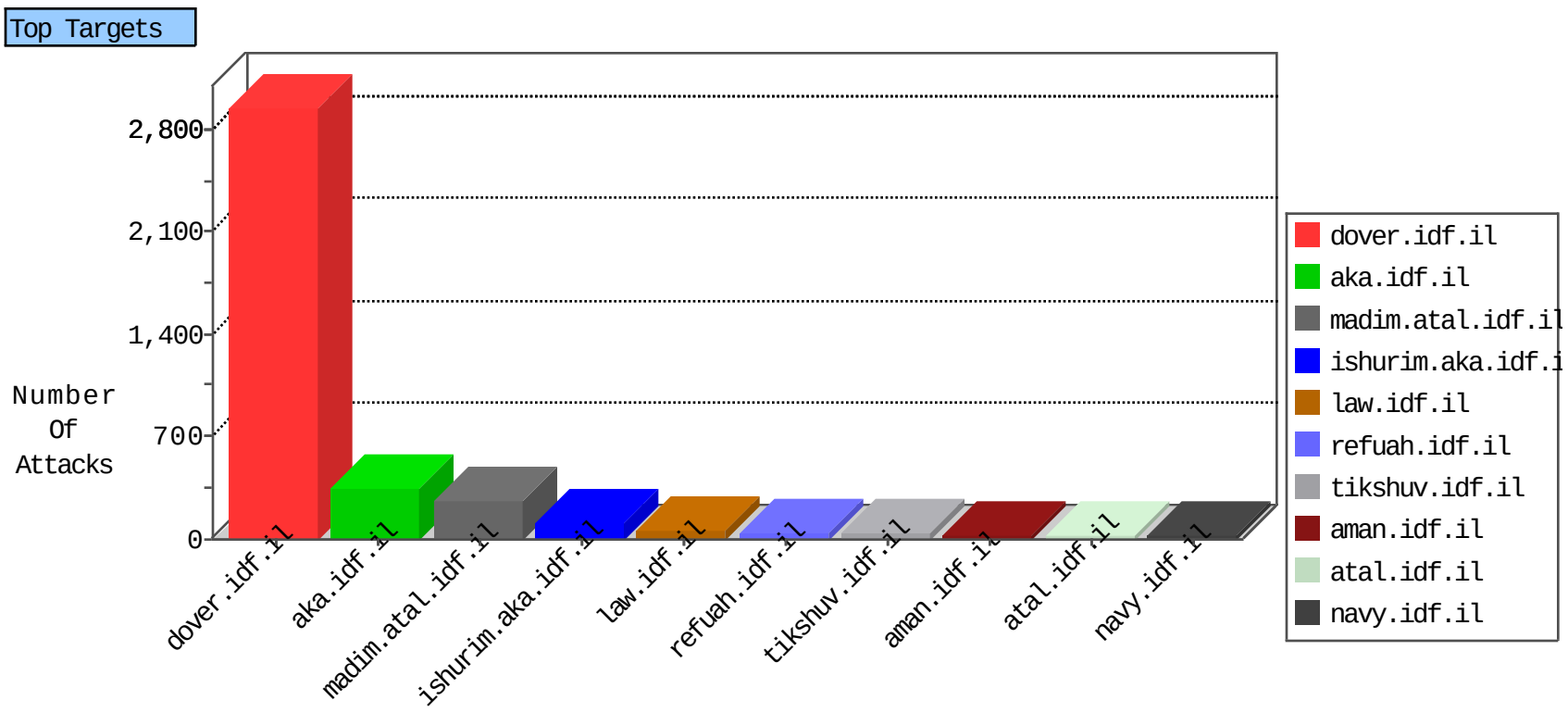
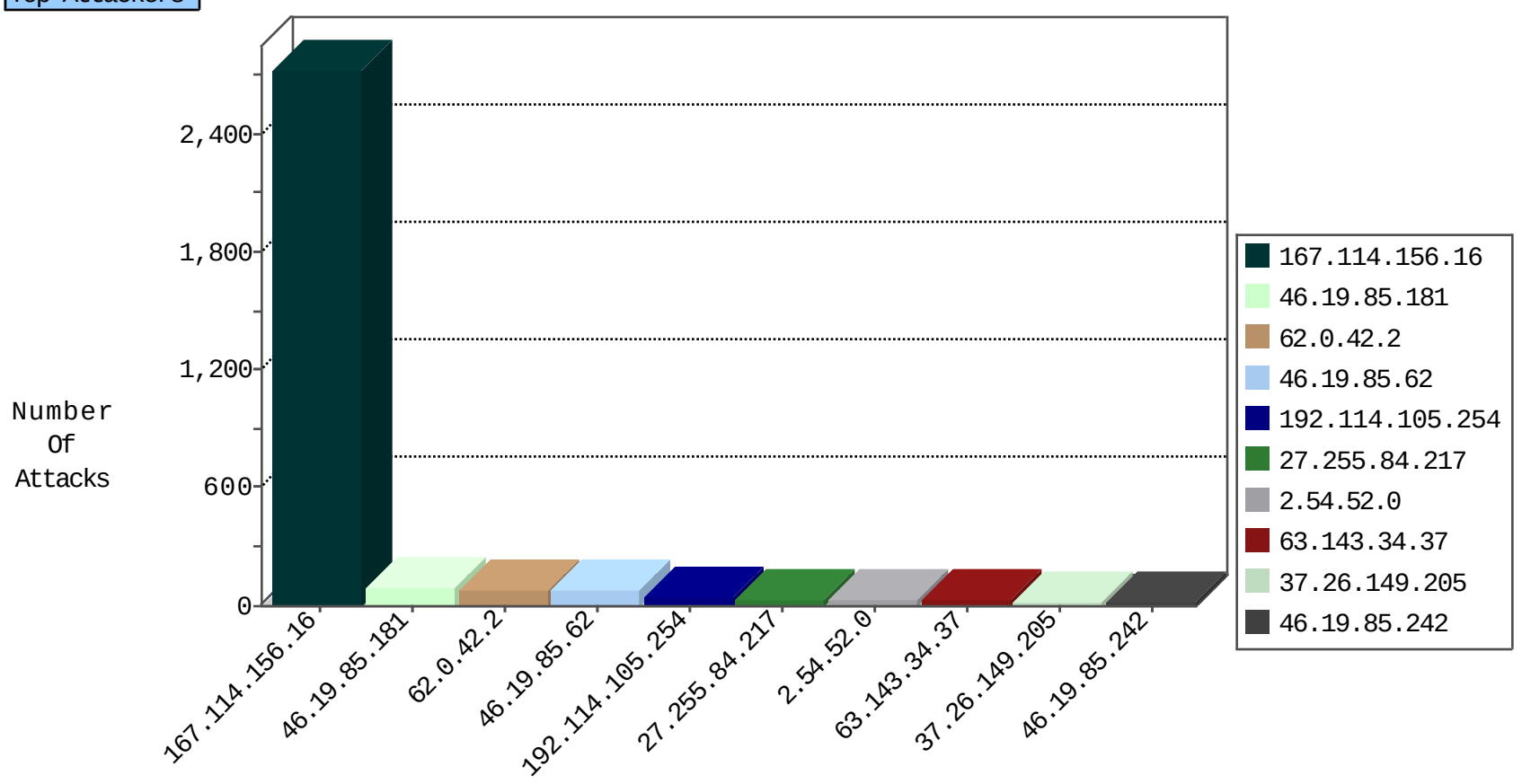
03-15-2016-11:04:03 to 03-15-2016-12:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-15-2016-11:04:03 to 03-15-2016-12:04:03

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	3520
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.1.74	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
104.255.66.38		147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

03-15-2016-11:04:03 to 03-15-2016-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.106.100	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
46.116.210.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
63.143.34.37	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
5.29.245.195	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
177.185.194.92	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
91.219.122.4	Poland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
91.219.122.4	Poland	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
66.135.63.82	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
200.59.205.238	Argentina	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
63.143.34.37	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
158.85.253.245	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
66.96.128.60	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
2.54.139.199	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
176.13.20.153	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	2
80.246.133.195	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.96.128.60	United States	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
199.30.24.192	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
27.255.84.217	Korea, Republic of	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
158.85.253.245	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-15-2016-11:04:03 to 03-15-2016-12:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.219.122.4	147.237.77.74	Poland	law.idf.il	SQL Injection - Select From	13
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	10
63.143.34.37	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	9
63.143.34.37	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	9
66.96.128.60	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	8
177.185.194.92	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	7
66.135.63.82	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	5
200.59.205.238	147.237.77.233	Argentina	atal.idf.il	SQL Injection - Select From	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
79.183.53.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.62.53.174	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
195.62.53.174	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.173	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.35.222.17	147.237.77.216	United States	dover.idf.il	ET DOS SSL Bomb DoS Attempt	1
13.71.146.233	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.14.195	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.194.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.9.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
66.249.75.223	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
195.62.53.174	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential SSH Scan	1
195.62.53.174	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Potential SSH Scan	1
45.243.61.22	147.237.77.216	Uruguay	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.24.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1

03-15-2016-11:04:03 to 03-15-2016-12:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	67
62.0.42.2	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	40
62.0.42.2	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	39
37.26.149.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
192.114.105.254	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	17
147.236.30.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
188.72.103.230	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	13
31.154.251.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.130.134	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
37.26.148.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.3.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
89.139.232.244	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
155.254.215.231	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
94.159.170.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.210	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.242	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.139.232.244	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
199.203.176.50	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.210	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.180.197.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.242	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.113.152	Israel	147.237.77.121	e.navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.160	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
193.43.246.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
5.102.195.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.30.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.1.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
87.68.74.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.0.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.131.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.96.128.60	United States	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	3
79.180.221.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-15-2016-11:04:03 to 03-15-2016-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
46.19.85.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
2.54.52.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
27.255.84.217	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 27.255.84.217	Block	26
46.19.85.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.160.166.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
168.235.205.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
46.19.85.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.130.191	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
84.228.16.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	3
213.151.45.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	2
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	2
80.178.122.47	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.16.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
27.255.84.217	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
147.236.30.122	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
197.38.175.202	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
37.26.148.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
197.38.175.202	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
5.29.201.64	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 5.29.201.64	Block	2
80.246.137.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.116.96.192	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
31.168.13.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.142	Israel	147.237.76.42	refuah.idf.il	Distributed Abnormally Long Request	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	NULL Character in URL [[#14]¿sµ“ıı9[[°”#16@צא˙]]2א•ח^-- [[#28]]s[[#0]]Û[[#25]][[©'')ı#18[[]]#28!•˙]]61#[[boiq~]]	Block	1
5.29.201.64	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/901-8008-he/	Block	1
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.75.78.160	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/31/	Block	1
37.26.146.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
31.168.142.114	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
54.193.54.34	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
197.38.175.202	Egypt	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
87.71.56.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
37.26.148.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1133-he/dover.aspx	Block	1
37.26.146.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.112	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.64.32	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list2.htm	Block	1
46.116.120.223	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
31.168.13.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
132.74.58.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/109154.pdf	Block	1
23.81.247.208	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-15-2016-11:04:03 to 03-15-2016-12:04:03