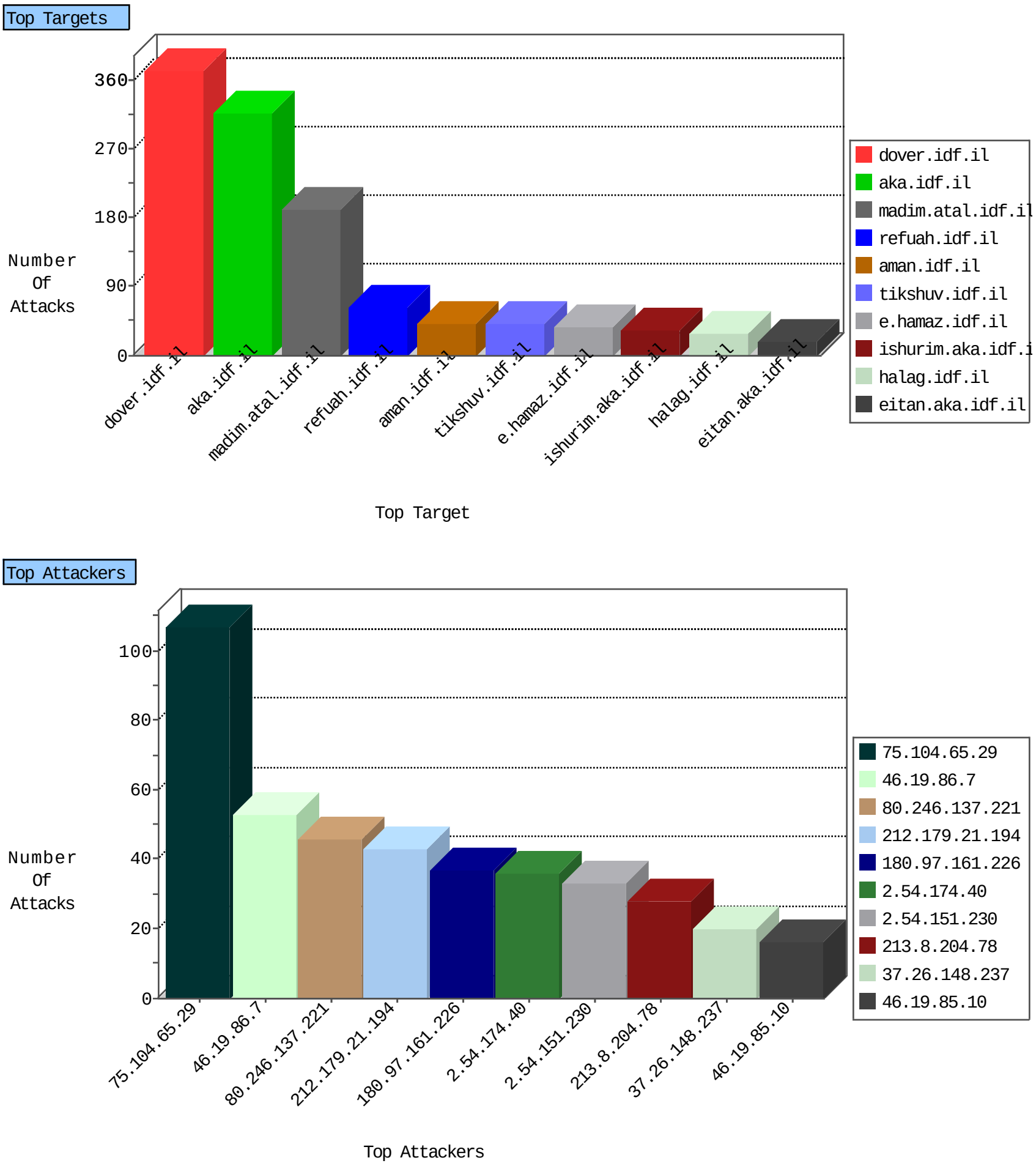
03-06-2016-16:04:01 to 03-06-2016-17:04:01

IDF Under Attack Daily Report



03-06-2016-16:04:01 to 03-06-2016-17:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
180.97.161.226	China	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	37
82.145.209.222	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
31.168.232.150	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	2
108.186.168.25	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
134.147.203.115	Germany	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

03-06-2016-16:04:01 to 03-06-2016-17:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.201.167	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
46.19.86.224	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
84.109.51.239	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
79.179.232.183	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
89.138.185.223	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.46.38.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
89.163.148.58	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.120.231.235	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
84.108.136.222	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
49.246.230.40	China	147.237.77.74	law.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
10.0.0.3		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
196.206.218.186	Morocco	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
94.230.93.24	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
5.29.243.29	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
94.230.93.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-06-2016-16:04:01 to 03-06-2016-17:04:01

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	2
212.179.155.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
185.55.217.55	147.237.77.216	Spain	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.51.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.17.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
12.28.51.140	147.237.76.42	United States	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
132.77.69.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
118.112.185.236	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
104.215.89.20	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
84.228.70.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.116.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.110.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.97.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.91.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.125.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.169.77.218	147.237.77.216	South Africa	dover.idf.il	ET SCAN NMAP -sS window 3072	1
167.220.196.184	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.242.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.68.49.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.215.89.20	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
85.250.182.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.21.181	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.109.2.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.151.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.134.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.50	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1

03-06-2016-16:04:01 to 03-06-2016-17:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
75.104.65.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
213.8.204.78	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
212.179.21.194	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
85.65.0.210	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
176.13.18.17	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
204.12.251.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
109.64.196.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.53	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.174.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.250	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
213.8.204.78	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
46.19.85.175	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.135.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
109.64.99.35	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
109.253.135.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
89.138.179.30	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.174.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.174.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.174.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.195.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.94	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.142.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.57.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.57.201	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.96	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.66.37.144	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
77.126.68.90	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.135.102.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.174.40	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	4
2.54.174.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
62.219.141.121	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
192.115.83.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.179.60.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.88.124.148	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.67.113.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.199.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.117.101.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.26.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
75.104.65.29	United States	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 75.104.65.29	Block	58
46.19.86.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
80.246.137.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
2.54.151.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
37.26.148.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
80.246.136.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.150.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
93.173.58.141	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	8
188.162.65.21	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
8.37.234.15	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
176.13.16.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.161.9.12	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
188.162.65.21	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.162.65.21	Block	5
82.102.136.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
46.161.9.12	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.161.9.12	Block	5
109.253.143.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.38	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	4
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.159.199.92	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.94.119.188	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
62.128.48.46	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.149.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
104.130.141.191	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 104.130.141.191	Block	2
162.243.109.121	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.109.121	Block	2
176.13.9.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.35.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
70.39.184.226	Satellite Provider	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
212.143.122.5	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
52.34.92.215	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
41.41.135.53	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.179.118.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.149.169	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/xmlrpc.php	Block	1
124.13.28.167	Malaysia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
107.182.230.72	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.66.15	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.66.15	Block	1
192.116.167.41	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
46.19.86.98	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
176.13.11.235	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.120.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.65.109.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
70.39.184.226	Satellite Provider	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
94.230.93.48	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
41.41.135.53	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
149.88.124.148	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.39.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/67906.pdf&sa=u&ved=0ahukewie37_6oqzlahwfb5okhq3dcuwqfggimaa&usg=afqjcnekfq4mo22t0gxa5ab010dusronwg	Block	1
132.74.1.4	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/110630.pdf	Block	1