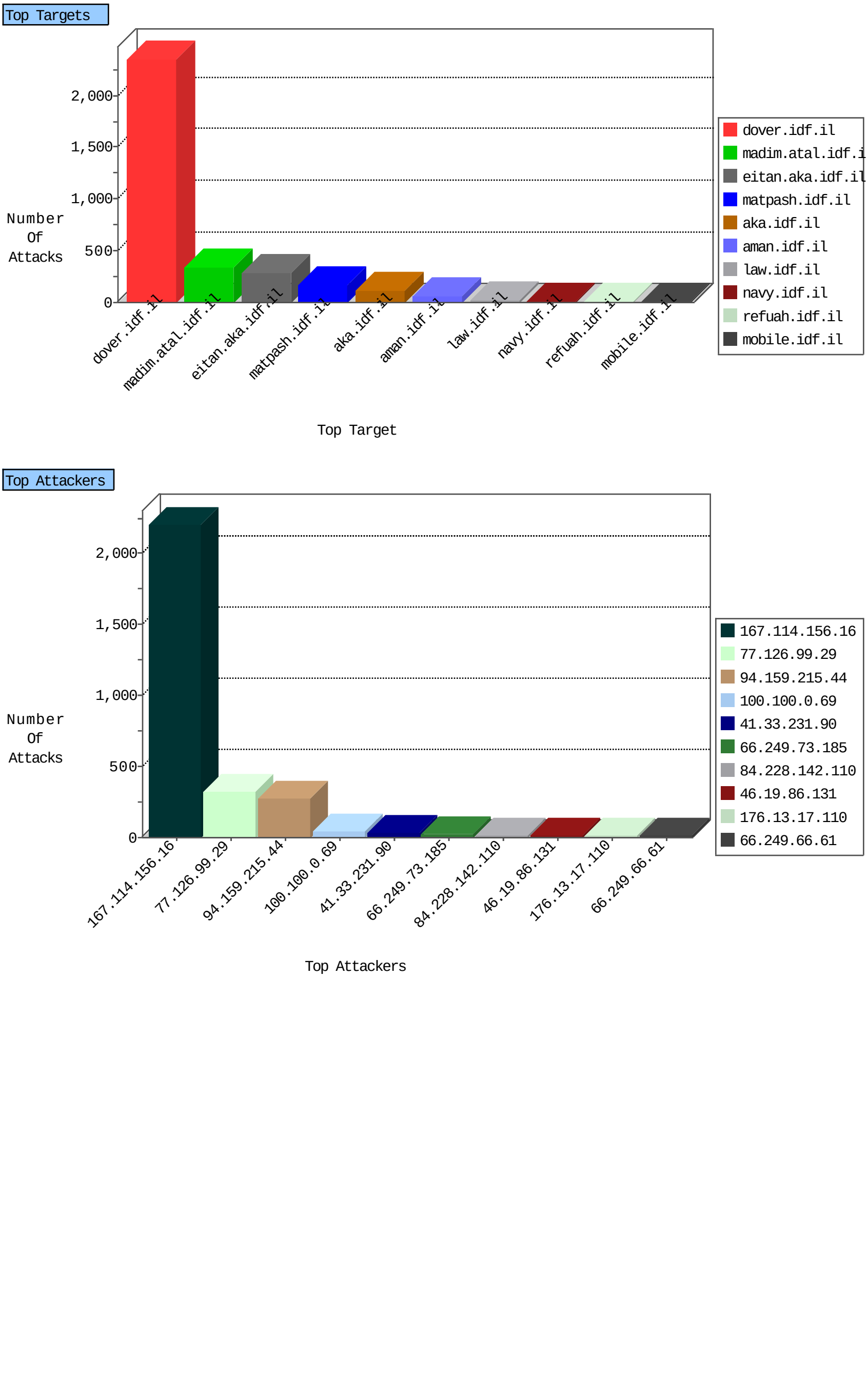
11-28-2015-09:04:07 to 11-28-2015-10:04:07

IDF Under Attack
Daily Report



11-28-2015-09:04:07 to 11-28-2015-10:04:07

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	3651
93.158.203.169	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.68	Switzerland	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
93.158.203.169	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
93.158.203.169	Netherlands	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

11-28-2015-09:04:07 to 11-28-2015-10:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.60	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.79	France	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-28-2015-09:04:07 to 11-28-2015-10:04:07

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
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.130	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
2.54.5.89	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
204.151.29.209	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
119.73.228.130	147.237.72.156	Singapore	aman.idf.il	ET SCAN NMAP -sS window 3072	1
204.151.29.209	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1

11-28-2015-09:04:07 to 11-28-2015-10:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
100.100.0.69		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
100.100.0.69		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
49.180.163.147	Australia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.159.215.44	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.171	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.182.173.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.142.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.142.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.230.86.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.173.227	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.64.214.64	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.247.36.110	Netherlands	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
85.64.214.64	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
78.46.5.136	Germany	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
79.180.168.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.147.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.215.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
78.46.7.81	Germany	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
79.181.57.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.142.224	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
78.47.17.5	Germany	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
85.65.149.70	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.34.163.163	Palestinian Territory, Occupied	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
79.182.26.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
119.81.64.59	Singapore	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
213.57.142.224	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.38.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
103.14.203.170	Australia	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	3
77.126.99.29	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.203.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.142.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
104.237.50.194		147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
87.68.51.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.65.0.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.17	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.131.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
179.43.147.207	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
76.164.208.98	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
100.100.46.73		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

11-28-2015-09:04:07 to 11-28-2015-10:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.159.215.44	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 94.159.215.44	Block	264
77.126.99.29	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 77.126.99.29	Block	175
77.126.99.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
77.126.99.29	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 77.126.99.29	Block	39
176.13.17.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
5.61.253.39	Netherlands	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
111.67.11.193	Australia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
193.169.188.230	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
176.106.227.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
74.120.220.114	Canada	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
213.57.49.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
96.30.56.141	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
217.199.164.217	United Kingdom	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
77.74.51.87	Netherlands	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
198.57.209.102	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
109.169.50.31	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
216.167.200.171	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
50.87.165.17	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
198.46.82.33	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
213.202.223.160	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
31.193.8.36	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
197.85.182.58	South Africa	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
75.98.175.92	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
185.11.164.14	Portugal	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
162.144.210.204	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
37.230.102.197	Netherlands	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
195.62.28.15	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
74.220.215.244	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
128.65.127.231	Italy	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
195.35.83.187	Sweden	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
74.220.207.112	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
87.106.179.206	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
79.182.108.167	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	2
195.62.28.15	United Kingdom	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 195.62.28.15	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
195.35.83.187	Sweden	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 195.35.83.187	Block	2
54.159.50.242	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
162.144.210.204	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
87.106.179.206	Germany	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 87.106.179.206	Block	2
193.169.188.230	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 193.169.188.230	Block	2
74.220.215.244	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.php	Block	2
176.106.227.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
74.120.220.114	Canada	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 74.120.220.114	Block	2
2.54.38.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
74.220.207.112	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
111.67.11.193	Australia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
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	2
77.74.51.87	Netherlands	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 77.74.51.87	Block	2
198.57.209.102	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 198.57.209.102	Block	2

11-28-2015-09:04:07 to 11-28-2015-10:04:07