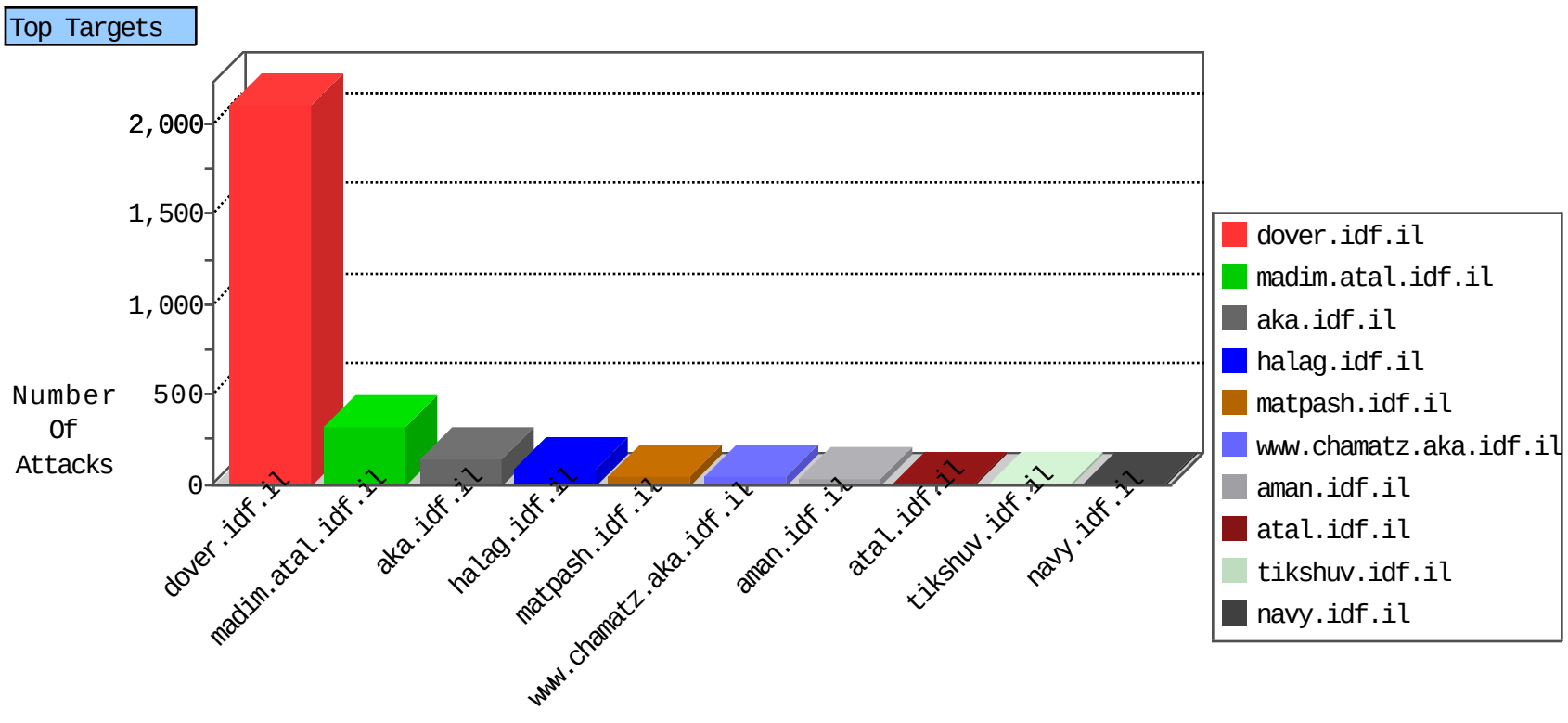
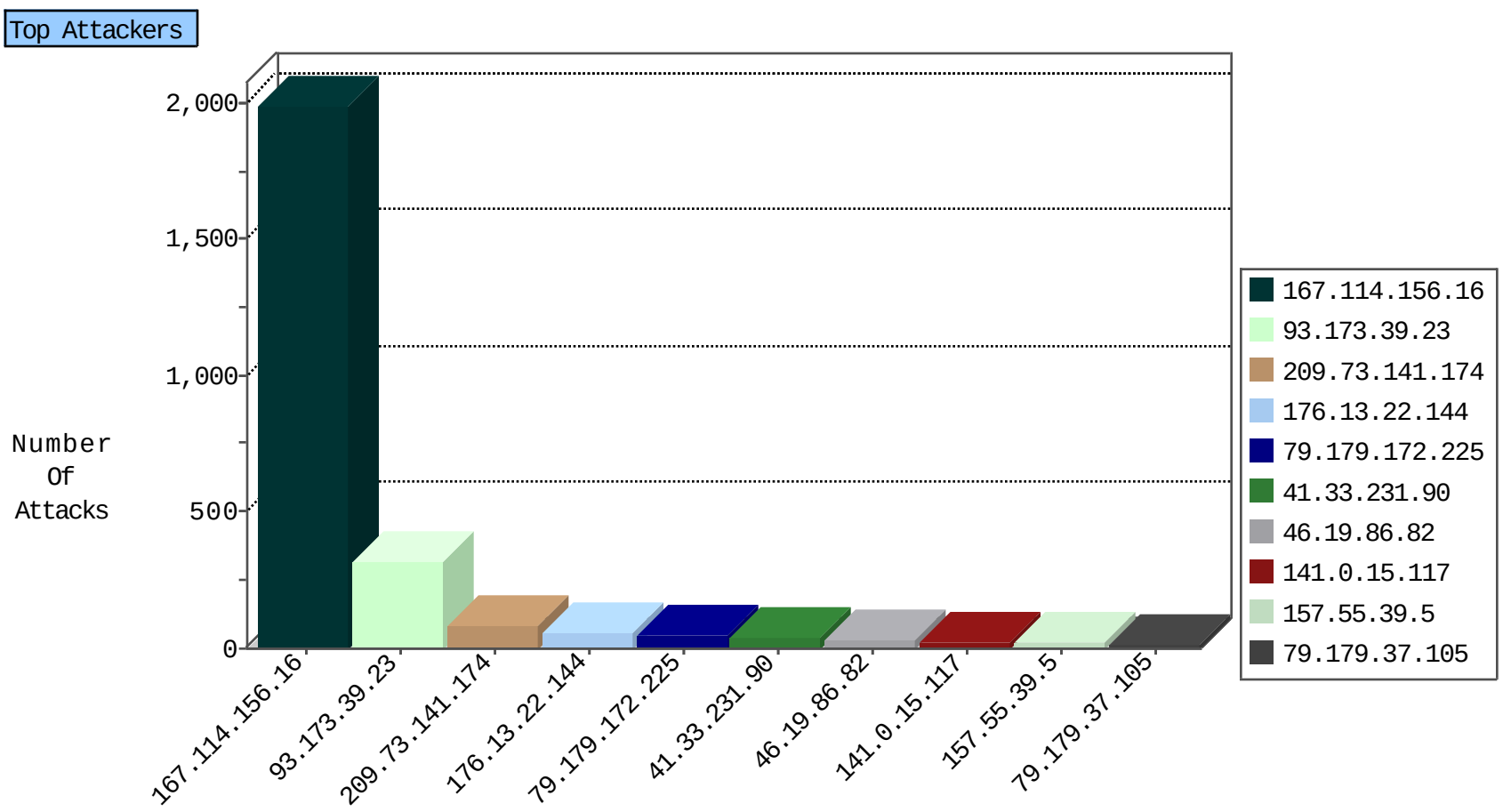
12-07-2015-00:04:00 to 12-07-2015-01:04:00

IDF Under Attack Daily Report





12-07-2015-00:04:00 to 12-07-2015-01:04:00

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	DOS-Tool-SwitchbladG	dest-reset	3338
115.230.124.164	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
192.0.78.26	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
192.0.78.26	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
115.239.228.8	China	147.237.0.19	madim.atal.idf.il	Frk_Under_Attack_Con_Http	drop	1
192.0.78.26	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
79.179.172.225	Israel	147.237.72.166	aka.idf.il	Invalid L4 Header Length	drop	1
115.239.228.8	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Http	drop	1
192.0.78.26	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
81.1.188.198	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

12-07-2015-00:04:00 to 12-07-2015-01:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-07-2015-00:04:00 to 12-07-2015-01:04:00

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	4
66.249.79.6	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
74.117.209.135	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.64	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
60.29.182.175	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
60.29.182.175	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
203.197.205.118	147.237.77.233	India	atal.idf.il	ET SCAN NMAP -sS window 1024	1
60.29.182.175	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
203.197.205.118	147.237.76.30	India	himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.146.220.220	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.91	147.237.76.42		refuah.idf.il	ET SCAN NMAP -sS window 1024	1
81.169.251.74	147.237.0.34	Germany	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
74.117.209.135	147.237.76.30	United States	himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
60.29.182.175	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
60.29.182.175	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
203.197.205.118	147.237.77.233	India	atal.idf.il	ET SCAN NMAP -sS window 3072	1
60.29.182.175	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
203.197.205.118	147.237.76.30	India	himush.idf.il	ET SCAN NMAP -sS window 3072	1
60.29.182.175	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.33	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
74.117.209.135	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

12-07-2015-00:04:00 to 12-07-2015-01:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.22.144	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	58
209.73.141.174	Anonymous Proxy	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	48
79.179.172.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	42
209.73.141.174	Anonymous Proxy	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
157.55.39.5	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
141.0.15.117	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
46.19.86.82	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
46.19.86.82	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.86.82	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
77.125.114.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
77.127.101.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.138.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
77.127.203.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.103	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.37.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.179.37.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
40.77.167.8	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.130.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
46.19.86.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.196.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.17.31.222	Switzerland	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.130.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
213.57.130.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.176.65.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.7.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.126.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.193.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.102.254.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.166.120.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
79.179.172.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.81.209	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.11.41.106	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
133.130.54.151	Japan	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.75	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
176.13.7.105	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
5.11.41.106	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
73.149.111.49	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.88.74.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.111	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

12-07-2015-00:04:00 to 12-07-2015-01:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
104.172.207.143	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
81.17.31.222	Switzerland	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.39.23	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 93.173.39.23	Block	199
93.173.39.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
176.12.143.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.65.32.118	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/sip_storage/files/8/size220x0/2128.jpg	Block	2
213.139.52.71	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 213.139.52.71	Block	2
213.139.52.71	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 213.139.52.71	Block	2
109.64.57.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.17.31.222	Switzerland	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
213.139.52.71	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 213.139.52.71	Block	2
46.121.214.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.7.105	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
107.178.195.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
31.168.208.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
149.78.38.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1521-en/kkkkkkk=ffd3c736kkkkkkk_ffd3c736	Block	1
107.178.195.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.178.100.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.60.41.95	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewir8ydfqcjjahwmbxqkhf9qbwaqfggnmaa&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	1
212.201.82.49	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.196	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdf×³Â¦×³×ŸÂ¿Â½×³Â?-×³×ŸÂ¿Â½×³×ŸÂ¿Â½×³Â¦×³×ŸÂ¿Â½×³×ŸÂ¿Â½	Block	1
87.69.155.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19369-he/idfgdover.aspx	Block	1
2.54.47.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.179.37.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.139.52.71	Jordan	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 213.139.52.71	Block	1
66.249.65.37	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
2.54.190.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.167	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.179.125.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.22	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
176.13.2.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
67.212.175.138	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/yohalan/main/main.asp	Block	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1

12-07-2015-00:04:00 to 12-07-2015-01:04:00