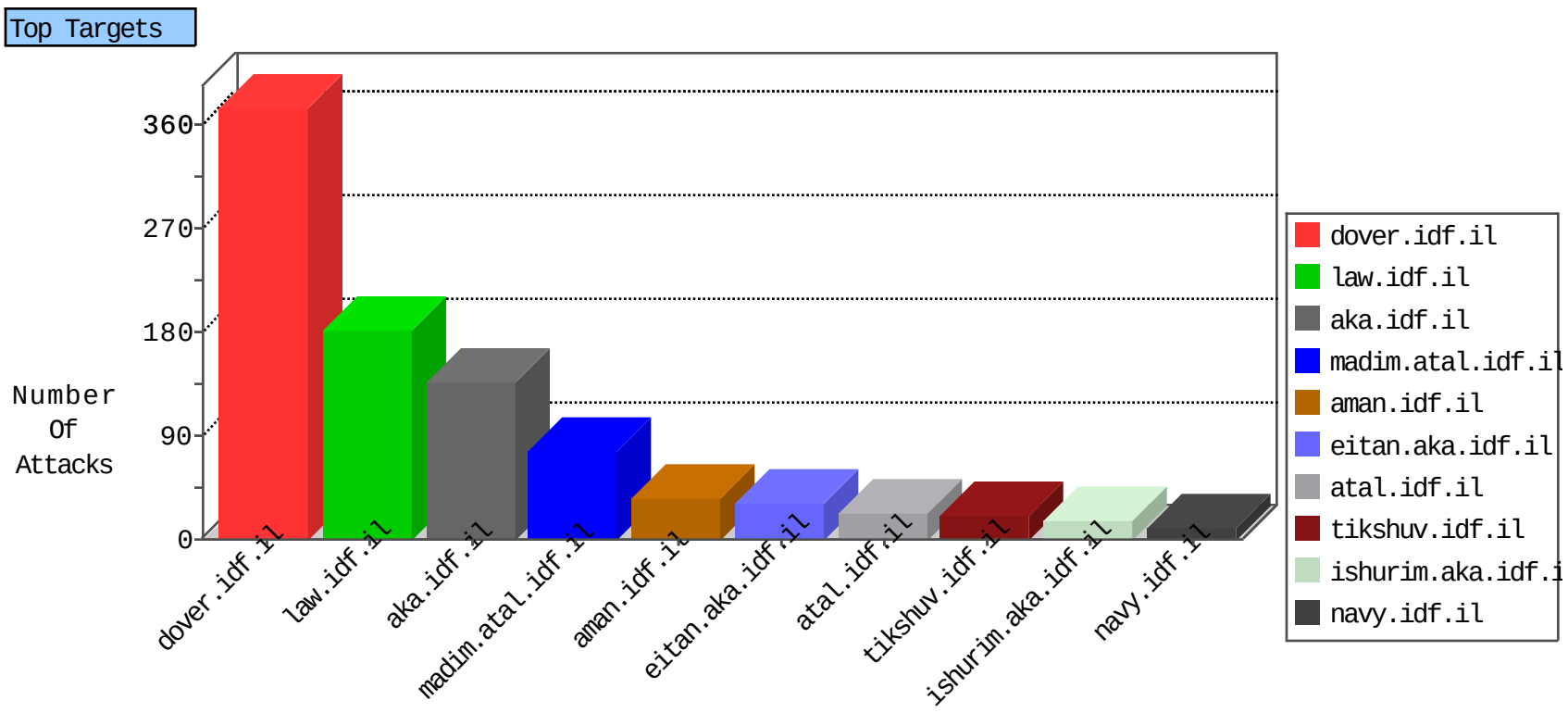
04-23-2016-23:04:09 to 04-24-2016-00:04:09

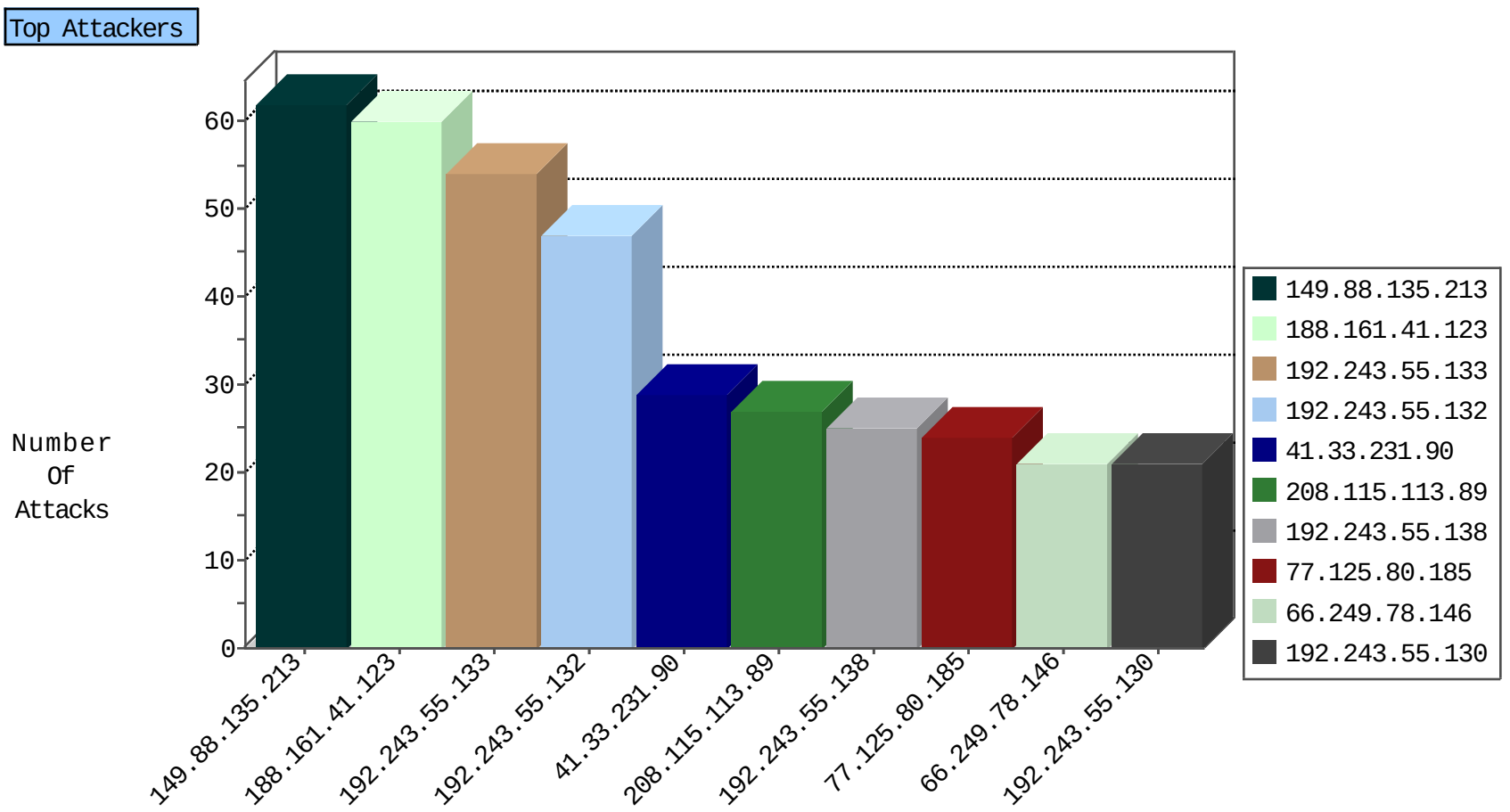
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-23-2016-23:04:09 to 04-24-2016-00:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3132
2.53.16.119	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2697
79.178.147.23	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
69.30.202.229	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
46.116.171.208	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.130.5.99	Lithuania	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.99	Lithuania	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.99	Lithuania	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
74.91.17.179	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
94.102.52.10	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.99	Lithuania	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
74.91.23.106	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1

04-23-2016-23:04:09 to 04-24-2016-00:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-23-2016-23:04:09 to 04-24-2016-00:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
31.44.139.72	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.249.66.18	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
23.96.109.87	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
5.196.199.232	147.237.77.216	France	dover.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.77.233	United States	atal.idf.il	ET DROP Dshield Block Listed Source	1
23.96.109.87	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
23.96.109.87	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1

04-23-2016-23:04:09 to 04-24-2016-00:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.161.41.123	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
77.125.80.185	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
89.13.123.96	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.85.47	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
212.179.212.215	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.179.214.113	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
212.179.214.113	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
188.120.154.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
149.78.35.12	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
66.102.9.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.121.25.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.138	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
188.120.154.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
79.181.29.134	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
141.0.12.26	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.19.221.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
196.217.244.191	Morocco	147.237.76.86	navy.idf.il	drop		drop	4
79.182.26.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.135.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
37.236.132.112	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.236.132.112	Block	14
2.53.166.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
109.253.207.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.64.86.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.182.21.157	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
149.88.79.78	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
2.55.137.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.97.116	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
69.30.202.229	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.qeqe11.com/	Block	1
207.46.13.162	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
37.236.132.112	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
109.67.141.82	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
80.246.130.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/resources/images/icons/favicon.png	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69051.pdf	Block	1
5.1.106.123	Iraq	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
107.170.20.192	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 107.170.20.192	Block	1
74.91.17.179	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to www.gege1.com/	Block	1
38.111.147.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 208.115.113.82	Block	1
80.246.136.246	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19666-he/idfgdover.aspx	Block	1
157.55.39.135	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
5.1.106.123	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/login.php	Block	1
107.170.20.192	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/14-he	Block	1
77.237.138.202	Czech Republic	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
46.19.85.98	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
212.76.103.209	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/newsflash/mobile	Block	1
141.0.15.21	Norway	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
84.109.1.219	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/default.aspx	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
31.44.139.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
109.64.16.14	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.126.45	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
52.16.137.212	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
149.50.7.54	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.55.137.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct in www.aka.idf.il/main/sachar/	None	1
85.65.109.18	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.230.45	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
188.120.134.13	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1