

Decision Computer Group

E-Forbiddler / WLAN Forbiddler

Moving forward with the security of networking and computer forensics

E-DETECTIVE®

Decision Computer - All rights reserved
2007





Introduction to WLAN FORBIDDER

- Control over wireless connection and auditing equipments
- Prevent and block illegal Wireless connections (from Internal to external network, from external to internal network).
- For instant, illegal user trying to access a company network will be blocked. A company user accidentally connect to external network will also be disconnect off.
- Working in IEEE 802.11 a/b/g Standard environment.



WLAN FORBIDDER WORKING PRINCIPLES

WLAN-FORBIDDER provides the various features:

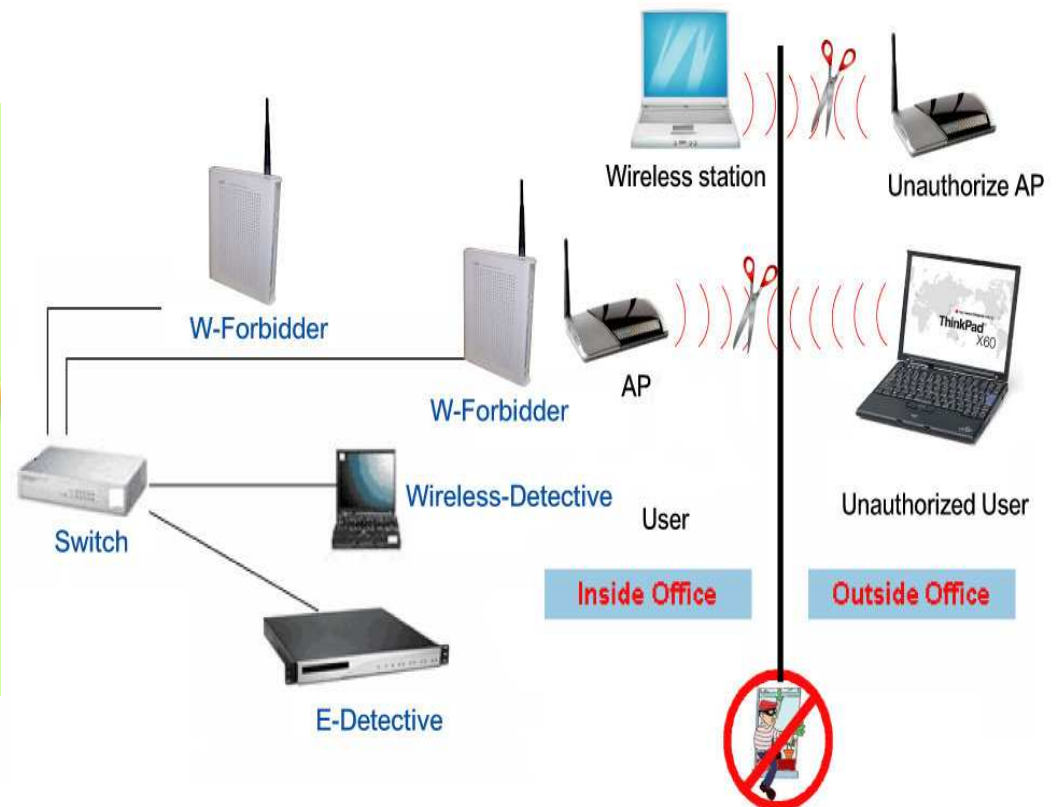
- Detecting the unauthorized AP/STA set up in inner and outer company.
- Blocking any illegal connections when the unauthorized AP/STA is detected and trying to make a illegal connection in order to prevent the information leaks.
- Recoding/Auditing the information issued by unauthorized AP and Sta.



Leakage of Information and Security Concern

- The criminal bureau ferreted out a suspect in Taipei who stole wireless bandwidth, brushed the credit card, money laundering. 15/June/2006
- The suspect was trying to steal wireless bandwidth and engaged in committing the network crime, Bureau Chief Hou Yui instructed a special case group to investigate into this event immediately...

WLAN FORBIDDER System – Equipments





WLAN FORBIDDER WORKING INSTRUCTION

1. Setup the allowed list in server system.
2. Server System checks whether the connection is allowed or through W-Forbidder (capture).
3. Cutting the connection if it's illegal one through W-Forbidder (Forbid).
4. Notifying Admin.
5. Auditing the notification.
6. Investigating the invader.

WLAN FORBIDDER – ALLOWED LIST

Condition Setup
Import

Para.:
allow
ap
add
mac
00:e0:98:51:0f:06
time:
01
01
23
59
Submit

finish !

NO.	ITEM	LIST
1	Server info:	ftp://user:111111@localhost/clipper (state: Off) (size: 0)
2	Clipper state:	Sniffer (Running)
3	Channels for scanning:	1 2 3 4 5 6 7 8 9 10 11
4	Banned AP list:	00:e0:98:51:0f:06 00:00-12:00 00:0d:0b:a1:cf:25 00:00-00:00
5	Allowed AP list:	00:0a:79:49:cd:00 00:00-23:59 00:0d:88:44:e7:f3 00:00-12:00
6	Banned station list:	00:16:01:18:0b:ce 00:00-00:59
7	Allowed station list:	00:0a:79:1a:87:08 00:00-23:59
8	Guard AP list:	

1. Scanned channels
2. Banned AP and Sta
3. Allowed AP and Sta
4. Backup via FTP

WLAN-FORBIDDER

Detecting APs and STA within coverage area

Hard Disk Information : - 55G / Used - 2.5G / Available - 49G / Available (%) - 95%

Capture Import Wepkey History Work Log Ids

MODE : ☐ AP ☒ STA

Capture Size : 280 K In Time Condition Dump Filter Condition Save List Refresh: 7 s. START STOP

STA	SCAN	MANUAL DUMP	AUTO DUMP	CLIENT MAC	STR.	PACKETS	BSSID	WEPKEY	CH.	ESSID
1	<input type="radio"/>	START	START	# ip 00:0C:F1:23:8D:AD	75	1177	00:17:9A:C2:F1:5A	OPN	6	SMC
2	<input type="radio"/>			# ip 00:17:9A:C2:F1:5A	5	5971	00:13:F7:31:BA:59		-1	

Count : 2 , Total : 1 , In page 1 | Rows per page : 20 Submit

Scanned Access points' Info.

Scanned Stations' Info.

STA	SCAN	MANUAL DUMP	AUTO DUMP	CLIENT MAC	STR.	PACKETS	BSSID	WEPKEY	CH.	ESSID
1	<input type="radio"/>	START	START	# ip 00:0C:F1:23:8D:AD	75	1177	00:17:9A:C2:F1:5A	OPN	6	SMC
2	<input type="radio"/>			# ip 00:17:9A:C2:F1:5A	5	5971	00:13:F7:31:BA:59		-1	

Count : 2 , Total : 1 , In page 1 | Rows per page : 20 Submit

DPI : 1024x768

Data Mining

WLAN FORBIDDER Features

1. POP3, SMTP, IMAP, Web Mails

The screenshot displays the WLAN FORBIDDER application interface. On the left is a 'MENU' sidebar with various protocols listed: POP3 (6), SMTP (7), IMAP (25), FTP (18), MSN (175), ICQ (1), YAHOO (7), VOIP (4), HTTP (1941), HTTP (DYNAMIC) (502), WEBMAIL (117), WEBMAIL (SENDER), TELNET (14), QQ (1), P2P (8641), SEARCH, ALARM, EXPORT, MANAGE, and LOGOUT. The main window shows a table of email records under the condition 'POP3 - 192.168.1.170 / ~ /'. The table has columns for NO., DATE / TIME, FROM, TO, CC, SUBJECT, ACCOUNT, and PAS. A red arrow points to the first record, which is highlighted. Below the table, a 'Detailed Record' is shown, listing the email's metadata and content. The email is from neoyuscor@hotmail.com to reedueme@decision.com.tw, dated 2006-04-01 12:35:05.0, with an attachment 'Cyclone Glenda hits Australia.doc'. The email body text is visible below the metadata.

Detailed Record:

1. Sender/Receiver.
2. Account, Pass.
3. Attached Files.
4. Email

click

Subject: Best of the era? Try Rivera
From: neoyuscor@hotmail.com
To: reedueme@decision.com.tw
CC:
BCC:
Date: 2006-04-01 12:35:05.0
Source: POP3 ABtA3H.eml.txt
Attachment: Cyclone Glenda hits Australia.doc
IP: 192.168.1.236
DATETIME: 2006-04-01 12:34:39.0

Dear Casper,
We will process the payment. You should be getting it early next week. We do hope you can ship some product brochure together..
Looking forward for more business with you in future. Thanks.
Best regards,
David
Manager Director

Decis

Done

Internet

WLAN FORBIDDER Features

2. HTTP Web Browsing (URL and Contents)



CONDITION : DYNAMIC - 192.168.1.131 / ~ /

NO.	DATE / TIME↑	URL
1.	2007-04-10 16:40:52	rad.msn.com
2.	2007-04-10 16:32:34	ad.addeliver.biz
3.	2007-04-10 16:32:34	ad.addeliver.biz
4.	2007-04-10 16:32:34	ad.addeliver.t
5.	2007-04-10 16:32:32	www.gofoxy.n
6.	2007-04-10 16:31:52	tw.yahoo.com

Count : 6 , Total : 1 , In page 1 | Rows per page : 20 Submit

Date/Time, Browsed Website content,...etc.



WLAN FORBIDDER Features

3. IM – Yahoo, MSN, ICQ, AOL, QQ

The screenshot shows the WLAN FORBIDDER interface. On the left is a 'MENU' with various protocols like POP3, SMTP, IMAP, FTP, MSN, ICQ, YAHOO, VOIP, HTTP, WEBMAIL, TELNET, and QQ. The main window displays a table of network conditions. A red box highlights the first row of the table, and a red arrow points to it with the text 'click'. Below the table, a large red text overlay reads: 'Date/Time, IP, Account, Messages Transferred Files,...etc.'

NO.	DATE / TIME↑	SCREEN NAME	PARTICIPANTS	CONVERSATION	COUNTS
1.	2007-04-11 15:11:09	rex_lin_11@hotmail.com	wedetector1@hotmail.com	CONVERSATION	26

Count : 1 , Total : 1 , In page 1 | Rows per page : 20

The screenshot shows an MSN chat window titled 'MSN | 192.168.1.6 - Windows Internet Explorer'. The address bar shows 'https://202.39.29.30/msn_msg.php?_IDX=1158'. The chat window displays a conversation between 'rex_lin_11@hotmail.com' and 'wedetector1@hotmail.com'. The messages are as follows:

Date-Time	User Handle	Message	File Name	File Size
2007-03-23 09:03:31	wedetector1@hotmail.com	hi..good morning..		
2007-03-23 09:03:47	rex_lin_11@hotmail.com	hi good morning		
2007-03-23 09:04:12	wedetector1@hotmail.com	Is there any solutions for the the network that we sent to u?		
2007-03-23 09:04:28	wedetector1@hotmail.com	We would have to get back to our client on this..		
2007-03-23 09:05:01	rex_lin_11@hotmail.com	i am talking w vincent now		
2007-03-23 09:05:08	wedetector1@hotmail.com	oh.i see..		
2007-03-23 09:05:36	rex_lin_11@hotmail.com	i send the draft to you first		
2007-03-23 09:05:44	wedetector1@hotmail.com	alrite..thanks...		
2007-03-23 09:05:50	rex_lin_11@hotmail.com	but for the sip part, i need some more days		
2007-03-23 09:06:01	wedetector1@hotmail.com	i see...		
2007-03-23 09:06:06	wedetector1@hotmail.com	no problem...		

WLAN FORBIDDER Features

4. Telnet

The screenshot displays the WLAN FORBIDDER interface. On the left is a 'MENU' sidebar with various protocols listed: POP3 (6), SMTP (7), IMAP (25), FTP (18), MSN (175), ICQ (1), YAHOO (7), VOIP (4), HTTP (1941), HTTP (DYNAMIC) (6), WEBMAIL (117), WEBMAIL (SENDE), TELNET (14), QQ (1), P2P (8641), SEARCH, ALARM, EXPORT, MANAGE, and LOGOUT. The main area shows 'Hard Disk Information : - 55G / Used - 2.5G / Available - 49G / Available (%) - 95%'. Below this is a table of Telnet connections:

NO.	DATE / TIME↑	ACCOUNT	PASSWORD	SERVER	FILE NAME
1.	2007-04-11 15:16:50			140.112.90.72	FILE NAME
2.	2007-04-11 15:16:47			140.112.90.72	FILE NAME
3.	2007-04-04 08:59:34			140.112.90.72	FILE NAME
4.	2007-04-04 08:59:31			140.112.90.72	FI
5.	2007-04-04 08:55:27			140.112.90.72	FI

At the bottom of the table, it says 'Count : 5 , Total : 1 , In page 1 | Rows per page : 20'. A red arrow points to the 'DATE / TIME' header, and another red arrow points to the 'FILE NAME' column with the word 'click' next to it. Large red text 'Date/Time, Account, Password' is overlaid on the table. In the foreground, a 'Telnet Sniffer' window is open, showing a list of captured Telnet packets with details like IP addresses, ports, and data lengths. The window title is 'https://192.168.1.90 - Telnet Sniffer - Microsoft Internet Explorer'. At the bottom of the Telnet Sniffer window, there are buttons for 'Play', 'Fast', 'Copy', and 'Clean'. The status bar at the bottom of the Telnet Sniffer window says 'Applet TelnetPlayerApplet started'.

WLAN FORBIDDER Features

5. FTP

CONDITION : FTP - 192.168.1.78 / ~ /

NO.	DATE / TIME↑	ACCOUNT	PASSWORD	ACTION	FTP SERVER	FILE NAME
1.	2007-02-16 12:10:42	user	111111	DownLoad	192.168.1.68	_image.php
2.	2007-02-16 11:40:47	user	111111	DownLoad	192.168.1.68	_http_search.php
3.	2007-02-16 11:36:52	us	111111	UpLoad	192.168.1.68	ftp.php
4.	2007-02-16 11:36:24	ser	111111	UpLoad	192.168.1.68	ftp.php
5.	2007-02-16	U-er	111111	UpLoad	192.168.1.68	ftp.php
6.	2007-02-16	user	111111	UpLoad	192.168.1.68	ftp.php
7.	2007-02-16 11:33:28	user	111111	DownLoad	192.168.1.68	_ftp_search.php
8.	2007-02-16 11:33:28	user	111111	DownLoad	192.168.1.68	_ftp_search.php
9.	2007-02-16 11:33:28	user	111111	DownLoad	192.168.1.68	_ftp_search.php
10.	2007-02-16 11:32:28	user	111111	UpLoad	192.168.1.68	ftp.php
11.	2007-02-03 14:31:02	alluser	jmyohxbc	UpLoad	192.168.1.68	ftp.php
12.	2006-11-06 09:46:09	alluser	jmyohxbc	DownLoad	192.168.1.68	ftp.php
13.	2006-11-06 09:46:01	alluser	jmyohxbc	DownLoad	192.168.1.68	ftp.php
14.	2006-11-06 09:45:53	alluser	jmyohxbc	DownLoad	192.168.1.68	ftp.php
15.	2006-11-06 09:45:45	alluser	jmyohxbc	UpLoad	192.168.1.68	ftp.php
16.	2006-11-06 09:45:36	alluser	jmyohxbc	UpLoad	192.168.1.68	ftp.php

Date/Time, IP, Port, Transfer Tool, Transferred File Name,...etc.

File Download

Do you want to open or save this file?

Name: FTP_FILE_NQ5Rsf.pdf
Type: Adobe Acrobat Document, 138KB
From: 202.39.29.30

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. [What's the risk?](#)

WLAN FORBIDDER Features

6. P2P (Kazaa, Bittorent, Limewire etc.)

CONDITION : P2P - 192.168.1.26 / ~ /

No.	DATE/TIME↑	PORT	P-IP	P-PORT	TOOL	FILENAME	ACTION	HASH
1.	2007-04-04 09:20:50	1471	210.201.1.122	7484	Foxy 1.9.0.0	MTV 金在元-韩剧-情敌(完整版).asf	UPLOAD	I6GQGZXYIX
2.	2007-04-04 09:15:17	1397	10.201.1.122	7484	Foxy 1.9.0.0	MTV 金在元-韩剧-情敌(完整版).asf	UPLOAD	I6GQGZXYIX
3.	2007-03-29 15:32:04	498	20.229.223.97	5807	Foxy 1.9.0.0	Foxy v1.9.0.OKAV Traditional Chinese Setup.exe	UPLOAD	F2E3ODXYTM
4.	2007-03-29 11:43:44	328	20.229.223.97	5807	Foxy 1.9.0.0	Foxy v1.9.0.OKAV Traditional Chinese Setup.exe	UPLOAD	F2E3ODXYTM
5.	2007-03-29 11:25:13	955	22.229.223.97	5807	Foxy 1.9.0.0	Foxy v1.9.0.OKAV Traditional Chinese Setup.exe	UPLOAD	F2E3ODXYTM

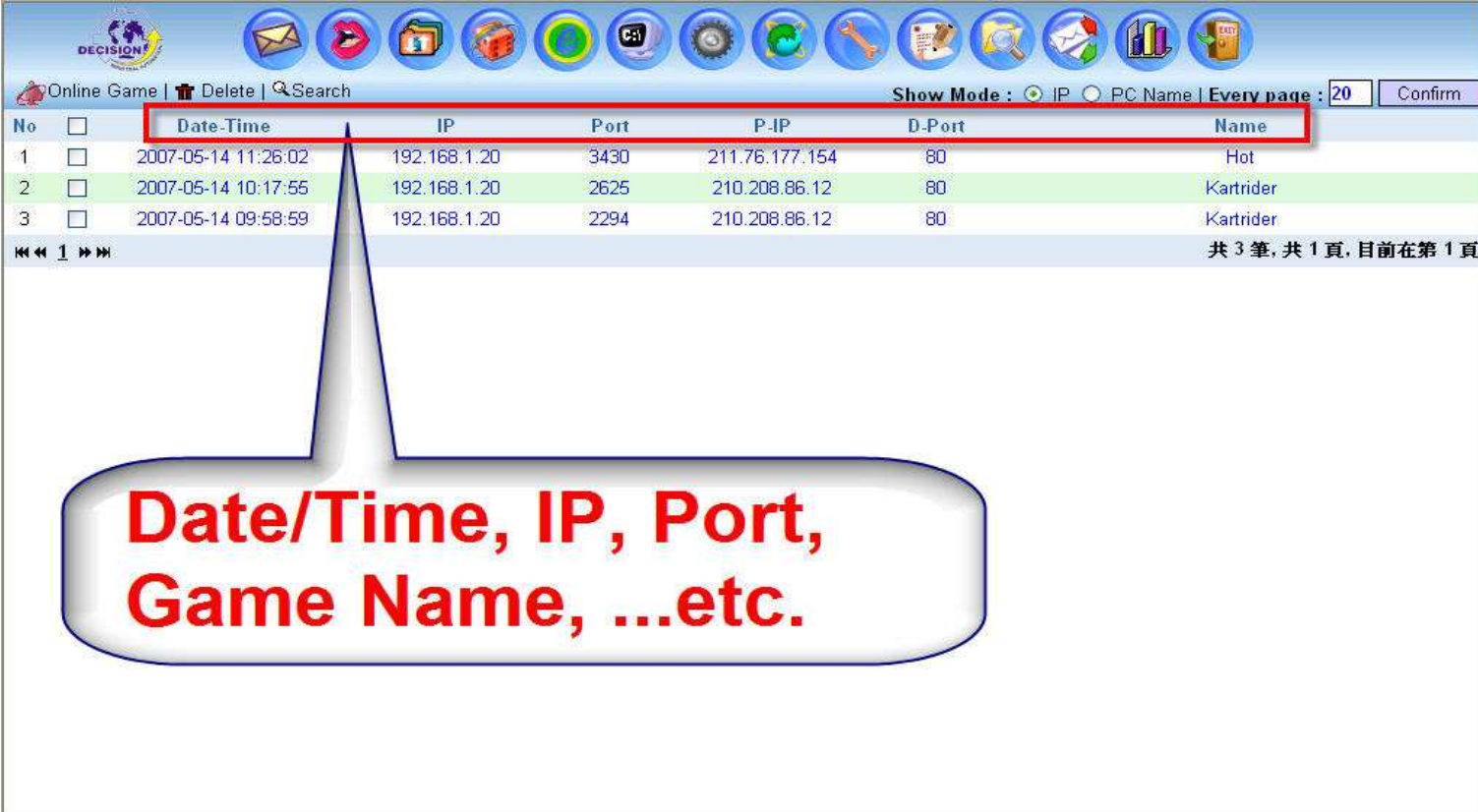
Count : 5 , Total : 1 , In page 1 | Rows per page : 20 Submit

Date/Time, IP, Port, Transfer Tool, Transferred File Name,...etc.

Data Mining

WLAN FORBIDDER Features

6. Online Games (Hot, Kartrider, Ragnarok etc.)



Online Game | Delete | Search

Show Mode : ☒ IP ☐ PC Name | Every page : 20 Confirm

No	<input type="checkbox"/>	Date-Time	IP	Port	P-IP	D-Port	Name
1	<input type="checkbox"/>	2007-05-14 11:26:02	192.168.1.20	3430	211.76.177.154	80	Hot
2	<input type="checkbox"/>	2007-05-14 10:17:55	192.168.1.20	2625	210.208.86.12	80	Kartrider
3	<input type="checkbox"/>	2007-05-14 09:58:59	192.168.1.20	2294	210.208.86.12	80	Kartrider

共 3 筆, 共 1 頁, 目前在第 1 頁

Date/Time, IP, Port, Game Name, ...etc.



Frequently Asked Questions

1. Why WLAN Forbidder?

WLAN Forbidder system is used to protect your Wireless network from external assault as well as to prevent insides wireless STA from accidentally connect to outside Opened Wireless network and loss the confidential information without any notice. Besides, all Internet traffic using Wireless can be archive in the server system for future reference if there is any legal issues.

2. Who should use WLAN Forbidder?

Security concerned organizations such as Government agencies and ministries, banking and finance, university and research centers, enterprises and SMEs that would want to prevent leakage of information through WLAN.



**YOUR Revolutionary Technology for Surveillance and
Audit of Internet Activities!!**

**Our
Awards!**



**World
Recognition!**

Thank You!!!

Decision Computer - All rights reserved
2007

