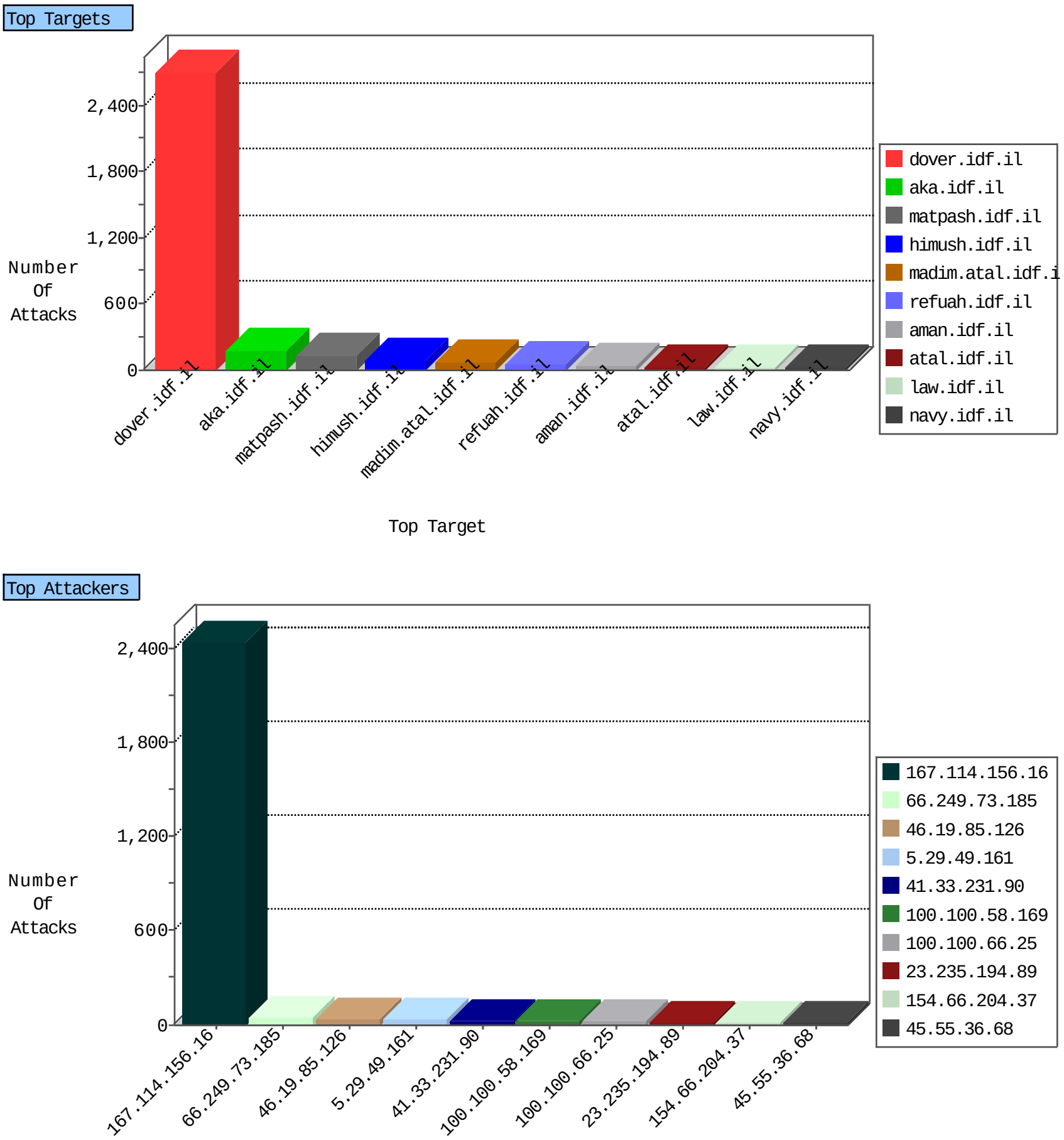
11-28-2015-00:04:05 to 11-28-2015-01:04:05

IDF Under Attack Daily Report



11-28-2015-00:04:05 to 11-28-2015-01:04:05

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	3671
66.249.66.1	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	137

11-28-2015-00:04:05 to 11-28-2015-01:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.188.43.181	Russian Federation	147.237.72.166	aka.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	2

11-28-2015-00:04:05 to 11-28-2015-01:04:05

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
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
94.102.48.195	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.32	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.172.71.252	147.237.77.233	Ukraine	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.56.32	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.127.207.216	147.237.0.200		m4u.idf.il	ET SCAN NMAP -sS window 4096	1
45.127.207.216	147.237.0.200		m4u.idf.il	ET SCAN NMAP -f -sS	1
115.182.17.13	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
111.93.198.54	147.237.8.46	India	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.195	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.216.3.114	147.237.72.166	Russian Federation	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
222.186.56.32	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.172.71.252	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.56.32	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.172.71.252	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.32	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.127.207.216	147.237.0.200		m4u.idf.il	ET SCAN NMAP -sS window 2048	1
115.182.17.13	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
115.182.17.13	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
104.192.0.226	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

11-28-2015-00:04:05 to 11-28-2015-01:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
100.100.58.169		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
100.100.66.25		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
46.116.110.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.186.228.29	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.186.228.57	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.154.92.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.8.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.214.188.214	Sweden	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
31.154.92.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.186.228.93	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.100	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.186.228.59	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
31.186.228.95	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.230.86.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.18.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.144	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.48.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.164.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.17		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.17.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.229.173.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.210.132.21	Netherlands	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
66.249.73.201	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.91	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
176.13.15.125	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.66.5	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.102.254.85	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.180.136.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
173.252.122.116	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.102.254.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
173.252.122.122	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
31.186.228.31	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
109.64.197.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
212.14.239.10	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
2.54.156.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

11-28-2015-00:04:05 to 11-28-2015-01:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.212.122.116	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
5.29.49.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	36
2.52.53.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
37.142.158.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
79.182.170.142	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
85.250.105.56	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
45.55.36.68		147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
104.237.50.194		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
188.40.52.182	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
50.62.176.26	United States	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	3
81.95.96.134	Czech Republic	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	3
94.126.71.156	Netherlands	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
173.247.248.14	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
223.27.20.235	Australia	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	3
23.235.194.89	United States	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	3
103.16.181.44	New Zealand	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
45.55.36.68		147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	3
81.95.96.134	Czech Republic	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 81.95.96.134	Block	3
195.62.28.15	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
45.55.36.68		147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 45.55.36.68	Block	3
94.23.12.182	France	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	3
173.230.131.89	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
217.199.164.217	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
23.235.194.89	United States	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	3
69.174.52.11	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
45.55.36.68		147.237.0.15	kosher-kravi.idf.il	Distributed PHP Attempt	Block	3
208.93.111.60	United States	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	3
103.16.181.44	New Zealand	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
192.145.239.21	United States	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	3
23.235.194.89	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 23.235.194.89	Block	3
5.153.225.110	United Kingdom	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	3
68.171.222.114	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
103.16.181.44	New Zealand	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 103.16.181.44	Block	3
87.195.106.39	Netherlands	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
162.242.152.71	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
216.172.180.60	United States	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	3
95.138.183.172	United Kingdom	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	3
116.12.55.118	Singapore	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
189.91.32.59	Brazil	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
50.62.176.26	United States	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	3
154.66.204.37	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
5.153.225.110	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
5.9.207.61	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
95.138.183.172	United Kingdom	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	3
78.46.7.81	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
107.190.137.66	United States	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	3
83.145.194.172	Finland	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
154.66.204.37	South Africa	147.237.76.147	chinuch.aka.idf.il	Distributed PHP Attempt	Block	3
5.61.251.87	Netherlands	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
95.131.251.47	United Kingdom	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	3

11-28-2015-00:04:05 to 11-28-2015-01:04:05