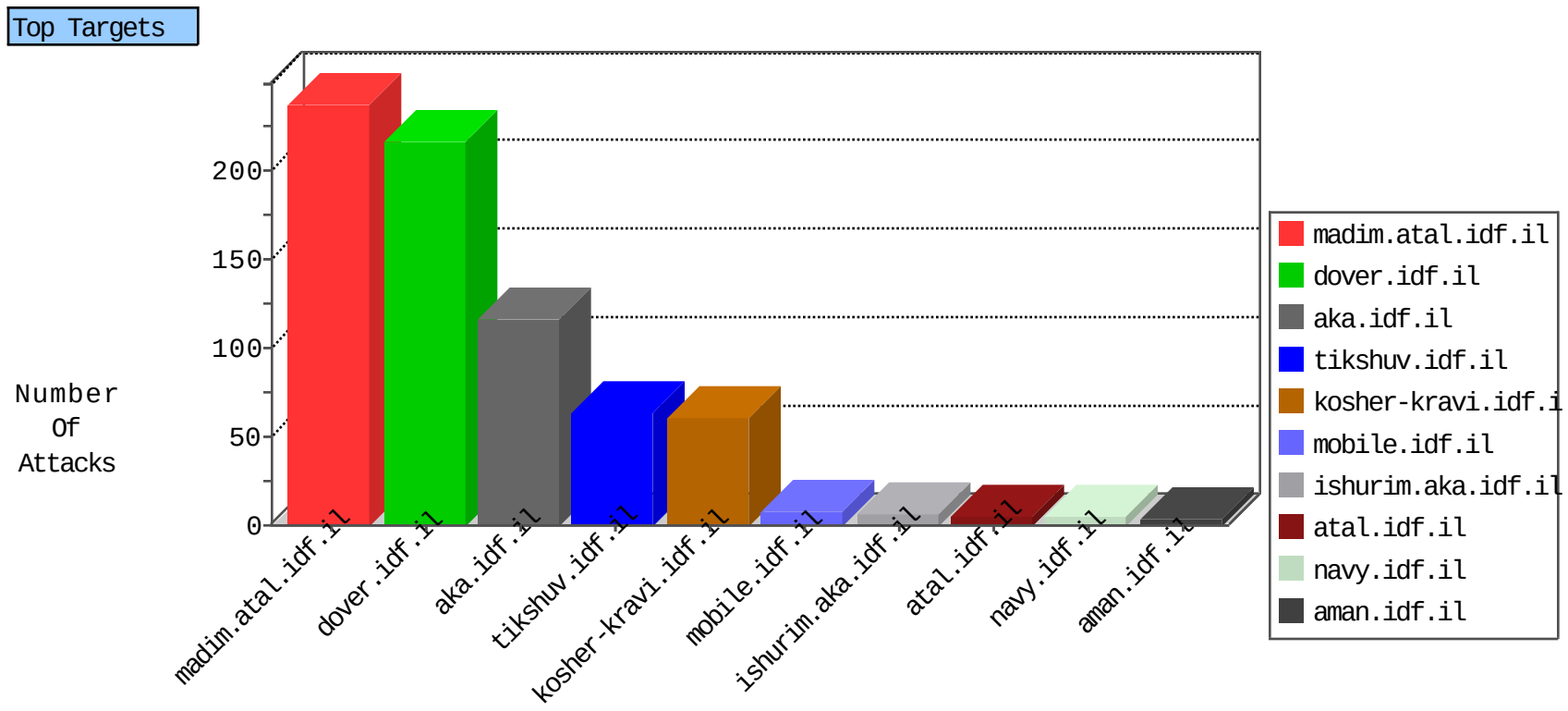
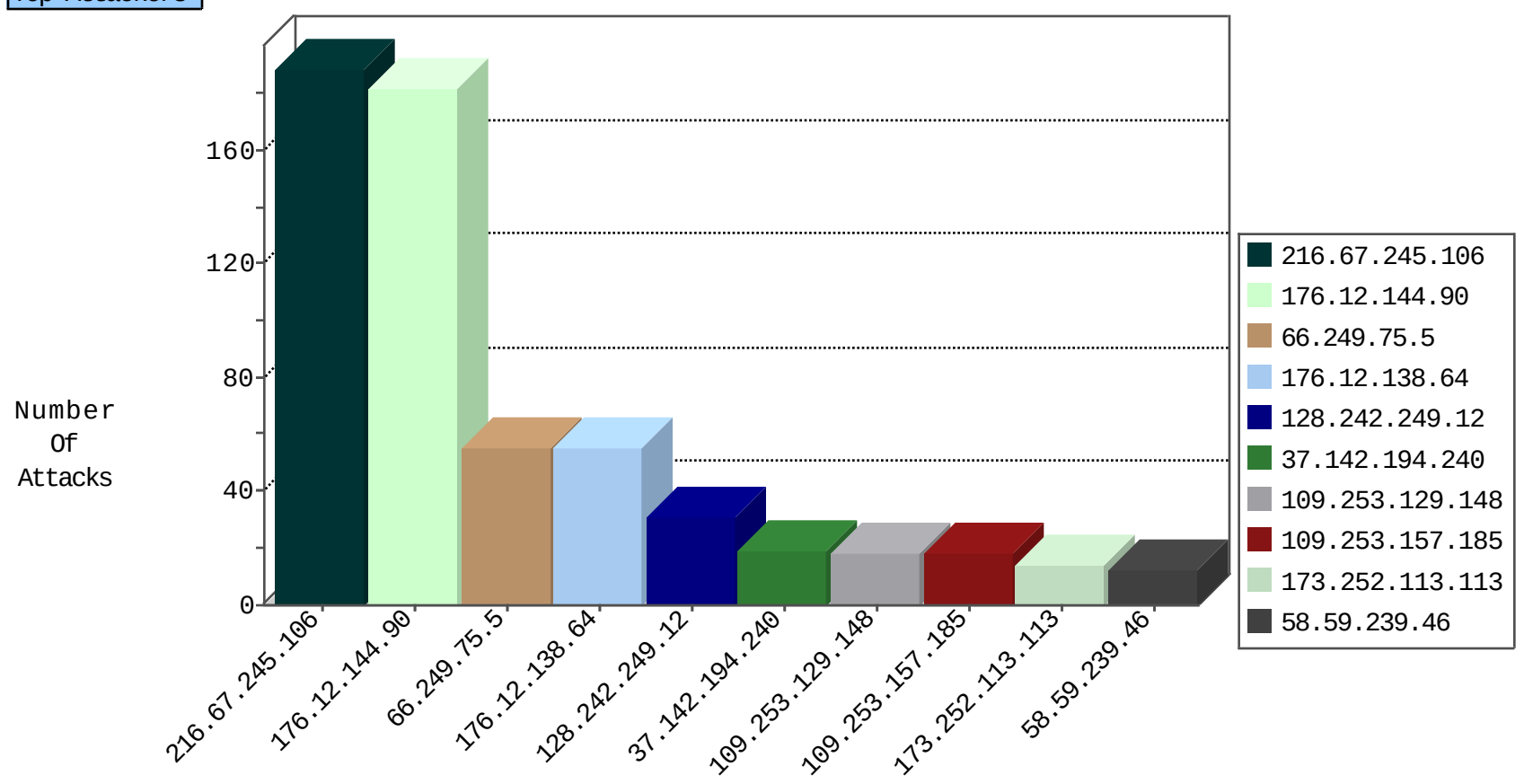
03-28-2015-01:03:09 to 03-28-2015-02:03:09

IDF Under Attack
03-28-2015-01:03:09

Top Targets



Top Attackers



03-28-2015-01:03:09 to 03-28-2015-02:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count

03-28-2015-01:03:09 to 03-28-2015-02:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	31
216.67.245.106	United States	147.237.0.15	kosher-kravi.idf.il	C003: HTTP: phpMyAdmin access	Block	5
216.67.245.106	United States	147.237.0.34	tikshuv.idf.il	C003: HTTP: phpMyAdmin access	Block	5
216.67.245.106	United States	147.237.77.216	dover.idf.il	C003: HTTP: phpMyAdmin access	Block	5
58.59.239.46	China	147.237.72.156	aman.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
58.59.239.46	China	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
58.59.239.46	China	147.237.72.167	ishurim.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
218.66.137.48	China	147.237.72.166	aka.idf.il	C076: HTTP: Access to - action=... (General)	Block	1
85.25.43.94	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1

03-28-2015-01:03:09 to 03-28-2015-02:03:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
216.67.245.106	United States	147.237.77.216	dover.idf.il	Admin login page scan - Havij	27
216.67.245.106	United States	147.237.0.34	tikshuv.idf.il	Admin login page scan - Havij	21
216.67.245.106	United States	147.237.0.15	kosher-kravi.idf.il	Admin login page scan - Havij	21
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
84.95.58.220	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
222.69.94.13	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
122.228.207.77	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
216.67.245.106	United States	147.237.77.216	dover.idf.il	ET WEB_SERVER Muieblackcat scanner	1
122.228.207.77	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
216.67.245.106	United States	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Muieblackcat scanner	1
122.228.207.77	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
216.67.245.106	United States	147.237.0.15	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
122.228.207.77	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
209.31.103.8	United States	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
203.114.104.30	Thailand	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
203.114.104.30	Thailand	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.69.2	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
202.162.210.109	Indonesia	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
122.228.207.77	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

03-28-2015-01:03:09 to 03-28-2015-02:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.75.5	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
37.142.194.240	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	19
109.253.129.148	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.157.185	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
173.252.113.113	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	14
82.102.251.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
173.252.113.118	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
109.253.139.34	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
173.252.113.115	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
173.252.113.116	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
2.54.134.198	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
2.54.134.198	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.121.232.189	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
190.152.130.56	Ecuador	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
173.252.113.112	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
77.237.138.51	Czech Republic	147.237.77.227	e.hamaz.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
46.19.85.159	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	2
173.252.113.119	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.68	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
173.252.113.117	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
109.234.36.176	Russian Federation	147.237.0.35	akaws.idf.il		drop	drop	1
46.116.122.253	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.116.122.253	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
2.54.134.198	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
85.64.108.141	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.19.86.51	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.138.17.205	France	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
85.64.108.141	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.46	United States	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1

03-28-2015-01:03:09 to 03-28-2015-02:03:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.144.90	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.144.90	Block	181
176.12.138.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	55
216.67.245.106	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 216.67.245.106	Block	33
216.67.245.106	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 216.67.245.106	Block	33
216.67.245.106	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 216.67.245.106	Block	33
109.253.139.250	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
207.46.13.113	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.113	Block	4
134.249.140.212	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
218.66.137.48	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	2
66.249.73.193	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
157.55.39.2	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/captcha.ashx	Block	2
79.181.192.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
216.67.245.106	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/muieblackcat	Block	1
46.116.250.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter captcha in aka.idf.il/main/giyus/authenticationservice.asmx/authenticate	None	1
180.76.4.226	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
218.66.137.48	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 218.66.137.48	Block	1
66.249.75.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/120203-2.stm	Block	1
157.55.39.130	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
79.182.35.19	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.69.2	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
180.76.5.194	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/1075-he/tikshuv.aspx	Block	1
134.249.140.212	Ukraine	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/giora.stm	Block	1
37.237.124.64	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//qar/	Block	1
207.46.13.113	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1039-he/dover.aspx	Block	1
82.102.251.11	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.102.251.11	Block	1
216.67.245.106	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/muieblackcat	Block	1
66.249.69.86	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
134.249.140.212	Ukraine	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 134.249.140.212	Block	1
69.171.230.114	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//qar/	Block	1
218.66.137.48	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/account/signup/	Block	1
37.239.248.37	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	Block	1
207.46.13.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1620-15785-he/dover.aspx	Block	1
176.12.144.90	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
82.102.251.11	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20187-he/dover.aspx)	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-13158-he/dover.aspx	Block	1
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.140.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/lomdim/forum/	Block	1
216.67.245.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/muieblackcat	Block	1
66.249.73.201	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/unitfs.asp	Block	1

03-28-2015-01:03:09 to 03-28-2015-02:03:09