

Chris Phillips

From: DakotaPro [support@dakotacom.net]
Sent: Thursday, October 09, 2008 3:37 PM
To: cphillips@dakotapro.biz
Subject: DakotaPro.biz Security Report for Gateway Demo_Unit_1.DakotaCom



DakotaPro.biz Security Report for Gateway Demo_Unit_1.DakotaCom

Thank you for using DakotaPro.biz Managed Security Services.

This report allows you to track suspicious and illegal activities which were blocked by your firewall.

Feedback or questions? For feedback, questions, changing your account details or unsubscribing from this report, please reply to this email message.

General Information

Owner Information :

Gateway:

Demo_Unit_1.DakotaCom

Description:

Demo Unit 1

MAC Address:

00:08:da:57:18:84

Firmware Version:

8.0.24x

Last Connection:

October 08, 2008

Report Period:

Sep 29, 2008 - Oct 05, 2008

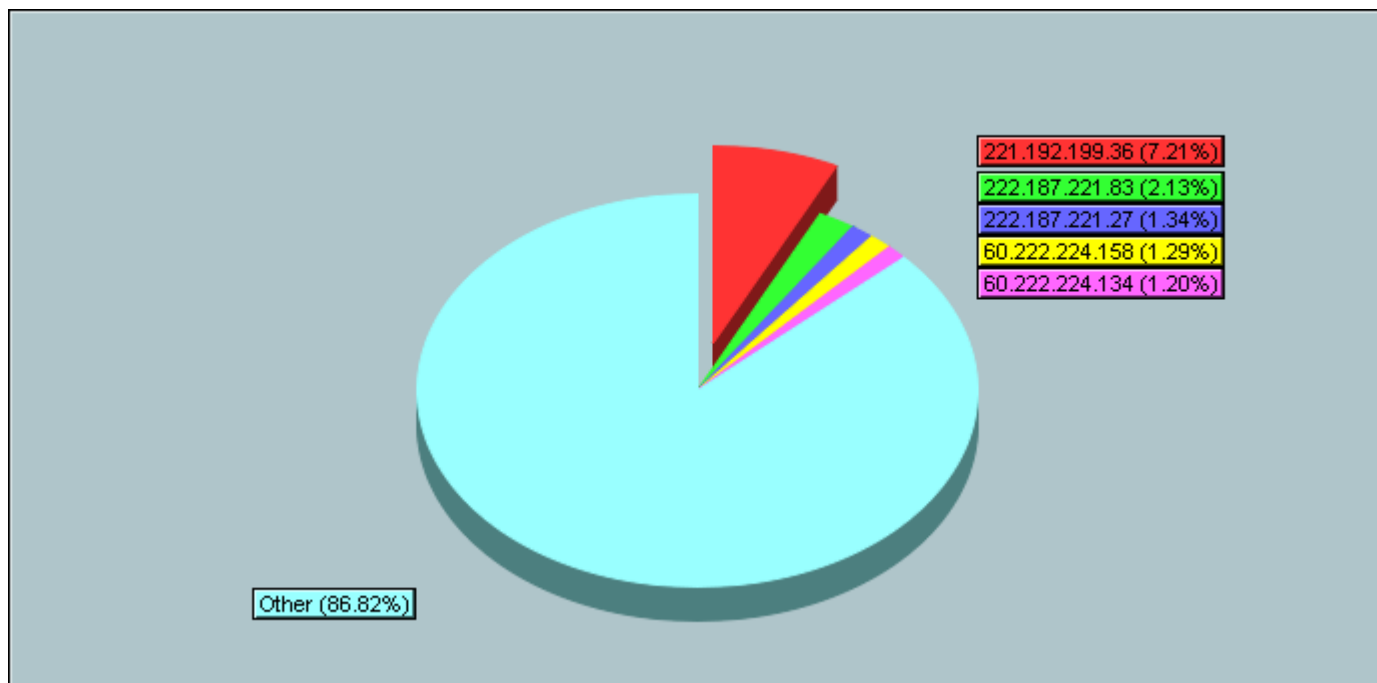
In this Report

Type	Count
1. Blocked Attacks	2,163
2. Blocked Attacked Services	2,163
3. Blocked Outgoing Connections	2
4. Blocked Connection Attempts by Reason	11
5. Blocked Web Sites	0
6. Allowed Web Sites	0
7. Viruses Blocked by Email Filtering Service	0
8. Connections Blocked by VStream Antivirus	4
9. Potential Spam Detected	0
10. Device Updates	0

1. Blocked Attacks

This report shows the top computers which have tried to illegally access your computers and were successfully blocked by the firewall. Click on the IP address to get more information about the identity of the suspected attacker.

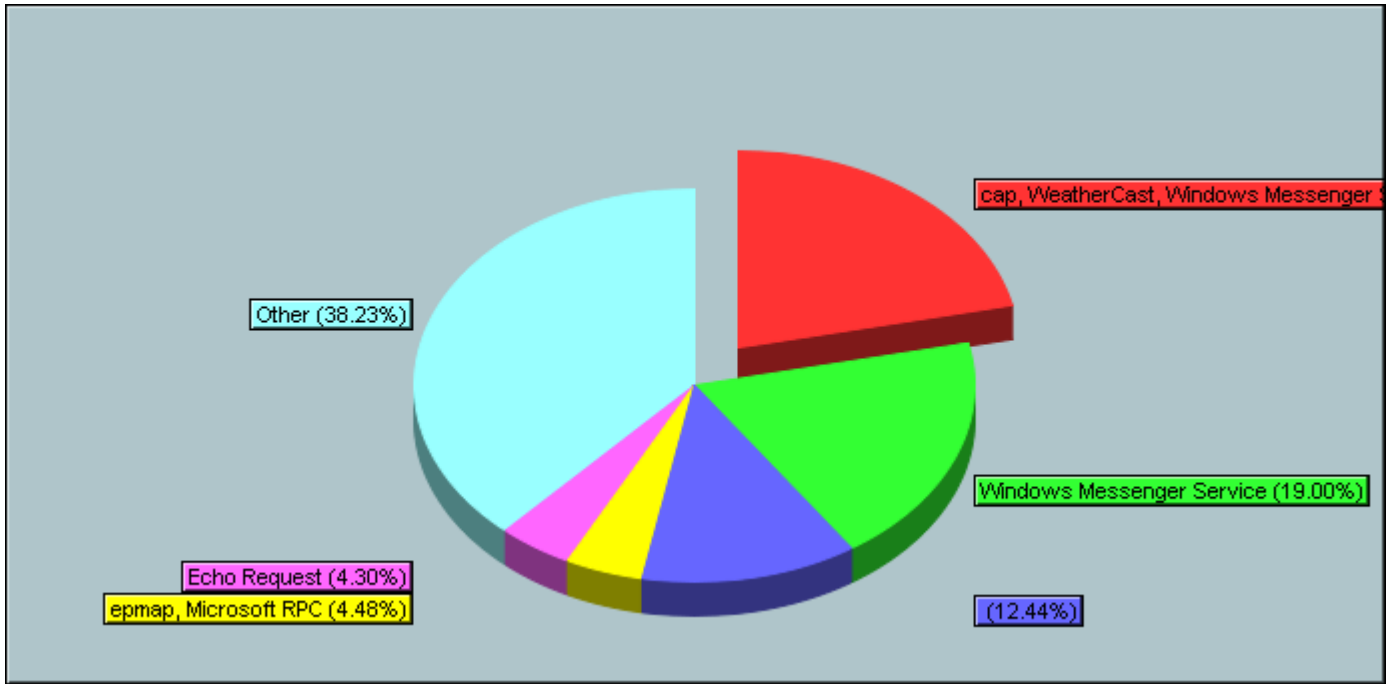
Source IP	Count
221.192.199.36	156
222.187.221.83	46
222.187.221.27	29
60.222.224.158	28
60.222.224.134	26
Other	1,878



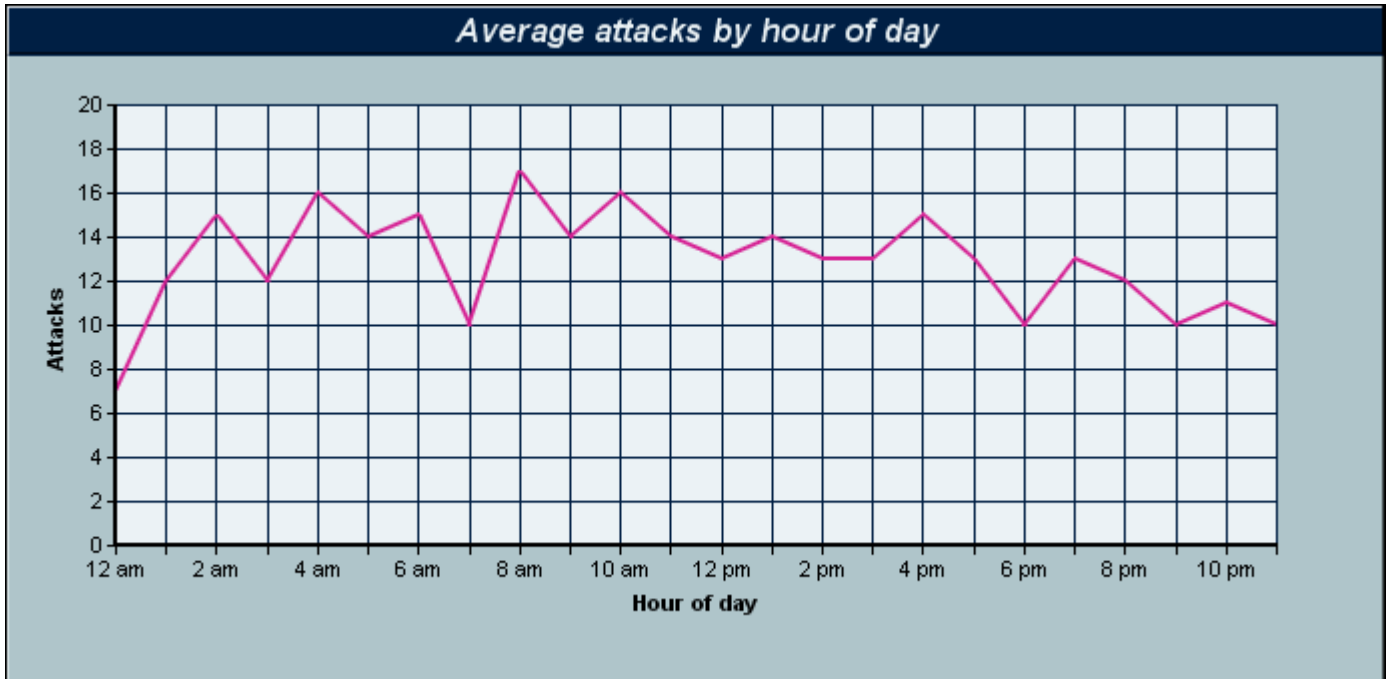
2. Blocked Attacked Services

This report shows the top services to which attackers have illegally attempted to gain access. All these attempts were successfully blocked by your firewall. Click on the Port to get more information about the identity of the service.

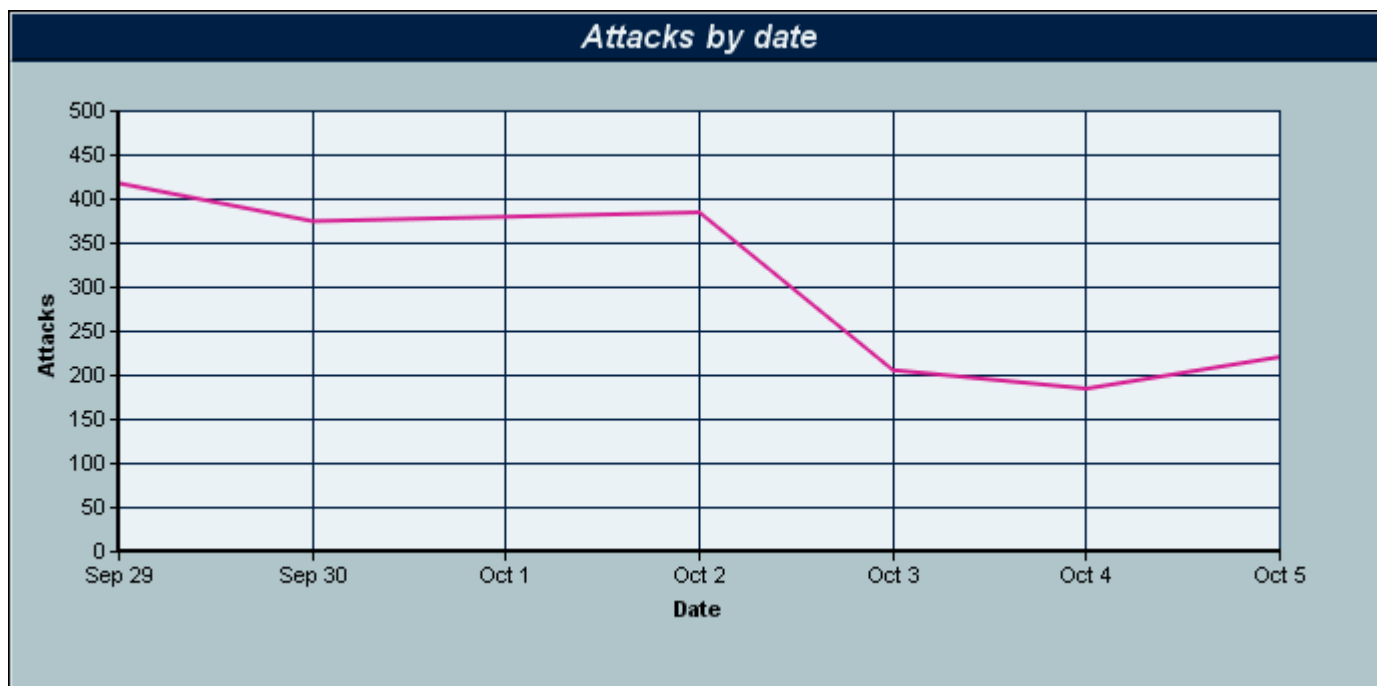
Service	Protocol	Port	Count
cap, WeatherCast, Windows Messenger Service, Windows Messenger Service	UDP	1026	466
Windows Messenger Service	UDP	1027	411
	UDP	1028	269
epmap, Microsoft RPC	TCP	135	97
Echo Request	ICMP	8	93
Other			827



This graph shows the average distribution of attack attempts across the day.



This graph shows the distribution of attacks attempts per day over the period of this report.



3. Blocked Outgoing Connections

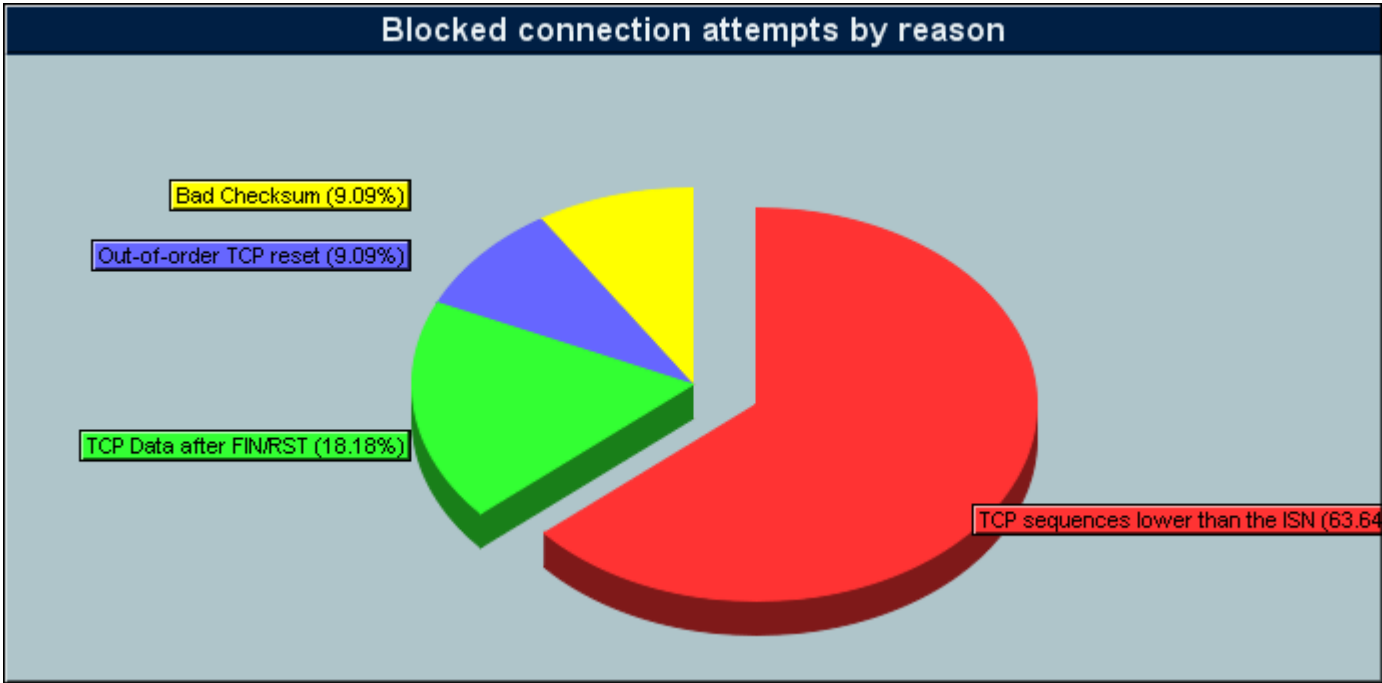
This report shows the top outgoing connections which were blocked by your firewall. Blocked Outgoing Connections may be harmless, or may indicate the possibility of a malicious application (Trojan Horse) existing in your network. Click on the Port to get more information about the identity of the service.

Source IP	Service	Protocol	Port	Count
69.9.31.192	swtp-port2	UDP	9282	1
192.168.1.129	www-http, www, http	TCP	80	1

4. Blocked Connection Attempts by Reason

This report shows the top connections attempts which were blocked by your firewall smartdefense.

Reason	Count
TCP sequences lower than the ISN	7
TCP Data after FIN/RST	2
Out-of-order TCP reset	1
Bad Checksum	1



5. Blocked Web Sites

Not Subscribed

6. Allowed Web Sites

No web sites were allowed

7. Viruses Blocked by Email Filtering Service

Not Subscribed

8. Top Connections Blocked by VStream Antivirus

This report shows the top blocked connections by reason.

Direction	Reason	Count
Inbound	Virus: Exploit.IFrame.Gen-1	2
	Virus: Exploit.W32.MS05-002 (animated avi exploit)	2

This report shows the top services which were blocked by VStream Embedded Antivirus.

Service	Protocol	Port	Source IP	Count
www-http, www, http	TCP	80	192.168.1.126	2
			192.168.1.120	2

9. Potential Spam Detected

Not Subscribed

10. Device Updates

No updates

[Privacy Statement](#)