Network
Fortinet Provides a Complete Solution for the Educational Network (1/2)

TANET Backbone

Central Manager

FortiManager

TANET 營網
200 * FGTs 中小學...
Fortinet Provides a Complete Solution for the Educational Network (2/2)

FG3600 adds antivirus and IDS/IDP protection at the gateway in transparent mode behind existing firewall

FG300 provides antivirus, IDS/IDP and firewall protection, and traffic shaping functionality for dorms

FG300 adds antivirus, IDS/IDP protection to existing firewall for administrative services

FG3600 provides in-line firewall, antivirus, IDS/IDP functionality to data center
High Availability Feature Highlights

• Fortigate Clustering Protocol (Real Clustering)
  Active-Active (TP / Routing mode)
  Active-Passive (TP / Routing mode)
• HA in transparent mode
• Stateful failover for both firewall and VPN traffic within 3 seconds
• Link status monitoring and failover
• HA Alert
  – During failover, the FortiGate units in an HA group send an email and SNMP trap, and log the event.
Enough?
Fortinet always think more for you
無線網路安全面面觀
What is users’ requirement we care?

- Only wireless Access Point with Complete Content Protection
Integrated SMB Wireless Solution

Security
• Gateway and AP not vulnerable
• AV scanning for all users at all times
• WLAN clients protected from each other
• Can enforce Security Policy at all points
• EVEN provide IPsec Tunnel directly to internet
Valuable Reporter is necessary
Good news is that Firewalls stream all activity in Syslog Messages. Syslog Servers capture this info into log files.

**But** finding valuable information in Firewall log files which contain huge amounts of cryptic information is not easy.
FirewallAnalyzer – Instant Reporting
## FirewallAnalyzer – Drill Down

**Firewall TP-FG60**

<table>
<thead>
<tr>
<th>MACHINE_NAME</th>
<th>LOG_TIME</th>
<th>rule_desc</th>
<th>PROTOCOL</th>
<th>SRC_IP</th>
<th>SRC_NAME</th>
<th>DST_IP</th>
<th>DST_NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2004/6/18 上午11:20:00</td>
<td>0</td>
<td>TCP</td>
<td>219.0.31.194.002</td>
<td>219.0.31.194.002</td>
<td>55.5.80.219.dynatic.fh.net.tw</td>
<td>219.0.0.05.155</td>
</tr>
<tr>
<td>2</td>
<td>2004/6/18 上午11:20:00</td>
<td>0</td>
<td>TCP</td>
<td>219.0.31.194.002</td>
<td>219.0.31.194.002</td>
<td>55.5.80.219.dynatic.fh.net.tw</td>
<td>219.0.0.05.155</td>
</tr>
<tr>
<td>3</td>
<td>2004/6/18 上午11:20:00</td>
<td>0</td>
<td>TCP</td>
<td>219.0.31.194.002</td>
<td>219.0.31.194.002</td>
<td>55.5.80.219.dynatic.fh.net.tw</td>
<td>219.0.0.05.155</td>
</tr>
<tr>
<td>4</td>
<td>2004/6/18 上午11:30:00</td>
<td>0</td>
<td>TCP</td>
<td>219.0.31.194.002</td>
<td>219.0.31.194.002</td>
<td>55.5.80.219.dynatic.fh.net.tw</td>
<td>219.0.0.05.155</td>
</tr>
<tr>
<td>5</td>
<td>2004/6/18 上午11:30:00</td>
<td>0</td>
<td>TCP</td>
<td>219.0.31.194.002</td>
<td>219.0.31.194.002</td>
<td>55.5.80.219.dynatic.fh.net.tw</td>
<td>219.0.0.05.155</td>
</tr>
<tr>
<td>6</td>
<td>2004/6/18 上午11:30:00</td>
<td>0</td>
<td>TCP</td>
<td>219.0.31.194.002</td>
<td>219.0.31.194.002</td>
<td>55.5.80.219.dynatic.fh.net.tw</td>
<td>219.0.0.05.155</td>
</tr>
<tr>
<td>7</td>
<td>2004/6/18 上午11:30:00</td>
<td>0</td>
<td>TCP</td>
<td>219.0.31.194.002</td>
<td>219.0.31.194.002</td>
<td>55.5.80.219.dynatic.fh.net.tw</td>
<td>219.0.0.05.155</td>
</tr>
<tr>
<td>8</td>
<td>2004/6/18 上午11:30:00</td>
<td>0</td>
<td>TCP</td>
<td>219.0.31.194.002</td>
<td>219.0.31.194.002</td>
<td>55.5.80.219.dynatic.fh.net.tw</td>
<td>219.0.0.05.155</td>
</tr>
<tr>
<td>9</td>
<td>2004/6/18 上午11:30:00</td>
<td>0</td>
<td>TCP</td>
<td>219.0.31.194.002</td>
<td>219.0.31.194.002</td>
<td>55.5.80.219.dynatic.fh.net.tw</td>
<td>219.0.0.05.155</td>
</tr>
<tr>
<td>10</td>
<td>2004/6/18 上午11:30:00</td>
<td>0</td>
<td>TCP</td>
<td>219.0.31.194.002</td>
<td>219.0.31.194.002</td>
<td>55.5.80.219.dynatic.fh.net.tw</td>
<td>219.0.0.05.155</td>
</tr>
<tr>
<td>11</td>
<td>2004/6/18 上午11:30:00</td>
<td>0</td>
<td>TCP</td>
<td>219.0.31.194.002</td>
<td>219.0.31.194.002</td>
<td>55.5.80.219.dynatic.fh.net.tw</td>
<td>219.0.0.05.155</td>
</tr>
<tr>
<td>12</td>
<td>2004/6/18 上午11:30:00</td>
<td>0</td>
<td>TCP</td>
<td>219.0.31.194.002</td>
<td>219.0.31.194.002</td>
<td>55.5.80.219.dynatic.fh.net.tw</td>
<td>219.0.0.05.155</td>
</tr>
<tr>
<td>13</td>
<td>2004/6/18 上午11:30:00</td>
<td>0</td>
<td>TCP</td>
<td>219.0.31.194.002</td>
<td>219.0.31.194.002</td>
<td>55.5.80.219.dynatic.fh.net.tw</td>
<td>219.0.0.05.155</td>
</tr>
</tbody>
</table>